Large-Scale StrelaStealer Campaign in Early 2024

By Benjamin Chang, Goutam Tripathy, Pranay Kumar Chhaparwal, Anmol Maurya, Vishwa Thothathri

Published: 2024-03-22 · Archived: 2026-04-05 13:24:17 UTC

Executive Summary

StrelaStealer malware steals email login data from well-known email clients and sends them back to the attacker's C2 server. Upon a successful attack, the threat actor would gain access to the victim's email login information, which they can then use to perform further attacks. Since the first emergence of the malware in 2022, the threat actor behind StrelaStealer has launched multiple large-scale email campaigns, and there is no sign of them slowing down.

Recently, our researchers have identified a wave of large-scale StrelaStealer campaigns impacting over 100 organizations across the EU and U.S. These campaigns come in the form of spam emails with attachments that eventually launch the StrelaStealer's DLL payload.

In an attempt to evade detection, attackers change the initial email attachment file format from one campaign to the next, to prevent detection from the previously generated signature or patterns. The malware author often updates the DLL payload with better obfuscation and anti-analysis tricks, which makes it increasingly difficult for analysts and security products to analyze.

This article delves deeper into the timeline of these more recent attacks and the evolving tactics employed by the malware.

Through detection and intelligence provided by Advanced WildFire, Palo Alto Networks customers are better protected from StrelaStealer through the following products:

- Cortex XDR with Advanced WildFire is able to help detect new variants of StrelaStealer. Cortex XDR helps prevent StrelaStealer's attack chain.
- Next-Generation Firewalls with Cloud-Delivered Security Services, including Advanced WildFire detection, Advanced URL Filtering and DNS Security categorize known C2 domains and IPs as malicious.
- Prisma Cloud Defender agents should be deployed on cloud-based Windows VMs to ensure they are protected from these known malicious binaries. WildFire signatures can be used by both Palo Alto Networks cloud services to ensure cloud-based Windows VM runtime operations are being analyzed and those resources are protected.
- Organizations can also engage the Unit 42 Incident Response team to help with a compromise or to provide a proactive assessment to lower your risk.

Introduction to StrelaStealer

StrelaStealer malware is an email credential stealer first documented by DCSO_CyTec in their blog on Medium published on Nov. 8, 2022. Since the first emergence of the malware, the threat actor behind StrelaStealer has

launched multiple large-scale email campaigns, typically across the EU and U.S.

For example, the last large-scale campaign launched in 2023 was around the November time frame. Our researchers have observed a new campaign launched in late January 2024 targeting multiple industries across the EU and U.S.

The basic goal of the StrelaStealer has not changed much, and the payload DLL is still identifiable with the strela string. However, we can see that the threat actor has updated the malware in an attempt to evade detection.

This new variant of StrelaStealer is now delivered through a zipped JScript and it employs an updated obfuscation technique in the DLL payload. We will provide more technical analysis and detail in this article.

Last Large-Scale Campaign of 2023

Since the emergence of StrelaStealer, we have observed its threat operators initiate multiple large-scale campaigns. WildFire researchers observed that the last large-scale campaign in 2023 happened in November, targeting organizations in the U.S. and EU. Figure 1 below shows the timeline of the 2023 November campaign.

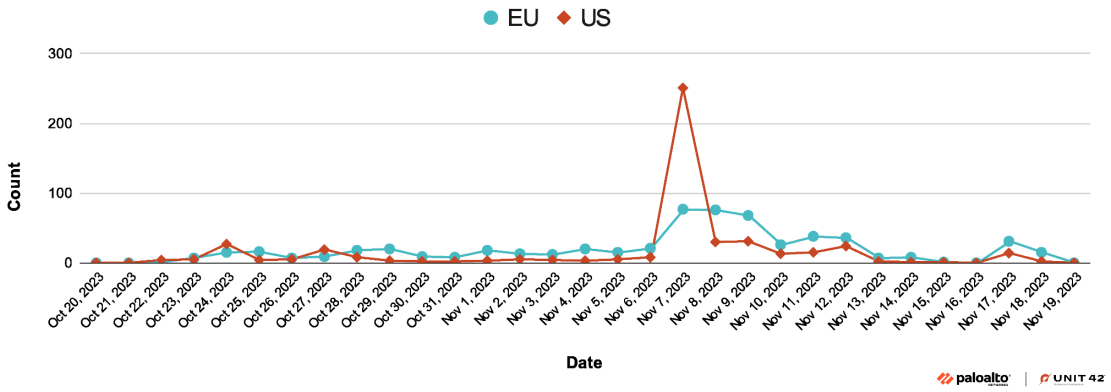


Figure 1. November 2023 campaign.

