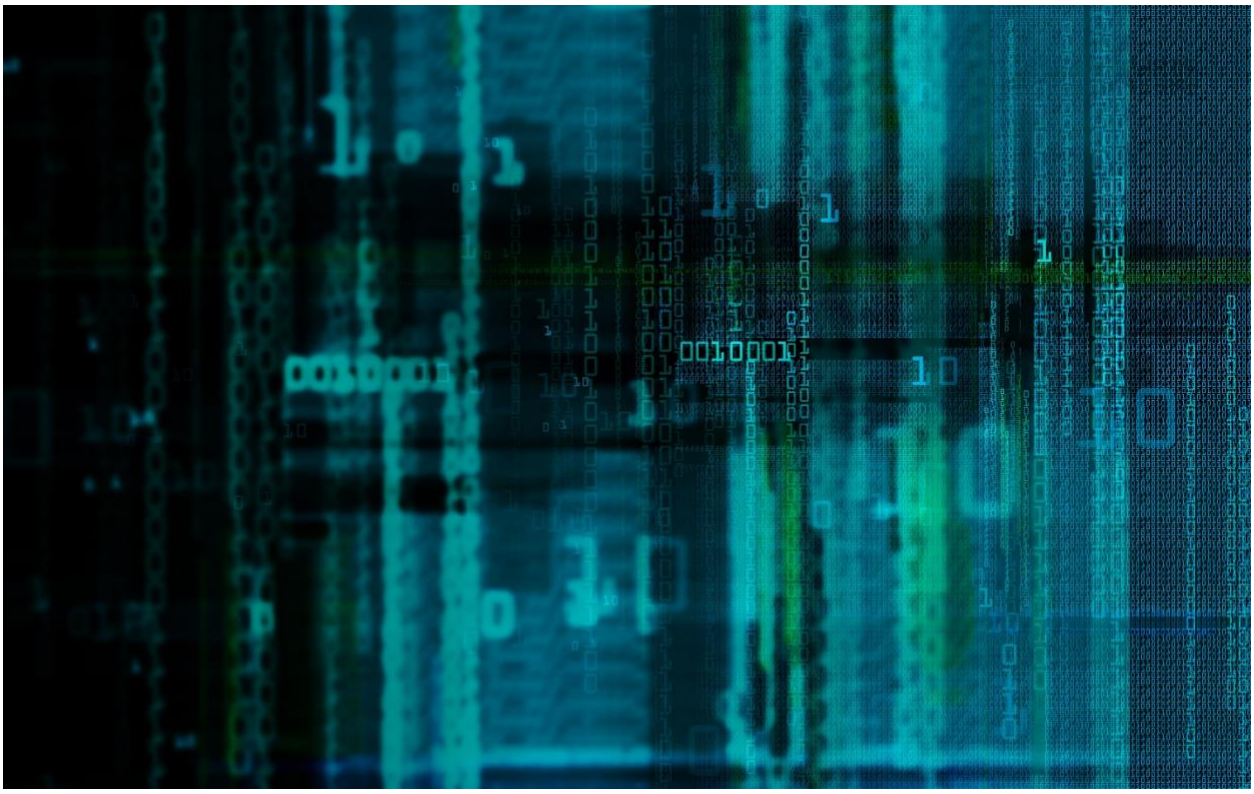
Content Checklist

Main Title	☒
Short Summary	☒
Protection	☐
Mitigation	☐
Indicators of Compromise	☐

Grayfly: Chinese Threat Actor Uses Newly-discovered Sidewalk Malware

Symantec Threat Hunter Team

Recent campaigns involved exploits against Exchange and MySQL servers. Group has heavy focus on telecoms sector.



Symantec, part of Broadcom Software, has linked the recently discovered Sidewalk backdoor to the China-linked Grayfly espionage group. The malware, which is related to the older Crosswalk backdoor (Backdoor.Motnug) has been deployed in recent Grayfly campaigns against a number of organizations in Taiwan, Vietnam, the United States, and Mexico. A feature of this recent campaign was that a large

number of targets were in the telecoms sector. The group also attacked organizations in the IT, media, and finance sectors.

Sidewalk was recently documented by ESET, who attributed it to a new group it called SparklingGoblin, which it linked to the Winnti malware family. Symantec's Threat Hunter Team has attributed Sidewalk to Grayfly, a longstanding Chinese espionage operation. Members of the group were indicted in the U.S. in 2020. The recent campaign involving Sidewalk suggests that Grayfly has been undeterred by the publicity surrounding the indictments.

Who are Grayfly?

Grayfly (aka GREF and Wicked Panda) is a targeted attack group that has been active since at least March 2017 using a custom backdoor known as Backdoor.Motnug (aka TOMMYGUN/CROSSWALK), a custom loader called Trojan.Chattak, Cobalt Strike (aka Trojan.Agentemis), and ancillary tools in its attacks.

