Certified OysterLoader: Tracking Rhysida ransomware gang activity via code-signing certificates

By Aaron Walton

Published: 2025-10-31 · Archived: 2026-04-05 13:59:39 UTC

TL;DR

- There's an ongoing malicious ad campaign delivering a malware called OysterLoader, previously known as Broomstick and CleanUpLoader
- The malware is an initial access tool (IAT) that gets onto devices to run a backdoor to gain access to the device and network
- The malware is being leveraged by the Rhysdia ransomware gang

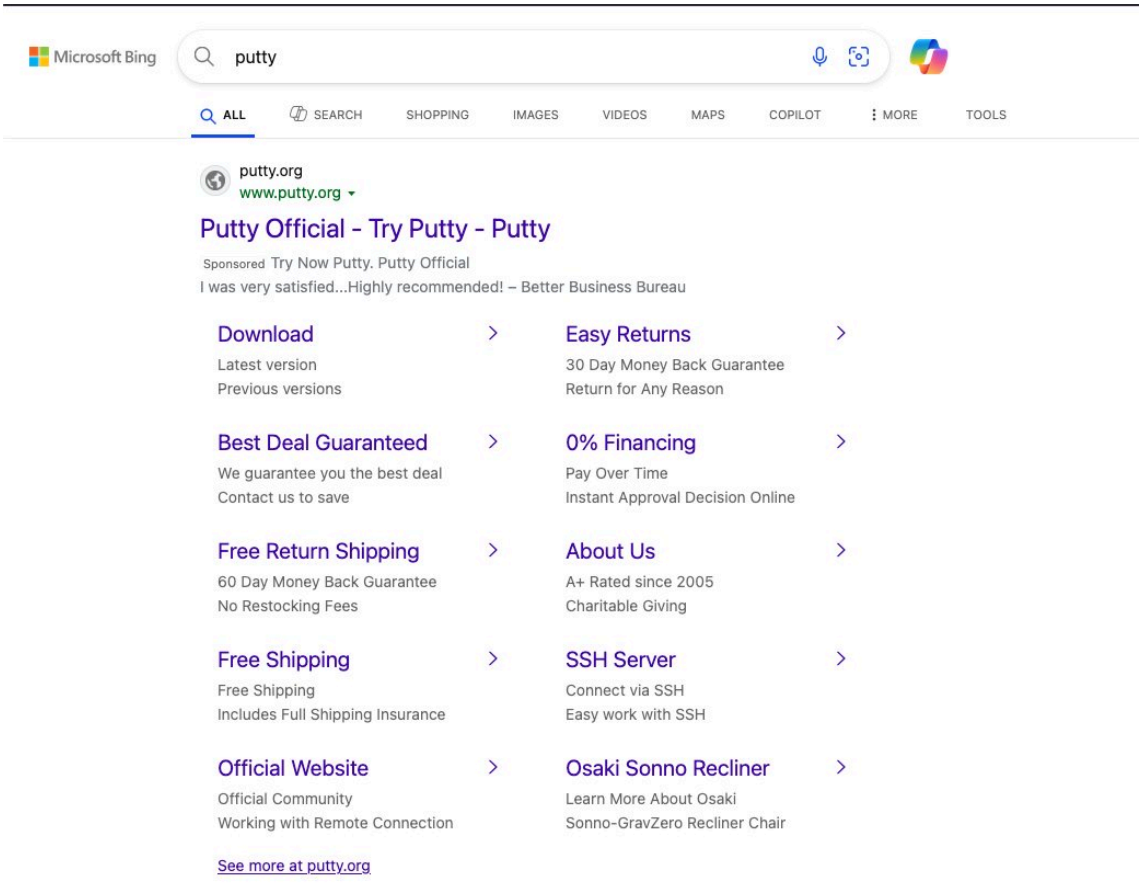
The Rhysida gang has been targeting enterprises for years now. First working as Vice Society in 2021, and then rebranding to Rhysida in 2023 [1, 2, 3]. While they may have rebranded to divert law enforcement, defenders don't forget just because of changed names or time passed.

We're tracking Rhysida's current campaign leveraging malicious advertisements to deliver OysterLoader malware (also known as Broomstick and CleanUpLoader). The first campaign ran from May to September 2024, and the current campaign has been running since June of this year.