Recent Large-Scale Campaign in 2024

A month into 2024, the threat actors behind StrelaStealer launched another large-scale campaign, again targeting organizations in the same geographic regions. Figure 2 below shows the timeline of the recent campaign that peaked on Jan. 29, 2024.

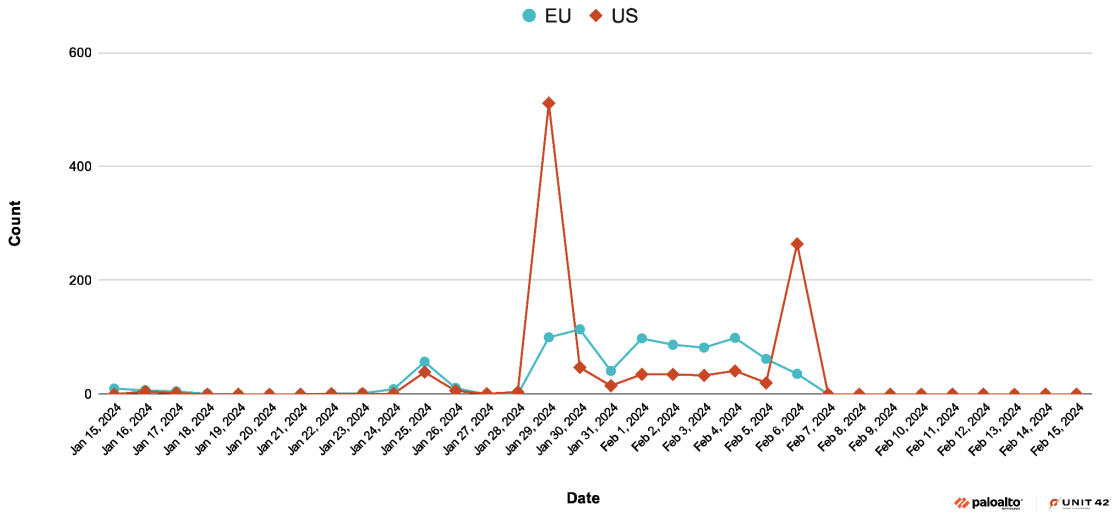


Figure 2. January 2024 campaign.

The language of the StrelaStealer spam email seen during this campaign is localized and the subject line has the pattern of Factura/Rechnung/invoice####. Figure 3, below, is a sample email in German.

Figure 3. Example spam email.

Figure 4 shows that while this recent campaign seems to target organizations in many industries, organizations in the high tech industry have been the largest target.

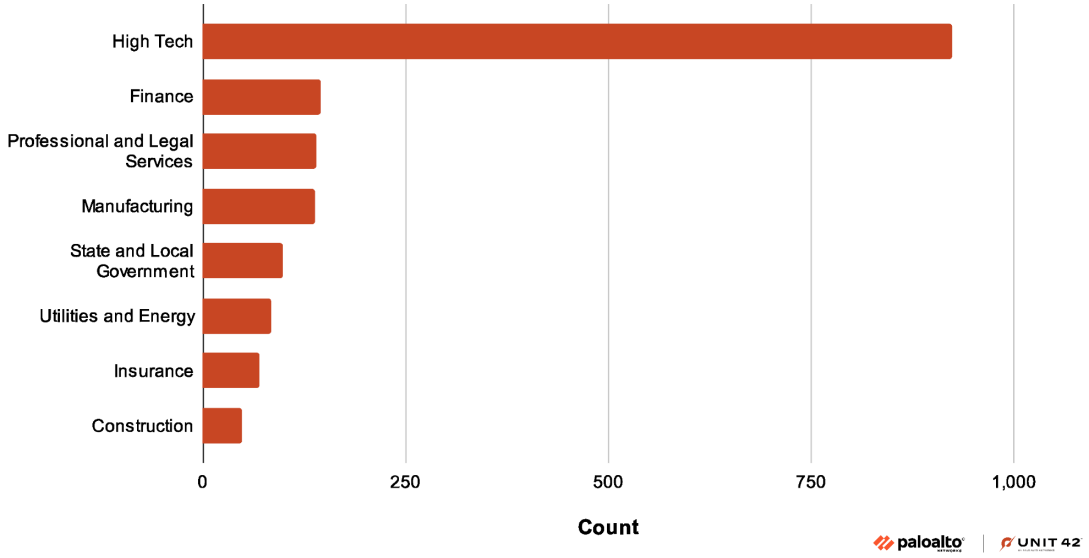


Figure 4. Count of StrelaStealer samples seen for top eight industries.

