CUCKOO SPEAR Part 1: Analyzing NOOPDOOR from an IR Perspective

By Cybereason Security Services Team

Archived: 2026-04-05 17:16:59 UTC

This Threat Analysis Report will delve into a newly discovered nation-state level threat Campaign tracked by Cybereason as Cuckoo Spear. It will outline how the associated Threat Actor persists stealthily on their victims' network for years, highlighting strategies used across Cuckoo Spear and how defenders can detect and prevent these attacks.

In this report, Cybereason confirms the ties between Cuckoo Spear and APT10 Intrusion Set by tying multiple incidents together and disclosing new information about this group’s new arsenal and techniques.

This is the first part of three regarding the Cuckoo Spear threat campaign. It introduces the Threat Actor, the related campaign and their arsenal, and details the TTPs observed during the various incidents. The two next parts are going to cover a reverse engineering of their arsenal (NOOPLDR/NOOPDOOR in particular) and how to fight against this threat actor.

We have published Indicators of compromise, Yara rules and Python scripts related to this report and they are available on the following public Github repository : https://github.com/Cybereason-Open-Source/CuckooSpear/

KEY POINTS

- **Nation-state Threat Actor targeting Japanese companies:** Cybereason observed similar Tactics, Techniques and Procedures (TTPs) of the threat Campaign targeting different Japanese companies. The attack focused on manufacturing, politics and industrial sectors, is assessed to be part of cyber espionage.
- **Stealthy and advanced malware use:** Cuckoo Spear is using the same malware across victims, which is a new version of the previously called LODEINFO malware, part of APT10’s arsenal.
- **NOOPLDR and NOOPDOOR:** Cybereason identified similarities with LODEINFO, but the identified malware across multiple cases included the unravel of two new discoveries:
  - **NOOPLDR** (Using two very different methods : C# language loading and persistence backdoor and a DLL file)
  - **NOOPDOOR** (DGA-Based C2 malware with C2 local network relaying capabilities)
- **Persistent :** Cybereason identified some of the victims had the associated Threat Actor present in their network for a time period between 2 and 3 years
- **Luring Techniques:** A variety of techniques were used to lure in potential victims, but the Threat Actors mainly rely on Phishing as the Initial Access vector

What is Cuckoo Spear?

For the past several years, since December 2019, the cybersecurity landscape has been continuously challenged by the emergence and evolution of the **LODEINFO** malware. Recent investigations suggest the involvement of a Chinese state-backed Advanced Persistent Threat (APT) group, likely APT10, in orchestrating these attacks. A recent development identified ties between the Threat Actor utilizing LODEINFO with a new malware family that is called **NOOPDOOR**. Cybereason named this threat Campaign “Cuckoo Spear”.

In this report, the Cybereason team examined several key aspects regarding Cuckoo Spear:

- **Techniques employed by APT10 group to load the highly sophisticated malware**: We'll explore the sophisticated functionalities and tactics that define the most recent iteration of **NOOPDOOR** and **NOOPLDR** malware and its surrounding capabilities.
- **A deep dive into the Threat Actor’s arsenal** : During recent incident response activities, our team has uncovered and meticulously analyzed the newest arsenal deployed by the Threat Actor. This analysis, fueled by advanced reverse engineering techniques, revealed a sophisticated set of tools designed for stealth infiltration, data exfiltration, and persistent access.
- **Strategies for Threat Hunting and Defense**: Leveraging open-source intelligence, Cybereason provides actionable insights on how organizations can effectively hunt and defend against these persistent threats.

Attribution

	Summary	
Victimology	Country	Japan
		India
		Taiwan
	Industries	Academic, Government, Manufacturing
TTPs	Initial Infection Vectors	Spear-Phishing
		Exploit against public-facing applications E.g. Array AG, FortiOS/FortiProxy and Proself

	Techniques	DLL Side-Loading
		MSBuild
		Exploitation for Client Execution E.g. CVE-2013-3900
Malwares	Downloader / Malware Loader	DOWNIISA
		NOOPLDR
	Backdoor	LODEINFO
		NOOPDOOR
	Infostealer	MirrorStealer
		MSRAStealer
Tools	Cobalt Strike	

Intrusion Set Table of Threat Actors Behind NOOPDOOR

***Note**: Cybereason began writing this article in the beginning of January 2024 after encountering multiple cases of compromise from the same Threat Actor. The adversary was using weaponized tools that were not public at the time. On the week of the 22nd of January 2024, threat intelligence reports from Trend Micro and ESET were published highlighting similar findings.*

Trend Micro and ESET published their research findings in JSAC2024 regarding Threat Actors leveraging **LODEINFO** and the new backdoor dubbed **NOOPDOOR**. From the intrusion sets observed in multiple campaigns, both companies have attributed Threat Actors behind this campaign to a group related to APT10, specifically Trend Micro have attributed the Threat Actors as “Earth Kasha”. Threat Actors behind NOOPDOOR consisted of Intrusion Sets represented in the table above during the campaign observed by Cybereason, ESET, and Trend Micro.

The actors behind NOOPDOOR not only utilized LODEINFO during the campaign, but also utilized the new backdoor to exfiltrate data from compromised enterprise networks. The intention behind these behavior is likely espionage, as Threat Actors targeted critical infrastructure sectors and academic institutions, which are often intelligence gathering targets.

APT10

APT10 is a sophisticated Chinese state-sponsored cyber espionage group that has been active as early as 2006, according to the Department of Defense. The information security community widely believes the group's focus is to support Chinese national security goals by gathering intelligence against the relevant targets. APT10 often targets various critical infrastructure sectors such as communications, manufacturing and various public sectors.

Cuckoo Spear

Cybereason documented the campaign as “Cuckoo Spear”. Cuckoo Spear is related to the APT10 Intrusion Set because of the links made between various incidents from Threat Actors “Earth Kasha” and “MirrorFace” including both APT10’s old arsenal (LODEINFO) and new arsenal presented in this report.

