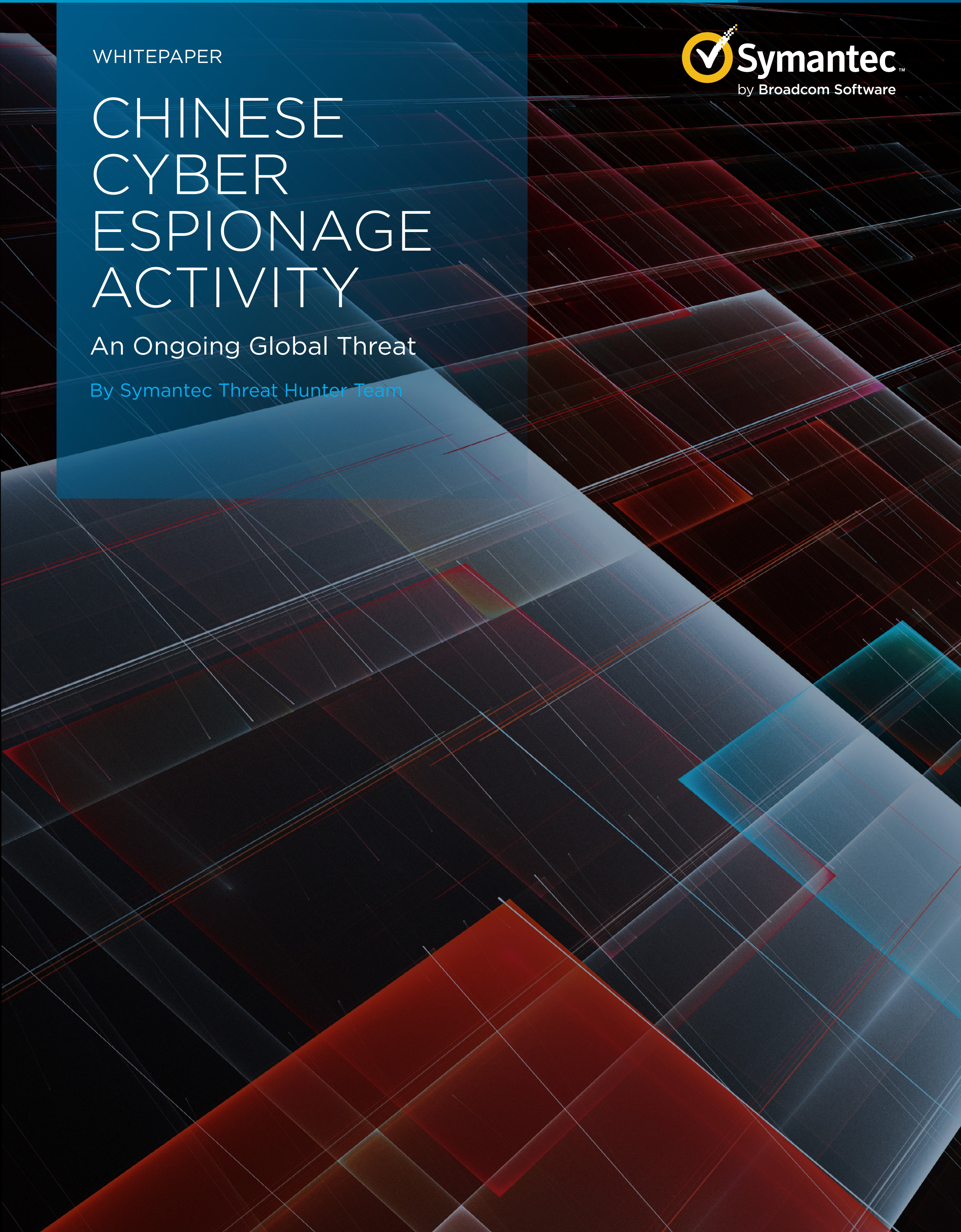
WHITEPAPER

CHINESE CYBER ESPIONAGE ACTIVITY

An Ongoing Global Threat

By Symantec Threat Hunter Team



WHITEPAPER

CHINESE CYBER ESPIONAGE ACTIVITY

An Ongoing Global Threat

By Symantec Threat Hunter Team

CONTENTS

Introduction

China-based threat actor activity has been prolific for many years. Most of the attackers that are tracked by Symantec, a division of Broadcom Software, and based in that country are state-sponsored advanced persistent threat (APT) groups. These groups are generally interested in espionage and intelligence gathering. However, some Chinese APT groups are known to have also carried out financially motivated attacks, which is not activity we generally see from APT groups, other than those operating out of North Korea.

However, it is not clear if the financially motivated attacks carried out by Chinese APT groups are the true aim of those groups or are essentially "side projects" of some of the contractors working for the groups, who leverage their access to networks to try and make some extra money for themselves. Blackfly (a sub-grouping of APT41) is a group that has been seen carrying out both financially motivated and intelligence-gathering driven attacks.

Chinese APT groups are also notable for being active for extensive periods of time, with many of the groups profiled in this paper first seen as far back as 2012 or even earlier. However, just because the group has been active for that long does not mean the personnel have remained the same. Chinese state-sponsored groups are known to use a lot of contractors, with movement between groups not uncommon. The sharing of tactics, tools, and procedures (TTPs) between different China-backed groups is also quite common, and sometimes makes attributing activity to a specific attack group difficult.

Another notable development emanating from Chinese actors in the last year was the discovery of Daxin, a new espionage tool that is the most advanced piece of malware we have ever seen from China-linked actors. We will discuss the significance of this new tool later in this paper.

Some of the main findings in this paper include:

- There is a significant amount of overlap between some Chinese APT groups, which sometimes makes attributing activity with high confidence to one specific group difficult.
- Chinese threat actors are primarily interested in cyber espionage, with some attacks appearing to also have financial motivations. However, those attacks are the exception, with espionage attacks very much the rule.

- Chinese threat actors have the skills and resources to develop custom malware, including highly sophisticated tools like the recently discovered Daxin malware.

APT41 in Focus: Blackfly and Grayfly – Two Sides of a Coin

For this paper we looked at a selection of the Chinese actors that we observed being active in 2021 and early 2022. One of the most active China-backed groups we observed in 2021 and into 2022 was a group tracked by many vendors as APT41. There can be a certain amount of crossover between Chinese APT groups, with disagreements sometimes between different security vendors about whether or not groups are affiliated or operate separately. For example, we track APT41 as two distinct sub-groups – Blackfly and Grayfly – whereas some vendors simply track all this activity under the APT41 umbrella. This crossover and sometimes confusion can often be explained by contractors moving between different groups, and the groups often sharing similar TTPs.

For now we track the two groups separately, and will detail some of their recent activity in this section, starting with an overview of both groups.

Blackfly

Aliases: **APT41, Winnti Group, Bronze Atlas, ETSO, BARIUM**

First Seen: **2010**

Malware used: **Backdoor.Winnti, Backdoor.Korplug, Trojan.Skelky, Backdoor.Slordu, Backdoor.Ghostnet, Backdoor.ShadowPad**

Infection Vector(s): **Email**

Exploits used: **CVE-2017-0199, CVE-2013-3906**

Active since at least 2010, Blackfly was initially known to primarily target organizations in the gaming industry for both financial and espionage purposes. The group is believed to use email as its infection vector. After compromising gaming organizations, the group would steal game source code, development plans, virtual game assets, user account information and private code signing keys, with the presumption that these were stolen for financial gain.

Between 2011 and 2015, private code signing certificates that were almost certainly stolen from computer game firms by Blackfly were used to sign custom malware that was then used in cyber-espionage activity carried out by Grayfly, suggesting that Blackfly had expanded from targeting game-related companies, or had links to the attackers involved in cyber espionage.

This may be what led to some vendors tracking Blackfly and Grayfly as one group. Symantec considers Blackfly to be involved in cyber crime, whereas Grayfly appears to be an arm of APT41 that is involved only in cyber espionage.

