NIGHT SKY AND CHEERSCRYPT: REVEALING A UNIFIED CHINESE RANSOMWARE GROUP

Key Takeaways

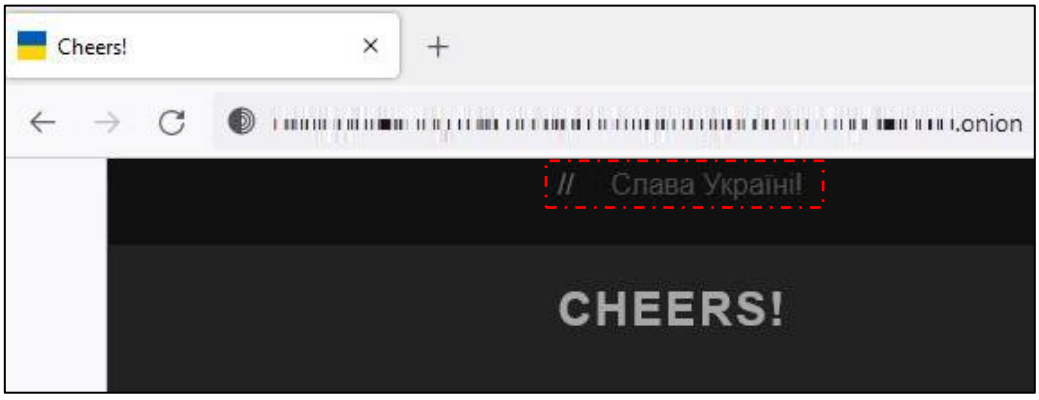
- Sygnia recently investigated a Cheerscrypt ransomware attack which utilized Night Sky ransomware TTPs. Further analysis revealed that Cheerscrypt and Night Sky are both rebrands of the same threat group, dubbed 'Emperor Dragonfly' by Sygnia.
- 'Emperor Dragonfly' (A.K.A. DEV-0401 / BRONZE STARLIGHT) deployed open-source tools that were written by Chinese developers for Chinese users. This reinforces claims that the 'Emperor Dragonfly' ransomware operators are based in China.
- Contrary to publicly available information, Cheerscrypt ransomware makes use of payloads that target both Windows and ESXi environments.

Introduction

Sygnia recently investigated an incident involving Cheerscrypt ransomware. As the investigation progressed, it became clear that the threat actors had successfully maintained their presence inside the compromised network for several months. During the investigation, our incident response team made a significant discovery: the Tactics, Techniques and Procedures (TTPs) that were used in this attack strongly resemble those used by another ransomware group – Night Sky.

The publicly-available information on Cheerscrypt is sparse and focuses on the final payload – the ransomware itself – and the subsequent encryption of ESXi servers. However, in this incident, Windows servers were also encrypted by Cheerscrypt's ransomware encryptor.

Sygnia decided to investigate the threat actors behind this attack, in an attempt to attribute the group to a known actor. Although Night Sky was previously identified as being associated with another threat group, Cheerscrypt was unknown. The only clue to their identity was that the threat actors behind Cheerscrypt present themselves as pro-Ukrainian, indicated by the phrase "Слава Україні!" ("Glory to Ukraine!")[1] and the Ukrainian flag that can be found on their dark web leak site.



[1] https://en.wikipedia.org/wiki/Slava_Ukraini

Figure 1: Cheerscrypt dark web leak site with the flag of Ukraine and the Ukrainian national salute

Finding the Link: Night Sky and Cheerscrypt

The attack kill-chain which Sygnia investigated can be broken down into four phases:

Initial access

In January 2022, a VMware Horizon server was compromised by threat actors leveraging the Log4Shell vulnerability (CVE-2021-4428). Shortly after, PowerShell was used to execute reconnaissance commands and communicate with a Command and Control (C&C) server. The TTPs and the specific IOCs of this stage match the published information about Night Sky ransomware[2].

Establishing foothold within the network

After the successful compromise, PowerShell was used to download three files, which consisted of a signed legitimate executable, a DLL, and an encrypted file. Next, the legitimate executable was abused to side-load a weaponized DLL, which loaded and decrypted a Cobalt Strike Beacon.