This attribution is made based on four main aspects :

- The arsenal used, mainly **NOOPLDR** and **NOOPDOOR**, which were first known to the public in January 2024 but remained on compromised networks for more than two years at most
- The **LODEINFO** malware was identified during an incident also involving **NOOPLDR/NOOPDOOR**, linking them together
- The domains used as C2 infrastructure, showing many similarities with other APT10 campaigns
- The similarity in techniques employed by the Threat Actor to carry out their attacks

Arsenal

This section describes the arsenal related to Cuckoo Spear observed on the different incidents Cybereason worked on and the links that tie them together.

Backdoor	Incident A	Incident B	Incident C	Incident D
Cobalt Strike **GOSICLOADER**			YES	
LODEINFO				YES
NOOPLDR-DLL	YES	YES		

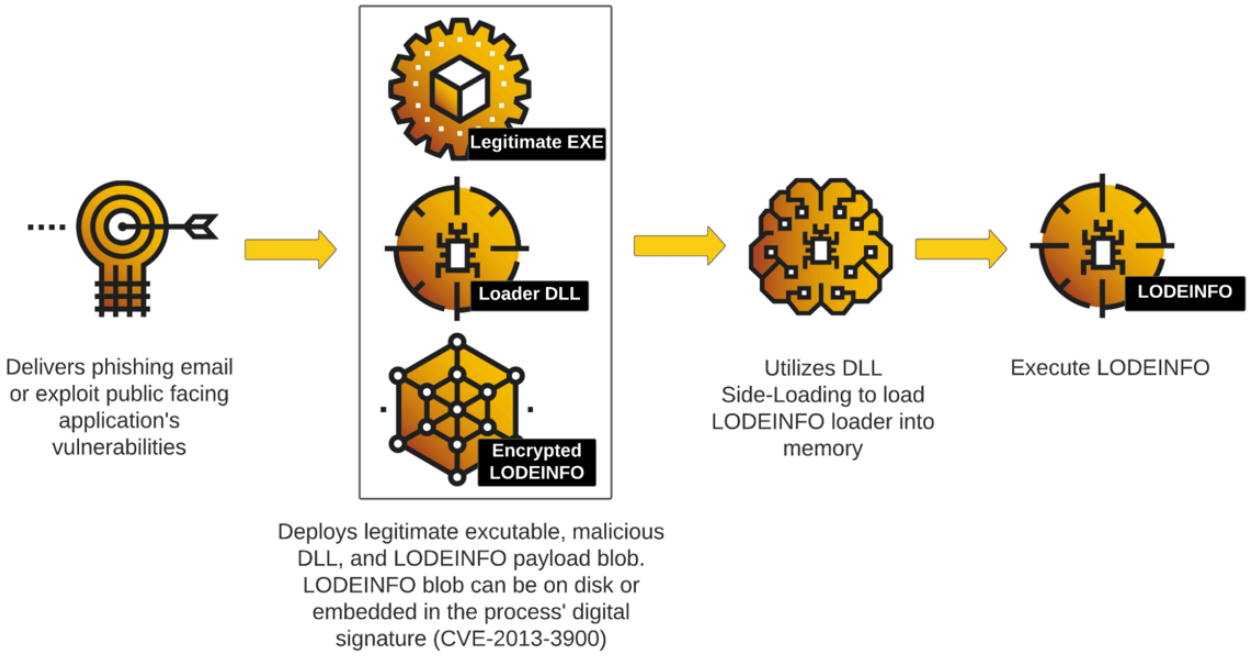
NOOPLDR-C#	YES	YES		YES
DOWNJPIT	YES			
Incident Start Date	**April 2021**	**May 2021**	**November 2021**	**October 2023**

Terminology

Cybereason re-used the naming convention established by Trend Micro and ESET, naming the loader **NOOPLDR** in reference to the **NOOPDOOR** backdoor that is loaded afterwards. The names used in this report are the following:

- **Campaign:** Cuckoo Spear
- **Intrusion Set:** APT10
- **Threat Actor:** Earth Kasha / MirroFace
- **LODEINFO:** Initial malware identified in one case where NOOPLDR and NOOPDOOR were discovered
- **NOOPLDR-C#:** C# Loader which loads NOOPDOOR
- **NOOPLDR-DLL:** DLL Loaderwhich loads NOOPDOOR
- **NOOPDOOR:** Shellcode loaded that will act as a Command and Control beacon

LODEINFO



LODEINFO Execution Flow

LODEINFO, named by JPCERT in their blog, is a backdoor known to be active since 2019. Threat actors often deploy LODEINFO by utilizing DLL Side-loading, which loads LODEINFO loader DLL into legitimate executables. This execution flow attempts to load LODEINFO shellcode and execute the backdoor in memory. The currently known LODEINFO version is v0.7.3 and was observed first in the wild in October 2023.

The interesting aspect of LODEINFO is that the developers change the C2 command functionality after the version update, often removing the previously supported commands. For example, developers removed the C2 command to remove files (*rm)* between v0.6.3 and v0.6.6, but this functionality came back after v0.6.8. The comparative graph of backdoor commands provided by ITOCHU Cyber & Intelligence Inc consists of detailed information of the backdoor commands as well as the changes over the version v0.6.5, v0.7.1, and v0.7.2/v0.7.3.

