WHITE PAPER

Relentless Force: China-Linked Espionage Actors

An Analysis from the Symantec® Threat Hunter Team

WHITE PAPER

Relentless Force: China-Linked Espionage Actors

An Analysis from the Symantec® Threat Hunter Team

TABLE OF CONTENTS

Introduction

China has long been home to some of the most significant adversaries in cyberspace, maintaining a huge and highly active espionage capability.

The scale of Chinese actors' operations is evidenced by the number of distinct groups that appear to be operating from the country. Chinese actors are targeting everything from economic espionage of organizations large and small, to domestic opposition groups and local non-governmental organizations (NGOs), to regional neighbors, to strategic rivals such as the U.S., including national critical infrastructure.

Monitoring Chinese actors presents several unique challenges. China-linked groups frequently share tools and infrastructure, making attribution to a single actor difficult. Frequent overlap in recent activity clusters may also suggest personnel changes, reorganization, or the use of contractors.

The key findings of this paper include:

- The degree of overlap between China-linked groups is increasing, which sometimes makes attributing activity with high confidence to one specific group difficult.
- While tools such as PlugX and ShadowPad are shared among multiple groups, several Chinese actors such as Budworm, Daggerfly, and Billbug continue to develop malware that is exclusive to them.
- China-linked actors are increasingly targeting multiple platforms rather than focusing on Windows-based environments.

Daggerfly

Aliases: Evasive Panda, Bronze Highland, StormBamboo

First seen: 2014

Malware used: Alias: MgBot, Backdoor.Korplug (PlugX)

Infection vectors: Emails, update hijacks, exploitation of public-facing applications

Exploits used: CVE-2012-0158

Other tools used: AnyDesk

Key developments: Creation of threats capable of targeting multiple platforms, including Windows, Linux, macOS, Android, iOS, and Solaris

Daggerfly has been active since at least 2014. At that time, VirusTotal wrote about how the group had disguised its backdoor as a legitimate MP3 encoder library and used CVE-2012-0158 to drop its Trojan. In 2020, this 2014 activity was linked by Malwarebytes to an MgBot campaign. Similarities were observed in tactics, techniques, and procedures (TTPs), including the methods used by the threat actor to execute MgBot. MgBot is exclusively used by Daggerfly. The group is continually updating the malware, having used it in all its attacks in recent years. Daggerfly has also been seen deploying the PlugX remote access Trojan (RAT) in attacks. PlugX is known to be shared among multiple Chinese actors.

In the 2020 campaign, the attackers used phishing emails as an initial infection vector. Malicious Excel sheets were the first malicious activity seen in the 2014 Daggerfly activity, indicating emails were a likely infection vector there, too.

Like many Chinese groups, Daggerfly uses DLL sideloading to get its malware onto victim machines. The folders and file names used by Daggerfly also tend to be in Chinese. Daggerfly's motivation appears to be intelligence gathering and espionage.

MgBot is the main malware used by Daggerfly, and it appears to have exclusive use of the malware. It is a well-designed modular framework made up of a dropper, a loader, and various plugins. The malware is generally installed on machines as a service using DLL sideloading. It employs various anti-debugging and anti-virtualization techniques to check if it is running on a virtual machine. The framework appears to be under active development by Daggerfly.

Symantec observed Daggerfly targeting a telecommunications organization in Africa in a campaign that began in November 2022 and continued into 2023. In this campaign, suspicious AnyDesk connections were the first sign of suspicious activity, so the initial infection vector used in that instance was not clear.

In that campaign, Daggerfly made use of living-off-the-land tools, including using BITSAdmin and PowerShell to download files. They also dumped the security account manager (SAM), system, and security hives of the Windows registry using the `reg.exe` tool to steal credentials. The attackers also created a local account to maintain access to victim systems. The attackers deployed multiple MgBot plugins in this campaign, including several that had not been seen previously. The plugins included a credential stealer, infostealer, keylogger, password dumper, network scanner, and more. Symantec was able to link this campaign with the 2020 Daggerfly campaign described by Malwarebytes due to crossover in file names and MgBot samples used in both sets of activity.

In April 2023, ESET published a blog saying that Daggerfly had leveraged the QQ messaging software developed by Chinese tech giant Tencent to deliver malware to victims. The software was infected with MgBot and was able to perform automatic updates. The goal of the attackers appears to have been to spy on the devices of individuals working for an international NGO located in the Chinese provinces of Gansu, Guangdong, and Jiangsu. This activity, which was discovered in January 2022, may have begun as far back as 2020. ESET said it was not clear if any of the attempts to compromise victims were successful. It is not known how the attackers leveraged the legitimate updates to deliver the malware, but ESET put two hypotheses forward: a supply chain compromise of Tencent QQ's update servers, or an adversary-in-the-middle attack.

Daggerfly continued to update its toolset in 2024, with Symantec warning about updates to its arsenal in January of that year. We uncovered the group using a new, previously undocumented version of the Macma macOS backdoor malware. In addition, Daggerfly was once again observed using the PlugX RAT and a new version of MgBot. Symantec warned that components and malware modules used by the attackers would allow them to target a diverse range of operating systems, such as Windows, Linux, macOS, Android, iOS, Solaris, and so on.

Daggerfly’s development of its toolset continued in 2024. Symantec most recently published a blog in July 2024 warning about the group’s newly updated toolset. For more information, see the following case study. This continuous updating is likely a response to exposure of the group’s tools by Symantec and other security vendors.

Case Study: Daggerfly Updates Toolset

Daggerfly’s ongoing development of its toolset continued in 2024, with the group making extensive updates. The new tooling was deployed in a number of attacks against organizations in Taiwan and a U.S. NGO based in China.

Among the additions to Daggerfly’s arsenal was a new malware family based on the group’s MgBot modular malware framework and a new version of the Macma macOS backdoor. The Symantec® Threat Hunter Team found evidence to suggest that Macma, a previously seen threat, is developed by Daggerfly.

Macma is a macOS backdoor that was first documented by Google in 2021, but it appears to have been used since at least 2019. At the time of discovery, Macma was being distributed in watering hole attacks involving compromised websites in Hong Kong. The watering holes contained exploits for iOS and macOS devices. Users of macOS devices were targeted with a privilege escalation vulnerability (CVE-2021-30869), which allowed the attackers to install Macma on vulnerable systems.Macma is a modular backdoor with the following functionality:

- Device fingerprinting
- Executing commands
- Screen capture
- Keylogging
- Audio capture
- Uploading and downloading files

Variants of Macma found by Symantec exhibited evidence of ongoing development.

Although Macma was always believed to be linked to advanced persistent threat (APT) activity, it had not been linked to a particular group. However, Symantec found evidence to suggest that it is part of the Daggerfly toolkit. Two variants of the Macma backdoor were connected to a command-and-control (C&C) server that was also used by an MgBot dropper.

In addition to this shared infrastructure, known Daggerfly malware such as Macma and Mgbot, all contain code from a single shared library or framework. Elements of this library have been used to build Windows, macOS, Linux, and Android threats. The following functionality is provided by this library:

- Threading and synchronization primitives
- Event notifications and timers
- Data marshaling
- Platform-independent abstractions, such as time

An example of this library code is seen when the magic string “`inp`” is sent over a SOCK_DGRAM socket:

```
sendto(*(_DWORD *)(v2 + 56), “inp”, 3, 0, (const struct sockaddr *)(v2 + 60), 16);
```

While `sendto()` may be used to communicate with other hosts in general, in this example the communication is with a local machine (127.0.0), and could even be threads in the same process. Another example involves the magic string `“tim”` being sent over a socket similar to the following example:

```
sendto(*(_DWORD *)(v1 + 56), “tim”, 3, 0, (const struct sockaddr *)(v1 + 60), 16);
```

Symantec has yet to find any matching code in public repositories. Shared code and shared infrastructure between Macma and other Daggerfly tools strongly point to Macma being a part of Daggerfly’s toolkit.

