Reaver: Mapping Connections Between Disparate Chinese APT Groups

threatvector.cylance.com/en_us/home/reaver-mapping-connections-between-disparate-chinese-apt-groups.html

The Cylance Research and Intelligence Team

When the New York Times published a story in December based on a combination of hacked diplomatic cables belonging to the European Union, as well as sensitive information belonging to the United Nations, we, the BlackBerry Cylance Threat Intelligence team, took notice. It was hard not to given that it ran on the front page (Sanger, 2018)[1].

But the story caught our attention for other reasons too. It was based in large measure on a report titled *Phishing Diplomacy*, published by Area 1 on the same day (Area 1, 2018)[2]. The researchers attributed the compromise of the diplomatic cables and the targeting of over 100 additional organizations (including foreign and finance ministries, think-tanks and trade unions) to the Chinese government's Strategic Support Force (SSF), a Chinese military organization, without any explanation as to how they arrived at that attribution assessment.

Even more intriguing was the fact that, according to the Times report, Area 1 researchers provided the compromised cables to the newspaper. The Times quoted extensively from the cables – a move that raised eyebrows and prompted interesting legal and ethical questions for both Area 1 and the Times.

But legal and ethical questions aside, there was yet another reason why we took notice of this report. Included in the Area 1 "indicators of compromise" (IoCs) was a single website/domain name they said the Chinese SSF used for Command-and-Control (C2) in both targeted attacks.

As we will demonstrate in greater detail below, we connected this domain to a host of other, disparate Chinese APT groups whose tasking, targeting, and toolsets have been literally all over the map. We also found evidence suggesting that different Chinese APT groups have also been using the same malware - and in some cases, the same exploit builder.

Analysis

The attribution of forensic artifacts to specific threat actors, at whatever level, is an evolving, dynamic process - not a static one. Yet, much of the public research that originally defined the "known APT groups" appears to be frozen in time.

When private security companies began declaring APT groups and minting an alphabet soup of threat actors bearing nicknames with numbers, animals, elements, demons and gods, they sketched profiles of nation states and their proxies by invoking the intelligence-version of a signature.

Pictures emerged that reflected a particular group's choice of tactics, techniques and attack procedures – the so-called TTPs that shape the way we tend to think about Iranian, Chinese, Russian and North Korean threats. This alphabet soup of nicknames engendered consequences not just for risk management at the enterprise level, but for national security policy as well.

Many of these profiles were sketched nearly a decade ago; however, attribution is as much a function of a given window of technical evidence as it is a function of a given window of time.

In the case of the forensic artifacts Area 1 associated with China's SSF, evidence of shared or overlapping tools by Chinese groups once thought to operate separately or to employ separate targeting suggests one of several potential developments:

- It could indicate that Chinese government groups are expanding their reach beyond traditional boundaries or have been given different tasking/targeting
- It could indicate the Chinese government cyber effort has matured enough such that different groups – even at different agencies – are now comfortable sharing tools and infrastructure
- It could indicate that the Chinese have developed some method of centralizing the activity of disparate government units for the purposes of coordinating technical access outside of China

Knowing which assessment is correct is probably of more interest to governments than it is to targeted organizations. Of course, every attack by a suspected state actor holds significance for both groups. There are always tactical considerations for the target, and there are often national security considerations for governments, policy makers, and those of us trying to understand the behavior of nation states in cyberspace.

Still, evidence of a shifting profile of Chinese APT groups offers a lesson for network defenders, as it impacts the threat modeling and risk assessment of organizations who have positioned themselves based on:

1. A dated understanding of these groups and their preferred targets, or
2. An explicit reliance on "indicators of compromise," or
3. Both.

What follows is discussion of our findings, detailing the crossover in malware and C2 infrastructure. Some, though not all, of these findings were arrived at independently by Anomali Labs, who published them last month (Anomali Labs, 2019)[3]. Anomali did not, for example, make the connection to the Area 1 research. And while our findings regarding some of the malware and infrastructure crossover support those of Anomali, we do not share their conclusion that the crossover portends supply chains or "quartermasters" shared between strategic rivals China and India.

Discussion

The Area 1 *Phishing Diplomacy* report that enabled the Times story attributed the attacks on the European Union and other related targets to China's Strategic Support Force. The SSF was modeled on America's Cyber Command (CYBERCOM), a blended unit that was initially part of Strategic Command (STRATCOM) before being stood up as its own combatant command.

