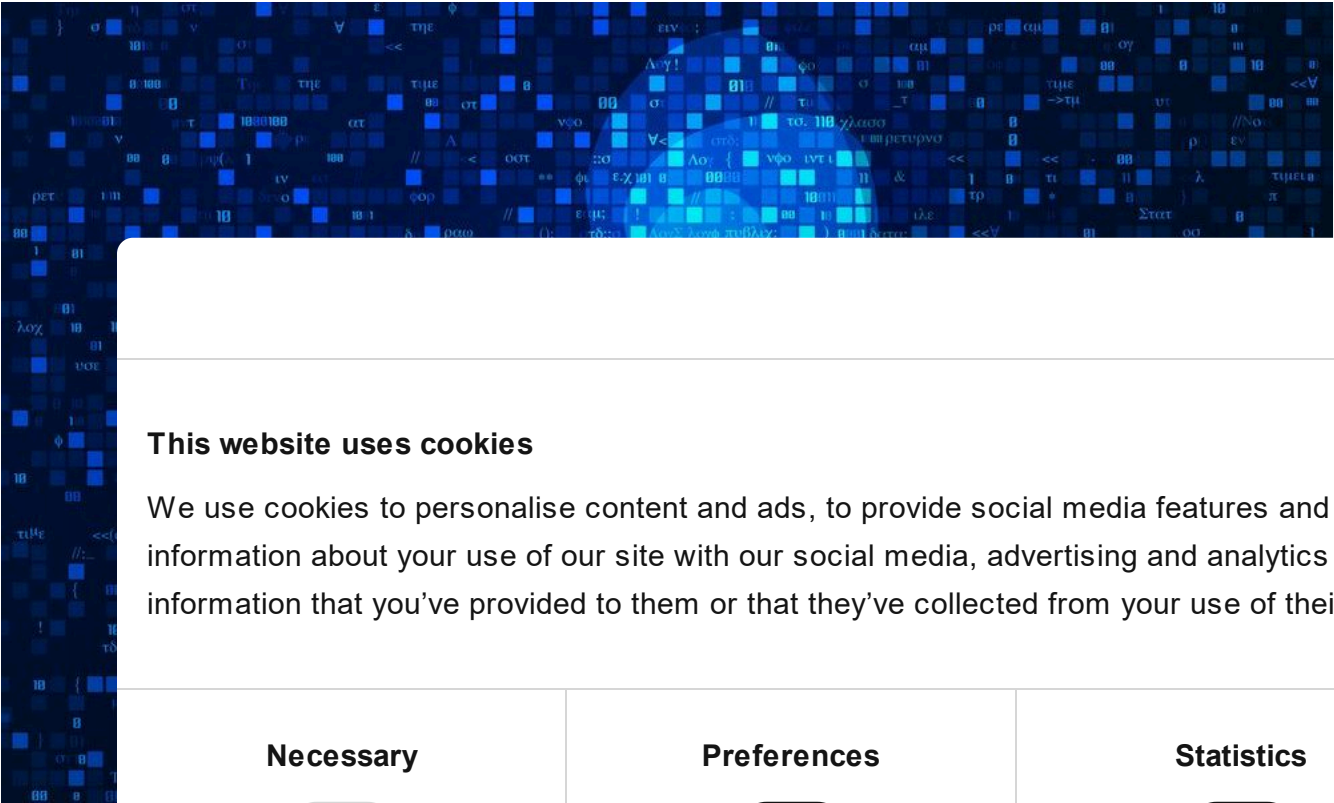


Lazarus on the hunt for big game

APT REPORTS

28 JUL 2020

5 minute read



GREAT WEBINARS

13 MAY 2021, 1:00PM
 GReAT Ideas. Balalaika Edition
BORIS LARIN, DENIS LEGEZO

// AU



We may rather understand the threat landscape around the world through the lens of these incidents and through discussions with some of our trusted industry partners, we feel that we now have a good grasp on how the ransomware ecosystem is structured.

22 JUL 2020, 2:00PM
 GReAT Ideas. Powered by SAS: threat hunting and new techniques
DMITRY BESTUZHEV, COSTIN RAIU, PIERRE DELCHER,
BRIAN BARTHOLOMEW, BORIS LARIN, ARIEL JUNGHEIT,
FABIO ASSOLINI

Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

Necessary



Preferences



Statistics



Marketing



Show details

Use necessary cookies only

Allow all cookies

Structure of the ransomware ecosystem

Criminals piggyback on widespread botnet infections (for instance, the infamous [Emotet](#) and [Trickbot](#) malware families) to spread into the network of promising victims and license ransomware “products” from third-party developers. When the attackers have a good understanding of the target’s finances and IT processes, they deploy the ransomware on all the company’s assets and enter the negotiation phase.