New Backdoor

Another new addition to Daggerfly’s toolkit was a Windows backdoor (`Trojan.Suzafk`). Suzafk was first documented by ESET in March 2024 as Nightdoor (also known as NetMM) when it was observed being used alongside Mgbot. Suzafk was developed using the same shared library used in Mgbot, Macma, and a number of other Daggerfly tools. Suzafk is a multi-staged backdoor capable of using TCP or OneDrive for C&C. The malware contained the following configuration, indicating that the functionality to connect to OneDrive is in development or present in other variants of the malware:

```
ReadMe=ConnONEDRIVE;Version=256;Tag=15ad490f332f3d9a;DownloadUrl=http://10
3.96.131.150:19876/30_1410402971.exe;token={“refresh_token”:”REDACTED”,”client_id”
:”4aa6708f-f3c8-4511-8118-
5a7208be6a44”,”client_secret”:”REDACTED”};DownloaderSavePath=C:\Programdata\Office
\;HttpServerFolder=C:\Program Files\Common Files\Cloudata\;
```

Another configuration to use a TCP connection for C&C purposes is also present in the backdoor:

```
ReadMe=ConnTCP;Version=256;Tag=15ad490f332f3d9a;DownloadUrl=http://103.96.131.150:
19876/30_1292836936.exe;IP=103.96.131.150;Port=40020;DownloaderSavePath=C:\\
Programdata\\Office\\;HttpServerFolder=C:\\Program Files\\Common Files\\Cloudata\\;
```

The loader adds two files: `Engine.dll` and `MeitUD.exe`. `MeituUD.exe` is a legitimate application named DAEMON Tools Lite Helper. `Engine.dll` is a loader DLL that sets persistence through scheduled tasks and loads the final payload in memory.

The backdoor has embedded code from the al-khaser project, a public code repository aimed at detecting virtual machines, sandboxes, and malware analysis environments. It also creates the folders `C:\ProgramData\Office\EFir` and `C:\ProgramData\Office\Temps` and stores additional network configuration data under the `C:\ProgramData\Office\sysmgr` file XOR encrypted with the key 0x7A.

Heavily Resourced

It is clear Daggerfly is a well-resourced group that can create versions of its tools targeting most major operating system platforms. In addition to the tools documented here, Symantec has seen evidence of the ability to Trojanize Android APKs, SMS interception tools, DNS request interception tools, and even malware families targeting Solaris OS. Daggerfly appears to be capable of responding to exposure by quickly updating its toolset to continue its espionage activities with minimal disruption, making it a challenging threat.

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 (also known as OwaAuth), Sybersyringe, SysUpdate, ChargeWeapon

Infection vectors: Email, watering holes, public-facing exploits

Exploits used: CVE-2015-5119, CVE-2013-3906, CVE-2021-40539, CVE-2021-26855 (ProxyLogon), CVE-2021-44228 and CVE-2021-45105 (Log4j)

Other tools used: WinCredEd, GsecDump, Hunter, NBTscan, WinRAR, Cobalt Strike, Lazagne, Fast Reverse Proxy, IOX Proxy, Fscan, PowerShell; AdFind; Curl; SecretsDump; PasswordDumper

Key developments: Major updates of SysUpdate malware. Attacks on telco sector.

Budworm is a Chinese group that has been active for a long time, with activity attributed to this group having first been spotted in 2013. Budworm is known for targeting high-value victims, often focusing on organizations in the government, technology, and defense sectors. Budworm has targeted victims in many countries in Southeast Asia and the Middle East, among other locations, including the U.S. Like many Chinese threat actors, Budworm makes heavy use of DLL sideloading to get its malware onto victim machines. The most recent publicly documented activity from the group dates from 2023. For more information, see the following case study.

In October 2022, the Symantec Threat Hunter team documented how the Budworm espionage group had mounted attacks over a six-month period targeting strategically significant targets. The targets included the government of a Middle Eastern country, a multinational electronics manufacturer, and a U.S. state legislature. This was the first time in a number of years Symantec had seen Budworm targeting a U.S.-based entity. In those attacks, Budworm leveraged the Log4j vulnerabilities (CVE-2021-44228 and CVE-2021-45105) for initial access. They used their HyperBro malware family in this attack, which they loaded through DLL sideloading. They also used the PlugX/Korplug Trojan as a payload at times during this campaign. Other tools they used in this series of attacks included Cobalt Strike, LaZagne, the IOX proxy, Fast Reverse Proxy, and Fscan.

In March 2023, Trend Micro documented how it had seen Budworm using an updated version of its custom SysUpdate malware. The malware included new features, and it also added malware infection support for the Linux platform. The first sample of this updated malware dated from July 2022.

The new version had similar features to the previous 2021 version of the malware, except that the C++ run-time type information (RTTI) classes had been removed, and the code structure was changed to use the ASIO C++ asynchronous library. These changes appear to have been made to make reverse engineering the samples more difficult. Other updates indicate that this sample could be used on Linux, and the attackers also added the ability for the malware to carry out C&C communication through DNS TXT requests. Trend Micro saw this updated sample being used to target a gambling company in the Philippines, which aligns with Budworm's known interest in organizations in Southeast Asia.

EclecticIQ documented an August 2023 attack that used a Taiwan Semiconductor Manufacturing (TSMC) lure. Most likely the purpose was to target the semiconductor industry in places such as Taiwan, Hong Kong, and Singapore. In this attack, EclecticIQ said it saw overlaps between this campaign and previous Budworm activity reported by Symantec. As we documented in our October 2022 blog, they observed the same DLL sideloading technique through the same CyberArk binary being used to load Budworm's HyperBro malware. In this instance, the attackers used the HyperBro loader to facilitate in-memory execution of a Cobalt Strike beacon. The researchers also found a previously unidentified malware downloader that utilized the BitsTransfer module in PowerShell to fetch malicious binaries from a very likely compromised Cobra DocGuard server. This server hosted a GO-based backdoor that EclecticIQ tracked as ChargeWeapon. ChargeWeapon is designed to get remote access and send device and network information from an infected host to an attacker-controlled C&C server. Symantec had reported on Cobra DocGuard being used in a similar fashion in August 2023 by a group we dubbed Carderbee. We could not definitively link the activity we saw to a known ATP group; however, we did speculate in that blog that there may be links between Carderbee and Budworm. Crossover among Chinese threat groups is not unusual.

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

Case Study: Budworm Uses Updated Tool in Attack Targeting Telco and Government

In August 2023, the Symantec Threat Hunter Team observed Budworm using a previously unseen version of its SysUpdate tool to target a Middle Eastern telecommunications organization and an Asian government.

Both attacks occurred in August 2023, with Budworm deploying an updated variant of its SysUpdate backdoor (`SysUpdate DLL inicore_v2.3.30.dll`). SysUpdate is exclusively used by Budworm.

Budworm executed SysUpdate on victim networks by DLL sideloading the payload using the legitimate INISafeWebSSO application. Budworm has reportedly leveraged INISafeWebSSO for the purposes of DLL sideloading since as far back as 2018. DLL sideloading attacks use the DLL search order mechanism in Windows to plant and then invoke a legitimate application that executes a malicious payload. It can help attackers evade detection.

SysUpdate is a feature-rich backdoor that includes the following capabilities:

- List, start, stop, and delete services
- Take screenshots
- Browse and terminate processes
- Drive information retrieval
- File management (finds, deletes, renames, uploads, downloads files, and browses a directory)
- Command execution

As previously mentioned, Trend Micro reported in March 2023 that Budworm had developed a Linux version of SysUpdate with similar capabilities to the Windows version. SysUpdate has been in use by Budworm since at least 2020, and the attackers have continually developed the tool to improve its capabilities and avoid detection.