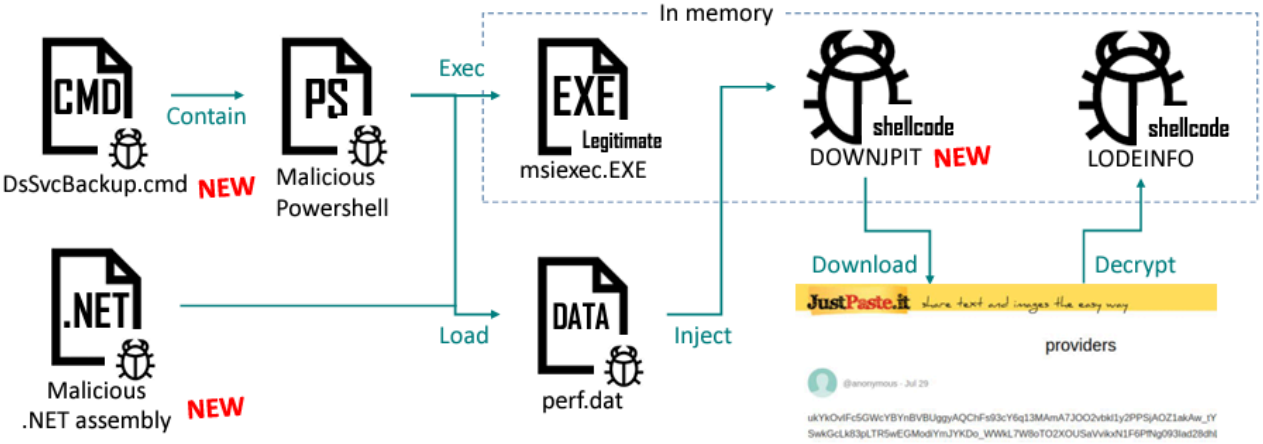
GOSICLoader

GOSICLoader is a Golang based malware loader, which is responsible for loading Cobalt Strike. The loader abuses DLL Side-Loading, which loads GOSICLoader into legitimate process *jcef_helper.exe*, a JetBrains plugin process.

GOSICLoader Execution Flow

DOWNJPIT

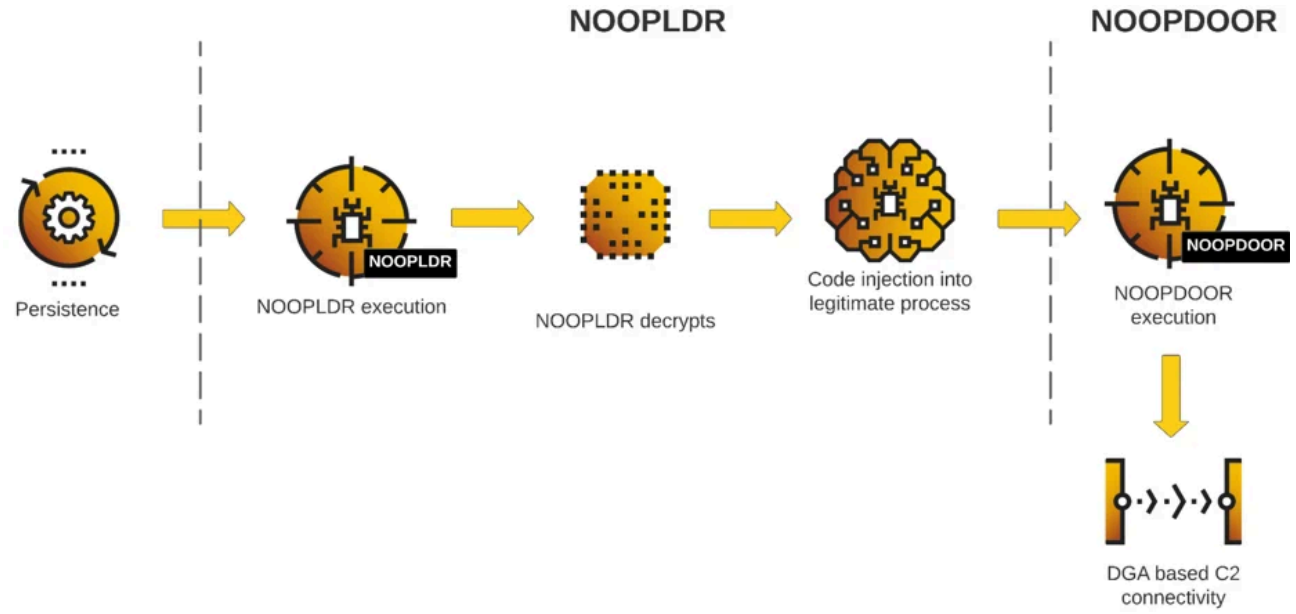
DOWNJPIT is a fileless downloader dubbed by Kaspersky. DOWNJPIT is responsible for downloading, decrypting and executing LODEINFO.



DOWNJPIT Execution Flow Presented By Kaspersky HITCON 2021

DOWNJPIT has been spotted in one of the incidents related to Cuckoo Spear .

NOOPLDR / NOOPDOOR



NOOPLDR/NOOPDOOR Execution Flow

In this report, Cybereason exhibits a new backdoor utilized by Threat Actors called NOOPDOOR, as dubbed by ESET and Trend Micro. NOOPDOOR is a 64-bit modular backdoor which utilizes DGA-based C2 communication. The backdoor is seen to be loaded by a loader called NOOPLDR, which appears to have two different variants.

- C#: Variant which relies on MSBuild task
- DLL: Variant which relies on DLL side-loading technique

NOOPLDR is responsible for decrypting and executing NOOPDOOR, which utilizes DGA to actively communicate with the C2 server.

Cybereason observed LODEINFO and NOOPDOOR both in one case. As mentioned in different reports, Threat Actors started to incorporate NOOPDOOR in the new campaigns. Based on the analysis of LODEINFO and as well as on the observation of these campaigns, LODEINFO appears to be utilized as a primary backdoor and NOOPDOOR acts as a secondary backdoor, keeping persistence within the corporate network.

Observed Behaviors / TTPs

In this section, Cybereason outlines all the behaviors observed during incidents associated with the Cuckoo Spear campaign.

