Analyzing Digital Quartermasters in Asia – Do Chinese and Indian APTs Have a Shared Supply Chain?

anomali.com/blog/analyzing-digital-quartermasters-in-asia-do-chinese-and-indian-apts-have-a-shared-supply-chain

Anomali Labs recently analyzed a large number of weaponized RTF phishing files related to APT groups aligned with Chinese and Indian state interests. This analysis has identified a shared object dimension and shared obfuscation methods across weaponized RTF files utilized by the APT groups known as Sidewinder (Indian State Interests), Goblin Panda/Conimes (Chinese State Interests), Temp.Periscope/ APT40 / Leviathan (Chinese State Interests), and Temp.Trident / Dagger Panda & Nomad Panda / Icefog (Chinese State Interests). Both unique object dimensions and multiple shared obfuscation methods are visible in the RTF files which appear to be artifacts of a shared RTF phishing weaponizer. In addition to shared RTF properties, a distinct pattern of post-exploitation TTP's is shared between the APT groups aligned with China, whereas a unique post-exploitation execution chain can be seen in Sidewinder APT campaigns. The use of a common RTF phishing weaponizer alongside distinct post-exploitation TTPs introduces the possibility that Chinese and Indian APTs may have an overlapping supply chain for the acquisition of exploits and phishing weaponizers. However, after these tools are acquired a distinct and complex network of APT digital quartermasters may determine how these tools are equipped with payloads and deployed in distinct operations.

Using Object Dimensions to Track RTF Phishing Weaponizers

RTF files are among the most popular file formats used in phishing attacks today. To create a weaponized RTF file capable of exploiting a common vulnerability exploit ("CVE"), RTF weaponizers are often used which consist of a script that injects a malicious RTF object into a pre-crafted RTF phishing document. The resulting weaponized exploit file can then be attached to a phishing email and sent to a victim. When RTF weaponizers are acquired or purchased, it is common for operators to change aspects of the weaponizer payload which occurs after initial CVE exploitation. However, it is less common for operators to change the object header and dimensions within the RTF Weaponizer, resulting in shared unique object dimensions across weaponized exploits created by adversaries. Object dimensions are represented in the RTF strings as "\objhN" for height and "\objwN" for width. Analysts can identify related samples with matching unique object dimensions by hunting for samples with object dimensions sharing these properties.

\objh*N*	***N*** is the original object height in twips, assuming the object has a graphical representation.
\objw*N*	***N*** is the original object width in twips, assuming the object has a graphical representation.

RTF 1.14 Specification

```
ASCII Strings:
======================
\object\objupdate\objemb\objw2180\objh300
\objdata 554567
\objdata 1389E61402000000B00000045717561746 96F6E2E330000000000000000000260000D
01\'cdCF11E0A1B11AE1000000000000000000000000000000000000003E000300FEFF090006000000000000000000000001000000010000000000000000
\0
0000000000000048905D006C9C5B000000000066FE01DABC0A01112
\yxe15478  \32
\object
2\'cd\'cd3
\pnaiud 7f8a
80000B9346F1D8AB808D2588A31C18B098B491483C140FFE13765303739613235323466613633613535666263666659B1545000000E97408000055
```

Anomali Labs identified a unique object dimension present in RTF phishing files weaponized with CVE-2017-11882 and CVE-2018-0802 which appear to be utilized by numerous Asian APT groups. The identified RTFs all share a unique object height and width, which determine how the object will be rendered in Microsoft Word. Specifically the object dimensions "objw2180\objh300" are present in the RTF files and have been observed in phishing files linked to the APT groups Sidewinder, Goblin Panda, Temp.Periscope, and Temp.Trident.

Additionally, object data present in the RTF files were shared between a number of samples utilized by these groups. There are multiple RTF obfuscation strings constant among these samples which is a byproduct of the obfuscation utilized by the RTF Weaponizer. This shared obfuscation output enforces the likelihood of this phishing weaponizer being utilized by multiple actors and possibly originating from an overlapping supply chain.

It is worth noting that similarities between Sidewinder and Goblin Panda RTFs have historically been identified by security researchers[1]. Additionally, the VietTimes in August 2018 wrote of a targeted attack against a number of Vietnamese State Agencies in Da Nang, Vietnam that were identified during an investigation into Sidewinder APT activity. This activity was later attributed to the Goblin Panda / Conimes group[2].