Blackfly is primarily identified by its use of the Winnti and Korplug backdoors. As well as the gaming industry, Blackfly attacks have also been aimed at the semiconductor, telecoms, materials manufacturing, pharmaceutical, media and advertising, hospitality, natural resources, fintech, and food sectors.

Grayfly

Aliases: APT41, WickedPanda, SparklingGoblin, Earth Baku

First Seen: 2017

Malware used: Backdoor.Motnug, Trojan.Chattak, Trojan.Agentemis, Backdoor.Powbearer, Alias: SIDEWALK, Hacktool.Mimikatz, Alias: StealthVector, Alias: StealthMutant, Alias: ChinaChopper, Backdoor.Cobalt, Backdoor.ShadowPad

Infection Vector(s): Exploits public-facing applications

Exploits used: CVE-2021-26855

Other tools used: Certutil; Whoami; Installutil; WMIC; BITSAdmin; CScript

Active since at least 2017, Grayfly typically targets a public facing web-server for initial intrusion, before spreading further within the network. Grayfly deploys custom backdoors on victim networks and its goal appears to be espionage. It has targeted victims in numerous countries across Asia, Europe, and North America, and has hit organizations in many different sectors. Grayfly is primarily identified by its use of the Motnug backdoor. The Sidewalk backdoor is also believed to be exclusive to the group. Grayfly has been observed on domain controllers in victim organizations, an asset that appears to be important to them.

Several overlaps between Blackfly and Grayfly activity have been observed, including:

- Malware used by Grayfly has also been seen in investigations involving the Winnti malware family traditionally associated with Blackfly.
- Grayfly malware is often signed with stolen gaming digital certificates, similar to how Blackfly operates.
- Grayfly has used customized versions of Mimikatz that overlap with Blackfly operations.
- Grayfly has used batch files to install malware as a Windows service, which Blackfly also does.

In September 2020, U.S. authorities charged seven men in relation to hundreds of cyber attacks against organizations in the U.S. and multiple other countries in Asia and Europe, and attributed the activity to APT41. Prosecutors in the U.S. charged three Chinese men – Jiang Lizhi, Qian Chuan, and Fu Qiang – with involvement in attacks we attributed to Grayfly. The trio were based in the Chinese city of Chengdu and all held senior positions in a company called Chengdu 404. The company described itself as a network security specialist and claimed to employ a team of white hat hackers who could perform penetration testing along with “offensive” and “defensive” security operations. Prosecutors also alleged that two Malaysian nationals – Wong Ong Hua and Ling Yang Ching – were involved in attacks linked to what we would term Blackfly activity. Wong is the founder and CEO of a company called Sea Gamer Mall, while Ling is its chief product officer and a shareholder. Two Chinese men – Zhang Haoran and Tan Dailin – who were charged appeared to have collaborated with both groups. The two men are both reported to have worked for a time at Chengdu 404, the company that prosecutors believe is linked to Grayfly attacks. However, they are also alleged to have collaborated with the Blackfly group in order to make additional money by mounting attacks on computer gaming companies.

Despite these significant arrests, Blackfly and Grayfly activity didn’t cease, with APT41 linked by other vendors to attacks that have occurred as recently as February 2022, while we also observed likely APT41 activity in early 2022, as detailed in our case study.

In September 2021, Symantec researchers also linked the recently discovered Sidewalk malware to the Grayfly operation. A large number of the victims in the campaign Symantec observed were in the telecoms sector in various regions, including Taiwan, Vietnam, the U.S., and Mexico. In that campaign, Grayfly appeared to be particularly interested in attacking exposed Microsoft Exchange or MySQL servers. This suggested that the initial vector may have been the exploit of multiple vulnerabilities against these public-facing servers. In at least one attack, the suspicious Exchange activity was followed by PowerShell commands used to install an unidentified web shell, and the malicious Sidewalk backdoor was then executed. After the installation of the backdoor, the attackers deployed a custom version of the credential-dumping tool Mimikatz. This version of Mimikatz had been used in previous Grayfly attacks.

Case Studies: Recent APT41 Activity

APT41 Targets Organizations in Taiwan

An APT41 campaign between April and December 2021 targeted organizations in various different sectors in Taiwan. While Symantec researchers were able to link this activity to APT41, it isn't clear whether the perpetrators of this activity belonged to either the Blackfly or Grayfly grouping, due to the frequent sharing of tools and tactics between the two groups. Taiwanese organizations are frequently targeted in attack campaigns by Chinese state-backed actors.

The victims targeted in this campaign were in the healthcare, education, manufacturing, and air transportation sectors. The motive is unclear. Both Grayfly and Blackfly are known to be involved in espionage campaigns, but Blackfly is known for carrying out financially motivated attacks too.

The first activity in this campaign was observed in April 2021, with the most recent activity seen in December 2021. While the amount of time spent on victim networks varied from days to months, in at least one case the attackers were able to maintain a presence on a victim network for as long as six months.

Links pointing to this activity being carried out by APT41 included:

The use of updated Trojan.Torutila (aka StealthVector) variants

- Several instances of updated variants of Trojan.Torutila (aka StealthVector) malware were found on victim machines. This is a known APT41 loader. According to research from Trend Micro, since October 2020 it has been used to deliver the Scramblecross/Sidewalk backdoor. However, we did not see what the final payload was in this campaign.

Domain overlap: mssetting[.]com

- This domain has previously been linked to APT41 activity.

Similar TTP: ServiceDLL as a persistence/execution mechanism

- The attackers' malicious DLL was installed as a Service DLL so that it is executed in the svchost.exe process. The service is then scheduled as a task using schtasks.exe, either to execute once or as a recurring task for persistence. This is a technique that has been reportedly in use by APT41 actors since 2020, according to reports.

Attack Chain

Typically, the first activity seen in this campaign was on a web server. In at least one instance, the attackers attempted to, and likely successfully, uploaded a web shell. A small amount of evidence on other organizations suggests the same activity occurred in those cases as well.

This was followed by the attackers downloading tools using Certutil, PowerShell, and BITSAdmin.

- **PowerShell –** a legitimate tool that can be used for a variety of malicious purposes, including executing commands directly from memory, and injecting malware into other legitimate processes. Because PowerShell has many legitimate uses it provides an ideal way for attackers to hide their malicious activity.
- **BITSAdmin –** a Microsoft command-line tool that can be used to create, download, or upload jobs and monitor their progress.
- **Certutil –** a command-line utility that can be abused for various malicious purposes, such as to decode information, to download files, and to install browser root certificates.

StealthVector appears to have been delivered via a backdoor that was loaded into memory, as it was seen in the process chain for lots of initial activity, including user and network discovery commands, downloading and moving tools, and credential theft.

Some additional tools seen being deployed in this campaign included:

- **Cobalt Strike –** deployed as a post-compromise tool in this campaign. An off-the-shelf tool, it can be used to execute commands, inject other processes, elevate current processes, or impersonate other processes, and upload and download files.
- **JuicyPotato –** an open-source privilege escalation tool.
- **IOX –** an open-source port forwarder.
- **Fast Reverse Proxy –** allows attackers to expose a local server behind a NAT or firewall to the internet by forwarding its port.
- A simple network host scanner.

Once they were on a victim network, the attackers immediately started escalating privileges on the web server using open-source tools, dumping the SAM and SYSTEM registry hives for credential theft, and using Comsvc to dump LSASS memory. They also zipped up stolen credentials and gathered discovery information, as well as attempting exfiltration using dual-use tools.

The attackers' malicious DLL was installed as a Service DLL so that it was executed in the svchost.exe process. The service was then scheduled as a task using schtasks.exe, either to execute once or as a recurring task for persistence. In one instance attackers also attempted to reach a VPN server of a victim organization.

In one victim, attackers were able to gain access to a domain controller. Once on the domain controller they used ndsutil to mount a snapshot of the domain controller, as well as dumping the SAM and SYSTEM registry hives for credential theft. StealthVector was also seen on the domain controller, where it was installed as a Service DLL to maintain persistence. In this case, it took the attackers a little over one week to make their way from the initial web server compromise to the domain controller. Grayfly is known to have shown an interest in domain controllers in previous attack campaigns.