This method of Cobalt Strike deployment is a known TTP of the Night Sky operators, and the Beacon was downloaded from a known Night Sky C&C server[3]. However, what Sygnia discovered next was surprising: in parallel to the Beacon deployment, three tools written in Go were also deployed. These binaries were compiled from open-source projects, created by Chinese-speaking developers, with documentation in English and Chinese. The binaries were identified as:

1. A forked version[4] of a keylogger[5] that supports uploading the key-stroke log to Alibaba Cloud Object Storage Service (Aliyun OSS).
2. A customized version of 'IOX'[6] – a port-forwarding and proxy tool. Based on its documentation, IOX can work as a simple ShadowSocks (an open-source encryption protocol used in China to circumvent internet censorship, tunneling under the Great Firewall), a fact which demonstrates that the target audience is Chinese.
3. A customized version of 'NPS'[7] – a tunneling tool that was deployed alongside IOX. The combination of the tools enabled the threat actors to create multiple connections through a single tunnel.

The threat actors utilized the same compromised user account to deploy both the Cobalt Strike Beacons and the Go binaries. This user account was also used to create a system service which functioned as the Go tools persistence mechanism.

---

[2] https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/
[3] https://www.avertium.com/resources/threat-reports/everything-you-need-to-know-about-night-sky-ransomware
[4] https://github.com/uknowsec/keylogger
[5] https://github.com/kmahyyg/keylogger
[6] https://github.com/EddieIvan01/iox
[7] https://github.com/ehang-io/nps

Lateral movement

The threat actors used the Impacket[8] open-source tool to move laterally and perform reconnaissance activities within the network by executing code remotely. This was achieved by utilizing two of Impacket's Python modules: 'SMBExec.py' and 'WMIExec.py'.

SMBExec was also used to check whether some of the Cobalt Strike Beacons were still running on compromised systems.

In the weeks following the initial infiltration, additional Beacons were deployed inside the victim organization's systems in the same way (using staging folders and executables previously attributed to Night Sky), communicating with a new C&C server – one which was not previously attributed to Night Sky ransomware activity.

Data exfiltration and ransomware execution

In the final stages of the attack, the threat actors used the Rclone open-source command-line tool to exfiltrate sensitive information to Mega, a cloud storage service.

Shortly after, the threat actors delivered the final payload: Cheerscrypt ransomware. Although most publications describe Cheerscrypt as a Linux-based ransomware family that targets ESXi servers[9], in the case Sygnia investigated, both Windows and ESXi machines were encrypted.

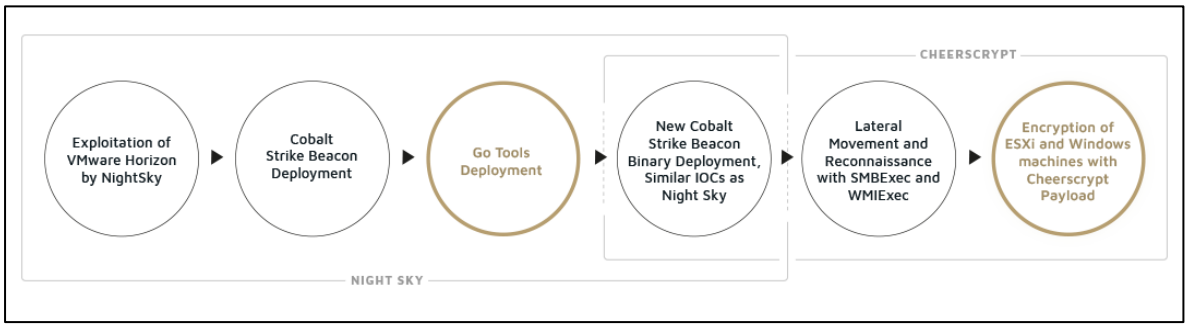


Figure 2: Emperor Dragonfly TTPs as observed during the investigation. The black circles are known TTPs, while the golden circles are newly discovered TTPs, and they encompass both Cheerscrypt and Night Sky campaigns.

Enter the Dragon: Emperor Dragonfly Ransomware Group

The fact that Night Sky IOCs were identified, but Cheerscrypt ransomware was deployed, prompted Sygnia's Incident Response team to delve deeper into Cheerscrypt's origins. It became clear that Cheerscrypt, like Night Sky, is another ransomware family developed by Emperor Dragonfly.