The SSF was created in 2015 following a reorganization of several disparate Chinese military units responsible for space operations, electronic warfare, information operations, psychological operations, espionage, technical reconnaissance, and network warfare. Included in the reorganization was the Third Department of the People's Liberation Army (PLA), members of which were famously called out by the U.S. Justice Department as the threat actors behind the "APT 1" persona.

But while China's Third Department has been traditionally focused on external operations, typically in support of military objectives, we found a connection via the infrastructure included in the Area 1 report to groups associated in other security research with Chinese government efforts to spy on and conduct operations against internal groups perceived as separatist or threatening to the government – a task normally left either to the (relatively new) National Security Commission by way of the operations of the state police or, by extension, the Ministry of State Security.

The Ministry of State Security is a Chinese civilian federal agency thought to be comprised of a combination of foreign intelligence and domestic intelligence services – sort of a combination of the CIA and FBI, if thought of in American terms.

The MSS has recently been the target of the U.S. Justice Department, which named the group (and publicly associated it with APT10 / a.k.a. "menuPass") in a couple of recent indictments (U.S. vs. Zhang Zhang-Gui et al, 2018)[4] (U.S. vs. Zhu Hua et al, 2018)[5] [indictment numbers 13CR3132-H and 18CRM891, respectively]. The MSS was also named by the U.S.-China Economic and Security Review Commission as the actor "widely believed" to be "either responsible for, or the ultimate benefactor of, the OPM breach" (USCC, 2016)[6].

Chief among China's domestic security concerns, and presumably targets of the MSS, have been groups known informally as the Five Poisons.

The name is a reference to five groups whose ideological, religious, or cultural differences have either directly challenged the ruling party structure or have put them at odds with the government's singular "One China" concept of its national identity. Traditionally, the Five Poisons has referred to:

- Members of the Muslim minority of ethnic Uyghurs
- Followers of Falun Gong
- Supporters of Taiwanese independence
- Tibetans
- Activists in support of democracy in China

Operations targeting these groups have often employed the use of a malware family identified by Palo Alto Networks as "Reaver" (Miller-Osborn, 2017)[7]. Palo Alto also associated Reaver with related malware known by the names SUTR and SunOrcal in campaigns targeting the Taiwanese presidential election, as researched by PWC (Yip, 2016)[8], and the Five Poisons more broadly as reported by Citizen Lab (Hardy, 2013)[9]. We found even newer variants and other as-yet unnamed samples as we started to dive in further.

Whether Reaver, and its predecessors, are tools wielded by Chinese groups focused internally on separatist movements, or by a division of the Chinese Army re-tasked to serve the same mission, is unknown. However, it is clear that the group behind Reaver used some of the same infrastructure as the group behind the Area 1 attacks on the European Union and United Nations (ostensibly, the military SSF).

In its *Phishing Diplomacy* report, Area 1 published a single C2 domain, *updates.organiccrap[.]com*, which previously resolved to the IP address *50.117.96[.]147* between November 16, 2017 and July 27, 2018, a period of roughly eight months.

Exactly one day before that "organiccrap" domain began resolving to that IP address, another domain was resolving to it, for a narrow period of two weeks (October 31, 2017 – November 15, 2017). That domain, *tashdqdxp[.]com*, was included in the Palo Alto research, where they indicated that it was used in conjunction with Reaver.

We found that several additional, recent Reaver C2 domains also resolved to this IP address including *etwefsfj[.]com, sfafgeht[.]com, and asdasfdsre[.]com.* The earliest resolution occurred on May 1, 2018 and the latest on January 10, 2019.

As we mentioned above, Palo Alto had previously linked this Reaver domain and other Reaver samples via passive DNS to a number of SunOrcal domains. They include:

www.weryhstui[.]com, www.fyoutside[.]com, and www.olinaodi[.]com.

Palo Alto also linked the same SunOrcal activity set to a number of previous reports that shed light on apparent Chinese government targeting of Hong Kong activists, among others (Brooks, 2016)[10], (Wilson, 2016)[11].

The new Reaver variants we found appear to use a hybrid subset of new and old network infrastructure. We break them down in the following technical section, along with a description of a new backdoor we discovered along the way.

Technical Findings: Malware

Reaver.v4

The new 2018 Reaver samples continued to operate in a manner similar to what was first described by Palo Alto as "Reaver.v3 TCP Payload." The only real difference was in the encoding of the relative address string lookup table and configuration data.

