Targeted Attacks in the Middle East Using KASPERAGENT and MICROPSIA

By Tomer Bar (https://researchcenter.paloaltonetworks.com/author/tomer-bar/) and Tom Lancaster (https://researchcenter.paloaltonetworks.com/author/tom-lancaster/)
April 5, 2017 at 5:00 AM
Category: Unit 42 (https://researchcenter.paloaltonetworks.com/unit42/)
Tags: Android (https://researchcenter.paloaltonetworks.com/tag/android/), ClearSky (https://researchcenter.paloaltonetworks.com/tag/clearsky/), Google (https://researchcenter.paloaltonetworks.com/tag/google/), KASPERAGENT (https://researchcenter.paloaltonetworks.com/tag/kasperagent/), malware (https://researchcenter.paloaltonetworks.com/tag/malware/), MICROPSIA (https://researchcenter.paloaltonetworks.com/tag/micropsia/), Microsoft Windows (https://researchcenter.paloaltonetworks.com/tag/microsoft-windows/), Middle East (https://researchcenter.paloaltonetworks.com/tag/middle-east/), mobile (https://researchcenter.paloaltonetworks.com/tag/mobile/), mobile network operators (https://researchcenter.paloaltonetworks.com/tag/mobile-network-operators/), SECUREUPDATE (https://researchcenter.paloaltonetworks.com/tag/secureupdate/), VAMP (https://researchcenter.paloaltonetworks.com/tag/vamp/)

This blog is the result of joint research between Unit 42 and Eyal Sela ClearSky Cyber Security (http://www.clearskysec.com/blog/).

Over the past few months Palo Alto Networks have been working together with ClearSky on preventing and detecting targeted attacks in the Middle East using two relatively new Microsoft Windows malware families which we call KASPERAGENT and MICROPSIA. In addition, our research has uncovered evidence of links between attacks using these two new malware families and two families of Google Android malware we are calling SECUREUPDATE and VAMP.

We named the first new Microsoft Windows malware family “KASPERAGENT” based on strings we found in the malware. (Note that we DO NOT believe this is a reference to Kaspersky Lab). We named the second new Microsoft Windows malware family MICROPSIA because the malware is very tightly packed making it appear smaller than it is, similar to the human condition micropsia (https://en.wikipedia.org/wiki/Micropsia). We named the first new Google Android malware family SECUREUPDATE because it masks its malicious updates a secure updates. We named the second new Google Android malware family VAMP because it’s focused on stealing data.

The attacks are not highly sophisticated, but the themes used, organizations and geographies targeted, as well the persistence of the attacker suggest a determined and noteworthy adversary. Some of this activity has been covered in a recent post by 360 security (http://zhuiri.360.cn/report/index.php/2017/03/09/twotailedscorpion), however there is still a great deal of extra detail we are able to add in this report.

Starting in March 2016, Palo Alto Networks began monitoring this threat following the successful prevention of the execution of a sample of the KASPERAGENT malware on a customer system, however the malware had likely already been used in attacks as early as July, 2015.

At the time of writing, we have uncovered:

- 113 samples of the KASPERAGENT malware
- 94 samples of the MICROPSIA malware
- 17 samples of Android Malware which are related to this activity.
- 39 command and control domains registered in relation to this activity

Most of the attacks discovered so far target users in the United States, Israel, Palestinian Territories, and Egypt; although there are occasional outliers. Notable outliers include media organizations in a variety of countries.

This post will begin by exploring how the attackers attempt to gain a foothold into target networks before briefly describing the malware families used.

One Bit.ly at a time

This group of attackers favors using URL shortening services to disguise the true links they are sending in spear phishing emails. In particular, a number of samples we analyzed were linked via the URL shortening service “bit.ly”. The URL shortening service then redirects users to the malicious payload hosted on attacker controlled pages, with the malicious payload nearly always contained in an archive file (most commonly a RAR file.) Using the statistics provided by these link-shortening services, we can gain an immediate insight into the targets clicking these links:

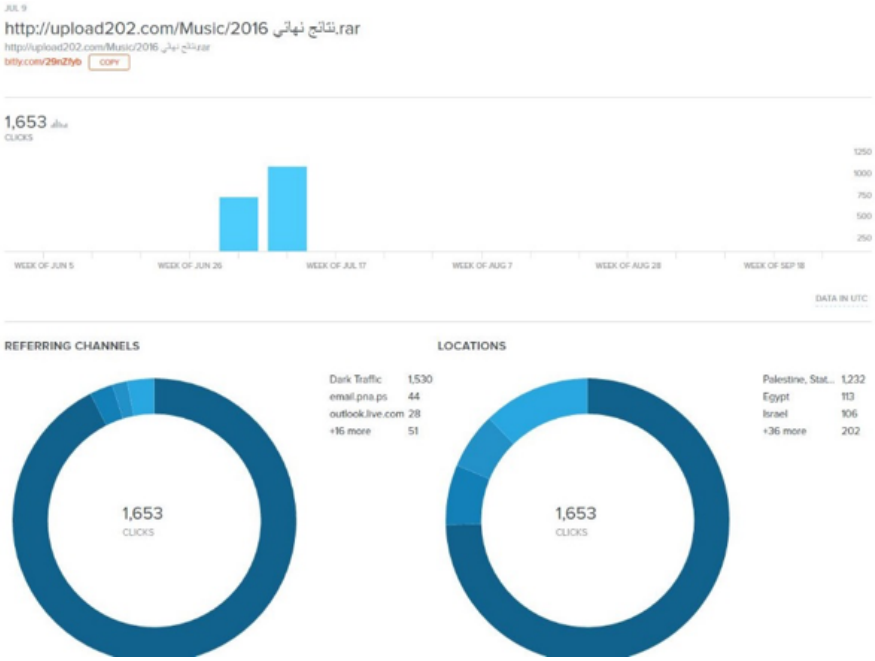


Figure 1: The bit.ly statistics for a link to a dropper for the MICROPSIA malware family.

The statistics vary per link, suggesting different target audiences for different waves of spear phishing. For example, the statistics shown in ***Figure 1*** the campaign targeted 113 users in Egypt, whereas in another example shown in **Figure 2**, Egypt did not make the top 3 countries targeted:

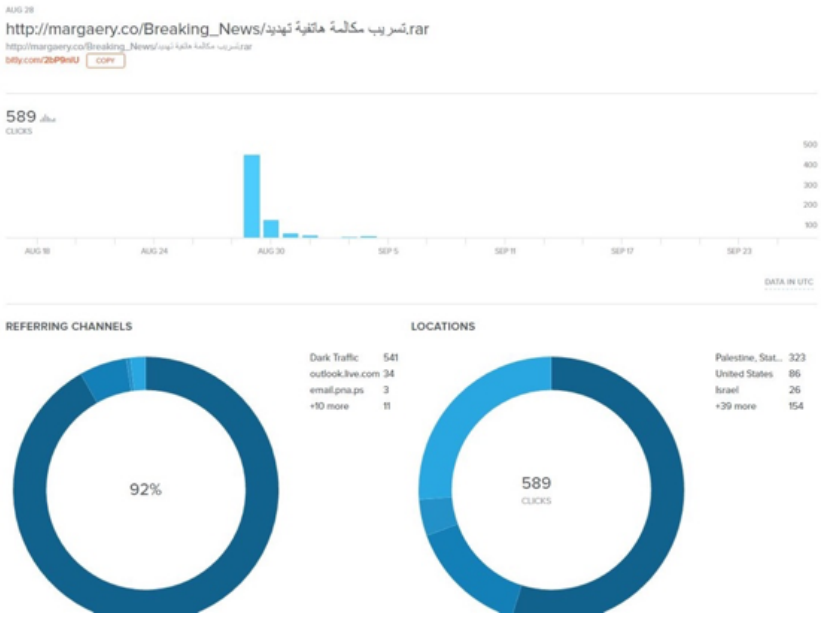


Figure 2: The bit.ly statistics for another link to a copy of the MICROPSIA malware family

FAKE NEWS!