Initial Access

Other reports documenting this Threat Actor mentioned the following vulnerabilities used as initial access vector :

- **CVE-2023-27997**: Buffer overflow vulnerability in FortiOS and FortiProxy, which allows attackers to execute arbitrary commands.
- **CVE-2023-28461**: Remote code execution (RCE) vulnerability on Array Network Array AG series and vxAG.
- **CVE-2023-45727**: Unauthenticated XML External Entity (XXE) vulnerability in Proself Enterprise/Standard Edition, Proself Gateway Edition, and Proself Mail Sanitize Edition, which allows attackers to gain unauthorized access to the environment.

In the Cuckoo Spear campaign, two out of those three vulnerabilities have been identified as initial access vector leads.

Spear-phishing is the common initial access technique observed by Threat Actors utilizing LODEINFO; however, malicious actors have started to shift their tactics to exploiting vulnerabilities.

Persistence

NOOPDOOR must be loaded first on the victim machines, which is done through persistence mechanisms and Cybereason observed three different methods.

- **Scheduled Tasks**
- **WMI Consumer Events**
- **Windows Services (Service DLL)**

Scheduled Task

Threat Actors maintain persistence within the environment by abusing Scheduled Tasks. The scheduled task consists of execution of MSBuild, which loads malicious XML files and compiles the NOOPDOOR loader at runtime.

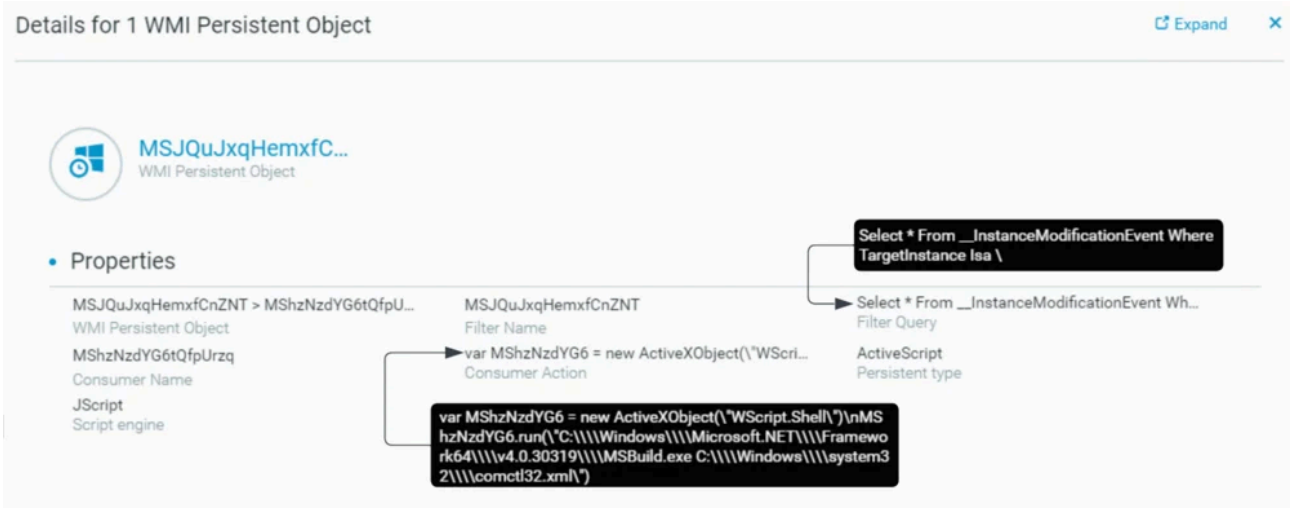
MSBuild Execution Via Schedule Task

WMI Event Consumers

The Threat Actors leverage the WMI event consumer, which executes the main action when it gets triggered by a filter. The Threat actor then utilizes ActiveScript, which appears to execute in the JScript engine. For the consumer

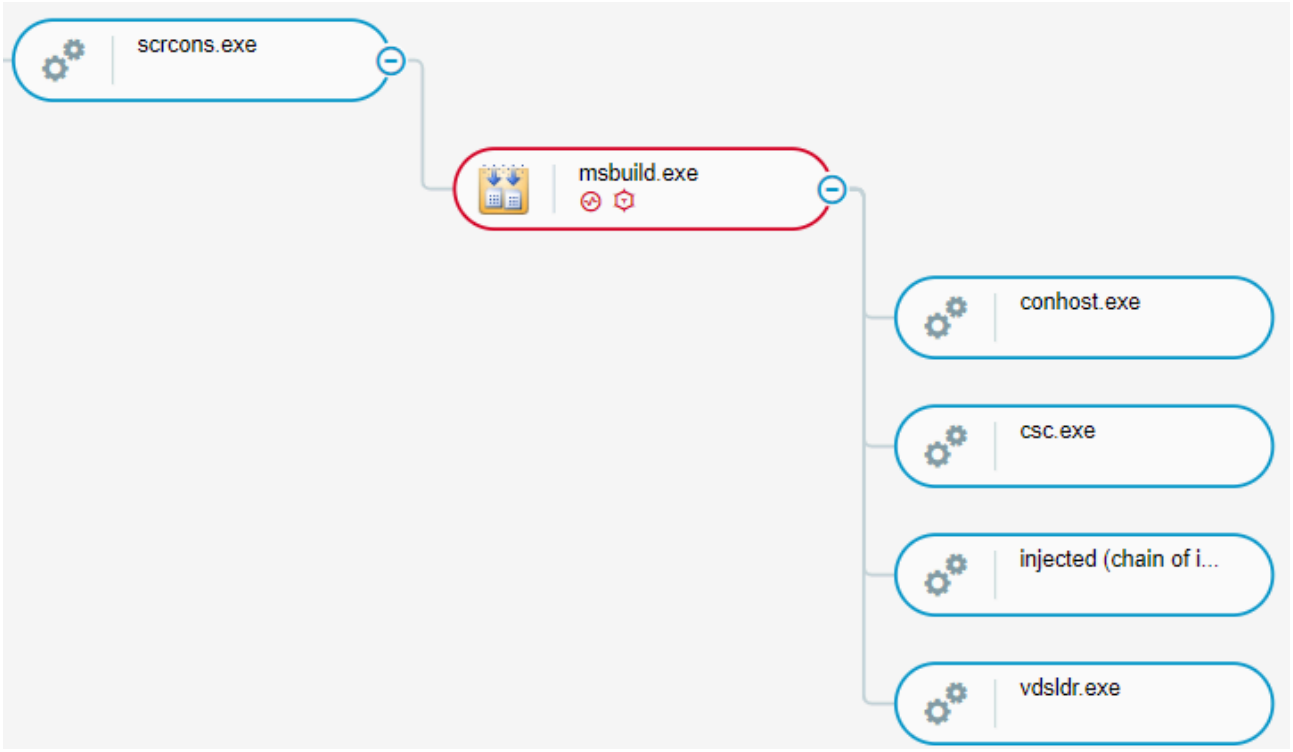
action in this WMI event, the Threat Actor leverages MSBuild execution for NOOPDOOR loader, similar to the scheduled task which also leverages MSBuild.

