

New Infostealer Campaign Targets Users via Spoofed Software Installers ~ VirusTotal Blog

blog.virustotal.com/2026/01/malicious-infostealer-january-26.html

Introduction

As part of our commitment to sharing interesting hunts, we are launching these 'Flash Hunting Findings' to highlight active threats. Our latest investigation tracks an operation active between January 11 and January 15, 2026, which uses consistent ZIP file structures and a unique behash ("4acaac53c8340a8c236c91e68244e6cb") for identification. The campaign relies on a trusted executable to trick the operating system into loading a malicious payload, leading to the execution of secondary-stage infostealers.

Findings

The primary samples identified are ZIP files that mostly reference the MalwareBytes company and software using the filename **malwarebytes-windows-github-io-X.X.X.zip**. A notable feature for identification is that all of them share the same **behash**.

behash: "4acaac53c8340a8c236c91e68244e6cb"

The initial instance of these samples was identified on January 11, 2026, with the most recent occurrence recorded on January 14.

Search: behash:"4acaac53c8340a8c236c91e68244e6cb" Save search Smart search

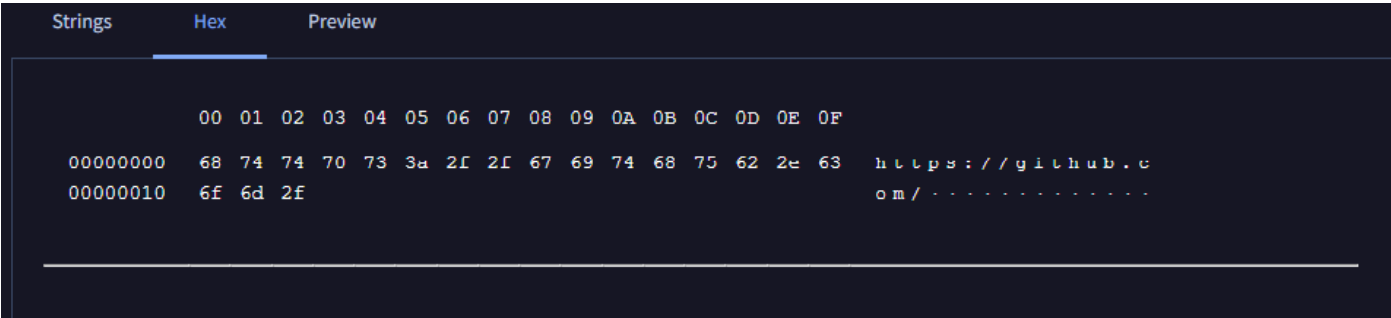
THREATS	IOCS	REPORTS & ANALYSIS	RULES	GRAPHS	COMMENTS
0	10	0	0	0	0

Matches - 10/10 Files

	Associations	GTI Score	Detections	First seen
5591156d120934f19f2bb92d9f9b1b32cb022134befef9b63c2191460be36899 malwarebytes-windows-github-io-1.5.3.zip zip contains-pe spreader checks-user-input detect-debug-environment long-sleeps	-	30 / 100	25 / 66	2026-01-14 21:33:47
42d53bf0ed5880616aa995cad357d27e102fb66b2fca89b17f92709b38706706 malwarebytes-windows-github-io-7.8.4.zip zip contains-pe spreader checks-user-input detect-debug-environment long-sleeps	-	30 / 100	25 / 66	2026-01-14 13:47:09
5aa6f4a57fb86759bcc9fc6c61b5f74c0ca74604a22084f9e0310840aa73664 malwarebytes-windows-github-io-6.5.5.zip zip spreader contains-pe checks-user-input detect-debug-environment long-sleeps	-	30 / 100	25 / 66	2026-01-14 13:43:33
84021dcfad522a75bf00a07e6b5cb4e17063bd715a877ed01ba5d1631cd3ad71 malwarebytes-protection-github-io-4.11.1.zip zip detect-debug-environment long-sleeps checks-user-input spreader contains-pe	-	30 / 100	27 / 64	2026-01-13 11:25:16
ca8467ae9527ed908e9478c3f0891c52c0266577ca59e4c80a029c256c1d4fce malwarebytes-windows-github-io-7.13.5.zip zip spreader long-sleeps contains-pe checks-user-input detect-debug-environment	-	30 / 100	30 / 68	2026-01-13 07:44:16
9619331ef9ff6b2d40e77a67ec86fc81b050eeb96c4b5f735eb9472c54da6735 malwarebytes-windows-github-io-3.88.4.zip zip contains-pe long-sleeps spreader detect-debug-environment checks-user-input	-	30 / 100	29 / 66	2026-01-12 19:32:01