Some of the activity carried out by the attackers in this campaign - such as zipping up data and attempting exfiltration - indicates the actors' motivation was espionage, but we cannot definitively state that was the case.

Middle Eastern Telecommunications Company Targeted

Meanwhile, a telecommunications company in the Middle East was targeted in an attack campaign that continued from mid-2021 to early 2022. While the payloads were unknown, there were some similarities and clues pointing to shared malware used by both Grayfly and Blackfly. In at least one instance, attackers accessed a system with software for mobile carrier related servers and gateways, including high availability devices to manage mobile network elements. Both custom malware and living-off-the-land tactics and techniques were deployed in this campaign.

Attack Chain

The initial infection vector used in this campaign could not be determined, but we do have good insight into the attack chain and the tools used.

DLL side-loading

- A legitimate Adobe Acrobat executable was abused to side-load malicious DLLs, which were loaders for an unknown payload.

Custom loaders

- Attackers used a set of 32- and 64-bit custom loaders to load AES-encrypted, unknown payloads in .dat files. These loaders, which are DLLs, verify system information of the infected system before they run, indicating the attackers had already obtained detailed information about the target before deploying these loaders.

Unknown payloads removed by attacker

- The .dat files containing the expected encrypted payloads were not found. Command lines executed by the attackers suggest they deleted the .dat files.

```
“cmd.exe /c del C:\ProgramData\Microsoft\Crypto\Keys\*.dat”
```

Discovery using WMI and VBS

- The attackers performed discovery against remote internal hosts using WMIC '/node:' commands, using them to enumerate network connections, display logged-on users, and gather system information. They also used several unknown VBS scripts to issue commands.

Lateral movement

- Both WMI and Schtasks were used for lateral movement. Attackers used WMI '/node' command to launch Acrobat.exe, likely to initiate the DLL side load of the loader that had been copied over.

```
“wmic /node: [HOST IP] process call create “cmd.exe /c c:\perflogs\Acrobat.exe
```

- Similarly, with Schtasks, a remote internal host was the target of a one-time scheduled task that executed Acrobat.exe.

```
“SCHTASKS /CREATE /S [TARGET HOST] /SC ONCE /TN “WindowsDemoHelp” /TR “cmd.exe
/C C:\Windows\vss\Acrobat.exe” /ST 12:30 /SD 09/08/2021”
```

Persistence via Service DLL

- To enable their malicious loader to execute persistently, attackers registered the malicious loader as a service using the ServiceDLL entry in the registry. A service was created for the loader and a ServiceDLL registry entry was added for that service. The service was added to the svchost key as a new service group so that the malicious DLL was loaded into an instance of the svchost.exe process.

  ```
  “reg add “HKLM\SYSTEM\CurrentControlSet\Services\WMPNetupdateSvc\Parameters” /v
  “ServiceDll” /t REG_EXPAND_SZ /d “CSIDL_SYSTEM\windows.media.update.dll” /f”
  ```

Defense evasion

- In addition to deleting the payload .dat files, attackers used PowerShell to ‘Timestomp’ the custom loader. They overwrote the metadata of the file to make it appear as though the file was created years earlier.

  ```
  “powershell.exe -command “ls ‘CSIDL_SYSTEM\windows.media.update.dll’ |
  foreach-object { $_.LastWriteTime = ‘07/26/2012 08:07:44’; $_.CreationTime =
  ‘07/26/2012 08:07:44’ }”
  ```

Links to Blackfly and Grayfly

Similar techniques seen in this campaign that are known to be used in shared malware associated with both Blackfly and Grayfly include:

- Similarities in the execution chain of the custom loaders to that reported in a previous McAfee report. In that report, an unknown group was using a similar execution chain to load what was suspected to be Backdoor.Winnti. However, there were some differences in the file naming scheme of payload .dat files.
- The technique of registering a Service DLL to execute the loader has been previously documented being used by APT41, as mentioned in the earlier case study.
- A legitimate BitDefender component was found alongside an Acrobat.exe file. In 2020, the same legitimate BitDefender component was reportedly used to side-load a loader for ShadowPad shellcode.

There were also various clues that the payloads may have been shared malware associated with APT41:

- One of the payloads may have been Korplug, based on indications of similar network traffic, which is known to be a tool shared by Blackfly and Grayfly.
- A little more than one month before a custom loader appeared, the same Bit-Defender component mentioned previously was used to execute an unknown DLL file suspected of being a ShadowPad loader. ShadowPad is associated with APT41. The suspected ShadowPad loader was in a subfolder where the custom loader (acrobat.dll) was also found.

While we do not see what payloads are deployed in this campaign, the targeting of a telecoms company indicates that the most likely motivation driving this campaign was espionage. This campaign was clearly highly targeted given the loaders would only run once they had verified the system information of machines, indicating that the attackers had carried out a significant amount of reconnaissance about the victim organization before carrying out this campaign. The steps taken by the attackers to try and hide their activity, including timestomping and deleting .dat files all indicate this campaign was the work of an experienced and sophisticated attacker.

Other Currently Active Chinese Threat Actors

Othorene

Aliases: **SoftCell, Gallium**

First Seen: **2018**

Malware Used: **Backdoor.Darkmoon, Alias: QuarkBandit, Backdoor.Ghostnet, Alias: PcShare, Alias: Blackmould, Hacktool.Htran**

Infection Vector(s): **Exploits public-facing applications**

Exploits Used: **CVE-2021-26855 (ProxyLogon), CVE-2021-26857, CVE-2021-27065, CVE-2021-26858**

Othorene is a cyber-espionage group that appears to be focused on surveillance of individuals. Symantec research indicates that the group is relatively small, and public reporting suggests it is optimized for low-cost, high-impact operations. Othorene does not appear to have access to custom malware, rather, its typical toolkit includes dual-use or off-the-shelf malware that has been slightly modified. However, although the group does not develop its own malware, it reportedly has access to zero-day exploits. The group was reportedly exploiting the ProxyLogon vulnerabilities before they were publicly known, indicating they may have had early knowledge of these vulnerabilities. The first group that exploited the ProxyLogon vulnerabilities was a Chinese group that Symantec tracks as Ant (aka Hafnium). Given the high degree of crossover between Chinese APT groups, it's possible that contractors working for Ant may also have worked with Othorene, possibly supplying knowledge of these vulnerabilities to Othorene. However, how Othorene gained knowledge of the ProxyLogon bugs in advance of public reporting isn't clear.

Additionally, the group's use of dual-use and common hacking tools, as well as variants of off-the-shelf malware (such as Backdoor.Ghostnet, Backdoor.Darkmoon, and PcShare), make the group's activity harder to identify. The group reportedly takes measures to prevent the detection of their malicious network traffic by modifying the communication protocols of the backdoors it uses. Othorene also installs VPN software on compromised machines, providing both a form of persistent access and a way to further disguise network traffic. The actors would then use common tools for credential theft, lateral movement, and data exfiltration, including Mimikatz, PsExec, WMI, and WinRAR.

Othorene has hit victims in the telecoms, government, and education sectors, with public reports suggesting that Othorene has targeted telecoms organizations in order to facilitate surveillance of individuals i.e. the telecoms companies' customers.

Speaking to the overlap we have noted as being a feature of Chinese APT groups, Symantec discovered potential evidence that Othorene and Blackfly use some of the same tooling. One sample of a slightly modified variant of an open-source backdoor, PcShare, was reportedly used along with a Trojanized version of the Windows Narrator utility (aka FakeNarrator). The same PcShare sample was reportedly used by Othorene, and Symantec has some evidence that the FakeNarrator sample was used by Blackfly. Other public reports have also suggested links between APT41 and Othorene, so it appears to be a possibility.