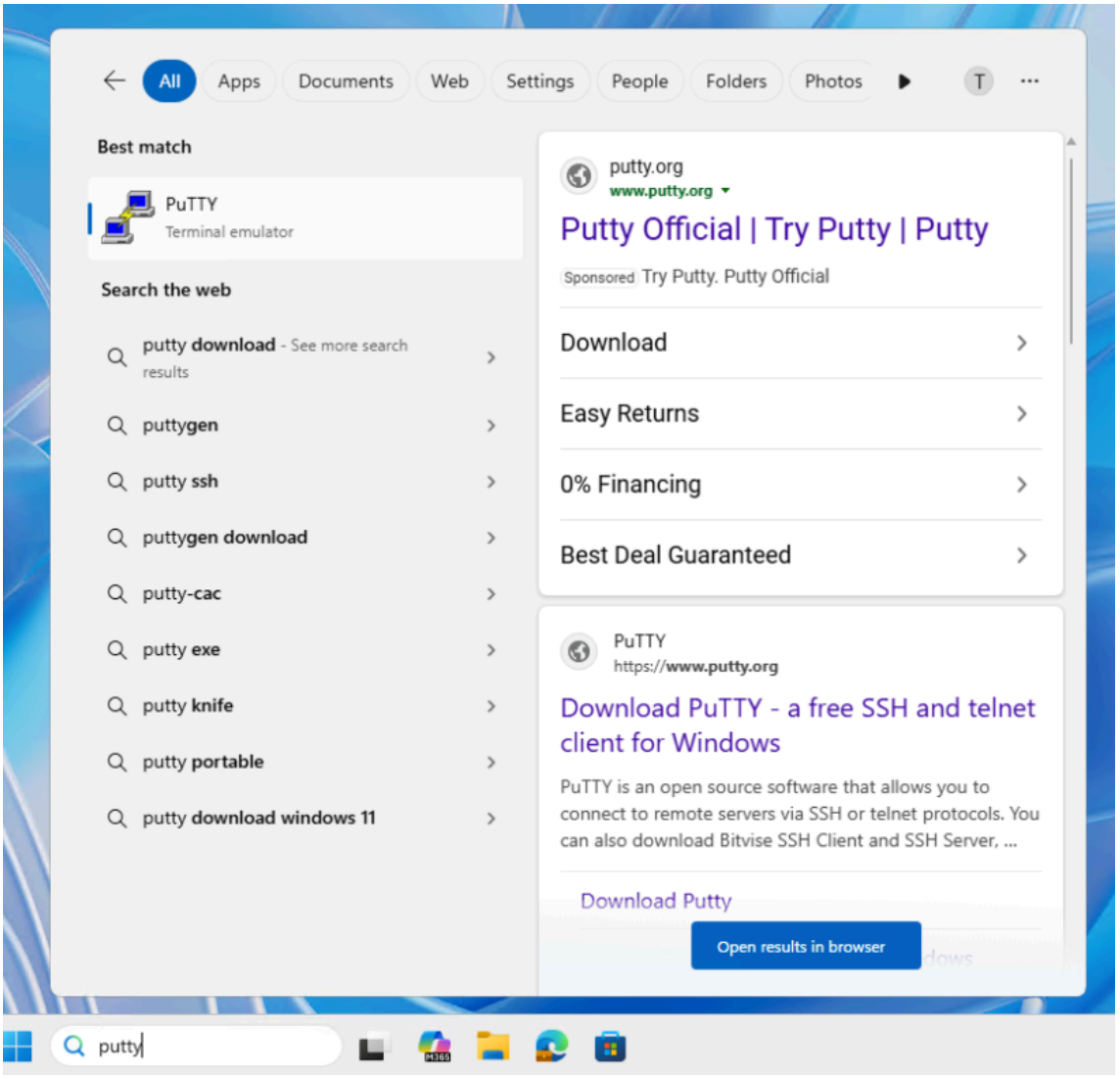
OysterLoader is, fundamentally, an initial access tool (IAT). Its sole function is to establish a foothold on a device so a second stage persistent backdoor can be dropped on the system and establish long-term access. Getting the first stage into a network is a common first step step in a larger network intrusion.

