Lookout®

SECURITY RESEARCH REPORT

Mobile APT Surveillance Campaigns Targeting Uyghurs

A collection of long-running Android tooling connected to a Chinese mAPT actor

June 2020

Contents

Executive Summary

The Lookout Threat Intelligence team has discovered four Android surveillanceware tools, which are used to target the Uyghur ethnic minority group. Our research indicates that these four interconnected malware tools are elements of much larger mAPT (mobile advanced persistent threat) campaigns that have been active for years. Although there is evidence that the campaigns have been active since at least 2013, Lookout researchers have been monitoring the surveillanceware families – SilkBean, DoubleAgent, CarbonSteal and GoldenEagle – as far back as 2015.

The mAPT threat actors behind this activity possess a mobile arsenal containing at least four other Android surveillance tools publicly known as HenBox[1], PluginPhantom[2], Spywaller[3] and DarthPusher[4]. By examining the surveillanceware apps, their signing certificates and supporting command and control (C2) infrastructure, we have discovered connections between these malware tools and the actors behind them which we detail in this report.

Evidence suggests that some of the mAPT activity described in this report is also publicly associated with desktop APT activity in China[5], a theme which is increasingly common with mobile malware tooling.

Lookout researchers have evidence to suggest that while the main target of this activity is indeed the Uyghur ethnic minority in China, these tools have also been used to target Uyghurs living outside China, Tibetans, and Muslim populations around the world.

Titles and in-app functionality suggest targets speak a variety of languages including: Uyghur (in all its four scripts: Arabic, Russian, Uyghur Cyrillic and Chinese), English, Arabic, Chinese, Turkish, Pashto, Persian, Malay, Indonesian, Uzbek and Urdu/Hindi.

The development timeline and targeting of these families also appear to align with Chinese national security directives and "counter-terrorism" efforts as defined by the Chinese government, perhaps suggesting a broader strategic goal behind the campaign. Lookout researchers have observed a peak in malware development beginning in 2015, which coincides with the "Strike Hard Campaign against Violent Terrorism" (严厉打击暴力恐怖活动专项行动) campaign in Xinjiang that began in May 2014, as well as the creation of the National Security Strategic Guidelines, the National Security Law and the Counterterrorism Law in 2015[6].

Additionally, the languages, countries, and services that were observed targeted by the mAPT are in line with China's official list of "26 Sensitive Countries," which according to public reporting, has been used by Chinese authorities as targeting criteria. During our research, we found evidence of at least 14 of the 26 countries being targeted by the malware campaigns discussed in this report.

[1] https://unit42.paloaltonetworks.com/unit42-henbox-chickens-come-home-roost/

[2] https://unit42.paloaltonetworks.com/unit42-pluginphantom-new-android-trojan-abuses-droidplugin-framework/

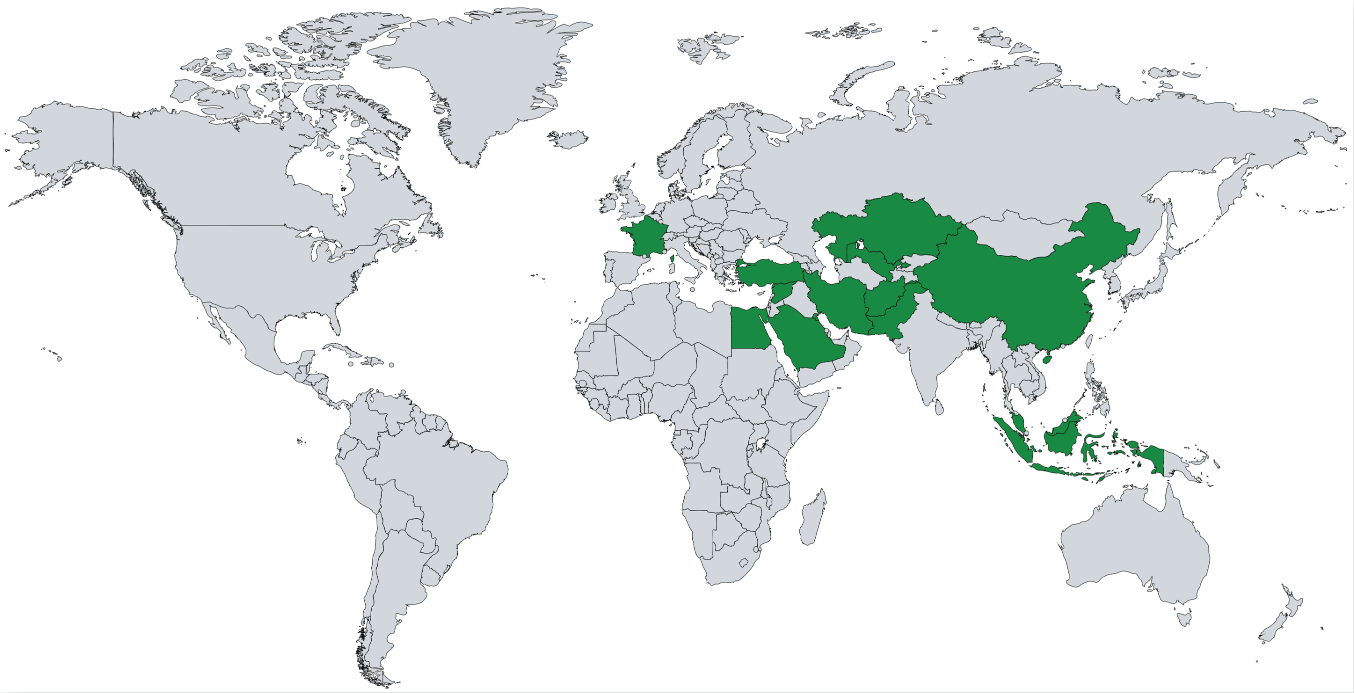
[3] https://blog.lookout.com/spywaller-mobile-threat

[4] https://thehackernews.com/2015/03/Xiaomi-Mi-4-malware.html

[5] https://www.fireeye.com/blog/threat-research/2014/09/forced-to-adapt-xslcmd-backdoor-now-on-os-x.html

[6] https://www.uscc.gov/sites/default/files/Research/Chinas%20Response%20to%20Terrorism_CNA061616.pdf

[7] https://www.hrw.org/report/2018/09/09/eradicating-ideological-viruses/chinas-campaign-repression-against-xinjiangs

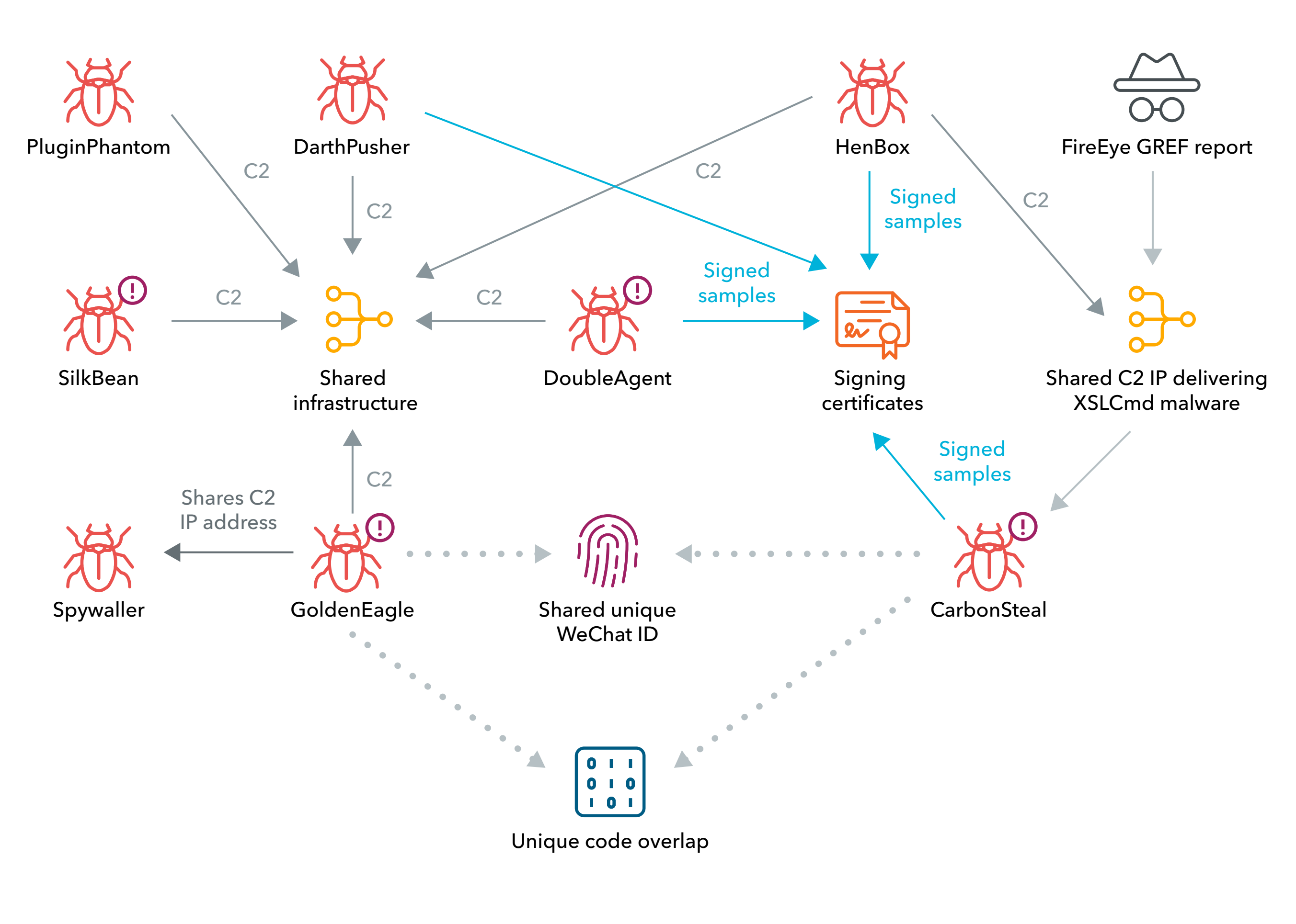


Map showing the countries targeted by the mAPT activity discussed in this report.

A sample of DoubleAgent has previously been reported to target the Tibetan people[8] and evidence found in our investigation suggests the surveillanceware classified as GoldenEagle may also target the same group. While SilkBean is a relatively small and targeted family for Uyghur individuals, shared infrastructure between SilkBean and DoubleAgent suggests that the two are operated by the same actor and have been for many years. That same infrastructure has also been seen communicating with samples of the malware families CarbonSteal, HenBox, PhantomPlugin, Spywaller and DarthPusher.

Users of the Lookout mobile security products are protected from all these threats. According to our data, none of the malicious apps covered by this report here were available on Google Play.

[8] https://citizenlab.ca/2013/04/permission-to-spy-an-analysis-of-android-malware-targeting-tibetans/



Lookout researchers have connected these four novel and publicly unknown Android surveillance tools together in the ways shown above. The malware activity primarily targets the Uyghur ethnic group. These families share command and control (C2) infrastructure, signer certificates, and overlapping code structure, indicating common developers and much larger ongoing malware campaigns. Some C2 infrastructure is also associated with publicly reported APT activity on the use of the XSLCmd backdoor[9] associated with GREF.

[9] https://www.fireeye.com/blog/threat-research/2014/09/forced-to-adapt-xslcmd-backdoor-now-on-os-x.html

Key Findings

Four new Android surveillanceware tools have been discovered by Lookout.

- The primary aim of these surveillanceware apps is to gather and exfiltrate personal user data to a command and control server.
- The apps fall into four separate malware families, each of which has its own unique data gathering priorities and techniques. We named these families SilkBean, DoubleAgent, CarbonSteal and GoldenEagle.
- Lookout researchers can trace some of the associated infrastructure as far back as 2013, along with changes in tooling.
- These surveillanceware tools have been used in conjunction with previously reported malware families such as HenBox, PluginPhantom, Spywaller and Darth Pusher.

Targets of these malware families are primarily Uyghurs, both in China and around the world, but also include Tibetans and possibly wider Muslim communities.

- Application titles and in-app functionality of the malware samples suggest the targets of all four surveillanceware families are the Uyghur Muslim ethnic minority group, centered in Xinjiang, China. Some applications and C2 domains appear to impersonate third-party Uyghur language app stores and focus on Uyghur-targeted apps and services.
- Evidence suggests Uyghur communities in at least fourteen other countries may also be targeted. Content within malware samples reference local services and news outlets in countries such as Turkey, Syria, Kuwait, Indonesia and Kazakhstan.
- DoubleAgent and GoldenEagle also target Tibetans, inferred from their titles as well as public reporting.[10]
- Application titles have also been seen in at least 10 different languages - Uyghur (in all its four scripts: Arabic, Russian, Uyghur Cyrillic and Chinese), English, Arabic, Chinese, Turkish, Pashto, Persian, Malay, Indonesian, Uzbek and Urdu/Hindi.

All four malware families are connected to each other through shared command and control infrastructure, signing certificates as well as code and target overlap.

- Samples of DoubleAgent, GoldenEagle and SilkBean share C2 infrastructure indicating that the same actor is behind the deployment of these malware tools.
- Infrastructure publicly associated with the actor known as GREF in 2018 has been found to be linked directly to CarbonSteal samples. In past public reporting, GREF has also been referred to as APT15, Ke3chang, Mirage, Vixen Panda and Playful Dragon.
- Overlap of non-compromised signing certificates indicates that a combination of these tools are being used in tandem by a single group of mAPT actors to target Uyghurs and other Muslim populations around the world.

[10] https://citizenlab.ca/2013/04/permission-to-spy-an-analysis-of-android-malware-targeting-tibetans/

SilkBean

Findings

In January 2019, Lookout researchers began investigating SilkBean, a small and targeted Android surveillanceware tool focusing on the Turkic minority ethnic group, the Uyghurs. The malware samples mainly trojanized applications for Uyghur/Arabic focused keyboards, alphabets, and plugins.

A hallmark of SilkBean is the comprehensive RAT (remote access trojan) functionality that allows an attacker to execute over 70 different commands on an infected device. SilkBean is delivered via applications that possess malicious functionality, but mimic titles and icons that a target may want to install. The legitimate app with functionality the user expects is packaged within the malware and installed after SilkBean successfully infects a target device.

Tracking SilkBean throughout 2019 led to the discovery that the actor behind this malware had a much larger Android toolset than was previously thought, and had also perhaps expanded their target group. Malware samples connected by common command and control infrastructure over a number of years suggests that the same group behind the activity of SilkBean was also making use of the malware families known as DarthPusher[11], HenBox[12], PluginPhantom[13] and the next surveillanceware family presented here: DoubleAgent.

The languages used in the titles and in-app content include: Uyghur (in all its four scripts: Arabic, Russian, Uyghur Cyrillic, and Chinese), English, Arabic, Chinese, Turkish, Pashto, Persian, Malay, Indonesian, and Urdu/Hindi. Locations referenced in these titles also point to individuals living in or visiting countries such as Syria, Kuwait, Indonesia and Turkey. Many topics reference either popular Muslim apps or applications that individuals who are interested in Islam might find entertaining. Other titles and domains reference legitimate services, websites and third party app stores that serve Uyghur-relevant content only.

Logging statements indicate that the developers of SilkBean speak Chinese. Chinese names and locations are also mentioned in non-compromised signer certificates used to sign samples of this malware, although this information is easy to falsify during development. Similarities in coding techniques and naming conventions between SilkBean and other known Chinese-developed malware families also add weight to this theory.

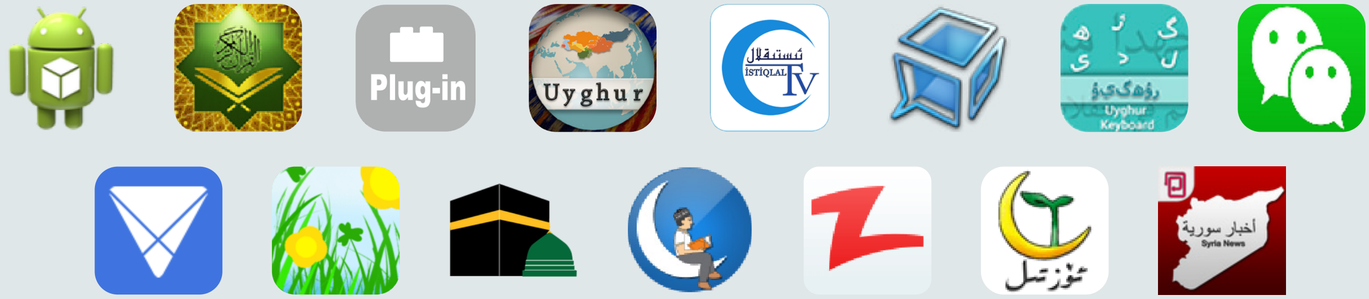
[11] https://www.androidphons.com/malware-spotted-xiaomi-mi4-smartphones/

[12] https://unit42.paloaltonetworks.com/unit42-henbox-chickens-come-home-roost/

[13] https://unit42.paloaltonetworks.com/unit42-pluginphantom-new-android-trojan-abuses-droidplugin-framework/

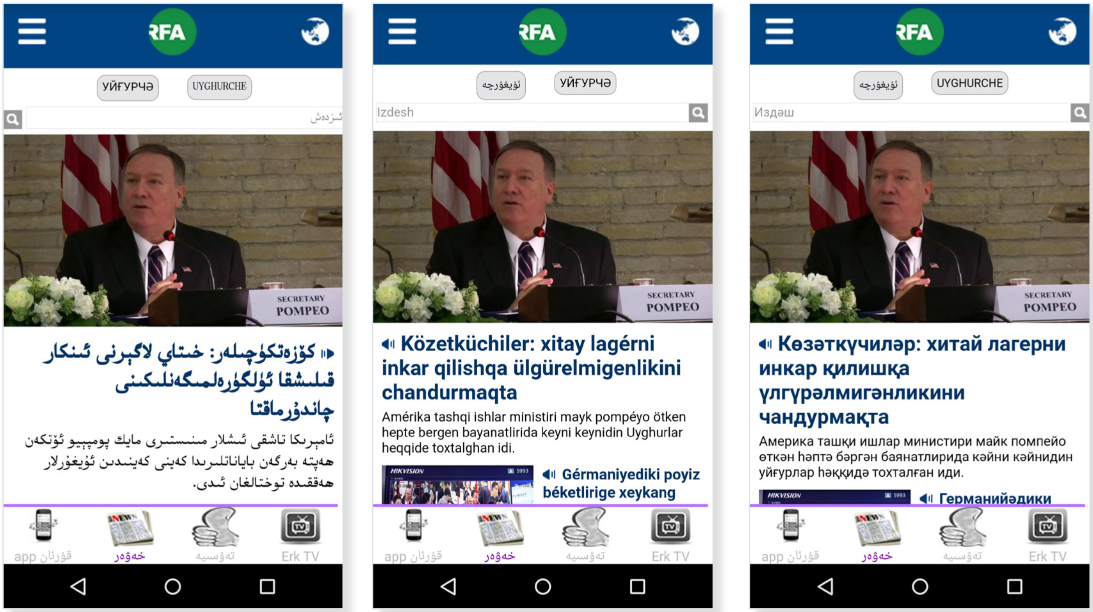
Targeting

The majority of SilkBean samples acquired by Lookout in 2016 and 2017 have titles like **com.google.pay** and **com.android.google.service**, which the average user might find innocuous on an Android device. Most later samples had app icons and titles identifying them as Uyghur targeted as shown in the following figure.



While at least two samples have a direct reference to Uyghur specific applications, such as Uyghur Keyboard, (Uyghur) Alphabet and Uyghur Plugin, one is titled "ئىستىقلال " which may be loosely translated as "Independence" in Arabic. Another recent sample is titled TalkBox, a push-to-talk messaging application commonly used in China.

A SilkBean sample (SHA-1: **3da34aaf95ffcb5c5d36c2a9fc5 42c1b08c36d2f**) uncovered in June 2019 prompted a closer look at the family. It had the title " اخبار سوريا", which translates to "Syria News" in Arabic. Despite the app title, the content of the application was still specifically Uyghur-focused - all news stories could be viewed in the three different scripts used for the Uyghur language.



كۆزەتكۈچىلەر: خىتاي لاگېرنى ئىنكار قىلىشقا ئۈلگۈرەلمىگەنلىكىنى چاندۇرماقتا

ئامېرىكا تاشقى ئىشلار مىنىستىرى مايك پومپېيو ئۆتكەن ھەپتە بەرگەن باياناتلىرىدا كەينى كەينىدىن ئۇيغۇرلار ھەققىدە توختالغان ئىدى.

Közetküchiler: xitay lagérni inkar qilishqa ülgürelmigenlikini chandurmaqta

Amérika tashqi ishlar ministiri mayk pompéyo ötken hepte bergen bayanatlirida keyni keynidin Uyghurlar heqqide toxtalghan idi.

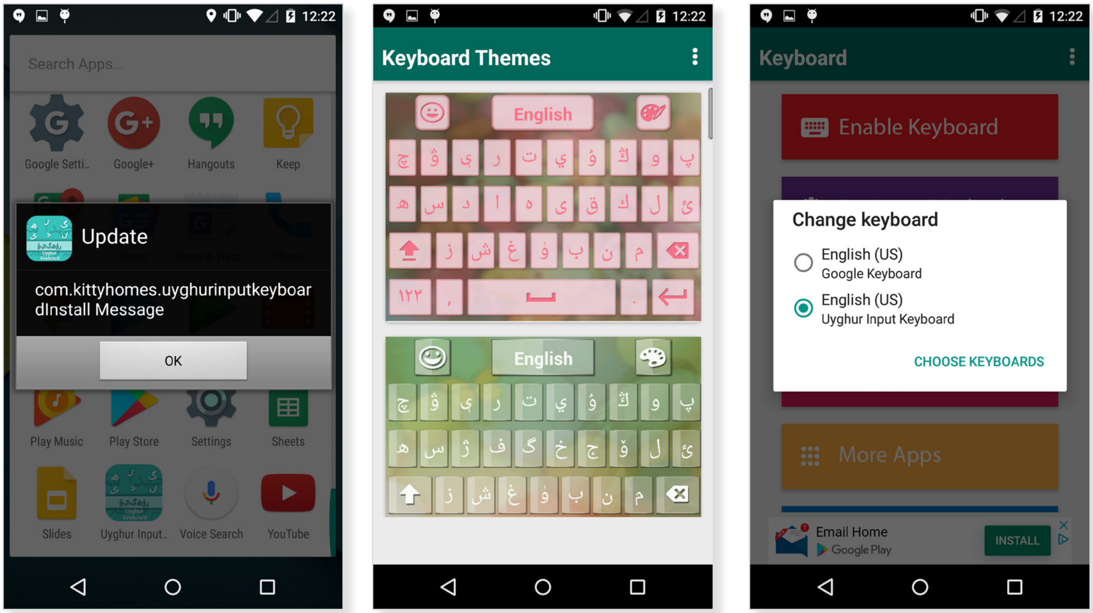
Gérmaniyediki poyiz béketlirige xeykang

Көзәткүчиләр: хитай лагерни инкар қилишқа үлгүрәлмигәнликини чандурмақта

Америка ташқи ишлар министири майк помпейо өткән һәптә бәргән баянатлирида кәйни кәйнидин уйғурлар һәққидә тохталған иди.

Германийәдики

Icons and screenshots of SilkBean samples which are examples of language-specific targeting used by this threat, where the same news article is presented in a number of Uyghur language scripts.



Update

com.kittyhomes.uyghurinputkeyboardInstall Message

Change keyboard

○ English (US) Google Keyboard

● English (US) Uyghur Input Keyboard

Screenshots from a sample of SilkBean masquerading as a Uyghur Keyboard application. The first stage of the application asks the user for an update immediately and uses this opportunity to install another application which contains legitimate functionality, also retrieved from it's assets folder (non-rooted device functionality). The application does not attempt to hide its icon either. As is discussed later however, the current C2 content encourages users to disable this security setting and allow app installs from unknown locations.

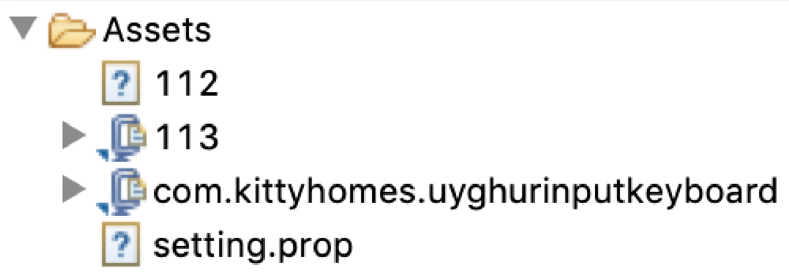
Malware details

Apps belonging to the SilkBean family have extensive surveillance and remote-control capabilities as is evident from the following list of 70 commands the app can receive from its C2 and perform.

CMD_ADDRESSBOOK
CMD_ADDRESSBOOK_DEL
CMD_ADDRESSBOOK_INFO
CMD_AUTO_SCREEN_STATE
CMD_BASICINFO_GET
CMD_BASICINFO_SET
CMD_BROWSER_DATA_DEL
CMD_BROWSER_DATA_GET
CMD_CALL_GEAR
CMD_CALL_RECORD
CMD_CALL_RECORD_DEL
CMD_CALL_RECORD_TOP
CMD_CHANG_TOKEN
CMD_CONTROLLER_CONNECT
CMD_CONTROLLER_VERIFY
CMD_ENVIRONMENT_RECORD
CMD_GPS
CMD_HEARTBEAT
CMD_INSTALL_APP
CMD_INSTALL_APP_DEL
CMD_INSTALL_APP_NORM_DEL
CMD_INSTALL_APP_SETUP
CMD_MESSAGE
CMD_MESSAGE_DEL
CMD_MESSAGE_MODIFY
CMD_MESSAGE_SEND
CMD_PHONE_BLOCK
CMD_PHONE_BLOCK_DELLOG
CMD_PHONE_BLOCK_GET
CMD_PHONE_BLOCK_GETLOG
CMD_PHONE_CAMERA_GET
CMD_PHONE_IM_DEL
CMD_PHONE_IM_GET
CMD_PHONE_MAIL_ATTACH
CMD_PHONE_MAIL_BODY
CMD_PHONE_MAIL_DEL
CMD_PHONE_MAIL_GET
CMD_PHONE_RECORD
CMD_PHONE_RECORD_FILES
CMD_PHONE_SWITCH_MACHINE
CMD_PHONE_WEIBO_DEL
CMD_PHONE_WEIBO_GET
CMD_PLUG_DELETE
CMD_PLUG_PATH_GET
CMD_PLUG_VER_QUERY
CMD_RECORD_APP
CMD_RECORD_FILES
CMD_RECORD_FILES_DEL
CMD_RECORD_RECORD_GET
CMD_RECORD_WATCHAPPFILES
CMD_RUNNING_APP
CMD_RUNNING_APP_STOP
CMD_SDCARD
CMD_SDCARD_DEL
CMD_SDCARD_DOWNLOAD
CMD_SDCARD_GET_FILES
CMD_SDCARD_MVFILE
CMD_SDCARD_RENAME
CMD_SDCARD_RUN
CMD_SDCARD_UPLOAD
CMD_SOCKETCLOSE
CMD_TROJAN_AUTOCONFIG
CMD_TROJAN_AUTOSEND
CMD_TROJAN_CONNECT
CMD_TROJAN_INFORMATION
CMD_UPDATE_THEIR_BYURL
CMD_WATCHAPP_RECORD_ADD
CMD_WATCHAPP_RECORD_DEL
CMD_WATCHAPP_RECORD_SYN

The list of all commands that can be received and processed by SilkBean samples. Note the get and delete commands for Weibo information on an infected device, which is a popular social media site in China.

Many samples of SilkBean had most of their malicious functionality in a second stage and read command and control information from a settings file in the assets folder.



Assets
112
113
com.kittyhomes.uyghurinputkeyboard
setting.prop

```
{
        “App_run_name”:””,
        “Aram_type”:”true”,
        “backup_path”:”www.englishedu-online.com:7082;213.128.81.82:7082;”,
        “Client_type”:”3”,
        “Install_type”:2,
        “Mm_group”:”attack_2”,
        “mm_path”:”C:\\Program Files (x86)\\ryingsoft\\mmserver\\data\\center\\
mm\\9365e76b-f9e3-4ac7-881f-c93ab1077a60.apk”,
        “Mm_type”:0,
        “Notfiy_phone”:””,
        “Os_type”:0,
        “other_path”:”C:\\Program Files (x86)\\ryingsoft\\mmserver\\data\\center\\
mm\\aa42b5bb-f43e-4841-80cd-917680909614.apk”,
        “Port”:7082,
        “Rs_type”:”3”,
        “server_ip”:”www.turkyedu-online.com”,
        “Sock_type”:0,
        “Update_config”:
{
                “Call_type”:2431,
                “Cyc_time”:”60”,
                “Save_path”:”c:\\auto_path”,
                “Screen_state”:1,
                “Start_time”:”22:00”,
                “Stop_time”:”23:00”,
                “Time_type”:1,
                “trans_type”:”WIFI ONLY”
        },
        “Use_weixin”:0,
        “version”:”2016-02-18new”
}
```

Top: Files seen in the assets folder of a sample of SilkBean. The file **112** is a sqlite database used to store some data for the application. The file **113** is the second stage and contains malicious functionality. **com.kittyhomes.uyghurinputkeyboard** is the application that contains legitimate functionality and **setting.prop** is the encrypted file containing C2 information. **Bottom:** In all cases, this settings file is encrypted using a set of bitwise shifting operations. Once decrypted, it contains a JSON Object, similar to the one shown above. The values of the “**mm_path**” and “**other_path**” keys may contain clues about the developer's build environment. “**ryingsoft**” is also a string found in signer certificate details of many SilkBean samples, possibly a reference to an IT company with the same name, based in Shanghai[14].