Sending spear phishing emails with direct links to malicious shortened URLs was not the only method employed by the attackers to entice users to install the malware, another method favored by the attackers was the setting up of fake news sites. **Figure 3** shows examples of pages created by the attackers to this end.

palestine2020.blogspot.ie/2016/07/blog-post_290.html

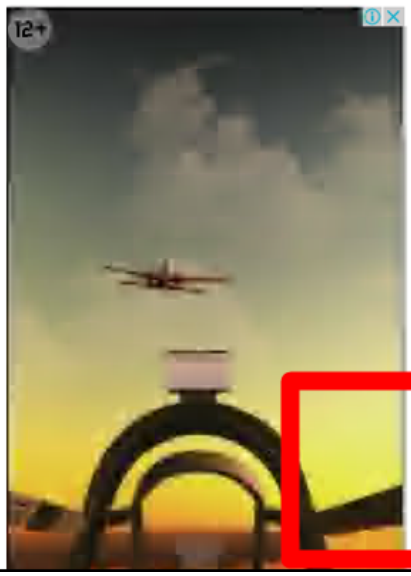
NETWORK INFORMATION - DIRECT NEWS FEEDS - NEWS AS IT IS FROM THE SOURCE

Informatics Network

HOW CAN YOU PUBLISH YOUR NEWS IN THE NEWS FEED ALAMBESHRH- CLICK HERE

أدخل كلمة بحث...

LATEST NEWS جنرالات السيسي في سوريا؟ رأي القدس Nov 05, 2016 AM 06:46



هل تعلم ان الدراسة في كندا هي أضمن طريقة حاليا للهجرة؟

Leaking the names of successful public secondary school this year

comments 0

Leaking the names of successful public secondary school this year

Leaking secondary school results before the official results of hours have been posted on social networking pages. For the results, click on the following link:

http://bit.ly/29nZfyb

Figure 3: Two fake new sites with links to shortened malicious URLs.

We are unable to confirm how traffic was driven to these sites, the attackers may have helped drive traffic via fake social media accounts, or they may have sent spear phishing links to these pages.

Malware Analysis: MICROPSIA, KASPERAGENT and the missing link

During our analysis, we discovered two distinct malware families which for the most part leveraged distinct infrastructure with no overlaps, initially leading us to categorize these campaigns separately. Later, we discovered a key link between the two sets of activity which leads us to believe they are related.

The MICROPSIA activity centers around domains registered using the email address adam.swift.2016@gmail[.]com – and no samples of KASPERAGENT talk to these domains. However, one of the domains (drive.acount-manager[.]net) registered by this address was used to host a sample (babf156ede8b5c2e6c961b6ffcccc5eb7a3d283b398370754061613f439d40f9) of KASPERAGENT, causing us to link the two sets of activity.

KASPERAGENT

We have named the most common malware involved in this campaign, KASPERAGENT, due to PDB strings left behind in many samples of the malware. An example of a PDB string left behind is given below:

```
1 c:\Users\USA\Documents\Visual Studio 2008\Projects\New folder (2)\kasper\Release\kasper.pdb
```

This analysis is based on the following file:

SHA256: babd654ef363e0645ce374dd9e2a42afe339c52f1cf17fc2285d8bebd3cfa11e

The file is compressed using the legitimate tool “mpress.exe” and once executed drops the payload to the directory C:\vault\igfxtray.exe which has the SHA256 hash f26caee34184b6a53ecbc0b5ce1f52e17d39af2129561dd6361fb4d4364e2c8b.

The malware also drops a decoy document containing Arabic names and ID numbers to the same folder and displays it to the user.

KASPERAGENT is developed in Microsoft Visual C++ and attempts to disguise itself as a product that does not exist: “Adobe Cinema Video Player”. The malware first establishes persistence using the classic method of adding a Run key, using the value “MediaSystem”.

The malware connects to a C2 serverhosted on www.mailsinfo[.]net. The C2 server string in the binary is “obfuscated” in the most basic of senses, with the author adding ‘@’ characters between letters and splitting the starting “www.m” to another string.

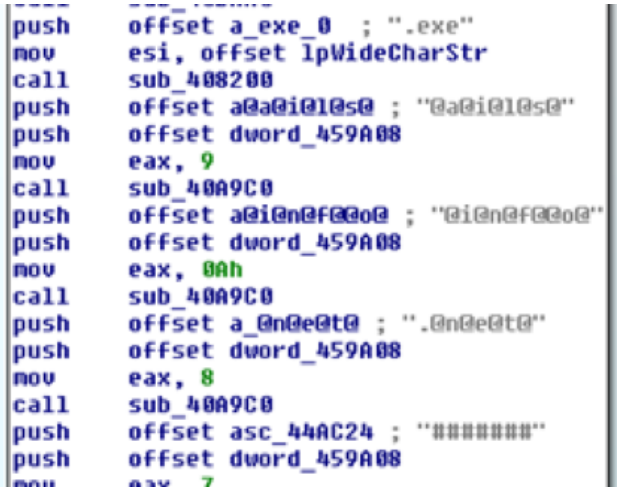


Figure 4: The Command and Control domain is obfuscated using a basic technique

Most of the samples of KASPERAGENT use “Chrome” as the user agent, but this recent sample uses “OPAERA”, possibly a misspelling of “Opera”, the browser.

The malware communicates with the C2 server via HTTP requests and in the most recent samples observed the callbacks are made to PHP scripts whose names relate to towns or navigation. Example URLs used include:

- GET request to /dad5/town.php
- POST request to /dad5/addCity.php and /dad5/sign.php

Most examples of the malware are nearly identical, and the malware simply acts as a basic reconnaissance tool and downloader for further payloads, however some examples of the malware include extended capabilities beyond that of a simple downloader. Examples of the extended-capability KASPERAGENT samples include:

- a52d3e65fe5bbf57bab79b1c5092b66d9650247249b72f667a927f266d09efe6
- c9ffb81a97a9458f1fc96f35cd187b1d7311479e77d031586abdc3d426da0859
- 7f11e0bbc892a97b7c42416c43fe178ebb240939d9dee70c3c598305ce8a2d4f

These extended-capability samples connect to www.stikerscloud[.]com and implement the following additional functionality:

- Theft of passwords for Firefox and Chrome browsers
- Take screenshots
- Recording user keystrokes
- Exfiltrate basic environment information such as the username and computer name
- Perform arbitrary commands
- Enumerate removable drives and copy files of interest to a new folder for exfiltration
- Update the malware to a new version
- Exfilitrate arbitrary files (zip compressed and encrypted)

It’s also worth mentioning that sometimes that both versions of the malware are wrapped in a Microsoft .NET Framework loader which is responsible for deploying the malware and displaying the decoy document. The author (imaginatively) calls this wrapper ‘Loader’ an example of this is the file is 4c1973278a30d1b4ce206eca63676624d234260758a0674d191d338a02914d23, which contains the PDB string: C:\Users\Yousef\Desktop\MergeFiles\Loader v0\Loader\obj\Release\Loader.pdb

MICROPSIA Analysis

The MICROPSIA malware family is written in Delphi (https://en.wikipedia.org/wiki/Delphi_(programming_language)) and is an information stealing malware family with a wide range of data theft functionality built in. This analysis is based on the following sample:

SHA256: 6e461a8430f251db38e8911dbacd1e72bce47a89c28956115b702d13ae2b8e3b

We named the malware MICROPSIA because of the way it is often packaged. The malware is often delivered as a RAR, which once extracted contains an EXE, which is further packed using UPX. Once unpacked from UPX, the next level is a further SFX RAR file, which then contains the actual malware files within. This effectively means the initial payload is extremely compressed and

appears much smaller than it really is. (https://en.wikipedia.org/wiki/Micropsia) The final payload contains four legitimate executables as resources:

1. Two embedded DLLs relating to the OpenSSL library used for traffic encryption.
2. A copy of a command line version of WinRAR – used for encrypting and compressing the exfiltrated data
3. The file 'shortcut.exe' from optimumx.com (Creates, modifies or queries Windows shell links)
   this is used for persistence by creating a link in the startup folder to the payload.

