

Top 10 Malware Q3 2025

 cisecurity.org/insights/blog/top-10-malware-q3-2025

By: The Center for Internet Security® (CIS®) Cyber Threat Intelligence (CTI) team

Published November 14, 2025

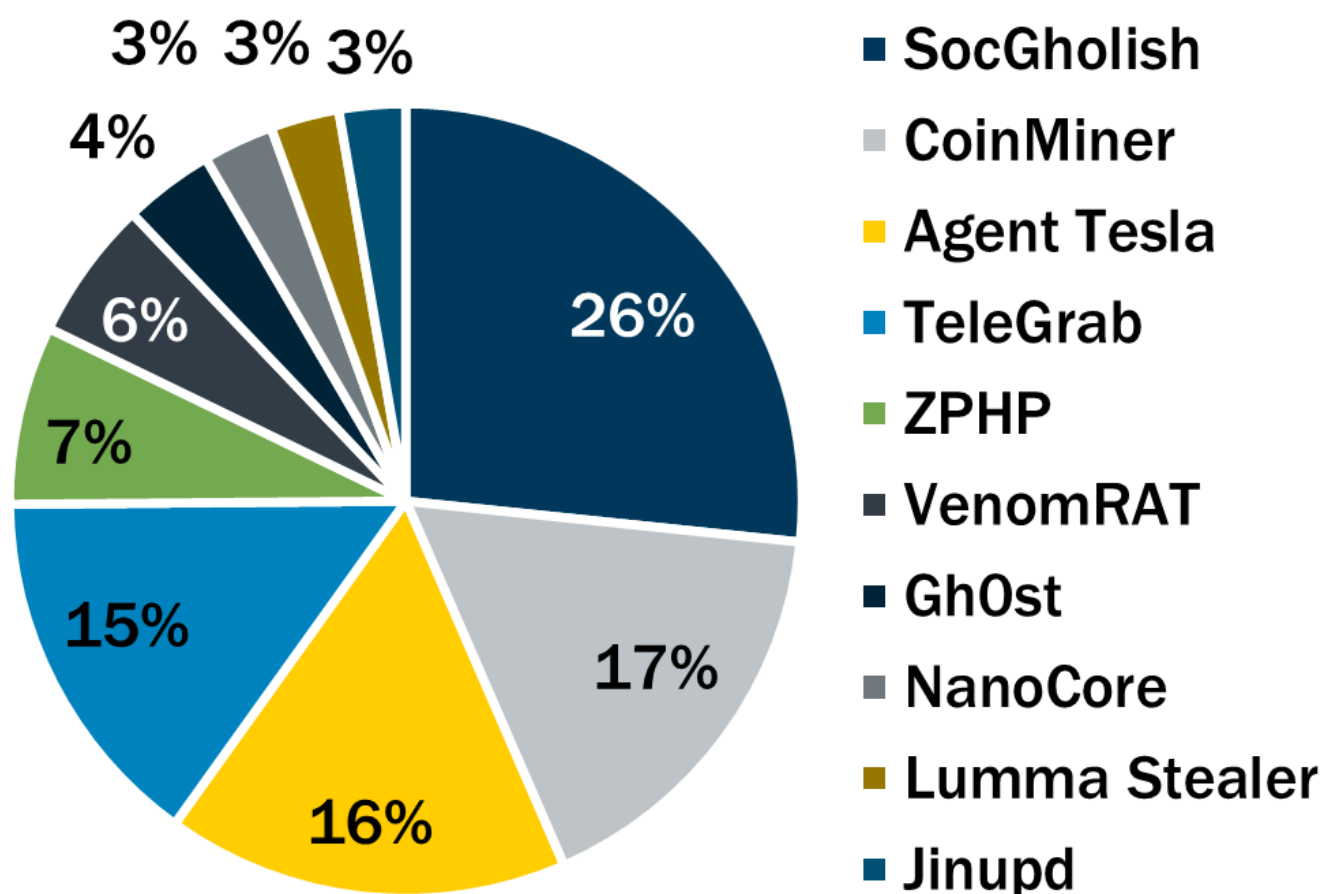


Total malware notifications from Multi-State Information Sharing and Analysis Center® (MS-ISAC®) monitoring services increased 38% from Q2 to Q3 2025. SocGholish continues to lead the Top 10 Malware as it has for the past two years, comprising 26% of detections. SocGholish is a downloader written in JavaScript that is distributed through malicious or compromised websites via fake browser updates. SocGholish infections often lead to further exploitation, such as NetSupport and AsyncRAT remote access tools. CoinMiner, a cryptocurrency miner, and Agent Tesla, a remote access trojan (RAT), followed SocGholish.

