

Large-Scale StrelaStealer Campaign in Early 2024

By Benjamin Chang, Goutam Tripathy, Pranay Kumar Chhapparwal, 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.

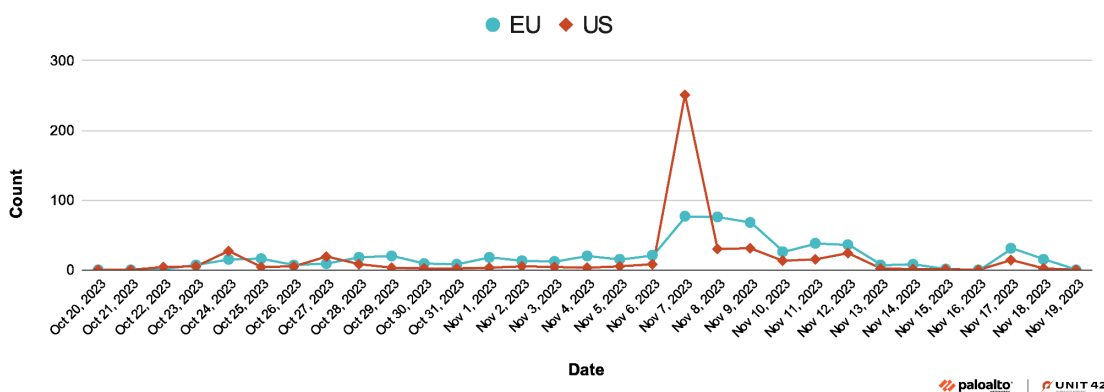


Figure 1. November 2023 campaign.

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.

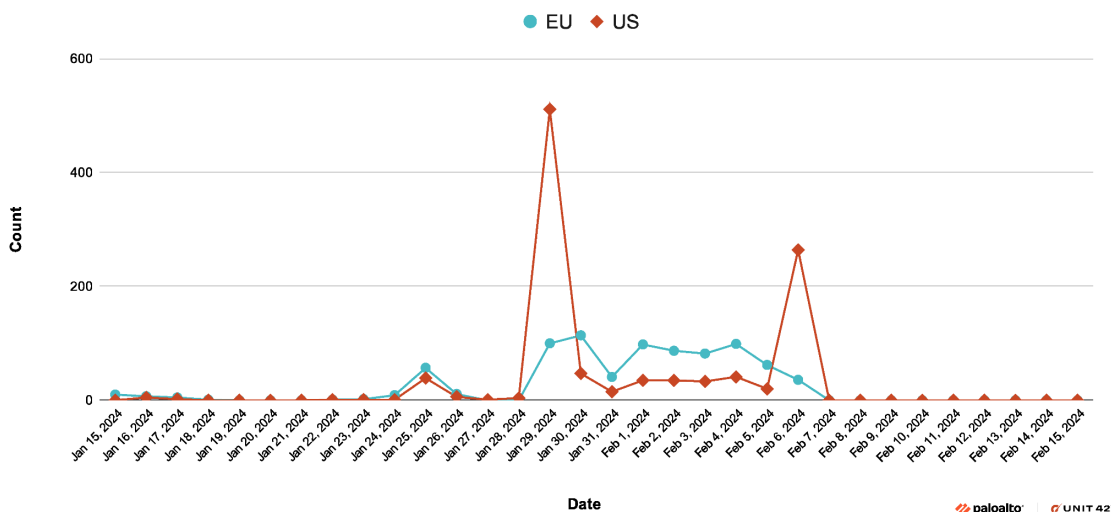
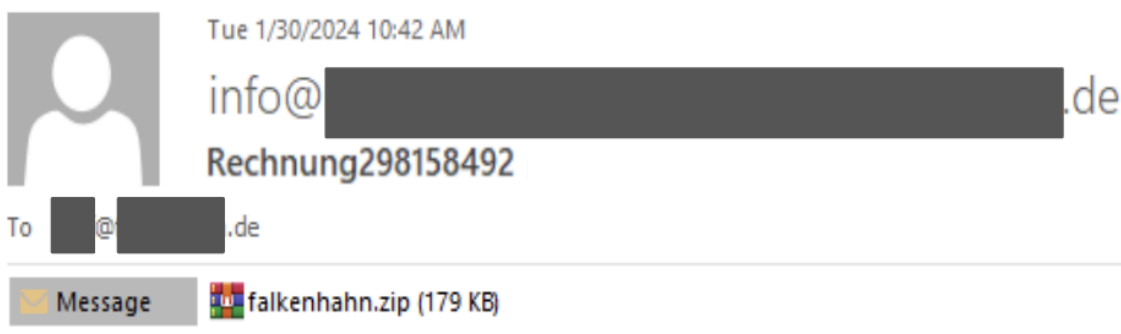