The delivery: malvertizing

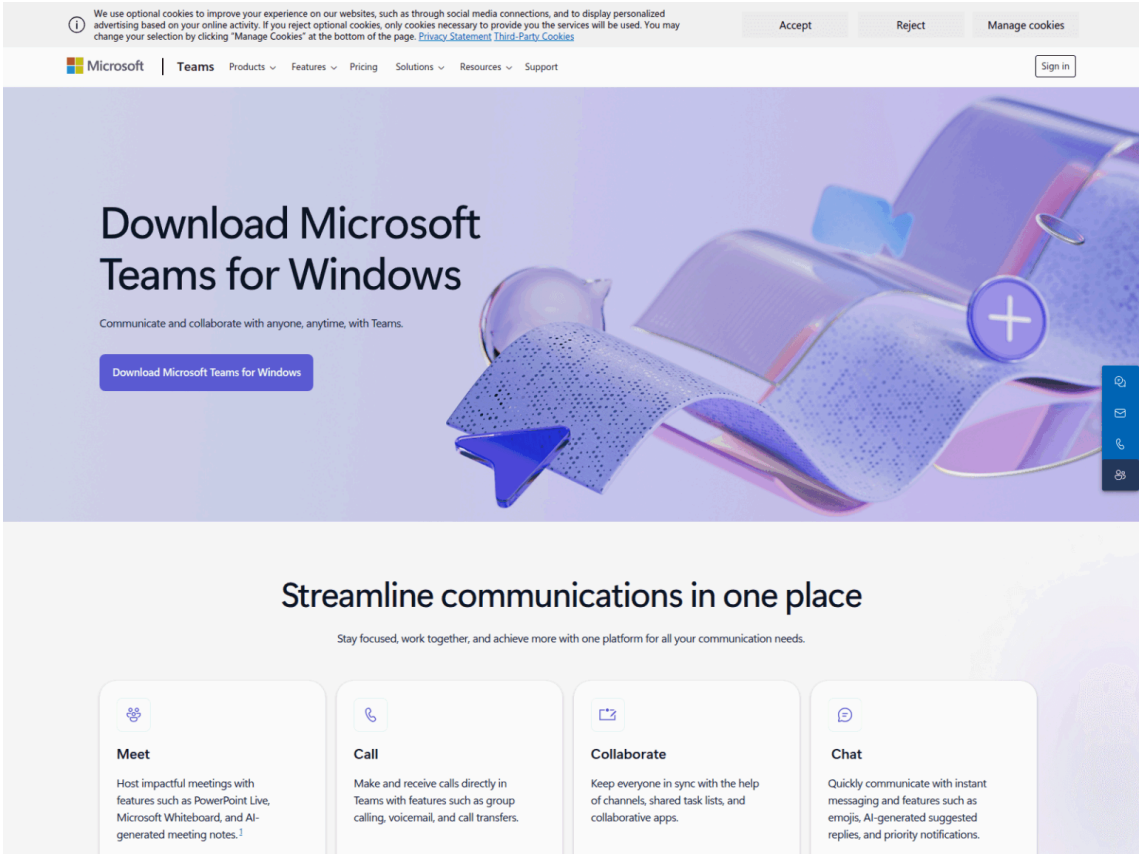
The current infection chain is built on a highly successful malvertising model. Threat actors buy Bing search engine advertisements to direct users to convincing-looking, but malicious landing pages. These search engine ads put links to the download right in front of potential victims. The most recent campaigns push ads for Microsoft Teams and impersonate the download pages. However, they've also cycled through other popular software such as PuTTy and Zoom.



Example malicious PuTTy Ad shared by [Tanner via X on July 18, 2025.]



Due to Bing ads showing up in the Windows 11 start menu, malicious ads can be served here too. Note that one result is sponsored and misspells PuTTy as “Putty”.