The malware begins execution by first copying itself to a predefined location, setting up persistence via an LNK file (hence the inclusion of the aforementioned shortcut.exe)

The main capabilities of the malware are as follows:

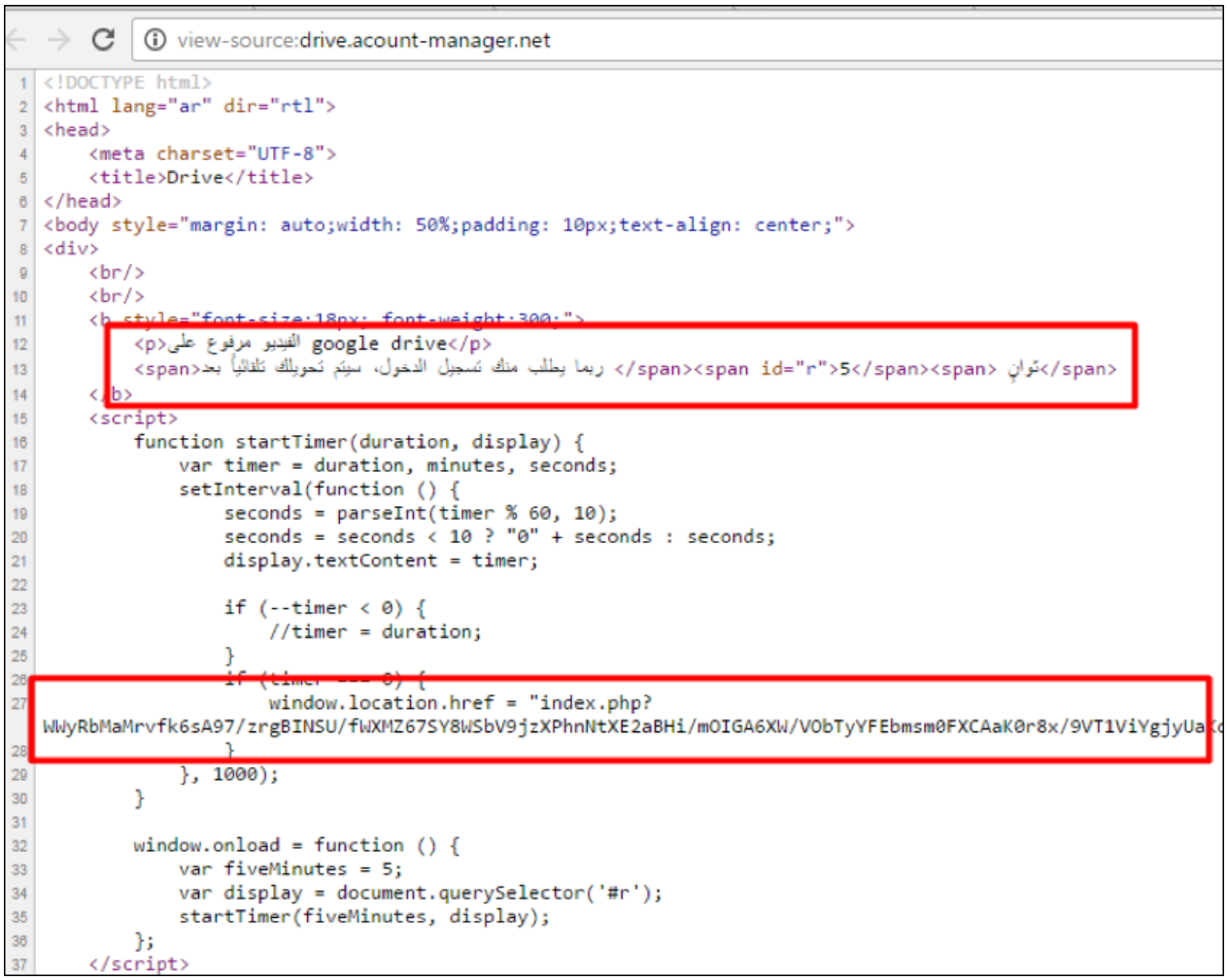
- Logging of keystrokes to a hardcoded text file and exfiltration to a remote server
- Capturing screenshots of the infected machines
- Searching for files with extensions matching Microsoft Office documents and using WinRAR to archive these prior to exfiltration. Example syntax of the command used is as follows:

```
1 "Rar.exe a -r -ep1 -v2500k -hpd58ccc009be55ff172a9039bf35cf270 -ta2016-12-11 ProgramData\Recovery\bin\sys\sysTime\LMth_E E:\*.x
```

The value "d58ccc009be55ff172a9039bf35cf27" is used to encrypt exfiltrated documents and appears to be an MD5 hash, but we have not identified a string that maps to this hash.

A side of phishing

Interestingly in some cases the attackers combined an attempt to infect targeted users with malware, with an attempt to steal their credentials via traditional phishing techniques. The attackers sometimes directed users to sites spoofing legitimate services such as Google Drive to download the malware, however first the target users would be asked to fill in their credentials in, giving the attackers two chances to successfully steal target users' data (via the phish and via the eventual malware infection):