Grayfly has been observed targeting a number of countries in Asia, Europe, and North America across a variety of industries, including food, financial, healthcare, hospitality, manufacturing, and telecommunications. In more recent activity, Grayfly has continued with its focus on telecommunications, but has also been observed targeting organizations operating within the media, finance, and IT service provider sectors. Typically Grayfly targets publicly facing web servers to install web shells for initial intrusion, before spreading further within the network.

Once a network has been compromised, Grayfly may install its custom backdoors onto additional systems. These tools allow the attackers to have comprehensive remote access to the network and proxy connections allowing them to access hard-to-reach segments of a target's network.

Although sometimes labelled APT41, we consider Grayfly the espionage arm of APT41. Similarly, Symantec tracks other sub-groups of APT41 separately, such as Blackfly, its cyber-crime arm.

Sidewalk campaign

A characteristic of the recent campaign was that the group appeared to be particularly interested in attacking exposed Microsoft Exchange or MySQL servers. This suggests that the initial vector may be the exploit of multiple vulnerabilities against public-facing servers.

In at least one attack, the suspicious Exchange activity was followed by PowerShell commands used to install an unidentified web shell. Following this, the malicious backdoor was executed.

After the installation of the backdoor, the attackers deployed a custom version of the credential-dumping tool Mimikatz. This version of Mimikatz has been used previously in Grayfly attacks.

Victim case study

The first indication of attacker activity was identified at 20:39 local time, where a Base64-encoded PowerShell command was executed via a legitimate Exchange Server related process. The command was used to execute certutil to decode and install a web shell:

```
>(^_certutil -decode -f C:\Windows\Temp\ImportContactList_-.aspx
C:\Windows\Temp\ImportContactList.aspx;if((dir
C:\Windows\Temp\ImportContactList.aspx).Length -eq 212){Remove-Item -
Force C:\Windows\Temp\ImportContactList_*-*.aspx}*
```

Next, another Base64-encoded PowerShell command was executed. This command was used to move the web shell to the Exchange install path, accessible by the attackers – specifically the ClientAccess\ecp directory.

- mv C:\Windows\Temp\ImportContactList.aspx $envExchangeInstallPath\ClientAccess\esp\ -Force

Several minutes later, a backdoor was executed via installutil.exe:

- CSIDL_WINDOWS\microsoft.net\framework64\v4.0.30319\installutil.exe /logfile= /LogToConsole=false /ParentProc=none /U CSIDL_WINDOWS\microsoft.net\framework64\v4.0.30319\microsoft.webapi.config

Roughly an hour later, the attackers were observed executing a WMIC command in order to run a Windows batch file. This file was used to create a scheduled task to execute the backdoor and ensure persistence:

- WMIC /NODE:"172.16.140.234" process call create "cmd.exe /c c:\users\public\schtask.bat"

Shortly after this, Mimikatz was executed to dump credentials:

- sha2:b3eb783b017da32e33d19670b39eae0b11de8e983891dd4feb873d6e9333608d (Mimikatz) - csidl_system_drive\perflogs\ulsassx64.exe

After this point, no further activity was observed.

Indictments

Three Chinese men were indicted in the U.S. in 2020 for their involvement in attacks that involved Grayfly tools and tactics. At the time of the indictment, Jiang Lizhi, Qian Chuan, and Fu Qiang were based in the Chinese city of Chengdu and held senior positions in a company called Chengdu 404. The company describes itself as a network security specialist and claims to employ a team of white hat hackers who can perform penetration testing along with other security operations.

The indictment charged the men with involvement in attacks against over 100 different organizations in the U.S., South Korea, Japan, India, Taiwan, Hong Kong, Malaysia, Vietnam, India, Pakistan, Australia, the United Kingdom, Chile, Indonesia, Singapore, and Thailand. Jiang was said to have a “working relationship” with the Chinese Ministry of State Security which would provide him and his associates with a degree of state protection.

Likely to continue

Grayfly are a capable actor, likely to continue to pose a risk to organizations in Asia and Europe across a variety of industries, including telecommunications, finance, and media. It's likely this group will continue to develop and improve its custom tools to enhance evasion tactics along with using commodity tools such publicly available exploits and web shells to assist in their attacks.

Protection/Mitigation

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise

SHA256	Description	Detection
1b5b37790b2029902d2d6db2da20da4d0d7846b20e32434f01b2d384eba0eded	Sidewalk loader	Trojan.Gen.MBT
b732bba813c06c1c92975b34eda400a84b5cc54a460eeca309dfecbe9b559bd4	Sidewalk loader	Trojan.Gen.MBT
04f6fc49da69838f5b511d8f996dc409a53249099bd71b3c897b98ad97fd867c	Sidewalk loader	Trojan.Gen.MBT
25a7c1f94822dc61211de253ff0a5805a0eb83921126732a0d52b1f1967cf079	Sidewalk loader	Trojan Horse
b3eb783b017da32e33d19670b39eae0b11de8e983891dd4feb873d6e9333608d	Mimikatz	Hacktool.Mimikatz