Chinese APT Uses Poison Ivy Malware to Target Government | Proofpoint US

By Michael Raggi and Dennis Schwarz with the Proofpoint Threat Insight Team

Published: 2019-07-23 · Archived: 2026-04-05 13:47:43 UTC

Overview

Proofpoint researchers have identified a targeted APT campaign that utilized malicious RTF documents to deliver custom malware to unsuspecting victims. We dubbed this campaign “Operation LagTime IT” based on entities that were targeted and the distinctive domains registered to C&C IP infrastructure.

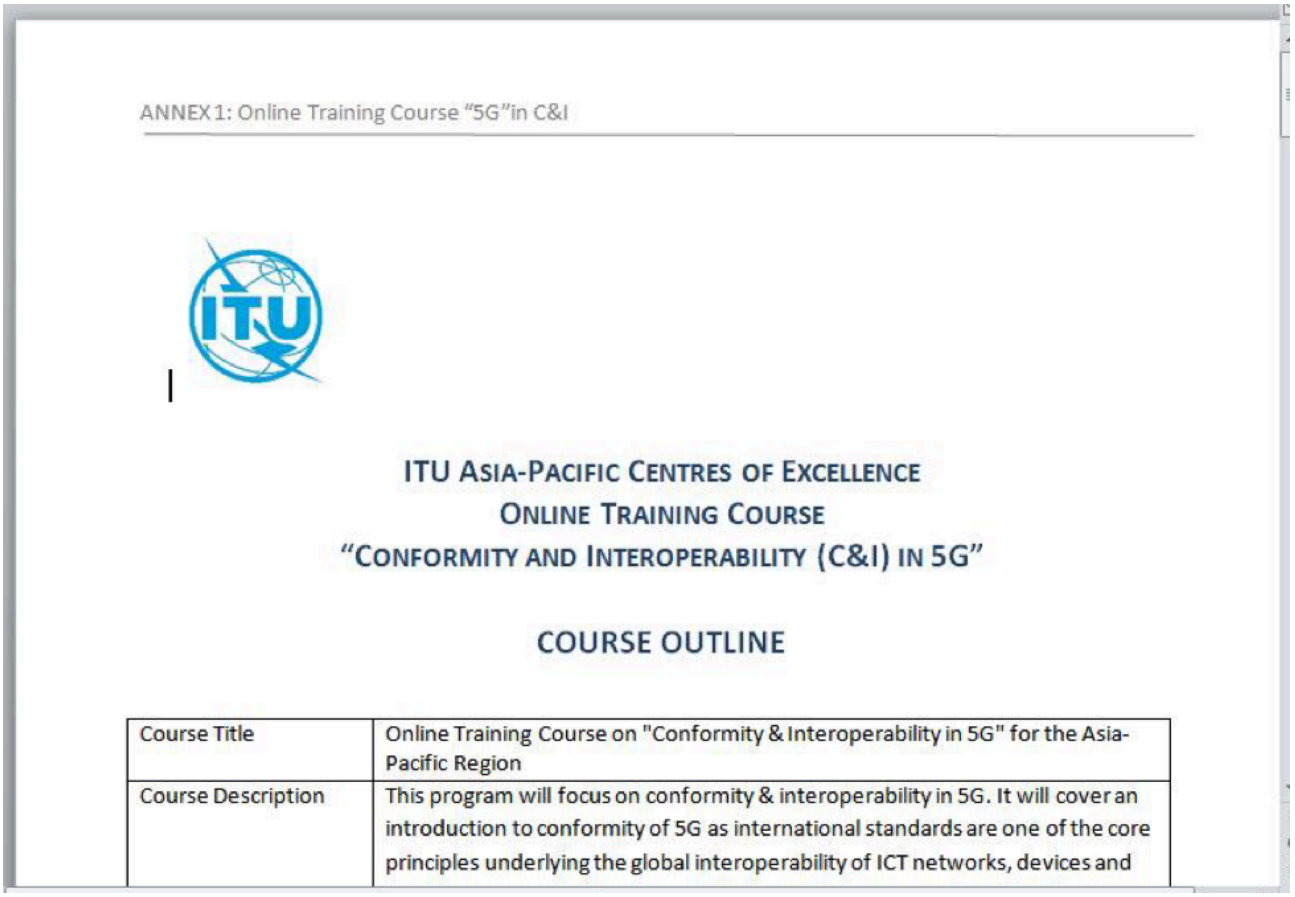
Beginning in early 2019, these threat actors targeted a number of government agencies in East Asia overseeing government information technology, domestic affairs, foreign affairs, economic development, and political processes. We determined that the infection vector observed in this campaign was spear phishing, with emails originating from both free email accounts and compromised user accounts. Attackers relied on Microsoft Equation Editor exploit CVE-2018-0798 to deliver a custom malware that Proofpoint researchers have dubbed Cotx RAT.