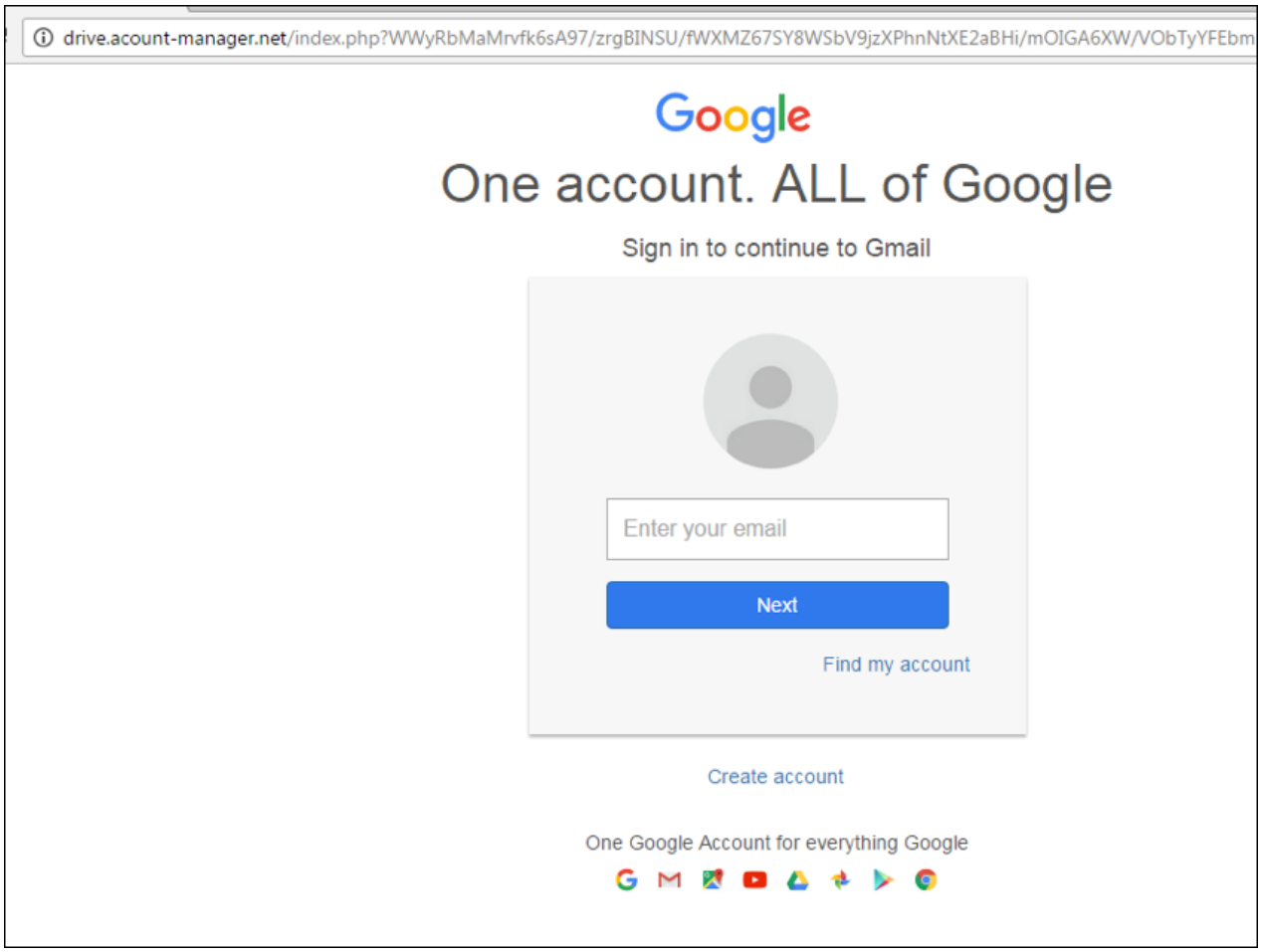


Figure 5: In some cases, users were required to fill in their credentials to download the malware

And there's an APK twist…

Whilst a large number of the domains associated with the adam.swift.2016@gmail[.]com email address are associated with MICROPSIA samples, some have been observed hosting Android apps or acting as C2 domains for Android malware samples. Analysis of these apps shows these are also malicious, and the apps also contain some social engineering tricks to enable installation.

There are two main APK malware families used by the threat actor. The first is a malware family used to gain a foothold on to the device, it is effectively a downloader with no additional functionality and we call this malware SECUREUPDATE.

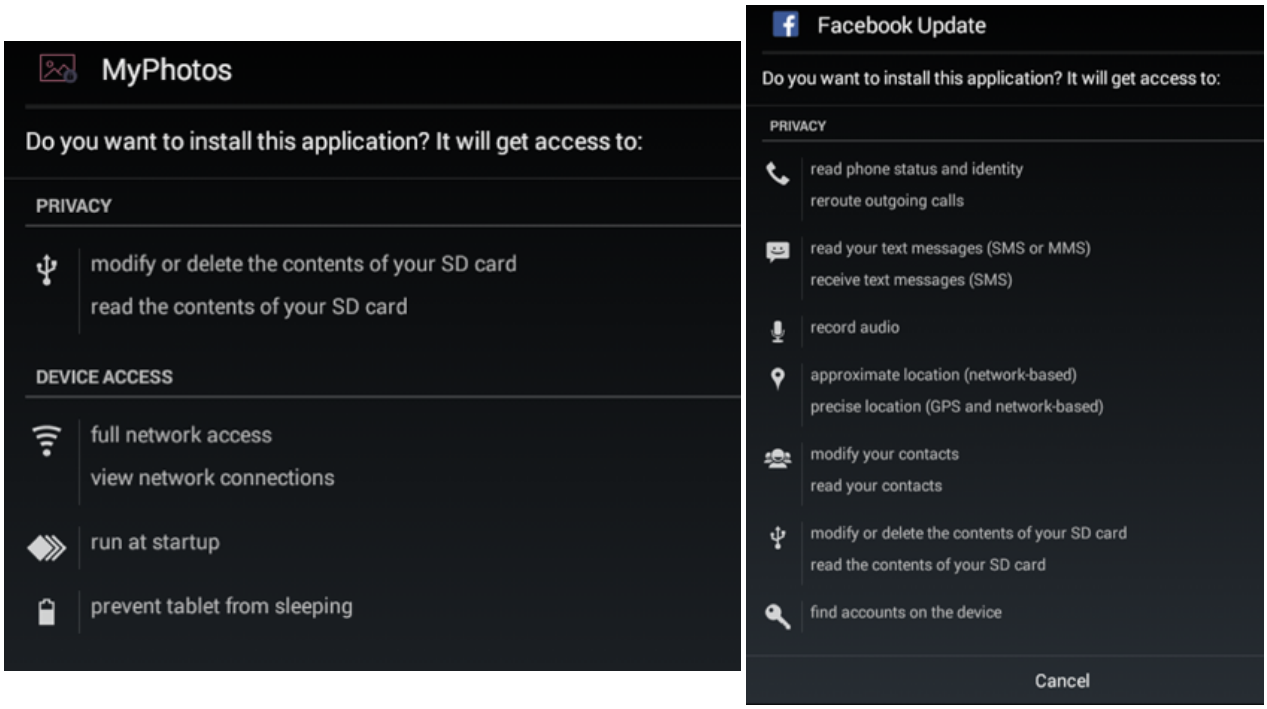


Figure 6: The applications often pretend to be social applications popular with end users.

In the sample we analyzed (6b4d65abf95cfb3cedd39b217ff0e4ee2229ae32aeda5170f34c5a3b9c5a0f3) the malware used the local calendar to sleep, creating an alarm in the future, at which point the malware would call back to receive an "Update":

```
private void a(Context paramContext)
{
  System.out.println("Setup Alarm");
  PendingIntent localPendingIntent = PendingIntent.getBroadcast(paramContext, 0, new Intent(paramContext, DownloadFileReceiver.class), 0);
  paramContext = (AlarmManager)paramContext.getSystemService("alarm");
  Calendar localCalendar = Calendar.getInstance();
  localCalendar.setTimeInMillis(System.currentTimeMillis() + 900000L);
  paramContext.set(1, localCalendar.getTimeInMillis(), localPendingIntent);
}
```

Figure 7: The alarm functionality in the SECUREPDATE malware was used to download and execute a further payload at a later date.

In a similar vein to the 'a side of phishing' section, some of the versions of SECUREUPDATE backdoor attempt to steal credentials for users, making them create accounts for these fake apps in addition to the installation of the malware. This technique relies on credential re-use across many accounts but will still yield some success for the attackers:

Figure 8: Some of the apps require users to "Login" giving the attacker the chance to record credentials of victims that may well be reused elsewhere.

