ScarCruft continues to evolve, introduces Bluetooth harvester

securelist.com/scarcruft-continues-to-evolve-introduces-bluetooth-harvester/90729

By GReAT

Executive summary

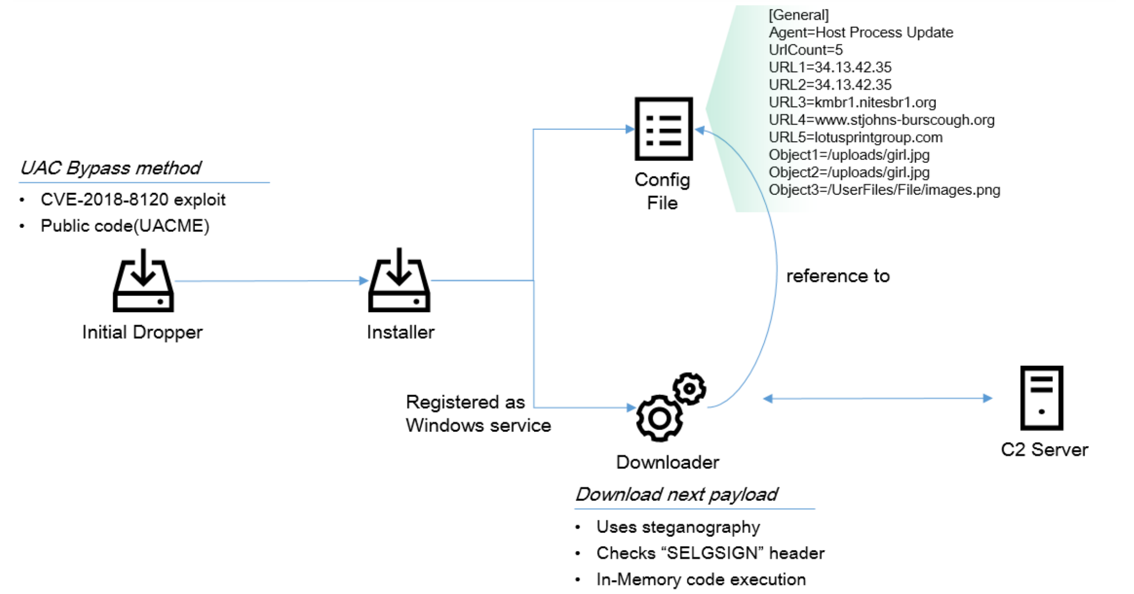
After publishing our initial series of blogposts back in 2016, we have continued to track the ScarCruft threat actor. ScarCruft is a Korean-speaking and allegedly state-sponsored threat actor that usually targets organizations and companies with links to the Korean peninsula. The threat actor is highly skilled and, by all appearances, quite resourceful.

We recently discovered some interesting telemetry on this actor, and decided to dig deeper into ScarCruft's recent activity. This shows that the actor is still very active and constantly trying to elaborate its attack tools. Based on our telemetry, we can reassemble ScarCruft's binary infection procedure. It used a multi-stage binary infection to update each module effectively and evade detection. In addition, we analyzed the victims of this campaign and spotted an interesting overlap of this campaign with another APT actor known as DarkHotel.

Multi-stage binary infection

The ScarCruft group uses common malware delivery techniques such as spear phishing and Strategic Web Compromises (SWC). As in Operation Daybreak, this actor performs sophisticated attacks using a zero-day exploit. However, sometimes using public exploit code is quicker and more effective for malware authors. We witnessed this actor extensively testing a known public exploit during its preparation for the next campaign.