Technical Analysis of New StrelaStealer Variant

Original StrelaStealer Infection Chain and Payload Recap

As discussed in DCSO's blog on Medium, earlier versions of StrelaStealer infect the system via email with an attached .iso file. The .iso file contains a .lnk file and a HyperText Markup Language (HTML) file. The technique makes use of polyglot files, which are files that can be treated differently based on the executing application.

When the victim clicks on the .lnk file contained within the .iso file, it executes the HTML and then invokes rundll32.exe to execute the embedded StrelaStealer payload. The initial payload has some encrypted strings, which are decrypted during the execution using a fixed XOR key, as shown in Figure 5.

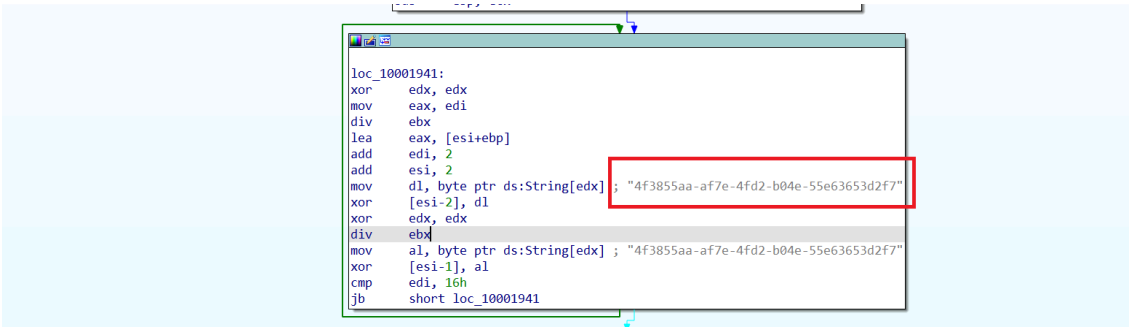


Figure 5. Decryption key.

Updated Infection Chain

The current version of StrelaStealer spreads through spear phishing emails that contain a ZIP file attachment. Once the user downloads and opens the archive, a JScript file is dropped onto the system.

The JScript file then drops a Base64-encrypted file and a batch file. The Base64-encrypted file is decoded with the certutil -f decode command, resulting in the creation of a Portable Executable (PE) DLL file. Depending on the

user's privileges, the file drops into either %appdata%\temp or c:\temp on the local disk. The DLL file is then executed through the exported function hello using rundll32.exe.

Please see Figure 6 for the infection chain of the previous version and the newer variant.

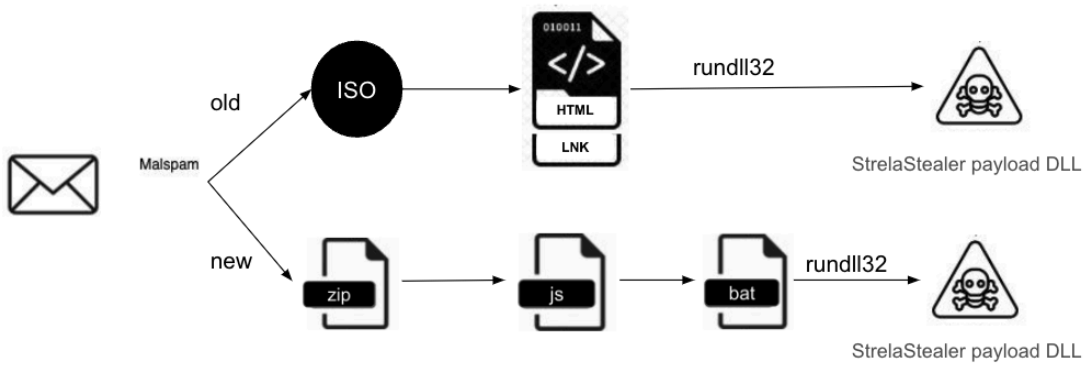


Figure 6. Infection chain.