All of these ZIP archives share a nearly identical internal structure, containing the same set of files across the different versions identified. Of particular importance is the DLL file, which serves as the initial malicious payload, and a specific TXT file found in each archive. This text file has been observed on VirusTotal under two distinct filenames: **gitconfig.com.txt** and **Agreement_About.txt**.

The content of the [TXT file](#) holds no significant importance for the intrusion itself, as it merely contains a single string consisting of a GitHub URL.



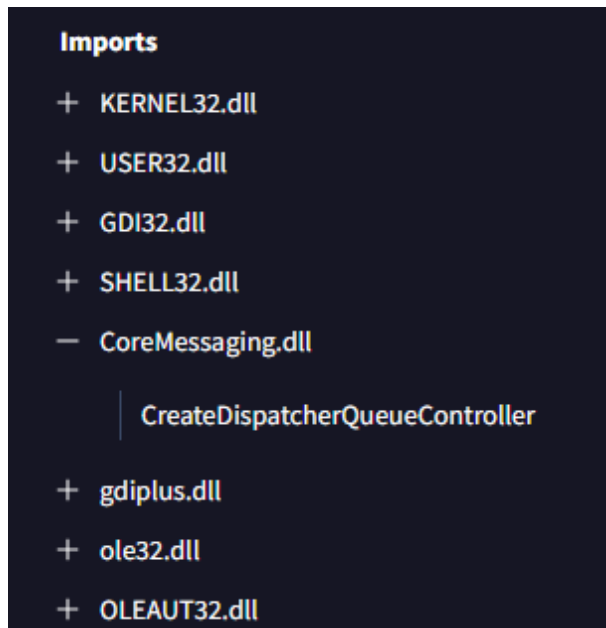
However, this TXT is particularly valuable for pivoting and infrastructure mapping. By examining its "execution parents," analysts can identify additional ZIP archives that are likely linked to the same malicious campaign. These related files can be efficiently retrieved for further investigation using the following VirusTotal API v3 endpoint:

/api/v3/files/09a8b930c8b79e7c313e5e741e1d59c39ae91bc1f10cdefa68b47bf77519be57/execution_par

A screenshot of a web browser displaying the VirusTotal API v3 endpoint response for the file 09a8b930c8b79e7c313e5e741e1d59c39ae91bc1f10cdefa68b47bf77519be57. The page shows a table of 'Execution Parents (290)' with columns for Scanned, Detections, Type, and Name. The table lists various ZIP files and their associated detection counts and names.