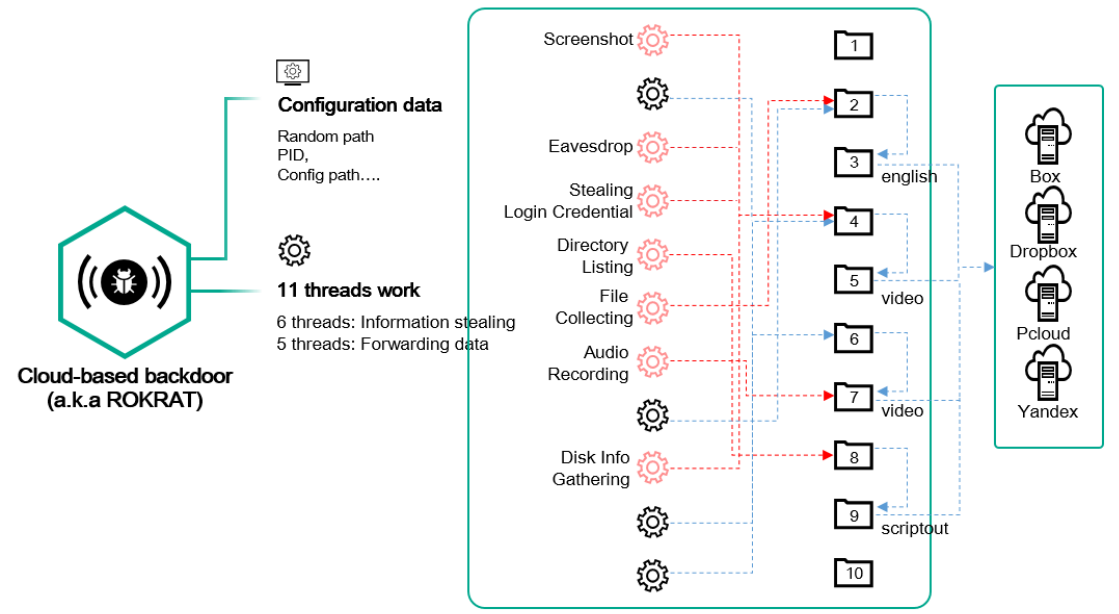
In order to deploy an implant for the final payload, ScarCruft uses a multi-stage binary infection scheme. As a rule, the initial dropper is created by the infection procedure. One of the most notable functions of the initial dropper is to bypass Windows UAC (User Account Control) in order to execute the next payload with higher privileges. This malware uses the public privilege escalation exploit code CVE-2018-8120 or UACME which is normally used by legitimate red teams. Afterwards, the installer malware creates a downloader and a configuration file from its resource and executes it. The downloader malware uses the configuration file and connects to the C2 server to fetch the next payload. In order to evade network level detection, the downloader uses steganography. The downloaded payload is an image file, but it contains an appended malicious payload to be decrypted.



```
[General]
Agent=Host Process Update
UrlCount=5
URL1=34.13.42.35
URL2=34.13.42.35
URL3=kmbr1.nitesbr1.org
URL4=www.stjohns-burscough.org
URL5=lotusprintgroup.com
Object1=/uploads/girl.jpg
Object2=/uploads/girl.jpg
Object3=/UserFiles/File/images.png
```

Multi-stage binary infection

The final payload created by the aforementioned process is a well known backdoor, also known as ROKRAT by Cisco Talos. This cloud service-based backdoor contains many features. One of its main functions is to steal information. Upon execution, this malware creates 10 random directory paths and uses them for a specially designated purpose. The malware creates 11 threads simultaneously: six threads are responsible for stealing information from the infected host, and five threads are for forwarding collected data to four cloud services (Box, Dropbox, Pcloud and Yandex). When uploading stolen data to a cloud service, it uses predefined directory path such as */english*, */video* or */scriptout*.



Cloud-based backdoor

The same malware contains full-featured backdoor functionality. The commands are downloaded from the */script* path of a cloud service provider and the respective execution results are uploaded to the */scriptout* path. It supports the following commands, which are enough to fully control the infected host:

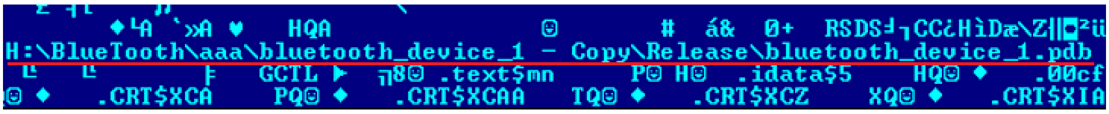
- Get File/Process listing
- Download additional payload and execute
- Execute Windows command
- Update configuration data including cloud service token information
- Save screenshot and an audio recording

The ScarCruft group keeps expanding its exfiltration targets to steal further information from infected hosts and continues to create tools for additional data exfiltration. During our research, we confirmed that they have an interest in mobile devices.

We also discovered an interesting piece of rare malware created by this threat actor – a Bluetooth device harvester. This malware is responsible for stealing Bluetooth device information. It is fetched by a downloader, and collects information directly from the infected host. This malware uses Windows Bluetooth APIs to find information on connected Bluetooth devices and saves the following information.

- Instance Name: Name of device
- Address: Address of device
- Class: Class of the device
- Connected: Whether the device is connected(true or false)
- Authenticated: Whether the device is authenticated(true or false)
- Remembered: Whether the device is a remembered device(true or false)

The attackers appear to be increasing the scope of the information collected from victims.