Emperor Dragonfly – also known as DEV-0401, and BRONZE STARLIGHT – is a Chinese ransomware group that started operating in mid-2021. Unlike other ransomware groups, Emperor Dragonfly does not operate in an affiliate model and refrain from purchasing initial

[8] https://github.com/SecureAuthCorp/impacket
[9] https://www.trendmicro.com/en_us/research/22/e/new-linux-based-ransomware-cheerscrypt-targets-exsi-devices.html

access from other threat actors. Instead, they manage all stages of the attack lifecycle on their own. The group often rebrand their ransomware payloads, which helps them stay under the radar and avoid sanctions – as they have the appearance of being several, smaller ransomware groups.

In the world of ransomware affiliates and leaked ransomware source code, it is difficult to connect two ransomware strains with one threat actor. However, the following points represent the cumulative evidence which illustrates the correlations between Night Sky and Cheerscrypt when compared with Emperor Dragonfly:

1. The observed TTPs are known characteristics of Emperor Dragonfly attacks. These TTPs include the initial access vector, lateral movement technique, and the unique Cobalt Strike Beacon deployment, using DLL side-loading and an encrypted Beacon in a separate file. Interestingly, the initial access was part of a wider exploitation of Log4Shell that was attributed to Emperor Dragonfly[10], and occurred during the same time frame.
2. Emperor Dragonfly routinely change their ransomware payloads. In the past year, the group used several ransomware families[11], including LockFile, AtomSilo, Rook, Night Sky and Pandora. The encryptors of these ransomware families share code similarities, as they were all created from the leaked source code of Babuk ransomware. Trend Micro's[12] analysis of the Cheerscrypt ransomware encryptor revealed that it was also created from Babuk, indicating a possible link between Night Sky and Cheerscrypt.
3. Emperor Dragonfly is described by Microsoft as a 'lone wolf'[13]. Unlike other ransomware groups, they don't work in an affiliate model (they don't offer their ransomware in a 'ransomware-as-a-service' model), and they don't purchase access from initial access brokers. This supports the assumption that a breach started by Emperor Dragonfly (with Night Sky TTPs) will probably be completed by Emperor Dragonfly (using a Cheerscrypt ransomware payload), and it is unlikely that this group sold or transferred this access to another group.
4. Emperor Dragonfly is a China-based ransomware operator[14], making it a rarity in today's threat landscape[15]. During Sygnia's investigation, we discovered that in parallel to the Cobalt Strike Beacon deployment, three Go binaries were also deployed (see above). These Go tools are not commonly used by ransomware operators, and their GitHub popularity rank is relatively low. Emperor Dragonfly used the tools throughout the entire

[10] https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/
[11] https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/#DEV-0401; https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader; https://www.forescout.com/resources/night-sky-ransomeware-threat-brief/
[12] https://www.trendmicro.com/en_us/research/22/e/new-linux-based-ransomware-cheerscrypt-targets-exsi-devices.html
[13] https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/#DEV-0401
[14] https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/#DEV-0401; https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader
[15] https://twitter.com/cglyer/status/1480738754906230790

compromise: they were deployed during early stages and were still running as a persistence mechanism after the ransomware deployment. This is another indication that a single threat actor conducted the entire operation.

The Hunt for Emperor Dragonfly

The following hunting ideas will help you search the organizational network for traces of Emperor Dragonfly.

- **Search for binaries, scripts, and executions from suspicious folders**. In the case of Emperor Dragonfly's attack, the same folders were repeatedly used for staging tools throughout the operation. '.EXE', '.DLL', '.INI', '.DAT' and more files were dropped and executed from 'C:\Windows\Help*', 'C:\Windows\Debug*' and 'C:\Users\Public*' folders.
- **Search for evidence of SMBExec executions**. For instance, a service called 'BTOBTO' was created on compromised machines with indicative command lines. The 'BTOBTO' service name is the default service name that is being used in SMBExec code, for remote code execution. The image command line had a specific format: '%COMSPEC%' /Q /c <COMMAND_TO_EXECUTE> ^> \\127.0.0.1\C$__output 2^>^&1 > %TEMP%\execute.bat & %COMSPEC% /Q /c %TEMP%\execute.bat & del %TEMP%\execute.bat'.
- **Search for evidence of WMIExec executions**. Files under 'ADMIN$' with the epoch timestamp of the tool's execution are created on the target machine on which the command was executed. In addition, 'cmd.exe' is spawned from the WMI provider process ('WmiPrvSE.exe'). The cmd.exe command line appears to be in a specific format, containing the string '\\127.0.0.1\ADMIN$\' as the destination folder for the execution output file.
- **Monitor users' authentications, and activity from unusual sources**. Throughout their operation, the threat actors leveraged compromised user accounts to perform lateral movement between servers. This kind of activity might be flagged as suspicious, as users generally perform authentication from endpoints, and not from servers.