In Q3 2025, the MS-ISAC also observed the return of Gh0st, Lumma Stealer, and TeleGrab, while Jinupd made its first appearance. Jinupd is a downloader that uses obfuscated scripts to fetch and execute additional payloads. It is typically distributed via phishing campaigns and compromised websites.

Additionally, this is Lumma Stealer's first appearance after law enforcement took down its infrastructure. Lumma Stealer is an infostealer malware sold on the dark web that targets personally identifiable information (PII), such as credentials and banking information. It also has numerous defense evasion capabilities, including detecting whether the infected system is a virtual environment, detecting user activity on the system, and encrypting its executable to prevent reverse engineering.

Top 10 Malware

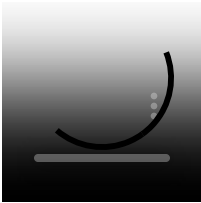


Malware Infection Vectors

The MS-ISAC tracks potential initial infection vectors for the Top 10 Malware each quarter based on open-source reporting, as depicted in the graph below. We currently track three initial infection vectors: *Dropped*, *Malspam*, and *Malvertisement*. Some malware use different vectors in different contexts, which are tracked as *Multiple*.

- **Dropped:** Malware delivered by other malware already on the system, an exploit kit, infected third-party software, or manually by a cyber threat actor. Gh0st used this technique at the time of publication.
- **Malspam:** Unsolicited emails, which either direct users to malicious websites or trick users into downloading or opening malware. Agent Tesla used this technique at the time of publication.
- **Malvertisement:** Malware introduced through malicious advertisements. SocGholish and ZPHP used this technique at the time of publication.
- **Multiple:** Malware that currently uses at least two vectors, such as *Dropped* and *Malspam*. CoinMiner, Jinupd, Lumma Stealer, NanoCore, TeleGrab, and VenomRAT used this technique at the time of publication.

The [CIS Community Defense Model \(CDM\)](#) v2.0 can help you defend against 77% of MITRE ATT&CK (sub-)techniques associated with malware regardless of the infection vector they use. Learn more in the video below.