Glowworm

Aliases: **FamousSparrow**

First Seen: **2019**

Malware Used: **SparrowDoor, Hacktool.Mimikatz, Trojan.Lumibug**

Infection Vector(s): **Exploits public-facing applications**

Exploits Used: **CVE-2021-26855 (ProxyLogon)**

Other Tools Used: **ProcDump, NBTscan**

Glowworm is believed to be an espionage operation that primarily targets organizations in the hotel and travel sectors, and has access to custom malware. This includes a backdoor, SparrowDoor, and its associated loaders that are currently known to only be associated with Glowworm, as well as custom variants of Hacktool.Mimikatz. These tools also accompany renamed legitimate K7 Computing executables that are used as abused binaries for DLL search-order hijacking to load the SparrowDoor backdoor.

The group has also been observed targeting engineering, government, and international organizations, as well as law firms, though its main focus is the hospitality industry. The group's primary motive appears to be collecting personally identifiable information (PII) for intelligence purposes, with victims seen on a global scale.

Glowworm was observed in one instance to have used a variant of Backdoor.Motnug, which is primarily associated with Grayfly. In a separate instance, a domain tied to a group Trend Micro calls DRBControl was also found communicating with a machine compromised by Glowworm. DRBControl was first written about by Trend in 2020, when it was involved in attacks on gambling companies in Southeast Asia. These overlaps suggest that Glowworm may have links to other distinct China-based groups, and, in some cases, common intelligence interests. As previously demonstrated, overlap between Chinese APT groups is not unusual.

Slug

Aliases: **Owlproxy**

First Seen: **2019**

Malware Used: **Trojan.Owprox, Trojan.Orex**

Infection Vector(s): **Unknown**

Other Tools Used: **BloodHound, Cobalt Strike, Mimikatz**

In October 2020, CyCraft published details on a targeted campaign that was aimed at Taiwanese government agencies in April 2020. These attacks involved previously unseen malware called Owlproxy. Symantec subsequently identified additional elements of these attacks, which targeted Afghanistan and Vietnam, as well as Taiwan.

Slug uses custom malware called Trojan.Owprox (aka Owlproxy) during its attacks. It also uses another custom malware called Trojan.Orex. Owlproxy is used for remote access, while Trojan.Orex is used for credential theft. The group has been observed attacking organizations in the IT, education, financial, healthcare, and telecoms sectors. The use of shared tools led CyCraft to conclude that Slug was likely a state-sponsored APT group originating from China. The targeting of victims linked to the Taiwanese government is also consistent with the targeting patterns of Chinese actors.

Owlproxy was also seen in two instances being used alongside the sophisticated Daxin backdoor that we discuss in one of our case studies.

Kelp

Aliases: **GhostEmperor**

First Seen: **2020**

Malware Used: **Alias: Kelpdoor**

Infection Vector(s): **Exploits public-facing applications**

Other Tools Used: **Netscan; Mimikatz; Shellcode launcher; PowerShell; Batch scripts; Enum tool; Powersploit**

Kelp activity has been identified by the use of its custom backdoor, Kelpdoor, in the following location:

```
C:\ProgramData\Microsoft\Network\Connections\msdecode.dll
```

Kelpdoor is a backdoor that provides remote control capabilities as well as the ability to launch arbitrary .NET-based payloads and PowerShell scripts.

Kelp uses a combination of custom malware and dual-use tools in its operations, and has targeted government, hospitality, and telecoms organizations in countries including Afghanistan, Singapore, and Vietnam.

Kelp and Squash (profiled next) are known to share a packer for their malware. They may be the same group and are both tracked by Kaspersky as GhostEmperor. However, Symantec identified two distinct sets of activity that could not be linked other than the shared packer, so for now we are tracking the two as separate groups. We may revise this in the future if we find further evidence that they are the same group. In both cases, the groups are believed to be Chinese, state-backed operators.

Squash

Aliases: **GhostEmperor**

First Seen: **2020**

Malware Used: **Alias: Demodex**

Infection Vector(s): **Exploits public-facing applications**

Other Tools Used: **PowerShell; Mimikatz; Scheduled tasks; Credential theft; FTP server; Archiving; Timestomping**

Squash uses a mix of custom malware and dual-use tools in its operations. Industries that have been targeted by the group include aviation, military, and telecoms, in countries including Afghanistan, India, and Thailand.

Squash is notable for using a distinctive file name for its custom malware:

- msmp4dec.dll

However, as this name has been publicly reported it is likely the group has now changed it.

Symantec has observed the group using PowerShell for decoding from the registry and launching malware. As well as the tools that Symantec has seen the group using, Kaspersky also reported seeing the group use additional tools including:

- Powercat
- Ladon
- Get-PassHashes
- GetPwd
- Token.exe
- NBTscan
- Pslist
- ProcDump

Kaspersky also said it saw Squash activity in Egypt and Ethiopia.

Squash and Kelp (profiled previously) are known to share a packer for their malware. They may be the same group and are both tracked by Kaspersky as GhostEmperor. However, Symantec identified two distinct sets of activity that could not be linked other than the shared packer, so for now we are tracking the two as separate groups. We may revise this in the future if we find further evidence that they are the same group. In both cases, the groups are believed to be Chinese, state-backed operators.

Cicada

Aliases: **APT10, Stone Panda, Bronze Riverside, Chessmasters, Menupass, CVNX, Red Apollo, Potassium, Bond, TA429**

First Seen: **2009**

Malware Used: **Backdoor.Chches, Backdoor.Darkmoon, Backdoor.Korplug, Backdoor.Vidgrab, Trojan.Agentemis, Trojan.Redleavy, Trojan.Wimhop, Backdoor.Leenania, Backdoor.Hartip, Alias: Sodamaster**

Infection Vector(s): **Emails, Supply-Chain Attacks, Watering-Hole Attacks**

Exploits Used: **CVE-2009-4324, CVE-2010-2883, CVE-2010-3333, CVE-2011-0611, CVE-2020-1472**

Other Tools Used: **Netsess, Tcping, PsExec, Csvde, Cobalt Strike**

Cicada has been active since at least 2009, and is believed to be involved in espionage-type operations. Cicada traditionally customized publicly available malware in concert with dual-use tools during operations. The group leverages a number of techniques during the initial stages of attack, such as targeted email, strategic website compromise, and supply-chain attacks. Cicada targeted managed service providers in 2016/2017, which indicated they are a well-resourced group and are willing to go to great lengths in order to compromise their intended targets.

Although not exclusively, since 2016, Cicada appeared to have a focus on targeting organizations in Japan across numerous sectors including government, media, research, and transport. Cicada leverages malware and delivery frameworks traditionally associated with espionage operations by APT groups believed to be of Chinese origin.

In 2020, Symantec published a blog about a large-scale Cicada attack campaign that was targeting multiple Japanese companies, including subsidiaries located in as many as 17 regions around the globe in a likely intelligence-gathering operation. Companies in multiple sectors were targeted in this campaign, including those operating in the automotive, pharmaceutical, and engineering sector, as well as managed service providers (MSPs), which Cicada has a history of targeting. Cicada compromised some companies for as long as a year during this campaign, and used a large number of living-off-the-land, dual-use, and publicly available tools and techniques in these attacks, including:

- **Network Reconnaissance –** gathering information from machines on the network.
- **Credential Theft –** stealing user names and passwords, potentially to provide them with further access to the victim network.
- **RAR archiving –** files are transferred to staging servers before exfiltration. They may be encrypted or compressed, to make them easier to extract.
- **Certutil –** a legitimate command-line utility that can be used for various malicious purposes, such as to decode information, to download files, and to install browser root certificates.
- **AdFind –** a command-line tool that can be used to perform Active Directory queries.
- **Csvde –** can be used to extract Active Directory files and data.
- **Ntdsutil –** can be used as a credential-dumping tool.
- **WMIExec –** can be used for lateral movement and to execute commands remotely.
- **PowerShell –** a powerful interactive command-line interface and scripting environment included in the Windows operating system. It can be used to find information and execute code, and is frequently abused by malicious actors.

