

Osiris: New Ransomware, Experienced Attackers?

✓ security.com/threat-intelligence/new-ransomware-osiris

 Osiris: New Ransomware, Experienced Attackers?

A new ransomware family called Osiris was used in an attack targeting a major food service franchisee operator in Southeast Asia in November 2025.

While this Osiris ransomware shares a name with a ransomware family from 2016, which was a variant of the Locky ransomware, there is no indication that there is any link between these two families. Investigation by the Symantec and Carbon Black Threat Hunter Team found that this threat is unique and appears to be a completely new ransomware family.

Nothing is known yet about who developed Osiris and if it is run as a ransomware-as-a-service (RaaS) but there are some indications that the attackers who used it were previously associated with Inc ransomware. A wide range of living off the land and dual-use tools were used in this attack, as was a malicious Poortry driver, which was likely used as part of a bring-your-own-vulnerable-driver (BYOVD) attack to disable security software. The exfiltration of data by the attackers to Wasabi buckets, and the use of a version of Mimikatz that was previously used, with the same filename (kaz.exe), by attackers deploying the Inc ransomware, point to potential links between this attack and some attacks involving Inc.

Ransomware functionality

Osiris has multiple typical ransomware functions. It can stop services, specify which folders and extensions to encrypt, terminate processes and services, encrypt files, and drop a ransom note.

It can take the following command-line options:

- **log:** Specifies a path to a log file
- **file:** File path for encryption
- **path:** Directory path for encryption
- **hyperv:** Disables hyper virtual machine (VM) and deletes configurations files.
- **hyperv-skip:** Skips specific VMs
- **mode:** This sets whether a file is encrypted partially or fully (values can be "head" / "full")

It skips the following extensions: *.exe, .dll, .msi, .mp4, .mp3, .mov, .m4v, .iso, .avi, .apk, .msu, .tib, .ai, .inf, .sys, .lnk, .url, .cat*

And the following folders: *"windows"; "perflogs"; "programdata"; "documents and settings"; "system volume information"; "\$recycle.bin"; "\$winreagent", and "all users".*

Other folders - program files, program files (x86), and programdata - are not fully skipped by the ransomware. After completing encryption, Osiris appends the .Osiris extension to affected files (e.g. curl.txt becomes curl.txt.Osiris), and deletes snapshots using VSS.

It also terminates the following processes: *sql; oracle; ocssd; dbsnmp; synctime; agntsvc; isqlplussvc; xfssvccon; mydesktopservice; ocautoupds; encsvc; firefox; tbirdconfig; mydesktopqos; ocomm; dbeng50; sqbcoreservice; excel; infopath; msaccess; mspub; far; onenote; outlook; powerpnt; steam; thebat; thunderbird; visio; winword; wordpad; notepad; wuaclt; onedrive, and sqlmangr.*

And stops the following services: *vss; sqlsvc; memtas; mepocs; msexchange; Veeam; backup; GxVss; GxBlr; GxCVD, and GxCIMgr.*

The ransomware uses a hybrid encryption scheme: ECC +AES-128-CTR, and uses a unique AES key for encryption for each file. It also uses completionIOPort to manage asynchronous I/O requests for encryption.

The ransomware also drops a ransom note titled Osiris-MESSAGE.txt, which details the data they claim to have stolen and contains a link to a chat where the victim can negotiate with the attackers.

Attack chain

The first suspicious activity occurred on the target's network a few days before the ransomware was deployed, when Rclone was used to exfiltrate data. This data was exfiltrated to a Wasabi bucket. Wasabi is a legitimate cloud storage service. The tactic of exfiltrating to Wasabi was previously used in October 2025 by Inc ransomware attackers. The overlaps with previous Inc ransomware activity could mean their tactics were being emulated in this attack, or that a former Inc affiliate is now working with or responsible for Osiris. The attackers also used a version of Mimikatz that was previously used, with the same filename (kaz.exe), by attackers deploying Inc, indicating another crossover in activity.

The attackers also deployed other dual-use tools like Netscan, Netexec, and MeshAgent. They also used a custom version of the Rustdesk remote monitoring and management (RMM) tool, which was modified to masquerade its functionality and to include the file description of "WinZip Remote Desktop" and the WinZip icon in an effort to hide its true use.

A malicious driver called Abyssworker or Poortry, which masqueraded as a Malwarebytes anti-exploit driver, was also deployed on the target's network, and was likely used as part of a bring-your-own-vulnerable-driver (BYOVD) attack to disable security software. Poortry [was first reported on by Google's Mandiant investigation team in 2022](#). In 2024 and 2025 it was used in attacks attributed to the Medusa ransomware gang. In a Medusa ransomware attack investigated by the Threat Hunter Team in December 2024, a loader called Stonestop was used to load and install Poortry on victim machines and to instruct it as to what actions to perform. Poortry is frequently employed alongside Stonestop.