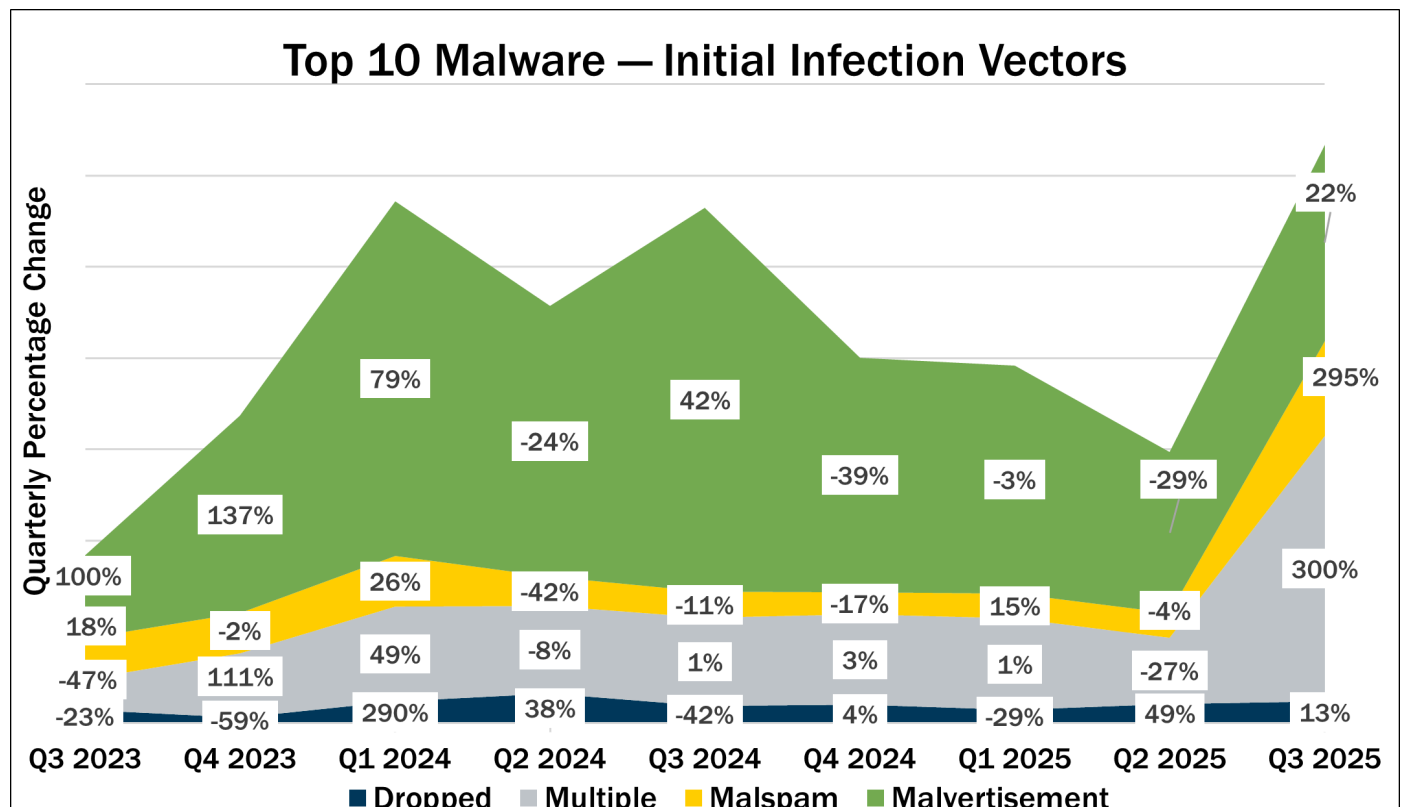


CIS Community Defense Model 2.0

with the CIS Community Defense Model 2.0. The updated CDM builds

0:55

In Q3, *Multiple* was the number one initial infection vector due to an increase in alerts related to CoinMiner, TeleGrab, and VenomRat.



Top 10 Malware and IOCs

Below are the Top 10 Malware listed in order of prevalence. The CIS CTI team provides associated Indicators of Compromise (IOCs) to aid defenders in detecting and preventing infections from these malware variants. Analysts sourced these IOCs from threat activity observed via [CIS Services®](#) and open-source research. Network administrators can use the IOCs for threat hunting but should vet any indicator for organizational impact before using for blocking purposes.

1. [SocGholish](#)
2. [CoinMiner](#)
3. [Agent Tesla](#)
4. [TeleGrab](#)
5. [ZPHP](#)
6. [VenomRAT](#)
7. [Gh0st](#)
8. [NanoCore](#)
9. [Lumma Stealer](#)
10. [Jinupd](#)

1. SocGholish

SocGholish is a downloader written in JavaScript and distributed through malicious or compromised websites via [fake browser updates](#). It uses multiple methods for traffic redirection and payload delivery, commonly uses Cobalt Strike, and steals information from the victim's system. Additionally, SocGholish can lead to further exploitation, such as loading the NetSupport and AsyncRAT remote access tools or even ransomware in some cases.

Domains

billing[.]roofnrack[.]us
cpanel[.]365axissolution[.]com
email[.]directoryindustry[.]com
feedback[.]fortunetaxs[.]com
folders[.]emeraldpinesolutions[.]com
keynotecapitals[.]com
photo[.]suziestuder[.]com
zone[.]ebuilderssource[.]com

2. CoinMiner

CoinMiner is a cryptocurrency miner family that typically uses [Windows Management Instrumentation](#) (WMI) to spread across a network. Additionally, it often uses the WMI Standard Event Consumer scripting to execute scripts for persistence. However, the malware's capabilities

vary, as there are multiple variants. CoinMiner spreads through malspam or is dropped by other malware.

SHA256 Hashes

063A65D2D36CAE110D6D6C400956A125B9C35176D628A9A8F4D8E2133EC4D887
0338C2CC1E83C851ADAA3EBB836A40B849DF0C48060BD3086193542CC6A7F26C
118AE6110A4B5708433EBD5809682E8C30F281F459A3B92B3E8ADA5023EB6640
3E59379F585EBF0BECB6B4E06D0FBBF806DE28A4BB256E837B4555F1B4245571
47ecaab5cd6b26fe18d9759a9392bce81ba379817c53a3a468fe9060a076f8ca
59F7C03A2021CB28A433AE0D018388B2A5B802686CA94699FA0BC9E1917AEAD0
9f1f11a708d393e0a4109ae189bc64f1f3e312653dcf317a2bd406f18ffcc507

3. Agent Tesla

Agent Tesla is a RAT that targets Windows operating systems and is available for purchase on criminal forums. It has various capabilities depending on the version purchased, including capturing keystrokes and screenshots, harvesting saved credentials from web browsers, copying clipboard data, exfiltrating victim files, and loading other malware onto the host.