As well as its custom malware, Budworm also used a variety of living-off-the-land and publicly available tools in these attacks. However, it appears the activity by the group may have been stopped early in the attack chain, as the only malicious activity seen on infected machines was credential harvesting.

The following legitimate or publicly available tools were used in this attack:

- AdFind: A publicly available tool that is used to query Active Directory. It has legitimate uses, but it is widely used by attackers to help map a network.
- Curl: An open-source command-line tool for transferring data using various network protocols.
- SecretsDump: A publicly available tool that can perform various techniques to dump secrets from a remote machine without executing any agent. Techniques include reading SAM and LSA secrets from registries, dumping NTLM hashes, plaintext credentials, Kerberos keys, and dumping the `NTDS.dit` Active Directory database.
- PasswordDumper: A password-dumping tool.

Billbug

Aliases: Lotus Blossom, Lotus Panda, Bronze Elgin, Thrip

First seen: 2009

Malware used: Trojan.Emysair, Trojan.Trensil, Trojan.Trensil.B, Infostealer.Catchamas, Backdoor.Sagerunex, Backdoor.Hannotog

Infection vectors: Email, watering holes

Exploits used: CVE-2009-4324, CVE-2010-0188, CVE-2012-0158, CVE-2014-4114, CVE-2014-6332, CVE-2015-0097, CVE-2017-11882

Key developments: Heavy focus on Southeast Asia with ongoing intrusion campaign in the region

Active since at least 2009, Billbug has largely focused on Southeast Asia, targeting governments and military organizations in particular.

The group first came to public attention in 2015 when Palo Alto published a report on its activities in Southeast Asia. The group was linked to over 50 different attacks over a period of three years. Its campaigns used spear-phishing emails and convincing lure documents to deliver the custom Trensil (also known as Elise) Trojan.

Palo Alto followed up with a second report in December 2015 describing an attack on a French diplomat based in Taiwan involving the Emysair (also known as Emissary) Trojan. Shared code linked Emysair to Trensil, allowing the attack to be attributed to Billbug.

In 2018, Symantec published an investigation on the group's activity describing an attack on a large telecoms operator in Southeast Asia. The attackers used PsExec to install a previously unknown piece of malware (`Infostealer.Catchamas`). The discovery of this attack led to the discovery of further attacks against the communications, geospatial imaging, and defense sectors, both in the U.S. and Southeast Asia. During that investigation, Symantec referred to the actor as Thrip. We subsequently determined that Thrip and Billbug were most likely the same group, and we began tracking all activity under the Billbug name.

In 2019, Symantec published another report on the group using two previously unseen backdoors known as Hannotog (`Backdoor.Hannotog`) and Sagerunex (`Backdoor.Sagerunex`). Targets of this campaign included at least 12 organizations in Hong Kong, Macau, Indonesia, Malaysia, the Philippines, and Vietnam. In addition to military targets, the group also attacked organizations in the maritime communications, media, and education sectors.

Billbug remained active in subsequent years. In November 2022, Symantec published new research on the group, highlighting an attack against a digital certificate authority in an Asian country. The targeting of a certificate authority was notable because the attackers could have accessed certificates and used them to sign malware, helping them to evade detection. Compromised certificates could also potentially be used to intercept HTTPS traffic. However, Symantec found no evidence to suggest the attackers were successful in compromising digital certificates.

Case Study: Billbug Intrusion Campaign against Southeast Asia Continues

Between August 2024 and February 2025, Billbug compromised multiple organizations in a single Southeast Asian country. The targets included the following groups:

- Government ministry
- Air traffic control organization
- Telecoms operator
- Construction company

In addition to this activity, the group staged an intrusion on an air freight organization located in a neighboring country.

Attribution

The activity appears to be a continuation of a campaign first documented by Symantec in December 2024, where multiple high-profile organizations in Southeast Asian countries were targeted. While it was clear that Chinese actors were behind the attacks, attribution to a single actor could not be determined.

However, a recent blog by Cisco Talos mentioned that recent Billbug activity contained the same indicators of compromise (IOCs) in this campaign, indicating that it was the work of Billbug.

Sideloaded Malware

In several of the intrusions, the attackers used legitimate software from Trend Micro and Bitdefender to load malicious loaders using the technique known as DLL sideloading.

One of the legitimate executables used for sideloading was a Trend Micro binary named `tmdbglog.exe` (SHA246: f9036b967aaadf51fe0a7017c87086c7839be73efabb234e2c21885a6840343e). This binary was used to sideload a malicious DLL named `tmdglog.dll` (SHA256: b75a161caab0a90ef5ce57b889534b5809af3ce2f566af79da9184eaa41135bd). Analysis of the loader revealed that it read, decrypted, and executed the contents of the file `C:\Windows\temp\TmDebug.log`. It then logged the execution progress to the file `C:\Windows\Temp\VT001.tmp`.

Another legitimate executable used was a Bitdefender binary named `bds.exe` (SHA256: 2da00de67720f5f13b17e9d985fe70f10f153da60c9ab1086fe58f069a156924). This binary is used to sideload a malicious DLL named `log.dll` (SHA256: 54f0eaf2c0a3f79c5f95ef5d0c4c9ff30a727ccd08575e97cce278577d106f6b). Analysis of the loader found that it read and decrypted the contents of the file `winnt.config`. It then started the process `C:\Windows\system32\systray.exe` and injected the decrypted contents to it.

Several variants of the `log.dll` file were used in the campaign, but only one was retrieved for analysis. The same Bitdefender binary was also used to sideload a file named `sqlresourceloader.dll`, which was also not retrieved. It is unknown if this file is related to the loader analyzed or a different tool.

Sagerunex Backdoor

The attackers also used a new variant of the Sagerunex backdoor, a custom tool that is exclusively used by Billbug. The variant (SHA256: 4b430e9e43611aa67263f03fd42207c8ad06267d9b971db876b6e62c19a0805e) appears to be related to variants of Sagerunex documented by Cisco in February 2025. As documented by Cisco, attackers created a persistence mechanism by modifying the registry to ensure that it would run as a service.

New Tools

Among the new tools deployed were two designed to steal credentials from the Chrome web browser. The following tools were deployed:

- ChromeKatz: Capable of stealing both credentials and cookies stored in Chrome
- CredentialKatz: Capable of stealing credentials stored in Chrome
- Reverse SSH Tool: Custom tool capable of listening for SSH connections on Port 22

Other Tools

The attackers deployed the publicly available Zrok peer-to-peer tool. They used the sharing function of the tool to provide remote access to services that were exposed internally.

Another legitimate tool used was called `datechanger.exe` (SHA256: b337a3b55e9f6d72e22fe55aba4105805bb0cf121087a3f6c79850705593d904). It is capable of changing timestamps for files, presumably to confuse incident analysts.

Dungbeetle

Aliases: Volt Typhoon, Voltzite, Vanguard Panda

First seen: 2021

Malware used: Frip

Infection vectors: Exploitation of public facing applications

Exploits used: CVE-2022-42475, CVE-2022-40684, CVE-2024-39717, CVE-2024-21887, CVE-2023-46805, CVE-2023-6548, CVE-2023-6549, CVE-2023-4966, CVE-2024-20272, CVE-2023-36553

Key developments: Source of major concern for U.S. government due to its targeting of critical infrastructure in the U.S.

Active since mid-2021, Dungbeetle is mainly focused on conducting covert and targeted operations against critical infrastructure organizations in the U.S. Its primary objectives involve post-compromise credential access, network system discovery, and maintaining undetected access within compromised networks.

Dungbeetle relies heavily on living-off-the-land techniques, emphasizes stealth, and minimizes the use of malware. These tatics make it challenging to detect. The group's activities have raised concerns about whether it may possess the capability to potentially disrupt critical communications infrastructure during future crises.

To date, the group has targeted critical infrastructure sectors that include communications, manufacturing, utilities, transportation, construction, maritime, government, information technology, and education. The group specifically targets Guam and the U.S.