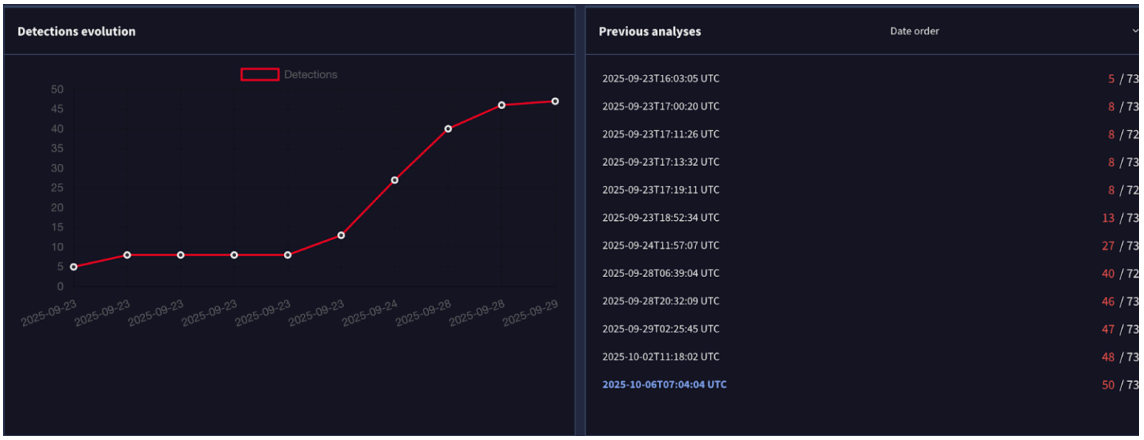
An example of teams-app[.]bet as [captured by URLScan.io.]

Using ads for Teams and other products is an identical tactic to what was [seen by the same actors in 2024]. This technique is a clear indicator of the gang's commitment to proven tactics, mimicking a highly effective campaign they executed previously.

To insure the first stage's success, the actors do two things to achieve low detection rates:

1. They pack the malware
2. They use code-signing certificates

[Packing] is a technique used to compress, encrypt, or obfuscate the function of the software. In the case of Rhysida, their packing tool effectively hides the capabilities of the malware and results in a low static detection rate when the malware is first seen.



> This graph of the detection rate by VirusTotal illustrates the general trend. Due to their obfuscation, it is common for 5 or less detection engines to flag the malware and it can take several days before more AV engines flag the malware. (This example is 32b0f69e2d046cb835060751fcda28b633cbbd964e6e54dbbc1482fff4d51b57.)

Code-signing certificates are standard for legitimate software. The Windows operating system uses code-signing as a measure of confidence that a file came from a valid source. The trust comes from the software publisher listed in the certificate going through a vetting process to get the code-signing certificate, but this system isn't without its flaws. The Rhysida ransomware gang uses certificates to give their own malicious files a higher level of trust.

Signing as signal

Due to their use of code-signing certificates, we gain an advantage in tracking and identifying new campaigns. The certificates they use regularly get revoked by the certificate's issuer, so new instances of the malware with a valid certificate indicate a new run of the campaign. Expel actively reports these certificates to be revoked as we encounter them, and the revocations help operating systems, antivirus, and browsers better identify and mitigate the malware.

On any given day the bad actors may use multiple certificates, but seeing their files with a new fresh certificate also helps us know they're still active. These new certificates further indicate steady investment into their campaign.

Campaign period	Code-signing certificates tracked	Context
2024 activity (May – September)	7 certificates	The gang's first Microsoft Teams malvertising campaign.
2025 activity (June – current)	40+ certificates	The second campaign with a dramatic increase of files and certificates, indicating higher operational tempo and resource investment.

CertCentral.org currently documents a total of **47 unique certificates** used to sign OysterLoader across the 2024 and 2025 timeframes, underscoring the larger scale of this campaign.

Not all Rhysida's eggs are in one basket

Though the main focus of this blog is OysterLoader, Rhysida's activity isn't limited to this one malware. During the current campaign, they're also using the Latrodectus malware to get initial access to networks. We identified this when analyzing files for the purpose of building detection rules: we observed that our YARA rules developed to detect their packer also detected Latrodectus malware. This was further confirmed when we observed an instance where the same code-signing certificate was used to sign both malware.

Signer	Malware & context	Date seen	Hash

Art en Code B.V.	OysterLoader disguised as MS Teams	2025-09-12	4e4a3751581252e210f6f45881d778d1f482146f92dc790504bfbcd2bdfa0129
Art en Code B.V.	Latrodectus delivered through ClickFix lure	2025-09-15	88e9c1f5026834ebcdaed98f56d52b5f23547ac2c03aa43c5e50e7d8e1b82b3a

In the majority of situations, Rhysida has smartly avoided using the same certificate across campaigns. However, this activity highlights their involvement with both campaigns.

In addition to this one certificate, the Rhysida ransomware gang are also one of the few cybercriminals leveraging Trusted Signing from Microsoft—Microsoft's own service for issuing code-signing certificates—*and* they use these Trusted Signing certificates for both OysterLoader and the second stage dropped from Latrodectus.