[14] https://www.dnb.com/business-directory/company-profiles.shanghai_rying_technology_co_ltd.ab959740ad32f7c72eaa04a4d449c866.html

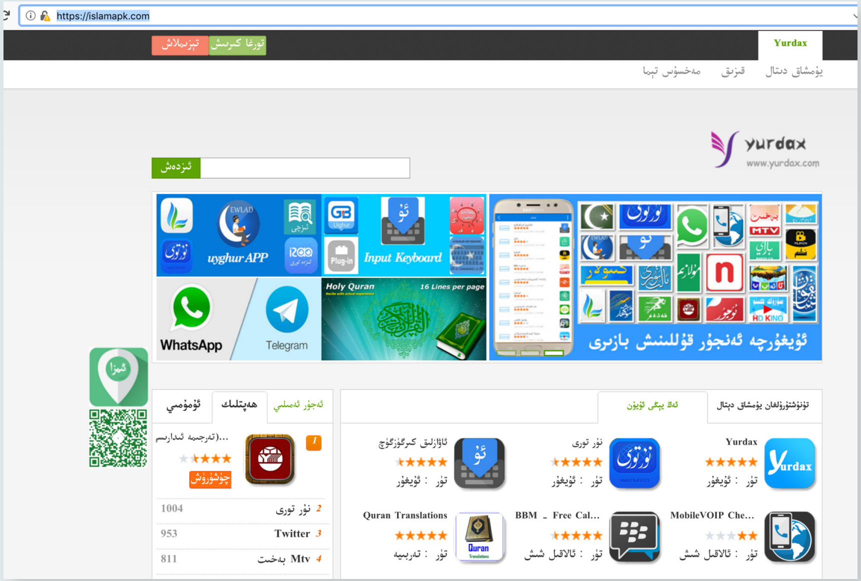
Command and control infrastructure and possible distribution mechanisms

Two C2 server domains retrieved from the settings files from SilkBean samples are **www.englishedu-online[.]com** and **www.turkyedu-online[.]com**. Navigating to these sites early on in the investigation redirected the request to a third-party app store called **www.islamapk[.]com** which hosts Uyghur and Islamic specific applications for download.

More recently however, navigating to these sites directs the user to an exact copy of **http://video.overxtube[.]com**, an adult content site, which also resolves to the same IP address as the SilkBean C2s. Site content encourages users to modify Android security settings, thereby allowing the installation of applications from an "Unknown Source".

All applications offered on this site (SHA-1: **eea64762788a3df961dc83ff5d48f227eddb8f25**, **5deaaa31ac24bced0215287c6dd74a0ba71abdc9**, **1fbc8c3abcc0e70743e182bc34ba2b459935d2f3**) are signed with a compromised key, but do not appear to contain any malicious functionality consistent with SilkBean and also do not have surveillanceware capabilities. However, all three applications have the capability to install an application package. This is a behavior explicitly explained away by the content on the web site as an expected "update" of the app. This behavior might provide insight into a possible distribution mechanism for the malicious apps.

Lastly, accessing either of the C2 servers over an HTTPS connection again redirected the user to **islamapk[.]com**. However, the site content delivered on this site appeared to impersonate yet another third-party app store, **yurdax[.]com**. It is possible that the targets for SilkBean may already be familiar with this site and this made infecting their devices with SilkBean easier.



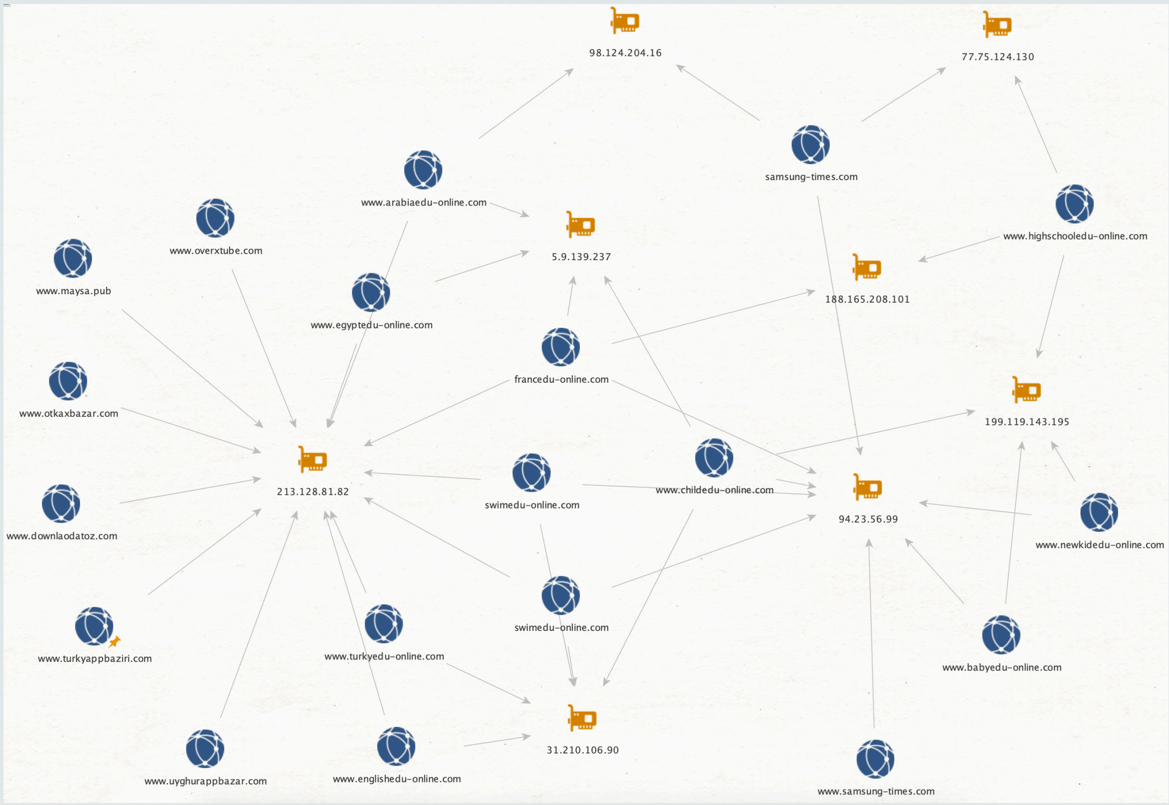
A screenshot taken during the investigation of **https://www.islamapk[.]com/** which is exactly identical in content to **http://yurdax[.]com/android/**.

None of the APKs downloaded from the site during the investigation were malicious, although a significant fraction of the links were either not accessible or the target files did not exist. Lookout also began ingesting the same APKs found on SilkBean C2 servers from other sources shortly before new samples of SilkBean started appearing in August 2018. The temporal correlation suggests that the site and malware campaign were being updated in parallel.

Lookout researchers also uncovered six applications requesting invasive permissions that connect to **islamapk[.]com**, with very telling package names as to who is being targeted. Two of the applications are known SilkBean samples, while the remaining are not yet classified into any known families, but appear to look for a second stage download from **islamapk[.]com**, which at the time of writing could not be accessed. Two of the applications' package names are **com.uyghur.hunter.islamapk**, and the other two are **com.islamapk.uy**, which is consistent with the targeting of Uyghurs that Lookout researchers have seen.

Connections to Other Uyghur-targeted Surveillanceware

The detailed investigation into SilkBean apps and infrastructure provided the starting point for piecing together the different elements of this mAPT into a larger picture. Starting from the IP address (**213.128.81[.]82**) of the two previously mentioned C2 servers of SilkBean (**www.englishedu-online[.]com** and **www.turkyedu-online[.]com**) we found that a number of similar C2 servers had also resolved to the same IP address. This resolution has not changed since January 2016 (for **turkyedu-online[.]com**) and October 2017 (for **www.englishedu-online[.]com**).



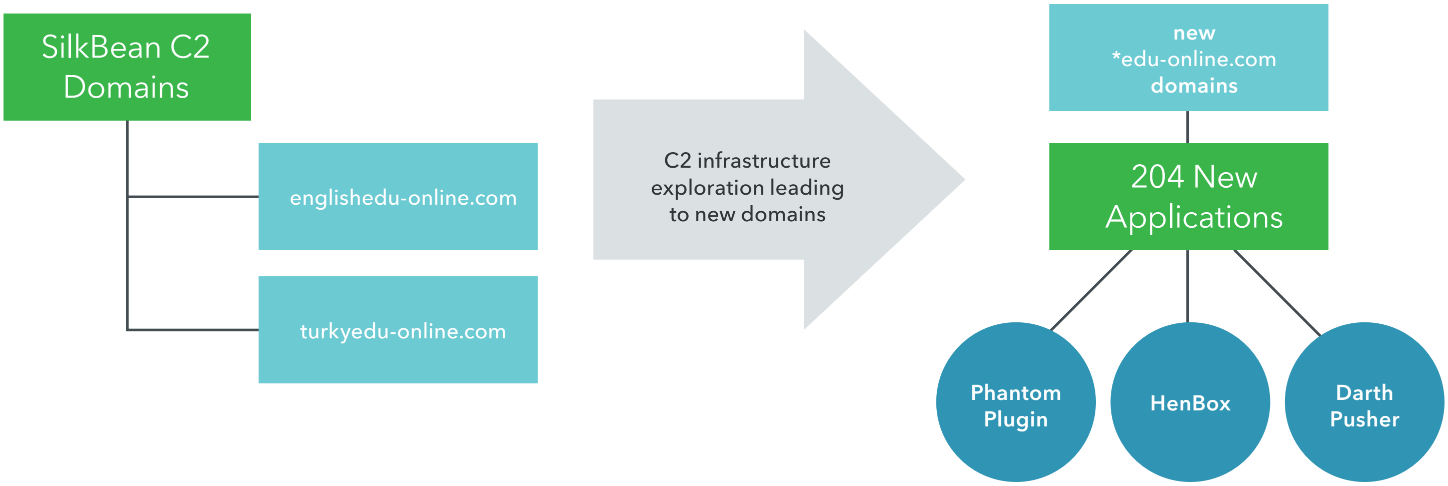
A Maltego graph showing the resolutions of SilkBean's C2 domains to the IP addresses **213.128.81[.]82** and **31.210.106[.]90** as well as some other domains resolving to the same IPs since February 2016. This image was compiled using RiskIQ's Passive DNS data. OSINT[15] and RiskIQ[16] research indicates that **uyghurappbazar[.]com** and **overxtube[.]com** are already publicly associated with Android malware[17]. Many sites have a naming convention with the pattern "***edu-online.com**" and the rest appear to contain innocuous names or reference Uyghur-specific content, such as **otkaxbazar[.]com**.

[15] https://www.malwareurl.com/ns_listing.php?as=AS197328

[16] https://community.riskiq.com/search/213.128.81.82

[17] https://www.malwareurl.com/listing.php?domain=uyghurappbazar.com

By retroactively searching Lookout's app database for apps communicating with domains seen in the above graph, a C2 domain pattern "*edu-online.com" emerged as a common theme for many associated domain names this actor has made use of. From this, Lookout researchers uncovered hundreds of samples communicating with these domains, not all of which are SilkBean surveillanceware. In fact, the majority of these downloaded samples belong to malware from the families DarthPusher, HenBox and PluginPhantom.



Flowchart highlighting the connection from SilkBean infrastructure to new APK samples tied to three other malware families, DarthPusher, PhantomPlugin and HenBox.

DarthPusher[18] is classified by Lookout as an app dropper, i.e. malware with capability that can arbitrarily install an Android APK. An adversary can use this capability to push any piece of surveillanceware to an intended target device.

PluginPhantom[19], or IHide, was found to contain many separate Android applications hidden within its resources. Each surveillance function of the malware, such as collecting call logs, location, SMS messages and more, was divided into separate APKs that were then loaded through the "DroidPlugin" framework for Android. Location tracking functions used only Baidu libraries and most debugging statements appeared to be in Chinese. Lookout researchers also noticed overlap with other Chinese-developed code from IronButler and SpyWaller malware, which continues the trend of heavily reusing already existing malware tooling by the actor behind SilkBean.

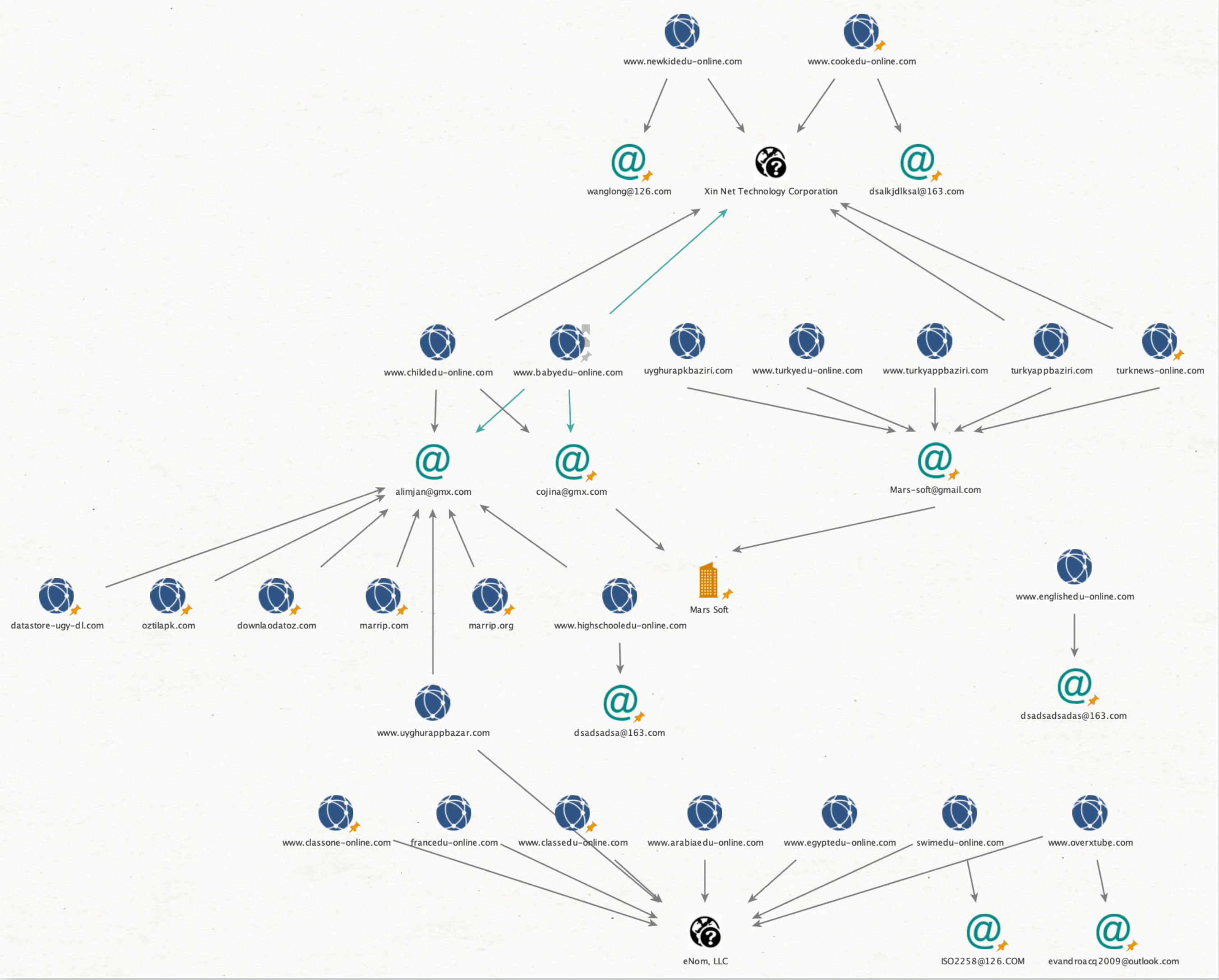
HenBox[20,21], is a previously discovered surveillanceware already known to target the Uyghur community. We can only attribute a small subset of these apps to the SilkBean actor through the use of shared infrastructure and the similarity of the used domains to the previously mentioned pattern.

[18] https://www.androidphons.com/malware-spotted-xiaomi-mi4-smartphones/

[19] https://unit42.paloaltonetworks.com/unit42-pluginphantom-new-android-trojan-abuses-droidplugin-framework/

[20] https://unit42.paloaltonetworks.com/unit42-henbox-chickens-come-home-roost/

[21] https://unit42.paloaltonetworks.com/unit42-henbox-inside-coop/



WHOIS record history links a number of these domains together, through the emails **mars-soft@gmail.com**, **alimjan@gmx.com**, and **cojina@gmx.com**

Branching out from WHOIS information, C2 domains, and IP resolutions, Lookout researchers were able to find other potential C2 domains in use by the actor behind this tooling using the same targets and patterns. The majority of known C2 servers were registered with Xin Net Technology Corporation, a Chinese domain provider that has a reputation for hosting phishing and malicious sites[22], and eNom[23]. All others were hosted by Hetzner[24].

[22] https://www.pcworld.com/article/167549/article.html

[23] https://en.wikipedia.org/wiki/Enom

[24] https://en.wikipedia.org/wiki/Hetzner

C2 domain name	Language of apps	Malware families	Notes
cookedu-online[.]com	Arabic and Chinese	HenBox, DarthPusher, DoubleAgent	Mostly focused on people practicing Islam.
babyedu-online[.]com	Uyghur and Pashto	DoubleAgent, GoldenEagle	The use of Pashto titles may indicate targeting of people in Afghanistan and Pakistan[25].
newkidedu-online[.]com swimedu-online[.]com	N/A	DarthPusher, HenBox	Overlaps with DarthPusher.
highschooledu-online[.]com	English, Pashto, and Uyghur	HenBox	Targeting newcomers to Turkey who speak English, with titles such as "Turkey Navigation" and "Cities of Turkey"; also secure messaging and VPN apps (Psiphon, Zapya and Voxer).
francedu-online[.]com	Arabic, Uzbek, English and Chinese	PluginPhantom	Domain names suggest possible targets in France.
englishedu-online[.]com	English	SilkBean, DarthPusher	Mostly apps focussing on people practicing Islam. Also secure messaging apps such as TalkBox.
turkyedu-online[.]com	Uyghur and Arabic	SilkBean, DarthPusher	App titles " اخبار سوريا " (Syria News), " ئستقلال " (Independence) third-party app stores and secure messaging. Targeting Uyghurs and people in Syria[26]. Continued to see samples into June 2019.
childedu-online[.]com	Indonesian/Malay, Turkish, Urdu/Hindi, English	PluginPhantom	Titles reference apps for live radio and TV (istiqlaltv, UYGHURTV and A2Z Kuwait FM Radio) and religious books and apps for Islam and Christianity in a number of languages including English, Arabic, Uyghur and Turkish.
turknews-online[.]com	English and Uyghur	SilkBean, DoubleAgent	Masquerading as portals to a number of third party app stores, some seen previously: **islamapk[.]com** and **yurdax[.]com**.
arabiaedu-online[.]com egyptedu-online[.]com	N/A	N/A	Domain names suggest possible targets in Saudi Arabia and Egypt.

[25] https://en.wikipedia.org/wiki/Turkistan_Islamic_Party_in_Syria

[26] https://www.reuters.com/article/uk-mideast-crisis-syria-china/syria-says-up-to-5000-chinese-uighurs-fighting-in-militant-groups-idUSKBN1840UP

uyghurapkbaziri[.]com turkyappbaziri[.]com	N/A	N/A	Registered by **mars-soft@gmail.com** who also registered **turknews-online[.]com** and **turkyedu-online[.]com** (see above).
oztilapk[.]com uyghurappbazar[.]com datastore-ugy-dl[.]com downlaodatoz[.]com marrip[.]com marrip[.]org	N/A	N/A	Registered by **alimjan@gmx.com** who also registered **babyedu-online[.]com** **childedu-online[.]com** **highschooledu-online[.]com**.
uyghur-soft-market[.]com 0ztil[.]com uyapkbazar[.]com uyghurapkbaziri[.]com	N/A	N/A	Other potential infrastructure related by Passive DNS information

C2 domains linked to SilkBean and information on apps communicating with them. Many of the domains collected during our research above appear to suggest hosting content for third party app stores. For example, Oztil App Baziri appears to be yet another Uyghur-focused third party app store (**www.oztil.com**), and also has been seen in other HenBox and DarthPusher titles. In fact, there are so many potential app stores that, without further insight into the targeted community, it is difficult to discern if any of these are legitimate stores or malicious watering holes impersonating legitimate stores.

As shown in the table above, the titles and languages used in these applications imply targeting of these malware families over a wide geographic area. There are titles in at least ten different languages, and many samples reference services in a number of countries around the world. While many apps are of interest to Muslims in general, Uyghur populations abroad in these geographic regions have reportedly continued to see targeting by the Chinese government [27,28,29].

At least eighteen third-party app stores were found during this investigation, all serving pages in Uyghur and Arabic. Among some other general and utility apps, these stores also contained apps specific to the Uyghur population or persons practicing Islam. If at least some samples of SilkBean were intended for Uyghur targets residing in China, the heavy use of third-party app stores makes sense since the Google Play store is not available in the region. Secure messaging applications such as WhatsApp and Voxer could also be downloaded from these stores, but are not malicious and appear to be popular, modified versions of those legitimate applications.

www.otkaxapp.com
www.turkyappbaziri.com
www.izda.com
app.oztil.com
islamapk.com
yurdax.com
islamapk.com
uyghurapkbaziri.com

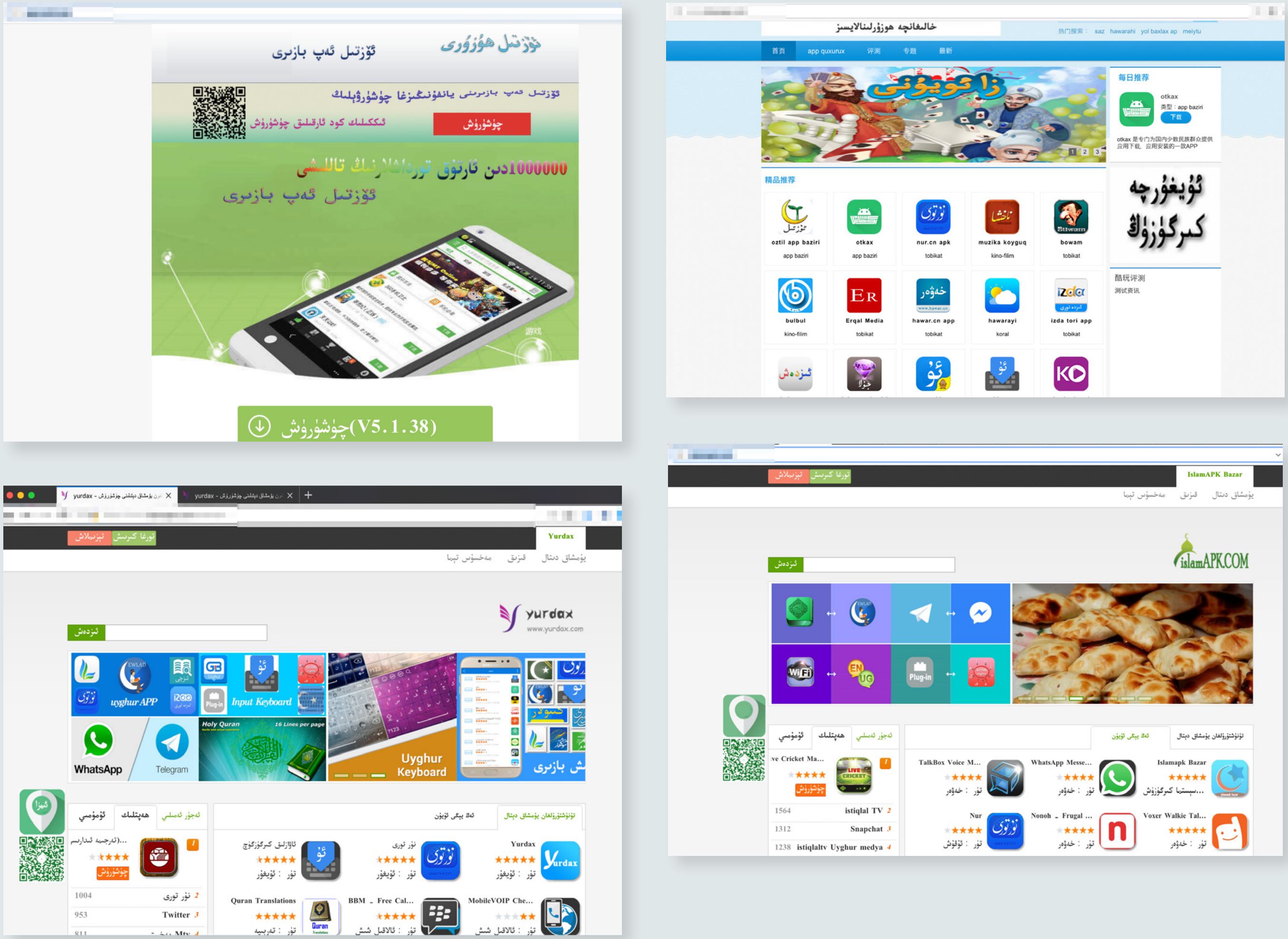
oztilapk.com
uyghurappbazar.com
datastore-ugy-dl.com
downlaodatoz.com
marrip.com
marrip.org
www.uyghur-soft-market.com
0ztil.com
uyapkbazar.com

A list of all third party app stores found connected to potential C2 infrastructure for SilkBean, past and present. Some of these appear to be imitations of others, but it is difficult to confirm this for all of them since many are now offline.

[27] https://www.npr.org/2020/03/13/800118582/i-thought-it-would-be-safe-uighurs-in-turkey-now-fear-china-s-long-arm

[28] https://www.amnesty.org/en/latest/news/2020/02/china-uyghurs-living-abroad-tell-of-campaign-of-intimidation/

[29] https://www.brookings.edu/wp-content/uploads/2019/09/FP_20190930_china_counterterrorism_byman_saber-1.pdf



Screenshots depicting some of the many third-party app stores found focusing on persons that speak Uyghur or practice Islam.

There was one group of malicious applications whose details are not described in this section. Applications that communicate to **turknews-online[.]com** stood out to Lookout researchers as a completely different piece of malware. These are samples from a long-running family Lookout researchers have been tracking called DoubleAgent, described next in this report. Titles and functionality were particularly noteworthy as they display content from **islamapk[.]com** and **yurdax[.]com**, previously associated with SilkBean C2 server content. The most recent samples ingested by Lookout were initially found on VirusTotal and were uploaded through IPs located in US, Germany, and Korea in March and June of 2019.

There are also malware samples communicating to the C2 server **babyedu-online[.]com** which belong to a surveillanceware known as GoldenEagle, described in the last section of this report.

It appears to be important to the threat actor using SilkBean to blend into the background noise while infecting their targets, and that is a recurring theme in their design choices. Many samples were signed with compromised signing certificates, and the campaigns involving SilkBean uses known and abundant malware (DarthPusher, Spywaller) to accomplish their tasks, perhaps so that there is no unique tooling to tie to them. Where custom tooling is used, it is blended into apps that may be downloaded by their targets, as well as making them as geographically and linguistically-specific as possible. There is also evidence that the actor has deliberately made use of titles, package names, and emails (found in WHOIS information) that mimic the names of popular Uyghur individuals and activists. For example, alimjan@gmx.com which was used to link may C2 domains together, may be referring to Alimjan Yimit[30], a Uyghur christian clergyman who was imprisoned in 2008.

Campaigns associated with SilkBean also appear to be long-running, at least since 2015, and this shows patience and perseverance by the operator in question. It also appears that this mobile tool is not only used to target the Uyghur population within China, but also around the world in countries such as Turkey, Syria, Kuwait, Indonesia, Malaysia, Afghanistan and Pakistan.

DoubleAgent

Findings

In 2013 Citizen Lab reported on a compromised version of KakaoTalk[31], which had been used to target a prominent individual in the Tibetan community. This app was the first publicly exposed sample of a malware family called DoubleAgent. When Lookout initially investigated DoubleAgent in 2015, it was already an advanced Android remote access tool (RAT). Early versions of this family trojanized apps such as Voxer and TalkBox, as well as Amaq News, the official Daesh news application. The extent of this malware family and its connections to other campaigns has not been publicly reported on until now. Lookout researchers have seen DoubleAgent used exclusively against groups with contentious relationships with the Chinese government.

Although Lookout has been tracking this malware family for many years, new samples discovered in the last year indicated that the actors behind DoubleAgent were continuing to evolve the surveillanceware and use new infrastructure. However, they maintained the same targeting, as well as several key malware characteristics, such as similar decryption keys for configuration files.

These recent samples, discovered in late 2019, are the focus of this section on DoubleAgent. A decryption of the configuration files from these samples revealed a direct overlap in C2 infrastructure between the operators of DoubleAgent and SilkBean at a time when both malware families appeared to be active. The C2s found also confirmed our findings that other domains resolving to the IP address **213.128.81[.]82** since February 2016 were part of the same actor's infrastructure. This leads us to believe that the same actor is behind the use of DoubleAgent and SilkBean.

Titles also suggest targeting of the DoubleAgent family has included the Uyghur population, with these most recent samples masquerading as third-party Android app stores (**islamapk[.]com** and **yurdax[.]com**) serving Uyghur-focused applications and overlapping with C2 content seen when investigating SilkBean. Consistent use of domain names that fit the pattern "***-online.com**" was also noted across both these families.

[30] https://en.wikipedia.org/wiki/Alimjan_Yimit

[31] https://citizenlab.ca/2013/04/permission-to-spy-an-analysis-of-android-malware-targeting-tibetans/

Malware details

Each DoubleAgent sample comes with an encrypted file in the **assets** folder that contains configuration information for the malware and its command and control servers. On launch, the malware Base64 decodes the file, most recently disguised with the name "**GoogleMusic.png**". This decoded text is then decrypted with a key formed by joining two strings hardcoded in the sample. MessageDigest is used to calculate the MD5 of this string, which is then used as the final key when decrypting the configuration file using the AES algorithm.