Distinct Execution Techniques

Despite all identified APT samples sharing unique RTF object dimensions and obfuscation methods, two distinct methods covered at length below for executing payloads were found. The Sidewinder APT downloads and executes a payload via an HTA file and the three clusters of Chinese APT activity drop shellcode via an OLE package which pulls down a source file for payload execution.

The Sidewinder APT has historically targeted organizations linked to the Pakistani Military and is believed by security researchers to be an actor associated with Indian espionage interests possibly operating as a contractor in the space. Sidewinder has conducted campaigns targeting Windows and Android-based systems. Their use of weaponized RTF files with unique object dimensions in phishing campaigns rely on the successful exploitation of CVE-2017-11882 in which the opened RTF file downloads and executes HTA files on the victim's machine[3]. Primarily English language phishing files that invoke topics involving the military borders of India, China, and Pakistan are weaponized and require execution by the victim to pull down additional files including a malicious .hta. Once the .hta has been downloaded from a C2 domain and executed, the powershell payload contained in the .hta file can then be executed on a victim's system[4].

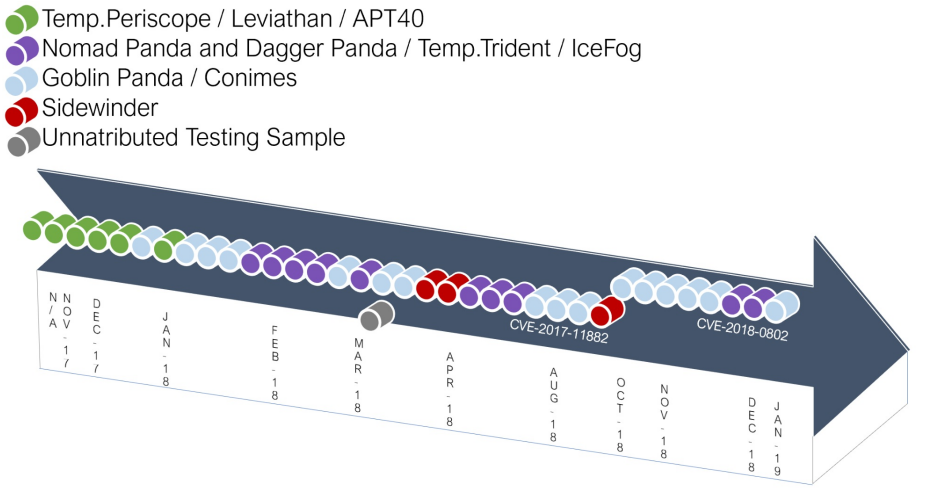
Alternatively, three distinct clusters of Chinese APT activity have been observed utilizing these RTF files sharing unique object dimensions. Goblin Panda / Conimes has historically targeted Vietnam utilizing RTF phishing attachments delivering a payload identified as "QCRat"[5]. Temp.Periscope / APT40 / Leviathan has historically targeted U.S. and international institutions associated with naval and maritime issues affecting the South China Sea while supporting the theft of intellectual property[6]. Temp.Trident / Dagger Panda & Nomad Panda / Icefog have historically targeted the Mongolia region (Dagger Panda) alongside Russian and Central Asia (Nomad Panda) likely as part of economic espionage efforts in support of the Belt and Road Initiative[7]. Versions of the custom payload Fucobha have been identified as part of these campaigns, which was first identified in 2013[8]. In addition to these distinct APTs using a common RTF weaponizer, they share a common post-exploitation execution technique. Rather than downloading and executing a malicious file, the RTF document drops and executes shellcode via an OLE package that then drops a distinctive source file to execute a payload. This method has been identified earlier by security analysts[9]. Anomali Labs identified the presence of the unique object dimension "objw871\\objh811\\objscalex8\\objscaley8" in RTF files involved with this post-exploitation method. This object dimension can be used to identify multiple malicious RTF files attributed to Chinese APT groups. The presence of both a shared phishing weaponizer and a shared post-exploitation execution technique between these groups is indicative of a noteworthy tool and TTP overlap. This overlap indicates that these APT groups may be part of a shared supply chain which receives tools for phishing exploitation from a shared Digital Quartermaster.