Additionally, this APT group utilizes Poison Ivy payloads that share overlapping command and control (C&C) infrastructure with the newly identified Cotx campaigns. Based on infrastructure overlaps, post-exploitation techniques, and historic TTPs utilized in this operation, Proofpoint analysts attribute this activity to the Chinese APT group tracked internally as TA428. Researchers believe that this activity has an operational and tactical resemblance to the Maudi Surveillance Operation which was previously reported in 2013 [1].

Delivery

Proofpoint researchers initially identified email campaigns with malicious RTF document attachments targeting East Asian government agencies in March 2019. These campaigns originated from adversary-operated free email sender accounts at yahoo[.]co[.].jp and yahoo[.]com. Sender addresses often imitated common names found in the languages of targeted entities. Spear phishing emails included malicious .doc attachments that were actually RTF files saved with .doc file extensions.

The lures used in the subjects, attachment names, and attachment content in several cases utilized information technology themes specific to Asia such as governmental or public training documents relating to IT. On one specific occasion an email utilized the subject “ITU Asia-Pacific Online CoE Training Course on ‘Conformity & Interoperability in 5G’ for the Asia-Pacific Region, 15-26 April 2019” and the attachment name “190315_annex 1 online_course_agenda_coei_c&i.doc”. The conference referenced in the lure was an actual event likely selected due to its relevance to potential victims. This is significant as countries in the APAC region continue to adopt Chinese 5G technology in government as well as heavy equipment industries.


ANNEX 1: Online Training Course "5G" in C&I

ITU ASIA-PACIFIC CENTRES OF EXCELLENCE
ONLINE TRAINING COURSE
"CONFORMITY AND INTEROPERABILITY (C&I) IN 5G"

COURSE OUTLINE

Course Title	Online Training Course on "Conformity & Interoperability in 5G" for the Asia-Pacific Region
Course Description	This program will focus on conformity & interoperability in 5G. It will cover an introduction to conformity of 5G as international standards are one of the core principles underlying the global interoperability of ICT networks, devices and

Figure 1: Example lure used by TA428 referencing an APAC IT conference

We identified several government agencies targeted as part of Operation LagTime IT. These agencies are responsible for overseeing IT, scientific research, domestic affairs, foreign affairs, political processes, and financial development.

Exploitation

As we previously noted, the malicious RTF attachments exploited vulnerabilities in the Microsoft Equation Editor, specifically CVE-2018-0798, before downloading subsequent payloads. The exploit uses an encoded RTF object to drop a PE file to the Windows temporary directory. The dropped PE file has the distinctive file name "8.t". When executed, writes a Word Add-In file with the ".wll" extension to the Windows Startup directory, which runs the next time Word is opened. It should be noted that this dropper methodology is not unique to TA428, and has been identified by security researchers in campaigns related to at least four additional Chinese APT groups. RTF files leveraging this technique have historically contained the string "objw871\\objh811\\objscalex8\\objscaley8" which has been noted by researchers at Anomali [2] and FireEye. Researchers have also recently observed this RTF weaponizer tool in commodity campaigns delivering Async RAT.

After it is executed, the .wll file renames itself as RasTls.dll. Simultaneously, it decrypts a legitimate Symantec PE binary commonly named IntelGraphicsController.exe or AcroRd32.exe. This legitimate Symantec binary is used to side-load RasTls.dll using DLL search-order hijacking leading to the execution of Cotx RAT malware. Once executed the RasTls.dll file next resolves the addresses of the DLL libraries it is programmed to access and ensures that it is only running in one of five predetermined processes. These processes are winword.exe,

excel.exe, powerpnt.exe, eqnedt32.exe, and acrord32.exe. The first four of these processes are associated with Microsoft Word, Excel, and PowerPoint exploits, as well as the Equation Editor exploit used by the initial malicious RTF in this campaign. The last process is utilized as part of the loading process for Cotx RAT and involves the legitimate Symantec binary noted above. The inclusion of the processes excel.exe and powerpnt.exe suggests that this stage one malware may be capable of utilizing .xls and .ppsx files as droppers. Researchers at SectorB06 [4] have noted this stage-one payload and indicated that throughout the above process it is running a “CheckRemoteDebuggerPresent” function to prevent analysis and debugging by researchers.

Malware: Cotx RAT

The RasTls.dll contains the Cotx RAT code. The malware is written in C++ using object-oriented programming. We named it by borrowing the name of the location of its stored configuration. The encrypted configuration is stored in the side-loaded DLL file RasTls.dll in a PE section named “.cotx”. The current encrypted configuration is also stored in the registry key “HKEY_LOCAL_MACHINE\SOFTWARE\Intel\Java\user”.