XOR decoding was abandoned in favor of a custom cipher which used an incrementing right bit shift. Interestingly, this cipher also did a reverse lookup for values which had previously been computed. The decrypted table looked very similar to what was previously identified:

RA@10016=ADVAPI32.dll
RA@10017=GetUserNameA
[TRUNCATED]
RA@10313=ChangeServiceConfig2A
RA@10314=QueryServiceConfig2A

Figure 1: Decoded String Look Up Table

The configuration of the malware was also encoded similarly and contained all of the information previously described by Palo Alto -- with one additional string: a network callback domain, network port, beacon interval, a service name, service description, service display name, and now two hardcoded strings "n-0625" and "2017-tq-s":

```
00003552  00 00 00 00 50 00 00 00 10 27 00 00 01 00 00 00  ....P....'......
00003568  00 00 00 00 00 B7 04 00 77 77 77 2E 66 68 6A 73  .....·..www.fhjs
00003584  64 6B 6C 61 2E 63 6F 6D 00 00 00 00 00 00 00 00  dkla.com........
00003600  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00003696  00 00 00 00 00 00 00 00 6E 2D 30 36 32 35 00 00  ........n-0625..
00003712  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00003760  00 00 00 00 00 00 00 00 4E 74 6D 73 53 76 63 00  ........NtmsSvc.
00003776  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00003792  57 69 6E 64 6F 77 73 20 4D 75 6C 74 69 6D 65 64  Windows Multimed
00003808  69 61 20 53 65 72 76 69 63 65 20 66 6F 72 20 6D  ia Service for m
00003824  65 64 69 61 20 64 65 76 69 63 65 73 00 00 00 00  edia devices....
00003840  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00003888  57 69 6E 64 6F 77 73 20 4D 75 6C 74 69 6D 65 64  Windows Multimed
00003904  69 61 20 53 65 72 76 69 63 65 00 00 00 00 00 00  ia Service......
00003920  32 30 31 37 2D 74 71 2D 73 00 00 00 00 00 00 00  2017-tq-s.......
```

Figure 2: Decrypted Configuration Data

The network protocol remained largely unchanged from Palo Alto's report and will not be covered here, for the sake of brevity.

Sparkle Payload

During the investigation into the newer Reaver network infrastructure, we identified an entirely new type of backdoor deployed in very limited instances. BlackBerry Cylance named this payload "Sparkle" to shy away from the ominous military lexicon commonly "deployed" by the information security industry.

An associated dropper was also identified:

295c942389ebdbf8ff9a8b1a81d3f63cb60577fa57ecaa660ce347666973b4f3

The payload attempted to read data from the file *%Temp%\wsm56d1.tmp* and communicated to the domain *www.sfeeleyses[.]com* on TCP port 443.

Reaver.v4 Downloader

We identified a unique Reaver downloader during our analysis which was coincidentally the only sample which had a valid PE checksum. This binary would download an encoded payload from *hxxxp://www[.]htuditey[.]com/l-0424.bmp* and save it to a file named: *w90sD32rS3H2jP75.bmp*.

Once saved, the downloader would decode a regular executable dropper from it using an incrementing XOR routine starting with the value 0xFF at file offset 0x36.

This executable content would be written to disk as *%Temp%\mstk.exe*, and the downloader additionally created an associated Run key with it under the current user's registry hive to establish persistence. The following python snippet can be easily adapted for other keys as well:

```
def inc_xor(buf,start):
        out = ''
        key = int(start, 16)
```

```
    for i in buf:
        if key < 256:
            out += chr(ord(i) ^ key)
        else:
            key = 0
            out += chr(ord(i) ^ key)
        key +=1
    return out

inc_xor(binary_data, 'FF')
```

Figure 3: Python Incrementing XOR Routine

The downloader also contained a highly unique PDB path within it as well:

e:\VS2005 Project\Doc_Pack\DownloadSample\release\DownloadSample.pdb

The PDB path suggested that this downloader was likely only one part of a larger malicious document project.

Technical Findings: Exploit

Malicious Documents Delivering Reaver

After examining the new Reaver malware, we then turned our attention to the delivery method. What we found was an exploit document leveraging CVE-2017-11882:

9ac09ea38c9cf11ca13a2c3dbdcfbe0fe4a15cb609be451f7159ecebdd20d311

After analyzing this document, we were able to identify a handful of others leveraging the same exploit that took advantage of the "Package" ActiveX Control to drop a temporary file to *%AppData%\Local\Temp\8.*t.