The second malware family is a malware family we call VAMP, which is already described in great detail (https://ti.360.com/upload/report/file/APTSWXLVJ8fnjoxck.pdf) in the blog by 360, VAMP is fully featured with all the capabilities you'd expect from a malware family that resides on a phone. Features of the malware include:

- Ability to record calls
- Contact theft
- Theft of documents stored on the device
- Theft of messages

Another outlier in terms of domains registered by adam.swift.2016@gmail[.]com is the domain AppPure[.]info. From the outset, the site appears to be a legitimate page:

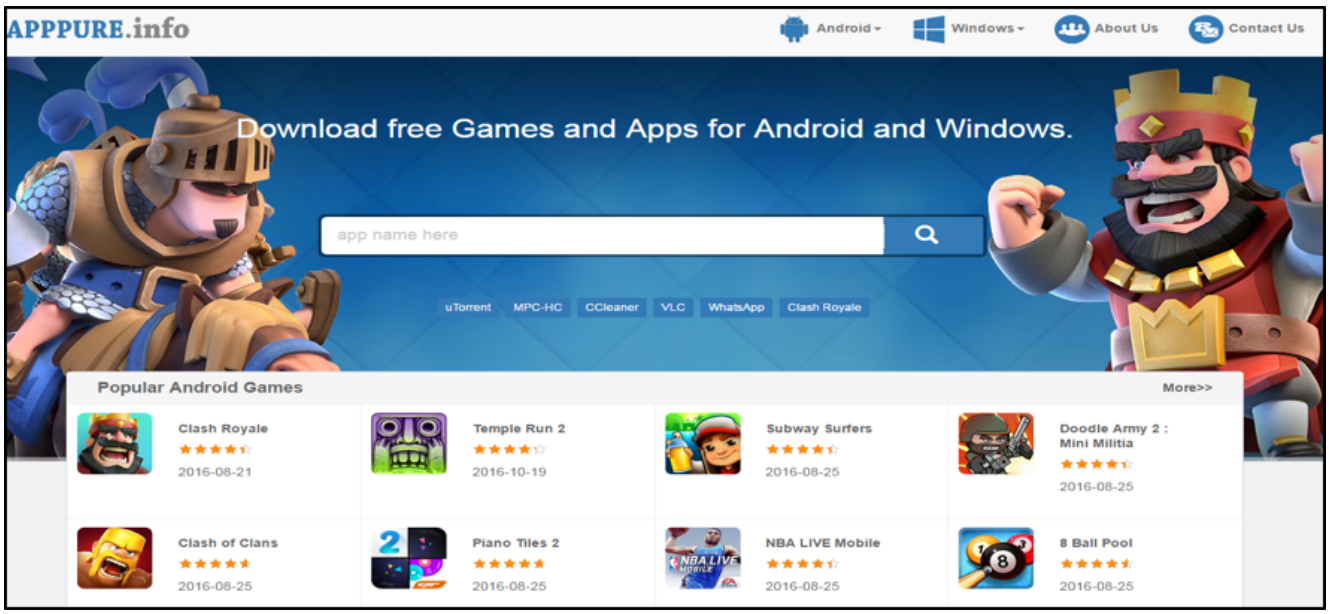


Figure 9: The app store created by the attackers which we believe was used to distribute malicious apps.

Although we have been unable to find malicious content hosted on this site, we believe that it is very likely that amongst the many legitimate apps available for download via this store some malicious apps may exist.

Concluding thoughts

Through this campaign there is little doubt that the attackers have been able to gain a great deal of information from their targets. We have been unable to uncover any evidence which allows us to confidently attribute this campaign to any known threat actor at present.

The scale of the campaign in terms of sheer numbers of samples and the maintenance of several differing malware families involved suggests a reasonably sized team and that the campaign is not being perpetrated by a lone wolf, but rather a small team attackers.

The campaign also illustrates that for some targets old tricks remain sufficient to run a successful espionage campaign, including use of URL shortening services, classic phishing techniques as well as using archive files to bypass some simple file checks.

Palo Alto Networks customers are defended from this threat in the following ways:

- WildFire and Traps detect all of the malware discussed in this report as malicious.
- The C2 domains listed in this report are blocked through Threat Prevention.
- AutoFocus customers can monitor this activity by looking at the tags:
- VAMP (https://autofocus.paloaltonetworks.com/#/tag/Unit42.Vamp)
- KASPERAGENT (https://autofocus.paloaltonetworks.com/#/tag/Unit42.KasperAgent)
- MICROPSIA (https://autofocus.paloaltonetworks.com/#/tag/Unit42.Micropsia)
- SECUREUPDATE (https://autofocus.paloaltonetworks.com/#/tag/Unit42.SecureUpdate)