The configuration data is AES-192-encrypted using CBC mode and base64-encoded. We determined that the encryption key was "98151137ab12780969b2c3612072018709a83a3352466a8b" (hex-encoded) and the initialization vector “IV” was “204212322431511703 1b1a0a3ccda53f” (hex-encoded). In plaintext the configuration appears as follows:

```
*\x00\x00\x00217.69.8.255|||1.187.1.187|mark3|P@SSaw1||\x00\x00

The first four bytes contain the size of the configuration (42-bytes). The configuration is pipe del
```

1. C&C host 1
2. C&C host 2
3. C&C host 3
4. Definition of two C&C ports
    1. An example string looks like an IP address: "1.187.1.187"
    2. The string is split on "."
    3. Port 1 is defined by (piece0 << 8) + piece1 = (1 << 8) + 187 = 443
    4. Port 2 is defined by (piece2 << 8) + piece3 = (1 << 8) + 187 = 443
    5. Alternatively, if the string is not an IP address, but looks like a host, it will resolve the host into an IP address and calculate the ports using the resolved address
5. "mark" field - sent in the C&C beacon
6. "passwd" field - sent in the C&C beacon
7. Proxy IP and port
    1. Discovered by searching the IPv4 TCP connection table for established connections with remote ports using common proxy ports (3128, 8080, 808, 1080)
    2. Or via WINHTTP_OPTION_PROXY

For persistence, Cotx stores files in a directory “Intel\Intel(R) Processor Graphics”. The location of this folder varies among samples with both the %AppData% and %PROGRAMFILES% directories being observed.

The command and control structure of Cotx RAT is proxy aware. It utilizes wolfSSL for TLS encrypted communication. The initial beacon contains “|”-delimited system information. The data included in the beacon is Zlib compressed and encrypted with AES-192 in CBC mode utilizing the same keys as the configuration. The following values are included:

- "id" value from "software\\intel\\java" subkey
- Computer name
- "mark" field from configuration
- Username
- Windows version
- Architecture
- Possible malware version. "0.9.7" is hardcoded in the analyzed sample
- Local IP addresses
- First adapter's MAC address
- Connection type (https or _proxy)
- "password" field from configuration

Commands from the C&C are received from the malware beacon. This data is AES-encrypted. We observed the following commands:

- 0 - Keep alive, sets a "poll again" flag and sends an empty response to C&C
- 1 - Sets "id" value in "software\\intel\\java" subkey, sends an empty response to C&C
- 2 - Get directory info or drive info
- 5 - Open command shell
- 6 - Open command shell as logged in user
- 7 - Send command to command shell
- 8 - Copy file
- 9 - Delete file
- 10 - Read file
- 11 - Check for filename. If doesn't exist, check for filename with ".ut" extension. If it exists, send file size back to C&C
- 12 - Write file
- 13 - Screenshot
- 14 - Process listing
- 15 - Kill process
- 16 - Send current configuration to C&C
- 17 - Update config in registry and ".cotx" PE section
- 18 - Set sleep time
- 19 - Close C&C comms
- 20 - Uninstall and remove self
- 21 - Get list of installed software
- 22 - Kill command shell
- 23 - Exit malware

- 24 - Send a "Ctrl-C" to the command shell and exit
- 25 - Execute an executable

Malware: Poison Ivy

TA428 threat actors also delivered Poison Ivy malware payloads. In a limited number of cases, we observed attachments utilizing the 8.t dropper methodology described above. However, the majority of Poison Ivy payloads were dropped as PE files named OSE.exe when the RTF attachment was executed and an Equation Editor vulnerability was successfully exploited. The Poison Ivy samples all communicated with the IP 95.179.131[.]29. We identified earlier variants of Poison Ivy malware that utilized the above IP via open source research, which used the file names bubbles.exe and sfx.exe. Examination of the Poison Ivy malware configurations indicated that all samples shared the password “3&U<9f*lZ>!MIQ” while campaign and group IDs, as well as mutexes varied across campaigns.

We identified significant operational overlap between Cotx RAT campaigns and Poison Ivy campaigns. Specifically, on several occasions users that were unsuccessfully targeted with Cotx RAT malware were later targeted with messages distributing Poison Ivy. Users were also targeted by Poison Ivy malware on successive occasions indicating the adversary’s persistent nature in attempting to compromise targets via spear phishing. In one example, a targeted user received an unsuccessful phishing email attempting to deliver Cotx RAT followed by a Poison Ivy phishing email seven days later. In addition to a shared targeting list, analysts observed adversary reuse of free email sender accounts to deliver both Cotx RAT and Poison Ivy malware to different users. It appears the adversary sender accounts utilized delivery TTPs and payloads interchangeably from March through April 2019. This vacillation of tactics further enforces Proofpoint’s classification of these campaigns under a single operation.