Contents of the decrypted configuration file are split by a sequence of hash signs ("**###**" or "**####**") and then dollar signs ("**$$$$$**"). This allows the malware to parse out C2 information, decryption/encryption keys, beaconing and timeout periods, among other configuration details on how the malware is run on an infected device..

```
androidapps.spdns.org:990 $$$$$comix_Qove $$$$$HaPyzi0o825-$^ $$$$$1 ####android.apps.us.to:990
$$$$$comix_Qove $$$$$HaPyzi0o825-$^ $$$$$1 ####androidapps.nsupdate.info:990 $$$$$holder-Peoq
$$$$$PhyOZ915_#@ $$$$$1 ####android.app.info.tm:990 $$$$$holder-Peoq $$$$$PhyOZ915_#@ $$$$$1
####http://heartsys.dnsapi.info ####30 ####600 ####21600 ####60 ####on
```

Decrypted contents of early configuration files called "google.ind".

```
[{"IP":"www.turknews-online.com","port":9701},{"IP":"www.cookedu-online.com","port":9701},{"IP":"www.turknews-
online.com","port":9701},{"IP":"192.168.10.108","port":9080}]####600####60####on
```

Configuration file formats appear to have changed slightly in more recent versions. The C2 list is now an array of JSON objects and the FTP server information is omitted. In this particular sample, the C2 server is **turknews-online[.]com**, a C2 domain tied to SilkBean.

Early versions of DoubleAgent used FTP servers as staging areas for exfiltrated content and required infected devices to authenticate with credentials from the decrypted text file. In addition to serving as a staging area for exfiltrated information, the FTP servers also hold files containing specific instructions that a device should carry out in the future. When an infected device beacons to C2 infrastructure it will check the FTP server for files with the format <device IMEI>.fmd. These files contain commands for a discrete action like uploading a file, enabling a service such as audio recording, searching directories for specific files, or installing additional applications.

Newer versions of DoubleAgent upload files, unencrypted, directly to the C2 servers using TCP sockets. Although the usual list of surveillance data is pulled and inserted into SQLite databases on the device (such as system information, calls, contacts, SMS texts, apps installed, browsing history, and more), it is not uploaded unless instructed by the C2 which indicates that the actor behind DoubleAgent prefers handling data exfiltration carefully, likely to avoid detection.

In addition, DoubleAgent also pulls the list of files, where possible, from the following set of locations when instructed to do so via C2 commands. It also monitors any changes and logs them in a SQLite database locally on the device.

- **/data/data/com.google.android.gm/shared_prefs (Gmail app)**
- **/data/data/com.google.android.gm/databases (Gmail app)**
- **/data/data/com.android.email/shared_prefs (Default email app)**
- **/data/data/com.android.email/databases (Default email app)**
- **/data/data/com.dropbox.android/databases (Dropbox app)**
- **/data/system**
- **/DCIM**
- **/Pictures**

Some samples of DoubleAgent feature code for downloading exploits in order to root the phone and install additional malware as a system app. Specifically, Lookout has seen the authors using TowelRoot in order to gain privileged access on victim devices and install additional malware on **/system**. This technique makes it difficult for the typical user to clean their device if infected.

Messages received from the C2 can contain an object that specifies two things: a number representing one of up to 39 commands handled by the malware, and optionally a String object that specifies any further parameters, each separated by a sequence of hash signs ('**#**').

The most noteworthy RAT capabilities found to be present in these new samples are discussed below:

- Runs arbitrary shell commands with or without root privileges, as specified by the C2 and returns the output of the command.
- Remounts system as Read-Write, installs a file as a system app at the **location /system/app/GoogleMail.apk**, and remounts **/system** back to Read-Only permissions if it has root.
- Installs a specified APK after a specified number of seconds.
- Hides or unhides app icon.
- Updates C2 configuration.
- Gathers a list of running apps and a list of apps in the foreground.
- Creates, deletes, and renames specific files.
- Records calls as **.amr** files, and zips them before sending the archive file out to the C2 server.
- Has the ability to kill its background service if needed, likely either to avoid detection or save battery.
- Stores all exfiltrated data in database (.db) files on the device.
- Has a database to track what files need to be uploaded to or downloaded from the C2 server, as specified by commands provided to the malware.
- Can either automatically or when directed by the C2 copy and upload data of popular communications applications, depending on the DoubleAgent sample.

Talkbox

DiDi (rideshare app in China)

Keechat

Coco

Voxer

WhatsApp

Airetalk

Viber

Telegram

Zello (Push to talk)

Skype

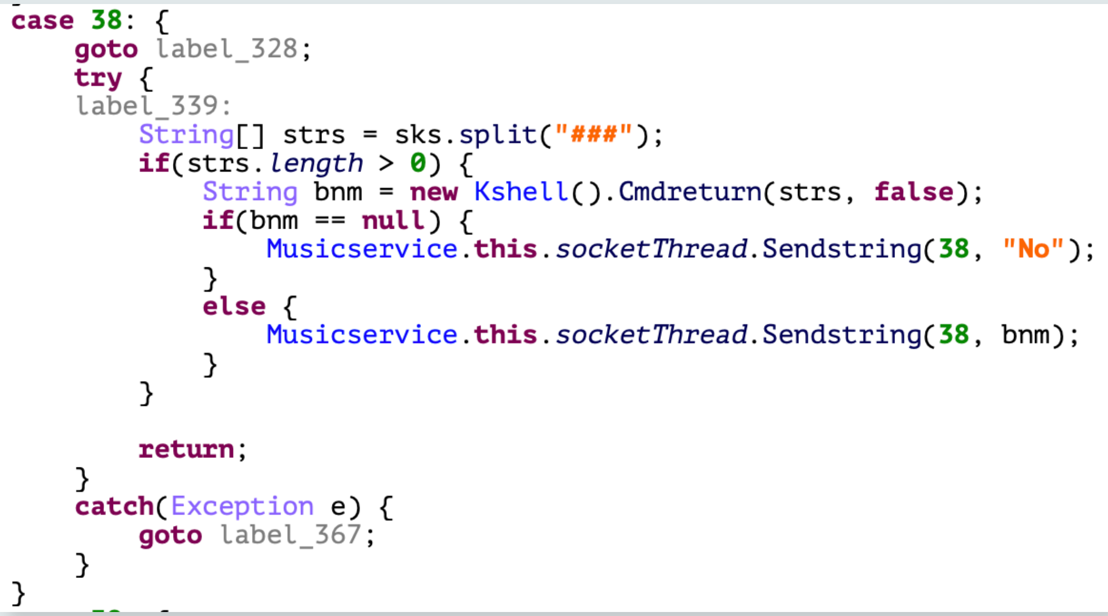
QQ

MicroMsg

MagicCall (Voice Changer app)

BBM

List of applications whose files or databases are uploaded to DoubleAgent C2 servers of DoubleAgent samples seen in 2019. The malware also attempts to change the file permissions for all files under the /data/data/ directory of the above chat applications to permit read/write/execute for any UID.



```
case 38: {
    goto label_328;
    try {
    label_339:
        String[] strs = sks.split("###");
        if(strs.length > 0) {
            String bnm = new Kshell().Cmdreturn(strs, false);
            if(bnm == null) {
                Musicservice.this.socketThread.Sendstring(38, "No");
            }
            else {
                Musicservice.this.socketThread.Sendstring(38, bnm);
            }
        }

        return;
    }
    catch(Exception e) {
        goto label_367;
    }
}
```

Instruction (command) 38, above, allows the attacker to execute a specified shell command along with an arbitrary number of parameters separated by a '###' string, without requesting root permissions. 'Kshell' is the class in DoubleAgent responsible for executing shell commands with or without root permissions, as specified. If the command successfully gets executed, the output is sent back to the C2.

DoubleAgent's connection to other malware families

In late 2019 novel DoubleAgent samples appeared that had evolved significantly from previous versions, and a closer look at their configuration and C2 infrastructure highlighted new connections to SilkBean, HenBox and DarthPusher. This strengthened the theory that the actor behind DoubleAgent is also involved in the deployment, and perhaps even development, of these other malware families.

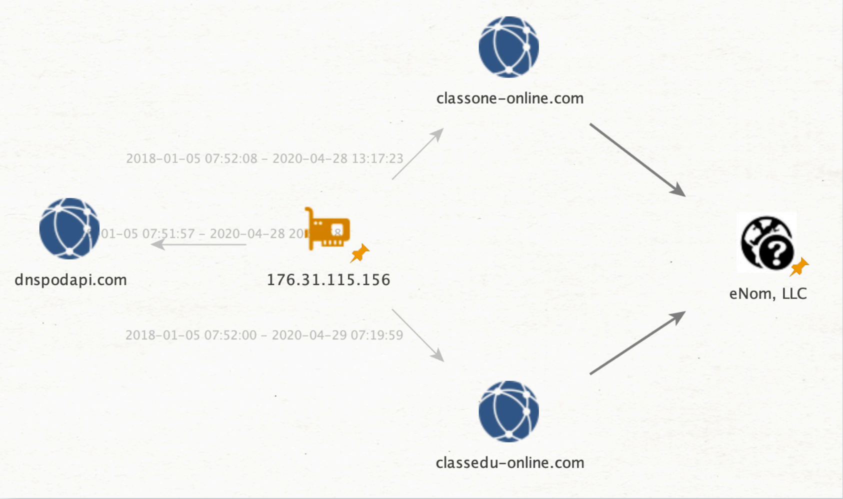
Icons of the newly uncovered DoubleAgent samples, which are titled “Disk photo recovery”, “SafeUM”, “Quran” and “Alphabet”, the last two being in line with past targeting profiles.

Many of the new DoubleAgent samples in Lookout's app database contained configuration files, which, when decrypted, contained links to known SilkBean C2 infrastructure.

```
[{
      “IP”:“www.turknews-online.com”,
      “port”:9701
   },{
      “IP”:“www.cookedu-online.com”,
      “port”:9701
   },{
      “IP”:“www.turknews-online.com”,
      “port”:9701
   },{
      “IP”:“192.168.10.108”,
      “port”:9080
}]
####600####60####on
```

```
[{
      “IP”:“www.turknews-online.com”,
      “Port”:9701
   },{
      “IP”:“176.31.115.156”,
      “port”:9701
   },{
      “IP”:“www.turknews-online.com”,
      “port”:9701
   },{
      “IP”:“176.31.115.156”,
      “port”:9701
}]
####600####60####off
```

Two configurations found in recent DoubleAgent samples.



The hardcoded IP address present in one of the DoubleAgent configurations is pointed to by two domains of interest: **classone-online[.]com** and **classedu-online[.]com**. As shown in the previous section on SilkBean, the naming pattern “***edu-online[.]com**” and “***-online[.]com**” is consistent with the actor behind SilkBean as well as activity linked with the same actor also employing HenBox and PhantomPlugin malware families.

Four non-compromised signing certificates that signed samples of DoubleAgent were also used to sign applications belonging to the HenBox, DarthPusher and CarbonSteal Android surveillance families. CarbonSteal is another novel malware family described in the next section of this report. This confirms the theory that the actor behind the deployment and use of the samples of these malware families is the same. An overlap in validity dates of these signing certificates may also indicate that these tools were under development and use in the same timeframe, starting in early 2015.

Finally, code similarities in these samples of SilkBean, HenBox, DarthPusher, CarbonSteal and DoubleAgent also suggest a common origin. For example, a malware sample (SHA-1: **1278654a7e6411f25c10a72e4db41468233ce519**) first seen in late 2016 has unique code characteristics that belong to both HenBox and CarbonSteal, while being signed with a certificate that has also been used to sign DoubleAgent samples. Another sample (SHA-1: **61c0837583e9bfa915b7d897ed9d6b6c0faf7e4a**), titled "Quran", possesses code similarities between HenBox and DoubleAgent malware families, while also being signed with a certificate that was used to sign 48 other HenBox, DoubleAgent, DarthPusher and CarbonSteal samples. This is another indicator that these malware tools are being used in tandem by the same actor.

CarbonSteal

Findings

In March 2018, Palo Alto Networks released a report on a Chinese surveillanceware family named Henbox[32], which was found to be targeting minorities in China. When examining this research closely, Lookout found numerous IoCs (such as C2 and signer certificates) overlapping with another long running surveillanceware family, CarbonSteal, so named due to signer certificates containing the phrase Yǐtiān jiàn, that may be referring to a sword frequently advertised for sale as made from carbon steel.

CarbonSteal is Android surveillanceware that has been tracked by Lookout since 2017, and more than 500 samples have been seen to date. While not as sophisticated as HenBox, certain samples of CarbonSteal do make use of a combination of native libraries and DEX classes, while others do not and are much simpler.

Hallmarks of CarbonSteal include extensive audio recording functionality in a variety of codecs and audio formats, as well as the capability in later samples to control an infected device through specially crafted SMS messages. Attackers can also perform audio surveillance through the malware's ability to silently answer a call from a specific phone number and allow the attacker to listen in to sounds around an infected device. Based on this functionality, we suspect that CarbonSteal might be deployed in areas with insufficient or no mobile data coverage.

Samples of CarbonSteal and HenBox also use the same non-compromised signing certificates in many cases, suggesting the actor behind their deployment is the same. Furthermore, overlapping validity dates of these certificates may indicate that the samples were produced around the same time frame. This evidence led Lookout researchers to the theory that these tools were primarily used in an ongoing malware campaign (at the time) and against similar targets, with titles and languages once again suggesting a Uyghur focused interest.

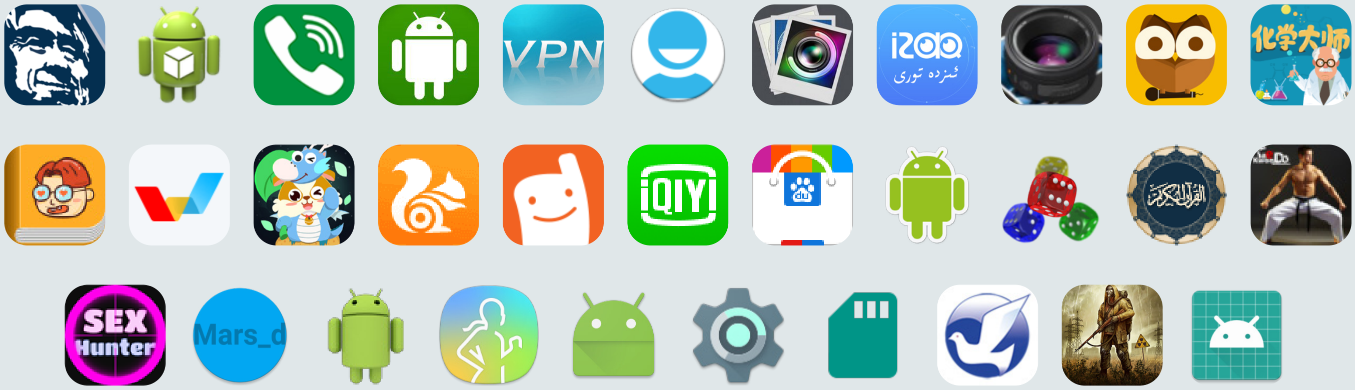
Other overlaps in C2 and signer certificate IoCs indicate that tools such as DarthPusher and PhantomPlugin are also in this actor's mobile surveillance arsenal.

Lastly, a C2 IP address that communicated with CarbonSteal and HenBox samples was also observed communicating with samples of an OS X backdoor that was tied to GREF activity in 2014 by FireEye[33].

[32] https://researchcenter.paloaltonetworks.com/2018/03/unit42-henbox-chickens-come-home-roost/

[33] https://www.fireeye.com/blog/threat-research/2014/09/forced-to-adapt-xslcmd-backdoor-now-on-os-x.html

Malware details



Titles for the vast majority of CarbonSteal samples are “设置”, which translates to “Setting”, however the operators behind this family also used various Google themed names and app icons for well known chat apps, VPN apps and popular games in China. They also impersonated Baidu apps (such as iQIYI, an online video platform based in Beijing and used by the Chinese Taiwan Affairs Office to further United Front (China) efforts)[34] and Izda, a Uyghur-focused search engine and content site. Titles such as “Quran”, “Dua” and “mullaim” also point to a Muslim focus of targets.

CarbonSteal samples exhibit a high level of sophistication, with recent samples splitting their malicious functionality between native libraries and secondary APKs that get decrypted and loaded during execution, at times using reflection. Early samples appear to be based on the Dendroid malware family. Throughout its implementation, CarbonSteal maintains a focus on audio recording functionality and collection of data from chat applications popular in China.

CarbonSteal samples contain an RC4 encrypted configuration file (usually **config.txt** or **conf.txt**) where information such as command and control details (IP/domain and port), a control phone number, and a UID are stored. Almost all samples also contain encrypted secondary JAR or DEX files in the **assets** folder, titled **googlej.jpg** and **googles.jpg**.

On compromised devices, CarbonSteal samples have the following functionality:

- Retrieve call logs.
- Retrieve all SMS and MMS messages.
- Retrieve device metadata including model, manufacturer, product, sdcard size, and memory specs.
- Retrieve disk usage information.
- Retrieve CPU information including device serial number.
- Retrieve QQ content from external storage.
- Retrieve installed apps and when they were installed.
- Retrieve notes and data from MiCode[35], a community-run, open source version of the Xiaomi sticky note app, and even masquerades as this application.
- Receive out-of-band instructions via SMS from numbers specified in the configuration or retrieved from the C2.
- Track the location of a device.
- Remotely record audio.
- Search external storage for various files such as audio recordings (.amr).

[34] https://en.wikipedia.org/wiki/IQIYI

[35] https://github.com/MiCode

- Call netcfg and get stats.
- Log when the device is powered on and off.
- Dynamically load additional functionality.
- If the superuser binary is present, use it to silently install additional applications
- Test for the Flyme operating systems or OPPO or VIVO phones in order to turn off various power saving features.

CarbonSteal's capability for operation without the use of mobile data or WiFi is particularly interesting. Apps of this family monitor the sender of incoming text messages and caller ID of incoming calls and match it against a number specified in the configuration file. If a call is received from the control phone number, the malware turns off the device's ringer and answers the call immediately. This allows the operator of the control phone to listen in on the environment around the infected device. Once the call ends, the call log is deleted from call records on the device.

CarbonSteal operators can also remotely control infected devices by sending them specially crafted text messages. The instruction set available via SMS in recent samples includes the following commands:

Text message from control phone	Function
@*a<digits>	Retrieves the contact details associated with the number specified by <digits>
@*b<digits>	Retrieves the call log details at a particular offset from the start of the call log list, specified by <digits>. Call log list is sorted with the most recent call first.
@*c<digits>	Retrieves the SMS details at a particular offset from the start of the SMS list, specified by <digits>. SMS list is sorted with the most recent SMS first.
@*d[1|*]	Responsible for silently starting or stopping environment recording. To start recording the sequence **@*d** needs to be followed by 1. To stop recording an adversary needs to supply any other value in place of the 1.
[*|null]	If the text contains any other data, including if it is empty, this will trigger CarbonSteal samples to get current cell information about the device including the 16-bit GSM Cell Identity, 16-bit Location Area Code as well as the the mobile country code (MCC) and mobile network code (MNC) of the mobile network operator.

Table showing the format of control SMS messages received and function performed by CarbonSteal as a result. The retrieved data is sent back to the control phone number using SMS messages. CarbonSteal expects the control phone number to start with +86, which is the dialing code for China. Analysis of sample configurations only found one control phone number (158 7172 6845) specified for a small set of samples, which may belong to a mobile number segment operated by China Mobile in Wuhan City, Hubei Province.

CarbonSteal samples are able to encode audio data into a variety of encodings, such as G711, G722 and Speex and store audio files in a variety of file formats, such as **.amr**, **.raw**, **.wav** and **.gms3**. CarbonSteal can send this audio data as complete recorded files through network sockets or by using RTP to stream data to a C2.

Audio and other data is stored at the following locations using timestamps as file names:

- /mnt/sdcard/google/db/mp/<timestamp> (general media recorder)
- /mnt/sdcard/google/db/mc/<timestamp> (general media recorder)
- /mnt/sdcard/google/db/pr/<timestamp> (phone call recorder)
- /mnt/sdcard/google/db/sr/<timestamp> (SMS-triggered audio recorder)
- /mnt/sdcard/google/db/ps/<timestamp> (screenshot capture)
- /mnt/sdcard/google/db1/<timestamp> (seen in older samples, no use of subfolders)

Audio data can also be recorded to the following paths on external storage:

- /<sdcard>/FinalAudio.amr
- /<sdcard>/RawAudio.raw
- /<sdcard>/FinalAudio.wav

CarbonSteal attempts to perform rudimentary SSL certificate validation by using the HostnameVerifier[36] interface to confirm that the hostname of the C2 server communicating back to the malware is indeed the same one in the SSL certificate the SSL connection is using.

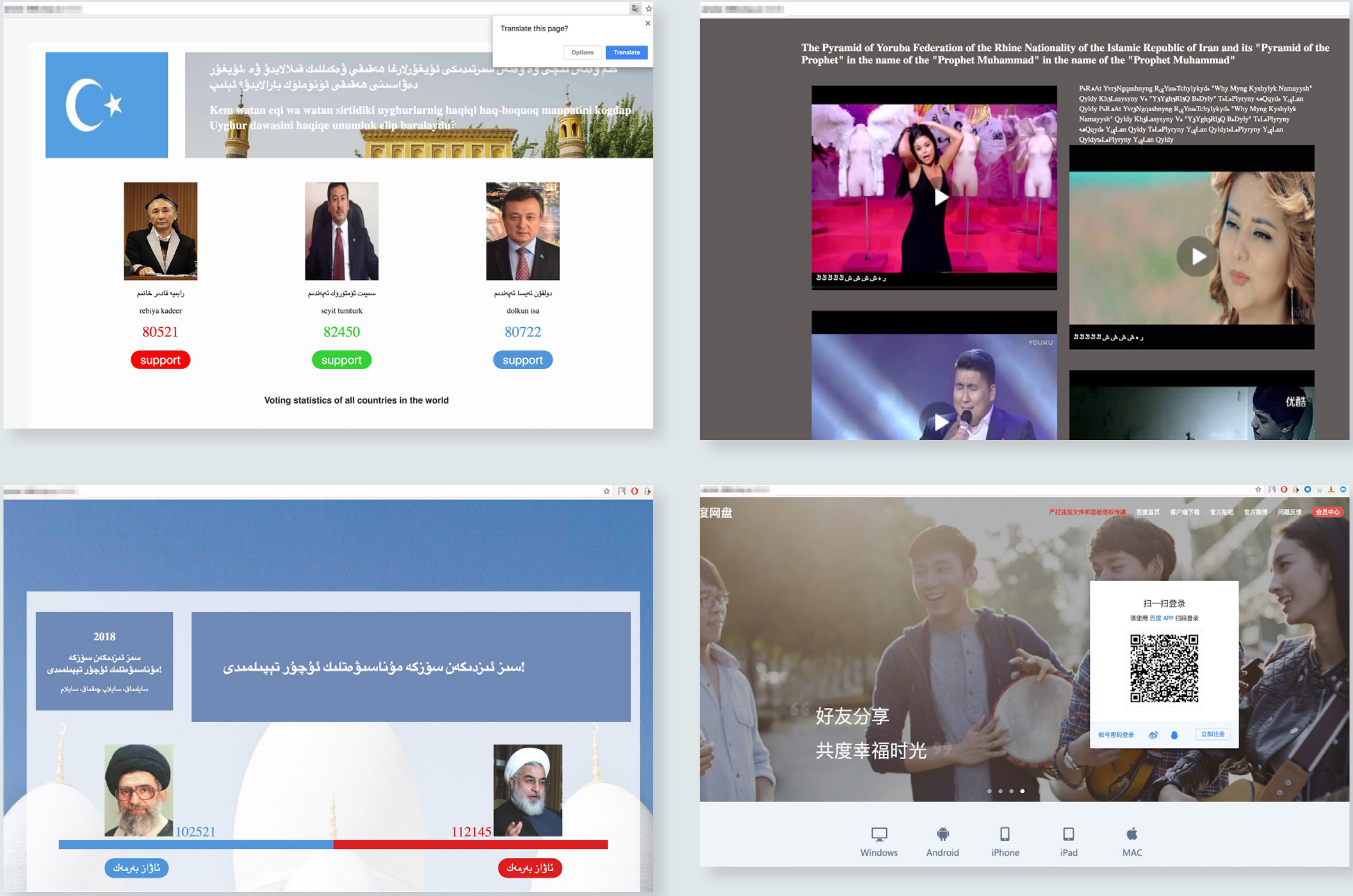
CarbonSteal appears to have been the most active in 2017, when the vast majority of new samples were seen. However, later samples of CarbonSteal seen in 2019 moved towards making extensive use of Android accessibility services to exfiltrate messages from secure messaging applications, a trend commonly seen in other recent Android surveillance malware. This suggests that CarbonSteal is still under active development and continues to evolve.

CarbonSteal C2 infrastructure and APT15 links

During the investigation of CarbonSteal, the C2 domain **amote-366.vicp[.]cc** was found to be hosting numerous websites on a number of subdomains some of which contained content restricted in China. Site content included a GoogleDrive link to the book "Freedom in the Sunset" written by Professor Yuan Hongbing, which has been banned by Chinese authorities. Other content included Uyghur-themed political content and content that appears to be Iranian specific.

Legitimate applications were also found hosted on the same site, such as versions of Baidu Netdisk for MacOSX, Android, iOS and Windows.

[36] https://docs.oracle.com/javase/7/docs/api/javax/net/ssl/HostnameVerifier.html



Kem watan eqi wa watan sirtidiki uyghurlarnig haqiqi haq-hoquoq manpatini kogdap Uyghur dawasini haqiqe unumluk elip baralaydu?

The Pyramid of Yoruba Federation of the Rhine Nationality of the Islamic Republic of Iran and its "Pyramid of the Prophet" in the name of the "Prophet Muhammad" in the name of the "Prophet Muhammad"

Examples of some of the hosted content on CarbonSteal's C2 domain **amote-366.vicp[.]cc.**

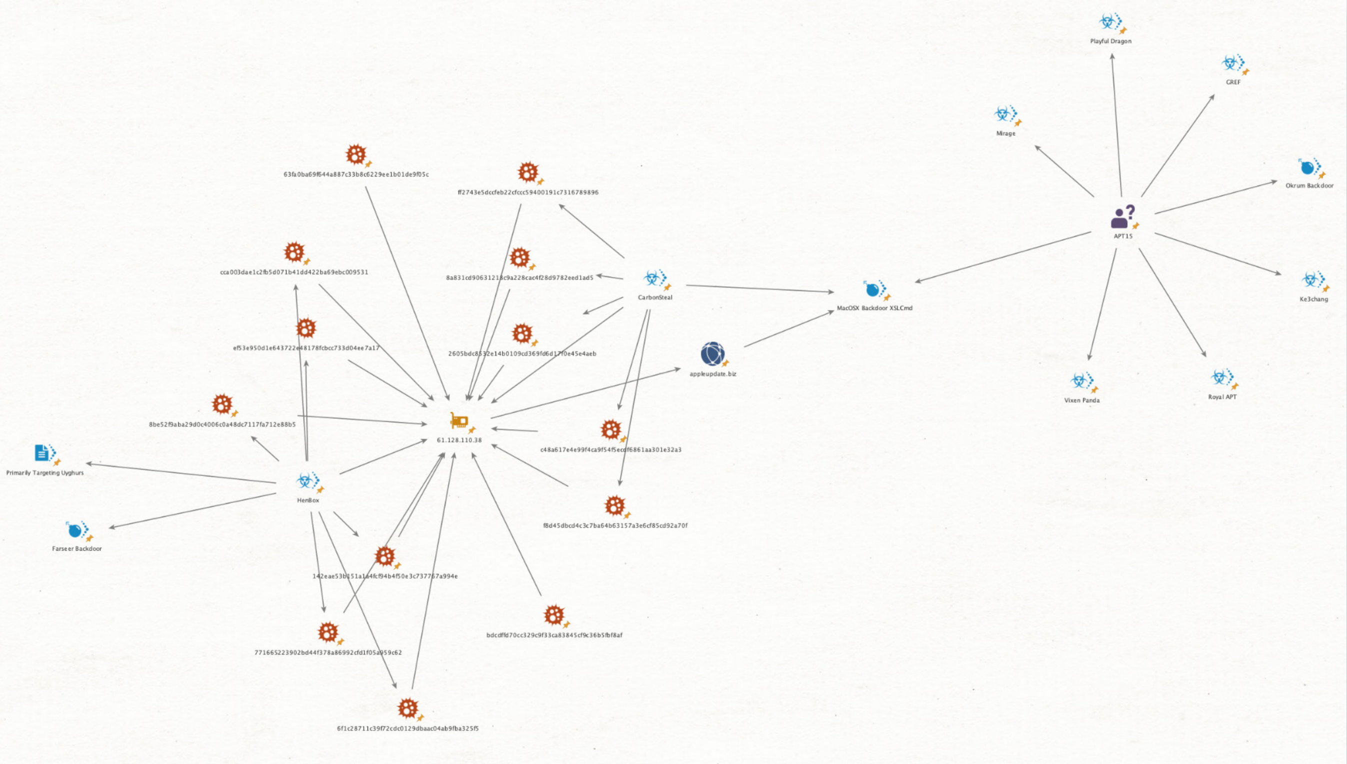
There could be a number of reasons a C2 server may be hosting this content. It is possible that the site originally hosted this content deliberately and was then compromised by the actor behind CarbonSteal. The alternative is that the actor may have used the same server with a secondary purpose of luring individuals who are inclined to access this content. In either case, this setup allows the actor to monitor access to this content and possibly target those that do.

Non-compromised signer certificates used to sign CarbonSteal samples were also used to sign a subset of malware samples belonging to the families known as Henbox and DarthPusher. This consistent use of the same mobile surveillanceware families was also seen when examining SilkBean and DoubleAgent samples. This may suggest that actors behind the use of these malware families not only share the same target groups but also resources and tools.

In March 2018, Lookout researchers discovered that certain CarbonSteal C2 domains overlapped with several HenBox samples found at the same time. A handful of these CarbonSteal samples were also found to communicate to a particular IP address (61.128.110[.]38) that overlapped with the deployment of an OSX backdoor XSLCmd reported by FireEye[37] in 2014.