Figure 2. January 2024 campaign.

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.



Sehr geehrte Damen und Herren,
anbei als Anlage Ihre Rechnung im Pdf -Format.
Wir freuen uns auf ein baldiges Wiedersehen

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.

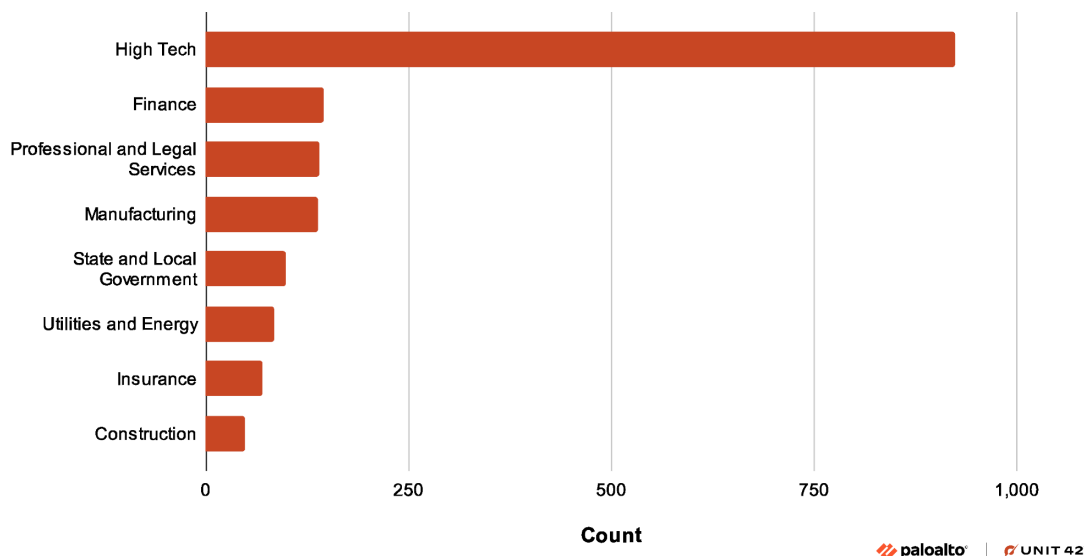


Figure 4. Count of StrelaStealer samples seen for top eight industries.

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.

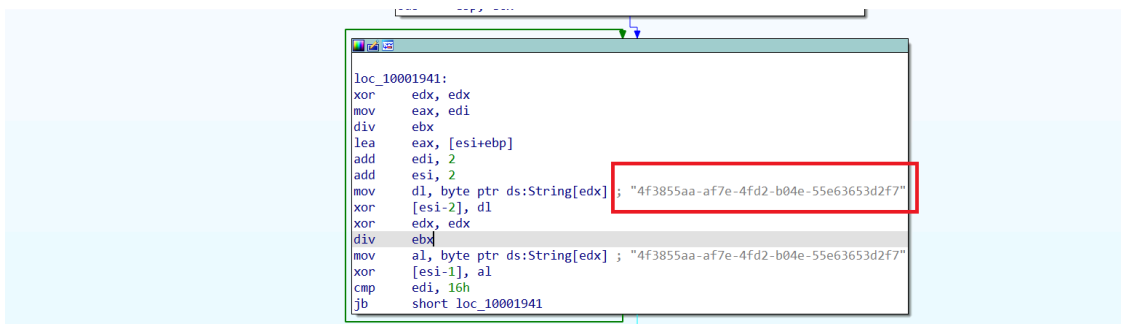


Figure 5. Decryption key.

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-encoded file and a batch file. The Base64-encoded 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.