Actor	Targeting	Potential Motivation	Methodology	Unique Tools
Goblin Panda a.k.a. Conimes	Vietnam and Southeast Asia	Espionage aligned with commercial and South China Sea issues	RTF Phishing followed by shellcode executed via an OLE package dropping distinctive source file	QCRat Payload
Temp.Periscope a.k.a APT40 a.k.a Leviathan	U.S. Defense; Maritime; Academic Institutions; International & Political organizations	Intellectual property theft and military espionage	RTF Phishing followed by shellcode executed via an OLE package dropping distinctive source file	DADBOD EVILTECH AIRBREAK HOMEFRY MURKYTOP
Nomad Panda & Dagger Panda a.k.a Temp.Trident a.k.a.Icefog	Mongolia and Central Asia	Economic espionage for Belt & Road Initiative	RTF Phishing followed by shellcode executed via an OLE package dropping distinctive source file	Fucobha Payload

Timeline of Activity - Temporal Indicators

The earliest public sample (c92a26c42c5fe40bd343ee94f5022e05647876daa9b9d76a4eeb8a89b7f7103d) of a CVE-2017-11882 RTF exploit document matching these identified object dimensions and using the Chinese post-exploitation execution technique contains a last modified date of November 18, 2017. Two samples attributed to Temp.Periscope contain last modified dates from 2007 that appear to be manipulated and therefore cannot be accurately dated based on this information. The first identified RTF samples can be attributed to Temp.Periscope with Goblin Panda later beginning to utilize these RTF files in phishing campaigns circa January 2018. Temp.Trident appears to have begun using these RTF files in late February 2018 based on publicly available samples. Notably the Sidewinder APT RTF phishing samples were observed in the wild subsequent to use by Chinese APT groups with samples not observed until April 4, 2018 based on last modified dates of public samples. Most recently a sample was identified in October 2018.

While CVE-2017-11882 was the primary RTF exploit observed between November 2017 and September 2018, a shift in TTPs was observed with an updated weaponizer targeting CVE-2018-0802. Subsequent to October 23, 2018. RTF phishing files attributed to Chinese APT groups and containing these unique object dimensions shifted their TTPs to target this new CVE. The targeted vulnerability is highly similar to CVE-2017-11882 and proof of concepts have been released which effectively target both vulnerabilities with minimal changes to the exploit code. No Sidewinder APT samples targeting CVE-2018-0802 were publicly identified at the time of analysis.



Conclusion: Are Exploits Being Traded from the Royal Road or Imperial Highway?

The presence of unique RTF object dimensions, object data strings indicative of shared obfuscation methods, and shared post-exploitation TTP's amongst Chinese APT groups indicate that a shared RTF phishing weaponizer may be in use by multiple adversaries in the APAC region. The constancy of the object dimensions and object data across APT groups, despite weaponzier updates targeting new CVE's, reinforces the shared nature of this tool. The distribution of a shared weaponizer for phishing is consistent with historic reporting regarding the Goblin Panda APT that previously utilized a shared phishing weaponizer for CVE-2012-0158. Additionally, the practice of utilizing a shared Digital Quartermaster and phishing builder was previously observed across Chinese APT campaigns unrelated to these actors as early as 2013. This provides a historic precedent for tool sharing of this kind[10]. The shared post-exploitation methods used by Temp.Periscope, Temp.Trident, and Goblin Panda, when examined in context of this shared RTF phishing weaponizer, supports a conclusion that these APTs may share a common supply chain and Digital Quartermaster.

Alternatively, analysis indicating this RTF phishing weaponizer overlaps with the otherwise unrelated Sidewinder APT campaigns raises a larger question about tool acquisition by APTs in the APAC region. Although not confirmed at this time, this occurrence could indicate that Indian & Chinese APT groups are using an overlapping supply chain for exploits. Similar supply chains have been known to consist of an ecosystem of underground exploit brokers and weaponizer developers providing tools to an exclusive list of clientele. However, despite the apparent overlap, this analysis has not determined if this RTF weaponizer originated in India, in China, or elsewhere. Publicly observed samples indicate that tool adoption was first seen by the Chinese group Temp.Periscope, with Goblin Panda, and Temp.Trident following suit prior to usage by the Sidewinder APT. While it is possible that this temporal adoption may indicate context about the weaponizer's origin, unlike the ancient trading roads that have historically connected India and China, the current exchange of offensive cyber tools remains opaque. Further research is necessary at this time to substantiate the possibility of an active shared APT supply chain in the APAC region.