[37] https://www.fireeye.com/blog/threat-research/2014/09/forced-to-adapt-xslcmd-backdoor-now-on-os-x.html

This article initially described the activity as belonging to the threat actor GREF, but it was updated in August 2019 to note that the activity is now being tracked as an uncategorized APT group. In past public reporting the actor known as GREF is also referred to as APT15, Ke3chang, Mirage, Vixen Panda and Playful Dragon. GREF is so named due to a variety of Google references in their activities, and the same can be seen in the activity of the threat actor behind CarbonSteal. This includes application titles, package names and encrypted files' names.


Playful Dragon
GREF
Mirage
Okrum Backdoor
APT15
Ke3chang
Vixen Panda
Royal APT
MacOSX Backdoor XSLCmd
CarbonSteal
appleupdate.biz
63fa0ba69f644a887c33b8c6229ee1b01de9f05c
ff2743e5dccfeb22cfccc59400191c7316789896
cca003dae1c2fb5d071b41dd422ba69ebc009531
8a831cd90631218c9a228cac4f28d9782eed1ad5
ef53e950d1e643722e48178fcbcc733d04ee7a17
2605bdc8532e14b0109cd369fd6d17f0e45e4aeb
8be52f9aba29d0c4006c0a48dc7117fa712e88b5
61.128.110.38
c48a617e4e99f4ca9f54f5ecdf6861aa301e32a3
Primarily Targeting Uyghurs
HenBox
Farseer Backdoor
f8d45dbcd4c3c7ba64b63157a3e6cf85cd92a70f
142eae53b151a1a4fcf94b4f50e3c737767a994e
bdcdffd70cc329c9f33ca83845cf9c36b5fbf8af
771665223902bd44f378a86992cfd1f05a959c62
6f1c28711c39f72cdc0129dbaac04ab9fba325f5

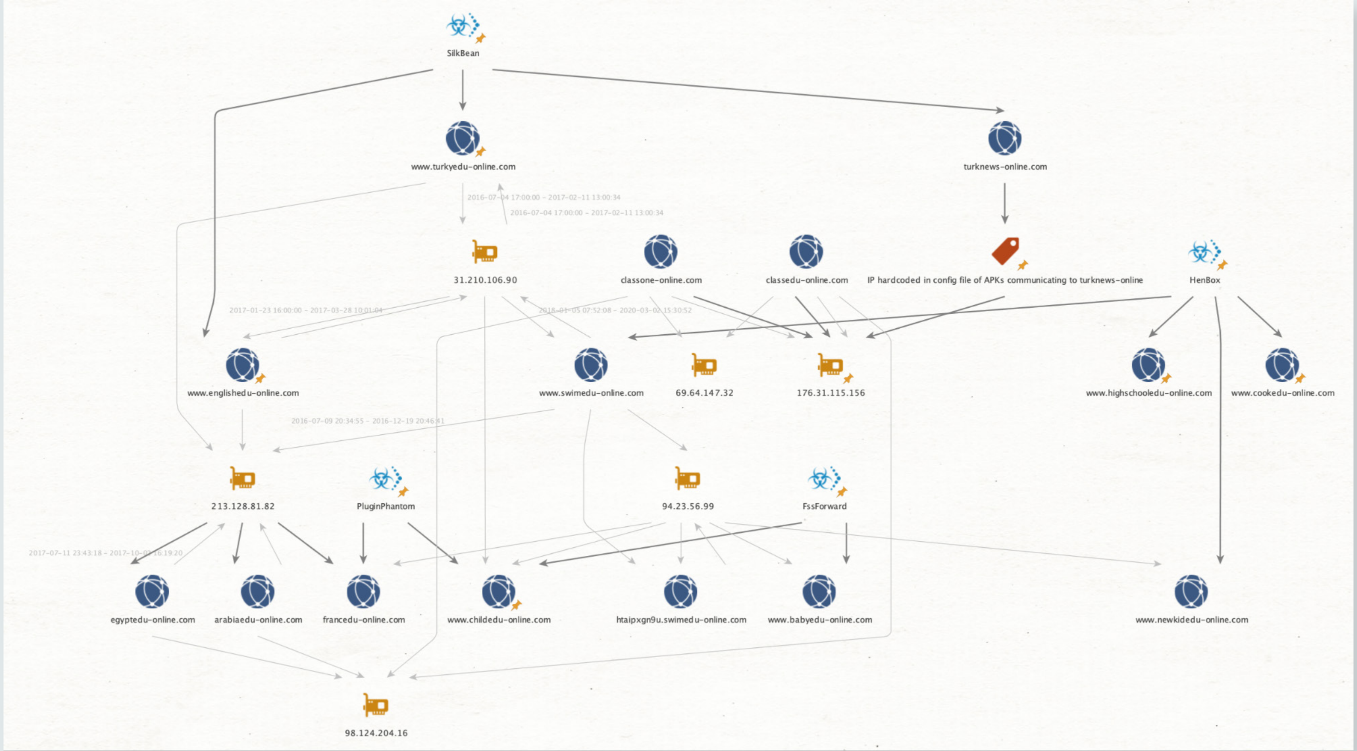
IoC overlap from 2018 between CarbonSteal, HenBox, and an IP address tied to APT backdoor use in 2014.

In July 2019, ESET published findings on a previously undocumented backdoor named Okrum, used to deliver Ketrican malware[38] and attributed to the Ke3chang group. According to this report, several Ketrican samples from 2017 communicated to subdomains of **babytoy-online[.]com**.

Ketrican SHA-1	C2 server
D3BFB10DB08C6828C3001C1F825ED6A6BF6F6E01	buy.babytoy-online[.]com
2C8B145EF5AC177C99DFCB8C0221E30B3A363A96	newflow.babytoy-online[.]com
D8AA9E4918E464D00BA95A3E28B8707A148EC4D7	buy.babytoy-online[.]com
F2BFDA51BDA3EE57878475817AF6E5F24FFBBB28	items.babytoy-online[.]com

[38] https://www.welivesecurity.com/wp-content/uploads/2019/07/ESET_Okrum_and_Ketrican.pdf

While not a concrete connection, this is reminiscent of the naming pattern seen in many past domains associated with Henbox, SilkBean and PluginPhantom infrastructure.



Other domains seen associated with HenBox, SilkBean and PluginPhantom, families monitoring Chinese minorities.

Given the overlaps of C2 infrastructure, it appears plausible that these three families have the same developer and targets. This belief, in conjunction with past public reporting[39] that HenBox is also tied to APT15, leads Lookout researchers to believe that SilkBean, PluginPhantom, and now CarbonSteal, can be tied to this mAPT threat.

GoldenEagle

Findings

The last family in this discussion is GoldenEagle, which Lookout researchers also believe is being used by the same group of China-based actors described in this report.

GoldenEagle, so called due to titles ("**Golden.eagle**") and package names ("**com.golden.eagle**") of samples believed to be test / development versions, targets primarily Uyghurs and Muslims in general, as well as Tibetans, individuals in Turkey, and in China. Golden eagles are used as part of ancient hunting traditions[40] throughout the Eurasian Steppe and diasporas in Mongolia and the Xinjiang Autonomous Region whose population is primarily Uyghur.

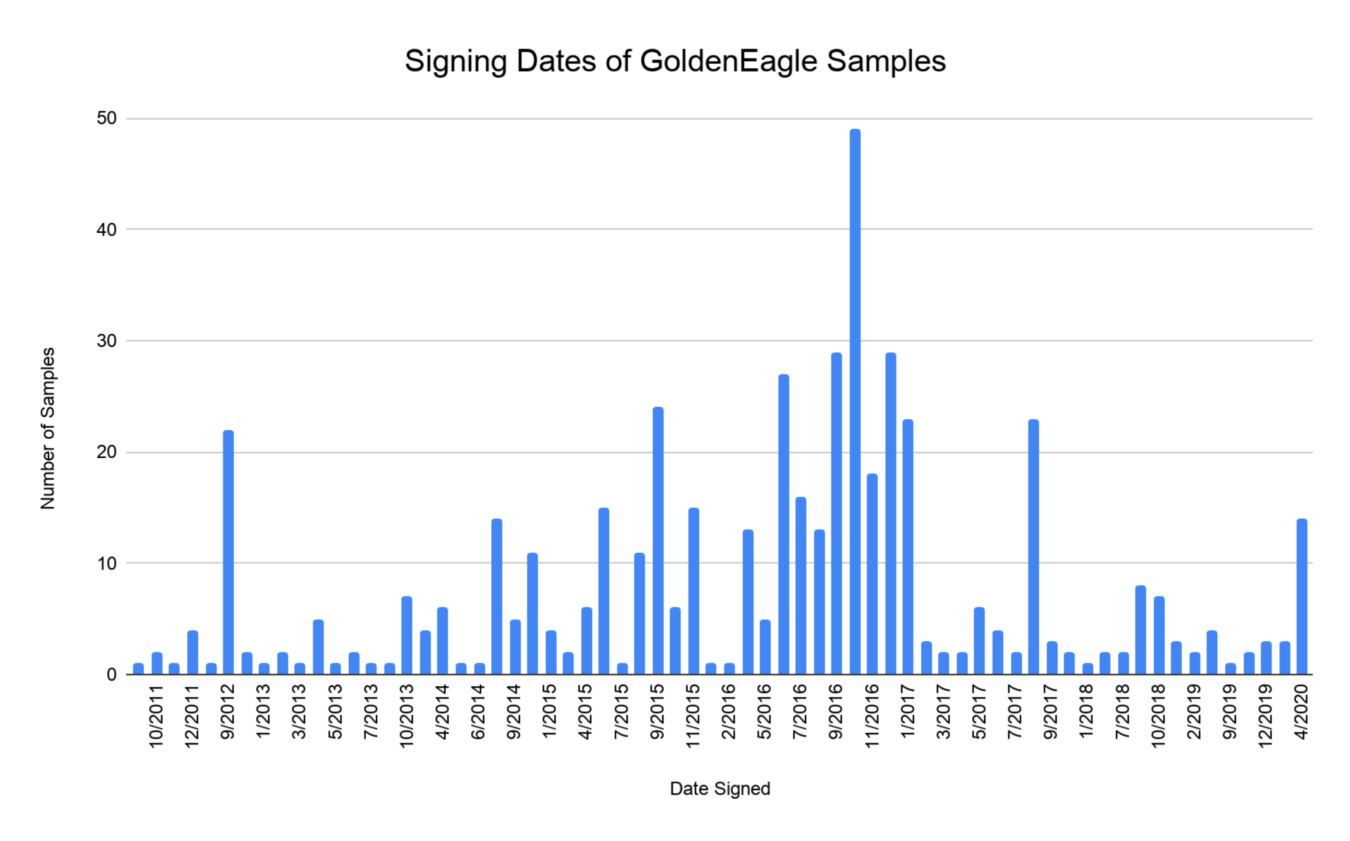
Among the aspects that make GoldenEagle particularly interesting is that the earliest test samples of this family appeared as early as 2012, making it one of the longest-running surveillanceware families we have observed to date. GoldenEagle code has been identified in an impressively

[39] https://www.virusbulletin.com/virusbulletin/2020/03/vb2019-paper-pulling-pkplug-adversary-playbook-long-standing-espionage-activity-chinese-nation-state-adversary/

[40] https://america.cgtn.com/2016/10/13/xinjiang-life-in-the-golden-eagle-village

large and diverse set of applications over the years. These samples can be divided into two major groups: those that exfiltrate data via HTTP and those that exfiltrate data via SMTP, i.e., by sending exfiltrated data in file attachments of emails to an attacker-controlled mailbox using innocuous-looking subjects and mail body content. The latter technique, while appearing in the early stages of GoldenEagle development, has resurfaced in samples signed and analysed in May 2020.

Insecure configurations in attacker infrastructure have also shown that the actor behind GoldenEagle is not only targeting Android devices, but also conducting phishing attacks in parallel from the same administration console. The actors behind GoldenEagle have shown themselves to be well resourced and capable of operating a long-running campaign.

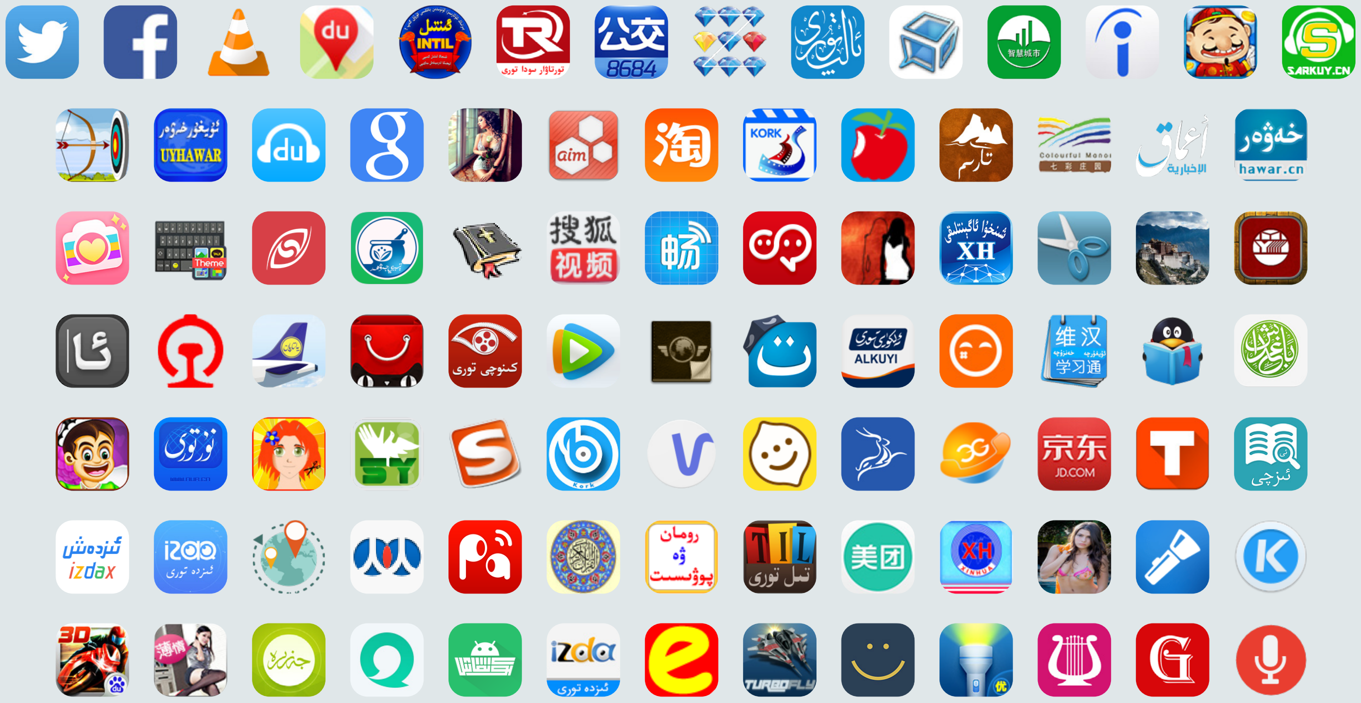


Mapping out when apps trojanized with GoldenEagle were signed shows the actors' activity. A clear spike in samples belonging to this family took place during 2016, and new samples have continued to be observed in 2020. At this point it is unclear whether these new samples are part of testing or a re-emergence of GoldenEagle activity, as these newer samples appear to be largely unchanged and possess the test title "Golden.eagle".

The majority of samples of GoldenEagle were clearly developed with targeting of the Uyghur minority in mind and included trojanized versions of apps such as Sarkuy (Uyghur music service), Tawarim (Uyghur e-commerce site), uyhurqa kirgvzvx (Uyghur input keyboard), Yeltapan Air (possibly an airline booking application - Yeltapan Inc. is a popular Uyghur app development company), TIBBIYJAWHAR (Uyghur Pharmaceutical app), Hawar.cn News (believed to previously provide Uyghur-specific news and content), Nur.cn News (also delivers Uyghur-specific content) and the Uyghur Quran, among others.

Other samples included trojanized apps with a broad range of functionality from VPNs, instant messaging, and social networking to games, adult media content, and Google searching. Notable trojanized apps include Twitter, Facebook, Calendar, AIM, RenRen, VLC media player, and the QQ messaging application.

The expanse of applications trojanized by GoldenEagle also indicated additional targets, with applications titled "快搜西藏" (Quick Search Tibet), "西藏同程游记" (Travel Notes in Tibet) and "美丽西藏精选壁纸" (Beautiful Tibet Featured Wallpaper) that appeared to focus on individuals living or travelling in Tibet. "Gundem News" was also seen in the array of titles suggesting individuals in Turkey are also targeted. "8684公交", the Beijing bus transit application, was also seen as an app title, possibly indicating broader Chinese targeting.



The actors behind GoldenEagle have deployed trojanized versions of a staggeringly large and diverse set of applications. This level of technical investment combined with the longevity of operations suggests that GoldenEagle is being managed by a well-resourced adversary. Shown above is a subset of app icons from the GoldenEagle family.

Malware details

GoldenEagle samples can be divided into two disparate groups; samples that communicate to attackers through HTTP requests and samples that communicate via SMTP to a hardcoded email address that is assumed to be operated by the attacker.

Early samples of GoldenEagle exfiltrated data through files sent over SMTP to an attacker-controlled email address. All samples had the same hardcoded attacker email - **twdwlgs2010@sina.cn**. On start up these samples also sent an SMS message to an attacker-controlled number (**18801206738**, a Beijing mobile number) with the message " **A host online**, **attention please!**".

Use of this version appears to have ended in 2017 and has only recently picked up again in May 2020 with samples labelled with the default name "**Golden.eagle**". The email address and phone number remains consistent. This makes it unclear whether this is testing by the actor or another wave of activity.

Data exfiltrated by these samples is limited to lightweight text files and includes the following content:

Data type	File attachment	Subject/body of email	Content of text file
Call Logs	C.txt	**Subject:** Hello,George **Body:** Forum Nokia Developer	<missed calls list> !-*RMC*-! <Incoming calls list> !-*RIC*-! <Outgoing calls list>
SMS	SX.txt	**Subject:** HELOS **Body:** MyBody	<Inbox list> !-*ISG*-! <Outbox list> !-*OSG*-! <Drafts lits> !-*DSG*-! <Sentbox list>
Contacts	P.txt	**Subject:** Hi,Peter **Body:** Launches N900-Newest mobile	<contact list>

Early versions of Golden Eagle exfiltrate data as an attachment to an email with subject, body, and attachment file name specific to the type of data being exfiltrated. Incomplete functionality for MMS message exfiltration as well as receiving emails from the attacker for command and control operations was also seen in later samples.

The following credentials were used in all samples of the SMTP version of GoldenEagle:

Smtp = "smtp.sina.cn"

User = "twdwlgs2010@sina.cn"

Password = [redacted]

From = "twdwlgs2010@sina.cn"

The second version of GoldenEagle vastly expands the malware's capability and makes use of HTTP POST requests as its primary communication method with C2 infrastructure. These samples contain plaintext configuration files stored in the assets directory of each application from where C2 information can be gathered.

There are two versions of these configuration files that accompany slightly different functionality as well. The earlier version is labelled "**goledn_config.json**" that has only one configuration setting beyond attacker C2 details, which registers if the malware has been run for the first time or not. In samples making use of the second, more advanced version of the configuration file (named "**ygoledn_config.json**") the configuration contains up to 15 different parameters and the malware includes functionality to update these parameters through C2 instructions, allowing an attacker to enable and disable various malicious functionality.

These more recent GoldenEagle samples come with the surveillanceware capabilities listed below.

- Get contact information.
- Retrieve installed apps.
- Retrieve call history.
- Notify operator if it has root permissions.
- Retrieve any doc, txt, gif, apk, jpg, png, mp3, and db files that are found on external storage.
- Retrieve text messages.
- Take screenshots.
- Take photos with the device camera.
- Request device administrator privileges.
- Allow proxy configuration.
- Record calls in **.amr** format.
- Record environment audio when instructed by the operator.
- Location tracking.
- Get messages from chat applications such as WeChat.
- Send notifications to specific SMS endpoints.
- Update themselves.

SMS messages are sent by GoldenEagle when a second stage is successfully installed, or when a SMS message containing a Telegram code is received.

GoldenEagle and CarbonSteal convergence

Lookout researchers discovered several code overlaps between CarbonSteal and GoldenEagle, suggesting that the malware families are developed by the same actor.

During our investigation, we noticed a unique WeChat ID (**wx09fa07f77f651c23**) in several CarbonSteal samples that was also found in one GoldenEagle sample. This ID is also used in an application (SHA-1: **30c34052ff4684b521e4a36038dd3d80a6693d20**) that is signed using the same signing certificate also used to sign known CarbonSteal samples. However, this particular sample appears to be an app dropper rather than a full-featured surveillanceware though it is also capable of tracking device location. The title and legitimate functionality of the app is called "**izda**" and it connects to a Uyghur content site of the same name[41]. Lookout researchers were not able to retrieve a malicious second stage from the app.

Code functionality not directly tied to malicious activity within the above-mentioned app dropper application was found to overlap with a number of other GoldenEagle samples all targeting Uyghur and Uzbek speaking individuals or groups. Their titles included, izda (Uyghur content site), Papap (a Chinese language vehicle information app associated with Autonavi), Baykuq (a Uyghur language news app), Misranim (a popular Uyghur language website), TIBBIYJAWHAR (Uyghur Pharmaceutical app), and Isimlar (an Uzbek child naming site, with a package name of **com.yeltapan.isimlar**).

[41] http://izda.com/

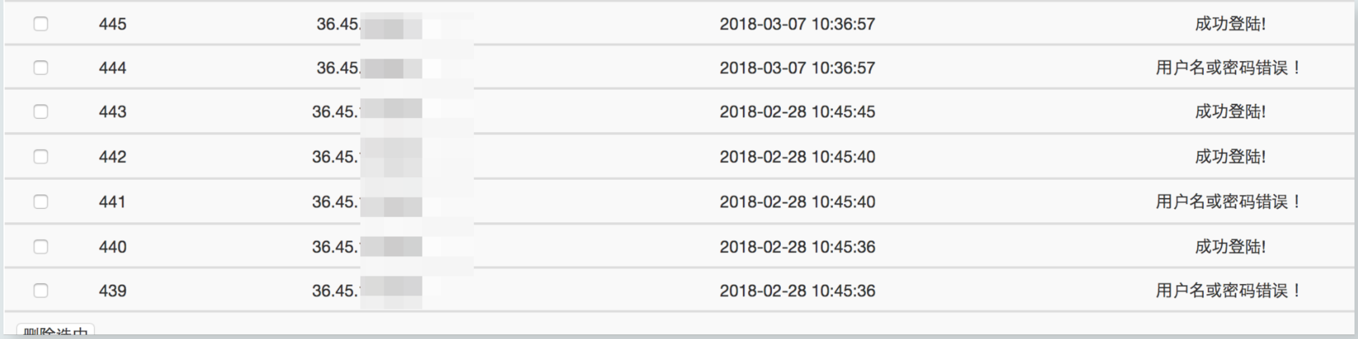
Application icons of malware samples that share overlapping code found in CarbonSteal and GoldenEagle.

All these titles are in line with past GoldenEagle and CarbonSteal targeting efforts, indicating that the two malware families have significant overlap in use. These new samples, in particular those with app dropper functionality may suggest the further evolution of this tooling and the continued activity of the actor behind these threats.

C2 infrastructure and connections with other malware

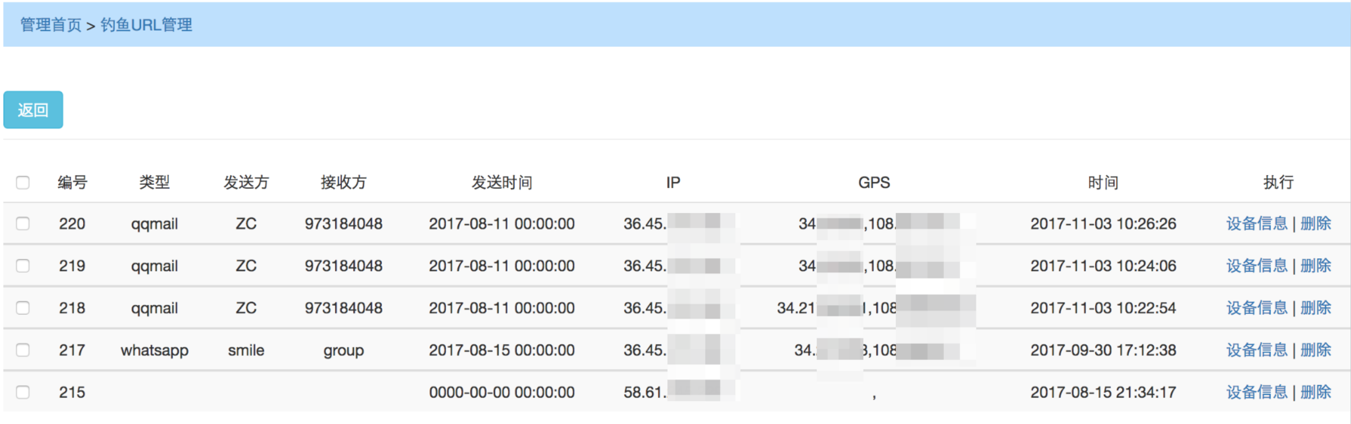
During this investigation we mapped out a sprawling infrastructure used by the actor behind GoldenEagle which resulted in over 50 domains and IP addresses being tied to this adversary. There was a consistent pattern of registering and using fake domains intended to fool users into believing that the domain names were associated with popular services such as Google, Norton, Symantec, and Voxer.

At the time of writing this report, all known C2 infrastructure supporting GoldenEagle is no longer active. However, during the investigation in 2017-2018 we identified several domains which were found to contain security flaws, allowing for a deeper insight into adversary behavior, targeting and attribution. Among the content accessible was a management panel that contained email addresses of targets, what we believe to be GPS coordinates of target devices, IPs of admin logins and target devices, and evidence that phishing campaigns were being run from the same infrastructure.



☐	445	36.45.[redacted]	2018-03-07 10:36:57	成功登陆!
☐	444	36.45.[redacted]	2018-03-07 10:36:57	用户名或密码错误！
☐	443	36.45.[redacted]	2018-02-28 10:45:45	成功登陆!
☐	442	36.45.[redacted]	2018-02-28 10:45:40	成功登陆!
☐	441	36.45.[redacted]	2018-02-28 10:45:40	用户名或密码错误！
☐	440	36.45.[redacted]	2018-02-28 10:45:36	成功登陆!
☐	439	36.45.[redacted]	2018-02-28 10:45:36	用户名或密码错误！

During the investigation in 2017 and 2018, Lookout researchers were able to retrieve the IP addresses for logins to the administrator panel since mid August of 2017. This included over 100 addresses.

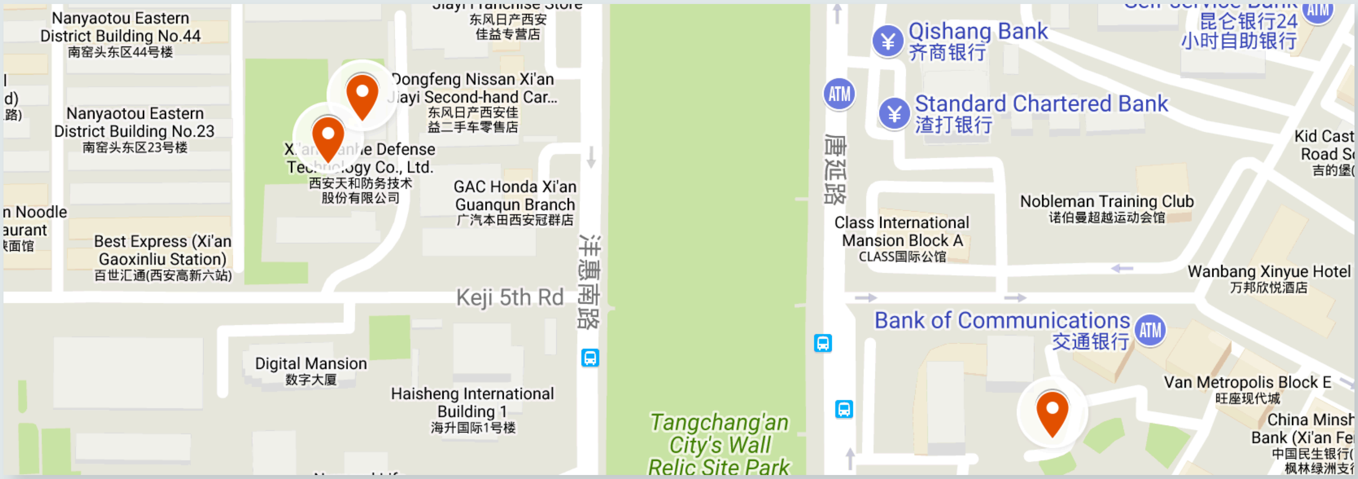


管理首页 > 钓鱼URL管理

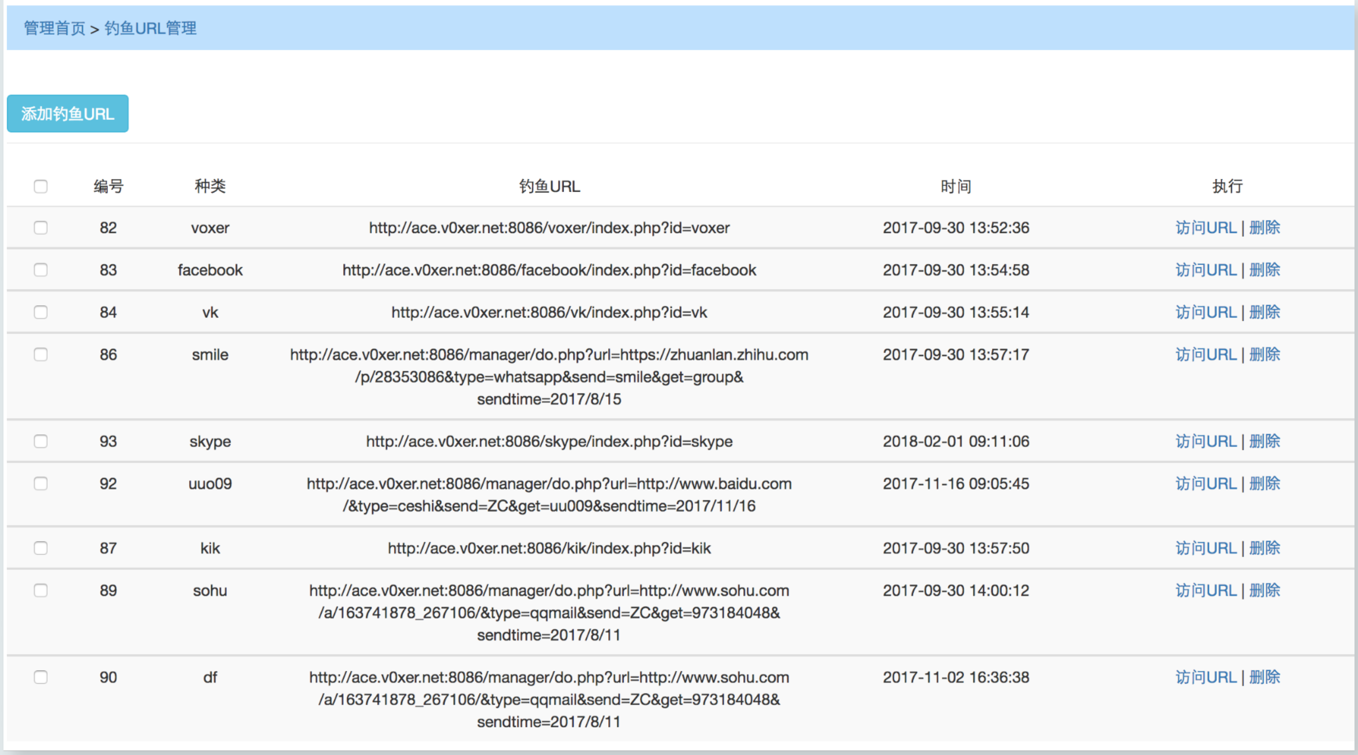
返回

□	编号	类型	发送方	接收方	发送时间	IP	GPS	时间	执行
□	220	qqmail	ZC	973184048	2017-08-11 00:00:00	36.45.[redacted]	34[redacted],108.[redacted]	2017-11-03 10:26:26	设备信息 | 删除
□	219	qqmail	ZC	973184048	2017-08-11 00:00:00	36.45.[redacted]	34[redacted],108.[redacted]	2017-11-03 10:24:06	设备信息 | 删除
□	218	qqmail	ZC	973184048	2017-08-11 00:00:00	36.45.[redacted]	34.21[redacted]1,108[redacted]	2017-11-03 10:22:54	设备信息 | 删除
□	217	whatsapp	smile	group	2017-08-15 00:00:00	36.45.[redacted]	34.[redacted]3,108[redacted]	2017-09-30 17:12:38	设备信息 | 删除
□	215				0000-00-00 00:00:00	58.61.[redacted]	,	2017-08-15 21:34:17	设备信息 | 删除

Target upload logs as seen on an open GoldenEagle administration panel showing some of the earliest uploads from infected devices in 2017. The logs shown in this figure are most likely test devices.