In August 2024, Lumen Technologies reported that Dungbeetle had been exploiting a zero-day vulnerability in Versa Director servers. Their goal was to hijack credentials to break into downstream customer networks. Versa Director servers are used to manage network configurations for clients running SD-WAN software, and they are heavily used by Internet service providers (ISPs) and managed service providers (MSPs).

The vulnerability (CVE-2024-39717) allows attackers to upload malicious files by exploiting an unrestricted file upload flaw in the Versa Director GUI.

In March 2025, Littleton Electric Light and Water Departments (LELWD), was compromised by Dungbeetle. LELWD is a small utility company in Massachusetts that provides water and electricity services to around 15,000 people. The breach resulted in a long-running intrusion on the company's network that lasted from February to November of 2023.

The group reportedly gained access through an unpatched FortiGate 300D firewall appliance when the attackers exploited the CVE-2022-42475 critical buffer overflow vulnerability.

Kelp

Aliases: Salt Typhoon, GhostEmperor, Earth Estries

First seen: July 2020

Malware used: Alias: Kelpdoor, Alias: GhostSpider, Alias: SnappyBee, Alias: Demodex

Other tools used: WMIC, PsExec, PowerShell, ProcDump, WinRar, Certutil, BITSAdmin

Infection vectors: Exploitation of public-facing applications

Exploits used: CVE-2023-20198, CVE-2023-20273

Key developments: Compromised multiple U.S. telecom operators in 2024

Kelp has been in operation since at least 2020. It was first documented by researchers at Kaspersky in 2021. At that time, the group was using its custom rootkit Demodex to target telecommunications and government organizations primarily in Southeast Asia for intelligence-gathering purposes.

Kelp generally exploits vulnerabilities in public-facing applications to gain access to victim networks. It was one of the many groups that exploited the ProxyLogon vulnerabilities when they were first revealed in March 2021. Kelp has been known to use DLL sideloading to get its malware onto victim networks and using multiple dual-use tools while on victim networks for lateral movement and persistence.

Kelp appeared to go through a quiet period of operation following its public exposure by Kaspersky. There was a gap in its activity between 2021 and 2023. However, in 2024 Sygnia reported that it had observed an updated version of the Demodex rootkit being used to target telecoms and government organizations in Southeast Asia. Sygnia said that the group employed more sophisticated defense evasion techniques in that campaign than had been seen previously.

Cisco Talos also reported in 2024 that Kelp had been targeting telecommunications companies in Southeast Asia since 2023 with a new backdoor dubbed GhostSpider. Cisco said GhostSpider was a sophisticated, flexible, and adaptable multi-modular backdoor designed for long-term espionage operations. It allows attackers to deploy or update different modules independently based on their needs. This approach complicates detection and analysis, making it difficult for researchers to understand the malware's functionality fully.

Kelp then came to global prominence in late 2024 when it was revealed that the group had compromised the networks of multiple U.S. telecom companies during the 2024 U.S. presidential election. The group had intercepted the communications of individuals in both the Democratic and Republican presidential campaign camps. The group managed to gain access to the wiretapping services used by U.S. authorities for legal interception purposes. It used that capability to eavesdrop on high-ranking U.S. officials. The campaign was believed to have been ongoing for up to two years before its discovery by U.S. officials. They said that it was not just the U.S. that was impacted by this campaign. Dozens of countries were reportedly impacted, including countries in Europe.

Among the companies impacted were U.S. telecom giants such as AT&T, Verizon, T-Mobile, and Lumen Technologies. Even after the activity was discovered, it was reported that the affected companies were struggling to remove the attackers' access to their networks. In addition, Kelp reportedly continued to target U.S. telecom companies, exploiting vulnerabilities in Fortinet and Cisco products to gain initial access to victim networks.

This intrusion prompted the Cybersecurity and Infrastructure Security Agency (CISA) and multiple U.S. agencies to issue guidance around the use of mobile phone devices for communication about sensitive topics in an attempt to protect against espionage activities.

The APT41 Nexus

One of the largest clusters of China-linked activity is known as APT41. For over a decade, it has been linked to a huge volume of attacks. While many vendors consider APT41 to be a single threat actor, Symantec considers it to be a supergroup with at least three distinct groups (Blackfly, Grayfly, and Redfly). The groups are loosely affiliated through the use of shared tooling.

For a long time, the nature of the link between the three groups was unclear. However, a 2020 indictment provided some insights into the relationship between the component groups. The U.S. government charged seven men in relation to hundreds of APT41-linked attacks against organizations in the U.S. and multiple other countries in Asia and Europe.

Prosecutors charged three Chinese men (Jiang Lizhi, Qian Chuan, and Fu Qiang) in the attacks that involved Grayfly tools and tactics. The trio were believed to be 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 ethical hackers who could perform penetration testing along with offensive and defensive security operations.

The indictment alleged that the three men were also involved in attacks against over 100 different organizations in the U.S., South Korea, Japan, India, Taiwan, Hong Kong, Malaysia, Vietnam, India, Pakistan, Australia, the U.K., 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.

Meanwhile, in a separate indictment prosecutors alleged that two Malaysian nationals (Wong Ong Hua and Ling Yang Ching) were involved in attacks that involved Blackfly tools and tactics. Wong was the founder and CEO of a company called Sea Gamer Mall. Ling was its chief product officer and a shareholder. The duo was alleged to have collaborated with other attackers to mount a string of attacks against computer game companies to obtain in-game digital items, such as currencies, and then sell them for profit.

While Grayfly and Blackfly appear to be distinct operations, the indictments alleged that there was a link between the two groups. Two Chinese men (Zhang Haoran and Tan Dailin) were charged in a third indictment for collaborating with both groups. The two men were reported to have worked for a time at Chengdu 404, the company that prosecutors linked to the Grayfly attacks. However, they are also alleged to have collaborated with the charged Blackfly actors to make additional money by mounting attacks on computer gaming companies. The indictment alleges that in several instances, they used their unauthorized access to gaming company networks to kick other attackers off the network, effectively eliminating their competition.

Blackfly

Aliases: Winnti, Brass Typhoon, Bronze Atlas

First seen: 2010

Malware used: Backdoor.Winnti, Backdoor.Korplug, Trojan.Skelky, Backdoor.Slordu

Infection vectors: Email

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

Key developments: Remains active despite exposure from U.S. indictments

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. The presumption is that these were stolen for financial gain.

Blackfly was originally 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, telecom, materials manufacturing, pharmaceutical, media and advertising, hospitality, natural resources, fintech, and food sectors.

Between 2011 and 2015, private code signing certificates were used to sign custom malware. The certificates were almost certainly stolen from computer game firms by Blackfly. The 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 activity may be what led to some vendors tracking Blackfly and Grayfly as one group.

In April 2024, Trend Micro reported that the group was using previously undocumented malware that allows malicious processes to run without being detected by security software.

The malware, dubbed Unapimon, monitors Windows application programming interfaces (APIs) for malicious activity. It disables the hooks used for inspecting and analyzing API-related processes for security issues. This behavior prevents any processes created by the malware from being detected or inspected by threat detection mechanisms.

In November 2024, new research from BlackBerry found that the group had begun using a sophisticated Windows-based surveillance toolkit in a campaign targeting organizations in South Asia.

The modular framework, known as DeepData, supports at least 12 separate plugins for carrying out the following activities:

- Stealing communications from WhatsApp, Signal, Telegram, and WeChat
- Stealing and exfiltrating system information, Wi-Fi network data, and information on all installed applications on the compromised system
- Stealing information related to browsing history and cookies
- Stealing passwords from web browsers, Baidu storage services, FoxMail, and other cloud services
- Stealing user emails and contact lists in Microsoft Outlook
- Stealing audio files from compromised systems

In December 2024, researchers from QAX XLab found that the group was using a new PHP-based backdoor named Glutton in attacks on organizations in China and the U.S., and on other cybercriminals.