Domains

mail[.]smc-energy[.]com
info-power[.]gl[.]at[.]ply[.]gg

SHA256 Hashes

ac5fc65ae9500c1107cdd72ae9c271ba9981d22c4d0c632d388b0d8a3acb68f4
c25a6673a24d169de1bb399d226c12cdc666e0fa534149fc9fa7896ee61d406f
dcfbe323a79ae16c098837ac947389f3fbd12587c322284cce541a4b482251f9
de4d1a23f283e7ad53706b8ba028d07d9e72ca3c2bf851245a360b6b93bd5588
d38fa4b7893995e5fc7e6d45024ffe0202b92769a4955cec29dc3bdb35d3c8ba
3df3f475fee2c5a74f567285fe848ceed1aff6e01b82710600af244b6529ef05
550f191396c9c2cbf09784f60faab836d4d1796c39d053d0a379afaca05f8ee8

4. TeleGrab

TeleGrab is an infostealer that targets the desktop and web versions of Telegram. It collects cache and key files, hijacks chat sessions, and captures contacts and chat history.

SHA256 Hashes

2be87bc7e1cee08a3abc7f8fefcfab697bd28404441f2b8ee8fafba356164902

5. ZPHP

ZPHP is a downloader written in JavaScript and distributed through malicious or compromised websites via fake browser updates. ZPHP is also known to drop the NetSupport remote access tool and Lumma Stealer malware.

Domains

ahmm[.]ca
anoteryo[.]top
ashesplayer[.]top
as5yo[.]top
buyedmeds[.]top
morniksell[.]com
retiregenz[.]com
trendings[.]top
warpdrive[.]top

6. VenomRAT

VenomRAT is an open-source RAT often dropped by other malware or spread via malspam. Since VenomRAT is open-source, there are multiple versions with varying capabilities. Most versions include capabilities associated with keylogging, screen capture, password theft, data exfiltration, and downloading and executing additional files.

SHA256 Hashes

A5D1E69076FD9F52D8A804202A21852FE2B76FB4534F48455DEF652E84CCEAAB
D6CC784BE51F8B784BD9AFD2485F3766D89CA5AE004AE9F2C4DAE7E958DBE722
EAD78CEBBB4CF8CF410E1D8674D89D89F35A7A9936C3FF61C16C534062B3E9B8
Ff939d8a377b37b1688edc3adb70925ffcf313f83db72278d14955b323b138b7
F308A8CC0790F07F343D82AE0D9DA95248FB1BA4D4E01F30D0A8A43B9E6D3CA0
0109B0D2C690FED142DAD85CED4F1E277464ACC49DF4BEF3C5F5ED58F3925AED
156943B1DF6141AB7C2910B7CD5B8BCB2FFE839AA6C99D663ABF12588F11615B
522D4528ED25FE6CE9422B45AC4D162E7567330C0FCB274DE247C4CB07ED794B
57CDECA5D774353B37AFFDB9F3BF50BFF0E16140A9CED996F5AC3925DE362074
706AAFE4ED32AA4B13E65629C2496D9B1E2E9D1753AA0F92833586ACD1AA591E
89C73024FC9D700209ECADDF3628B59224D27750E188DCE0015313DA77346925

7. Gh0st

Gh0st is a RAT used to control infected endpoints. Gh0st is dropped by other malware to create a backdoor into a device that allows an attacker to fully control the infected device.