Mapping out GPS coordinates listed in the management panel shows a close clustering centering around Tang chang'an Wall Site Park. One of these is located in an area labelled Xi'an Tianhe Defense Technology, which is a large defense contractor in China.



管理首页 > 钓鱼URL管理

□	编号	种类	钓鱼URL	时间	执行
□	82	voxer	http://ace.v0xer.net:8086/voxer/index.php?id=voxer	2017-09-30 13:52:36	访问URL | 删除
□	83	facebook	http://ace.v0xer.net:8086/facebook/index.php?id=facebook	2017-09-30 13:54:58	访问URL | 删除
□	84	vk	http://ace.v0xer.net:8086/vk/index.php?id=vk	2017-09-30 13:55:14	访问URL | 删除
□	86	smile	http://ace.v0xer.net:8086/manager/do.php?url=https://zhuanlan.zhihu.com/p/28353086&type=whatsapp&send=smile&get=group&sendtime=2017/8/15	2017-09-30 13:57:17	访问URL | 删除
□	93	skype	http://ace.v0xer.net:8086/skype/index.php?id=skype	2018-02-01 09:11:06	访问URL | 删除
□	92	uuo09	http://ace.v0xer.net:8086/manager/do.php?url=http://www.baidu.com/&type=ceshi&send=ZC&get=uu009&sendtime=2017/11/16	2017-11-16 09:05:45	访问URL | 删除
□	87	kik	http://ace.v0xer.net:8086/kik/index.php?id=kik	2017-09-30 13:57:50	访问URL | 删除
□	89	sohu	http://ace.v0xer.net:8086/manager/do.php?url=http://www.sohu.com/a/163741878_267106/&type=qqmail&send=ZC&get=973184048&sendtime=2017/8/11	2017-09-30 14:00:12	访问URL | 删除
□	90	df	http://ace.v0xer.net:8086/manager/do.php?url=http://www.sohu.com/a/163741878_267106/&type=qqmail&send=ZC&get=973184048&sendtime=2017/8/11	2017-11-02 16:36:38	访问URL | 删除

Screenshot showing one of the open GoldenEagle management panels where attacker-specified phishing links for Voxer, Facebook, VK, and Kik are listed. The translated table column titles from left to right are: "Number", "Type", "Phishing URL", "Date", "Action". The button in the top left is labelled "Add Phishing URL". **ace.v0xer[.]net** was seen live as late as August 2018 and resolved to an IP address to which a GoldenEagle C2 server (**www.vipapkdownload[.]com**) also resolved until September 2019, suggesting GoldenEagle was used in multi-year campaigns and may have leveraged phishing attacks at the same time.

A small number of GoldenEagle samples were also found to communicate to a C2 server known to be associated with DoubleAgent activity and tied to SilkBean infrastructure mentioned previously in this report (**babyedu-online[.]com**). Titles of these applications appear in English, Uyghur, Chinese, Arabic and Uzbek. One title "Abdulweli Qari" may refer to the prominent Uyghur Muslim cleric Abdukerim Abduweli, also known as, Kerem Qari, who was imprisoned in northwest Xinjiang[42].

This follows the consistent pattern we have observed in IoCs within the four malware families discussed here of leveraging the names of prominent figures in the Uyghur community as email addresses in WHOIS information, and titles and content of malware samples, intended to entice individuals who are engaging in these topics.

A handful of GoldenEagle samples also share a C2 IP address (**203.124.14[.]109**) with known samples of Spywaller[43] and titles of those samples were Uyghur targeted, yet another addition to the actor's Android surveillance arsenal.

[42] https://www.rfa.org/english/news/uyghur/cleric-12142018153501.html

[43] https://blog.lookout.com/spywaller-mobile-threat

About Lookout

Lookout is the leader in mobile security, protecting the device at the intersection of the personal you and the professional you. Our mission is to secure and empower our digital future in a privacy-focused world where mobile devices are essential to all we do for work and play.

The broad adoption of smartphones and tablets have created new and endless ways for cybercriminals to convince you to willingly use your mobile device for their unlawful gain. The most common start of a cyberattack is a phishing link and mobile devices have enabled new ways to send them to you. Phishing risks no longer simply hide in email, but in messaging, social media, and even dating apps. Because we use these devices for both, protecting against phishing is critical for our personal and professional lives.

Lookout enables consumers and employees to protect their data, and to securely stay connected without violating their privacy and trust. Our platform uses artificial intelligence to analyze data from nearly 200 million devices and over 100 million apps to protect you from the full spectrum of mobile risk. As a result, Lookout delivers modern endpoint security with the most comprehensive protection from device, network, app and phishing threats without prying into your data.

To learn more, visit lookout.com.

Acknowledgements

This report encompasses years of research carried out by a number of researchers over the years. We would like to thank all the current and former security engineers at Lookout that have contributed to this research. A special thanks to Katie Kleemola, Michael Flossman and Andrew Blaich for their pivotal contributions to this work.

Contributors

Apurva Kumar, Staff Security Intelligence Engineer, Lookout

Kristin Del Rosso, Senior Security Intelligence Engineer, Lookout

Justin Albrecht, Security Intelligence Engineer, Lookout

Christoph Hebeisen, Head of Research, Lookout

Contact information

threat-advisory-service@lookout.com

Appendix A: Targeted countries

While studying the malware in this report, evidence suggests the targeting of fourteen different countries based on language-specific app titles, in-app content and domain names. Twelve out of the fourteen countries are on the Chinese government's "26 Sensitive Countries" list, as found in the Human Rights Watch report on "Eradicating Ideological Viruses: China's Campaign of Repression Against Xinjiang's Muslims"[44]. This compounds our understanding that this long-running toolset is a nation state actor at work and their target is the Uyghur population.

Country	On the Chinese government's list of sensitive countries	Targeted by the Surveillanceware discussed in this report	Evidence of targetig
Afghanistan	✓	✓	Titles and in-app content in Pashto E.g. " ئىستىخارە دۇئاسى "
China		✓	Chinese titles for all malware in this report E.g. "设置", "安卓更新"
Egypt	✓	✓	Domain name **egyptedu-online[.]com**
France		✓	Domain name **francedu-online[.]com**
Indonesia	✓	✓	Titles and in-app content in Indonesian E.g. "**Marbel Doa Islam**" "**Tafsir 1001 Mimpi**"
Iran	✓	✓	Titles and in-app content in Persian
Kazakhstan	✓	✓	Titles and in-app content for Kazakhstan E.g. "**Kazgu**"[45]
Kuwait		✓	Titles and in-app content focusing on Kuwaiti services E.g. "**A2Z Kuwait FM Radio**"
Malaysia	✓	✓	Titles and in-app content in Malay E.g. "**Fiqih Islam Lengkap**" "**Doa Harian Islam**" "**Kumpulan Doa-Doa**"
Pakistan	✓	✓	Titles and content in Pashto and/or Urdu E.g."**Shadi Ki Pehli Raat**"

[44] https://www.hrw.org/report/2018/09/09/eradicating-ideological-viruses/chinas-campaign-repression-against-xinjiangs

[45] https://m.facebook.com/neombbs/posts/2183704765076748

Soudi Arabia	✓	✓	Domain name **arabiaedu-online[.]com**
Syria	✓	✓	Titles and in-app content focusing on Syria E.g. "**Syria News**"
Turkey	✓	✓	Titles, domain names, and in-app content focusing on Turkey E.g. Domains: **turknews-online[.]com** **turkyedu-online[.]com** Titles: "**Türk Tarihindeki imparatorluklar**" "**Turkey Navigation**" "**Al Quran Turkish**" etc.
Uzbekistan	✓	✓	Titles, and in-app content in Uzbek E.g. "**Qum basqan sheher**" "**Uyghurum radiosi**"

Appendix B: Indicators of compromise

SilkBean

Command and control infrastructure

www.turkyedu-online[.]com

www.englishedu-online[.]com

www.turknews-online[.]com

SHA-1 hashes

6f233bd2dd5a14cdfe9fa3ff47e690b6d053dd57

cd899fa2da860994ee8de197630ea8ce11133417

3da34aaf95ffcb5c5d36c2a9fc542c1b08c36d2f

c04f65fbe15d0162c42e4d2537a17fe961e926d1

ace3fdf12a5fd099043840e0925347485f5557a2

cd754dcc9c32e0c8f6bd2823a2f14a77a3908d75

588a6f6e34fefb22c5d60660e469789d9ae68776

3161fa0a46dd453bb7afb61ed0baf827778011c4

d43a4918d893122d7a3a18bb7b7d465a4b68f232

1c2ffb37d5c4821adb87ff410084fe4190c67c93

c892e2e6b4bac797ef826053381ddf4fa9d78a0b

90605deb3f359e4deb917b85a38ea40715f1355d

4cc10ba6821b25c162f06d9efcbb4b19d664599d

2efef5273548b11b76fea477a47daf7892ecced3

ea9874a592a870849bd9eb5d6ac491a83726ec9c

e69fb314116badd439a3fc73a8b6e048c6308d4d

03b83059b08976afcadac42b79f867c5601b2b1f

f11d10431c9ac9a58891768739b65b428114ba16

cfba235a82ce2a8293ad784acf85a73109637339

f29be82a97189dd06f50d5354e8c22db9af4923e

3d201dd0d3c316cb73063c63651d8f3c97f2d2f2

c5c2b8bcf3944690a9a19da6e1b0cf047e98f5af

18d047a7a36ff489f12b8a69088ccf46fcf3f44f

881b1650c66017a16d0d150378ff58282ba082d6

c360eff533848fea55fc9f5b63873730ec3454c4

f439a70c07813a030d89b555919e067c51f60d0d

749641dcbe24f38691fd5766817fbef4ca8984cc

c265a6bc184e29089be6947e67760af1a7fc52f6

d5a8dc01ed4fc7c0548954076636c0fe49b800f0

ef75e14b049d38a32b134ca1a3588a04476ecf10

7b2c30d93f014bbfa3fd91e0a437f60713356e50

87988ad69bf8710c520ea825c35b571d6eb60db3

d924a562e1d3e5bb86dd76094b177d9864b5ac62

e51bd4f55650bfd940425cf6d3f9fc77380fa19a

f99a071e2a1da49872a50d8a6b1a8b5b9b927233

5fa892e32fb62cb6cef04b1fae8c45efcee99c48

1e51597ec11b7066ecae2b1d96d997498b727612

5aa316acf821cd913157352633f5c7ee683c045d

5d2273c0211c90816b70900657a7b5d858410cf3

2090646d0aed8f25fdf86f29cebb8a3712d3bf0c

d74ee17da62392bce9f78d8528476738e8fc3aa1

c06f8494d8ed28bc82de12b779c646b10ab22b50

5dace7ff4225b27beaf073fcc156753cc702dd7e

4b816090bc6258dcde0f294ff0ffcdffd67d37d0

ec60708f36c1e83ae2609b82330cc65871b377d9

675dccb83682838a69786996ae8b64a194e4b77c

185824386afcb27ca08d333fecc742dd6c68d71c

e26939bd17f0be5c8b83638553c2800d9348b5cf

1e8f424e6b0dd3c31c217f1fa57af23792a71c2e

25b26500ed0407edddb6586dd319529ac793dc60

b7441a192202a8af142fbc43d2b48cab9bc2505a

2bbc387ae74db7a01e80915f9cfc3519ebb52fcd

279d1f93a2a000ce16f4af8ac94344bad29f2f32

896e198988792ed72a17c32e6ec16b4028c77a3e

effede7095a158b4ded6d8dcfcc1cbf18ae6ccc5

be1fd0c561fcfb1123e88e48a66fcb406be27994

eb8cceabc7e127347c7c02e75526f505de7c7baa

25cb46005c80632f1a7a352194efd1320c2f8f0a

63ad2d88e8132a561184c70b37d02eab034b8977

cab9c8c190e357e79ed7c27242824b8cdac31acc

abdf752e0aa4b0fd1da73aaf98479f2e647a29d7

466ca8bdcbea9d436533d8deecfc6b4a8cb0cbc6

70c18146191376dd8eb8195dbf3ac627a2fad5d7

fdd94086c2bfc5af7cf491f3242b4e15687da866

756e685261d2dddb91f9752c9ddda5e353fdfbcd

913861b0229fd80a267070fb3f5596eceaf2fa6e

f1e261665b244a165cff1f3471cb17054174696e

54b35b018e5d92dfef9ea26249b945d53b7b8773

51c6014bac840dc80c650c7797195ace86150530

85bc52ddb37041aa8dfda74628a15153ebc83fcd

1a5e4c13509dd61bad7965ce3a022ae84f8fc13c

fe11cc20ad8fb2eaaa744c7db05dbb5d0918744a

54e826db05deb440bbf376b807febeeed9c0cc01

ba86afd3acda00bc356acbf2eee9c069ef123db6

52a5b29219abba162d1e17457a29778c55e42b23

4dc1e7fb8d84fed80691d084433e8119edba9285

dda6f46e083001af13da1e1074d8ae4ffc4e8542

6b89f5446a6b48e0ac3efb5b641add8b756cb8f5

74c10c0b3d944012088dffc9cac96656f54b996e

f15273a9447adc02e91f350a2c725f533acffa05

e4606d7e05bfa4d5546a5ab2f323785b6ab0b3a9

cc2264f3c7a848709edd476c726eea2c303d5e8e

c703345fd302bb718675896473967b25751dba0a

7b091f30fff28aa41afd61caec11e6e5a6e7d9e0

2f78757c9ba96a48f7014371fb1784c7c4508367

b67f28ef3a23e0a0e3f4a6d3e0478cc81059e2df

a1f8837d7e4745df39bfb35434860d2366c65301

465ef90ed1b178b9fa0aa193dbab2a42aa4c8b15

048f450b9611011bb71444f46262f37ca53aded3

6760fd139d51961d9786f9a609ad4c173f9317ad

9bccbdee2254819957a166bf6a64eb5e6a8d5cac

fd99270e56cfefa94fd5a3b56eedb2b72c5a3e3c

ba3870f2266e314acf1e78ec7215a9fcffb8fa36

f4e9952991b5b9b77825d4ef88c944e8f61596af

f17826b9a8e1f0a786e08b60efbe52950ce16722

f063e2320d77ee66a2fab624a4536bbf252384d5

a30c7eb9fdfca04518bbed9f25b086ecaaaa2e68

7f2a4225291abfaf317b342e925af9f6184c6e9c

ac90079f7c63bfa595b3e9bb1e60b9f365938e9a

ba9bc94a2ff722712f70268264e3e52ee05dc4c9

0c721159c6e73ede8fcdd398b56e2a2ae33544a0

359a0e662eca9f13841387e8b0f3276185d207af

b4612ce01770d280efb3c035c660879674156500

DoubleAgent

Command and control infrastructure

youtube.dynamicdns.org[.]uk
tree.ddns[.]us
coco.wikaba[.]com
umare.zyns[.]com
phpyahoo.mrbasic[.]com
androidapps.spdns[.]eu
androidapps.fvk[.]cc
androidapps.linkpc[.]net
androidapps.duia[.]in
heartsys.dnsapi[.]info
androidapps.nsupdate[.]info
android.apps.us[.]to
androidapps.spdns[.]org
androidapps.npff[.]co
androidapps.home.hn[.]org
androidapps.nerdpol[.]ovh
androidapps.myfirewall[.]org
androidapps.jetos[.]com
androidsapps[.]ml
androidapps.tempors[.]com
wephone[.]top
www.turknews-online[.]com
www.cookedu-online[.]com
176.31.115[.]156
babyedu-online[.]com

SHA-1 hashes

4ffc6f6e5d54d2cac14efebcf4d63c0310cce2e6
19e96c58db322f4d7f4f074fc75a1236cbd44db8
884dda8df2f3a5d85d6475fab3e38f8fdefa2f5e
2e52d2cbbfe98702bfbd72efbee5674665472632
4c108d925d6b0acf1b940bc56034f812a8f53b83
d9e61ef6966510920fd2bdce5af33a2e9136cbd5
dc9c90b95712911e589764bdf407c6e3c67a8bae
ae599259900433b82692d8b07a696a0c5c3897cf
bc617634a5a40176c9af6040fe56b1907fb026ee
9814797aab670b7054378c050e35f1a7cb960bd4
8a1594d91c3a795c019f92140d9a5c0a26f4b470
e6b0b95f22d843892de6c497819c8099d0c80101
057d174eec03e19a61b5f53998dca028c499359f
04d710458fe84ab9731ec71a585206a0d6078b84
1b6af2bf7255ebd07d069e0347ca3f3d183cabe4
e63b80390ea82bac912d30b1eafe61326f0e707f
1030f7e362cbaddc8965fde9a664e4d21d8ceafd
9c7c6eb949b3cb25ab3dabd6470cdc3cc4ec59e6
528e84f9029e20d999760db629dba881395d9a5b
11c0e0502f9cf7515806f74c424d7c7d43067dfc
da5128cb25c91ce56c614369ca16e610213aa872
70445020477a181c3616af3fc5f70884dde73125
a747c1c17efc4b4c3afcc80e9943297e1abe9497
ac664ac57f4b32b1c71d91b8a0ca4f9fcbda8a8d
61c0837583e9bfa915b7d897ed9d6b6c0faf7e4a
20848e59e23509f3386759cf6ab1eeabceb5cc68
03b136350422f40e9d5720ecb53518b587727d78
9771ca4315c13d8e85d465dd6d9d4e169947ba24
2f966edfc175c367c95dc7292bc7b1203bd93a4e
ae08317008f7cf7ed4e26cb27fba3c55aa884bce
584dfae56ba04776d630f8a0179c9799617dfc85
ae7b653af51f5216af8e11042370239dcc1f4873
766d67455a5e15ad0fd15b530592776c63aa3726
4ec4bfc9cfe555e2990b447962181c43272afd3b
34de7568ade42cdce527b218f465098a200e4115
ae9339dae4030729de951fac46df93839b952515
d5e569428cabae25c6ff7b3fe56cb687947a846d
4ef9f46ec78e3e02597e8d3b89a765d815b7ab59
f88ecacd1e5a79fdffea0b4a47f37cb262d1df7b
d2809652569fa8446f1d0361e3ba0063a503fc94
0b3f1c266db60e0423463a45321f20fefab619e3
5462c92eb482379aef3e79e1b965640ec3901541
1ccd2a6f6b9875b3e41becc2f4436f40b9bcd6b1
1d440ce51a85a2bd145e80e093237a57188ab056
8bcf7788cebe1343d7602bb24e19db4e5a4c50b0
ab724367d7ae9e75a5d9d46f29b74df157aea446
54543f096981770b397e72fff1c138628f010cbf
015ea52dba3b0e13d1acb4c1f2904b90eca2312c
495b622d8209820022fe743c340b39e6e9313cd9

CarbonSteal

Command and control infrastructure

61.178.79[.]131:8888
joke.upupdate[.]cn:6006
sz.secpert[.]com:8080
103.66.217[.]15:8443
103.75.3[.]59:8443
6006.upupdate[.]cn:8443
ss903.w3.ezua[.]com:8443
ss904.w3.ezua[.]com:8443
119.36.193[.]210:8888
58.49.109[.]166:8011
58.49.109[.]166:8012
59.188.236[.]193:8012
59.188.85[.]70:8089
61.134.50[.]45:801
61.134.50[.]45:8011
103.66.217[.]15:8008
103.85.21[.]175:8088
6006.secpert[.]com:8008
s101.secpert[.]com:8088
111.172.155[.]190:60066
s2.upupdate[.]cn:8088
113.57.68[.]223:15005
amote-366.vicp[.]cc:15005
103.105.59[.]47:8081
110.153.177[.]126:1882
103.74.193[.]122:8081
183.94.24[.]18:15005
59.175.144[.]74:9091