The modular backdoor consists of core components, including task_loader, which determines the environment; init_task, which installs the backdoor; client_loader, which introduces obfuscation; and client_task, which operates the PHP backdoor and communicates with the C&C server.

Glutton masquerades as a php-fpm process, facilitates fileless execution by dynamic in-memory execution, and injects malicious code into PHP files on ThinkPHP, Yii, Laravel, and Dedecms frameworks.

Case Study: Blackfly Targets Materials Technology

Blackfly targeted two subsidiaries of an Asian conglomerate in 2023, both of which operated in the materials and composites sector. The group may have been attempting to steal intellectual property.

The following tools were used in the attacks which occurred during late 2022 and early 2023:

- Backdoor.Winnkit: Rootkit driver known to be associated with Blackfly.
- Credential-dumping tool: Creates a dump of credentials from `lsass.exe` in `C:\windows\temp\1.bin`.
- Screen capture tool: Captures all open windows and saves them as `.jpg` files.
- Process-hollowing tool: Injects shellcode in `C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted`. The shellcode is a simple "`Hello World`" alert message.
- SQL tool: SQL client tool used to query SQL databases.
- Mimikatz: Publicly available credential-dumping tool.
- ForkPlayground: Proof-of-concept application to create a memory dump of an arbitrary process using ForkLib.
- Proxy configuration tool: Configures proxy settings by injecting into `C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted`.
- Proxy configuration tool: This tool requires a file called `conf.dat` to run properly, located at `c:\users\public\conf.dat`. `Conf.dat` contains the configuration to set up proxy settings.

Undeterred

Despite being the subject of a U.S. indictment, Blackfly has continued to mount attacks. The group seems to be undeterred by the publicity. Although it originally made a name for itself by attacking the gaming sector, the group now appears focused on targeting intellectual property in a variety of sectors.

Grayfly

Aliases: APT41, WickedPanda, SparklingGoblin, Earth Baku

First seen: 2017

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

Infection vectors: Exploitation of public-facing applications

Exploits used: CVE-2021-26855

Other tools used: Certutil, Whoami, Installutil, WMIC, BITSAdmin, Cscript

Key developments: Remains active despite exposure from U.S. indictments

Active since at least 2017, Grayfly is known for targeting public-facing web servers 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. It has hit organizations in many different sectors. Grayfly was originally 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 the group.

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 telecom 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 behavior 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.

In July 2024, Zscaler reported that the group had added a new loader to its toolset. Named DodgeBox, there were *striking similarities* between it and several variants of StealthVector, a known Grayfly tool.

DodgeBox is used to load a new backdoor named MoonWalk. This backdoor appears to have been built with many of the evasion techniques used in DodgeBox. MoonWalk uses Google Drive for C&C communication. While the initial infection vector is unknown, DodgeBox is sideloaded from a malicious DLL into a legitimate executable (`taskhost.exe`) signed by Sandboxie. It will then decrypt a second-stage payload (MoonWalk) from an encrypted DAT file (`sbiedll.dat`).

Later that month, Mandiant reported that Grayfly had launched sustained data exfiltration attacks against multiple organizations across the shipping and logistics, media, technology, and automotive sectors. The majority of the targeted organizations were located in Italy, Spain, Taiwan, Thailand, Turkey, and the U.K. Grayfly had managed to infiltrate these organizations and maintain prolonged, unauthorized access since at least 2023, Mandiant said.

To carry out the attacks, Grayfly used web shells on Tomcat Apache Manager servers to execute a dropper that then deployed a backdoor for C&C communications. The attackers then used a multi-stage plugin framework called Dusttrap.

A month later, in August 2024, Cisco Talos found that Grayfly had compromised a Taiwanese government-affiliated research institute working on sensitive technologies.

Cisco tied the attack to Grayfly based on the specific kinds of malware, tactics, and open-source tools used. The hackers deployed the ShadowPad malware favored among China-based hackers, and several additional tools were written in Simplified Chinese.

The initial access method used by the attackers is unclear; however, Cisco said the hackers compromised at least three devices and were *able to exfiltrate some documents from the network*. The attackers used backdoors and compression tools to exfiltrate stolen data.

Redfly

Aliases: RedEcho

First seen: 2019

Malware used: Backdoor.Shadowpad, PackerLoader

Other tools used: PowerShell, ProcDump. WMI, Keylogger

Key developments: Known for targeting critical infrastructure in Asia

There are indications that Redfly has been active since as far back as 2019, but it first came to prominence in 2021 when it was reported that the group had been aiming attacks at critical national infrastructure (CNI) organizations in India since mid-2020. Recorded Future reported that 10 Indian power stations and two seaports were targeted with the ShadowPad malware in a concerted campaign that they attributed to the group, which they track as RedEcho.

The use of ShadowPad and the targeting of CNI are both hallmarks of Redfly-attributed activity. The Symantec Threat Hunter Team reported in September 2023 that it had observed Redfly targeting a national grid in an Asian country for as long as six months in 2023. The attackers managed to steal credentials and compromise multiple computers on the organization's network. ShadowPad was also used in that attack, alongside other tools.

ShadowPad is a modular RAT that was designed as a successor to the Korplug/PlugX Trojan. It was sold in underground forums for a period of time. However, despite its origins as a publicly available tool, it was only sold publicly for a very short time. It was reportedly, sold to only a handful of buyers. It has since been closely linked to Chinese espionage actors. ShadowPad is known to be used by multiple Chinese APT groups, many of whom come under what could be described as the APT41 Nexus, which would include Redfly, Blackfly, and Grayfly. These groups appear to share infrastructure, tools, and perhaps even personnel, but seem to operate in a distinct fashion. In the case of Redfly, it appears to be solely focused on targeting CNI, while Blackfly and Grayfly have different targeting. Links between Chinese threat groups are common and are something we have discussed previously, as well as elsewhere in this document.

The group has also shown a preference for using the hosting services HKBN and EHOSTICT in their attacks. This information could be another data point to help identify Redfly activity.

Redfly has commonly exhibited the following additional behaviors in compromised environments:

- Abuse of the legitimate Windows OLE/COM Object Viewer to perform DLL sideloading
- Use of PowerShell along with WMI for system information discovery
- Use of Windows scheduled tasks to perform lateral movement
- Credential dumping using dual-use tools such as ProcDump and exporting SAM and SYSTEM registry hives
- Use of keylogger malware
- Use of a modified version of a publicly available packer to pack malware

Redfly's motivations for compromising critical infrastructure in India are unknown, but tensions between China and India have lead to speculation that the group's purpose was to give the group a foothold for future potentially disruptive attacks.

Shared Resource: ShadowPad

ShadowPad is a RAT that was designed as a successor to the Korplug/PlugX Trojan. It was sold in underground forums for a short period of time. However, despite its origins as a publicly available tool, it was reportedly only sold publicly to a handful of buyers. It has since been closely linked to espionage actors. Many of the actors who use ShadowPad are believed to be linked to the Chinese authorities. Because of its modular nature, ShadowPad can be continuously updated and have additional functionalities added to it. This capability makes it a powerful tool.

The Trojan is believed to have existed since 2017, although it started to be deployed more widely by various Chinese APT groups in 2019. ShadowPad has been deployed by multiple Chinese APT groups, including Blackfly, Grayfly, and Redfly (the APT41 Nexus), and Mustang Panda. It was used in the following attacks:

- CNI in India in 2020 that were attributed to Redfly
- Critical infrastructure in an Asian country in 2023
- NetSarang, ASUS, and CCleaner

More recently, it has been used in attacks where ransomware was deployed. It was also used in 2024 activities by the FamousSparrow attack group, which was the first time that particular group had been observed using this malware.