C&C Infrastructure

An examination of the separate C&C infrastructure utilized by Cotx RAT and Poison Ivy payloads revealed further overlaps between these campaigns. A review of passive DNS information indicated that the C&C IPs hosted subdomains that share the root domain vzglagtime[.]net. We found that the Poison Ivy C&C IP hosted the domains f1news[.]vzglagtime[.]net and news[.]vzglagtime[.]net. The Cotx RAT C&C IP hosted the hostname mtanews.vzglagtime[.]net. The latter of these domains was previously reported by security researchers to have been a C&C address observed in a malware implant targeting the East Asian Telecommunications and Transportation sectors in January 2019. The presence of related domain registrations on disparate malware IP infrastructure also contributed to analysts’ decision to classify these campaigns collectively under Operation LagTime IT.

	Poison Ivy	**Cotx RAT**
C&C IP	95.179.131[.]29	217.69.8[.]255

Domains Hosted by IP	f1news.vzglagtime[.]net news.vzglagtime[.]net	mtanews.vzglagtime[.]net

Conclusion

Proofpoint analysts assess that Operation LagTime IT is likely a continuation of targeted activity by APT actors aligned with Chinese state interests. This operation, centered around East Asian governmental agencies, may represent efforts to satisfy espionage and intelligence requirements relative to China's regional neighbors. While not revolutionary in its approach or malware design, TA428 actors demonstrated significant persistence in compromising victims and utilized custom malware. The defined scope of targeting in this operation including government information technology agencies demonstrates a focus on high-value targets. While ultimately the motivation for this APT campaign remains opaque, what is certain is that TA428 persists in targeting users responsible for the orchestration of governmental systems in East Asia.

References

[1] https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2012/NormanShark-MaudiOperation.pdf

[2] https://www.anomali.com/blog/analyzing-digital-quartermasters-in-asia-do-chinese-and-indian-apts-have-a-shared-supply-chain

[3] https://speakerdeck.com/ashley920/into-the-fog-the-return-of-icefog-apt

[4] https://threatrecon.nshc.net/2019/04/30/sectorb06-using-mongolian-language-in-lure-document/

Indicators of Compromise (IOCs)

IOC	IOC Type	Description
304115cef6cc7b81f4409178cd0bcea2b22fd68ca18dfd5432c623cbbb507154	SHA256	Cotx RAT
d0ccb9a277b986f7127199f122023c79a7e0253378a4a78806fbf55a87633532	SHA256	Cotx RAT
81898df69e28a084ea37b77b568ccde34afdf96122ab784f8a361f055281ed0f	SHA256	Cotx RAT
93ac0ff3f01f8b8dfad069944d917e4b0798d42bc9ff97028e5a4ea8bda54dbc	SHA256	Cotx RAT

3dbff4e82dd8ddf71f9228f68df702b8f4add47237f2aee76bd5537489ed2fa9	SHA256	Cotx RAT
cbf607725d128d93fed3b58cde78e1feb7db028a1ed1aa5c924e44faa1015913	SHA256	Poison Ivy
9a477b455a20a26875e5ff804151f9f6524131c32edf04366cfbaf9d41c83f2a	SHA256	Poison Ivy
eb0191d1b8e311d2716795e9fa7c0300c5199ebf3d8debff77993f23397d2fb5	SHA256	Poison Ivy
1bc93ef96134be9a5a7b5f5b747be796a9ff95bdc835d72541673565d1c165b8	SHA256	Poison Ivy
4c22eb33aa1d10511eaf8d13098e2687e44eaebc5af8112473e28acedac34bea	SHA256	Poison Ivy
93f56ec68e072ccba8102c71d005604763d064021795c7c8bb1cade05ddb6ff6	SHA256	Poison Ivy
e9fa0a6223b0e4e60654dc629cd46174b064d5a0968732e6f05bc212a2cdf3f4	SHA256	Poison Ivy
b7cfea87d7de935e1f20e3c09ba4bd1154580682e75330876f21f241b33946f2	SHA256	8.t Dropper
ae3e335cc39c07bda70e26e89003e0d1b8eea2deda2b62a006517c959fc0a27a	SHA256	8.t Dropper
1d492e549d2cbd296bc8e1368c8625df0c82c467c1b4addea7191e4a80bf074e	SHA256	8.t Dropper
b541e0e29c34800a067b060d9ee18d8d35c75f056f4246b1ce9561a5441d5a0f	SHA256	8.t Dropper
95.179.131[.]29	C2 IP	Poison Ivy C2
217.69.8[.]255	C2 IP	Cotx RAT C2

f1news.vzglagtime[.]net	Domain	Domain Related by IP
news.vzglagtime[.]net	Domain	Domain Related by IP
mtanews.vzglagtime[.]net	Domain	Domain Related by IP

ET and ETPRO Suricata/Snort Signatures

2836210 ETPRO TROJAN SSL/TLS Certificate Observed (SectorB06 Dropper)