SHA-1 hashes

5724ede472e9ab95118445af8a51f3c6d926cc6a
bdd778a75a8ea74c1dd0a06fc1ae4d41e5518d91
a3f91dde5854bd781b15c307ce03bcada1baf6fc
2fddc6122fb8bf9c02d5e6fbd5c8acecf506282e
f55a23e54e91c843f8fffb243ba0d1ebaf4d5d3f
dae02a7e00bec86f832069c2ff1328054e0e45ef
fc8251d0ded073fbc9f433f74e7c862b27d9778a
349388eae390ccfaad2bcc7b06c1419d3577c7f9
5ffc5fb3e6dc994cbcf0953be46fad5909725ed1
915d1c78343f0cd7d75abf03b4b33be415f194be
65cac7c80f3ab562b0a239bc36218bcec70f6ae9
7f50149d9d8d852f05a95016db788b04d0b30139
314ef5243aefb9b5d9142ce92efc3dde5d3fa041
60604d7a9c42c2becf2f2f5af6822d058eb6ae98
b7417c10b7a0fa613fe997d305abcde8dbcc1f2c
b2686fb961e4294996986166aef3bd4254e99cde
d56ec882a1d2e9176c13c3fa46677ead65060347
96437decfde286eb946e87b47d8049c6901ea229
f2341bef7212cd6d15638c30076460b11321a2d3
d69efaa8134305062af65d778fb79d678634b143
6ab2414fd44d84303e8698548ee6c2fd4dfd78c1
099ea7ad09561b928fbe3a7a4a80df5e0513bc2f
2db31f2975ad14c41c543c424224ab8f7d632b51
d9ad43d4192c16190786ae89190113931b438909
02dce68dcb63259ec960b768bf5a1587db7c2de6
aefaab4fd236b25cd7fe91210c0176d631b7bb6c
8bbb3fb5cb9bf6ea01c3f7ad576eb5f46b563adc
db665ee1390a7e5af882f249e8e3dffe9fea341c
aef186dbc332d564aa3873254d5a50f307289195
1ee4b076895c38de7cbd99a8db79b281c9175fb8
e54b53507f07122648f44168059a483cbc26d985
0fc290c6448dfaca535768c594a91e5d19855079
5c320a735af73e42d39304259166cc37bb43d4ad
3c2e1847ff78d715204f3df9cac88c78ec99abcc
cbca9b0b9c0e6698d8613f7b316be17fcd3f9452
a55f370b17346b95cba4632c6a96eb147995568b
d00cd405739905863846d3f50a380f1eb11dd95d
2742ea663ae1e139ad15176318c1bdb4a1bce342
eeafcaed236a56f75aa63e209106c5268c8a51f9
9becc7919a63ec5188629047e7ca02d7a592f314
e29cb6451f6d65051367f1c85702db29b3fab9d3
d7f5effd58242607ebf73b934dccf0757d516e61
797034d3094e38d0a9b662c793a1ca5c94279886
f81f2dc7cb0912c59c83c4631ff822b00e4bcf5a
9e6297136ca7bc8da094bf3421c8be4595ee0db4
1df29ec83d0858c04557a56d10e5ee482ffc03c4
0e548d81f9d643c738d2268987e487e48f84310e
56ad6fe0f396aa404a12a6632e3a617258933bc2
6f97ed9ac4a513cc336478bbd3052b2bb0ffd5f7
921fbd8b97ee504d9d50a40b7647a631a5c32112
5dc6e3e4800cf975f1b387d7d4e2cadd1133955f
047a86dedb4f7b8f40d9437b77240f5999ec0618
4d0a86cacb7d3ca4a6cfd5afb5ab9090e39a242e
17a8bce4443652c054d303c99c97930effd9fe65
c452211eb86106045cdfe0bcc275bb9ecd492a30
e104339eac2a930aa0a4ccf549e0f49f32779aae
eb1243d5f293087643db7263a40516026b69e697
024d96f53ae8ab0f88950c3a9c64a512fd9ba15f
3e164390e6e1ba6353c59ccf7e369a93c6d8fba5
ecf28386567295548a521c171bd272e1462892d5
abaf1b3bc5124996c3e71e1ef518b180231bdaaf
0b82a9c1fa175131769e3b04ceee24517f37df63
23c78f97d649e6a4ede3245b171fc25ead1a1919
8dc1a5d02ae3a2b94d26737fda5935e8b2ea3373
0bbc2ddc25c3dac95910ed999409d5ef75338a0d
125ce4e75849fd89628b99d354f195add80fef1e
18187e97027041bad10e8788a521e926c7a50d8a
8dafe7dafa243cfb4e1380322117f7acfe1ea762
cfe527d6c5334881b43aac5913a8705e5ee3e063
25cd850805d4046f69a655ebb4c1e402ed25d820
2a7e4de77e689e5f9eb46085845e3b97fa987b7d
75b8ac15b40e64010e89a0eda5c8d61b70955a6e
f7314f7f5b45275376e78ca3703fea7576f33c85
f14275d6997727a5d12b0bf5679822e9d00663be
e935800fe076e4d9f5a82e4931ffeb39e35d1048
baa91c6598f4cf23552b0e71c7a68fdd22c6a41e
b9fb09c14458eaf3820196e26500f3e99b21b8cc
a1f7e8964f326582997c9d3f7f6a78506103e89c
8de0e7c3593470e58bb86f496f99c3d2a66cffd9
1e6a8534ff7268565ab7060489c2615028dd8dac
4b14342c3615fb9c87e67c690d379fa1c4a50627
112384a853044d02898366c6c85367ccb7d3aba1
b33b6594f26a3714a456db835f1fc7a11a76841d
d7b679b16f4ca0c4b9028d05c280f1d9c9ba0936
6b7557b4f9f70741da96cee66a26dd3d84564cf3
6861526b0227fea0c81a8083d7fb3d7b03b5e3c8
555ff1569ec8ae7a7d337f0c4b152f4461f40151
85da33fb9a885ff3a21678a649ff9f342a1ea0f0
036cceba8cc2a3af153cf0b64318e11d00fda1fb
8b2df91a33166f6b92e33b229d05e11ba4da240d
23d03c2fa5ee3675ce4b9d50cff956e9125c45ac
cb1f29c3b47a18e5dbc970f2111a8ceb04d2629b
afdd9ca1cc49a058e5dd703989a7cc613b565e30

```
6f604d0623f02e7756cb40a75f1a126f68217ae3
e7402a223c1850f24a548c58cb64312039c84181
cfb6e691db3b1bdf312083de1d43c1ae328368e6
2ff068afdef4eaed0435328bd0b835648d21a703
d317dae23a958cfeeac80fdc8d8587fd07f1e190
7303c87a81c02007d524d471f45575580c26d946
dfc7dccc9a0738a591ef302baa45ecd8e45c0a34
ecbe302daafb23eba47960031c659c42e1f9b24b
82fe511a4fda38816eea0b3e4c13cf1b6c188e37
da7891b4929d4584e0a23aa7db348717d1676de2
f97aaa8aed12a8c7dcc03820bc5a4aa3627c5fc0
13283513e0f878c2917f35b60eacffbe1ba642b5
baaf2d9bf2aa0ec1a054debe6a7dcff08c84c806
ad7ed76b9ef57c5652aae1768411f7526bd8a4dd
ef188556c8bef4d57a780531ad8c8acce06aa152
5bb57b72cca53ac426c05c65c05e7494f11861a9
77c76297455ab30316cd73050c6a0b34d9bfb908
ac7c7a79e3e3542a83653f666ea9a1d051a61e3c
51516de8b4fc06c0b5962bd0df8feb21049bcf2e
a683095322d9bcf0a53ba0897a70680a1922aeb0
9651e092e97efdd569a83fd1945c82acf1ff4b7d
559a0c3e3bb956c3064558e087ec45ef1d4851b8
caabc9337548d077850dd7d56c89bcc09b4fd7c5
8d663a5e72c6f5873eb40f35f1e37ad7ce5e7c93
86d0272c5b4785838461d543a5be99968f73c39f
e20db7481cd4b717d428ecded61cba976912e442
4b7ba950b06ea3648bdd075070f2b5d2b1932d9c
216be9f014648d88f2604fcfd451fdb263d13869
8a831cd90631218c9a228cac4f28d9782eed1ad5
9c553a3d9a31fbb606212b45ed2b88a7ca4145f8
7c8bcb76b70ed5c1e4508d8fb3e068d7d5d954cd
6ca5b82ebc47c5f1e9250c13f6934349fc22d6a1
d4f7d9d5e23411174eab5d76b6e54ceda27a878d
7c18c34e4cb334d068b2a228b429c9a24fa101e9
84c3e4dc896e5b2bf879e0e79c2de50ed874846e
bb887c4c52b0c70b64e54bd21b512b60d67dbe58
94baf1c21be2fdb4b4cb67e148f5e9c1a3c78ea6
b424e5889b959808992da819ab572f59792f6565
0722ba84781fa8bcf3a158bcfef69808cb7f5dc5
565055cc4c9242b937750453ab4aa05afdc05076
e1095326109c253601396e2ee69253daf67b35f6
8b10b32e68b007e98f370f31c9d3832021c67694
e890c65e1a9f1e44132442b530637601c2cfedd1
93819cb8759df31bef7398ce9db1c64c5189c20c
73d6d47324d5d9a58ba822221c21eb32d9b56a24
956b5c8bdb7a5bc73456046b2002bc6042b94d11
df7008f974cc6cf91ef8774dcbfa8de09c04c157
8065ac802407ead2d64be8910691a16f6298a61d
2ab4a32bcab2634d089af7f1bbb7770cc9d042b9
7fa0f7bc7a937168cc9f59ec8928e0c1063872db
aa08c1c64365c1e9f76aac842436c07752306009
55a84ac6a566d2452cd64e1211f6938837c67e7e
58182aaa2ddfefce02b22bb95e61a889e87c1ff5
b8a85fd804282f06ef3959224e3ce4c8bb82f5fd
adef0426ba512b1ec5d63efce493ba68560869f9
2e205004e054955ed3056d0675fd3c7f4c1b9065
89c5d6ad1c71fbfa502ef13332808fd99ec81ffb
59ddc262e0a7bc550c68bb3072aced37594f47c2
627e4071647e5102f8bf0db0ad9023e93de39513
db66fccb0c310c08bef2073272ba2959a870d32f
d5444a9ed5fd6bb44fde63879f26731c2c9329de
dc54aa8d7c9b20910d62186f8ac93fc9717a38a1
64e704c32aeb22f3d53875fae697a82124c92675
96b4392a7fc36f4aa0ddc766e0ba46693087cbdf
4d2c94a3e133a4fc62e9192b5114d0c18af268bd
f1ea22e79544b1387a80b6c01b832c76c17520b4
53683276b45a602226937b1af279f7825830c312
b30176e7d1393ee5e6c60ab1d5bf1c13f3ff8b7c
0793477a2e681de9ecde4a7deec97acee2f5a381
34a4125869b2c529a3b2a2d1fdedc8b366151acf
2cf9bbb75daebb7bf45f3ff4eb2e070d06df7811
9abe5260de010b033537a5b46d301f449c9f7610
2612d3bbe2ca2d496b64de2d35da3ecadd681b50
5d12a334c3e29217d859ef485a61e6f1e8add44f
d95e8cabc37e70928f7ae19a67ca43b13aa032a8
292481294740a62f6b03dff8f62a561d748fd703
ce1967084161ec5de75944430005f62899393a56
e6f6adbbdef2d7b8249c2c34550ad04522819dd8
0a662befee849282355c6741b1dc664e55a24ea3
a01f01e1fb71eef258bb13a711f442f220c5470f
4d17242540ec8b3b2121b4ef9e709ee2e2705891
b43fb877639cb9499456e75f9dbcb7b0a4737f65
1687562d7cabfb70c21edc6bed72dac446d30c23
140d0aeade124097346e742d14133e98204e013b
246b54f0c7401ceea4d3621d7a665cbb0c9ec1eb
d46c526d3cf32cf1a137ad0e1a4dce4be32879a8
da47014c615c42089e2a802f0fedebb67f57a696
af6bcbc1697008480e0fec1b33cdad45cbaff71a
cc71a0165307765daeee63591a9dbdeef6af213f
b0e05d19231fa60525abe553b2703357cb239e0f
20c5076642f47028e95cb8cefda0956b2f75f0a5
be38147ad07d92918f4b897d3c89dba06d768f18
6ab0db39ab402495422949243544bfa884416b82
59e4fd71b2cfdcb8b7875afcb1493d19b31f9f11
30ee6055d0014f9b61b255980e34391f7a1542bf
0b4a7658e9c6872e5136bf5fecbc3e0a74787004
93a05195cf1cfab0a619c0b23ead04ad4d71ca67
aa1914fbbbac325f8d1ea286f3cffdf4352be74c
8487e9ebc5895c403a90ccb3c8de74210fdd96e5
1a27ba2cd009ec0e2d20157fd885045a7193e451
b070dc1180f02d3087daa18c696f9ec5a47f4e05
e5b0652393300931032d253ab4ef5aa5bcd9149f
0173c75595151fd9528c98e9b4b122417dc0be39
84d1f7209dd96407119f64959ca99aeaa31983f0
60a299c52e42cd642b8d9b3d2b4002f51fc22304
e1776dd5f073448685560adfbdcc2935deca12cd
ce22bbbbf456ad7bb116be413761a9861a17270b
ff24a49453984bcbe5ad21b7234f47961dd8ef79
e53add8a18a1a4fa533df2b83b6d6a4792c22a3d
5ec7be551e191487723882f2057c9315c30e233a
4b866ca93d780813e176591f9bb068a8a0a1be69
f024b7f0351ed8b9c4c976789e546d0da58287a3
757070c70536372e6d6819e6d9dafda9fcd43541
7e9e1b4592a4b0f452756fb336970dcf3cd67b16
40051d7efcf981e2c9e4111e301c612a81d76ce9
6569edb6106e24bd70cd98337ffdcf9cdd478bc4
fb486b21faf725293cf825822ad3985cc4794d01
f18e0ff59871d0fed7bbb8fb0532299c8bb1c92f
ef80d10a89351387c04b9da5bd3e876fb55f350e
234fbdc5457390202d0025ed26cd779e2c003e62
7576ed2e6939c18ccebbdf40e322bff7fb15bfaa
ddbd18a28712b0ec34743cc28d15f73f6765ff34
d6b99179db1e48953158e5f88d64685925bb1c7b
570b7f3eefe96bd90216116017101a39cb1960ed
d8034442c03d878a4beeaeec56b3134d835a8661
29632ac2b1a9df3baa2a902d57f801a470d08a0c
5947431d3ec1034e32eb63bfa51907c6b6d6e636
b2cbacfc4f38bc11d2b45cd5ed2773fbacd9474a
51e8d35912e444f3c84765d84b87b2c95a2ae5e7
0269381e64df80d1578d5e26cbe50eb064e05baf
5e4763cdd2bc724315cda493cbec59e0a27f174f
7ab78b309d1ff8febac01ca022a28a25405a6412
c1cc1ef8cd86f7d4c416ab81b8d3761b665f2634
f5df123a072a8722ad72f56d9f25424ae0996876
b6e2bee8110b15ff97dc6574e5b83b4ed6b44380
640b97ba93f587934e474fcb41c8a673c957911d
d60192d677d1cfea79001ef3335bf6a310a7d073
482810f768968e48d2b81506af12f30f07373533
4fa17915a95539f5dfcc23c92a0d23e3f944f238
e9196aeea3c18aae07ab35404d038f9327dbb50a
05fc39025ea168e09ce1155d417d3ef7e19fa6ba
95eb169d3db1df0e1e12eeecc6f3abce4c36c16d
e931cae0e9a1e5eb45f0bb13c9a1f99cbd630e2a
ee6a2fd62a4af5d639235835e2076b7b873e8c79
8d1444fb219b95d43682a97a19398e760e9ca1e7
d2bb4e76346ada3fccf97bc04c48fd4b5dc2e8db
ea675f3e7f70157cc3b022c691a074ebf7e8ee37
7b39abe0cc0765ec21da6bff50d88453f6902ae0
2138f222c7e03f34d9cf24f0445880c473f196dd
458dd3f7b98fc934f0be4d622c3ed55f26cdf373
978a92470c348e39fd026bc6a837f97b5836a732
7ad9f960b711f4850c4899a8703b5ee32dba5838
98e56742188c7425469876a3a1e588be66d1a826
b46058fdc99ac46b5b3191c3558391faa4f9dfe9
37617eeab96b49b775d9762bb191e816a749b5ef
b617398df31b46bb64bfdab5d2cc40e4847b5122
```

bb10bc8c40ed9f355ab7de9b17aee1c7ea2433de
54e9d977dc62d1e106c5e04ac1df1e20b5393b7e
1065031035687f6ae77b8ded183781f02b4cf086
dfab785a05940c0177fef7220bddda612402e249
1564d93d463d50ffabd090e82759595d9815ddfb
9617db2bb67bba700c7274d92a9181362b305ee0
9516a3d24346b751d2886a8390bfe07f7a0dd01d
7de36b546e0bfe3491d94cfcc2e3712fbeaea7ae
9df0eca28fbe43d9ff6395352f459a9d9d0f8fa4
9a3f104627a230b72aeba048e209db516df748dc
e5c2428ec5ac7b9c8006f4e9ee8f16645d49463f
d2ce5eef92513ae09d058e04bc5f4ec73088dcc9
ad728e4149c3d14b41109e4307282426b980249c
dcc9af898ad14075cc6187812917c91639623ad7
a3a7b44d2cd165578392959b71eba5341b3b7835
828ba08b033a73b291a1d1374626cc24435c7e39
bb895ac7509556962de4485db940b90577d8dbb2
36edfa97c178dfbf19f6e0dc3f7dffa32747d3d5
c686cdc89c525264becc6adebff478e79ac106a7
b39914094b8aa08d6dbaa7d925b43db4edd92ebf
262aa0c4c02508a93bd768c1b092f4de994e24f7
0404cbce95f67bb7c745f6d3d077e4eeafdef3b6
8e3a41c5617ee9fd10bd6004c0e95547e53568ff
2a14663b00800d2abf454f3778ccab97dac8cf2f
708c4836e36d87dc0a75aa22a8f2f495156c903b
1f13a4316370d7172bbe6a9c744e32f13564336c
fbe9b1cbaaf66f8e225f9b974b30b0351dcb1e6a
d39ef8c71f48c503d8d5232bc3231d592f0d8ac7
e20130e98240514922f37594f0b533e58c5620a0
704026ec2fe31e43241f77c9c20f9a8af7722a76
17d2e5493ef7b0a589c7d26cd60d8ac519fe7d5a
a19371fd36bce8b5b78ec385f1dc2f15a50043ee
3bfa6925f88b4e1400a00556ce45c1eace95d72d
14f2d0d869c70875528dd0390006a811767e10d1
fdae5711b48e9e85408c870caea29065821ea444
d11f0ba31c1edd0d219a4f446c741d0d79248cf8
29dd34a517e3442c07f1fd76b2bca184d11fab51
e6607b642c58c3e065a3a0aea697640f5e76b26d
2fec337501cb19cd6b52ef2098a26c5026996b04
002d1ff08c8a058cf65eee591d33ed96c3e03881
362d6ac2c498875f83b54c83ac0fb7d6a805b118
374d8c3477ebf20003b268fc65b45332abd89d46
bd7c65bb1032237c368e5b05b2bab4657d4a3b1d
64ab1802f02d513660001b69be34268d2ce662f1
00ca9bf4eff6d0ddb784c3de0fc692ff289099f7
4ebff3d6543d25e7b4a4f1badd73e1676edd711e
60b1b47572b157244450a9e31d381138e78a4488
3bf98a26f6a6614c90b513457eff180373ce9ef2
a9f51cde2a3aa34d7d5d28ac1f8211117949da67
410da91e6e676901e71db6b8a01301cf1c5bff0f
f99c8aace362a76609ef4e9b1c6684880b7beb38
bb2f09c8e8bb2b84505aa50a7d7f13f713608b21
2d3c79522b094b43c3f641cc0943e812ef0a605e
da572238550c49af3e619ef38ef070c68e9ee267
c25be97c057b3ff388b0a54d38047f87d688b4cc
0004e8760347120541b175a4f3a45a431e48c916
f8d2eff0ecd047fb157a65d873601952676443be
1c1cc46cf43df567c8e7f7d59a4f4b414a62ff16
9ce7ba50052cf4e174f9f22b022cfae5ca5f9c3c
6f766545836382721c625e803085b06eb1f3eb33
5015f8c9813e6f80baecf26e05f87b5984c9c1c2
dcbf474a1f47b57508cd3bf946044dff54d7e791
72699e58bc274e85c99bb99ff774f9304a736eef
77b7b880c27e03d2e97c9b31f82cbae9bff62ae1
a991e6a767185b1398113302ecb5e3a567f89287
57880d3b76c2cb18fe608e44069f76ff9e0b5705
5ab9489b692a0bab25a2e423cc055faa30df9f45
d45009dd3e231735989701ed597120dfc6299dfb
8ee21a04cf33223c44a1634aa61f3d498e9e9476
f9f70cfbfbf5b93445d459de9137d73505f1f7c6
67cf0d0ec1bd0f3961eaf5720c6470193d76896a
13e62c461e76256a9f88807d0ccd9ef1a03e71ff
88f47016bdbe06b2829ad061affb1aa5718b21b7
8ba53b85a24ec09b98e865cfe20b99ddbd9494c9
a353d2637597ac434c3fdf4c4a7ded3c78b100ac
0a1493bd111403f2d1e3139cfd71c2c44f1f646e
33e762264f5cc53a98cffe4fa91138f2d00feecf
3e4c0a2aaa74861d16f5855951080b659cdadbe1
785281d70b72dcfc179bca2fb13b63f5b9336774
8b96180489fbacbec9e42bc2cf4ebb02d741d308
c82e540c6ce81d941c265eff01ce34a603f96618
d70ab8d4e89e6c0ba3dec422f49e6b69fc8f8fca
4dfd7175714462da2ddc386f8c8ec8957d3a0e46
0dab9f6a808d02420c8cc97b68a0f4555c596999
b07b5c20e9a212ddbae91e17f5ce421d58980dc2
2b3beb402c1a66a7ed315c19533f6e0cb2dc4a6c
3040b00fc192d96d5a639b554a2eb73d291602a5
5bac664a002c40808508dfe91078c2c5d95d3df8
127b25d622ba41d271c4032bab15db3025d6908b
8e74ab2651f98d0059eeef16891f8df7eb301090
f3a87cf7e606f8053921be4b57758046a25015c6
744a3a6f4abd0f22bb3d6b58b3c914190c5cf5f2
837030e79a6ea6440bad5d60aadd613abf521837
4c3df3fed542f1782fe23e686f0c89fc2e54f0a0
9db725ba69faaf1c2b3fa99653f5d09c8b676a4d
732fef32ed70d63b61fcca6ffcd9255710515c13
4bfc9a3edefb9b6757e3483eb4b6fd680efd6f47
bf65a4f8e9735e0b4699be262edaa406513d944a
0d92462b25d9eee170f088ba283d60de3edda58e
e5f8c21659032ff90a7c79872e5a99638fb5fef3
5d1dcd92749e3a1825f24b9ab8f346223faba226
3ea027570a0366ff9112ec9a0f4a0059473fdcb1
cb4949c5f9debedac1298bd95251f83cc4b228b3
bd3246701904c1464d1deed06f38264d826a1ebf
36176c1c2af7d16ecdf308dd2e92b3c729d08a44
598e78462cc3152238ea438481d7d29b880b2b60
5269c8591ff0d25c07f442b67440175269f0c880
72b7906cc35a99502572220c766d96e8013c189f
8b001074cb50cde92a82235c694424d622fdfc2f
b7eae1e90a99630da8f3bf9e18c611f66753c73b
c842d59e57947ee068c891ea105a503a0093d3f1
440777725fe8f6b6536b97bf6af48a02f9b35bb0
1bfb020cf6f137ac26c8e9de528e2d7b849266a4
21717a490c25815224fac764f28ca8d4db68eae6
0148d3706e9a81df8ac2712abaf030bd8227ef6c
f14129e89bd2290fc75b1b8c6560dd1e9863221a
62a17f2b9876ff585846a49d5b701242b31bbd15
1da204fd7e3ea676cbe12d38fc6949b111aad433
c786a0c3d8b948355efce786044b4c6849296683
30956798391f50db7d1780726f2180ef927df33b
573694de1b67c6b6b830bc1e59c9e89a8a429286
18c5b08098dc89d0289b6de5d48f10e7a59c421f
5ca705c564fc19bbde36de7442eb90555593cbf0
0eb4c90c5eaa7a2dd162dad524ac80b7155298ae
f93a527f00f5168022dc37d0369ee22b644caf13
5216af5348dea834b8b771afd4bac9b76923cbcf
56f830e46de2d74733833b490eca7f2c60dbc6c2
baef09335afb61c134b35359f15bd88dc1acea87
7dd50d88b015b3c8cc10a8ee3b8c4d6eb9dec876
4d086e38fca7fa1146408a9532809fc9db3022ff
9b3bb7353cb1b6ae986d0ec4fa4ad382275d1b6d
93955ff5d71e4964da3e22a1e039119bfefbd06b
a807a0ab709871bfe06b3e337e5dc9e83674d232
f8aea398bd66be254ccb72f10c872eefd8d58dc0
52fd86264619a214051407ea9653c60569e22b03
c248bcd40bf276312e6e2ab0ff11aac32dfff864
ecf439cf0e77cedb2934e144fba54a0e1b208541
1a3cf34cb593a649f8795437f4fc6dfe9a84eb90
09e3b207bad6dcb00ca39c14b6a93cf97d4a7070
620384ff65f7ac2f4ff20dd0ef27baa669bb7828
dff29972e74dc4114dd93540aa421f37223fe166
0296e4c9015a869fb42db167a3b9fca4f842cef8
008135dbfea63c36b03a5691e3db8b8df5ffff3a
eed5ca2b8bf72aee2e821aa8a627983b8092cc6d
1c9ca715d77867396b287466d56f18c6fdc41e4b
5856ef764eecb25bf6da2d3c48b8a5dfc0f34a66
b353d88de53ed3b34926269fc6b8f803fa8acc02
0886795dccb94e4e34f2c04c6221ed35c2e706af
05b8c008ea72bd485d6de2c0c95e21e7de448235
d7d6e1446f2ffb9474cad04edca07d18f4eb6da5
3f032b054a2634154914501e3234bf922cfdb384
206a2a7a9011f8020fa988aec43aa52cefe0699a
329164b6af83d0ea6b300bb874a9240925d0aed2
0788a429e6223c9836f5e46bcfca59a4f07ec091
2047eb02c07341340e1f82a7f3444d4d25f434d3
d932f5f078422b2ca16899b90ec4f6a4abc36969

```
1579f00f41e4644ff6df25d4284fd8e2d70fcb5e
43d3731329fc78c45a43d4e89126d3777fcbe383
3308d260cd2e3cf2a856a357df41e93b4d97ec1f
ba9fa9557636a9238c7fbd7a79cf3cb5d399d3c8
56e469b9a72fc6d8ca1500582dff77eea6b1f4ae
4cb374f7e1f91b2691e58022a74b266aafa54b67
e9a88dfb490cc0b083bee1119b4796e5cf39b925
22de053ea12f57055c09558761b0dadf3da57b46
58258eff3e5d9c9f61b740fccf086bfae5fe7454
6879b2f6cda5da2916f069ba8fd6222a3d21874a
0299fe126b104502f34d4ef7a964771c5d36ddee
e88ab7bb2b418e98c7560354759d15152115de6b
11ab33efbc0b70c9bcbbab42995dc76e822d5ab7
28e691b578115a2171adf7654a681374553f5c57
71a19e54e8bf46c35cd79a7078c1841207229787
ab3d1f5aba9ee8153e97459ae77042af908cf418
7d628596470cacc66bd1faa1fb175d9e1bf6c126
bf52ce3a2f91fcc5de550aaa4cc9b60cef6bd6fb
5ad8264755033050d423da1edf21c012d8d49c00
f28122340fc2ca3e79dbff5449914b2516a61bc3
3b369ff510e0098edf7ed88464d095447d1f8ca3
3dbf54a86c8f1aa26c37961fe6b4a2283d1abad9
24ff8f9fcef0bff883cb4dbf37e2202468d13a91
4056e7862be099690100548c0918783c4de7004e
5794093562594a695928d1e6f051bbe1f118e4d3
aefb443cac09273cc7f17da7a670bade5de29390
28f6ff4632db73a336cfe1214f9f677fb5865eb6
af33dd391de2e8c9d3307ce6ae394b3d77f205e0
69ba343215d46ba5e08d738905e497631e6a9ef7
a8a416165392ec5eeb3cb8fdeda5ebbc7744ade6
ed7ba3cc070a7fe5853eedb5f0aae16bca35f6dc
ec5df323523469945b80dace3f417cc79e3ffb16
b3ad4beb46023093f08532c3a31d2f10a8818df3
3ed6f2a51573cfed02573f63357fab985f8fec7b
bcb4495e78f4a5000a0ba73f82f2b5270f106464
85c005aa88e7140043e22cc8712a8271ec49f51a
9ec115e22a8bda7c0aa32ff2e3422da112902ffc
bc1beebdda6060a6e1adf1153b152ca152c94d8a
81d36899693b5ab30544e8e729cce70728e7bd37
0e7a011ee337364101b70a001ce479fff4b59a2d
158d93b1abaff0cd5fd4cb438aa01470bd9f5baf
70301deaf25f6c1dcaff0686fce17a242cb628e4
8352ba0156d7c2bbc92cb31171c27a4c1b25da6c
e6b30cdf61d98098804911fb6834d490dc4fcdee
857ed678c87dbad8369a40f94b5ef242d9454cc6
36afefa0ad3e292c668e8330cecee303199c5fd0
5d290346b0b3871df9495815ffe6e982de82004f
8746828e3e398b5a838bc158a474dd3d0d57a4ac
d6ebbcfba4b8320d6adcafbbb073b65c0a4a26af
ff887221ae06a78df7f1f0c45464a46c973a87c3
a6bf302a5c778dcc48e596b82cc7a61371fb8842
91a8ba791dab943e684baf03f3700e780dc11530
dd97ec5160d5c2642186635dd0a033eb7692bd1a
167ce97a9758bb5ed1fa9c6b929c93cdb2a92e46
9fc041afd11ad0079f88d5afc62d1b9902240671
54e7d85ea3cf90bd8258e3235e49fcbf9e73a5b4
de392a7dbc908d18a4ba55325adcbbe6fae23187
daaf2a7247fb0dbb477ce0ab67ca90490c90b7e1
98b98b9be2c506b6c6a2550de5f46886450e726a
e0aaa8cfc5ce666fb262a29b51d0bcf85f942a87
61a9897b2f08009bdc5e549890f535252013d0c3
52766e87123398e00e7c7144da434e708c641042
0c6bfc3ce3aace76751e90660e5ce5b33e87f5a9
9c99c41954b3f33721f2d996a2d5e383babd50af
c29810a164a92486c02d3f5a82e400bbec122139
fb9f1138d09bf90de3c801c68f15a40bf225f58f
ef73d2aca39e4c50d823a219df8d8a51e0449c1f
19c685aa3423e983f2a0641dd019389f2fb91d65
dba3fc1a5982ad1d3118b38910d9995b0625ec68
4baee97351cc7d1e1088ebbda5096558bccd4d1f
0b9409a2408fa6e622c5059cd9c9990e796be23e
83dc27a6df08934940a4bf48b28f0e56443551bd
c2fdb478f25b5cfdc5093c12edad76b40394027e
1cc2b9a92578730cb856e0cc2ab3483291e3416f
af7aeead1fac295241174f540adbde3e4c2b3a54
7c8dfe81f20156a42a0226d0b3445d3e28108195
118f1603c572693ef128249d1db48e90d002a740
99300a0d949e5df4bebcf71b13cb301e9c2cf5f2
eb57bdc5f5a74b60fa0e71680356b2ec20500439
c78286236ae536210bcdd77007396bffdaeeea02
5c6aeb32d710268cbeb45c0116fba943f187cbe7
cc3ac9d3d2fb2fccabd1cc1bd48f21bb50267ddd
701e50b395a7a013b5ef086e60a1808ba3165804
99131e7607d41468a44a1e9061995d43002ce30f
b42dc34ebc6e7ffbb75cdb73838250e8fbeb0fb8
fdcf92645ca201e55cb53f3b2c78c5319097df70
369627216b41156a96028bb4b68857d7866ea65d
d4ebd1678acc585eb664a356948b8d34ab79c562
634cc658fdf24f47b479374a6b0f2257cf8df2d5
fdb6ec0664d18933d91d2734489fe4ba2ea1de72
83c8ca3d3f6211e3ea86e926d33b273e5b73256d
7e4d558e8db088eab802d5a7e7b3d976255395d7
b5d956f9f09c6c1d0bd4d395f67a681f8f73ef33
b3a0d6bb00c754a8c3efb1248b1505dda85035e7
84aeb9ca460ed69c464a2720e79f47a9b403f5a5
f1d9c7bf9da9b4fa0b1265e189d32f8b3ebf6519
20b53374242baeb54decccae555ada6b0b5a153b
fde9ae2f54d02e7770e5ca34a154d1293fceb6ce
477cce71ca1504a6cd0ba8215e6dfc78e877d505
134b29d1f3a5ae62ee5a742513a381cf5d3e2954
44f2728d6ed91c97d0f70f2c15a1e2c32b72e90d
1ec7f8204b61131e205c63aedbc8d02129dbca2a
bb8996f02844ab7ef29900b0510d04328b43988a
1f3f19f894bdf9ce298e194e78d9da6db256d3df
efbd1e3aa1e48d07381807f221b6fb0fa2ec987e
6f27cc9cde5330bd74b2723e163d8e095e2682a1
87be1edb0ba540991a6dc2e0fdc68a6366416378
9bb5500eaaba68c7d82ee0b01e51fd9c62c5c97c
b8aab84699a7e3ddd39c7b38ce1b74f856ba6da2
799fe7ed2b6ae2308664997ca4c8a3a5263840ea
0331f592ab66676640e4a2ff2076a48372d92c8a
8449837f90ab21bf1d24a92d72e9b81b92be0f23
ee9460f6d7e0ec4f1aa37c49d957e46a598c899e
b00414c42d87cad756006039e3bc106bf9d07286
6bf44379c13ab7a195d54fa1187230c82b68eced
4a8453a22eb48e140f0fdd3b94e3a8fccf6f4dff
6c779a7ba4be76a69b0ec547a79e5f84509ecb01
ee073e97acebdeabdedc0c150af426f2fe6f129c
76c603212b81b6e030fdc7a57ae6e8820e0485e9
cb93a224daf89565312850f0a19e3a11f14fd8ff
0d6fcce08fa0329ad140a02dfcf91ee8a055911c
4a96080b61a3ecd4fa74458c679a1fa676ec606b
2abffd3e17ac3a61dd21cc550387053c9b657026
0f2a280fe2422b153b1c6bfe3f1ee5636194d29b
6bd64722216ce72e28ae2c18c66e3f848df99275
3f2286c4e1d081400fe5b10600934df65e6b20f8
cf9b88c79f963d3e744cc3807992cc638e01912e
eef463530fff552be5aa0143bfa61de18ebf754b
bcf5437c76aa3cab567da4ab822d9d4de83736b1
dd40d6a05cba394a3c3cf4f3e2d6b822e9602cde
64863b4a3cf338584cbcf304f2bcd680102cdff5
0e3878116163aa642aa69dc87da736d796072436
038649c067d72a5e6a08df10545149c0d805becc
267c0b45df39344e14b7a7981cb5ee42c8ea9a49
921308061a3557f8726c47e573c05fb5ff32b384
9b5b22ff6ebde900e2d85cc52c5e1d3640925bca
0fe95613ba4dd0c74ad7a9fa9c022834ca7f1518
8771154eab866298223dec79bc8daae1b642b99d
a07966f8737d416c31d54903063fd362b5244fde
d0a5f0c89919c77082cf9b29fd3467817d5c9d1f
5f775efe84b51a6977dafea385890a86296950d5
50aa9f1db95ff2e114ce92f7dd61f9922ab54971
dd932fa37552b0ab162670778719b69b42440d2c
c2ad7aab5ecc90ef7bfea03dd98dd752faf3fe2f
a7e4c00c2c35858b65420b4993a3566878c2bc3e
67357353ecad1e01d3a5387d2e572d77f63f832a
d7e2a5750944831404f0758c58651a9d4a1c317e
aeeb2622d10e613c911639ed4bfb8463a0afa88d
f962e56f02947e240fe60fddfce3d701719fb6d8
235eef1a44d6c36016ab77e4fcd98fa01deef643
86e276521b92486f03c9608fe72f042a874ca722
4a65f909543e2eab41f853c4ab2dfa26bcec7fc1
ba9c05568d5656ce5c337c6147803abb11b664b6
cb0f0cc1b82353cee6e54bfab9eaee0ec03369df
6f8dadd3c091691327fc0c338517ee32cf0f05c3
f5dd0de3ebe44081c81a2fea9150fd5c0e725a5b
```

```
39277347a8d565f055a5209b16b7015fa6fc5f88
ac9adf61d65d567f7f46653d0afa64fdbaba273f
28102453a3f06123812161c2e48735ef3aadbed2
ab01e47d3c823ad633581ed217cf3b1a67a21e57
9a95d6d885ccb145e47ea5ff4c328a78ba156dc9
7d70e0e6e0aa5a5aa8841b37886e8b005c99329f
c5432306eafd9092c57243273e26584455db00dc
1172b979591f2037dcaa8074db1f2883b3491149
145055ae8f99b98dba60acc95db6c5a447663782
6f3b28881a0401cd9e66d57717631f0698910415
d1b3a708548eb7ab8aab7487669c76062a2ce2ee
8ca0919a188c4d937fc0818638823b18e971b1d7
eb17b09934e1e9493c7ea3b8b6ca8f45ad86ff67
fd0d60411fa23c9e4fcdaea00e6b19275133f847
57ed698e98175a6ff4c07889bb431f5052d7f316
778dd234089a1f4d234025ec943b302ed9ea4169
885e21465e0cf146d20ad0d9a7ebbcaeb455458d
b758ddf068817dd991e5f011f40ffed29e49e560
f2a74fb227e32499d3e63fa4f7c051e8a556996e
4bc520ce4315012f3c153ce85583fcf35de73963
e6752c78a3ddbad8b95402fabddabcee361e55d6
7122ce8ac118fefa69f20b9fe0ad52d3d44f948b
ed4cdc83597e76fe962cff4382e09a6444484122
63146a0eca13d3cdf998552e452891ecb1309d16
7d62c1838a409cd3eba13088d812eaa8940f95e6
487c8eaacf3abcb3e069dcfa7e7cd0eb49716831
69da0c9724e4703e52a23055bdb74cdaa7776fcf
15c67046baaf35b694fd488ada1f2c5f2deb309f
7bc3c85b1b0f06258a17cf7817996248ed6d23f3
9331fef881280211acfb875626f25a53c808c93e
94cacf124e96b075bceb82992adb9029eb031751
6c363e2425c1d23926d631d4a6b14284300bf1e1
3c0d9f996f57236cb720d3d65dd9266ff096eaf3
1eb8c69ad8de3c4b367970fe45c99d9764f5f972
7ca307c6e6f112c8091a90850628e35e3e81a648
349d048f959476b9b11e9d44fbb2c3fa1482af58
441542068e66e766cb0ca5305484d62a7002ae27
b3a13d15f4a95f16088ea49f7a94fc1e3aca4b5c
5cdbdb489f6e5a0408fc827872cf84f165f8cf2a
d7b7d3ace7049fcaebb6f09787ecb488e9d2bc34
5e6b00e72c598435b96411fe8d6f04e81611ce3c
6a5652b3a06f5ab769f0e71eec2e799067eb9f21
3fa86998d9adc1cc696615a40add2b28fedda7c6
e8628a15713bdacf242cb96c310d2be7d3218e58
219d5720f35912b735ed4860d3177a39a91109c6
3293da3dbe270604217459e50a803bf4b2a08851
e62704c309c5ecc4c4174744eaeb78d7297af9f2
d7a7562902c1f933276197d8bfd0ef044cda8750
40a951c449db274a8dfd3e96d40723d0d4fbd464
189f126e383cf99f9d33ae6ea26ff6bdfc34bba7
5547489e1536a58aacd912401610f3cf0f73f057
7c65862ad51422305d64e5b70f95755e7b635159
fc342dff8e28081498b8c948d7821b7a2089e4df
9bfc3356cc5bc6ae051fdc0e87ead53ce9c103ed
d02d102e2aca72a70144eee6eb36849a69a98d0f
9cef689ca6a2614c13626e188bb574f8da432859
16e4479fae035d679761efe8e8e6ea94e12184b3
9f2adc96a3c95d082af25b7b38fc2205c3048c81
3425ab4f83344ebea5e729ef4fdf85376af73fea
d9ad63102be4279b49987826730ac87190e184d4
3a6b00b5a6549cb5dcc4180162d07b242f0263f1
0db79d01baaf504b7eb9cafead361a3dd268a55b
bae16b682774aad941572ff0e1c55100b4a8b6bb
5a0f27c9e0344a256c4eb40d89cd59da913d4b96
8ed133700cffe3c88e2f512f73a0ea7e17dd250f
a25737c1cfd7cf73aa2d2e04689b90dfdc78383e
93f89717f875cf43388e3dc822bac62c7952671e
6bf3e5a05481770bf91785d93d682f93caafd0c5
9f387b3ff244bee89737c87937aca10306bebb47
5c623198c87644409739b8c23901212f4a2dba99
6d755a23e6c32111e57b9a6d8bd256115165c7af
f00dd167f2806bfcf72173d35626f43ff48729b6
4b65241851ae09d427d693d0167db55576a9cfa7
779fe3b66faa4d570bfed61d6117ef0b8fb1d388
2f520d5cb1ed3320daaab549710cfe330e4b7ebf
94399830d7b05ab0274c0807425b868c73b85875
604032ed7cf8d3e53eb089001c80943d1c52e4a7
269c0b920a69218a5eb8af7544bc93c2d9e3f3bb
0af7b23f0071ad12b3f0d0e66d7a616fb1a8c1b0
b395d3d3ba15f786b65ba795576b38948a9bc1f3
6da16b8b62f541ba8102e9496cfa4c86483eab29
8244d18a3acf26253ba3863f2943e6058dad24c4
8bc913173bf2b81c88556fe2cc7672835e4dccea
a37797c09acc7898a31845e2d689fcd824feead3
a0eb732552ac2bca7885dccff30ab36cf8c97757
e1a654ae91ad8c315b79acd630a58827f45863eb
47f091a76c5e336062d414fe781d583ad63978d4
12575c05d83b72f6d2088c0c1cf31f5348d9ac6d
b546b43909610c811585e5b9452dcd06e923dca0
d07cfad4000037c75a61572e22f1dfd6a233b407
6d0b46b05a6b224b5341604457cf7c67ed893d1d
36cbf1680cdf84fec700ea3d76b9396022ec2281
a5859483bef1cb1c1c3a3b35d8fffcbd9520b3c4
fc6e453dbc95c347585fbebeb30117bbc215dadf
9e770308dfb3f0f71b5a84a04c6ad0f746672c5d
a1a52b19b7d978c18f0f8ba242076d17ef78c876
725d20c7902c340d453278b3b7400a9128fea373
ffb8f0faa2679732d91534a54410da835023caba
639a20ad4035d1ff02d150a9046e8995c447c6f3
7eb0991b0a7956c672f708312098161af7eccb36
c8a938c4166b95f45702b1aa4046e5088c720edd
f25cfa3f98b9c140fc474e98d6eea11b992c680a
4b39142f9500149644f0bdbb99f58a86eccf6950
6ead39a1fa6978ca1f9e385fe749654c2f781509
e86dd54edf248819b5d45745336ad780208858bb
58511ed3844b8bffd6b573166081d94f1e80f6e1
4e877419481dad44b0d5ad7dc2817357d2eefbe2
2ed3cce3a8a556c3c40a43df58d26889985eb446
d72031514943ae836bed880742aeccf47f515694
b8d83b8851aa05272f44cb131462108f47d0a1fc
f4dc7a0d23869631a05d9b4869991be9cbcc67a9
6a443d0acb0dfea045cbaf3f478c42eefb4ca249
2240823f46b20a5406f3372265467958e044af84
29c1da5192b57b99df2dd1140db6ac40e9ae20e0
2342a0e833f92d3c43cfc71c51ceb5edf8d28162
b117b5e989c31a0c389b906e7c4b47dca64115a0
113d89b1f0bff15b7821523a572d9dbd6b952511
addfe6c6c6d94aade6ad82f2ef9eba40c0b01b09
1939f87dabe4621d325e036aca4b09ab8715aa1c
3fab2400dde3d229998d075bac54827253441a36
5c2454abfb5feb2cf2b3e9d9e22eeb8ef221f445
abb292010043f608f7429b9b908d0a3a9ae5f504
d08b30ea39cf802f764508cedeea61666fb86d10
f97a4ddf8e247ab96f54c66ece6d83a1744b7901
59f4e76743aaf7f4a80d04d63082467ab9f4155b
4b7722534b19e8600ff912f6a8975b146e876b42
2637770eb73a9539687212ff16b70aaed4ea487b
c32eb393ee5d2f772837026465f3b4c339bae334
6beb9288597e6b5e74f5a28838669b3b9eae2a8b
f99dc1635d003524c0239b8ed4141501f789c36e
80c852bcc46af1c69e07bfe450df85644f6ea727
381ed152446d752f713c39a413a078f04e1c50c0
6abe2f6a2b6ae4e76c093e031449977840b415b6
c2a2b951d520c322dbfe6e64c54e019cd6d2ef03
2919d408de4fab9e8b626e1f0754445c7c46c561
c155bef15bc158086a76529467b23fb83ad7b958
bdfa08b2be9094eb3a33100a444219c1c264dc9c
b180a0b496e127606639d133f9022a266c085fce
5a497ffe6a1ad7362afbabae8117b7084b782683
b1dfc4a25ce74ff4c335b08beb24883498407450
33463abedfb81a0187d3e52b7d259128da800394
3247d7dc362e86a4a6203ff2beed7388b0a3c359
8daad06c2bd28a864540acbb43b5341549903309
0585bf57453fe8de8eeea31a59fdf1bc9ff8d384
e651e5ed418ace30674943bc88c04562f4dc9e42
3a3de5c8a02b88909075ee80480270051f703ba3
9d69517424b5a439c9a4ef58092455a90a948811
498f33c0e2714dc6f04a72690f825d11d73d3aea
d70578464081de52ecce785b6cbb89239dde3576
6f28e5ee2ba5a3220f017e714941d9ceea68bc5d
889fe8ef6f42a8fac54b29df12172cab753bb8a9
f4641543385e3294a8c6fa6acd0f38ac9948b7d8
9248a7596d6586fc396c3708fd3ddcee6ebbd16b
8001857f6b3ab3d008bdcd9067bf5f9788907e8c
80c4395855e156cbec2a935a2774b6be58ea3656
ff2743e5dccfeb22cfccc59400191c7316789896
```