Scanned	Detections	Type	Name
2025-11-09	27 / 66	ZIP	openiv-download-8.87.2.zip
2025-12-16	21 / 69	ZIP	logitech-g-hub-github-io-3.21.3.zip
2025-12-28	15 / 66	ZIP	unlocked-fps-windows-git-github-io-1.43.5.zip
2025-12-04	25 / 70	ZIP	05e5a9bb50a54b8ba682d9741024d795a3302d79f9272f093702523b44c3bc49
2025-11-05	23 / 70	ZIP	r-e-p-o-download-game.github.io_1.41.3.zip
2025-12-07	17 / 69	ZIP	lonelyscreen-download-github-io-2.89.1.zip
2026-01-12	28 / 68	ZIP	malwarebytes-windows-github-io-8.8.9.zip
2026-01-13	28 / 68	ZIP	krita-download-windows-github-io-2.96.4.zip
2025-12-24	14 / 68	ZIP	netlimiter-desktop-github-io-8.89.3.zip
2025-12-17	23 / 69	ZIP	letsview-download-github-io-1.55.5.zip
2026-01-11	0 / 66	ZIP	asus-armourycrate-github-io-8.40.1.zip
2025-12-21	25 / 69	ZIP	10aeffc682c8c639ca4e4a678350b61f48d36b54761367268e044087b76d539d

The primary payload of this campaign is contained within a malicious DLL named **CoreMessaging.dll**. Threat actors are utilizing a technique known as [DLL Sideload](#) to execute this code. This involves placing the malicious DLL in the same directory as a legitimate, trusted executable (EXE) also found within the distributed ZIP file. When an analyst or user runs the legitimate EXE, the operating system is tricked into loading the malicious CoreMessaging.dll.



The identified DLLs exhibit distinctive metadata characteristics that are highly effective for pivoting and uncovering additional variants within the same campaign. Security analysts can utilize specific hunting queries to track down other malicious DLLs belonging to this activity. For instance, analysts can [search](#) for samples sharing the following unique signature strings found in the file metadata:

```
signature:"Peastaking plenipotence ductileness chilopodous codicillary."
```

```
signature:"© 2026 Eosinophil LLC"
```

Furthermore, the exported functions within these DLLs contains unusual alphanumeric strings. [These exports](#) serve as reliable indicators for identifying related malicious components across different stages of the campaign:

```
exports:15Mmm95m11RbfjH1VUyelyFCf exports:2d1SKetPzvo1mHDN4FYgv
```

Finally, another observation for behavioral analysis can be found in the **relations** tab of the ZIP files. These files document the full infection chain observed during sandbox execution, where the sandbox extracts the ZIP, runs the legitimate EXE, and subsequently triggers the loading of the malicious DLL. Within the **Payload Files** section, additional payloads are visible. These represent secondary stages dropped during the initial DLL execution, which act as the final malware samples. These final payloads are primarily identified as infostealers, designed to exfiltrate sensitive data.

Payload Files (9) ⓘ			
Scanned	Detections	Type	Name
-	-	file	472cc3a240bc552c2a0d75866e942ee2cb9e9454ab7b00378a8ed0196be1eb97
2026-01-14	38 / 72	Win32 EXE	C:\Windows\u2r6mchdl.exe
-	-	file	6a2d6a4a547dac5faec8c76438d77066b3b6fa550cb01e76f1c56f471888004a
-	-	file	6e850d1541c90f161b5bbe2f3bdceaab92fc29391b76dcfb5b3f6ee3b05c8cc6
-	-	file	871938c1a6d6b5e33627be3ade5a11b266e0d7fe90dadedb3dde87fe83e4fcc78
-	-	file	ba27682751f190f8233253026d187f9903fb57a9b2f8df7733d445e07028b833
-	-	file	cbc5990644a752545ea150c5ce5c52ba522c975886c12588a433ca013c9f2cc5
2026-01-14	27 / 72	Win32 DLL	C:\Windows\9g4z1.exe
-	-	file	fa2d63916b01987ed7f98e4729dbf119211a7974ab1b69d0af889034690668a7

Analysis of all the ZIP files behavioral relations reveals a recurring payload file consistently flagged as an infostealer. This malicious component is identified by various YARA rules, including those specifically designed to detect signatures associated with stealing cryptocurrency wallet browser extension IDs among others.