Utilizing WMI event consumers are the alternate methodologies to persist within the environment.



WMI Event Consumers For NOOPDOOR

The process responsible for hosting WMI event consumers for scripting, such as ActiveScript, is *scrcons.exe*, which then spawns necessary processes declared in its scripts.



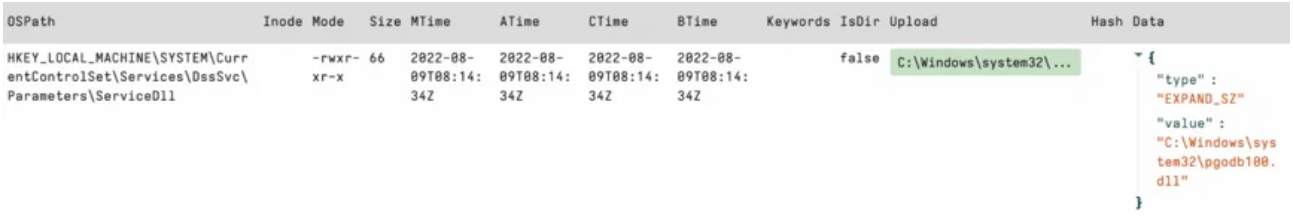
NOOPLDR/NOOPDOOR Attack Tree

Windows Services

Threat actors also maintain persistence within the environment by creating malicious services that load unsigned DLL files.

In this case, unsigned DLL files are written to the C:\Windows\System32\ folder.

An entry in the registry is found, indicating that this DLL is loaded under svchost.exe process through a Service DLL.



Extract From Velociraptor IR Tool

The screenshot above shows a registry key involving a Service named *DssSvc* and a ServiceDll configured to be C:\Windows\System32\pgodb100.dll, which is in fact NOOPLDR (DLL version).

To summarize how Service DLLs are used as persistence, one technique involves creating a new Windows service hosted by svchost.exe. Here is an overview of the process:

- **Threat Actor drops the NOOPLDR (DLL version) file on the disk**: The DLL (for instance, *pgodb100.dll*) containing the code to execute on system reboot is located in *C:\Windows\System32*.
- **Create a New Service**: Establish a new service (for instance, *DssSvc*) with binPath set to *svchost.exe*.
- **Add ServiceDll Value**: Include the ServiceDll value in the *DssSvc* service, pointing to the DLL dropped in step 1.
- **Modify Registry**: Adjust HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost to specify the service's loading group.
- **Start the Service**: Initiate the *DssSvc* service.
- **Execution**: The *DssSvc* is launched, and its service DLL (pgodb100.dll, in our example) is loaded into an *svchost.exe* process.

This method leverages the Windows service infrastructure to achieve persistence by loading a custom DLL into *svchost.exe*, ensuring execution of specified code on system restarts.

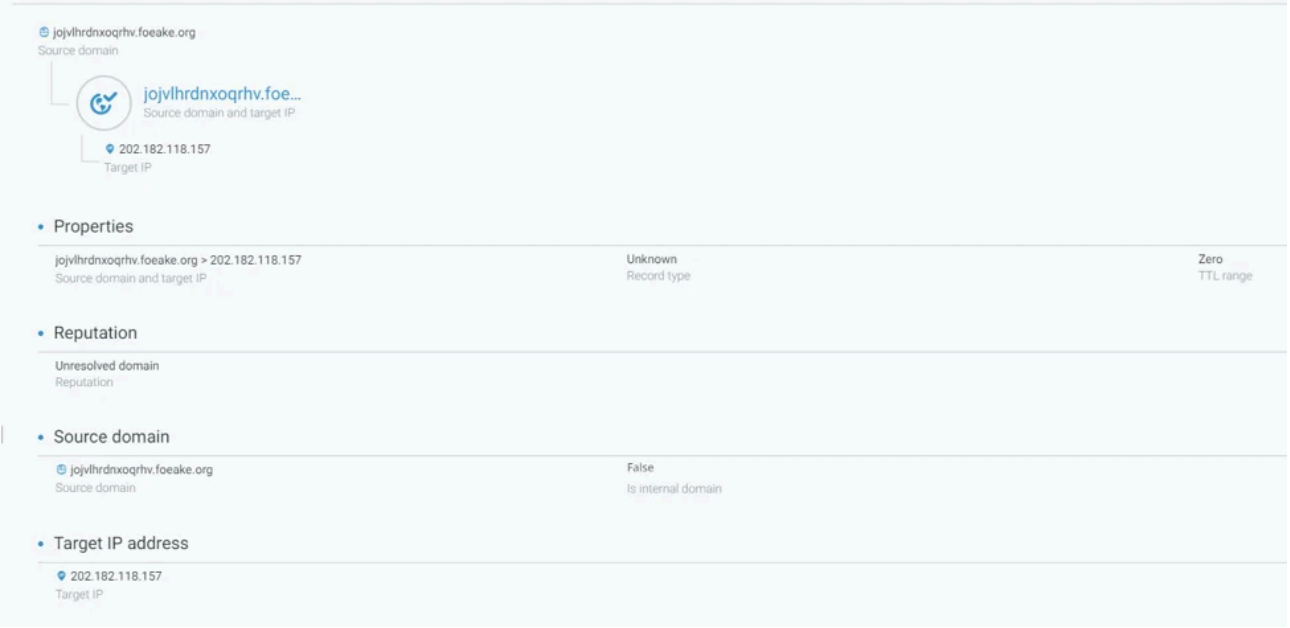
In a detection perspective, defenders can look for the loading of unsigned DLL under the following process:

- **svchost.exe -k netsvcs**

Command & Control

Domain Generation Algorithm (DGA)

Cybereason observed several domains created by the DGA, and will detail these aspects in the following sections.



DGA Sample

Connection To Internal Pivot

Aside from the C2 domains that connect to external ip addresses, Cybereason has also observed internal C2 communications amongst the infected machines.

Cybereason identified processes injected with NOOPDOOR listening on the following CP ports :

- 5984
- 47000
- 8532

This allows the Threat Actor to connect to internal machines in case the external C2 is unavailable, streamlining C2 connections to an internal server that will be the sole point of communication with the Internet.

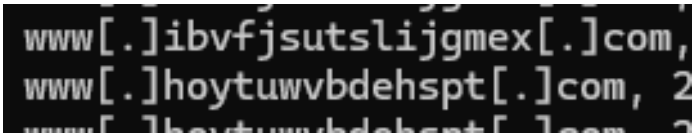
Internal Communication To NOOPDOOR On Port 5984

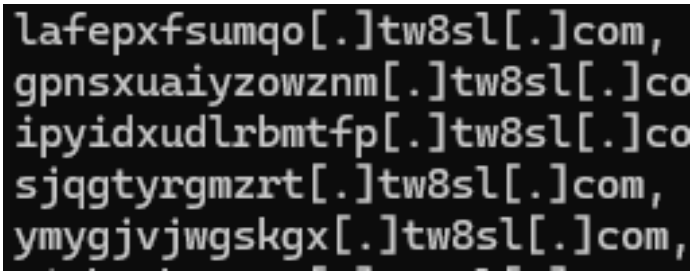
This also gives the Threat Actor a capability to remotely control a machine that is not connected to the Internet or has limited outbound network capability.

C2 Servers & Domains

During the different cases Cybereason observed, Domain Generation Algorithm (DGA) have been used :

- *www.[DGA][.]com* with [DGA] being the generated domain based off parameters such as the current date and a C2 URL hardcoded in LODEINFO
- *www.[DGA][.]net* with [DGA] same as above
- *[DGA].[C2 domain].com*





Use of NO-IP Services

Threat actors often use dynamic DNS services like No-IP to manage their command and control (C2) infrastructure. Since the IP address of a C2 server can change frequently, using a dynamic DNS service helps maintain consistent communication with malware or compromised systems.

Due to their nature, it's more difficult for cybersecurity systems to track and blacklist IP addresses associated with Dynamic DNS services as, by design, the IP addresses change on a regular basis. This dynamic aspect helps Threat Actors avoid detection by security tools that rely on IP blacklists. Threat actors can create redundant systems, ensuring that if one domain is taken down or blocked, others are still operational.

Cybereason identified the Threat Actor behind these attacks using the following domains through a service similar to NO-IP :

- *3utilities[.]com*
- *onthewifi[.]com*
- *redirectme[.]net*

- *serveblog[.]net*
- *zapto[.]org*
- *hopto[.]org*

Use of Specific Domains

In addition to these NO-IP domains, Cybereason also witnessed additional domains being used. These domains were mainly registered by companies such as NAMECHEAP or Tucows.

Infrastructure IP Addresses

In the screenshot below, Cybereason lists the IP addresses related to the domains that were resolved during the observation period of each incident :

IP ADDRESSES - 40

Country code desc | Sort by | Export | Tools | Help

	Detections	Autonomous System	Country Code
124.157.64.0/18			
168.100.10.238 168.100.8.0/22	8 / 89	399629 (BLNWX)	NL
159.223.211.201 159.223.192.0/19	0 / 89	14061 (DIGITALOCEAN-ASN)	NL
172.104.71.234 172.104.64.0/18	0 / 89	63949 (Akamai Connected Cloud)	JP
172.105.202.138 172.105.0.0/16	0 / 89	63949 (Akamai Connected Cloud)	JP
172.105.210.214 172.105.0.0/16	0 / 89	63949 (Akamai Connected Cloud)	JP
202.182.118.157 202.182.96.0/19	0 / 89	20473 (AS-CHOOPA)	JP
207.148.97.235 207.148.64.0/18	3 / 89	20473 (AS-CHOOPA)	JP
45.76.212.38 45.76.0.0/15	2 / 89	20473 (AS-CHOOPA)	JP
45.77.12.11 45.76.0.0/15	0 / 89	20473 (AS-CHOOPA)	JP
45.77.12.212 45.76.0.0/15	2 / 89	20473 (AS-CHOOPA)	JP
5.180.44.139 5.180.44.0/22	0 / 89	18978 (ENZUINC)	JP
89.233.109.69 89.233.108.0/23	1 / 89	29802 (HVC-AS)	JP
108.160.130.45 108.160.128.0/20	0 / 89	20473 (AS-CHOOPA)	JP
139.162.81.6 139.162.0.0/16	0 / 89	63949 (Akamai Connected Cloud)	JP
139.162.89.34 139.162.0.0/16	0 / 89	63949 (Akamai Connected Cloud)	JP
144.168.36.38 144.168.32.0/20	0 / 89	29802 (HVC-AS)	JP
164.90.235.245 164.90.224.0/20	0 / 89	14061 (DIGITALOCEAN-ASN)	DE