Microsoft Trusted Signing

Microsoft Trusted Signing certificates were created with certain features to limit misuse, however, the Rhysida ransomware gang appear to have found ways around those restrictions. The certificates are issued with a 72-hour validity period. After that, the certificates expire and need to be renewed. This short period makes the standard process of purchasing and reselling certificates infeasible. However, the Rhysida ransomware gang—or a supplier of theirs—has identified a means to abuse Microsoft's Trusted Signing system, allowing them to sign files at scale. Microsoft themselves report having revoked more than 200 certificates associated with the Rhysida ransomware gang and OysterLoader. The majority of these were revoked before they were actively abused to sign malware and deployed, though there is no sign of Rhysida ransomware stopping their use of Microsoft's service.

Keeping track

This campaign is likely to continue and may change as a result of this blog and we plan to continue to monitor it and track it. Indicators associated with these campaigns are on GitHub here: https://github.com/expel-io/expel-intel/blob/main/2025/10/Rhysida_malware_indicators-01.csv

Signer	Malware	Hash
Alternative Power Systems Solutions LLC	OysterLoader	e25db8020f7fcadaec5dd54dd7364d8eaa9efd8755fb91a357f3d29bf2d9fbad
Assurance Property	Latrodectus, stage 2	9ce7fa41d8088472dcda120012d025f16c638c57511ac4b337f16893c4580105

Management L.L.C		
BRANCH INVESTMENTS HAWAII LLC	OysterLoader, stage 2	**f21483536cbd1fa4f5cb1e996adbe6a82522ca90e14975f6172794995ed9e9a2**
CARLMICH MANAGEMENT, LLC	OysterLoader, stage 2	c41f42e11e699f45a77ac4e8aef455a07b052180863748f96589d45525e250f6
Chidiac Entreprises Commerciales Inc.	OysterLoader	b52dddf4022ee45243ad01705d5a8d5070cd62aa89174f1ab83f5b58f66d577a
DELANEY HOME INSPECTIONS LLC	OysterLoader	5c797080fa605cab2cd581645f00843f9c91c9c2d0ad4598ccb7886f990c916b
ECHO PADDLES INC.	OysterLoader	fdfae96c3e943c16f7946d820598b2d205395fe7483b5b82e4a9903dc96c1eb1
GALVIN & ASSOCIATES LLC	OysterLoader	dae9df9ce0f5286cfe871fda680e4de440c8444a44ceb434c28d5ccf786f5e8d
HCCO Retail Ltd.	OysterLoader, stage 2	d19a497670314a3bbff5bc958db3eacfe591c04f866f779cbc06e0f0f48b991f
IceCube Software, Inc.	OysterLoader	0bcdbd79c13fc50955804d0f2666c878542157fc3d4987d18d13c72e9697209e
IMMEUBLES DAVECLO INC.	Latrodectus, stage 2	c92081585c525afba5abcb773c7ca9532fba6ce5e7aca340a226e2b05ff3b0d2
KUTTANADAN CREATIONS INC.	OysterLoader	32b0f69e2d046cb835060751fcda28b633cbbd964e6e54dbbc1482fff4d51b57
Micros in Action, Incorporated	OysterLoader	cd671cfa42714a6d517476add60690081a16a5c6abaacce25fcb9c5ddf41b7d3
Mobiquity Technologies, Inc.	OysterLoader, stage 2	b4a4d565a4d69e1e54557044809fc281591cdc5781126f978df8094467ba59fd

NEW VISION MARKETING LLC	OysterLoader	e9f05410293f97f20d528f1a4deddc5e95049ff1b0ec9de4bf3fd7f5b8687569
Nitta-Lai Investment Corp.	OysterLoader	a3b858014d60eaa5b356b7e707a263d98b111b53835ae326cd4e0fb19e7f5b35
NRM NETWORK RISK MANAGEMENT INC.	OysterLoader	ac5065a351313cc522ab6004b98578a2704d2f636fc2ca78764ab239f4f594a3
QUANT QUEST ACADEMY INC.	Latrodectus, stage 2	2528df60e55f210a6396dd7740d76afe30d5e9e8684a5b8a02a63bdcb5041bfc
TOLEDO SOFTWARE LLC	OysterLoader	51c85e40fb4f5bc3fd872261ffef181485791e2ffbe84ab96227461040a1ca4d

---