Updated Packer

In the newest variant of StrelaStealer seen in the January 2024 campaign, the packer has evolved and employs a control flow obfuscation technique to render analysis more difficult.

The initial function shown in Figure 7 contains an example control flow obfuscation technique of excessively long code blocks consisting of numerous arithmetic instructions. This serves as an anti-analysis technique, potentially leading to timeouts during the execution of samples in a sandbox environment.

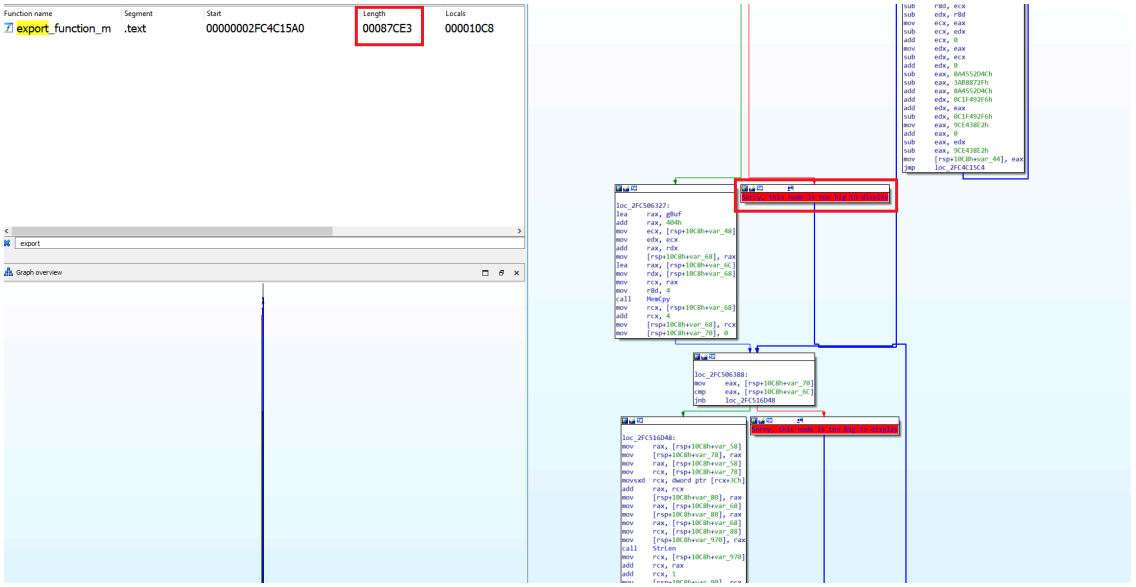


Figure 7. Obfuscation (excessively large code block).

Both the original and the new StrelaStealer payload are DLL files with a malicious export function called to launch the attack. Figure 8 shows the payload DLL's malicious export function side by side.

We can see that the older version of StrelaStealer (left side of Figure 8) was not well obfuscated as these function blocks are clean and easily readable when disassembled. However, the latest version on the right side of Figure 8

shows that the threat actors have employed control flow obfuscation to evade analysis and detection.