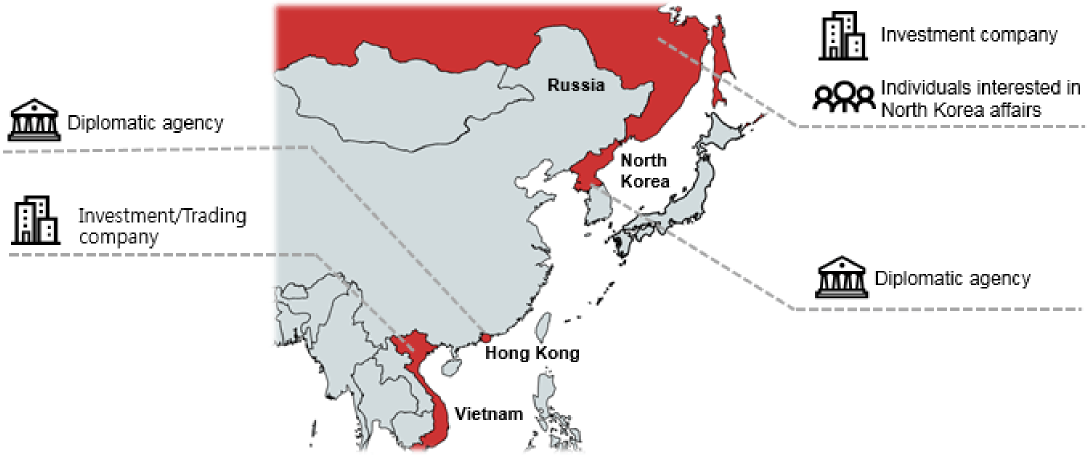


```
     ♦╘A `»A ♥    HQA                  ☺         #   á&   0+   RSDS┘┐CC¿HìDæ\Z║■²ü
H:\BlueTooth\aaa\bluetooth_device_1 - Copy\Release\bluetooth_device_1.pdb
 ╚    ╚          ╞   GCTL ►   ╗8☺ .text$mn        P☺ H☺   .idata$5      HQ☺ ♦     .00cf
☺ ♦    .CRT$XCA     PQ☺ ♦    .CRT$XCAA    TQ☺ ♦     .CRT$XCZ     XQ☺ ♦    .CRT$XIA
```

Build path of Bluetooth information harvester

Victimology

We have found several victims of this campaign, based on our telemetry – investment and trading companies in Vietnam and Russia. We believe they may have some links to North Korea, which may explain why ScarCruft decided to closely monitor them. ScarCruft also attacked a diplomatic agency in Hong Kong, and another diplomatic agency in North Korea. It appears ScarCruft is primarily targeting intelligence for political and diplomatic purposes.

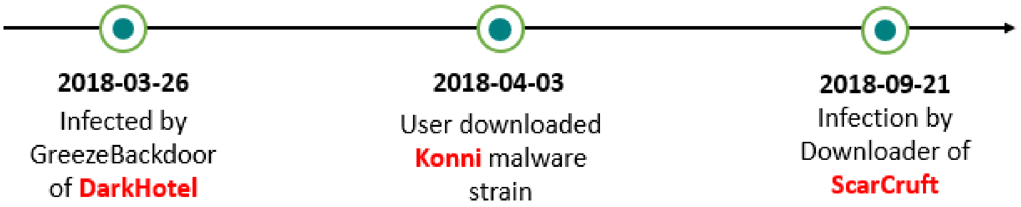


Victimology of this campaign

Overlap with other actors

We discovered one victim from Russia that also triggered a malware detection while staying in North Korea in the past. The fact that this victim visits North Korea makes its special and suggests that it may have valuable information about North Korean affairs. ScarCruft infected this victim on September 21, 2018. But before the ScarCruft infection, however, another APT group also targeted this victim with the host being infected with GreezeBackdoor on March 26, 2018.

GreezeBackdoor is a tool of the DarkHotel APT group, which we have previously written about. In addition, this victim was also attacked by the Konni malware on 03 April 2018. The Konni malware was disguised as a North Korean news item in a weaponized documents (the name of the document was “Why North Korea slams South Korea’s recent defense talks with U.S-Japan.zip”)


2018-03-26
Infected by GreezeBackdoor of DarkHotel
2018-04-03
User downloaded Konni malware strain
2018-09-21
Infection by Downloader of ScarCruft

Infection timeline

This is not the first time we have seen an overlap of ScarCruft and DarkHotel actors. Members from our team have already presented on the conflict of these two threat actors at security conferences. We have also shared more details with our threat intelligence customers in the past. They are both Korean-speaking threat actors and sometimes their victimology overlaps. But both group seem to have different TTPs (Tactics, Techniques and Procedures) and it leads us to believe that one group regularly lurks in the other’s shadow.

