

# Lazarus experiments with new ransomware

The Lazarus cybercrime group uses traditional APT techniques to spread VHD ransomware.

 Nikolay Pankov

July 28, 2020



The Lazarus group has always stood out for using methods typical of APT attacks but specializing in financial cybercrime. Recently, our experts detected fresh, previously unexplored VHD malware, which Lazarus seems to be experimenting with.

Lazarus Ransomware targeted attacks

Volume Information folders (thereby sabotaging System Restore attempts in Windows). What’s more, it can suspend processes that could potentially protect important files from modification (such as Microsoft Exchange or SQL Server).

But what’s really interesting is how VHD gets onto target computers, because its delivery mechanisms have more in common with APT attacks. Our experts recently investigated a couple of VHD cases, analyzing the attackers’ actions in each.

# Lateral movement through the victim’s network

In the first incident, our experts’ attention was drawn to the malicious code responsible for spreading VHD over the target network. It turned out that the ransomware had at its disposal lists of IP addresses of the victim’s computers, as well as credentials for accounts with admin rights. It used that data for brute-force attacks on the SMB service. If the malware managed to connect using the SMB protocol to the network folder of another computer, it copied and executed itself, encrypting that machine also.

Such behavior is not very typical of mass ransomware. It suggests at least a preliminary reconnaissance of the victim’s infrastructure, which is more characteristic of APT campaigns.

# Chain of infection

The next time our Global Emergency Response Team encountered this ransomware during an investigation, the researchers were able to trace the entire infection chain. As they reported, the cybercriminals:

- 1 Gained access to victims’ systems by exploiting a vulnerable VPN gateway;
- 2 Obtained admin rights on the compromised machines;
- 3 Installed a backdoor;
- 4 Seized control of the Active Directory server;
- 5 Infected all computers on the network with the VHD ransomware using a loader specially written for the task.

Further analysis of the tools employed showed the backdoor to be part of [the multiplatform MATA framework](#) (which some of our colleagues call Dacls). We’ve concluded that it’s another Lazarus tool.

You’ll find a detailed technical analysis of these tools, together with indicators of compromise, [in the relevant article on our Securelist blog](#).

# How to protect your company

The VHD ransomware actors are clearly a cut above average when it comes to

infecting systems. While most ransomware is available on hacker forums, rather, it’s specifically developed for targeted attacks.



## Related



ShrinkLocker ransomware employing BitLocker for encryption




Ransomware: the most high-profile attacks of 2023

The techniques used to penetrate the victim’s infrastructure and propagate within the network recall sophisticated APT attacks.

This gradual blurring of the boundaries between financial cybercrime tools and APT attacks is proof that even smaller companies need to consider using more advanced security technologies. With that in mind, we recently unveiled an integrated solution with both Endpoint Protection Platform (EPP) and Endpoint Detection and Response (EDR) functionality. You can find out more about the solution on [its dedicated page](#).

# Most tested. Most awarded.

Kaspersky solutions top independent testing ranks year after year.



k

↓ Read next

## Five regular checks for SMBs


Five things that, if neglected, can cost SMBs dearly.



• July 27, 2020



## Tips

 Tips

### Subscribe or treat? Manage your subscriptions with ease

Many of us have dozens of online subscriptions and recurring payments. How to take control, save money, and stay on top of expenses?

 Tips

### How to set up security and privacy in adidas Running (Runtastic)

A detailed guide on setting up privacy in the adidas Running app.



• October 30, 2024



Tips

## Taking a selfie with your ID card — is it safe?

Many popular online services these days require a selfie with your ID card or passport to register. We explore whether taking such photos is safe (spoiler: it's not) and how to minimize the risks.



• October 23, 2024



• October 24, 2024



Tips

## Will AI replace SOC analysts?

We share our experience on the optimal use of AI models in the SOC of our Kaspersky MDR service.



• October 22, 2024

# Sign up to receive our headlines in your inbox

Email Address

☐

I agree to provide my email address to "AO Kaspersky Lab" to receive information about new posts on the site. I understand that I can withdraw this consent at any time via e-mail by clicking the "unsubscribe" link that I find at the bottom of any e-mail sent to me for the purposes mentioned above.

### Home Solutions

Kaspersky Standard

Kaspersky Plus

Kaspersky Premium

All Solutions

### Small Business Products

1-100 EMPLOYEES

Kaspersky Small Office Security

Kaspersky Endpoint Security Cloud

All Products

We use cookies to make your experience of our websites better. By using and further navigating this website you accept this. Detailed information about the use of cookies on this website is available by clicking on more information.

ACCEPT AND CLOSE



Medium Business Products

101-999 EMPLOYEES

Kaspersky Next

Kaspersky Endpoint Security Cloud

Kaspersky Endpoint Security for Business Select

Kaspersky Endpoint Security for Business Advanced

All Products

Enterprise Solutions

1000 EMPLOYEES

Kaspersky Next

Cybersecurity Services

Threat Management and Defense

Endpoint Security

Hybrid Cloud Security

All Solutions

Copyright © 2024 AO Kaspersky Lab. All Rights Reserved. • [Privacy Policy](#) • [Anti-Corruption Policy](#) • [License Agreement B2C](#) • [License Agreement B2B](#)

[Contact Us](#) • [About Us](#) • [Partners](#) • [Blog](#) • [Resource Center](#) • [Press Releases](#) • [Trust Kaspersky](#)

[Securelist](#) • [Eugene Personal Blog](#) • [Encyclopedia](#)



Global