A more recent campaign saw Cicada widen its targeting, as detailed in the following case study.

Case Study

Cicada Widens Targeting in Recent Espionage Activity

Victims in a recent Cicada campaign appear to point to a widening of the group's activity. They included government, legal, religious, and non-governmental organizations (NGOs) in multiple countries around the world, including in Europe, Asia, and North America. The wide number of sectors and geographies of the organizations targeted in this campaign is interesting, given Cicada's previous heavy focus on Japanese-linked companies, and also MSPs with a more global footprint. This campaign appears to indicate a further widening of Cicada's targeting.

The attribution of this activity to Cicada was based on the presence on victim networks of a custom loader and custom malware that are believed to be exclusively used by the APT group.

The earliest activity in this current campaign occurred in mid-2021, with the most recent activity seen in February 2022.

Activity on infected networks

In several cases, the initial activity on victim networks was seen on Microsoft Exchange Servers, suggesting the possibility that a known, unpatched vulnerability in Microsoft Exchange may have been used to gain access to victim networks in some cases.

Once the attackers successfully gained access to victim machines they deployed various different tools, including a custom loader and the Sodamaster backdoor. The loader deployed in this campaign was also deployed in a previous Cicada attack.

Sodamaster is a known Cicada tool that is believed to be exclusively used by this group. It is a fileless malware that is capable of multiple functions, including evading detection in a sandbox by checking for a registry key or delaying execution; enumerating the username, hostname, and operating system of targeted systems; searching for running processes, and downloading and executing additional payloads. It is also capable of obfuscating and encrypting traffic that it sends back to its command-and-control (C&C) server. It is a powerful backdoor that Cicada has been using since at least 2020.

In this campaign the attackers are also seen dumping credentials, including by using a custom Mimikatz loader. The attackers also abused the legitimate VLC Media Player by launching a custom loader via the VLC Exports function, and used the WinVNC tool for remote control of victim machines.

Other tools utilized in this attack campaign included a RAR archiving tool, System/Network discovery, WMIExec, and NBTScan.

The victims in this campaign were primarily government-related institutions or NGOs, with some of these NGOs working in the fields of education and religion. There were also victims in the telecoms, legal, and pharmaceutical sectors. The victims were spread through a wide number of regions including the U.S., Canada, Hong Kong, Turkey, Israel, India, Montenegro, and Italy. There was also just one victim in Japan, which is notable due to Cicada's previous strong focus on Japanese-linked companies.

The attackers spent as long as nine months on the networks of some victims.

The victims targeted, the various tools deployed in this campaign, and what we know of Cicada's past activity all indicate that the most likely goal of this campaign was espionage. Cicada activity was linked by U.S. government officials to the Chinese government in 2018.

Budworm

Aliases: **Emissary Panda, Lucky Mouse, Bronze Union, Iron Tiger, APT27, Iodine, Wekby 2.0**

First Seen: **2013**

Malware Used: **Backdoor.Korplug (PlugX), Trojan.Browrat, Alias: Hyperbro. Backdoor.Owashell (aka OwaAuth), Alias: Sybersyringe**

Infection Vector(s): **Email, Watering holes, Public-facing exploits**

Exploits Used: **CVE-2015-5119, CVE-2013-3906, CVE-2021-40539, CVE-2021-26855 (ProxyLogon)**

Other tools Used: **WinCredEd, GsecDump, Hunter, NBTscan, WinRAR**

Budworm is a Chinese-state-backed attack group that has been active for a long time, with activity attributed to this group having first been spotted in 2013. The group has been linked to attacks on multiple different sectors in numerous countries.

As well as the malware listed in this profile, Budworm is known to use China Chopper web shells in its attacks, which are frequently leveraged by China-linked groups for remote access. The OwaShell malware can be used for remote access on Microsoft Exchange Servers, which appear to be of interest to China-based actors. More recently the group has leveraged the ProxyLogon vulnerabilities in Microsoft Exchange Server, as well as vulnerabilities in enterprise password management solution Zoho Manage Engine ADSelfService Plus (CVE-2021-40539) to gain initial access to victim networks.

In January 2022, Germany's domestic intelligence service, the BfV, issued a warning about Budworm carrying out ongoing attacks on German businesses. The BfV said the attackers were using the HyperBro remote access Trojan (RAT) for backdoor access on targeted networks, likely for espionage purposes. However, it did also say some of the victims may have been targeted as part of a supply-chain attack.

Sheathminer

Aliases: **APT31, Zirconium, Judgement Panda, RedBravo**

First Seen: **2017**

Malware Used: **Alias: Trochlius**

Infection Vector(s): **Emails, Trusted relationship**

Exploits Used: **CVE-2017-0005**

Sheathminer uses custom malware to target individuals, IT, and MSPs in Europe and the U.S. to reach targets of interest. The group is known to use spear phishing, credential harvesting, and abusing trusted relationships as infection vectors. The group is also known for using legitimate cloud services for malicious purposes, with a report from Google in 2020 revealing that Sheathminer had used GitHub to host malware, and Dropbox for its C&C infrastructure.

The group has been linked to multiple attacks on government targets. It was linked to an attack on the Norwegian parliament in 2018, an attack on the Finnish parliament in 2020, as well as attempted attacks during the 2020 U.S. Presidential Election campaigns.

Also, in July 2021, the French national cyber security agency issued a warning about an ongoing series of attacks against a large number of French organizations carried out by Sheathminer. The agency said that Sheathminer used a network of compromised home routers as operational relay boxes in order to perform stealth reconnaissance and attacks in that campaign.

Antlion

Aliases: **Tropic Trooper, Keyboy, APT23, Iron**

First Seen: **2011**

Malware Used: **Backdoor.Kboy, Downloader.Picproot, Trojan.FakeInstall, Trojan.Yahamam, Alias: xPack, Alias:JpgRun, Alias: EHAGBPSL, Alias:CheckID, Alias: MMC, Alias: NetSessionEnum**

Infection Vector(s): **Emails, Public-facing exploits**

Exploits Used: **CVE-2018-0802, CVE-2017-11882, CVE-2017-0199, CVE-2014-1761, CVE-2012-0158, CVE-2010-3333, CVE-2019-1458, CVE-2017-0147**

Other Tools Used: **WinCredEd, AsyncRAT, CreateProcessAsUser, frp, JuicyPotato, WMICCmd, Ladpon, RDPScan, Mimikatz**

Antlion has been active since at least 2011 and is believed to primarily be engaged in cyber-espionage activities. Antlion has targeted victims in the government, healthcare, media, military, technology, and transport sectors, as well as activist groups. The group uses a combination of publicly available code and custom malware during operations, and is known to use both email and exploits in public-facing applications to gain initial access to victim networks.

While Antlion has targeted organizations in several different parts of Asia, including Tibet, Hong Kong, India, the Philippines, and Vietnam, in 2020 and 2021 it appeared to be primarily focused on targeting organizations in Taiwan. This activity was notable for the extended period of time Antlion spent on victim machines. One of these campaigns is detailed in the following case study, where we detail a campaign that targeted organizations in the manufacturing and finance sectors in Taiwan over a period of 18 months.

Case Study:
Antlion Uses Custom Backdoor to Target Financial Institutions in Taiwan

In a blog we published in February 2022, we detailed how Antlion had been targeting financial institutions in Taiwan in a persistent campaign for at least 18 months.

The attackers deployed a custom backdoor we have called xPack on compromised systems, which gave them extensive access to victim machines. The backdoor allowed the attackers to run WMI commands remotely, while there was also evidence that they leveraged EternalBlue exploits in the backdoor. The attackers appeared to have the ability to interact with SMB shares, and it was possible that they used mounted shares over SMB to transfer files from attacker-controlled infrastructure. There was also evidence that the attackers were able to browse the web through the backdoor, likely using it as a proxy to mask their IP address.

The goal of this campaign appears to have been espionage, as we saw the attackers exfiltrating data and staging data for exfiltration from infected networks.

