

Researchers Warn of 4 Emerging Ransomware Groups That Can Cause Havoc

📅 August 24, 2021 👤 Ravie Lakshmanan



(<https://thehackernews.com/images/->

[tgm9D2gCAQc/YSTRfpc9g3l/AAAAAAAAADnk/kyacqu6ahyQEuuD8qH-mRh4v5fnzmoM-QCLcBGAsYHQ/s0/russian-ransomware-hackers.jpg](https://thehackernews.com/images/-tgm9D2gCAQc/YSTRfpc9g3l/AAAAAAAAADnk/kyacqu6ahyQEuuD8qH-mRh4v5fnzmoM-QCLcBGAsYHQ/s0/russian-ransomware-hackers.jpg))

Cybersecurity researchers on Tuesday took the wraps off four up-and-coming ransomware groups that could pose a serious threat to enterprises and critical infrastructure, as the ripple effect of a recent spurt in ransomware incidents show that attackers are growing more sophisticated and more profitable in extracting payouts from victims.

"While the ransomware crisis appears poised to get worse before it gets better, the cast of cybercrime groups that cause the most damage is constantly changing," Palo Alto Networks' Unit 42 threat intelligence team [said](https://unit42.paloaltonetworks.com/emerging-ransomware-groups/) (<https://unit42.paloaltonetworks.com/emerging-ransomware-groups/>) in a report shared with The Hacker News.

"Groups sometimes go quiet when they've achieved so much notoriety that they become a priority for law enforcement. Others reboot their operations to make them more lucrative by revising their tactics, techniques and procedures, updating their software and launching marketing campaigns to recruit new affiliates."



(<https://go.thn.li/1-free-300-9>)

The development comes as ransomware attacks are getting bigger and more frequent, growing in size and severity, while also evolving beyond financial extortion to an urgent national security and safety concern that has threatened schools, hospitals, businesses, and governments across the world, prompting international authorities to [formulate a series of actions](#)

(<https://securityandtechnology.org/ransomwaretaskforce/>) against both operators of ransomware and the broader ecosystem of IT and money laundering infrastructure that's abused to siphon funds.



AvosLocker - Ransomware [ACCEPTING AFFILIATES]

by /u/avos · 1 week ago in /d/malware

AvosLocker Ransomware is looking for new affiliates.

Features:

- Encrypt all drives & network shares (hidden or not)
- Multi-threaded encryption process
- Fail-proof
- Overwrite files instead of creating copies:

Files are encrypted & overwritten in blocks, causing no memory issues while proving to be way more efficient, as the original files do not need to be overwritten before deletion.

- Delete shadow copies/backups

- Proper memory cleaning of cryptography keys:

Memory is cleansed of any keys that may be used in decryption right after each file is encrypted. No trace of decryption keys will be found in memory.

- Written in C++
- Low detection rates
- Compatible with all crypters/evading methods
- Other applications interfering with encryption are terminated instantly
- Large file support

After you infect the target, we take care of negotiation, hosting of leaks, publishing it on our blog and so on. Payments are strictly done through Monero.

Our services (affiliate panel, payment, blog) are strictly hosted in Tor.

You may apply for an invite through my

XMPP: avos@thesecure.biz

Tox: 9A751AC90A5F020521EE40D58208C272BD18D2E0C934AB6DA9B918627578095CD9847E24CE59

1 comments Hide

(https://thehackernews.com/images/-Usj9v4__Plo/YSTSp6u8col/AAAAAAAAADn4/vrfPBsq3-OMQFQVLRy0QdVFkWTWuCEsWQCLcBGAsYHQ/s0/malware.jpg)

Chief among the new entrants is AvosLocker, a ransomware-as-a-service (RaaS) group that commenced operations in late June via "press releases" that are branded with a blue beetle logo to recruit new affiliates. The cartel, which also runs a data leak and extortion site, is said to have breached six organizations in the U.S., U.K., U.A.E., Belgium, Spain, and Lebanon, with ransom demands ranging anywhere from \$50,000 to \$75,000.

In contrast, Hive, despite opening shop in the same month as AvosLocker, has already hit several healthcare providers and mid-size organizations, including a European airline company and three U.S.-based entities, among other victims located in Australia, China, India, Netherlands, Norway, Peru, Portugal, Switzerland, Thailand, and the U.K.