Conclusions

The ScarCruft has shown itself to be a highly-skilled and active group. It has a keen interest in North Korean affairs, attacking those in the business sector who may have any connection to North Korea, as well as diplomatic agencies around the globe. Based on the ScarCruft's recent activities, we strongly believe that this group is likely to continue to evolve. For more information please contact: intelreports@kaspersky.com

Appendix I – Indicators of Compromise

File hashes (malicious documents, Trojans, emails, decoys)

ScarCruft tools

- 02681a7fe708f39beb7b3cf1bd557ee9 Bluetooth info harvester
- C781f5fad9b47232b3606e4d374900cd Installer
- 032ed0cd234f73865d55103bf4ceaa22 Downloader
- 22aaf617a86e026424edb7c868742495 AV Remover
- 07d2200f5c2d03845adb5b20841faa94 AV Remover
- 1f5ac2f1744ed9c3fd01fe72ee8d334f Initial Dropper
- 4d20f7311f4f617104f559a04afd2fbf Installer
- 03e5e566c1153cb1d18b8bc7c493025f Downloader
- C66ef71830341bb99d30964a8089a1fc Loader
- 5999e01b83aa1cc12a2ad6a0c0dc27c3 Installer
- 4d3c34a3070643c225be1dbbb3457ad4 Injector
- 0790F1D7A1B9432AA5B8590286EB8B95 Downloader
- 04371bf88b598b56691b0ad9da08204b Installer
- e8b23cfc805353f55ed67cf0af58f305 UAC bypass(UACME)
- 5380a173757e67d9b12f316771012768 Installer
- Ec0e77b57cb9dd7a04ab6e453810937c Downloader
- 25701492a18854ffdb05317ec7d19c29 Installer
- 172b4dc27e41e4a0c84a803b0b944d3e UAC bypass(UACME)
- 7149c205d634c4d17dae33fffb8a68ab Image file embedded ROKRAT
- A76c4a79e6ff73bfd7149a49852e8916 ROKRAT
- F63fc2d11fcebd37be3891def5776f6c Dropper
- 899e90a0851649a5c270d1f78baf60f2 Simple HTTP Downloader
- E88f7f285163d0c080c8d3e525b35ab3 Simple HTTP Downloader
- D7c94c5ba028dc22a570f660b8dee5b9 Simple HTTP Downloader
- A6bd2cf7bccf552febb8e8347d07529a Simple HTTP Downloader
- 7a338d08226f5a38353385c8a5dec746 Simple HTTP Downloader
- 46F66D2D990660661D00F5177306309C Simple HTTP Uploader

GreezaBackdoor of DarkHotel

5e0e11bca0e94914e565c1dcc1ee6860

Konni

4c2016df6b546326d67ac2a79dea1343

URLs

- http://34.13.42[.]35/uploads/1.jpg
- http://34.13.42[.]35/uploads/2.jpg
- http://34.13.42[.]35/uploads/qwerty.jpg
- http://34.13.42[.]35/uploads/girl.jpg
- http://34.13.42[.]35/uploads/girllisten.jpg
- https://34.13.42[.]35/uploads/newmode.php
- http://acddesigns.com[.]au/demo/red/images/slider-pic-6.jpg
- http://kmbr1.nitesbr1[.]org/UserFiles/File/image/index.php
- http://kmbr1.nitesbr1[.]org/UserFiles/File/images.png
- http://www.stjohns-burscough[.]org/uploads/images.png
- http://lotusprintgroup[.]com/images.png
- https://planar-progress.000webhostapp[.]com/UserFiles/File/image/image/girl.jpg
- https://planar-progress.000webhostapp[.]com/userfiles/file/sliderpic.jpg
- http://www.jnts1532[.]cn/phpcms/templates/default/message/bottom.jpg
- http://www.rhooters[.]com/bbs/data/m_photo/bottom.jpg
- https://buttyfly.000webhostapp[.]com/userfiles/file/sliderpic.jpg

Domains and IPs

- buttyfly.000webhostapp[.]com
- planar-progress.000webhostapp[.]com
- 120.192.73[.]202
- 180.182.52[.]76