Crowdsourced YARA rules ⓘ

Matches rule `INDICATOR_SUSPICIOUS_Binary_Embedded_Crypto_Wallet_Browser_Extension_IDs` from ruleset `indicator_suspicious` at <https://github.com/ditekshen/detection> by `ditekSHen`
↳ Detect binaries embedding considerable number of cryptocurrency wallet browser extension IDs. - 1 day ago

Matches rule `INDICATOR_SUSPICIOUS_Binary_Embedded_MFA_Browser_Extension_IDs` from ruleset `indicator_suspicious` at <https://github.com/ditekshen/detection> by `ditekSHen`
↳ Detect binaries embedding considerable number of MFA browser extension IDs. - 1 day ago

Matches rule `Macos_Infostealer_Wallets_8e469ea0` from ruleset `Macos_Infostealer_Wallets` at <https://github.com/elastic/protectioins-artifacts> by `Elastic Security`

Matches rule `HKTL_Meterpreter_inMemory` from ruleset `gen_metasploit_payloads` at <https://github.com/Neo23x0/signature-base> by `netbiosX, Florian Roth`
↳ Detects Meterpreter in-memory - 1 day ago

Matches rule `ReflectiveLoader` from ruleset `gen_loaders` at <https://github.com/Neo23x0/signature-base> by `Florian Roth (Nextron Systems)`
↳ Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended - 1 day ago

Matches rule `INDICATOR_SUSPICIOUS_Binary_References_Browsers` from ruleset `indicator_suspicious` at <https://github.com/ditekshen/detection> by `ditekSHen`
↳ Detects binaries (Windows and macOS) referencing many web browsers. Observed in information stealers. - 1 day ago

Matches rule `INDICATOR_SUSPICIOUS_References_SecTools` from ruleset `indicator_suspicious` at <https://github.com/ditekshen/detection> by `ditekSHen`
↳ Detects executables referencing many IR and analysis tools - 1 day ago

Dynamic Analysis Sandbox Detections ⓘ

The sandbox `C2AE` flags this file as: `STEALER (BrowserStealerGeneric)`

Security vendors' analysis on 2026-01-12T14:36:56 UTC ▼

Popular threat label ⓘ `trojan.lazy/chromelevator`

Threat categories `trojan` `hacktool`

Family labels `lazy` `chromelevator` `hack`

To identify and pivot through the various secondary-stage payloads dropped during this campaign, analysts can utilize a specific `behash` identifier. These files represent the final infection stage and are primarily designed to exfiltrate credentials and crypto-wallet information. The following [behash](#) provides a reliable pivot point for uncovering additional variants.

`behash:5ddb604194329c1f182d7ba74f6f5946`

behash:5ddb604194329c1f182d7ba746f5946

Save searchSmart search

THREATS0

IOCS-203

REPORTS & ANALYSIS0

RULES0

GRAPHS0

COMMENTS0

▽ >

First seen asc

Brief

Sort by

Matches - 20/-203 Files

Associations

GTI Score

Detections

First seen

62006477bba363227cfe00d9a3d936adba8be1e42a143226f5bb384406b55bc

C:\Windows\kfa4w4.exe

peexepayload64bits

-

60 / 100

32 / 72

2026-01-06 14:25:39

154e345c71a981eb70215103ca3cb3434c07c7deed99c40e5e7fd9a24e6cae81

/home/pet1k/ss/malware/2026-01-08_2c6f1cf03760ef98a76da3f2d04fc594_cobalt-strike_icedid_luca-stealer_njrat_satacom_stealc