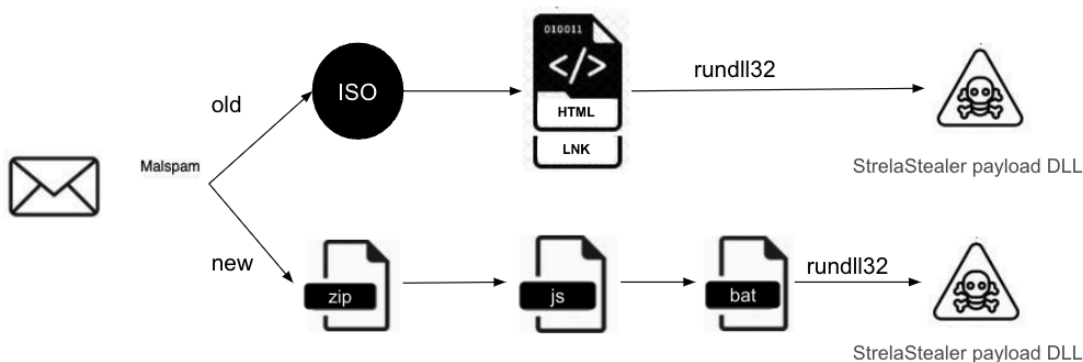


Figure 6. Infection chain.

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.

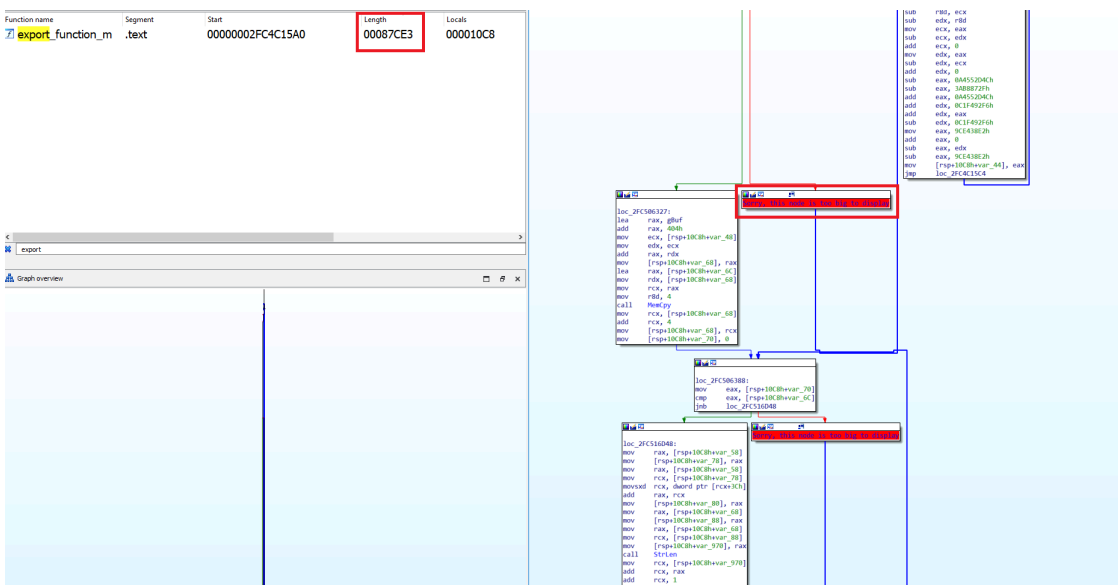


Figure 7. Obfuscation (excessively large code block).

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.