06e324fb4d221b6c0111e88952174c99b3a2000b
6715b5b985cd736ad08e3945f30b074f5c3a7509
bdbdcd6d55c40a9946d9d75837334d0b3f695cc8
813678a24783dfde9b6875e71be5fa7dda60dbb8
4b7c9cd5226f5977bf6a7e397734769d4e648f25
f685d555fa2dc14066930003ee59b39533eac38d
23ec71dc9cd52a51c1d3797d5bb15e1de85a9712
19533a6fc29349659aa5f37c29ae42d7d91c8fa7
f20c2e15f1b3cc85c3a9d36f12e9881ef38a3a38
c72a8434390f345bac50f4bbd39834b938c4419d
23596e0d4f5cc9e53bc8de92f3899dd16e44448d
73abe4f7e237393380b61f55cc11037d6d0c6f85
497bdb9b5642fe31397c730652d0bffc208b9486
ea770f79a81a529cb51172d6754218fb1884f374
c09a7edd439eb41394c7cbe836fade89950fe9df
ebb5ddc4de40c215829f89f9013e7b98b4fe03aa
f75c4cfc4ed2bb062ee4ed3f4a8a78809b384ee6
e24df3659561781185bf30097da8fa0f5474e015
4ffb0c625cc38aaf86e73ebecf7c40e9bdc7d363
efef898afe7172a1ff24c5875f4b5c76dbe5982d
ba1ac70e8c026f05c499d2bdd65a0999bb94e5e4
c48a617e4e99f4ca9f54f5ecdf6861aa301e32a3
2605bdc8532e14b0109cd369fd6d17f0e45e4aeb
902999e9e023dc9668eec12617b772b708b306cd
0cdd43d12c51e1554a0b85ced666b219bc44f19c
06922b02ee86db06137183451ac8a380e7bc3499
1eddb5dd9c1b7ebfc9531bb17f5b87563346b24b
0eb6c0e31cb8cf5cc97b86c1de4b4fc484deca72
56f07337fe3370c82fd1e7e03b3a4c9e18de415b
6e477c8587cf580a4e2edc28b7731cafa6c60d97
3b86a2ff869093c46414492ccffe9a4543c6fe93
ccad622f7715aa68b544d9e26a3132b9623cfb70
4419c600b5b118453b9bd8d7eba1add20bd3b65a
9014d8e1825c30c9b7d05f2544bcf3ad43fd9f46
019d3f86ceb072af8d1fb5f391b65dac28d96e66
2d79a64ed66fe2fa1caff37788b3c410bad34c83
bece1ab7392ef52cbb393f13fd952f2a19352b8a
927fd5265f9fc7d945475847e6c1859674b40302
e44499489e234344569972e4711e71d4d3ae9043
72b1fd337e2f00a00a29b1bdb2d875d0e2118f50
29b2caabee895c3d97b9367dd260a9bfc33f31bf
813eac605073923a3c480a3cfd0fb1181c6a1a63
3ca9ee43ee35869c4fdeb15194e552281fd6b5ef
bdec8affaae684de9844a410f2f642828c7352e2
a55ae91d20cd2f55a9310bf853875a04d895800b
991ac9c87d40f5267a392f1e4ad175bfb49e7099
7e710d08822b183c08e2c79cd5a86fd3cb2d4b00
9f6f32d98aa76266ef67c0852e6eb2b3a3d51603
0c09c19a9b6dc56297a18a29e82f8798a1b0ccd9
ceee377a48a6ae6dbcaa1256502482e812e5a8f7
a76c6170c7c22d3caa07f26988ff4b5a0f196f0b
e0dbbbd3fe58c64c631c6878791cca709f56e046
7322a91e9a28acd4f9d82031261902d026298b7e
c19767c3a4c9f21e9872f669dbfb6e7022bb98e3
9681e3a7772c67a691cb327c3b18072a0ed23345
afbc793a4886480fb570ca2f6e4884a816a32b4e
86ebc0f8afb2a743ac84ab37e277455456e7b9db
25e36f7f3cd16ed62d3ef3bb12ff0d26a8f61217
0129bbfee36fd3418742397f03ab434df53a0754
02847f51a9ae8d97d703f372f8b77a1e1a40774d
1278654a7e6411f25c10a72e4db41468233ce519
7f8c19c2b34389c66aec08604bad03c796699138
68b699e269a1024aa16bbcbec336cf6fadc7420a
ba250b1700d771d08f01b53a6dde5e1a4626b676
8a6ab2df8deab2805fce0fe576e7783328b96c3d
e5eeb6427bb337d80982d93b708e62caa15ed2e7
3109b5b1272d1538c556f278ab473b474ef21ccc
d483ae5cab92d5a5367b9664a028ed2afd66e611
27c468f85421389aa8afbeb33d5bf41b1f678e88
b07b478dc16aacfd10da16db2f8c58321283a1a8
e97009a6b9f37fa0226d4dbedfcc0fcaf5ea6478
553ed921af5b9527f9c60a8c4660d18e16aeb131
da7d4d83aefbb0b94b0d936097dd46ec34856dd0
0769379b96ca753ad688cb3ec9bbbddc07ff8e13
a7d0a7d47ae220f79240404466857e87718f3283
d2e566a00cf6ff64ce40455e562098a84c546e3d
097b153e28a4a2ce54b2930339909cd0b4f961e9
13ef1f90a7206017df337443f96426c8da61b77a
0b13e467b620403c0d5b9811c213876ee4a3e8a8
45c3c713bee898dffa92421ad1316ffb2274c716
d7fa5d1af176d96c97bb18228c2df8faebe48a8a
f8d45dbcd4c3c7ba64b63157a3e6cf85cd92a70f
07c9710a7b671838282b84c063895215463e8bfe
677a2a8f89f1013340ffc39c47c4ce9f009e624e
0c7de955e909b5e266d993cb9e84c0593af32591
c350f8f72dd796cc7ae9dcb688742aadca5aaf03
29dc457ed85593ce5f774d367c8186c033abbb25
007ce346218a220909f228e694d984799d165b0c
72491926bd13246a3f8b90e17cc8d5778019c8a9
024143168cc00e312fd2bff293ab2b33ad72e856
0e695c82a496397a6e13ff72876be74c4bfa2635
2b4ca66400a3cddce57932a72c1f1bb5aa8d7ffb
56d4402b95bd7d9c3ed32c729f5a610259dfc4a3
7ded0d8e5164d84f93f34cf244517b649416f644
4af7f4bc0db5e33b03db2f4b5c5b0143e15df8e6
e4cedbf102c14776b90ef65d4bcb802fca48c41a
15199836134aa6d7167ab6e721a569685814ccfa
8bbc7f5e62a4935753ea37064c2e6186e897fe2f
6b19fbfd1a3cf48477d8e04a61097327159a9159
0cbce9656ad397416620e4d16814adf36b54fd02
777da268c76fec768a5979b682923478f575699f
357dcb13aa5b700cf21614a07f2b7e358dc25fb1
eb07786d5824200587a4475639708084e1cf1790
acef24a5108112beae12b13d761cc90d312fe8ea
acbb73d57c5dcd4423905a83b64b04247dac2494
df1065d17799fce30a64ca05e91512b45af4e58e
56c7e64cda3c557443675505e46508a386007137
a43ea877ea9023ee06232df7eb5437d7a4fd44d5
0bbf816097726fadb83d5ccb9ad38505c4d8ddcb
f3eff26dec1fb7c1eadd7ff5cd52f51616407abf
2a2693509b0eb12436327f3d93b4c0292d301da7
824999bf3e1ebfa77aefef1b557072779a6a625e
576204b0c4fd237afe61c208bcb39d95028c92f6
31e5548b0c74acbc0f49c8a6984861f0cac9e862

GoldenEagle

Command and control infrastructure

64.185.228[.]252:8080
203.124.14[.]109:8080
113.200.218[.]226:8086
103.255.177[.]45:8086
150.107.3[.]188
118.193.232[.]169:8086
185.170.210[.]98:8086
103.59.166[.]106:8086
www.vipapkdownload[.]com
103.255.177[.]60:8086
www.nortonservice[.]net:4430
106.12.39[.]148:8086
100.64.223[.]251:8888
10.194.103[.]47:8086
vipappdownload[.]com
103.56.17[.]108
101.78.230[.]99
103.255.177[.]61:8086
googlleservice[.]com
symantecupdate[.]net
googleanalyseservice[.]net