peexe64bitspayload

-

60 / 100

49 / 71

2026-01-06 15:35:49

e96ef7d5f8729c30ed6dbe55531a7d4813299f236df60df771e02f0019239b4f

C:\Windows\j1eyk.exe

peexepayload64bits

-

60 / 100

33 / 72

2026-01-06 17:13:10

205411fa4df352db90e10529e92662f300cbe16db37df149e430de10fb49267f

C:\Windows\lka8p55uu.exe

peexe64bitspayload

-

60 / 100

34 / 72

2026-01-06 18:06:22

IOCs

We have created a [public VirusTotal Collection](#) to share all the IOCs in an easy and free way. Below you can find the main IOCs related to the ZIP files and DLLs too.

```
import "pe"

rule win_dll_sideload_eosinophil_infostealer_jan26
{
  meta:
    author = "VirusTotal"
    description = "Detects malicious DLLs (CoreMessaging.dll) from an infostealer campaign impersonating Malwarebytes, Logitech, and others via DLL sideloading."
    reference = "https://blog.virustotal.com/2026/01/malicious-infostealer-january-26.html"
    date = "2026-01-16"
    behash = "4acaac53c8340a8c236c91e68244e6cb"
    target_entity = "file"
    hash = "606baa263e87d32a64a9b191fc7e96ca066708b2f003bde35391908d3311a463"
  condition:
    (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550 and pe.is_dll()) and
    pe.exports("15Mmm95ml1RbfjH1VUyelyFCf") and pe.exports("2d1sKEtPzvo1mHDN4FYgv")
}
```

sha256	description
6773af31bd7891852c3d8170085dd4bf2d68ea24a165e4b604d777bd083caeea	malwarebytes-windows-github-io-X.X.X.zip
4294d6e8f1a63b88c473fce71b665bbc713e3ee88d95f286e058f1a37d4162be	malwarebytes-windows-github-io-X.X.X.zip

sha256	description
5591156d120934f19f2bb92d9f9b1b32cb022134befef9b63c2191460be36899	malwarebytes-windows-github-io-X.X.X.zip
42d53bf0ed5880616aa995cad357d27e102fb66b2fca89b17f92709b38706706	malwarebytes-windows-github-io-X.X.X.zip
5aa6f4a57fb86759bbcc9fc6c61b5f74c0ca74604a22084f9e0310840aa73664	malwarebytes-windows-github-io-X.X.X.zip
84021dcfad522a75bf00a07e6b5cb4e17063bd715a877ed01ba5d1631cd3ad71	malwarebytes-windows-github-io-X.X.X.zip
ca8467ae9527ed908e9478c3f0891c52c0266577ca59e4c80a029c256c1d4fce	malwarebytes-windows-github-io-X.X.X.zip
9619331ef9ff6b2d40e77a67ec86fc81b050eeb96c4b5f735eb9472c54da6735	malwarebytes-windows-github-io-X.X.X.zip
a2842c7cfaadfba90b29e0b9873a592dd5dbea0ef78883d240baf3ee2d5670c5	malwarebytes-windows-github-io-X.X.X.zip
4705fd47bf0617b60baef8401c47d21afb3796666092ce40fbb7fe51782ae280	malwarebytes-windows-github-io-X.X.X.zip
580d37fc9d9cc95dc615d41fa2272f8e86c9b4da2988a336a8b3a3f90f4363c2	malwarebytes-windows-github-io-X.X.X.zip
d47fd17d1d82ea61d850ccc2af3bee54adce6975d762fb4dee8f4006692c5ef7	malwarebytes-windows-github-io-X.X.X.zip
606baa263e87d32a64a9b191fc7e96ca066708b2f003bde35391908d3311a463	CoreMessaging.dll DLL loaded by DLL SideLoading
fd855aa20467708d004d4aab5203dd5ecdf4db2b3cb2ed7e83c27368368f02bb	CoreMessaging.dll DLL loaded by DLL SideLoading