Anomali Labs has developed the following Yara signatures that can be used to identify RTF samples containing the object dimensions consistent with APT phishing activity:

YARA RULES

```
rule RTF_weaponizer_objh300

{
meta:
    author        = "Anomali"
    tlp           = "GREEN"
    version       = "1.0"
    date          = "2018-11-13"
    hash          = "9d0c4ec62abe79e754eaa2fd7696f98441bc783781d8656065cddfae3dbf503e"
    Bulletin        = "https://ui.threatstream.com/tip/262672/"
    description   = "Rule to detect Malicious RTF based on object dimension "

strings:

$S1= "objw2180\\objh300"
$RTF= "{\\rt"

condition:

$RTF at 0 and $S1
}
```

```
rule  RTF_Malicous_Object

{
meta:
    author  = "Anomali"
    tlp           = "GREEN"
    version       = "1.0"
    date          = "2018-11-13"
    hash          = "9d0c4ec62abe79e754eaa2fd7696f98441bc783781d8656065cddfae3dbf503e"
    Bulletin        = "https://ui.threatstream.com/tip/262672/"
    description   = "Rule to detect Malicious RTF based on object dimension "

strings:

$S1= "objw871\\objh811\\objscalex8\\objscaley8"
$RTF= "{\\rt"

condition:

$RTF at 0 and $S1
}
```

Hash	Actor	CVE Exploit	RTF Object Contents	Modify Date
c0b8d15cd0f3f3c5a40ba2e9780f0dd1db526233b40a449826b6a7c92d31f8d9	Temp.Periscope	CVE-2017-11882 V1	objw2180\objh300{*\objclass Equation.3} {*\objdata 010500000200000000B0000004571756174	2007:01:30 09:12:00
c63ccc5c08c3863d7eb330b69f96c1bcf1e031201721754132a4c4d0baff36f8	Temp.Periscope	CVE-2017-11882 V1	objw2180\objh300{*\objclass Equation.3} {*\objdata 010500000200000000B0000004571756174	2007:01:30 09:12:00
c92a26c42c5fe40bd343ee94f5022e05647876daa9b9d76a4eeb8a89b7f7103d	Temp.Periscope	CVE-2017-11882 V1	objw2180\objh300{*\objclass Equation.3} {*\objdata 010500000200000000B0000004571756174	2017-11-18 21:52:00'
c67625e2b5e2f01b74e854c0c1fdf0b3b4733885475fe35b80a5f4bca13eccc7	Temp.Periscope	CVE-2017-11882 V1	objw2180\objh300{*\objclass Equation.3} {*\objdata 010500000200000000B0000004571756174	2017:12:08 00:50:00
138d62f8ee7e4902ad23fe81e72a1f3b7ac860d3c1fd5889ed8b8236b51ba64b	Temp.Periscope	CVE-2017-11882 V1	objw2180\objh300{*\objclass Equation.3} {*\objdata 010500000200000000B0000004571756174	2017:12:08 06:29:00
941868f366d65c8859253c869e405c5bbb91e1ed0227090656295c54bb0be9f2	Conimes/Goblin Panda	CVE-2017-11882 V1	objw2180\objh300{*\objclass Equation.3} {*\objdata 010500000200000000B0000004571756174	2018:01:10 09:47:00
9d0c4ec62abe79e754eaa2fd7696f98441bc783781d8656065cddfae3dbf503e	Temp.Periscope	CVE-2017-11882 V1	objw2180\objh300{*\objclass Equation.3} {*\objdata 010500000200000000B0000004571756174	2018:01:15 14:47:00
332aa26d719a20f3a26b2b00a9ca5d2e090b33f5070b057f4950d4f088201ab9	Conimes/Goblin Panda	CVE-2017-11882 V1	objw2180\objh300{*\objclass Equation.3} {*\objdata 010500000200000000B0000004571756174	2018:01:16 11:32:00
bd1e7b42a9c265266b8cc5cc966470497c4f9cba2b247d1f036b6b3892106b52	Conimes/Goblin Panda	CVE-2017-11882 V1	objw2180\objh300{*\objclass Equation.3} {*\objdata 010500000200000000B0000004571756174	2018:01:17 09:09:00
8f81142a9482c2a96c43c4b325f90794c2a32b61e8261da55f306a36df9ec18c	Conimes/Goblin Panda	CVE-2017-11882 V1	objw2180\objh300{*\objclass Equation.3} {*\objdata 010500000200000000B0000004571756174	2018:01:31 11:24:00
f5365387320ae6e6907fd2700f340ba8712cb08f7e52b2ec4dccfe99b3d648ef	Temp.Trident	CVE-2017-11882 V2	objw2180\objh300{\objdata 554567{*\objdata 010500000200000000B000000457175617 4696F6E2E	2018:02:22 20:08:00
9d239ddd4c925d14e00b5a95827e9191bfda7d59858f141f6f5dcc52329838f0	Temp.Trident	CVE-2017-11882 V2	objw2180\objh300{\objdata 554567{*\objdata 010500000200000000B000000457175617 4696F6E2E	2018:02:22 20:08:00
a95bbc1f067783c1107566ed7897549f6504d5367b8282efe6f06dc31414c314	Temp.Trident	CVE-2017-11882 V2	objw2180\objh300{\objdata 554567{*\objdata 010500000200000000B000000457175617 4696F6E2E	2018:02:22 20:08:00