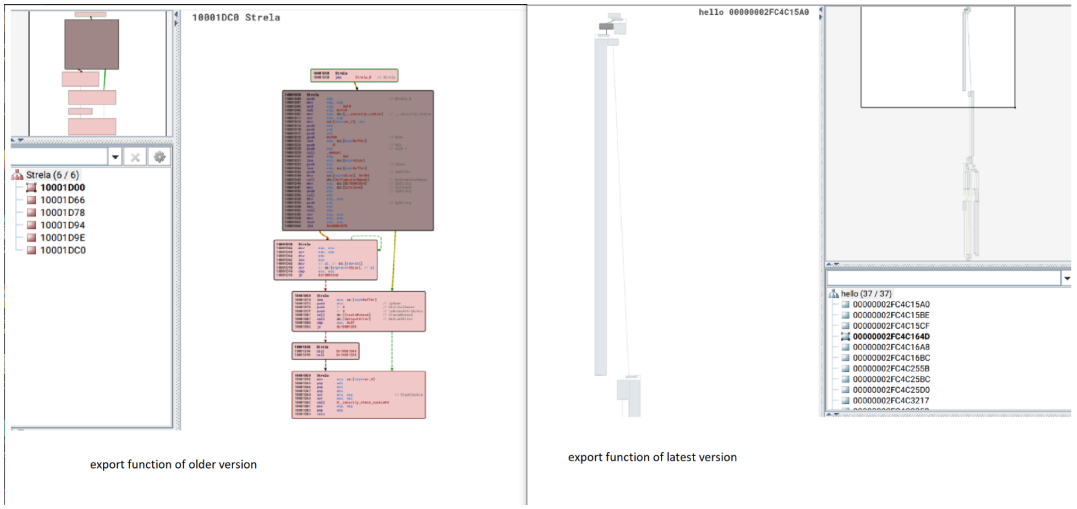
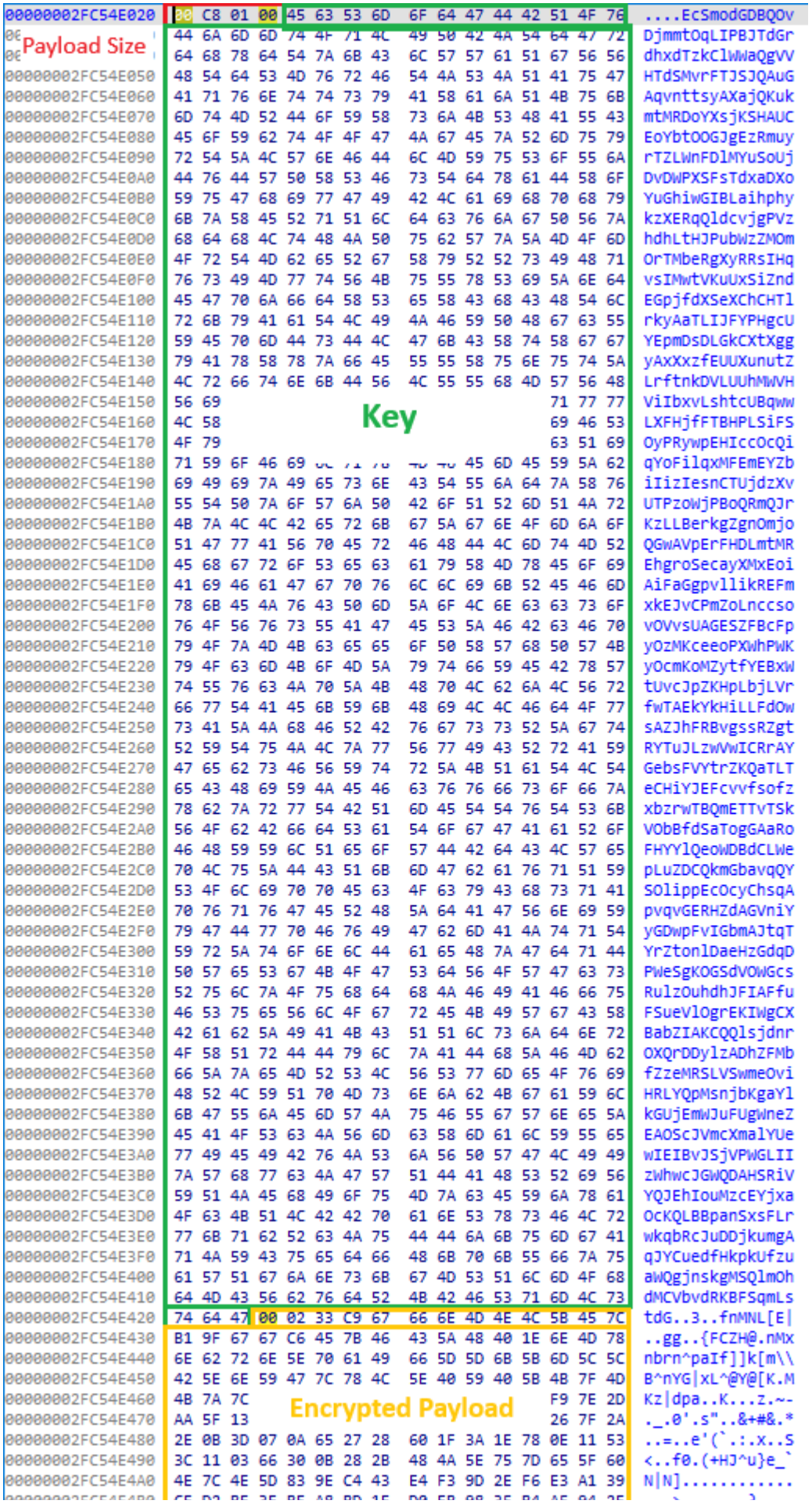


Figure 8. Export functions of old (left) and new (right) versions of StrelaStealer.