Domains

gmhyc[.]vip5944[.]com
kinh[.]xmcxmr[.]com
whseel.f3322[.]org
yinhunzhiren[.]e2[.]luyouxia[.]net

SHA256 Hashes

eb012c3bc2ff9dc0710c4de9dd0da5ae5a962e4521b7ae33035bf69dd897a255
ef686d3726ef3f2ec5dee9390a6430cc74aae5c0b24a30441154aa1415ab9887
0d1b1e53089001d5ba3e3e81083bd29a38a989a9791dd1432eb5331ee100336e
085e647900df354e4ef17451b8a644169a473f5e175383f6cf7666a5ff66a191
3a4cef94dd1a37c78f34e9d5912930ad4e8a858f7672435eea186c5148b05dd6
9baec10376d3661ed20d953b718a975433cc1299a6db8fd3b690b4e3bc01058d
92d1eada419273a87ee66170826f94aab7af63a521bdfc20273620a5bb9e012b
967833fc5afa92793c2a1b1e190726a0dbc15c2d103280495b1f94c5e2ba39ae

8. NanoCore

NanoCore is a RAT sold on criminal forums and usually spread via malspam with an attachment, such as a malicious Excel (XLS) spreadsheet. NanoCore has a wide range of capabilities including keylogging, screen capture, password theft, data exfiltration, downloading and executing additional files, and adding registry keys for persistence.

SHA256 Hashes

ac7c3c0c3906c4d93e34b91fa34941277f044ac26d037c113c9756a4f18619dd
ae9384f6fc3fea2276f6897e910a5d5b7a3ad995420363788815e0754ff9469f
b41b8e7fa701068d5adb73d80ab7582f2affa1bad904fa01f413c0775abb162
b5d0552aa20ae4bec3f41829abfb9e3b797512bcc9cdb9e6454b63f6a6727cea
cb221204dda7694c9ecd227681ada701093386b6bb290e128acd0db44aab56e3
edcddea73fb45a758b91322ed6b64f182d353d5760c71e7afcce7340f522b40b
4a0e6efe7da756a13dd1f1f7fe3a9a24f62e03ac4181e56a9b1e9e46045ff036
480a1166729945af333cf8a6f5d51a4ed13ac5e4af1487ecea6e87f7aefbf656
677ce0d368b44c16550269a5f337c5d8c67cf025664c614ab1add706627b0594
6945a4190b825daeb27ad63f21aade3053099ddba38dea4e25a5d1cc7471f74d

9. Lumma Stealer

[Lumma Stealer](#), also known as Lumma, is an infostealer malware that operates as a Malware as a Service. It targets PII, such as credentials, banking information, cookies, browser autofill data, and cryptocurrency wallet information. Additionally, it has numerous defense evasion capabilities, including virtual environment detection, user activity monitoring, and executable encryption to hinder reverse engineering.

Domains

lzh[.]fr
digitbasket[.]com
duholdown[.]fun
kowersize[.]fun
marvelvod[.]com
mouseoiet[.]fun
plengreg[.]fun
zamesblack[.]fun
zamesblack[.]fun

SHA256 Hashes

FA8BE0CE6F177965A5CD2DB80E57C49FB31083BD4DDCB052DEF24CFBF48D65B5
388F910E662F69C7AB6FCF5E938BA813CF92C7794E5C3A6AD29C2D9276921ED3
64F6C0C0FD736C4A82F545AAD7A1C49D4CEA77B14F4B526EF9DA56A606EEB3D

10. Jinupd

Jinupd, also known as JackPOS, is a point of sales (POS) infostealer that steals credit card information by scraping memory from payment-processing applications. It often masquerades as a Java updater, establishes persistence through registry modifications, exfiltrates stolen data, and downloads additional payloads. Jinupd typically spreads via drive-by downloads, compromised websites, or as a secondary payload from other malware.

SHA256 Hashes

b9f8c7b020be54cc25d73d0fdf75378a87fa5729a9464366f33c274af795c050
7da2b0790888196277f45b32162c355c0b68c8a83479c5c3bbb3dd6deed80c8a

Leverage the Power of Tailored Threat Intelligence

This threat intelligence briefing illustrates how the CIS CTI team supports paid members of the MS-ISAC. Available to U.S. State, Local, Tribal, and Territorial (SLTT) government entities, MS-ISAC membership enables organizations to share information and collaborate on defending against cyber threats. The CIS CTI team supports members by maintaining the only [STIX/TAXII threat intelligence feed](#) tailored to U.S. SLTTs. It also routinely releases threat intelligence briefings along with detailed reports, such as the Quarterly Threat Report and Operational Cyber Analytic Report, to provide decision-makers with actionable threat intelligence they can use to take a proactive approach to their organization's cyber defense.

Ready to augment your cybersecurity posture using the expertise of the CIS CTI team? As of June 23, 2025, the MS-ISAC has introduced a fee-based membership. Any potential reference to no-cost MS-ISAC services no longer applies.