This is a particularly interesting trick that first rose to popularity in 2014 and appears to have dropped off almost entirely. Simply opening an RTF document is enough to trigger the behavior if the ActiveX control is not disabled via:

HKLM\SOFTWARE\Microsoft\Office\Common\COM Compatibility\{F20DA720-C02F-11CE-927B-0800095AE340}

Upon closing the document, the temporary file will be removed. The native Windows program "Wordpad.exe" is also capable of triggering this same behavior regardless of the aforementioned registry key. (Li, 2014)[12].

In cases where the exploit was successfully triggered, it would launch some shellcode to decrypt and execute the content stored within "8.t". The shellcode within the document utilized a unique custom XOR cipher with a seed value of "0x7BF48E63" shown in python below:

```
def mixer(eax):
    ecx = eax
    ecx = ecx >> 0x1B
```

```
        ecx = ecx ^ eax
        ecx = ecx >> 3
        ecx = ecx ^ eax
        eax = eax + eax
        ecx = ecx & 1
        eax = eax | ecx
        return eax

def custom_loop(buf):
        eax = 0x7BF48E63
        out = ''
        for x in buf:
                edi = 7
                while edi !=0 :
                        eax = mixer(eax)
                        edi -=1
                xor_key = eax & 0xFF
                out += chr(ord(x)^xor_key)
        return out
```

Figure 4: Python Code to Decrypt Contents Stored in Package Object

We were able to locate two additional documents which operated in a similar fashion and retrieved encoded payloads from *www.htuditey[.]com*. We confirmed these documents to be directly related to the group behind the Reaver malware.

We also found several other documents which used the same executable encoding mechanism and seed value; however, these documents had previously been publicly attributed to “Gobelin Panda” (Sebdraven, 2018)[13] and dropped an entirely different payload named “Sisfader RAT” (Humphrey, 2018)[14].

Gobelin Panda, a.k.a. Goblin Panda, is a group that has been identified by CrowdStrike as a Chinese threat actor known to target defense, energy, and government organizations belonging to South Asian countries - especially Vietnam. CrowdStrike observed Goblin Panda activity spike as tensions among South China Sea nations has risen.

Though we are not able to determine whether Gob(e)lin Panda is associated with the MSS or the SSF, it is clear to us that the exploit builder used in the set of samples we have discussed above has been shared across multiple Chinese APT groups, including Leviathan, Temp.Periscope and Kryptonite Panda.

Anomali also published a comprehensive report on this series of exploit documents and termed the Reaver family “Temp.Trident” (Anomali Labs, 2019)[15]. *[Editor’s note: corrected on May 29, 2019]*.

Technical Findings: Infrastructure

All the domains we have identified in this report used random combinations of letters and were registered using the e-mail address *yuming[at]nuo.cn,* which seems to be a generic address for the hosting provider (www.nuo[.]cn).

This provider has a direct link to the Chinese group or groups using or sharing this infrastructure, going all the way back to 2013, where it was used to register the domain, *eyestouch256[.]com*. The following six domains were registered on November 15, 2017:

- etwefsfj[.]com
- sfafgeht[.]com
- strenthuy[.]com
- fhjsdkla[.]com
- htuditey[.]com
- xuitrdgt[.]com

As a reminder, that date marked the last day in which the *tashdqdxp[.]com* and associated IP was used in connection with Reaver (according to Palo Alto, which published that information five days later), and one day before Area 1 says the SFF started using the same IP address with a new domain for the attack on the European Union.

We found that six other domains were registered on two different earlier dates in 2017 and were likely not operationalized to quite the same extent. We have not listed them here since they were not relevant to this discussion.

Then, an additional two domains were registered on August 30, 2017:

- djstoern[.]com
- jorehkn[.]com

Four other domains were registered on May 9, 2017:

- menrotefit[.]com
- norejike[.]com
- poticxny[.]com
- qidaterstu[.]com

We strongly suspect yet another four other domains were registered by the group on July 31, 2018. However, they either have yet to resolve to any unique IP addresses or we have yet to identify any malware samples associated with them. Those domains are:

- asdasfdsre[.]com
- fdvvbnf[.]com
- hdjyrtuy[.]com
- kiggdssad[.]com

Conclusion

In this Threat Intelligence Bulletin, we've demonstrated how, after a close technical analysis of a set of tools and infrastructure used by several suspected Chinese state or state-sponsored actors over nearly a decade, we were able to establish and/or confirm connections between them – connections that provide insight into a dynamic set of actors whose targeting has changed dramatically over the years.