Defending against Emperor Dragonfly

The following measures will help you defend against Emperor Dragonfly TTPs (as well as similar threats):

- **Identify and patch critical vulnerabilities.** If you are running VMware Horizon, follow VMware advisory[16] to ensure the currently installed version is patched against the Log4Shell[17] vulnerability, which was exploited as the initial infiltration vector. More generally, it is essential to conduct frequent vulnerability scans and swiftly mitigate discovered issues, with a special focus on internet-facing systems. External Attack Surface Management (EASM) tools, or even more traditional vulnerability or port scanners, can be leveraged to identify publicly exposed vulnerable interfaces.

[16] https://kb.vmware.com/s/article/87073
[17] https://blog.sygnia.co/log4shell-remote-code-execution-advisory

- **Limit outbound internet access from servers.** Denying egress traffic by default would've blocked the ability to communicate with the threat actor's C&C server, as well as with the cloud storage services (Alibaba, Mega), thus mitigating persistence and data exfiltration activities. Allow outbound connectivity to only specific destinations (FQDN or IP addresses), on a strict need-to-have basis.
- **Protect the virtualization platform.** Ransomware attacks targeting virtualization platforms is a growing trend, due to their simplicity and efficiency from the perspective of threat actors. Among the most prominent security controls for VMware against this threat are allowing traffic towards vCenter and ESXi hosts only from protected bastion hosts, enabling strict lockdown mode[18], and restricting unsigned scripts by enabling the 'execInstalledOnly' flag[19]. In addition, ensure virtual machines are securely backed-up; for example, if VM backups are made using snapshots which are stored on the same folder as the machine, threat actors may encrypt backups as well.
- **Limit lateral movement through the network.** Threat actors often leverage common management ports to move laterally between hosts, and Emperor Dragonfly is no different, with the use of SMBExec and WMIExec. Restricting traffic over such ports (namely SMB 445, RPC 135, WinRM 5985-5986, RDP 3389, SSH 22), and allowing traffic only from designated specific hosts, may be cumbersome in complex networks, but brings immense value. This may be achieved by host-based firewalls, proper network segmentation, or modern microsegmention technologies.
- **Protect privileged accounts.** Minimize the risk of privilege escalation by hardening the Active Directory environment[20], applying the principle of least privilege and AD administrative tier model, employing robust credential and password hygiene practices, and considering the implementation of Privileged Identity and Access solutions. While these security measures are by no means unique to Emperor Dragonfly TTPs, compromising privileged accounts and using them to move laterally and execute the ransomware is a practice noticed in the described incidents as well.

[18] https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-88B24613-E8F9-40D2-B838-225F5FF480FF.html
[19] https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-9047A43D-BB1F-4878-A971-EEFCAC183C86.html
[20] https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory

Appendix I: Indicators of Compromise

Cobalt Strike Beacons

MD5	Description	File Name
37011eed9de6a90f3be3e1cbba6c5ab2	Encrypted Cobalt Strike payload	C:\Windows\Help\OEM\ContentStore\vlcplayer.dat
240118f6205effcb3a12455a81cfb1c7	Weaponized DLL loaded by FCAuth.exe	C:\Windows\Help\Corporate\utilsdll.dll
e5fd4d5774ad97e5c04b69deae33dc9e	Weaponized DLL loaded by mfeann.exe	C:\Windows\debug\LockDown.dll
2893d476408e23b7e8a65c6898fe43fa	Encrypted Cobalt Strike payload	C:\Windows\Help\Corporate\auth.dat
8161d8339411ddd6d99d54d3aefa2943	Encrypted Cobalt Strike payload	C:\Windows\debug\debug.dat
5a852305ffb7b5abeb39fcb9a37122ff	Weaponized DLL loaded by vlc.exe	C:\Windows\Help\Corporate\libvlc.dll
f0656e3a70ab0a10f8d054149f12c935	Encrypted Cobalt Strike payload	C:\Windows\Help\Corporate\auth.dat
37011eed9de6a90f3be3e1cbba6c5ab2	Encrypted Cobalt Strike payload	C:\Windows\Help\Corporate\vlcplayer.dat