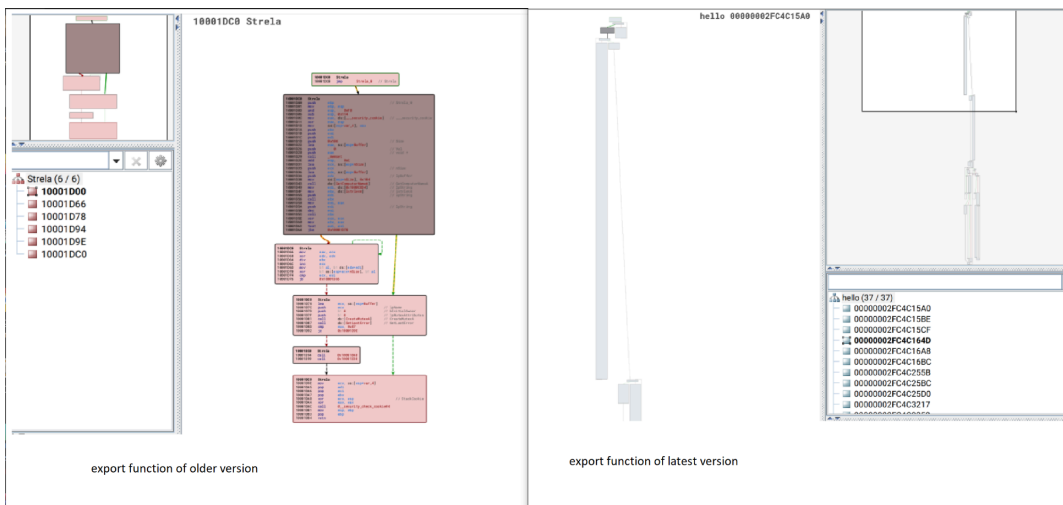


Figure 8. Export functions of old (left) and new (right) versions of StrelaStealer.

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.