Interestingly enough, the change in targeting, perhaps a reflection of shared tools or tasking among Chinese military and civilian intelligence services, was presaged by our own research on this same subject six years ago.

In 2013, at a time when Citizen Lab and other research groups were issuing reports about the Chinese targeting of the Five Poisons, we published a technical blog on the use of essentially the same tools (later called Reaver) in use against U.S. automakers for espionage purposes (Gross, 2013)[16].

Findings of this nature should be of concern to enterprise administrators and network defenders in every vertical, not just those who see themselves within a threat model for the established Chinese state threat groups. That's because, as our analysis has shown, we assess that the Chinese threat groups are either sharing "Indicators of Compromise" or adopting the targets and tasking of other Chinese groups.

That means that if defenders are overly reliant on blacklisting indicators of compromise, or else making risk assessments based on what they perceive the interests of Chinese APT groups to be, they will remain vulnerable to an attacker who is changing both its tools and its targets.

To borrow an analogy from the health industry, defenders should make an effort to vaccinate themselves in hopes of preventing sickness, not just try to bar entry to everyone they know is sick.

Appendix

Hashes:

Reaver 2019 v.4 Backdoors

ff973e7c7a9d629011fb8c5bf766216e5e33da66656d9bf8386054fd8e99262a

126f2e4d6766d901ea0cb78b8cb4827be7d6aecea0c817eef6b572cb5b4e2442

1d7a3eaf48a19908f4f6cdffa596b4db1d5346b47958424b72e186af061367c6

Reaver 2018 v.4 Backdoors

363f7b8024efd8205ae8e74bfdc387b3a5aad8ff166cbc2475fad5d3a708dcb0

78b7b0253020edc80ea31eb60b42e47dec83b7cf41c952949c80b82679ece744

da9e1317ecc3cbceda45a838d954b8750d118ef1ce072b32c913819780fbb9b7

e1793859b3a3136c5d816fe7300303098847894241052820429a0584eed45ed1

Reaver 2019 v.4 Droppers

d6305a64d45e6443bf3bad2ccc4d2144f4632aec0ae1f3dedb1e526e1790770b

Reaver 2018 v.4 Droppers

738d5326c48fd81d147927d6e5d43933956e8f6a36f085b2130b780ccfc3fa86

538dd5cb32482a30a3676b328f275f37cbe16883a4368d3959b68e8f97fe70a1

b36464ea655330b993a5fc992ddb981f503bbeb4f7cb081d5da67f83a4b49049

7f5f294d96c3fb36499c9049cdb337e58f06fb8531b3eac796f8deaf88060ed2

15ab48aaaabd4462ac8ba5b511879a0f4502408a500b556078ca129fc92c2628

***Reaver Downloader*:**

44cda3eea271613ddfc820014c9fdd829c30ebbe57614e1a4dafaf76905301dc

9aab954f9fb84c82e588b2c90b1bb7eb2a65b08c739358a320d767650b6d9453

8971ac72939783d14d0ff0d4bebe1764b69e54a15627a149708f4253531a9df2

Reaver Exploit Documents:

1c6cb02ae9dceb3a647260f409dd837fa5c66794804623c9cf97395cf406d4df

3df19abbf961a6d795362f5408d65aa5a31e34620aa3518a010d4d6d9e79c60e

9ac09ea38c9cf11ca13a2c3dbdcfbe0fe4a15cb609be451f7159ecebdd20d311

Command & Control Infrastructure

Domains:

asdasfdsre[.]com

djstoern[.]com

etwefsfj[.]com

fdvvbnf[.]com

fhjsdkla[.]com

hdjyrtuy[.]com

htuditey[.]com

jorehkn[.]com

menrotefit[.]com

norejike[.]com

poticxny[.]com

qidaterstu[.]com

sfafgeht[.]com

strenthuy[.]com

xuitrdgt[.]com

IP Addresses:

103.226.153[.]235

103.234.99[.]74

103.36.54[.]119

103.61.137[.]210

104.160.190[.]2

104.160.191[.]10

104.224.141[.]75

107.161.80[.]56

142.252.252[.]241

182.16.118[.]91

204.44.65[.]128

208.77.43[.]76

210.56.51[.]66

45.121.48[.]12

45.121.50[.]19

45.121.50[.]5

50.117.38[.]74

50.117.47[.]129

50.117.96[.]147

64.32.22[.]151

67.229.134[.]170

67.229.159[.]218

67.229.168[.]2

67.229.28[.]82

74.121.151[.]158

Works Cited

[1] Sanger, D. a. (2018, December 18). *Hacked European Cables Reveal a World of Anxiety About Trump, Russia and Iran*. Retrieved from New York Times: https://www.nytimes.com/2018/12/18/us/politics/european-diplomats-cables-hacked.html