ShadowPad is generally loaded onto victim networks through DLL sideloading. The payload is decrypted in memory using a custom decryption algorithm. It extracts information about the host, executes commands, interacts with the file system and registry, and can deploy new modules to extend its functionality.

ShadowPad is notable because while its use is shared, it does seem like its use is tightly controlled. The malware appears to be only available for use by a small number of Chinese APT groups.

Wave of Activity Targets Asian Governments

In September 2022, the Symantec Threat Hunter team reported how espionage attackers who had previously been associated with ShadowPad had adopted a new, diverse toolset to mount an ongoing campaign against a range of government and state-owned organizations in a number of Asian countries. The intelligence-gathering attacks had been happening since at least early 2021. Among the targets were a prime minister's office, financial government institutions, and state-owned aerospace, defense, telecoms, IT, and media companies.

The attackers in this campaign leveraged a wide range of legitimate software packages to load their malware payloads using DLL sideloading. Usually, the attackers used multiple software packages in a single attack. In many cases, old and outdated versions of software were used, including security software, graphics software, and web browsers. In some cases, legitimate system files from the legacy operating system Windows XP were used. The reason for using outdated versions is that most current versions of the software used would have mitigation against sideloading built in. DLL sideloading is a well-known technique that is favored especially by Chinese threat actors. The technique involves attackers placing a malicious DLL in a directory where a legitimate DLL is expected to be found. The attacker then runs the legitimate application themselves (having installed it themselves in most cases). The legitimate application then loads and executes the payload.

Once a malicious DLL is loaded by the attackers, malicious code is executed, which in turn loads a `.dat` file. This file contains arbitrary shellcode that is used to execute a variety of payloads and associated commands in memory. In some cases, the arbitrary shellcode is encrypted. The attackers also leverage these legitimate software packages to deploy additional tools, which are then used to further aid lateral movement. These tools include credential dumping tools, a number of network scanning tools (NBTScan, TCPing, FastReverseProxy, and Fscan), and the Ladon penetration testing framework.

The attacks usually unfolded in the following manner:

- Once backdoor access is gained, the attackers use Mimikatz and ProcDump to steal credentials. In some cases, the attackers dump credentials through the registry.
- They then use network scanning tools to identify other computers of interest, such as those running RDP, which could facilitate lateral movement.
- They leverage PsExec to run old versions of legitimate software, which are then used to load additional malware tools such as off-the-shelf RATs through DLL sideloading on other computers on the networks.
- The attackers also use a number of living-off-the-land tools, such as Ntdsutil, to mount snapshots of Active Directory servers to gain access to Active Directory databases and log files. The Dnscmd command-line tool is also used to enumerate network zone information.

While this group of attackers was previously using ShadowPad, in this attack they deployed a range of payloads. The payloads included a feature-rich information stealer (Infostealer.Logdatter), which appeared to be custom built. The information stealer had the following capabilities:

- Keylogging
- Taking screenshots
- Connecting to and querying SQL databases
- Code injection: Reading a file and injecting the contained code into a process
- Downloading files
- Stealing clipboard data

Other payloads used by the attackers included known payloads such as PlugX, Trochilus RAT, QuasarRAT, various keyloggers and process dumpers, and more. ShadowPad was not deployed in this particular attack, but it is worth taking note of the attack chain and tools used. They could be reused by these attackers in future ShadowPad attacks. Also, notice that the tools used by these ShadowPad attackers are evolving.

This activity appeared to be continued in a campaign observed by Symantec that targeted Asian governmental organizations in 2022. This campaign had some overlaps with the activity seen in 2021, indicating that it was carried out by the same group of attackers. The following notable activities occured in this campaign:

- Use of multiple different legitimate applications for sideloading:
  - Bitdefender Crash Handler
  - Hp HPCustParticUI
  - Intel PROSet/Wireless iconvrtr Module
  - ESET SSL filtering certificate importer
- Use of SharpChromium (a publicly available infostealer) for extracting passwords
- Use of dismap for asset discovery
- Use of the Ladon penetration testing tool for vulnerability scanning
- Use of multiple versions of FastReverseProxy
- Deployment of infostealers and loaders
- Use of ffsend, a command-line utility, to send files
- Creation of scheduled tasks for persistence
- Use of netsh portproxy to redirect from port 80 to port 445
- Exfiltration of data from the infected network.

The Ladon penetration testing tool and FastReverseProxy were also used in the 2021 activity observed by Symantec. In that activity, Bitdefender Crash Handler and Hp HPCustParticUI were also used for DLL sideloading. It appears that the ShadowPad attackers are using the TTPs first seen in the 2021 attack in this more recent activity. The victimology is also similar, with Asian governmental organizations being the victims in this activity.

Fireant

Aliases: Mustang Panda, Stately Taurus, APT31, Earth Preta, Temp.Hex, TA416, Bronze President, HoneyMyte, Red Delta

First seen: January 2012

Malware used: Alias: TONEINS, Alias: TONESHELL, Alias: TONEDROP, Alias: Mirogo, Alias: QMAgent, Alias: PUBLOAD, Alias: ACNSHELL, Alias: COOLCLIENT, Alias: HUIPAN, Alias: NUPAKAGE, Alias: TROCLIENT, Backdoor.Korplug (PlugX)

Infection vectors: Emails

Exploits used: CVE-2017-10271

Other tools used: Cobalt Strike, Curl, WinRaR, PowerShell

Fireant is a long-running Chinese cyber espionage group that has been active since at least 2012. Fireant predominantly targets governments around the world, but it is also known to target private industry and education. Fireant often uses lures related to high-profile global events, such as the COVID-19 pandemic, the war in Ukraine, and so on. The group has targeted the Vatican, Russian speakers, and governments in Europe and Southeast Asia.

Fireant's TTPs continuously evolve. It is capable of developing and deploying custom malware onto networks of interest. The group's initial infection vector is typically email, after which it targets machines of interest for data exfiltration.

Fireant generally sends victims emails with malicious links or attachments to install first-stage payloads. This first stage typically includes a decoy document to distract users from the fact that a malicious payload is being executed. Fireant is also known to use DLL sideloading, shortcut links, and fake file extensions when launching its payloads on compromised machines. DLL sideloading is a favorite technique of many Chinese espionage groups.

From 2022, Fireant started using a number of new malware families. To bypass email-scanning services and email gateway solutions, the malware was often downloaded from a Google Drive link embedded in a lure document. The embedded link led to a malicious password-protected archive which contained the malware. Using a technique like this can allow the malicious actor to bypass security services.

The following list provides some examples of the tools Fireant has used since late 2022:

- Toneshell: Backdoor payload dropped on victim machines.
- Toneins: The installer for the Toneshell malware. It drops the Toneshell malware and establishes persistence for it. Toneins is heavily obfuscated, likely in an attempt to impede analysis of it.
- Tonedrop: Dropper for Toneins and Toneshell.
- Pubload: A stager that can download malware from a C&C server. It also attempts to establish persistence on victim networks by adding a registry run key or creating a scheduled task. Pubload also has features to help it evade detection by security software or researchers.
- Qmagent: Leverages the MQTT protocol to tunnel communications to and from a C&C server. Generally delivered through spear-phishing emails to individuals working in government agencies.
- Mirogo: A backdoor written in Golang.

Fireant also used tools such as Mistcloak, Bluehaze, and Darkdew. For more information, see the following case study. Fireant is continually developing its arsenal and making subtle changes to its attack chain in an attempt to avoid detection.

As well as its custom malware, Fireant has been known to frequently deploy the PlugX Trojan in attacks. PlugX is shared among multiple Chinese threat actors, so it is not always easy to attribute the Trojan to the group.

Fireant is a very well-resourced group based on the scale, persistence, and longevity of its operations, and its ability to continually develop its malware arsenal.

Case Study: Fireant Campaign

The Symantec Threat Hunter Team observed a wide-ranging Fireant campaign that started in July 2022 and continued into 2023, impacting many companies and organizations in multiple countries and sectors. The campaign may even have begun before the period investigated by Symantec, possibly as early as late 2021.