4e1a2f731688f9aab80b1f55d9101bb1cddec08214d4379621c434899a01efbf	Temp.Trident	CVE-2017-11882 V2	objw2180\objh300{\objdata 554567{*\objdata 01050000020000000B0000004571756174696F6E2E	2018:02:22 20:08:00
b70069e1c8e829bfd7090ba3dfbf0e256fc7dfcefc6acafb3b53abcf2caa2253	Conimes/Goblin Panda	CVE-2017-11882 V2	objw2180\objh300{\objdata 554567{*\objdata 01050000020000000B0000004571756174696F6E2E	2018:03:07 11:22:00
597c0c6f397eefb06155abdf5aa9a7476c977c44ef8bd9575b01359e96273486	Temp.Trident	CVE-2017-11882 V2	objw2180\objh300{\objdata 554567{*\objdata 01050000020000000B0000004571756174696F6E2E	2018:03:14 17:34:00
dd89d33e275e99e288e4c50bdafbb4584a9565189491af0a66f8a506eaf53859	Conimes/Goblin Panda	CVE-2017-11882 V2	objw2180\objh300{\objdata 554567{*\objdata 01050000020000000B0000004571756174696F6E2E	2018:03:27 09:30:00
42162c495e835cdf28670661a53d47d12255d9c791c1c5653673b25fb587ffed	Conimes/Goblin Panda	CVE-2017-11882 V2	objw2180\objh300{\objdata 554567{*\objdata 01050000020000000B0000004571756174696F6E2E	2018:03:27 09:30:00
892859ea9d86fc441b24222148db52eb33cd106c2ac68eafbe83ab0064215488	Sidewinder APT	CVE-2017-11882	objw2180\objh300{\objdata 554567{{*\objdata 1389E614020000000B0000004571756174696F6E2	2018:04:04 08:54:00'
22062b6bcda194e3734285fed6b2de341c694c52a8f60c9f389f880cefab7644	Sidewinder APT	CVE-2017-11882	objw2180\objh300{\objdata 554567{{*\objdata 1389E614020000000B0000004571756174696F6E2	2018:04:05 10:32:00
71c94bb0944eb59cb79726b20177fb2cd84bf9b4d33b0efbe9aed58bb2b43e9c	Temp.Trident	CVE-2017-11882 V2	objw2180\objh300{\objdata 554567{*\objdata 01050000020000000B0000004571756174696F6E2E	2018:04:22 11:39:00
722e5d3dcc8945f69135dc381a15b5cad9723cd11f7ea20991a3ab867d9428c7	Temp.Trident	CVE-2017-11882 V2	objw2180\objh300{\objdata 554567{*\objdata 01050000020000000B0000004571756174696F6E2E	2018:04:22 11:40:00
c580d77722d85238ed76689a17b0205b4d980c010bef9616b8611ffba21b142e	Temp.Trident	CVE-2017-11882 V2	objw2180\objh300{\objdata 554567{*\objdata 01050000020000000B0000004571756174696F6E2E	2018:04:23 01:01:00
c374f7f30b34d95dd99d9cf16f54192d439f830918d342558945e5809809b847	Conimes/Goblin Panda	CVE-2017-11882 V2	objw2180\objh300{\objdata 554567{*\objdata 01050000020000000B0000004571756174696F6E2E	2018:08:19 18:12:00
344fbc5e86e6477cdb24848ace149303e22b41f7b01b2eca923109868c1f458f	Conimes/Goblin Panda	CVE-2017-11882 V2	objw2180\objh300{\objdata 554567{*\objdata 01050000020000000B0000004571756174696F6E2E	2018:08:23 08:28:00
46714a1fd1a5ce598f761a885857dee8d90b6e7d6f4a303ecaec246a77b58fff	Conimes/Goblin Panda	CVE-2017-11882 V2	objw2180\objh300{\objdata 554567{*\objdata 01050000020000000B0000004571756174696F6E2E	2018:08:23 08:28:00
b45087ad4f7d84758046e9d6eb174530fee98b069105a78f124cbde1ecfb0415	Conimes/Goblin Panda	CVE-2018-0802	objw2180\objh300{\objdata 554567{*\objdata 01050000020000000b0000004571756174696f6e2	2018:10:23 09:08:00
44e564ab86be5be2ce5f31c9072cd05adb91663be4904759cbcafa30c5b87660	Conimes/Goblin Panda	CVE-2018-0802	objw2180\objh300{\objdata 554567{*\objdata 01050000020000000b0000004571756174696f6e2	2018:10:29 15:42:00
ab35b2b22718624fcaf1a290b3f138c009469b7449d1a280ec67767ea55b44ae	Conimes/Goblin Panda (NO QCrat)	CVE-2018-0802	objw2180\objh300{\objdata 554567{*\objdata 01050000020000000b0000004571756174696f6e2	2018:11:28 09:56:00
130daacff74d57bb2319fc5cf815e783c6505883f69e4adcd4c2b1cac3e598ce	Conimes/Goblin Panda	CVE-2018-0802	objw2180\objh300{\objdata 554567{*\objdata 01050000020000000b0000004571756174696f6e2	2018:12:11 10:43:00
c6a01f392e4c317e6c9b6b3ce860f6368fad7687336ce995246d01fb52b83ca4	Conimes/Goblin Panda	CVE-2018-0802	objw2180\objh300{\objdata 554567{*\objdata 01050000020000000b0000004571756174696f6e2	2018:12:14 09:22:00
9be6d671dd901326fc834296fbd2ed015d64e6037e83d8d1d08a9dcdc107cb33	Temp.Trident	CVE-2018-0802	objw2180\objh300{\objdata 554567{*\objdata 01050000020000000b0000004571756174696f6e2	2018:12:19 04:37:00
5898e729b7305c4e5db54847396b15d06b74153213a242d295cf64c951a021ca	Temp.Trident	CVE-2018-0802	objw2180\objh300{\objdata 554567{*\objdata 01050000020000000b0000004571756174696f6e2	2018:12:19 13:54:00