BYOVD is by far the most frequently used technique for defense impairment by ransomware attackers now. Generally, attackers will deploy a signed vulnerable driver to the target network, which they then exploit to elevate privileges and disable security software. Since the drivers operate with kernel-mode access, they can be used to terminate processes, making them an effective tool for disrupting security measures. Poortry is somewhat unusual because, unlike many drivers, it appears it may have been developed by attackers who then succeeded in getting it signed. In most cases, attackers use a legitimate vulnerable driver to carry out BYOVD attacks, rather than using a custom driver they have developed themselves. KillAV, which is a tool used to deploy vulnerable drivers for terminating security processes, was also deployed on the target's network. RDP was also enabled on the network, likely to provide the attackers with remote access.

New ransomware, old tricksters?

The impact this new Osiris ransomware will have on the ransomware landscape in general remains to be seen. However, it is an effective encryption payload that appears to be wielded by experienced attackers. The use of the Wasabi cloud service and using a version of Mimikatz with the same name as one previously used by Inc ransomware attackers point to potential links with

that group or one of its affiliates. Meanwhile, the use of Poortry, previously favored by attackers deploying Medusa, may indicate a link, though Poortry is not believed to be exclusively used by one actor.

With the constant shifting sands of the ransomware landscape, the emergence of a new ransomware family is always something to keep an eye on.

Further reading

To find out more, read our whitepaper: [Ransomware 2026: New Actors and Threats Emerge as the Threat Landscape Evolves](#)

Indicators of Compromise (IoCs)

File indicators

fff586c95b510e6c8c0e032524026ef22297869a86d14075cd601ca8e20d4a16 - KillAV - 33.exe, payload.exe

c74509fcae41fc9f63667dce960d40907f81fae09957bb558d4c3e6a786dde7d - KillAV - payload.dll

fc39cca5d71b1a9ed3c71cca6f1b86cfe03466624ad78cdb57580dba90847851 - Mimikatz - kaz.exe

d78f7d9b0e4e1f9c6b061fb0993c2f84e22c3e6f32d9db75013bcfbba7b64bc3 - MeshAgent - meshagent64-philip.exe, meshagent.exe, mesh.exe

824e16f0664aaf427286283d0e56fdc0e6fa8698330fa13998df8999f2a6bb61 - KillAV - payload.dll

231e6bee1ee77d70854c1e3600342d8a69c18442f601cd201e033fa13cb8d5a5 - windows.exe

44748c22baec61a0a3bd68b5739736fa15c479a3b28c1a0f9324823fc4e3fe34 - Driver - multia.sys

Ce719c223484157c7f6e52c71aada496d0dad77e40b5fc739ca3c51e9d26277 - chromesetup.exe

8c378f6200eec750ed66bde1e54c29b7bd172e503a5874ca2eead4705dd7b515 - Netexec - nxc.exe

79bd876918bac1af641be10cfa3bb96b42c30d18ffba842e0eff8301e7659724 - Rclone - rclone.exe

C189595c36996bdb7dce6ec28cf6906a00cbb5c5fe182e038bf476d74bed349e - Rclone - rclone.exe

5c2f663c8369af70f727cccf6e19248c50d7c157fe9e4db220fbe2b73f75c713 - Osiris ransomware - 1.exe, windows.exe

44e007741f7650d1bd04cca3cd6dfd4f32328c401f95fb2d6d1fafce624cc99e - Rustdesk - winzip.exe

D524ca33a4f20f70cb55985289b047defc46660b6f07f1f286fa579aa70cf57a - MeshAgent - meshagent64-philip.exe

5bd82a1b2db1bdc8ff74cacb53823edd8529dd9311a4248a86537a5b792939f8 - Netscan - netscan.exe

534bd6b99ed0e40ccbefad1656f03cc56dd9cc3f6d990cd7cb87af4cceebe144 - buildx86.exe

39a0565f0c0adc4dc5b45c67134b3b488ddb9d67b417d32e9588235868316fac - chromesetup.exe

Network indicator(s):

ausare[.]net

wesir[.]net

About the Author

 Threat Hunter Team

Threat Hunter Team

Symantec and Carbon Black

The Threat Hunter Team is a group of security experts within Broadcom whose mission is to investigate targeted attacks, drive enhanced protection in Symantec and Carbon Black products, and offer analysis that helps customers respond to attacks.

You might also enjoy

 [Ransomware: Tactical Evolution Fuels Extortion Epidemic](#)

[Ransomware: Tactical Evolution Fuels Extortion Epidemic](#)

- [14 Jan 2026](#)
- [4 Min Read](#)