Technical details

Antlion compromised at least two financial organizations and a manufacturing company in Taiwan during this campaign. The xPack backdoor was deployed frequently in all three victims, while there was also a lot of evidence of credential dumping. In the manufacturing target, also, we saw the attackers attempting to download malicious files via SMB shares.

The attackers also spent a significant amount of time on both these targeted networks, spending close to 250 days on the network of one financial organization, nine months on the network of another, and around 175 days on the manufacturing organization.

We were unable to definitively determine the initial infection vector used in these attacks, but in one instance the attackers were seen utilizing the MSSQL service to execute system commands, which indicates that the most likely infection vector was exploitation of a web application or service. However, Antlion is also known to have previously used malicious emails to gain initial access to victim networks.

The main custom backdoor used by Antlion in this campaign was the xPack backdoor, which is a custom .NET loader that decrypts (AES), loads, and executes accompanying .bin files. Its decryption password is provided as a command-line argument (Base64 encoded string), and xPack is intended to be run as a standalone application or as a service (xPackSvc variant). The xPack malware and its associated payload seem to be used for initial access; it appears that xPack was predominantly used to execute system commands, drop subsequent malware and tools, and stage data for exfiltration. The attackers also used a custom keylogger and three custom loaders.

- EHAGBPSL loader - custom loader written in C++ - loaded by JpgRun loader
- JpgRun loader - custom loader written in C++ - similar to xPack, reads the decryption key and file name from the command line - decodes the file and executes it
- CheckID - custom loader written in C++ - based on loader used by BlackHole RAT
- The attackers also used a custom SMB session enumeration tool (NetSessionEnum), a custom bind/reverse file-transfer tool named ENCODE MMC, and a Kerberos golden ticket tool based on Mimikatz

The attackers also used a variety of off-the-shelf tools, as well as leveraging living-off-the-land tools such as PowerShell, WMIC, ProcDump, LSASS, and PsExec. The legitimate AnyDesk tool was also abused by the attackers for remote access in one of the victim organizations. The attackers were also observed leveraging exploits such as CVE-2019-1458 for privilege escalation and remote scheduled tasks to execute their backdoor. CVE-2019-1458 is an elevation-of-privilege vulnerability that occurs in Windows when the Win32k component fails to properly handle objects in memory.

Legitimate versions of WinRAR appear to have been abused by the attackers for data exfiltration, while there is also evidence of data exfiltration via PowerShell, specifically using the BitsTransfer module to initiate an upload to attacker-controlled infrastructure. There is also evidence that the attackers likely automated the data collection process via batch scripts, while there is also evidence of instances where data was likely staged for further exfiltration, though it was not actually observed being exfiltrated from the network. In these instances, it appears the attackers were interested in collecting information from software pertaining to business contacts, investments, and smart card readers.

The length of time that Antlion was able to spend on victim networks in this campaign is notable, with the group able to spend several months on victim networks, affording plenty of time to seek out and exfiltrate potentially sensitive information from infected organizations. The most recent activity in this campaign was seen in September 2021.

Daxin: Super-stealthy Malware Leveraged by China-backed Actors

One of the most significant findings we have made about China-based actors in the last year is the discovery of Daxin, the most advanced piece of malware we have ever seen being used by China-backed actors.

Daxin exhibits technical complexity previously unseen in malware used by such actors. It appears to have been used in a long-running espionage campaign against select governments and other critical infrastructure targets.

There is strong evidence that Daxin, which allows the attacker to perform various communications and data-gathering operations on the infected computer, has been used as recently as November 2021 by attackers linked to China. Most of the targets appear to be organizations and governments of strategic interest to China, and other tools associated with Chinese espionage actors were found on some of the same computers where Daxin was deployed.

Considering its capabilities and the nature of its deployed attacks, Daxin appears to be optimized for use against hardened targets, allowing the attackers to burrow deep into a target's network and exfiltrate data without raising suspicions. Symantec researchers worked with the Cyber Security and Infrastructure Security Agency (CISA) to engage with multiple foreign governments targeted with Daxin and assisted in detection and remediation.

Daxin arrives on victim machines in the form of a Windows kernel driver, a relatively rare format for malware nowadays. It implements advanced communications functionality, which both provides a high degree of stealth and permits the attackers to communicate with infected computers on highly secured networks, where direct internet connectivity is not available. These features are reminiscent of Regin, an advanced espionage tool discovered by Symantec in 2014 that others have linked to Western intelligence services.

Daxin's capabilities suggest the attackers invested significant effort in developing communication techniques that can blend in unseen with normal network traffic on the target's network. Specifically, the malware avoids starting its own network services. Instead, it can abuse any legitimate services already running on the infected computers.

Daxin is also capable of relaying its communications across a network of infected computers within the attacked organization. The attackers can select an arbitrary path across infected computers and send a single command that instructs these computers to establish requested connectivity. This use case has been optimized by Daxin's designers. Daxin also features network tunneling, allowing attackers to communicate with legitimate services on the victim's network that can be reached from any infected computer.

Daxin: Technical details

Daxin is a backdoor that allows the attacker to perform various operations on the infected computer such as reading and writing arbitrary files. The attacker can also start arbitrary processes and interact with them. While the set of operations recognized by Daxin is quite narrow, its real value to attackers lies in its stealth and communications capabilities.

Daxin is capable of communicating by hijacking legitimate TCP/IP connections. In order to do so, it monitors all incoming TCP traffic for certain patterns. Whenever any of these patterns are detected, Daxin disconnects the legitimate recipient and takes over the connection. It then performs a custom key exchange with the remote peer, where two sides follow complementary steps. The malware can be both the initiator and the target of a key exchange. A successful key exchange opens an encrypted communication channel for receiving commands and sending responses. Daxin's use of hijacked TCP connections affords a high degree of stealth to its communications and helps to establish connectivity on networks with strict firewall rules. It may also lower the risk of discovery by SOC analysts monitoring for network anomalies.

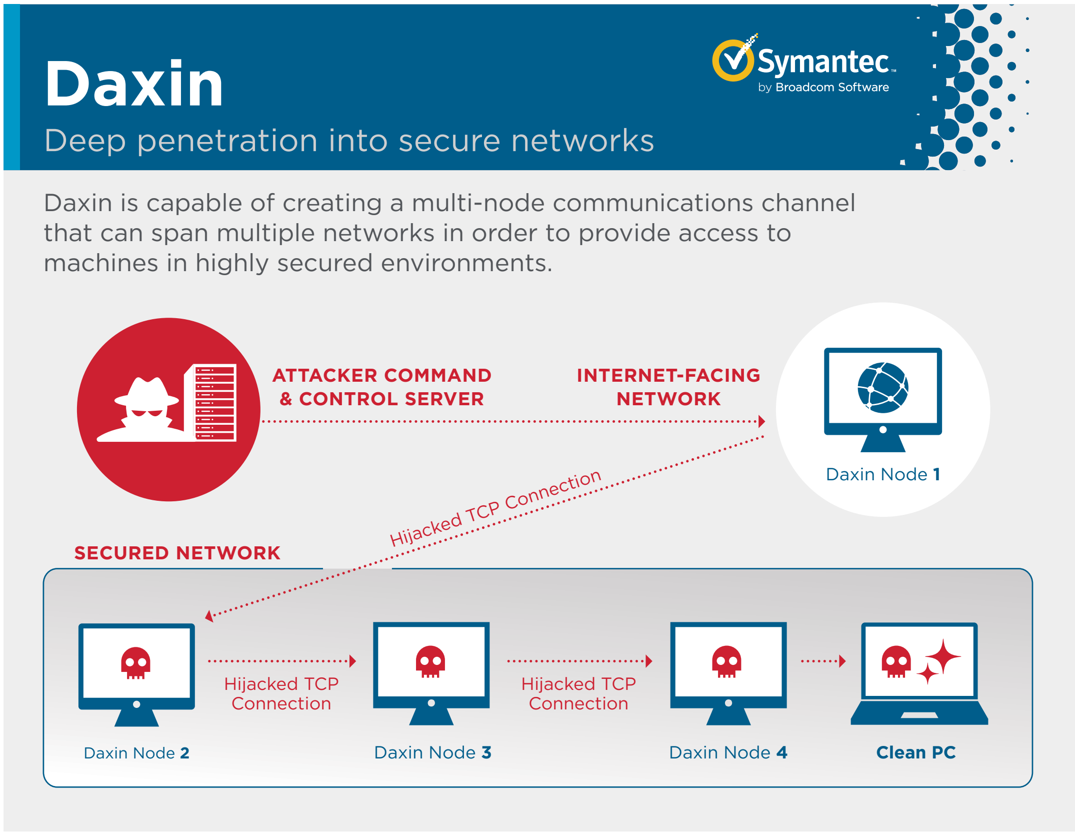
Daxin's built-in functionality can be augmented by deploying additional components on the infected computer. Daxin provides a dedicated communication mechanism for such components by implementing a device named \\.\Tcp4. The malicious components can open this device to register themselves for communication. Each of the components can associate a 32-bit service identifier with the opened \\.\Tcp4 handle. The remote attacker is then able to communicate with selected components by specifying a matching service identified when sending messages of a certain type. The driver also includes a mechanism to send back any responses.