Go Tools

MD5	Description	File Name
5695de561a065123178067fcedf39ce3	NPC client for NPS tunnel tool	C:\Windows\Help\mui\0409\WindowsUpdate.exe
ea4ca87315d14f5142aaef1f5e287417	Keylogger	C:\Windows\Help\OEM\ContentStore.exe
5a6008cf994779cde1698a0e80bb817d	IOX port forwarder and proxy	C:\Windows\Help\Windows\dec.exe

Additional Artifacts

Artifact	Description
GrPpQGgI4se5fTIRkxBj/nfbcPvfJWpyY5Et RD0hf/CW9u6cXM4f4VKyyzaHJG/OLcdj B95YaMDP6Y1d-Mg	Go Build ID of NPS client-side binary (WindowsUpdate.exe)
GriAm-TYSQig04-nXbTE/ 9gsYQSitnL9GPHKgpNUX/ QA-vmpyo7vFHuU7RQ\ Y/ _NwncoU6QsMYGeukgxTd	Go Build ID of the keylogger (ContentStore.exe)
System Service Update	Service name; persistency mechanism for NPS client-side binary
C85A6814B99C8302AF484563D47D9658	MD5 hash of SharpShares, an open-source tool to enumerate shares
07d14d16d21d21d00042d41d00041d47e 4e0ae17960b2a5b4fd6107fbb0926	JARM hash of the Cobalt Strike C&C servers

Network Indicators

IP Address	Description	URL
207[.]148[.]122[.]171	C&C server	api[.]rogerscorp[.]org
139[.]180[.]217[.]203	C&C server (Cobalt Strike Beacon was downloaded from this IP)	
178[.]128[.]102[.]13	Cobalt Strike C&C server	
139[.]59[.]243[.]219	Cobalt Strike C&C server	
128[.]199[.]151[.]146	NPS server	

Legitimate Executables

MD5	Description	File Name
f9322ead69300501356b13d751165daa	Signed McAfee file used to side-load LockDown.dll	c:\Windows\debug\mfeann.exe
51be3e3a8101bc4298b43a64540c422b	Signed FortiClient file used to side-load utilsdll.dll	C:\Windows\Help\Corporate\FCAuth.exe
e2904f5301b35b2722faf578d1f7a4d4	Signed VLC file used to side-load libvlc.dll	C:\Windows\Help\Corporate\vlc.exe

Appendix II: MITRE ATT&CK TTPs

1. Initial Access
    a. T1190: Exploit Public-Facing Application
2. Execution
    a. T1059.001: Command and Scripting Interpreter: PowerShell
    b. T1059.003: Command and Scripting Interpreter: Windows Command Shell
    c. T1047: Windows Management Instrumentation
    d. T1569.002: System Services: Service Execution
3. Persistence
    a. T1543.003: Create or Modify System Process: Windows Service
4. Defense Evasion
    a. T1027.002: Obfuscated Files or Information: Software Packing
    b. T1574.002: Hijack Execution Flow: DLL Side-Loading
    c. T1070.004: Indicator Removal on Host: File Deletion
5. Discovery
    a. T1135: Network Share Discovery
    b. T1087.002: Account Discovery: Domain Account
    c. T1082: System Information Discovery
    d. T1016: System Network Configuration Discovery
6. Lateral Movement
    a. T1570: Lateral Tool Transfer
    b. T1021.001: Remote Services: Remote Desktop Protocol
7. Collection
    a. T1039: Data from Network Shared Drive
    b. T1056.001: Input Capture: Keylogging
8. Command & Control
    a. T1090: Proxy
    b. T1095: Non-Application Layer Protocol
    c. T1572: Protocol Tunneling
    d. T1071.001: Application Layer Protocol: Web Protocols
    e. T1132.001: Data Encoding: Standard Encoding
    f. T1573: Encrypted Channel
9. Exfiltration
    a. T1048: Exfiltration Over Alternative Protocol
    b. T1567.002: Exfiltration Over Web Service: Exfiltration to Cloud Storage
10. Impact
    a. T1486: Data Encrypted for Impact

Contributors: Oren Biderman, Amnon Kushnir, Noam Lifshitz, Ori Porag, Yoav Mazor, Erez Kalman, Haim Nachmias

has been obtained from reliable sources and to perform rigorous analysis, this advisory is based on initial rapid study, and needs to be treated accordingly. Sygnia is not responsible for any errors or omissions, or for the results obtained from the use of this Advisory. This Advisory is provided on an as-is basis, and without warranties of any kind.