Appendix A – Associated C2 Domains

mediafreeuploader[.]co[.]uk

appppure[.]net

upload404[.]club

upload999[.]net

upload999[.]com

upload999[.]org

arnani[.]info

al-amalhumandevelopment[.]com

acount-manager[.]net

gooogel-drive[.]com

acount-manager[.]org

acount-manager[.]info

appppure[.]info

stikerscloud[.]com

upload999[.]info

apppure[.]info

mary-crawley[.]com

mydriveweb[.]com

google-support-team[.]com

mavis-dracula[.]com

9oo91e[.]co

useraccountvalidation[.]com

mailsinfo[.]net

acount-manager[.]com

upload202[.]com

upload909[.]net

upload101[.]net

mediauploader[.]me

ran-togomory[.]com

shildon-cooper[.]info

mediauploader[.]info

akashipro[.]com

beauty-dance[.]net

margaery[.]co

go-mail-accounts[.]com

kagami-adam[.]com

kalisi[.]org

kalisi[.]info

cecilia-dobrev[.]com

kalisi[.]xyz

appppure[.]pro

cecilia-gilbert[.]com

gooogel[.]org

feteh-asefa[.]com

Appendix B – Associated Windows Malware Samples

KASPERAGENT

2c8a67f8118b6aef159dd280d5998b1c41edb406a1bc8e3960254a9642b6ae4b

a72178289bb518f9f100b78e56a9425332bf3a5220a6c5abd3d07c669a5d8b25

7fdf2bdc500a8703cceb76a427752ee70164b8283b4df42c5b13ed2124a88dbd

6926f430865bd08b621bd1c6581bfe77db3e9891b14f97d00563770186fc5e74

46b0f586a646e800ab63d1404a08864fb09aca73a13fd22542a9fce038643219

e9050c541859f2fabff6dcd492df02a48dd32d99b1f3e98ef7c14bbb6aa734a2

2709506acdb0c6aba5ce794ceada11b64078f5731b91359cb398bc967cb67eba

fcfe51fd23aadcab5a7878bd59b5354d3491d237b259e230ac51e49306b253c7

1bb2a7a6c271b7e607cf87f2a4003eae1653f304cde104fc0311611cbb96e431

b384ed2a4f484b70786e5ea84ff513d30fe4d068fd76cc214d448f7f1c4329fb

1bbd9498f50259917d737b70a875772f963424f69fb942b86d626283e154cab2

babd654ef363e0645ce374dd9e2a42afe339c52f1cf17fc2285d8bebd3cfa11e

f26caee34184b6a53ecbc0b5ce1f52e17d39af2129561dd6361fb4d4364e2c8b

325c5aa819dbd1596464ec018b9efb5938dbc59ac6a94c459932ef07412bca02

4b77194c47b5abb04b1395955ca25aa0bb63ce796247d22946bc07919c8e1b56

9ae853b1e678926358ac8c1cd583eb2d5968b99c2a16cf34334a22051bb630ec

1184916919ea9790adcd53b60c4bf875e54733e508344ffe6baf10b919a0fd1d

beb05e01b87e1a432b3ef37eb55db723a5a5231872a53ab777d7821358e97574

433d2c8a3e93191d09e11994438ec3413152baf64e26e8d9e43c2d2e056b700c

783486dd30ca43d3a6c6807530c023f61631e4b3e6f2e6c2830b5209ee384e13

2813409822b56ae81f08adcaed29a215b3bef0e4f1cc5a22c7169f9e16a188a0

6eca9aacc7d9ef570bf2521f5a1156825832282650d2d3734d964a834f97b3f4

b8285b66aa42f61de1c43423ea25f8cbe03ebb96d0917c153476e185a5909e57

6c51b3ca96d06cc695de3875f4d31962bb936331a82541ab610f269fec0b0a8c

cd051cb14f118e33a2299925a704a56d89ba92a310f2176a0942ec29babedee6

d5e145bf964b91210b79b25fc92ce19aacacadac14ebeb6f4111b6f4cabfd6c7

98553dacbb2fdd8d655907f29e8ba36265f931fd5c6fe83c4defafc10767d4f0

e1addb50f0fea302317c40017fcdad84e1b8bc0f6d5b3f2609de2a0576ad8f9a
a8825be2145fb5cc25194aa13f5168ac7ede1132632cdeebadfb640d063fc781
ae5625a0fe39b34884cfd33832181392e9cf5157b8070b2e1b3d04c87fb46eec
4eca7eedcb5cfa0f02306774b9ed685a5ffc738669bb90cb5d57dad87a46833b
400c9fa4012a67e88b986d206deb8b10acff3091b6e7c98f0f98ac553ebd021b
c7d2a0803f9d4f9f37d5a0f3a37b97eaa672d4b3c700163847736cb9f91aabad
71aa4f9bc78fd5d457e4a2f2914516fc0081d2d5d22da26e1c70f86d9bd6bab1
117f80111e0fb67f728091a1b96042ea6f1633ece8c8a519e45e38d408a6691e
4ae00d8000510629bbffc55652401ee4124109c55500075049f9440fe86391cb
df2f111c952ac720cb9e33afb24a1c9d0c9ecaeaea4c079f48fadc1a4ed333d5
2321fbde63ceb3d0086a9bbce55940cc6f05919acf49fdb731f75447863c795c
fa80f9b2163d7db3e026316967d241818c9e57c1376830899352115bc08d51ac
f296539deddb1b661868c69cde1783a2a2be15456ea3e31523652b5f10cc7d36
11cbd7a2ce58191e4dbd3efffba97c5c4c0edd437511e2ecbd42811dac1cfa3d
646b6591002c125108fa1e108aa9be84f4c83f3130836279745e372ee12867cf
4c1973278a30d1b4ce206eca63676624d234260758a0674d191d338a02914d23
e771f7512bd1efc86884fad12115f2fb5abc97eef78ca7dce1fbc9fb6f23360d
787f581acd27f8c8b449b3bc0ca214a1b3421197ff789333ef1b44a5de850c03
b119b2530baf4c80a5543b7c6bacb615357b2deff27d9b6a638f799617ec1641
00b9fe607cb0b6ba45cd7ffbc3d710264c6109fdbad992933f68bbfc15785a18
34a4a989a6d83eea916c455a9c304823786f11d39c7525583f75a0fd35906a1e
967fd8f1e08cde8dbc960f3d9fcac5a86b77003cae88d59be78ce0a7e6ad0d88
83d07d027709c724b146aaf44ff63d969b9c2824bb5f0b3c1be5af4f18b3cd97
42c12d9b35abbb79212bf9d35d7c391d18e2635e558eb6ab8472510df79da09f
f602d059bc6f7e1e5353b716fbbaf42fa5746e844532674198f59deec367490d
365be95490051c077b2bea93eb8e647cc4ab76cc51ebc6781abfca8b6d55b551
a52d3e65fe5bbf57bab79b1c5092b66d9650247249b72f667a927f266d09efe6
a8635544eab476c6128793b00bf1bd48ce9d41692585aab1690f2a44837efaac
4d54b94d081fa2d0c0626805f71bca86314201a6215fbd910c98024b372158c2
1a609b82e95501f56f0f47014c4224fdba457b27c58672292231c3adfcfdd7eb
babf156ede8b5c2e6c961b6ffcccc5eb7a3d283b398370754061613f439d40f9
e58267f9ff31408d0bb1b84948e1fd3c02231cfd0628797cc2a6045354e0b065
2dae0b95ba31c12c59d577b32c11ed3d1dff6db76f9c92064a2bc2764eb8611f
5e977ffbfc3d048c79640459ab33a932f1e17f77dae76d7a062c4cb0221b91f8
78536b8ba75ba8269950099bb8205a11e94db9c28558293971e981c3a9e57b24
f0cb1d8a58b389425f691522163a1cc3b2b6c4ca0004248c0f0daad7f4ffa12a
865bf72cd5f23350cba26bb185340ebc0def6b5bbd5d8c9c184e1d1e4d11c5b8
dff184a646f67fdf04fc7702e2a4ef60b4a165e56abb7e3a424f785ac8b02da9
3554b267dec35b5072ed5fce2510e70960e32195a0920811e83eb6207cc4bed0
baf0fe69b670a6b96489cfb0bd80b03d8b454d5a3d2407d3c1570f1db9b58927
e926cf1e40c46f9578c76bb0df3a3ba7667853b63cc58b0f064f529b4365fbe0
bacbcb52516bb1d54b82a8d128f460843827a9dff65024d4bedb88936fc40c97
618fc941c00005b02f62d9ebdb31363e4d51b2f927f3d0b36c238a333f080ad0
64c5bfc0a1c76aaf9ed8b8f2a45d229afa9353a63fa7a2bba6d4a8c47980e70b
27b3a779d2e3d44cf0c4cc8e9f2862226fe329db7127b2272ba42011332832f3

2a71fcd81cf6c3bc6a43260b23cd7ef1c0694b0d85cdcdfdc8b25b139922a352
244621fad10485386493efec3818196fc50f1a66e3048a62de456d64a2331720
7b1a513520f18612c4cd2ac9e5e5a1d660274a77b8f190bd277339247b6a51ee
7d74e531dafdb6e645ac429c17aba3903e9c0f4fe7e4f93688d37eb638c52f48
722cfac01badf1106887fbc985060a2fb31eabf9943520bd24abf2fa208217b8
5a83a289c0c4c222bb190152bb8bc5f429e6799ac233ba99b7a860b8519872bc
50cb597f33f8252bd94c54927bd2e0259a732ad64fb8b413a205e1f290870445
c721b5d3abc978ea8608f23b9a9a6ba81afe87d6d6660bc6006ee1ba83491d06
16e43f8d2e439b5ce8e48b75bb25e90011f1ccbb41278fe15f7982a304a832de
5579cfef934b47519388719f0bf532bd4326d0221b6ab47c69ca098f3d2d2de3
7e476fb1089b95bfb08ec3ab3931ae31da9fd1f742928bab339d297b70b9fcc2
6279030f7e5eaeacd28232de35382c38614fefc90ef753f2492300c1150e54f0
e4f015b6cc0539fff746dc39229d25385d95e827204695b8b0003457cd206dab
ea6dffd2bb7c13eebdb605060b26ff2319f6f4ab81e9c41998351c039c177d5a
4546413de0c2df37c83a88808cebe265dc74dd87c550c378f1d23d8e5430a7db
a02bdf36048e6440c50782dbbbc8e0529e4ee480bf2be43dcad2d22f3b47bc08
5e82f68b6560c959975b9e8c20a82de71fedc8dc7277d2a16c9a13829c91dd22
30912cc80cf7defaec360cdd08952ceed493e88d87ad705ec80831581c5c867d
44d0c56f4037d21b85fe00e944456cf2a67e71ca3133c3afd0ea1f35d29e7b33
bdb17c29b31fbe557200569f584c589104b52f188799dc5b45a33f3a7a16a34d
c1ab9ec3f1d6050a77cc8d976dac441c13ba2fd3c0229076c20a2406258198bf
397087699aa240e8a74a687902ad3c8b2a0f1535179fab046673cc1032c72796
2088d5f31b8f8a75464def9b02c159a2a1aa3056fc3c82056272c9b39cea0639
bb3676b9ea838344e955cf58b01d2df4384f6ba8b62fa00259ab8c449e77f358
a2e979e03c32e5de9ba34407b37143b6a887ab6f9d8cdcb07a6276f41202dc5d
c24e30b7a32f096bad4385012a1c1b3a61198156b19081f7658a4f1c25d055c4
7be574a767acb4fe9a1af425fe1fddcda17a97f4653837384352cebec21801e1
54b07adba4b1fd4467a2cae45480ae8f764866e8ae6bf66150f2cd860b36aaf2
4550e8b216c2ef7d78be2ef572fefbdde76c0c6640c6c1cb6757a3867a9710d7
455be9cff65b2178189444572b0a9b31d5cc5b709bcefc7381eaf4b9141ca46f
81410d2a560984fe41d371bd745f6de9f9f120dc929f439947f3cfc330774a95
5329652e9eb2aa681abc8e69955b24165a23a807a69ae76e67c07d1fdfe8fc38
42e8118271ce2df0a3313e271d8a86f425bdcd15e1b5bd6c6239701cfad6da3f
8ee8572d912eca16470679fcd4d98e6e22e4446c2dd74d5d96f1056ce3a93e22
c5fc26f84955a041de20f3ff2ee04a59f9d8a2ab5d6c4702b8da0cf03b4147ef
e75d209025a34fda854cb9289c1f329671fe010ba6616e24c0338eb9f17266c9
2c0ba35cdc0ef302fc52aef368565b61edbf9c7a962661cafa4b2cfc26eda371
1c1d858934f278abac6bce5f609db8649d58ceaada00f661b6e18b0dd13946b0
31a4d2f12b5e8ab7ca06a61dc117cc5742ea222e3101e495b60f4c289f14b547
7f11e0bbc892a97b7c42416c43fe178ebb240939d9dee70c3c598305ce8a2d4f
c9ffb81a97a9458f1fc96f35cd187b1d7311479e77d031586abdc3d426da0859
a136bc03de8cf0b99b8aa500460a8be6aa1c98ce78515c217ad03d6faa9e08f1
874febea579812e0fbbc3dc1e591264108e61864c48f9b8e15fc9644edee0621
f7bd43323917ce3ce71da472593e0899dd54ce957e2621083a29680a04a263e8
5ba356e5e96ce8b9cbccdcb11d817bb53924afdb7e3af72155898fc7bfae0920