9001056791a03ec998f26805d462bc2ca336b2c3aeac2e210f73ff841dfe3eec	Sidewinder APT	CVE-2017-11882	\objdata 554567{{*\objdata 1389E6140200000000B000000457175617469 6F6E2	N/A
226aff8ae77d224e696bf77f97508152df26ecf5	Test Sample that Runs Calc	CVE-2017-11882 V1	*\objclass Equation.3}{*\objdata 010500000200000000b0000004571756174	2018-03-20 02:38:36'
81f75839e6193212d71d771edea62430111482177cdc481f4688d82cd8a5fed6	Conimes/Goblin Panda	CVE-2018-0802	objw2180\objh300{\objdata 554567{*\objdata 010500000200000000b000000457175617469 6f6e2	2019:01:18 09:26:00'

[1] https://medium.com/@Sebdraven/malicious-document-targets-vietnamese-officials-acb3b9d8b80a

[2] https://viettimes.vn/nhom-hacker-trung-quoc-dung-sau-cuoc-tan-cong-co-chu-dich-vao-da-nang-300128.html

[3] https://medium.com/@Sebdraven/apt-sidewinder-changes-theirs-ttps-to-install-their-backdoor-f92604a2739

[4] https://s.tencent.com/research/report/479.html; https://brica.de/alerts/alert/public/1221860/apt-sidewinder-tricks-powershell-anti-forensics-and-execution-side-loading/; https://medium.com/@Sebdraven/apt-sidewinder-tricks-powershell-anti-forensics-and-execution-side-loading-5bc1a7e7c84c

[5] https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-august-goblin-panda/

[6] https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html

[7] https://medium.com/@Sebdraven/goblin-panda-changes-the-dropper-and-reused-the-old-infrastructure-a35915f3e37a - Nomad Panda / Temp.Trident Samples

[8] https://media.kaspersky.com/en/icefog-apt-threat.pdf

[9] https://medium.com/@Sebdraven/gobelin-panda-against-the-bears-1f462d00e3a4

[10] https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-malware-supply-chain.pdf

About the Author

Anomali Labs