Based on the configuration shown in Figure 9, the payload size and decryption key are used to decrypt the payload. The decrypted payload is a memory-mapped PE file that is not similar to the one found in the earlier version of the StrelaStealer.


Payload Size
Key
Encrypted Payload

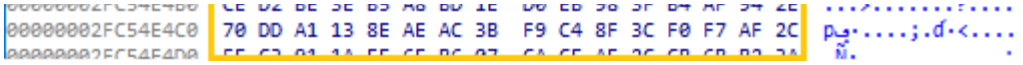


Figure 9. Encrypted payload.

The presence of strings like strela, server.php, key4.db and login.json within the decrypted payload provides an indication that it is associated with StrelaStealer.

The main purpose of StrelaStealer is to steal email login data from well-known email clients and send it back to the C2 server defined in the malware configuration, as shown in Figure 10.

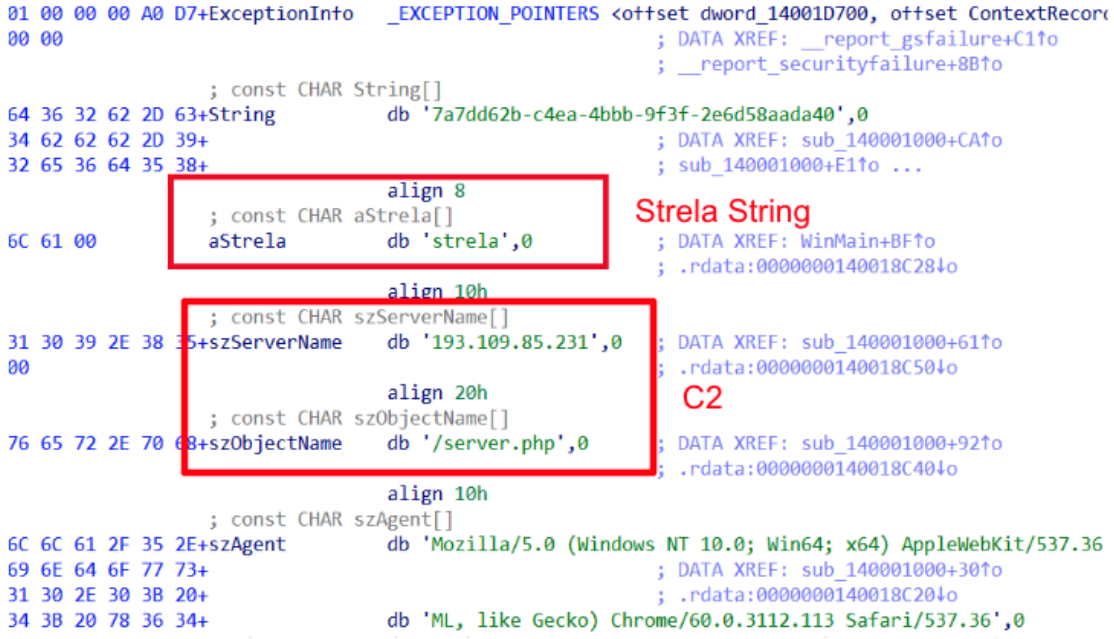


Figure 10. StrelaStealer string as well as C2 server name.

The StrelaStealer threat actor incorporated several noteworthy modifications, possibly as means to avoid being detected. For example, PDB strings (debugging symbol strings built in by the compiler) that were present in earlier versions of StrelaStealer, shown in Figure 11, can no longer be found in the samples from the latest campaign. This makes it less obvious that this is a StrelaStealer binary and could render certain naive static signatures useless if they relied on the existence of this string.