There are also dedicated messages that encapsulate raw network packets to be transmitted via the local network adapter. Daxin then tracks network flows, such that any response packets are captured and forwarded to the remote attacker. This allows the attacker to establish communication with legitimate services that are reachable from the infected machine on the target's network, where the remote attacker uses network tunnels to interact with internal servers of interest.

Perhaps the most interesting functionality is the ability to create a new communications channel across multiple infected computers, where the list of nodes is provided by the attacker in a single command. For each node, the message includes all the details required to establish communication, specifically the node IP address, its TCP port number, and the credentials to use during custom key exchange. When Daxin receives this message, it picks the next node from the list. Then it uses its own TCP/IP stack to connect to the TCP server listed in the selected entry. Once connected, Daxin starts the initiator side protocol. If the peer computer is infected with Daxin, this results in opening a new encrypted communication channel. An updated copy of the original message is then sent over this new channel, where the position of the next node to use is incremented. The process then repeats for the remaining nodes on the list.

While it is not uncommon for attackers' communications to make multiple hops across networks in order to get around firewalls and generally avoid raising suspicions, this is usually done step-by-step, such that each hop requires a separate action. However, in the case of Daxin, this process is a single operation, suggesting the malware is designed for attacks on well-guarded networks, where attackers may need to periodically reconnect into compromised computers.

Figure 1. How Daxin can create stealthy communications channels in order to interact with computers on highly secured networks.



Daxin

Deep penetration into secure networks

Daxin is capable of creating a multi-node communications channel that can span multiple networks in order to provide access to machines in highly secured environments.

Timeline

While the most recent known attacks involving Daxin occurred in November 2021, the earliest known sample of the malware dates from 2013 and included all of the advanced features seen in the most recent variants, with a large part of the codebase having already been fully developed. This suggests that the attackers were already well established by 2013, with Daxin features reflecting their expertise at that time.

We believe that before commencing development of Daxin, the attackers were already experimenting for some time with the techniques that became part of Daxin. An older piece of malware – Backdoor.Zala (aka Exforel) – contained a number of common features but did not have many of Daxin's advanced capabilities. Daxin appears to build on Zala's networking techniques, reusing a significant amount of distinctive code and even sharing certain magic constants. This is in addition to a certain public library used to perform hooking that is also common between some variants of Daxin and Zala. The extensive sharing indicates that Daxin designers at least had access to Zala's codebase. We believe that both malware families were used by the same actor, which became active no later than 2009.

Links to Known Espionage Actors

There are several examples of attacks where tools known to be associated with Chinese espionage actors have been observed along with what we believe to be variants of Daxin.

In a November 2019 attack against an information technology company, the attackers used a single PsExec session to first attempt to deploy Daxin before then resorting to Trojan.Owprox. Owprox is associated with the Slug (aka Owlproxy) group. In May 2020, malicious activity involving both Backdoor.Daxin and Trojan.Owprox also occurred on a single computer belonging to another organization, a technology company.

Daxin is without doubt the most advanced piece of malware Symantec researchers have seen used by a China-linked actor. Further in-depth technical analysis of Daxin can be found in our two deep-dive blogs:

- Daxin Backdoor: In-Depth Analysis, Part One
- Daxin Backdoor: In-Depth Analysis, Part Two

Conclusion

China continues to be a major player in the world of cyber espionage, and it is apparent that groups operating out of China still have a lot of firepower behind their activities.

The development of the Daxin backdoor would have taken a significant amount of resources and skills over a long period of time that would generally only be available to nation-state-backed groups. The Cicada activity, detailed in our case study, also points to that group widening its targeting and expanding its activity in a campaign that targeted multiple large organizations in different geographies at the same time. This points to a group that is still well-resourced and highly skilled, almost 15 years after its activity was first spotted. It's clear many of the groups operating out of China still have a lot of resources and skills behind them.

The geo-political situation in the world at present may also affect the activity we see coming from China in the future. China has been mooted as an ally of Russia since that country's invasion of Ukraine, though authorities in China have not made the country's stance on the matter entirely clear. There has been a report of a Chinese attack group hitting organizations in Ukraine since the invasion started, but it isn't clear if there were any real links between that incident and the ongoing invasion. However, the instability and upheaval that is likely to continue due to the ongoing Russian invasion is likely to continue to impact the world – including the cyber world – for some time to come. If Russia's invasion of Ukraine, combined with international sanctions, impacts Russia's malicious cyber activity it may be an opportunity for China to become an even more powerful operator in the world of malicious cyber actors.

Protection

How Symantec Solutions Can Help

Symantec, a division of Broadcom, provides a comprehensive portfolio of security solutions to address today's security challenges and protect data and digital infrastructure from multifaceted threats. These solutions include core capabilities designed to help organizations prevent and detect advanced attacks.

Symantec Endpoint Security Complete
Symantec Endpoint Security Complete (SESC) was specifically created to help protect against advanced attacks. While many vendors offer EDR to help find intrusions, there are gaps. We call these gaps blind spots and there are technologies in SESC to eliminate them.
LEARN MORE

Symantec Data Center Security
Symantec Data Center Security (DCS) System and Application hardening prevents zero-day threats against data center workloads such as Microsoft Exchange. Protected Application control and Application isolation provide runtime protection for your mission critical servers and secure application data from known and unknown threats, while the File and System integrity monitoring provide full visibility into any configuration drifts.
LEARN MORE

Privileged Access Management (PAM)
PAM is designed to prevent security breaches by protecting sensitive administrative credentials, controlling privileged user access, proactively enforcing security policies and monitoring and recording privileged user activity.
LEARN MORE

Symantec Web Isolation
Symantec Web Isolation eliminates web threats and solves the challenge of providing access to unknown, uncategorized and potentially risky web sites by creating a remote execution environment between an agency's enterprise systems and content servers on the web.
LEARN MORE

Symantec Secure Web Gateway (SWG)
SWG delivers high-performance on-premises or cloud secure web gateway that organizations can leverage to control or block access to unknown, uncategorized, or high-risk web sites.
LEARN MORE

Symantec Intelligence Services
Symantec Intelligence Services leverages the Symantec Global Intelligence Network to deliver real-time threat intelligence to several Symantec network security solutions including Symantec Secure Web Gateway, Symantec Content Analysis, Symantec Security Analytics, and more.
LEARN MORE

Symantec Content Analysis with Advanced Sandboxing
Within the Symantec Content Analysis platform, zero-day threats are automatically escalated and brokered to Symantec Malware Analysis with dynamic sandboxing for deep inspection and behavioral analysis of potential APT files and toolkits.
LEARN MORE

Symantec Security Analytics
Symantec Security Analytics delivers enriched, full-packet capture for full network traffic analysis, advanced network forensics, anomaly detection, and real-time content inspection for all network traffic to arm incident responders for quick resolution.
LEARN MORE

Mitigation

Symantec recommends customers observe the following best practices to protect against targeted attacks.