MICROPSIA

453b9f7aed67f41ec192db3011459e2dd865bb729265c544ee1b8814c6e7dc53
c9e55094b84a06b3a40b7df1cd76fc287fdc02a2cdd30af359743bbc23475917
a627d2bff74ce07a619cc8fd36294f66eab94b92d41e50b06e63d736ffafd254
f70681c7e8ab419fd0938802a823337abad936cccc0ace9ee232f2b874e561f1
e3963ee9bf892d3f3eea0620585e2e773a30cf536c73a01dd51d6ce36f4daf5d
e2ac3cf79e7267d2e088c3a269aa84fc71fc6073019abb94d16a024d3ad16f3e
b08b96eb46b65af20688c3910a8edcc7dd072a5149ca4b541183acfa81220b97
cdada29d7cd7d88a49a4475a50ee0401d11e2d9a61c4396a60ab0a2fb3da0d01
ca438526ad398f240d3ba551cdd59ada402a6270755c4b0750bc0b120e058320
2fc2263416b3b55e1dfe67ab6435eed00a74a82e3fbdfdbb6a3a102a7f404641
15c9dc07d2858f496ea7f4110a13e58e6828fe836704582dbbdc630df18d3de5
579cf5f112c5b542f7240e200fec6312983255b497c6f0a65f2fe2d3b78391c5
15e3cd8a698d30ac7851b3232f8b7cbc7fbbb821c9eece34ef327b67dc281883
1e5739d640e24504a5e03d0847ad720622c64d0effcd2e1b80528a055049ca82
8f1ff9588630c3bc017468ff0eadb69c65cf77aae47a148e132eb4b48ae5c988
eb5e920dd1e2b2df4cede82d0efbda1556fa35ac1c4589533fca58832fd07a62
2fac7aab5c3b922b883941fa67fdd7c197e6aaef429e723dccb3fc2150083c8d
368845729255ab7fcfb5c0b6c153929d5ccb8d1f9a40cc02ca7c026b4b6813ec
41b3e90442c97e40abdf29d8b7ecedea1026a1fb4dbd6d6cc410d3f3463cb205
b284c718d5b6c30eea2a0df34d9d75d3a22baa776b8d6f75b579da5549529f43
74a94b549fd52e8c23c1fca23a80262a50ae8e08ae56adf9e94c54acf2b313bf
39aa9cc3747a7fc9c80a04ef47107950c1946386525d79fe97b0bfb593e4bdc2
6c3bcef39b3892b5c3ed5602624ca5ee244cca7bf86aebe293bbd11eaf57834f
c4e79e151986dc5e16ce763321de90d8c214909df7210ec05e590c4375423a76
5bab8a360d1d08e37e4e6c052f7fce13a291ad9b99f950770a647222bfc4d6b4
accf87a349b0cfe6403e827089d7a97a8a9bf94dc4535d9ce2e54ecf9bc699fa
4f1be1f1c28dfc337a37cf22611aa288565c294910083524be4a317306b5490c
6e461a8430f251db38e8911dbacd1e72bce47a89c28956115b702d13ae2b8e3b
7dd7cc9e90b074ecc3d8f5540864e105fc0cc034a18a0681bd0ab14252bd0387
023cee622d8ddd7afd7603c1ba13447931508140cfe0dfd85bf4adc5b0d2cf8e
63d9a5ef92a18dc7238bcc59330b41149cec4ef7602b18c0b99abdae83c0114c
adbb67b004131990598009162a195b04107231a79de25945de94d2978f96dcd5
39e4e3637e651d2d8251c0f891dc4b0f0494c9bada2da930761d3fe6cc6ebaae
6aeebb3cdb2ca9b325e042e76d195a5ac958b119baa559532c22d344f1491a30
fb95a719c4b26bb577cea5837cac6ba9fdfcfd240bc2fc7b1d0759bf392d5191
dd185667015d23438a994adc9e9b30572a1e7479c05f563e0b6c71b8c6023685
2cbafd6a0461e7ae1929897a8039ce5f198b76281465c49b4547abf9a139dd89
b6f8b5ba026af863e878eded79f40e5efa1dd7ce725cd0479e5f062dbf4fdd4f
cfbe077d7a4807203c889292668695e114ed9524a11a00b0d670a2f4da74a27c
d8d87ac1e004de113a5a394b757f612bcde22eaaab574e53d4b1909193b77b7f
6eea4d800b3af9363abcea6f5051039c2fe7bec3e690500077f022204588db6f
2b644917074452c385e4a960d9ef504ce22733047dc282ef31ba7c012041e58c
499569d014d6b05e2187b8aa5966e4b56133cd67ff7a110c259cda5299cdd4b9