sha256	description
a0687834ce9cb8a40b2bb30b18322298aff74147771896787609afad9016f4ea	CoreMessaging.dll DLL loaded by DLL SideLoading
4235732440506e626fd4d0ffad85700a8fcf3e83ba5c5bc8e19ada508a6498e	CoreMessaging.dll DLL loaded by DLL SideLoading
cd1fe2762acf3fb0784b17e23e1751ca9e81a6c0518c6be4729e2bc369040ca5	CoreMessaging.dll DLL loaded by DLL SideLoading
f798c24a688d7858efd6efeaa8641822ad269feeb3a74962c2f7c523cf8563ff	CoreMessaging.dll DLL loaded by DLL SideLoading
0698a2c6401059a3979d931b84d2d4b011d38566f20558ee7950a8bf475a6959	CoreMessaging.dll DLL loaded by DLL SideLoading
1b3bee041f2ffcb9c216522afa67791d4c658f257705e0feccc7573489ec06f	CoreMessaging.dll DLL loaded by DLL SideLoading
231c05f4db4027c131259d1acf940e87e15261bb8cb443c7521294512154379b	CoreMessaging.dll DLL loaded by DLL SideLoading
ec2e30d8e5cacecdf26c713e3ee3a45ebc512059a64ba4062b20ca8bec2eb9e7	CoreMessaging.dll DLL loaded by DLL SideLoading
58bd2e6932270921028ab54e5ff4b0dbd1bf67424d4a5d83883c429cadeef662	CoreMessaging.dll DLL loaded by DLL SideLoading
57ed35e6d2f2d0c9bbc3f17ce2c94946cc857809f4ab5c53d7cb04a4e48c8b14	CoreMessaging.dll DLL loaded by DLL SideLoading
cfcf3d248100228905ad1e8c5849bf44757dd490a0b323a10938449946eabee	CoreMessaging.dll DLL loaded by DLL SideLoading
f02be238d14f8e248ad9516a896da7f49933adc7b36db7f52a7e12d1c2ddc6af	CoreMessaging.dll DLL loaded by DLL SideLoading

sha256	description
f60802c7bec15da6d84d03aad3457e76c5760e4556db7c2212f08e3301dc0d92	CoreMessaging.dll DLL loaded by DLL SideLoading
02dc9217f870790b96e1069acd381ae58c2335b15af32310f38198b5ee10b158	CoreMessaging.dll DLL loaded by DLL SideLoading
f9549e382faf0033b12298b4fd7cd10e86c680fe93f7af99291b75fd3d0c9842	CoreMessaging.dll DLL loaded by DLL SideLoading
92f4d95938789a69e0343b98240109934c0502f73d8b6c04e8ee856f606015c8	CoreMessaging.dll DLL loaded by DLL SideLoading
66fba00b3496d61ca43ec3eae02527eb5222892186c8223b9802060a932a5a7a	CoreMessaging.dll DLL loaded by DLL SideLoading
e5dd464a2c90a8c965db655906d0dc84a9ac84701a13267d3d0c89a3c97e1e9b	CoreMessaging.dll DLL loaded by DLL SideLoading
35211074b59417dd5a205618fed3402d4ac9ca419374ff2d7349e70a3a462a15	CoreMessaging.dll DLL loaded by DLL SideLoading
6863b4906e0bd4961369b8784b968b443f745869dbe19c6d97e2287837849385	CoreMessaging.dll DLL loaded by DLL SideLoading
a83c478f075a3623da5684c52993293d38ecaa17f4a1ddca10f95335865ef1e2	CoreMessaging.dll DLL loaded by DLL SideLoading
43e2936e4a97d9bc43b423841b137fde1dd5b2f291abf20d3ba57b8f198d9fab	CoreMessaging.dll DLL loaded by DLL SideLoading
f001ae3318ba29a3b663d72b5375d10da5207163c6b2746cfae9e46a37d975cf	CoreMessaging.dll DLL loaded by DLL SideLoading
c67403d3b6e7750222f20fa97daa3c05a9a8cce39db16455e196cd81d087b54d	CoreMessaging.dll DLL loaded by DLL SideLoading

sha256	description
5ee9d4636b01fd3a35bd8e3dce86a8c114d8b0aa6b68b1d26ace7ef0f85b438a	Payload dropped by one of the malicious DLLs
e84b0dad0b6be9b00a063ed82c8ddba06a2bd13f07d510d14e6fd73cd613fba	Payload dropped by one of the malicious DLLs