[2] Area 1. (2018, December 18). *Phishing Diplomacy*. Retrieved from Area 1 Security: https://cdn.area1security.com/reports/Area-1-Security-PhishingDiplomacy.pdf

[3] Anomali Labs. (2019, February 5). *Analyzing Digital Quartermasters in Asia – Do Chinese and Indian APTs Have a Shared Supply Chain?* Retrieved from Anomali Labs: https://www.anomali.com/blog/analyzing-digital-quartermasters-in-asia-do-chinese-and-indian-apts-have-a-shared-supply-chain

[4] U.S. vs. Zhang Zhang-Gui et al, 13CR3132-H (U.S. District Court, Southern District of California October 30, 2018).

[5] U.S. vs. Zhu Hua et al, 18CRM891 (United States District Court, Southern District of New York December 17, 2018).

[6] USCC. (2016, June 9). *China's Intelligence Services and Espionage Operations*. Retrieved from U.S.-China Economic and Security Review Commission: https://www.uscc.gov/sites/default/files/transcripts/June%2009%2C%202016%20Hearing%20Transcript.pdf

[7] Miller-Osborn, J. G. (2017, November 10). *New Malware with Ties to SunOrcal Discovered*. Retrieved from Palo Alto Unit42: https://researchcenter.paloaltonetworks.com/2017/11/unit42-new-malware-with-ties-to-sunorcal-discovered/.

[8] Yip, M. (2016, March 17). *Taiwan Presidential Election: A Case Study on Thematic Targeting*. Retrieved from PWC Blog: https://pwc.blogs.com/cyber_security_updates/2016/03/taiwant-election-targetting.html

[9] Hardy, K. K. (2013, August 2). *SURTR Malware Family Targeting the Tibetan Community*. Retrieved from The Citizen Lab: https://citizenlab.ca/2013/08/surtr-malware-family-targeting-the-tibetan-community/

[10] Brooks, M. e. (2016, April 18). *Between Hong Kong and Burma*. Retrieved from Citizen Lab: https://citizenlab.ca/2016/04/between-hong-kong-and-burma/

[11] Wilson, C. (2016, April 13). *The Four Element Sword Engagement*. Retrieved from Arbor ASERT: https://asert.arbornetworks.com/wp-content/uploads/2016/04/ASERT-Threat-Intelligence-Report-2016-03-The-Four-Element-Sword-Engagement.pdf

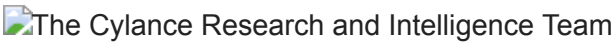
[12] Li, H. (2014, July 28). *Dropping Files into Temp Folder Raises Security Concerns*. Retrieved from Securing Tomorrow - Mcafee: https://securingtomorrow.mcafee.com/mcafee-labs/dropping-files-temp-folder-raises-security-concerns/

[13] Sebdraven. (2018, August 2). *Goblin Panda against the Bears*. Retrieved from Medium: https://medium.com/@Sebdraven/gobelin-panda-against-the-bears-1f462d00e3a4

[14] Humphrey, B. (2018, June 12). *CVE-2017-8570 RTF and the Sisfader RAT*. Retrieved from NCC Group: https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/june/cve-2017-8570-rtf-and-the-sisfader-rat/

[15] Anomali Labs. (2019, February 5). *Analyzing Digital Quartermasters in Asia – Do Chinese and Indian APTs Have a Shared Supply Chain?* Retrieved from Anomali Labs: https://www.anomali.com/blog/analyzing-digital-quartermasters-in-asia-do-chinese-and-indian-apts-have-a-shared-supply-chain

[16] Gross, J. (2013, November 20). *Grand Theft Auto Panda*. Retrieved from Cylance Threat Vector: https://threatvector.cylance.com/en_us/home/grand-theft-auto-panda.html



About The Cylance Research and Intelligence Team

Exploring the boundaries of the information security field

The Cylance Research and Intelligence team explores the boundaries of the information security field identifying emerging threats and remaining at the forefront of attacks. With insights gained from these endeavors, Cylance stays ahead of the threats.