Resolved Cuckoo Spear IPs (VirusTotal)

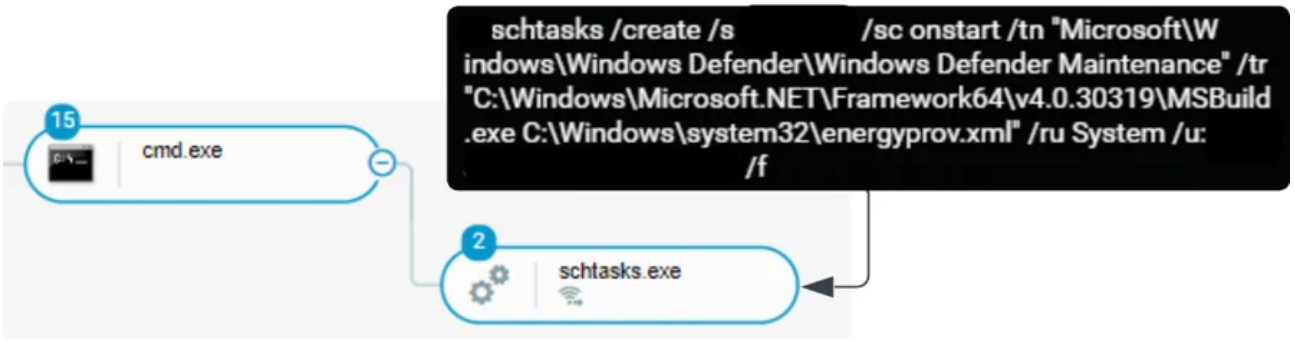
Those IP addresses are mostly hosted in Japan under hosting services such as Akamai or AS-CHOOPA. The other countries are :

- US (Cloudflare)
- DE
- NL
- VN

Lateral Movement

Scheduled Task

In one instance from Cuckoo Spear, the Threat Actor utilizes scheduled tasks to conduct lateral movement within the environment. They create the scheduled task by abusing *schtasks.exe*, which then creates the scheduled task responsible for executing the C# Loader via MSBuild execution on the startup.



Scheduled Task Creation On Remote Machine

Once the scheduled task creation is complete, another instance of *schtasks.exe* executes the created task immediately on the remote machine

Defense Evasion

The Threat Actor deployed several techniques of defense evasion in both NOOPDOOR and NOOPLDR.

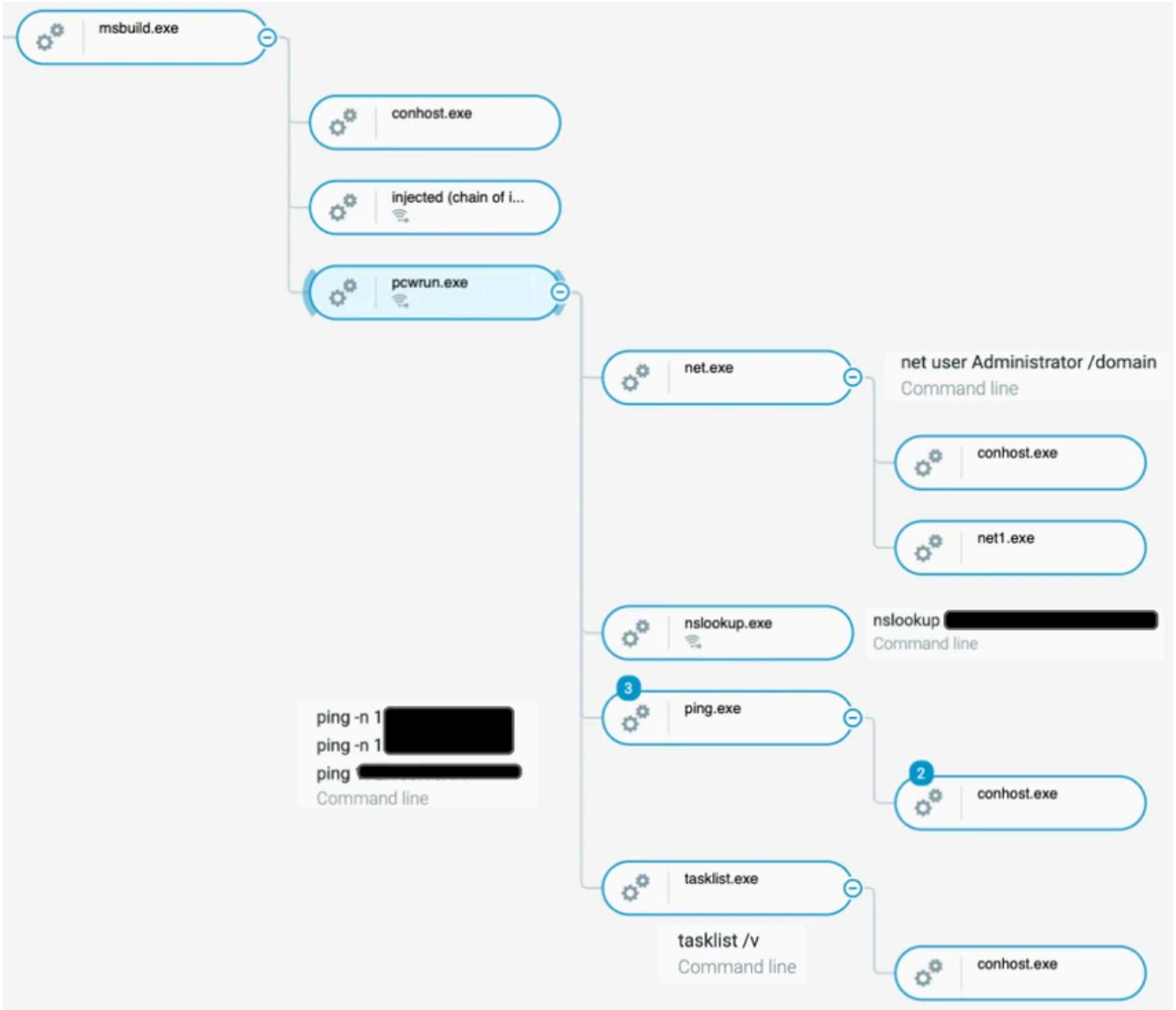
Aside from the attacker tools, the Threat Actor also deleted event logs on target systems.