00000002FC54E020	00 C8 01 00	45 63 53 6D	6F 64 47 44 42 51 4F 7E	...EcSmodGDBQOV
00000002FC54E050	44 6A 6D 6D 74 4F 71 4C	49 50 42 4A 54 64 47 72	DjmmtoQlIPBjTdr	
00000002FC54E060	64 68 78 64 54 7A 68 43	6C 57 57 61 51 67 56 56	dHxdTzkClwWiaQgVv	
00000002FC54E070	48 54 64 53 4D 76 72 46	54 4A 53 4A 51 41 75 47	HTdSMvrFTJ5JQAug	
00000002FC54E080	41 71 76 6E 74 74 73 79	41 58 61 6A 51 48 75 68	AqvnttsyAXajQKuk	
00000002FC54E090	6D 74 4D 52 44 6F 59 58	73 6A 48 53 48 41 55 43	mtMRDoYXsjKSHAUC	
00000002FC54E0A0	45 6F 59 62 74 4F 4F 47	4A 67 45 7A 52 6D 75 79	Eoybt0OGJgEzRmuy	
00000002FC54E0B0	72 54 5A 4C 57 6E 46 44	6C 4D 59 75 53 6F 55 6A	rTZLWnFDlMYuSouj	
00000002FC54E0C0	44 76 44 57 50 58 53 46	73 54 64 78 61 44 58 6F	DvDWPXSFsTdxadXo	
00000002FC54E0D0	59 75 47 68 69 77 47 49	42 4C 61 69 68 70 68 79	YuGhiwGIBLaihphy	
00000002FC54E0E0	68 7A 58 45 52 71 51 6C	64 63 76 6A 67 50 56 7A	kzXERqQldcvjgPVz	
00000002FC54E0F0	68 64 68 4C 74 48 4A 50	75 62 57 7A 5A 4D 4F 6D	hdhLth3PubwzZMOM	
00000002FC54E100	4F 72 54 4D 62 65 52 67	58 79 52 52 73 49 48 71	OrTMbeRgXyRRsIHq	
00000002FC54E110	76 73 49 40 77 74 56 48	75 55 78 53 69 5A 6E 64	vsIMwtVKuXSiZnd	
00000002FC54E120	45 47 70 6A 66 64 58 53	65 58 43 68 43 48 54 6C	EGpjfdXSeXChCHTl	
00000002FC54E130	72 68 79 41 61 54 4C 49	4A 46 59 50 48 67 63 55	rkyAaTLIJFYPhgCU	
00000002FC54E140	59 45 70 60 44 73 44 4C	47 68 43 58 74 58 67 67	YEpmDsDLGkCXTXgg	
00000002FC54E150	79 41 78 58 78 7A 66 45	55 55 58 75 6E 75 74 5A	yAxXzFEUUXunutz	
00000002FC54E160	4C 72 66 74 6E 68 44 56	4C 55 55 68 4D 57 56 48	LrftnkDVLUuHMVH	
00000002FC54E170	56 69	71 77 77	ViIbXvLshtcUBqww	
00000002FC54E180	4C 58	69 46 53	LXFHjffTBHPLSiFS	
00000002FC54E190	4F 79	63 51 69	OyPRYwpEHIccOcqI	
00000002FC54E1A0	71 59 6F 46 69	45 6D 45 59 5A 62	qYoFilqxMFEMeYZb	
00000002FC54E1B0	69 49 69 7A 49 65 73 6E	43 54 55 6A 64 7A 58 76	iIiIesnCTUjdZxv	
00000002FC54E1C0	55 54 50 7A 6F 57 6A 50	42 6F 51 52 6D 51 4A 72	UTPzowjPBoQRmQOr	
00000002FC54E1D0	48 7A 4C 4C 42 65 72 68	67 5A 67 6E 4F 6D 6A 6F	KzLLBerkGZgnOmjo	
00000002FC54E1E0	51 47 77 41 56 70 45 72	46 48 44 4C 6D 74 4D 52	QGwAVpErFHDLMtMR	
00000002FC54E1F0	45 68 67 72 6F 53 65 63	61 79 58 4D 78 45 6F 69	EhgroSecayXmxEoi	
00000002FC54E200	41 69 46 61 47 67 70 76	6C 6C 69 68 52 45 46 6D	AiFaGgpvllikREFm	
00000002FC54E210	78 68 45 4A 76 43 50 6D	5A 6F 4C 6E 63 63 73 6F	xKEJvCPmZolNccso	
00000002FC54E220	76 4F 56 76 73 55 41 47	45 53 5A 46 42 63 46 70	vOVvsUAGESZFBcFp	
00000002FC54E230	79 4F 7A 4D 48 63 65 65	6F 50 58 57 68 50 57 48	yOzMKceeoPXwhPwK	
00000002FC54E240	79 4F 63 6D 4B 6F 4D 5A	79 74 66 59 45 42 78 57	yOcmKomZytfYEBXw	
00000002FC54E250	74 55 76 63 4A 70 5A 48	48 70 4C 62 6A 4C 56 72	tUvcJpZKHplbjLvr	
00000002FC54E260	66 77 54 41 45 6B 59 68	48 69 4C 4C 46 64 4F 77	fwTAEkyKHILLFdow	
00000002FC54E270	73 41 5A 4A 68 46 52 42	76 67 73 73 52 5A 67 74	sAZJhFRBvgssRZgt	
00000002FC54E280	52 59 54 75 4A 4C 7A 77	56 77 49 43 52 72 41 59	RYTuJLzWwICRrAY	
00000002FC54E290	47 65 62 73 46 56 59 74	72 5A 48 51 61 54 4C 54	GebSfVYtrZKQaTLT	