Also detected in the wild is a Linux variant of the HelloKitty ransomware, which singles out Linux servers running VMware's ESXi hypervisor. "The observed variants impacted five organizations in Italy, Australia, Germany, the Netherlands and the U.S.," Unit 42 researchers Doel Santos and Ruchna Nigam said. "The highest ransom demand observed from this group was \$10 million, but at the time of writing, the threat actors have only received three transactions that sum up to about \$1.48 million."

A black banner advertisement for Keeper. On the left is the Keeper logo, a yellow circle with a grid pattern, followed by the word "KEEPER" in white. To the right of the logo is the text "Seamless SSO Integration for Password Security & Authentication" in white. On the far right is a yellow button with the text "Start Free Trial" in black. The background of the banner features a hand holding a glowing blue sphere with various icons and a smartphone in the foreground.

(https://go.thn.li/auth_728)

Last to join the list is LockBit 2.0, an established ransomware group that **resurfaced in June** (https://twitter.com/Intel_by_KELA/status/1406905385580118017) with 2.0 version of their affiliate program touting its "unparalleled benefits" of "encryption speed and self-spread function." Not only do the developers claim it's "the fastest encryption software all over the world," the group offers a stealer named StealBit that enables the attackers to download victims' data.



ALL YOUR **IMPORTANT FILES** ARE **STOLEN AND ENCRYPTED!**

All your files stolen and encrypted
for more information see
RESTORE-MY-FILES.TXT
that is located in every encrypted folder.

Would you like to earn millions of dollars?
Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company.
You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc.
Open our letter at your email. Launch the provided virus on any computer in your company.
Companies pay us the foreclosure for the decryption of files and prevention of data leak.
You can communicate with us through the Tox messenger
<https://tox.chat/download.html>
Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.
If you want to contact us, use ToxD:
3085B89A0C515D2FB124D645908F5D3DA5CB97CEBEA975959AE4F95302A04E1D709C3C4AE9B7
If this contact is expired, and we do not respond you, look for the relevant contact data on our website via Tor or Brave Browser
<http://lockbitapt6vx573eeqjofwgcgmultr3a35nygvokja5uuocip4ykyrd.onion>

(<https://thehackernews.com/images/-pxxrlpjAJw0/YSTSXMESxmi/AAAAAAAADns/YRWjb8Bz0E0ES1JwEKbsTGIhdePk-Nx4gCLcBGAsYHQ/s0/ransomware.jpg>)

Since its June 2021 debut, LockBit 2.0 has compromised 52 organizations in accounting, automotive, consulting, engineering, finance, high-tech, hospitality, insurance, law enforcement, legal services, manufacturing, non-profit energy, retail, transportation, and logistics industries spanning across Argentina, Australia, Austria, Belgium, Brazil, Germany, Italy, Malaysia, Mexico, Romania, Switzerland, the U.K., and the U.S.

If anything, the emergence of new ransomware variants show that cybercriminals are doubling down on ransomware attacks, underscoring the extremely profitable nature of the crime.

"With major ransomware groups such as [REvil](https://thehackernews.com/2021/07/revil-ransomware-gang-mysteriously.html) (<https://thehackernews.com/2021/07/revil-ransomware-gang-mysteriously.html>) and [DarkSide](https://thehackernews.com/2021/05/us-pipeline-ransomware-attackers-go.html) (<https://thehackernews.com/2021/05/us-pipeline-ransomware-attackers-go.html>) lying low or rebranding to evade law enforcement heat and media attention, new groups will emerge to replace the ones that are no longer actively targeting victims," the researchers said. "While LockBit and HelloKitty have been previously active, their recent evolution makes them a good example on how old groups can re-emerge and remain persistent threats."

Found this article interesting? Follow THN on [Facebook](https://www.facebook.com/thehackernews)

(<https://www.facebook.com/thehackernews>) , [Twitter](https://twitter.com/thehackersnews) 

(<https://twitter.com/thehackersnews>) and [LinkedIn](https://www.linkedin.com/company/thehackernews/)

(<https://www.linkedin.com/company/thehackernews/>) to read more exclusive content we post.