Discovery Activity

The Threat Actor also displayed post-exploitation behavior, discovering the Active Directory through *net.exe* commands or the local network through *ping.exe* and *nslookup.exe* tools.

- **Msbuild.exe** : resulting from the persistence capability, this command will be responsible for injecting NOOPLOADER inside *pcwrun.exe* after spawning the process

- **Pcwrun.exe** or another arbitrary executable file present in C:\Windows\System32\ - This process is created by the code loaded by *msbuild.exe*. As stated earlier, that process name varies depending on the C2 configuration
    - **net user Administrator /domain** - Active Directory discovery related to the domain administrator account
    - **nslookup** - This command was used to discover existing machines on the network and their internal IP addresses
    - **ping -n 1 [redacted]** - This command is used to check connectivity to the specified IP of internal machines being searched by the Threat Actor
    - **tasklist /v** - This verbose command line under tasklist.exe indicates that detailed information about running processes is being gathered, potentially for reconnaissance or to find processes to inject into or terminate.



Post-Exploitation Behavior Attack Tree

In one incident, the Threat Actors utilized the following CMD commands as part of the post-exploitation.

/ccopy \\[REDACTED]\C$\Windows\System32\Winevt\Logs\security.evtx

/cdel C:\Users\[REDACTED]AppData\Local\Temp\Cookie-* /f /q

/cdel \\[REDACTED]\C$\Windows\System32\RegSSHelper.exe

/cdel security.evtx

/cnet group "domain controllers" /domain

/cnet use * /del /y

/cnet use \\[REDACTED]\ipc$ [REDACTED] /user:[REDACTED]

/cnet use \\[REDACTED]\netlogon [REDACTED] /user:[REDACTED]

/cnet user [REDACTED] /domain

/cnet user [REDACTED] /domain

/cnet user [REDACTED] /domain

/cnet user [REDACTED] /domain

/cnslookup [REDACTED]

/cschtasks /create /s [REDACTED] /sc onstart /tn "Microsoft\Windows\Windows Defender\Windows Defender Maintenance" /tr "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\MSBuild.exe C:\Windows\system32\[REDACTED].xml" /ru System /u:"[REDACTED]" /p:"[REDACTED]" /f

/cschtasks /run /s [REDACTED] /tn "Microsoft\Windows\Windows Defender\Windows Defender Maintenance" /u:"[REDACTED]" /p:"[REDACTED]"

These findings are very similar to those from JPCERT published back in 2023 :

- **No change in infrastructure trends**
  - Using hosting service such as Vultr, CHOOPA and LINODE
  - IP Geolocation is mostly Japan

CnC server	version	Hosting service	location
45.77.28[.]124	v0.5.9, v0.6.2	Vultr	Ōi, Saitama, Japan
172.105.223[.]216	v0.6.2, v0.6.5	LINODE	Tokyo, Tokyo, Japan
202.182.108[.]127	v0.6.2, v0.6.5	CHOOPA	Ōi, Saitama, Japan
103.175.16[.]39	v0.6.3	Mondoze	Kuala Lumpur, Kuala Lumpur, Malaysia
5.8.95[.]174	v0.6.3	G-Core Labs S.A.	Urayasu, Tokyo, Japan
172.104.112[.]218	v0.6.5	LINODE	Ōi, Saitama, Japan

Source : https://jsac.jpcert.or.jp/archive/2023/pdf/JSAC2023_1_6_minakawa-saika-kubokawa_en.pdf

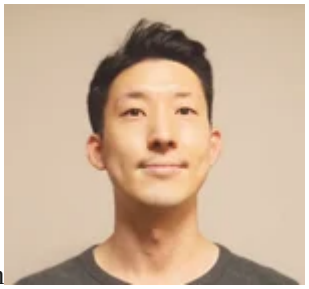
About The Researchers

Jin Ito, Incident Response Engineer, Cybereason IR Team

Jin Ito is an Incident Response Engineer with the Cybereason Incident Response team. Formerly an Incident Response Engineer at Fujitsu, he holds several cybersecurity certificates such as GREM, GCFA, and OSCP. Aside from his digital forensic responsibilities, he loves creating and reverse engineering malware.

Loïc Castel, Incident Response Investigator, Cybereason IR Team

Loïc Castel is an Investigator with the Cybereason IR team. Loïc analyses and researches critical incidents and cybercriminals, in order to better detect compromises. In his career, Loïc worked as a security auditor in well-known organizations such as ANSSI (French National Agency for the Security of Information Systems) and as Lead Digital Forensics & Incident Response at Atos. Loïc loves digital forensics and incident response, but is also interested in offensive aspects such as vulnerability research.



Kotaro Ogino, CTI Analyst, Cybereason Security Operations Team

Kotaro is a CTI Analyst with the Cybereason Security Operations team. He is involved in threat hunting, threat intelligence enhancements and Extended Detection and Response (XDR). Kotaro has a bachelor of science degree in information and computer science.

Source: https://www.cybereason.com/blog/cuckoo-spear-analyzing-noopdoor