Local Environment:

- Monitor the use of dual-use tools inside your network.
- Ensure you have the latest version of PowerShell and you have logging enabled.
- Restrict access to RDP Services. Only allow RDP from specific known IP addresses and ensure you are using multi-factor authentication (MFA).
- Implement proper audit and control of administrative account usage. You could also implement one-time credentials for administrative work to help prevent theft and misuse of admin credentials.
- Create profiles of usage for admin tools. Many of these tools are used by attackers to move laterally undetected through a network.
- Use application whitelisting where applicable.
- Locking down PowerShell can increase security, for example with the constrained language mode.
- Make credential dumping more difficult, for example by enabling credential guard in Windows 10 or disabling SeDebugPrivilege.
- MFA can help limit the usefulness of compromised credentials.
- Create a plan to consider notification of outside parties. In order to ensure correct notification of required organizations, such as the FBI or other law enforcement authorities/agencies, be sure to have a plan in place to verify.
- Create a "jump bag" with hard copies and archived soft copies of all critical administrative information. In order to protect against the compromise of the availability of this critical information, store it in a jump bag with hardware and software needed to troubleshoot problems. Storing this information on the network is not helpful when network files are encrypted.

Email:

- Enable MFA to prevent the compromise of credentials during phishing attacks.
- Harden security architecture around email systems to minimize the amount of spam that reaches end-user inboxes and ensure you are following best practices for your email system, including the use of SPF and other defensive measures against phishing attacks.

Backup

- Implement offsite storage of backup copies. Arrange for offsite storage of at least four weeks of weekly full and daily incremental backups.
- Implement offline backups that are onsite. Make sure you have backups that are not connected to the network to prevent them from being encrypted by ransomware.
- Verify and test your server-level backup solution. This should already be part of your Disaster Recovery process.
- Secure the file-level permissions for backups and backup databases. Don't let your backups get encrypted.
- Test restore capability. Ensure restore capabilities support the needs of the business.

Indicators of Compromise (IOCs)

These IOCs relate to the Recent APT41 Activity case studies, as this was previously unpublished information and the IOCs for those attacks have not been shared publicly before. IOCs relating to the other case studies contained in this whitepaper can be found in our public blogs, which are linked in the Further Reading section.

SHA256	Description	Protection
2df1b99237780ca62e6a570413c9277346a1431ffde019a2954f11456f9c2b73	Trojan.Torutila	Trojan.Torutila
904888c833709f1d10f84e0148fadae1c2e805159d8d7c66c4a9fb6bf2f47b88	Trojan.Torutila	Trojan.Torutila
21c91d7b0b8537126b38bb7d85b44ab2878326680ef8a0fb1d78213809ee85f6	Trojan.Torutila	Trojan.Torutila
0c13b1b7c84c9b37b3d189d9b0e3f7639a559ae54533768d473279c849ab0eeb	Trojan.Torutila	Trojan.Torutila
32d2a3c56cb247a985147edab4e0f485a7e56999c65aaf7c13fe5494c2540dc2	Trojan.Torutila	Trojan.Torutila
d7491d9746ae6c6bd08938972cb679ba66835991545b266d2cda9239552ab155	Trojan.Torutila	Trojan.Torutila
a66daf5a8e43ed37f31478c77e14241e289fa43425addaecbf90a1b925332d88	Trojan.Torutila	Trojan.Torutila
c56faba92264d88f8da8a7ec23225186db28c01474a3888b416f67e070136696	Trojan.Torutila	Trojan.Torutila
6424c21769312d52fdb773ae0aae95169ad1da75a35525b7829637b0e9d80425	Trojan.Torutila	Trojan.Torutila
c4d065b0a6bbdccfa37a30b01ee22a06474ef41deb07500a29a5c83707bb5847	Trojan.Torutila	Trojan.Torutila
b62fa2268a346ae585188e854682883eab7d09fd19c800d2a05916600780180a	Trojan.Torutila	Trojan.Torutila
55b9264bc1f665acd94d922dd13522f48f2c88b02b587e50d5665b72855aa71c	FastReverseProxy	Grayware
beeb11da52fb81320473e1cfa983dfe50316387af15256bd61d442e77b14e9f6	Iox open-source port-forwarding tool	Hacktool
f0761ad307781bdf8da94765abd1a2041ac12a52c7fdde85f00b2b2cab6d6ce8	JuicyPotato	Hacktool
a96c690bd7b3dc8a96130a3364423a0d5a3da8d2f19fbcdd827c8985e1e81f3c	Backdoor.Cobalt	Backdoor.Cobalt!gm1
7b443cfbdea1fd36fba53e1ebf5f574dfa66dd0044ab22b3994824a6f83e7b96	Backdoor.Cobalt	Backdoor.Cobalt!gm1
10ac71ce245be61a137ee093c87a1aa906d2976669958b208834647f4273cb8c	Loader	Trojan Horse
b32040e7daa64b4c0d57742e3bae65ecad3391a871c7e43fecb4da5a36eaa9ef	Loader	Trojan Horse
3f5c07239be5dd4e86181993705cf4e8e8bfc4e3a90bf764c04ca3223363b233	Loader	Trojan Horse
f2c60e54409ea9dfa8f1db3378524ed612a4495c46a1515daa179aee911ab20f	Loader	Trojan Horse
f023f791e6433d1690ae7667a10a9e3b85fde4430db45674d7d459685bea69b1	Loader	Trojan Horse
18fc8fe5f71a123315b5594fe868be51e16f1719320647459de7df24f37d1231	Loader	Trojan Horse
37c1159876e7e6765b639df0b6067087381a7fe42ec98f7df1e09d895f4be953	Loader	Trojan Horse
59f716bf19ff87b40e556c1bdef71fe68bee1125ade927b5ebfd30b7353539e9	Loader	Trojan Horse
6571162cf69e395eacbdca90d85268bb4cfa275e88ad68c43b7ecd215a91fdd6	Loader	Trojan Horse
a3e988c5f802f034a47548044afeebefb200a6e124b7d6234939bb93a6b8883c	Loader	Trojan Horse
d59add525d6aee18d549799abed0ae8b7fae278084f42abfbd6509f98391103b	Loader	Trojan Horse
ead908082f49514d7652feb8b494e57d4d1e6f526b76427cd10423caff786685	Loader	Trojan Horse
86c7323e442c07704f089c2557a4654eee3155acd8f72902fc9184cacae9cb39	Loader	Trojan Horse
ff512fabece2be4bd6c0100a767a6c557d5656b3d1cf15086c397615cc44c9dc	Process Minidump tool	PwDump

IP/URL	Description
45.137.155[.]165	Used for file/tool delivery
www.mssetting[.]com	Used for file/tool delivery
185.244.140[.]217	Used for file/tool delivery
185.141.25[.]222	Used for file/tool delivery as well as webshell upload
www.chromenu[.]com	Used for file/tool delivery as well as webshell upload

Further Reading

- Cicada: Chinese APT Group Widens Targeting in Recent Espionage Activity
- Antlion: Chinese APT Uses Custom Backdoor to Target Financial Institutions in Taiwan
- Daxin: Stealthy Backdoor Designed for Attacks Against Hardened Networks
- Daxin Backdoor: In-Depth Analysis, Part One
- Daxin Backdoor: In-Depth Analysis, Part Two

About Us

Broadcom Software is one of the world's leading enterprise software companies, modernizing, optimizing, and protecting the world's most complex hybrid environments. With its engineering-centered culture, Broadcom Software is building a comprehensive portfolio of industry-leading infrastructure and security software, including AIOps, Cybersecurity, Value Stream Management, DevOps, Mainframe, and Payment Security. Our software portfolio enables innovation, agility, and security for the largest global companies in the world.

For more information, visit our website at: software.broadcom.com