In the course of this activity, Fireant was primarily seen deploying its Mistcloak and Bluehaze malware. These malware families were first written about in a Mandiant blog in November 2022, when the company documented activity it attributed to Chinese nation-state actors.

Mistcloak is a launcher written in C++ that executes an encrypted executable payload stored in a file on disk. The payload in the activity tracked by Symantec is Bluehaze. In this campaign, Mistcloak operates as a USB worm, spreading automatically to networks where a removable drive is used. This automatic spread likely accounts for the prevalence of this campaign, with Mistcloak and Bluehaze seen on more than 2400 machines.

Bluehaze is a backdoor written in C/C++. It launches a copy of NCAT, a command-line networking utility that was written for the Nmap Project to perform a wide-variety of security and administration tasks. The utility creates a reverse shell to communicate with a hardcoded C&C server.

A smaller number of machines also contained an encrypted version of Darkdew that was also capable of self-propagating. Darkdew is a dropper written in C++ that is capable of infecting removable drives. It is possible that more of these encrypted implants were used by the attackers but not yet identified.

It is unusual to see APT activity infecting so many machines, because it is generally more targeted. However, the self-propagating nature of the malware used is probably the reason why it is spreading so widely. It is possible that Fireant was only interested in accessing and stealing information from a small number of the infected machines.

The sectors impacted by this campaign were government, oil and gas, finance, retail, hospitality, professional services, transport, and IT. In many organizations the malware was only seen on one machine, indicating that the organization may not have been of interest to the attackers. The malware might only have been on the network due to its self-propagating nature, rather than the organization being targeted.

We cannot see exactly what the attackers are doing on the infected machines. We assume that Fireant is accessing machines of interest to carry out espionage and exfiltrate data. The ability to develop its own malware and carry out long-lasting campaigns like this supports the assumption that Fireant is a highly skilled and well-resourced group.

Shifting Sands: The Attribution Problem

Attribution to China-linked attackers is rarely difficult, but attribution to a specific China-linked group is becoming more challenging. Now there is the longstanding practice among the actors to share tools such as the PlugX and ShadowPad backdoors and infrastructure. In addition to this tool and infrastructure sharing, there appears to be frequent movement of personnel between groups or the use of contractors (see the APT41 Nexus).

However, in recent years, the distinction between groups has further blurred. Frequently, attack campaigns have links to two or more China-based actors. The reasons for this are unknown. Possible scenarios include a general reorganization of cyber operations, increased use of contractors, increased co-operation between groups, or a strengthening of the practice of sharing resources.

An investigation published by Symantec in June 2024 illustrates this attribution problem. It found that China-linked actors had breached multiple telecoms operators in a single Asian country in a long-running espionage campaign. The attackers placed backdoors on the networks of targeted companies and also attempted to steal credentials.

The following custom malware was associated with a number of China-linked espionage actors in the campaign:

- Coolclient: A backdoor associated with the Fireant group (also known as Mustang Panda and Earth Preta). Its functionality includes logging keystrokes, reading and deleting files, and communication with a C&C server. Variants of the backdoor used in this campaign were similar to one documented by Trend in 2023. A version of the legitimate VLC Media Player masquerading as a Google file (`googleupdate.exe`) was used to sideload a Coolclient loader (file name: `libvlc.dll`). The loader reads an encrypted payload from a file named `loader.ja`. This payload will, in turn, read a second encrypted payload from a file named `goopdate.ja` and inject it into the `winver.exe` process.
- Quickheal: A backdoor that has been long associated with the Neeedleminer group (also known as RedFoxtrot and Nomad Panda). The variant of Quickheal used in this campaign was a 32-bit DLL named `RasTls.dll`, which had an export named GetOfficeDatatal. Analysis of the malware revealed that it was almost identical to Quickheal variants documented by Recorded Future in 2021, the only differences being new configuration details in the compiled code and VMProtect obfuscations.

The backdoor communicated with a hardcoded C&C server named swiftandfast.net using TCP port 443. It used a custom communications protocol that was designed to look like SSL traffic, but it used its own encryption instead.

Rainyday

Rainyday is a backdoor associated with the Firefly group (also known as Naikon). Most of the Rainyday variants used during the campaign were executed using a loader named `fspmapi.dll`. The loader is sideloaded using a legitimate F-Secure executable named `fsstm.exe`. When loaded, it obtains the disk folder of the executable that started the process and sets it as the current directory. It then obtains the memory location of the executable and patches its memory image. This appears to be done to hijack the execution flow when the malware is loaded by a certain executable. If the hijack is successful, the loader reads from a file called dataresz, decrypts the payload with a single byte XOR key (0x2D), and executes it as shellcode.

The tools used in this campaign have strong associations with multiple Chinese groups. The nature of the link between the actors remains unclear. The ultimate motive of the intrusion campaign remains unclear. The attackers may have been gathering intelligence on the telecoms sector in that country. Eavesdropping is another possibility. Alternatively, the attackers may have been attempting to build a disruptive capability against critical infrastructure in that country.

Lancefly

First seen: January 2018

Malware used: Backdoor.Merdoor, ZXShell, BlackLoader, PRCLoader, PlugX (Backdoor.Korplug), ShadowPad,

Infection vectors: Emails, exploitation of public-facing applications

Other tools used: Mimikatz, Impacket Atexec, WinRAR, NBTScan, LSASS Dumper, PowerShell

Lancefly was first documented by Symantec in May 2023. Lancefly's custom malware, which is dubbed Merdoor, is a powerful backdoor that appears to have existed since 2018. Symantec researchers observed it being used in some activity in 2020 and 2021, as well as a campaign that continued into the first quarter of 2023. The motivation behind both these campaigns is believed to be intelligence gathering.

The backdoor is used very selectively, appearing on just a handful of networks and a small number of machines over the years, with its use appearing to be highly targeted. Lancefly also has access to an updated version of the ZXShell rootkit.

Merdoor is a fully featured backdoor that contains the following functionality:

- Installing itself as a service
- Keylogging
- A variety of methods to communicate with its C&C server (HTTP, HTTPS, DNS, UDP, TCP)
- Ability to listen on a local port for commands

Instances of the Merdoor backdoor are usually identical with the exception of embedded and encrypted configuration, which determines the following information:

- C&C communication method
- Service details
- Installation directory

Typically, the backdoor is injected into the legitimate processes `perfhost.exe` or `svchost.exe`.

The Merdoor dropper is a self-extracting RAR (SFX) file that contains three files:

- A legitimate and signed binary vulnerable to DLL search-order hijacking
- A malicious loader (Merdoor loader)
- An encrypted file (`.pak`) containing the final payload (Merdoor backdoor)

When opened, the dropper extracts embedded files and executes a legitimate binary to load the Merdoor loader. Merdoor dropper variants have been found that abuse older versions of five different legitimate applications for the purpose of DLL sideloading.

From mid-2022 into 2023, Lancefly targeted organizations in South and Southeast Asia, in sectors including government, aviation, education, and telecoms. Symantec researchers previously saw the Merdoor backdoor used in activity that targeted victims in the same geographies in the government, communications, and technology sectors in 2020 into 2021. This activity was highly targeted, with only a small number of machines infected.

The infection vector used by Lancefly is not always entirely clear. Evidence from Lancefly's 2020 campaign suggested that in that instance the group may have used a phishing email with a lure based on the 37th ASEAN Summit as an initial infection vector. There have been indications that in other campaigns the initial infection vector may have been SSH brute forcing, while in another it may have been an exposed public-facing server.

As well as using Merdoor, Lancefly also uses a variety of living-off-the-land and dual-use tools in its attacks.