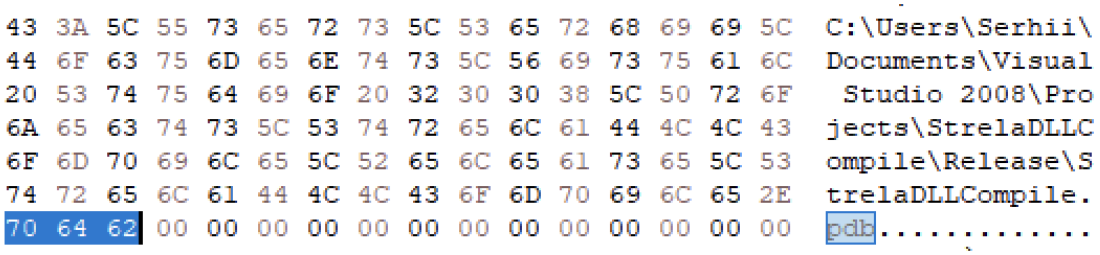


Figure 11. PDB string from an early StrelaStealer sample.

Figure 12 shows that the export name has changed from StrelaStealer to hello.

Ordinal	Function RVA	Name Ordinal	Name RVA	Name
(nFunctions)	Dword	Word	Dword	szAnsi
00000001	00001DC0	0000	0000AF87	Strela

earlier version of strela

Ordinal	Function RVA	Name Ordinal	Name RVA	Name
(nFunctions)	Dword	Word	Dword	szAnsi
00000001	000015A0	0000	0002903A	hello

latest version of strela

Figure 12. Export name changes from Strela to hello.

Conclusion

StrelaStealer malware is an active email credential stealer that is always evolving. With each new wave of email campaigns, threat actors update both the email attachment, which initiates the infection chain, and the DLL payload itself. Attackers do this to evade detection by security vendors.

Information stealers are not new to the threat landscape. Though not exactly novel, the various evasion techniques and updates employed by StrelaStealer are effective at evading detection from more reactive signature or pattern-based solutions.

Palo Alto Networks Protection and Mitigation

Through the detection and intelligence provided by Advanced WildFire, Palo Alto Networks customers are better protected from StrelaStealer through the following products:

- Cortex XDR with Advanced WildFire: With cloud-delivered static and dynamic analysis capabilities, Advanced WildFire is able to help detect new variants of StrelaStealer. Cortex XDR helps prevent StrelaStealer's attack chain.
- Next-Generation Firewalls with cloud-delivered security services including Advanced WildFire detection, Advanced URL Filtering and DNS Security categorize known C2 domains and IPs as malicious.
- Prisma Cloud Defender agents should be deployed on cloud-based Windows VMs to ensure they are protected from these known malicious binaries. WildFire signatures can be used by both Palo Alto Networks cloud services to ensure cloud-based Windows VM runtime operations are being analyzed and those resources are protected.
- The Unit 42 Incident Response team can also be engaged to help with a compromise or to provide a proactive assessment to lower your risk.

If you think you may have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

- North America Toll-Free: 866.486.4842 (866.4.UNIT42)
- EMEA: +31.20.299.3130
- APAC: +65.6983.8730
- Japan: +81.50.1790.0200

Palo Alto Networks has shared these findings with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Indicators of Compromise

SHA256 Hash	Filetype
0d2d0588a3a7cff3e69206be3d75401de6c69bcff30aa1db59d34ce58d5f799a e6991b12e86629b38e178fef129dfda1d454391ffbb236703f8c026d6d55b9a1	DLL
f95c6817086dc49b6485093bfd370c5e3fc3056a5378d519fd1f5619b30f3a2e aea9989e70ffa6b1d9ce50dd3af5b7a6a57b97b7401e9eb2404435a8777be054 b8e65479f8e790ba627d0deb29a3631d1b043160281fe362f111b0e080558680	EML
3189efaf2330177d2817cfb69a8bfa3b846c24ec534aa3e6b66c8a28f3b18d4b	ZIP
544887bc3f0dccb610dd7ba35b498a03ea32fca047e133a0639d5bca61cc6f45	JS
193[.]109[.]85[.]231	C2 server

Additional References

- New StrelaStealer malware steals your Outlook, Thunderbird accounts – Bleeping Computer
- Malware analysis/Digital forensic: Strela Stealer – Medium
- #ShortAndMalicious: StrelaStealer aims for mail credentials – Medium

---

Source: https://unit42.paloaltonetworks.com/strelastealer-campaign/