00000002FC54E2A0	65 43 48 69 59 4A 45 46	63 76 76 66 73 6F 66 7A	eCHiYJEFcvvfsofz	
00000002FC54E2B0	78 62 7A 72 77 54 42 51	6D 45 54 54 76 54 53 68	xbzrwTBQmETTvtSk	
00000002FC54E2C0	56 4F 62 42 66 64 53 61	54 6F 67 47 41 61 52 6F	VobBfdSaTogGAaRo	
00000002FC54E2D0	46 48 59 59 6C 51 65 6F	57 44 42 64 43 4C 57 65	FHYy1QeowDBdCLWe	
00000002FC54E2E0	70 4C 75 5A 44 43 51 68	6D 47 62 61 76 71 51 59	pLUzDCQkmGbvqqY	
00000002FC54E2F0	53 4F 6C 69 70 70 45 63	4F 63 79 43 68 73 71 41	solippEcOcyChsqA	
00000002FC54E300	70 76 71 76 47 45 52 48	5A 64 41 47 56 6E 69 59	pvqvGERHZdAGVniY	
00000002FC54E310	79 47 44 77 70 46 76 49	47 62 6D 41 4A 74 71 54	yGDwpFvIGbmAJtqT	
00000002FC54E320	59 72 5A 74 6F 6E 6C 44	61 65 48 7A 47 64 71 44	YrZtonlDaeHzGdqD	
00000002FC54E330	50 57 65 53 67 4B 4F 47	53 64 56 4F 57 47 63 73	PWeSgKOGSdVOWGcs	
00000002FC54E340	52 75 6C 7A 4F 75 68 64	68 4A 46 49 41 46 66 75	RulzOuhdhJFIAffu	
00000002FC54E350	46 53 75 65 56 6C 4F 67	72 45 48 49 57 67 43 58	FSueVlogrEKIwgCX	
00000002FC54E360	42 61 62 5A 49 41 48 43	51 51 6C 73 6A 64 6E 72	BabZIAKcQqlsjdnr	
00000002FC54E370	4F 58 51 72 44 44 79 6C	7A 41 44 68 5A 46 4D 62	OXQrDDylzADhZFMb	
00000002FC54E380	66 5A 7A 65 4D 52 53 4C	56 53 77 6D 65 4F 76 69	fZzeMRSLSVnmeOvi	
00000002FC54E390	48 52 4C 59 51 70 4D 73	6E 6A 62 48 67 61 59 6C	HRLYQpmsnjbkgayl	
00000002FC54E400	68 47 55 6A 45 6D 57 4A	75 46 55 67 57 6E 65 5A	kGUjEmwJufUgwneZ	
00000002FC54E410	45 41 4F 53 63 4A 56 6D	63 58 6D 61 6C 59 55 65	EAOScJVmcXmalyUe	
00000002FC54E420	77 49 45 49 42 76 4A 53	6A 56 50 57 47 4C 49 49	wIEIBvJSjVPWGLII	
00000002FC54E430	7A 57 68 77 63 4A 47 57	51 44 41 48 53 52 69 56	zWhwcJGWQDAHSrIV	
00000002FC54E440	59 51 4A 45 68 49 6F 75	4D 7A 63 45 59 6A 78 61	YQJEhIouMzcEYjxa	
00000002FC54E450	4F 63 4B 51 4C 42 42 70	61 6E 53 78 73 46 4C 72	OckQLBBpanSxsFLr	
00000002FC54E460	77 68 71 62 52 64 7A 75	44 44 6A 68 75 6D 67 41	wkqBrcJUDDjkumGA	
00000002FC54E470	71 4A 59 43 75 65 64 66	48 6B 70 68 55 66 7A 75	qJYCuedfHkpkUfzu	
00000002FC54E480	61 57 51 67 6A 6E 73 68	67 4D 53 51 6C 6D 4F 68	awQgjnskGMSQlMh	
00000002FC54E490	64 4D 43 56 62 76 64 52	48 42 46 53 71 6D 4C 73	dMcvbvDRKBFsqmLS	
00000002FC54E4A0	74 64 47 00 02 33 C9 67	66 6E 4D 4E 4C 5B 45 7C	tdG...fnMNL[E]	
00000002FC54E4B0	B1 9F 67 67 C6 45 7B 46	43 5A 48 40 1E 6E 4D 78	..gg..{FCZH}.nMx	
00000002FC54E4C0	6E 62 72 6E 5E 70 61 49	66 5D 50 68 58 6D 5C 5C	nbrn^paIfj]k[m\	
00000002FC54E4D0	42 5E 6E 59 47 7C 78 4C	5E 40 59 40 58 48 7F 4D	B^nyG xl^@y@[K.M	
00000002FC54E4E0	4B 7A 7C	F9 7E 2D	Kz]dpa..K...z.~	
00000002FC54E4F0	AA 5F 13	26 7F 2A	..'.s'..&+#&.*	
00000002FC54E500	2E 0B 3D 07 0A 65 27 28	60 1F 3A 1E 78 0E 11 53	..'.e'(`.:.x..S	
00000002FC54E510	3C 11 03 66 30 0B 28 2B	48 4A 5E 75 7D 65 5F 60	<<.f0.(+H^u)e_	
00000002FC54E520	4E 7C 4E 5D 83 9E C4 43	E4 F3 9D 2E F6 E3 A1 39	N N].....	
00000002FC54E530	CF 02 05 25 05 48 00 15	00 50 00 25 04 45 04 25	..	

Key

Encrypted Payload

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
544887bc3f0dcc6b10dd7ba35b498a03ea32fca047e133a0639d5bca61cc6f45	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/>