The ZXShell rootkit was first reported on by Cisco in 2014, but the version of the tool used by Lancefly in 2022/2023 was updated, indicating that it continues to be actively developed. The new version of the rootkit used by Lancefly appears to be smaller in size, while it also has additional functions and targets additional antivirus software to disable. The source code of this rootkit is publicly available, so it may be used by multiple different groups.

The use of Merdoor is the primary means of identifying Lancefly. However, crossover among Chinese threat groups is not uncommon, and Lancefly has multiple potential links to other China-based groups. The ZXShell rootkit used by Lancefly is signed by the certificate "`Wemade Entertainment Co. Ltd`", which was previously reported to be associated with APT41 (also known as Blackfly and Grayfly). However, it is known that Chinese APT groups, such as APT41, often share certificates with other APT groups. The ZXShell backdoor has also previously been used by the HiddenLynx/APT17 group, but as the source code of ZXShell is now publicly available. This code does not provide a definitive link between these two groups. Also notable is that the ZXShell rootkit loader component has the name `formdll.dll` and it has the ability to read the file `Form.hlp` and execute its contents as shellcode. Those same files were mentioned as being used in a previous report describing activity by the Iron Tiger (also known as Budworm/APT27) group. The prevalence of these file names is low, pointing to a potential link.

Lancefly also uses PlugX and ShadowPad, both tools that are known to be shared among China-based groups.

Carderbee

First seen: 2023

Malware used: Backdoor.Korplug (PlugX)

Infection vectors: Update hijacks

Other tools used: Cobalt Strike

Carderbee activity was first seen in April 2023. The Symantec Threat Hunter team documented how a previously unknown APT group had used the legitimate Cobra DocGuard software to carry out a supply chain attack with the goal of deploying the Korplug backdoor (also known as PlugX) onto victim computers.

In the course of that attack, the attackers used malware signed with a legitimate Microsoft certificate. Most of the victims in the campaign were based in Hong Kong, with some victims based in other regions of Asia. Malicious activity was seen on about 100 computers in impacted organizations. However, the Cobra DocGuard software was installed on around 2000 computers, indicating that the attackers were selectively pushing payloads to specific victims.

The location the malicious software was delivered to on victim computers indicates that it was a supply chain attack or malicious configuration involving Cobra DocGuard that gave the attackers access to affected computers. Cobra DocGuard was previously used in a similar fashion to compromise a gambling company in Hong Kong in September 2022, ESET had reported. They linked that attack to Budworm. However, as it was not possible to link the activity we saw in the April 2023 attack definitively to a known group, we attributed it to a new group which we called Carderbee.

Over a period of a few months in 2023, multiple distinct malware families were observed being deployed onto victim networks by leveraging Cobra DocGuard. In one interesting case, a downloader deployed by the attackers had a digitally signed certificate from Microsoft, called Microsoft Windows Hardware Compatibility Publisher. This downloader was used to install the Korplug backdoor on targeted systems. Korplug is known to be used by multiple China-based APT groups. Using signed malware makes the attack harder to detect.

EclecticIQ documented an August 2023 attack that used a Taiwan Semiconductor Manufacturing (TSMC) lure, with the likely purpose of targeting the semiconductor industry in places such as Taiwan, Hong Kong, and Singapore. In this attack, EclecticIQ said it saw overlaps between this campaign and Carderbee activity, as well as Budworm activity previously reported by Symantec. The researchers found a previously unidentified malware downloader that utilized the BitsTransfer module in PowerShell to fetch malicious binaries from a very likely compromised Cobra DocGuard server. This server hosted a GO-based backdoor that EclecticIQ tracked as ChargeWeapon. ChargeWeapon is designed to get remote access and send device and network information from an infected host to an attacker-controlled C&C server. They also observed the same DLL sideloading technique through the same CyberArk binary as we documented in a October 2022 Budworm blog, pointing to links to that group as well.

Some unanswered questions remain about the activity of Carderbee, including whether or not it is a truly independent group or if it has links to other Chinese threat actors such as Budworm. Budworm is the group whose activity Carderbee has been most aligned with. It is not unusual to see cooperation and personnel overlap between Chinese nation-state-backed groups, which can sometimes make attribution of activity challenging.

Sheathminer

Aliases: APT31, Zirconium, Judgement Panda, RedBravo

First seen: 2017

Malware used: Trochlius, GrewApacha, PlugY, CloudSorceror

Infection vectors: 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 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.

Members of the group were sanctioned by the U.S. Treasury's Office of Foreign Asset Control (OFAC) in 2024. Officials said a company in China called Wuhan Xiaoruizhi Science and Technology Company was a front for Sheathminer, which it said had targeted *a wide range of high-ranking U.S. government officials and their advisors*. It said other Sheathminer victims in the U.S. included a Texas energy company, a California managed service provider, and several aerospace contractors with the U.S. military in Alabama and Tennessee. The Treasury Department levied sanctions against Wuhan Xiaoruizhi and two Chinese nationals (Zhao Guangzong and Ni Gaobin) linked to the firm's operations targeting U.S. critical infrastructure. The Justice Department also unsealed indictments of Zhao, Ni, and five others for their work within the Sheathminer group. The U.S. State Department announced a reward of up to $10 million for information on the group. A government spokesperson said that the group had targeted journalists, political officials and companies to repress critics of the Chinese regime, compromise government institutions, and steal trade secrets.

It was also reported in 2024 that Russian government organizations as well as IT companies were targeted by Sheathminer. Sheathminer had previously been linked to attacks on industrial targets in Eastern Europe in 2023. The 2024 campaign reportedly began with a targeted phishing attack involving emails containing a RAR file. The RAR file contained a decoy DOCX file, a DLL file containing the initial malware, a legitimate copy of `desktop.exe` used to sideload the DLL, and an LNK file. The LNK file when clicked by the victim, strings together all the files so that they are copied and executed correctly. When executed, the malware attempts to contact Dropbox for commands, which include exfiltrating local information, and downloading and executing additional files. The malware was seen downloading and executing additional malware, including GrewApacha, CloudSorcerer, and PlugY.

GrewApacha is a slightly updated version of a previously known malware. It acts as a RAT and reaches out to a GitHub profile to receive commands. CloudSorcerer downloads and decrypts additional malware, which also use sideloading to launch. It uses a Russian social network site called LiveJournal as its C&C server. CloudSorcerer then downloads and installs PlugY, a malware seen for the first time in this attack, which is said to be similar to the PlugX (Korplug) malware used by multiple Chinese threat actors. PlugY allows the attackers to carry out an extensive range of commands on the compromised computer, which include downloading and executing additional files, stealing data, and capturing screenshots and keystrokes. It can also use TCP, UDP, or named pipes to contact its C&C server.

The group has also been linked to multiple other attacks on government targets. It was linked to an attack on the Norwegian parliament in 2018, an attack on the Finnish parliament in 2020, and attempted attacks during the 2020 U.S. presidential election campaigns. The group also breached the U.K.'s Electoral Commission in 2021 using the ProxyShell vulnerability, where it accessed the personal information of 40 million U.K. voters.

Also, in July 2021, the French national cybersecurity 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 to perform stealth reconnaissance and attacks in that campaign.

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 allow listing 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. 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. 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 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.

Protection

How Symantec Solutions Can Help

Symantec 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 (SESC)

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 at www.broadcom.com/products/cyber-security/endpoint/end-user/complete

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 at www.broadcom.com/products/cyber-security/identity/pam

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 at www.broadcom.com/products/cyber-security/network/gateway/web-isolation

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 at www.broadcom.com/products/cyber-security/network/gateway/proxy-sg-and-advanced-secure-gateway

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 at www.broadcom.com/products/cybersecurity/network/web-protection/intelligence-services

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 at www.broadcom.com/products/cyber-security/network/gateway/atp-content-malware-analysis

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 at www.broadcom.com/products/cyber-security/network/atp/network-forensics-security-analytics.

BROADCOM®
connecting everything®

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

RFC-CEA-WP100 April 21, 2025