0edc4424c8eeb9708b6b8bc74806b6c17c9cfbb49e2688f711092381823fc733
a9ad6b278cabc7c9ac063c37b0656cd924639a227977ff250339479d5aa0863a
e477b5e00699a9ccb3868de543c29087042fd44c631f8fcda5faaf7922382146
114ef36f968912ef885d06e3d092dad739f9b6afe2f246e52fb3ba5e6bf8ee00
85d2d2293364c90d51fba7696a44908e0fae50dae1337e59441692e91c25c9d1
7efaff81e5be73608bccad93185f6b559597d2819bb33c95436d9246ef602f49
2e225c32dc320ab2441274fc7acf6fe52bd9621314c27e806fa8c4bec409b5e3
8f3e3b93eddb3f1fecc75d46e9ea5eb5d2ba3283c1e040ca12cb7530b7eb2455
75329e7b79284f63c1383244b20fb0d9c4bb1e9c4feba04307f1223db30c9203
04f6422325cf3fbe35879cb6532745d3a3b555144ef7b4e88ed96bf3fe4e70ac
fb64d608573ba1b1fd4254e7a1c7b3ffa1dfdc678300cc5d16eb4a88cf7592e3
a2cad08db8e151a90857df70d9e9c5e605aac6fa0e6e5d5ad150c96027743612
b5846554ee1ef9de0a8d83527f609abf5b328d104056b7a763ed89e75152ddbf
cf9287ded9b5a6543afc66ca60c4d20e6f7e4c318e8f303567d781eb98e4168c
def8065164959595de2ff6b35141985e7fd7a6c836db0b7a3f389b022c7f3650
3a4498a6e4213a680dd2e57516637f7480c0bd7a342ec24788fdb9694b0d1150
6c21e4331ec2d02e427025efeb6fbaf8c779513027720d24365283d5166add77
e05a329bbfe8cc0f7f3e2296fe0bdf86b6d4df70a8242409feb6c846db0b221c
559e6970861563f815e097a7a152970508323666c511afbc8165c4869256f692
54e5f4ecd18c6a18a6f25be6b7a392cbbd5bc107b868d8a078bf3e3fa701e453
e0b2671b1ba7ac123b6ec3e152711691e8690839b8e04fbb748d2fa8a4f5e982
1adbad10e5193b7533bccbae9bfa660f29162730fd4bd89c332bf8ae5b96ae78
e8ab81ee03aca399d8e4e3f6ca9d6e98c7c75e68f22e12d6213c15d8b9cc3ace
425d427828205811258e22cd04eb9acb4e497590eecefed77cdb9252b3e45fcb
876919233b24808b457fe83c815a4e6b30e415771bb6fe2e68a5cdae8e9a6c6c
6b676728f3206db8aa7ae57d8ee0747f2919a64ab8157b28bd1add0c15d2bb59
76573e0c213dbdba3283887eee7418f2b0c0ce6506145567547319bec8f0d6a6
d1bbde1ddd5bb1b421f230ba2213013b098f2abe3ac526be142371e2728ba40f
9a32cc01c4e6120cec03aba783087df35724d5b1feb3f75fa0b78963e8cc7735
699f4f0513de49db7dafa3760daa3c27ca9cd12e216ff3e042966212870bb906
1a4d7b935cb365f75a3f33c6490023aad054facf55a1411cd7b9d723eb99cf53
14b34347a75bc46ee69e1782cb658f7f404487a8fc40b973649d53d008bc0e75
8cf8d06d2935153d3c8d570ecd5990432bb4933ca89845bc2cd763b40ba7edb4
a5daa9cf58a2f6bf3f39ae022b0c87458b3ade2d4a006e5489f2417ff639e011
582cd41417aeb2f3f86d2c9fb7f8add4e5edacfed7cae0aecc8cb088a823d240
0d94f4aaebcdcfaf5b377af33da42e69b453297cf6b90387db95868a48c172bc
2f40c95693d1c0b0aa8195a7b943b935634745a1aae3ea91752ca4a535e69007
7f02e8bece61a3fa6400e9dcbb0972a136b1818bf1629afe4456819beb04b4cf
77dc371fcdcaae8f38e942e9084855d62f2daf81460c33f2ea64c77a470f8c8c
06a69598b2251200cbdf51c53be45ad90240fd69502063aa4afa5b1086fc34b3
e73381e591dd8538641236530bda5bc0daa014e3486b11a4da820657b48db9f9
027b0d9ee5258bb18c824be1b6aff33aeb3060ca3e577f2f8fff06ed4854883d
7d4e98f9136c4c7952e3acbb328ad06e522718ad4d05bcd04eeb225335e75631
b033de3c20701482bd375ea6e45ecae38295de72336a5f96f4ab994e6cef212a
b22b98b8d50aab1b0bea0e458e0736940215365752797de892745bafda5d9ce9

75a708bf42ac01d857ecb3bff18c633e334329d4b89ae4201a989f564a2410b6

b679878e940eaee79436a895aa4f43e32416c3ad2fbfeb812fc39022c84b82d9

3fce85b9c279d94dd7018a656027a496b4b5df719933630d7375c42ac088dd87

d63da6f863609c87cf283cd6da7c325f9622bff986b05c47e106855a514da4b6

0e7507e955dfe8027ed5740400dda772c403510f75d066baf0077ca1ab478048

Appendix C – Associated Android Malware Samples

d909669b000c479b8bdd9f86fa62879a7c8b4dca8cde4f4a404862a4604c52e2

b6abeffe986eb38e411a4fe956280e2028d8bef699d9dd3244bde721a99b1dee

c1564c56c46146db36ec97afd994c45f3621f39c82cc692adba5b9f6d9a62897

c20438ba8c9e008c1e2eb4343f177757fc260437aeac52df61b156671b07ac14

5f3b4eddcc72598721b9ca395d1e5881acbd4fc562e09b688b2d42f65d3a4a93

544a1c303ef021f0d54e62a6147c7ae9cd0c84265e302f6da5ed08b616e45b78

522ae87e792fd0b2021af0edcdad283505d6258316783c489f37234231b9d6bf

22078e0d00d6a0f0441b3777e6a418170e3a9e4cce8141f0da8af044fdc1e266

58e70e498397acae9b5e84a153e27578ee25e0ee0aca16bcf8a1746423f210f6

e23d689fff3907cbc6f495d1ebaa9c4cdf6f93f9fd26b790f60680dedf489618

02e1692dbc95bffe12083786208a966bf6b184a428378aabebbd3fee501021c5

758dc6aff09885abf9a6503e4a6473bca83c878f6131acf41290a3c8a5df7cdb

f67356c2bcd99009f1d68806a1214b4108771926e423908d8997cd881277e76e

d066c1c5eccfcf64e8398a49ac7efacc9d70a8c8544fb71ba22e0e2f77bff543

16b4d65abf95cfb3cedd39b217ff0e4ee2229ae32aeda5170f34c5a3b9c5a0f3

43f2e20933638594c02c83e85bc058b46c308b4f851477e2c0a2a92b4fb1168b

2a28c199eeb622fedc9b0b16f65f9a2da113dddd264966a76654546ce70804a4

53ca656dd54c14b14ddc758e2160443e1d5d761ffecb37e15216da67fc94c468

B2036d2b31c75684527a8850182363fefbe436dd8f5ccb5e792df2a8535981bf

Appendix D – Observed PDB Strings

C:\Users\USA\Documents\Visual Studio 2008\Projects\New folder (2)\kasper\Release\kasper.pdb

C:\Users\Yousef\Desktop\MergeFiles\Loader v0\Loader\obj\Release\Loader.pdb

c:\Users\USA\Documents\Visual Studio 2008\Projects\New folder (2)\s7 – Copy – Copy 19-2-17\Release\s7.pdb

c:\Users\USA\Documents\Visual Studio 2008\Projects\New folder (2)\s7\Release\s7.pdb

C:\Users\Progress\Desktop\Loader v0\Loader\obj\Release\Loader.pdb

D:\Merge\Debug\testproj.pdb

c:\Users\USA\Documents\Visual Studio 2008\Projects\New folder (2)\kasper – Copy – 21-2-17\Release\kasper.pdb

C:\Users\Yousef\Desktop\MergeFiles\merge photos\Loader v0\Loader\obj\Release\Loader.pdb

C:\Users\Yousef\Desktop\Loader v0\Loader\obj\Release\Loader.pdb

Notify me of followup comments via e-mail

Name (required)

Email (required)

Website

SUBMIT