SHA-1 hashes

d39eb56dd1e7e374f542fbc6cceca48faac65dbd
229a77423021651418538 8ed3855cafc63facdd3
eb9b518bff0e5b215ca77f9bb63f575035099286
17d98e02304015b066f613c9bf697a372019e0bd
198b7853a0aa0516a4d3e243772812fc17347681
e8fdb2ed0c9bebb60cf2e7411adbccb40490b5a3
e8b7649ccf05323712661b80e44b7cd10cb0cbeb
fe1bafaa0608c3f1d188394e9c0140f1a0714f3d
67b4833325bb9d45c4c44c81cec1d00fb9a43c6d
dce7baa3f526468af18ac2d8edb262c1edcfa32e
8c944305cf372f06ce0d7f306967f7891acab8b6
ad13ec3a6761e5f31b7b4726068ed6b4ca268086
f30594053f73be9823130a1fb4048efbae17a116
85cace9b025ffdb2ce7430a305ba2177cee83d20
98f6476f081bf2acc555c87661fb3c3eb8c1864d
c49d8f5d971b8523f16773ea246256c18f2f0ac1
23a7ab67cbb622eff3fb6de6c6a5ab10225a3e03
aac796671e1b25d7de3ddcf2546b3c05d91f3f7b
a2815ac0b5e188d4102ae54c19e7ccfd1b2c1ebf
65704f75653fe579ac5878eadb16a3ec66a18b3c
10b50cb86c0914c7493a359bf74ff230d47239c8
b72d8827a6897136d1aed8f3c5fab3e6fd855f45
5d1659bd3fd3e3b343d23831ff95390f21166e24
bf4cf901d4fe09de459e94a9959637f07ceb61d7
8df2cadd69154e76b61850d6be45cea0ea383530
e844ecf71deda475609220672a78b1080513adc0
7456d2f83d25a935e221c141817b25c48c5995c7
75f99e7de3083e56757c293333efdae9acbd3ae2
26479bc69b61ff5e79f6f51c4fbb0584cf6c9b8b
3b4bb768df50fbc77a4cdd2fe2b14984d69376dd
a9cc262587833e97b0f496250426b099f01d27d7
74d9c117fbe8a45457a6f3aca907a226cbf9a66d
d26ae361f80639fb9a9684821b191e688796f191
e7fd8270bc43187b91d7a8a64c9de21dca39795c
0ca4ab718bf285fe08bc0b94e4b29fe9155b56fe
c879dbc37eb905d2974c0d0abb3e7fbd2d221c29
823b7997a386a109fb48a81820eabec922c751bd
d866c6e42abd4e63c8293866f2f664ed2f4d156b
5414ec1fa516046cdadbd4dc3ef93218a1eb92b8
9976433a3d48fce45cbbcbe773194926bc38a3dc
219ee1ef5fcfe33735d90e00e512548c923dad0b
e43f3c510830ab5484cba49c45b99b0ec43988fe
091d492fe28854bda0559aadd41a427d2fe19267
e4b5d5943a596e614c8c27f11d91da5630489e85
d2690c4b8b4415bf798829ba5d0eb910fd7cf124
ae9c31a8acda9b9e69a49e9afddebcc2513df490
d8ad9ba493a96dd6db68232034c6fe7ad1682d91
40e1cf2aa4633d8bb7448672f917422b1b6e65f3
d8efbfbe499b3d42542fd3444325a417df23759c
e29dc44d25e24cdd6024032b9457e8a22b58eb53
64831fd7011f0857c3eb292017eba237f3b72dd2
c31b4b5302635133170c60391f316fa9f7b194ed
34068c7e54d13f079fe4a6391207107fc15012ae
b179d1d1ec51fd1f1280429df8f6be498cc2b6a1
91a830fca66e695ce7fe05fe909ce21eaa874c2b
1fc1ee870ce89e5d7a3e510547895b1be30de6d6
e1b390284b6fefeeae2242d29e5b68531931777c
04a6b54e850e6f5d3369dc13fd461e5539b61f30
ff6b5e212d64bf919580c3d82f397b3a0dfd1857
da77d13413576f45ddce673eb6b7f29b4093873f
2078746fbd38cad3e1189aa6007089619d626bca
69120120969e387fe92af6103970491be4a2111b
e3c73b80834db812ee5bebf271305fcfcf040a00
54f30f879fe04c50d287656a2764976671743ce0
d75e0c9922cd6c5800709c022660e24908293452
de234de134d2801e37992df6c627e65d021f1733
d11c1e822242f589e394000d46fd53b86f2c700e
72693496c6db07ee745423157067cc4bbf1bf972
84239dc90d3d3d31a7f4cd6b4e0629f753323279
481d5bf7e28d423b5a3c2a2a55e66134fa1b5edf
c9168234320ebbbfa832f9942fdb9f022563905f
0b2ff1231fd8985d54c0508fb541ecd4ed56c10e
0705220d3126268b1c064b73b40f6df82b7d3147
d79bb5d6a0a0e3210b2481d55e465678407451fe
ffaf565119fdaa51d82846dd9b79d87d16e22e25
e95dec5e15e6b8847a9b299791d1344ca8c866f9
6a3f009af163391f3aa420d12ae30891654d78dd
75e7cf299648154142ad93d2c52a4327b3f61dd3
ec98d978d14d58938b30169f1e82987b85afc9c5
871a3be47c66dbb715c5cb05bf247a9a1e112f89
a8c7b7cccb99d52cc3de9b97c6c5367dff451ebd
bb46a77fc40ac9fe114ba13a7cbe9d30f5981250
b239c5ada30bd8bfa65610a21e2f99caad80dcd7
d48f3a9a892d77a2229688748af7cc3b6c225c7c
d5f492a29ad5b1afa832430bd3304c1c88a04e13
a4ecdb38ea10a55901785f6470e343748bbff5c3
074eb796609c3d010e74146b1fba58c4d590901c
aa1a2783b430432bab9af9d9b9c3aff35acc1475
26f1b6b3611cac105a8dd89ce87470a452d0fde4
e25d3b8f75f6430f6ef62f9d98ac9147032d6559
7f092bb6e6aade89976a9820474a9e990848914e
d53908a5ccd4caf308973d546df95165f5c262b0
deff4085cd22c9f2fc03a6bf91f4ea3a2660dc81
bcaab0ac153a86e54928ac73024aa846a596163a
ade125921418eda9c60c12a2bb2bfeef746cbdae
30a3b6aedd070638653f7ad6eb5c879680ec1ec3
776976e0183fca824f94609096839f0f0c460b86
d0b0a2c733414dc5c8c9790bc6b15f9347e4f283
7c5b7839b24ead303b37acbd228a724d6f815def
4aaa1c7f19157676e922ca3061848487fd389938
d9c31894333fffb820ae24d294f84a683bfd9080
5cee1360c9c10c80b843cf5f9d2f1ef08ab54c7a
13e7b1c9c27b7989867dd9302ea35cbfbd619bec
d068a0933df3303e09e3c74657b4beed1be5ba51
10415a7bc8367ff7d511c43823dfc71fbddcc718

```
652d9fe6212d3af5164e777d369ddddd1fee0b54
27f50c8e280e1ccf31d159b4d419f0e9887cc2e7
899b7b30098e33af625647214dc23baf16352fc9
2714b06332e7aef368b0b3383a383f60d6b1b1f3
4e67e40f7e6f6ccea733c599e7d76a1f78364013
f792bce9999d9c1a5a34efc8e584358e0fc18db7
ba7b57606b749d99a059f1eb7be32158c6ccbb67
5c77781e5a31460a52f867ff374819731266be50
c0bfdebc6152654d5691f33fcfb2c3cf7ab459dc
04558261cc51d3a16e97e0464c1c911d22c58590
7f10f0ff4b465015328f6553ec65e0c81b70c4ee
ac7d702298a284633e26ea93da87c92cd9ff2e25
40d86fca9edc82da799979f657e3a08a72fc4dd2
328db6f66b769170d99dfc29e5251a4f9f6e94a7
f3ba54440afddbfbb51210d969fd71d5d351c63e
e6491b524b5d4801c75370a71a1d39c9141c14dc
22673d362a370d28412b4e6fe395c18fafe2a091
71d9a46d6a64d42ef4825a08643a1b4919fd3b82
b0b308c2206f8c5fd6d196e8844bacf9d3a52442
f0dd360b0b5ed198db1a2182a6229b847cd8ca4f
53d757b005ca55d40efd47aed5aa73146b2ec834
e0e4f7126321f8198da51c9a6f5fffdc1292583f
79139ffb36580e7d0477089c5109488cad7fc937
58a4c56858e62af6273d74d649032b4158ab3b25
b2c85c694eaefe17044ebdf271fb7552a74d82e8
8d6aeca1e778e3a6897c64aa05f39c364c4af523
f64562d020ae592686fed700d70f25f968c415f7
598347afe23f5e7466ab4bb6d95a71958ad91b92
842b7b138a0f400f8b4593844169e55115693c8d
dedc470a8facc78077025fa864f7ca7fc311dce5
f31518c32f0cb167190434864a348daf878b36b4
da8495d34d2d9058635bced02f0d6c4b14a688de
b1f3461611e4fe3502c7370c736ca7ddb849f7bb
35aaaf011bb42ba963f9250666406464e58559f9
7fd196a0ca199bd216cd9ff0575167ad0b464461
fc366591211c3a80b512f14a826a5c86d7ff4015
c18e5d00eae2d30d8dbc725bc58f30940dac8a6a
6addf03db381861d664329a15b5a51dabad532fb
c6c5abd0ad92caf84fde038e0e55631b0d1b8aa2
5c4e69b2bfabb608c37fb49db91fa54d06170341
c74e7a1e790b0c8757c85be5d6120eb21f92aaaf
c00ae59b7d18d5271fd04534a59ae274f34c7721
caf5ea00aaa16a91372d464a6baa07aeb8fb0b2e
6e1df33ce941adb77e7818cf96cebca304c1648a
d9ebd7dd06f9fba609e6484b120b82f106a37866
b1b3df9a265adebd3c9385a17c91d6af81cb1e8a
7f73af57c7b2f3cfdb694047d12038387a6e5e8a
d3743aaee231ea3743d85f1f68e718dd7b35acd8
5b78b7b71bed60a9028ee20af0249cd8296887c1
6e43f1271b1413802a080715813478b024143a86
75d4e604703a7458b44a17bbfee17ee525e1ae38
cdcb8a77f40847f362ac70119e7177d38f8403d1
5b7be1ec39295ca49e3824492f15c3e22ffffc11
8c80ae0f9651990348ad53d61d28637852ceb1a2
140ea25b4ee305ae5116c5a58315747804fc44a7
c33e347bd5d9481b8000486f91c52b5fc345b482
4e13bebb1f0f18ec561ad745f0ddf4d028af319b
3c1bafcdc14729db053cdbc59804521f1f14b061
f9c152fc61b42f8d80f725fcb31cae18a4dd1975
76f44679f71c009951fe493a9e376b3dc73aa406
36e608ebd9fda913285654e0cb1a2b2e3ee34f2f
4554333b1120758af86faec1143e4779be4d2636
446082c7a6eb1ef6d5bd555f9ba2f7bf6fe8616e
8f96a863a04470aba169a3940fb71de57897e49b
87cafbcbebdc328ca6ddddf776c553c520eaf5d0
ca8857cc834dc7557a1c37ae3866e906725f4fed
0dd5c47a85bbc25c6dff7443ee96ebf9723e3cdb
5bab802ab6eb70b86f2e436e40ce83df051ffabc
cc8eb55f4887e12752b33d011f53244506823c8f
93fd86932eda177e1e05ce7aa84e5e7568fe97de
8427c127162f055be1015822cde51d3e674492a4
99314c4705f7da18f8eba4f29cd45497828dc820
58a04b1eacd8bcfc33569f444927a745a5bca69a
447e3ecd17c1b5ceeb47c0ce7124efb42bd6acee
80b8e3684d761fe990fde8276adbb694ad4bb499
e5a9ee25b6628a9e9bc326f812dee5b95c38fb37
3cd74daa24ae45697cda79fbf1a4c497c09401b5
7dafa6834d420e890bd2ff24a9580c475382baa9
8b8b77e0ecfd1bbfe73c3d37f0185c7640527767
a4d0ead47e56fb3fc6dbdd9861de8a7f0c414c1a
42b205cacb746610fe1ca2637c45ef395d97e418
4e76471a20efe5617d99d26a80affd51c1af7433
772210206b767a8fedee1bdf2c4aaa055e36f421
3f0a84cf01b45d57c30fc4476bc4b31abe761c10
60d0734f23643a44dbcfb7c6c36dace5c8f1a6a0
3485fc62744db4210f8c061284a9a3ce91ad5900
fb3c0f051481a6d6bbe60605ee2e8715413fc11c
1ba72175814d72afa33d65b13b1658cff228c5da
f4f82d2dfcfadf9b48e4bd5f962c57ff1fa7ea2e
367d8f71429475e9d30d5118dc68b6f617ab00bd
142afb52f4cdea2a03c4c78e869e8b4ebff9bb61
f4452d7efae73b322ac4b88a1046ac4d0a26dcfe
50435cfe0d697a30c658657c0afff11cc3bd4de3
8b4ae4f7935d117b6ac1d17916d7b7244606ff4e
3dc80c1fd875af9b707e9e8d607347fa1aade665
40fc40484c93b55bacf384eba034656f60db65f0
8e52e27d87bfbaac8846ddb25be99c45fc9c7a20
9a02f0c79295f91eec64d79f70dec4ae0aeddf83
8757337a5fa5b0ce1090040b8989b24fcc5b826f
3b787498f2d2a9e3aee5e9dc914f980a8dcca214
2293d2c694e7f990e30ccbc2880cad5b470270ee
73b5e53ec38e80fd364f099fdd4c4316ef0ef86a
981a82151b8cd9e3f37dbc2ffdfee3d99f85c9f4
3485abbd4c95f0a71ddd5561b34dd4c979ef0859
31fece1d863466f5fa0b10c00b4207a0bcfebdf2
98f1f95f30acdb0582b59a7c97895c27751f72fe
04271b3af715cedad2703f7bec7dc352e0299dbc
3bc3a96af78ea7b7589662abce70dd1a9184975b
2b4a0511f3eae28f0d95a8b3d730d74ce88dd303
321b5197145937d505b813497dac2edb9986104b
5016610c874faac3f44d48384447d029f57d3b4d
bff9a82f113e200bd9eca910fdb1a729230cb02c
df5d3987300f0af79538aaa0a4b198a9ff2ebabb
ee4b079cea13caae3148ec9b09e26f6f1f6f0f1f
1058b7a3535e379967e673bc68193fb980d8795b
7ff6003ac49832f9b64f7916a975a58552153181
e8350dab4dd59b5c3d312a50c1f46e577ce348a5
bbab22444ea4f26dff2cd63a75a12d09296aff0c
15c195a3d76241990730ee6eb7e96a944a70a1a5
232438aa4b1c0249c2df7f02c8698710351a3b61
50b5afc9fab03542884e14fcb82bd3b68dfa89e5
d080a46a6e49588e6e90bac4d1d5aa7b9c4fc5c6
7508df4a81b705139786611a6c8f962428dc0677
b461d8a51b72f3b1ffad020a43e673f5a94abb04
b308aff1b23eb41fbd747c9944fb8c59427b5fa2
f87aa4a5a85406d64ec16687fbce4a80f4e5cd93
2c936843de3dffb5578dce3a278bdead3a5e7f27
99a73d0a3e456edfb62d2a28010da77124460990
6041d1c59b8047fb75595cbb52a9bdd27b596e01
b2540b61cc6ee8fe461195655722cb4792933931
3da569af4f955eff3479e0fbdbfaa1907048482f
15b541fc86b8decabcdff13fe6cdf0d445df639e
caceb51d372534be8891f11848a2b170d5982590
4133e41f0ebfa36b8f6439476bb12652f8f941f7
473eb02668f42faff3f617ec6bc96ec05b9deda6
fa5e44c7b039899ea518dba45f420861114abecb
bbb9842680a7f87bc2518adf0d5caa980395c107
5824e9b11bf0fbd0b6993438d46082a975297deb
dfba4a6bb90517e2471dbc037f662af09de760e6
92a5e7bc4777d7813927b62fbac7330694f82416
df1b85273c182b8227d96f8473c48b6c42a4b478
5e63d9b60fc57bfff0db524e0a9adb47e5dc32e0
aa271a7b07a9233a7d5682c5d58a86b5e7c93709
ef12316e639a38a76f152f4eb1cbbe680ea1e6ec
6cd80fbe743278ecbe8816d3f8f7b81d944fac25
d307c30d503ff15f74406fef70e548c653fd9714
d5fa5c9f8bcb34dff4d2632e48a2b23c129207e3
1d8227b33517e82dc61035954a4664f7af0166e8
46090f7c1017c6b6ab67cac741dbea4e1e8fb6f9
69319dc0d420418722aa9accb6a8be15fc61de2b
310b0e416d8ff5438e3255d23b281398988db52f
faf494ad90d851ed9229f0866f7c377c99cc2f08
ea38afb2e11ed913e9246e262db3268bda25e843
437360e0c4c68f9dd124a0770af94334a39861fb
382f0fc2fa3e9d023b127c4f8612eeb562af48ff
792c071c605512588284ce35178e9b0b67d34852
```

```
317b07e0fedecbfe0b4fedece93b86363db245b5
05e450f452576e270a0cb48f9b0d7b715a7ef257
552f9444b7657a7c96a8c0a7c022ce401889c54e
9ab1a92e58b4e20b0bdaf3d14e6e3793fcec5538
95a65ad4bd25e0bb90ee9d57e18bd5398df96c30
0d84e1ff51fe5bf07189a2c70055d8d52ea51739
4b3300c498cc222d1e299c3313e3f4c5f482510d
3cda106c00fc8cb6fb595271a8405557d135d830
2e1000d3e0cd33b56a717d1144b64dc46c78b60e
940ba46ce833f5d2823718a9ff8b5af90c82f61c
f514dd1199dda25bf703358747c77843fd68309d
4ab9374ef42ac6d2a728e66242096e54c6bbcc4e
4fb499dfd20c3771af957b87dbe2537d2d6034e7
02ebb441b2f667a03df24b2bd39f6d765aec8fdd
30dabf1c4275c5de94c3128d6b882d6123ea2ed1
5cde5ad71f1c6f09b84de0899bfaa007788b108a
3941cadaf4f05bd4101299a74a8dabf8ea19e1a7
3102c7c9c4ea34b64f817547260378e086a07e30
a7885770f762e31a1883f0b1af4e079ec1f0dd51
bd14054affdb00f14392dfb9f37136f875a0306a
c4dbfa8ef6842f56c2748a9d3c05b9d2a0cb7f5f
22c2a60f7ea317b06ec572984ef69d6f0013e9f6
f56606a3ac5a9082b09b9e07867364d598570f07
ca5add44b56ab6cded0afc6a2dbc4ba954dd04f2
c724a3c1308e5602049536d7025b2a4eaafe17ba
8c994e3384f9a943e32796d745f32f895c9adea1
5e5b329bcbe757e77048cc285681ea130c489171
59d1ad3ffd92049df277f7ac9a3f476c87a36ed3
4455a6ac1deedc9ae296e2f1159f121c6e5a6780
9dd9d90a0dd5096c231ef2b989fdae577b04a477
f93eef54800d557af9cdc3eee5526e11b5ae6a67
8d771da0d0ea7431c4a2026462d2c27e5ee8e4a8
86c9bf97eb7526399bf48d328803a7e515d098d8
74aa41840a2484b7769131c1d49aecbddbc9a2e8
92382d223a64554522cd4a07e0012d85341e9afe
89272d2be2db5c77afc4456a7c8270e349d4cce5
7e7d59f2227c7e280f875779f6e80bd019df175f
557d60c116a83844123fb1f7b344bbce468894c9
45c1948631265bad60c44706e30c89449fa020b5
75162d480f720f17f69109065aae8f42660dcab5
71ee2262b534dbde0ccc1d319b031ac277af7090
17ee0259ee253a615e074bff1529f1dc6ac80ae3
9b384dba5b39e9d1cf5dc741d19fea66c162f9c9
5a1fdca8dc82778c50cff9b8c7cde6c0ba661a18
ef93c323f2a6cf8aa53e9f5c9a6a0c8024b31fab
ae79ce15047daa2d6f597795f79505e1ef08d642
ed1acc367691a8318dfebde6b9feb81fbccaeb39
c0eb3e60595b5c9361d6ec209286eb31d70ffe08
43f46b9ca29bdc976012469f158ea7fc5f17830d
00809f74188056d9c2befff624d6c429e1389fe2
ac565e76a573adc9c4fe66a7320bf6bbebff4757
7618b38ea8ab7604d11a1e0086945688a619aef9
38b8a22b4e3a8803abf437916e39be0de22eea95
9caf7e5b773a104bf45dff1e9e5d3f3556270fed
75c2f8d10553782855dbc2c195aea5734d68f060
99f9b338e13e9c9f3cc32bf574aae87d08b6162d
80f6611e6b611ba941fe4b5720d7384f564c00dd
8702f83ffd8c0f4440260c426caa0e17a6150972
858e937c6821d58997a41ce3eddec5c386be701b
a3c4d2290fb09b3eea4df6f18aa881ae03ea72bb
5e202ce29efa6eaa6ec91bfa2a4d714ffc4ddeff
1db82cfb1071671a7a2e784556e77d766d1b3113
2af3d8111a08a4fb2fc2ba0d66af92ffd1236db2
6b8bdc804fabe6a6cfbb03d671e713918b8910f4
1b13da69d56dbe381b457c54270438583a1aa164
37425e9ae7ef834449e86a59ecbd366e4b9d4335
bfa19dfb2e15d88c0b3ae7fa13868dbf2c8fd0bf
7b6616da128e3e1472bb7211328efbb04206e849
35e7b08ad5fb0411501e931b01992cc013bdaa94
6ff9f32c941664900b176f0cdd665db96c6e2dbf
6f19a2f1665f036357e102a5415b07cdcbffe0e5
6e43ed98f5166de0569c4fe7d6ab796ecfa4c579
cabdb8c5089cd191203b840971cc49712294dc34
ee11a13f46c055ff046d2d327824b9c25efc5a5a
eb9dd24a71c222889e212ec686811c41f9340a00
244da024ea4660ad9c7b430a8f4ddd7fc356441e
1e8fd27dd28154295511a62a2e017eccaf6c34e1
f24cb30e39a28497c83e1e28e391df88ce3fc550
ecf4cc2d20c672fd14c4df305bc97be3e5e8e1cd
1f92a358356472b69b9d7c4fc1d20dd7be257a6c
7471165eb24516d4fc6de1be009eff1ea1286b4b
9f92714f044540a025b4a549a97b1381d363a7fa
efe13045e63d52cd089f740a338aa4e81b709108
b91f2d4a00fdcf25f2d3cb00237b5286e5bb9b2f
cbfa0e352b3d10cd653b07dd93234c94a8f806fd
4d4c48adb2d302d7bb48ff4971f66b6259520dd3
ee4840927ada412ad42f43990edafc3883268c2a
b0358134635b31d174bd2cfe6fe353b0bb0e89b7
96932a1ce116e2fbf60e960908153a04fa140867
2d208c5a3d17221376e560b19b9de713535390e1
76900d0cb75717b0dba93cffd598a194795019ea
089a16c31b11226fd28b647c38bb13de2ae28f0b
bb4f91e376adc2917ceb6ad4012b9ca544771e3f
651da970b060d3983e435f2e142bde217af70130
dbe6dd7abd2252763df261b35c016dbf5a168158
dc443b130810d4620e97872e2acbdadd52cc0a5d
88c3c69c094efe5616836d741f55cdd66113c2d8
3c97aab4715fb1458002a348fd30a48eb124ce92
5d327d795bdbd744c0962763cae786280ac5a52c
e01ecba5d7f140514fed7700dade8432f9885bad
ec4d1a48383c63be7975012d48945c21987cb4e2
de64c26c36a38a1fa1579db0e96c5433cc42fe76
9f380437ceaf4b61f60827f622855db6c5cfbb8c
695c7fd001c5f8527e6d94a27c89746b845a7199
2eef125cc7fb80cd5d7ffbb24622dd0aae4ee601
6c4d22d617804ecbb9e3fbdb5c64cb739a4e02d0
c1a91c045eca76fe6a3a9d47ea13d4e0dbd50e16
10bcb2fe654eb31f92e35ef9cb05d7810006c8ab
349dc8a48ae91867923573cc6fc5b1cb9b8dde41
87e687ccf687572281391c7bafb722989eee01f3
7066ea75bfc263a1c541f4f65c8760beb1178b4e
a2eb290e2fbbf7857a01c210816bbf50f2074f1a
16a5bd929f369d0da6a22cae98d80baa9af9b141
06ff1236e6675e84d678aad588865a5fce14f5ed
8595aa82e2a3430731b8aaef036c78b30570d6d3
0a6e5d09bed7ddf37de690e1d24ca84aaecac9ea
2277e62c41edc3616d7c0dac792bdea384a5c094
a12dce71084c80d225ddc4e4c83122c0ad38d80f
df506296c76a1b280f2b512c7912fc344fca4677
b3e40ceda7258188ec539c9d6f1bd2fac6700462
21f9c5f6270cb896169586743a40376f8b617963
733498db23f2ba0fff5ad356151d34b233057b5f
6a37905c44a13559d7758eb29369c2ca890ce2c9
11560ca63c246aea5ad429c1f40e39aa94cb3cd7
470a76ce74789facad79c7502f4e5b9fde4a7b87
23207ac1d0853956e94b4359f60f6f56c180381a
7f413dfa4eb29a6de6914beec1c4b6ad35e6d4bc
aa279151cdb8b0a10849a031c8ad72588b6bbc57
28cb1f101d723e43456e82edb8cb1e151ac39789
82ebbdaf78da11ba9955cee520759b1e93718f7c
009c39e5aa24c191ea3b0ede96a84355d02961f7
8c6240db21b600f1ee25d9917a1ff8f9d2999db3
cd5c4c4dbba24f0a0503a016867868411a516edc
f4c9e9c7530f6e0dbb0e8d1e8c3159dbde7826bb
a03f1103b8ef71f7d54e26dff267ba501f5f7b41
542f72a10ff28c3c92ac0ae1366976439239e86c
8356bb9bf8c0bb38e9790884c5ccc8df7b920cba
b327a0683a14e598f8d73bb31a2114d969199f17
21b6a7376afcc165c2f215d64d2e87dc78581f5f
eff08ae43a7aa18cbdabe2e468bde8711c5b0e8e
4358b0c3644a42e6862fe10798edc886fc117455
8a4948b47b4de1d1bde9b75d43b80f22744790bf
f3913f8f5d3c723cf13ad5ad8499c48f65593152
fab98248ed5e4a5fe9561caee979c4081d5aea2e
38a8ef423302d29ba7924d8e376cdb97a792f713
eb7e2bbc63c3941d7caa835f751d0075749bdd19
c068aee34fab06d089a208276f01597362dfdb7b
e80f1012cd10bd7bcacc4106b2f80120bd9c13ff
cb131857ac060b291b0fdcc35795e96b1ce99d46
bb7f7f0fc05165b7826b0ef32d38295574f6422a
acc72a6fe915f7cba5833c11418e9a31afd0a9d1
d07060ae3691c4ce6ee36c4fdf87c6191fc88911
cd261bc2dcf83e41000e979d924c52ede00cd054
f28a9e73245c00b890a1d711bc20310d10bf4631
14dc0b4c4ebf7450c14ef443484f41f75472d2a6
cd40f6d802fa3200881322ae36ee77cbb204ac01
```

```
a65c8b792028f4b771050316ba8c5e3897700622
ed942c10b0cb71b4d9dd4fb148cb18acca8af63e
3fcfa990ef8d597a20e2432993c41546b8fc74b0
455898f6b0367fde95ace83084828881c5372c10
84b6629d013938a8892d03fad1445248d8acca37
21dffa6d169f2dc0f5c322fcf2b32bd385fe92ce
c506119eef287bd4549ea185cdb664dcc6900b97
fc6fd74b8191b36759a15ad19d34a2450ad300df
e0c840e1e1db8b5442ca986c530432ecf89de026
c737c427f23a45109e5b2092526e5938b29d8adb
d92b5a557e6eb733123ecf3c4f89bd5c263f67e7
2d2f8b84178d859ffcbabccd653152586b9a75e5
d3cf783cf7d942a4ce04a6d207a38a887d834642
e6c9b65f906a54b0938460ab61bf27eda9274b7e
55d79457eca2adaacf352fc6df7ce852dca1eaa2
d8ae4016f714885111e4673b51d67f663866c289
95d574ad6982aa4ad06d54bd38a4138bcb9de42e
f0ae1c72cdf55cd34aec3191c458ac068bdc5156
91d29f098be5327fb66a3742c2d5b4b023e7e198
5771fdc5ad4cc0d3d454941d0fbf061a088d836a
723206de69cc96d99a8528dfc3ceed879fbfc7fd
56cfb708463bfd5adda3084e8ad1a9e98ef1fe33
32c65b040ecabacee0057b07fdeeb77b64bbf808
0bf03acc5c27b553b1cbafe92d58cd8ab35be50f
7aebf59b64a379067fca92964c0e4aa71b119f10
51c1f63659b0188abfb1863e64eee92b12268119
908e3ba4a327ea4e81a6b314190b3405cf7a2afe
b13d4fb3e652f7328647ef3a8e6384edd96d8658
fb4132068fcaa341a2359f48fae32571f68890cf
5416d50dbce74275be18cda2eefd168219da3407
9eca14045dfd8a3096a0606ccb3485107c893ead
7f8d01c5d35f26a746a3de6dbf3271c69ae7f9eb
dfb57a5f01c2810303996afe81ac88b2448662d8
e9c9041154b6417bc750444f642f0a0ee924eba5
823914d4e7188f38c6cb8bb59ef33a45c41edd18
948d9062c2f1328010638b6e5bfbe8c84fb805b5
16f41e1d2210910caf17c5cf0b868a82699c2c69
aa9cb60ccfe0e38c351ed49bc86d559021f0435e
729038d3484eac980786b10d5bfa1b1b7cb7fa15
c6a3a67b4d5a32b760130dc29fedd7fe25f1cac7
824ec7e35edf7abb6a70e2f820c31ebe40625858
0d7eb23a068795f76e1a86e732726dc0aa6044ca
ef4c3ab70057f74512c65f2bc3787df47e8cfa71
88cf17c64b6067d4dcee0ccbeb4baa1922b160a0
ae1330bab7f51e99f6c19d5618bd2205bccc5b73
e59ab24f27fbd4802eccef4ef14255c16814485d
d51930a82ba46cf147b0a2a330aa47f988cd3bf0
85d03fb0af199fe08001a1e0bd6a969270724449
4feca56e08310b5023e85dd83b4ab98cfd4df369
787af5eadb0cf27fe8436e654bbd7039249b51e6
c7c6281b467e3a6d841e3d4d947f55d90779ebdd
617329e7abbba813a8748fe22b5bdc0d7bd1e1c3
c7e809a031c97ab1ddf4b0d1bd872152557bf4dc
a4307b9cd922d651a0da0153d9a43a5d1cb3e24b
8477808664f5976a751c4516c6ec5cf5d9a5a7cb
d5842b06cedd65dc848bec8e6719d64124149547
b74a41df31e0acf900d3d391571e783f49a64e0c
98fe94b436b295ee812a53884729349a02432e9b
ad6a490df62a3e776ce8c41e6e9fa45d86f35444
01cfe5b403fed07c18425f2bea24575c72f95548
375466aba3dd1bbbad5ede67e64e01d62f01b90d
4e713ea6b6d825f38910c02339fb5410aa1c74d8
67677a9d358aab98519a70ab038fc65eb8636793
25fd220364b0fd934ef7abaa875dfbe9de5a479a
426fd64ca556db1173bcf9159daf6d6274f88f2d
84af6b460ac8d9d25ea084c37768404d48198234
6abb105fb449bfdf7170a1d9dd8b8f564b1f269e
ebad4351528c89dbc43b178da59a812e5561fbca
153f9272effe3432ec895d8dc0493621bebe43e9
dc088bcceae0668806ace46c7a0927b85d08ef22
52898556b1c26f3c3723bee4d911f1d704e59012
f4b44fc9fd7ab38409b459944ec7ecd56ad3625b
b0daa921d0f49d7e69f515fcdcdc278582420838
3251602552a34248bcb5b12ec41a797c0ee3f12d
ba46c85efd5415cbb501972483690f221764d9e6
a1d2940b319dd73daa37a495955589ae30bf3446
6f91882247213b6cde85f9c7c26da448777c39c5
b40d1d7919a1392308c9559e2a4756886602a495
1663b53f5e177d6b99918a3a226fba137ab76a33
cf7d81f513d258c97b91ed97b3c9a81e688ff6fd
ffd3ba9e0cb8e789b9a72a3b6f7b5fa97d50ac5b
e4b0c4a1e7747c4b1c25655f839089291f08cff2
9c514ad6c869bbf311e011168bbead8c9c7aaf66
7b5ae2450fff2fcaf14757cbdad11f85fa6ee751
d39971e3e55195dc23132cb10d1da6ee188ee458
17c728f072f57417e6b764b89d6cb149e3956dc9
578689b394f9f6f1e99bb5928b6bc96ace4c0498
a62e131399287bdbfa477770776ab4e293ded9d3
820615e51440db2c68d05a70dbd478969777238a
a06b9b8fff7c336b4035ce36a5244b775460a190
9bd1004ed6168e40f83353073e1394fef1807ae8
2aaaa3cb3169c2e8aa37d8375981c6ee487db1fd
457d4f69fd718e74d37218df81bbb409eb0d226e
3f36f6cc62283d7cbfd1df8680592fdf205bf7ba
5578f62352d2624335e855838309e2e80f55a791
9fd7d811bcd57fe589176f75426cf93a53a9b898
1ce10de70e64660eb3e0173b8c97e7d2c2cd4fad
b87556541a19a560f874d7a8a594243f7c3fcaad
8410c29c9df95799c5ce57fc39a85c2397eacfcf
4df2b7fc56e2ec1a54b14f67e0dd32db05596d62
222839c52600d39d231d72b8afabb4b421461a34
1ad8554f3946b0cf59fe9611bdc85060051a81da
eff5bac51dd79c609bcaa63a956ef14b8386f473
574c5d67d89b0d3c6e111a7c959b2171feb9aa85
81ac6026004103dc21dabbc1643c4aef39208161
d2fd7517a9132c822d0e53787d365d38678ba6f5
84f934fa54c31b0104e5ea016ed341bc6d1fe533
93d2821565c35307fb0d38728a2176ab151a7137
ba60888f18205e8e961e1ade2598a7171825d0fb
d6822efb9bf0944952daedfcf64b989afdbbb24a
cf11b15717afd973331bd1bb63c399dca363cef6
d4938819d6bb6e35f3474d753da8b3f13c3c88bd
68ccea577ea7fa40ccc81ca1913d763d355e1efe
f1bbd1cd1c2e3cc6643ac7973849c176397b4d80
fc37725f6ea5659ff88f92b6f04edd827c5d478a
2d67a75e7b119c0a806f70b054e23175f75109d6
c12e2d0b2d7920dc4b64d0d31be4aa8c1b8e497b
fec8f0c34c5575f85ba4a2c956711ac0c7670dcf
9ac1bfe526788a1367291329206dbb585675b060
55e707569a523d9ea473bcc11b77459a21c5101f
994bcea1cf0c4a708ccff5ea1f351d9d6323c83d
526866a446e4fefbab765612630c9f0d44f8a03b
a53d3c91e7691e00291c91f25c90532d93e7a8a0
0a078b519a4e9612cd646fc6d19c472ff71d7177
4009f4af56aea5169e754db66cf21d02a05fe8b2
69d1180eec5f4c66acfa28a004953b68d72b5b2c
38a36722cb87e2dff96092747f5878f5b6574396
3e2496638fde3cd31788160935aab5e2fa58d409
c1eb5a58fb0740d0e2021cc0a6c23a320f50abf3
ca5e2adaeb4369e4ea0b0616e928d31625634b3e
828d93f5348a1ed51f2d11da80abd128fa90d552
85242e1fa7e01dd913b369e695d8b979e47a9f66
7aa054fbe3f1e2d99cd0a40caf12efd69c8fc9cc
2c7795270633d2940837a32f4d897b9dd923e1ca
0e6ca5f74ad538552977d09e1694bc4e671803e7
c5f5b4d7a3ffc067d1ffab160ea61bc68389e5ea
ba2f191801e930f4fa810450c9678de5f4017276
481193e2e882f5856aac0bfbec0afb74bdff98fc
12bd7e9309522b74f0aa2532cd4a704a666e3fcd
2ba9a4649eaea16d6a4891ea91de56b091ff3715
c1376a6da6a10d28f4a483141f2fe53434136cf7
6115adc88b8006af897a18b5cfee0cd7607da938
b0512e5f26e344b76a2d11f9bb04d8dbcda77e3b
53685512c4d58f4c470a0883123d455b89c01ac3
17aefee2a290ea7575d803ee27042cd247c546e1
9cd977982aa8e00d3cdfd43b18e2cc386fe285ef
c9288d5626a4e458e688a16a6d81b8de8363e53b
29738b969e4bdd11aa7d50d629db538d3cbd6a05
6abc64a4f05692419fc2f168392fca8db13d32e7
43b9c2c4774a0fac1eb138cb2db8f98093f56563
32032b3866e5bf4362e2c52be0276344e37857cf
c3c1fbf8a1292e69fd8543f08c9803f29ad59b3d
b9e9abb3b391e513299f13a2bd341008475cc39f
9227a68ccb59aba48b09bb16834546047cf53b3b
e1609d9afe0e0e7caba9d80f1e833cd7947f66bc
50bb54348e0ef8601514ed2aa953a4914fb3a93e
```

```
bb1b5ee6f24884781c28fe07f08af186421938b6
764b3880e1f6e294a2c7fea50d70c92861728f03
e21bd9ea372beee45b191fd7a892a534fd0afc3b
5b7bd8cdf905f6e37b5691c935fe6261f5bde46a
6a1f93227e197efb74c2b60218fdb1ed5e45cfd3
0a122d03433e7f8bf71cd259fd8d728933daa0a8
7ec47b97880bea893d2706ee1fe16f5cd665beba
9bb2dd80005aadb2d99b365407659645ae3d0c4c
e0c5858f4b9554185bcfe3c2ac952f41ffad7bce
56bf1aafc393d890dc4aa32f4471d9fbb0792e83
236b72bc5157fea762d4ffc9508c0edc384f1165
95301fe41c094dd839ed8f2daa64e583adc369c8
4789f0df5aa1fff6459ca078cc6ca47242ea87e6
399ad36e79d8224a9bfe06f4703bf35856800d5c
81b78f05bbc7e8699cff4faaa5ebda6ffcf66e7b
8ad04bbe3f97286003bea7801d46b4dd0a2c8cff
8994b7de678e2201d5119f50987bb730572c732e
6e25ea4f5bc179d2170da1c4778447b6ecb31ff7
75b20addbc24da86f1dd2ea961654f981842e349
aba96eac06e3302e7d667daa37146fcce21a1848
89124d0acfeba0a6bedc513248a5ee6018311147
e062b72942c3107d4b1d7dec7d645dfb6662935a
a0a4d1f6c981794e39f8810da54ab7e7ee31c01c
a70e80280d198ff6c50ece6994316fcfbd0f126a
9d58baad45b130b8d076da53f610c94b8acb7ca4
d3cf7ff6b8c159415956a2f9110247d08058f5f2
294e8456996002e5fd1adc7f002503acd34f1d20
0d97370d0e76cd019873018b117225e1c31e86d5
2cf14527b7fe7db7f9c87498dbc84dbbdbc89efc
97832e73ea20e2250677a2f467c3d9caae122e22
a7f068b0db77f396fcc2e0b30086c040d4171e8c
9dc3437c41828fe7ea5109948bd6a2676fa333be
d0eec291516d695e411a48f6bc69ad460e4e2eb3
cf629bd135657ca98c812c787188c8290ff19b73
cc5dabc34f4657035642c0ba805450c579a8a786
a55b2ac55a5bc18e4c2e9e61cbb6acbaf00b1aef
a5841edd44ad78b2139a1640990d81f8a45ff4b8
7eba4906a148cf6dfa3a21f5f8d8d3f02d5a89ae
4f6add8846b93e6e6746d664b2e0700ce9e5024a
312cc7fbb434430c4e985515355354779b27b3e2
3a9bca25b988abd382717f10019aba369c49deea
1143e5f1a80bc35e125f3b0cd3fc9935e58602e9
2bb0482fa57e737b110b271ae5be107bf49d8c06
41c59a7fed82886db1b0cb45fbcd7d2b7a9f31a5
35a4cdb57309d7027fe7e6298d81366f927ad254
33ef493276ded6a64649e2a3c22563971af51965
3c1e14eee98a54e0cce7e6133ff25cfe37571578
f1e85a300c8defbf12088848299db6049f3c64ab
e9b7d256fb19c9c2c3474e253cc85e2d342bc53b
c760ce4ff7ba602599fc71a101d1315fa7056f20
145220a2012c06a26415b1c67323d0f339f5e32a
d2e8aab68e2951b81973de6d9e627e3a87abfbfd
7fdbe1dabe043accde97f9f03bfadfdcb6dbaf03
a6bf884496e4919c9fd707cb640fafd6feebed46
aa505c8c255c0dd82ac338f63e940ecdf579a471
2d758b663724317b34f018c304558a858aa48230
53b088707341ac7b333693af4c6f496628fc8f4d
a86e4de4043bda2760a3abfe4642a4692738ec36
fabe87356facfcece41add31009fa25791bdb372
c21cc62116dc6209db9ae0d827a573a9e8cef787
1522727b4816364da320270fe80c14002e634029
d16a945556f2fd89b5585246269cb17e88caeb40
1533f453013cc1177742f334607535283b383369
e51a42ee0e2fc4b1577c63553495284b62e1233a
```