This ecosystem operates in independent, highly specialized clusters, which in most cases have no links to each other beyond their business ties. This is why the concept of threat actors gets fuzzy: the group responsible for the initial breach is unlikely to be the party that compromised the victim’s Active Directory server, which in turn is not the one that wrote the actual ransomware code used during the incident. What’s more, over the course of two incidents, the same criminals may switch business partners and could be leveraging different botnet and/or ransomware families altogether.

But of course, no complex ecosystem could ever be described by a single, rigid set of rules and this one is no exception. In this blog post, we describe one of these outliers over two separate investigations that occurred between March and May 2020.

Case #1: The VHD ransomware

This first investigation was about a ransomware group (VHD) that had been written in 2017. The group’s “System” was a ransomware that also stole data from the SQL Server database and our initial investigation implemented the following:

- The ransomware used the victim’s cryptographic algorithm to encrypt the data and the pattern of the cybe
- VHD ransomware stored internal materials on the hard drive, in clear text. This information is not deleted securely afterwards, which implies there may be a chance to recover some of the files.

FROM THE SAME AUTHORS

Tomiris called, they want their Turla malware back

VileRAT: DeathStalker’s continuous strike at foreign and cryptocurrency exchanges

The SessionManager IIS backdoor



This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services.

Necessary



Preferences



Statistics



Marketing



Show details >

The Mersenne Twister RNG is reseeded every time it is called.

To the best of our knowledge, this malware family was first discussed publicly in [this blog post](#).

A spreading utility, discovered along the ransomware, propagated the program inside the network. It contained a list of administrative credentials and IP addresses specific to the victim, and leveraged them to brute-force the SMB service on every discovered machine. Whenever a successful connection was made, a network share was mounted, and the VHD ransomware was copied and executed through WMI calls. This stood out to us as an uncharacteristic technique for cybercrime groups; instead, it reminded us of the APT campaigns [Sony SPE](#), [Shamoon](#) and [OlympicDestroyer](#), three previous wipers with worming capabilities.

We were left with more questions than answers. We felt that this attack did not fit the usual *modus operandi* of known big-game hunting groups. In addition, we were only able to find a very limited number of VHD ransomware samples in our telemetry, and a few public references. This indicated that this ransomware family might not be traded widely on dark market forums, as would usually be the case.

Case #2: Hakuna MATA

A second incident, two months later, was handled by Kaspersky’s Incident Response team (GERT). That meant we were able to get a complete picture of the infection chain leading to the installation of the VHD ransomware.

In this incident, we discovered a backdoor on a server. The backdoor was a custom-written in Python that we still believe to be in development. The whole infection took place over the course of 10 hours.

A more relevant piece of information is that the backdoor used during this incident is an instance of a multiplatform framework we call MATA (some vendors also call it [Dacls](#)). On July 22, we published a [blog article dedicated](#) to this framework. In it, we provide an in-depth description of its capabilities and provide evidence of its links to the Lazarus group. [Other members of the industry](#) independently reached similar conclusions.

The forensics evidence gathered during the incident response process is strong enough that we feel comfortable stating with a high degree of confidence that there was only a single threat actor in the victim’s network during the time of the incident.

Conclusion

The data we have at our disposal tends to indicate that the VHD ransomware is not a commercial off-the-shelf product; and as far as we know, the Lazarus group is the sole owner of the MATA framework. Hence, we conclude that the VHD ransomware is also owned and operated by Lazarus.

Subscribe to our weekly e-mails

The hottest research right in your inbox

Email(Required)

☐ 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.



This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services.

Necessary	Preferences	Statistics	Marketing
<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>

Show details >

IN THE SAME CATEGORY

Beyond the Surface: the evolution and expansion of the SideWinder APT group

Circling back to our introduction, this observation is at odds with what we know about the cybercrime ecosystem. Lazarus has always existed at a special crossroads between APT and financial crime, and there have long been rumors in the threat intelligence community that [the group was a client of various botnet services](#). We can only speculate about the reason why they are now running solo ops: maybe they find it difficult to interact with the cybercrime underworld, or maybe they felt they could no longer afford to share their profits with third parties.

It's obvious the group cannot match the efficiency of other cybercrime gangs with their hit-and-run approach to targeted ransomware. Could they really set an adequate ransom price for their victim during the 10 hours it took to deploy the ransomware? Were they even able to figure out where the backups were located? In the end, the only thing that matters is whether these operations turned a profit for Lazarus.

Only time will tell whether they jump into hunting big game full time, or scrap it as a failed experiment.

Indicators of compromise

The spreader utility contains a list of administrative credentials and IP addresses specific to the victim which is whv it's not listed in the IoC section

As the in
be provi

VHD ran
6D12547
D0806C
DD00A8
CCC602
EFD4A8

Domains
172.93.18-
23.227.19
104.232.7
mnmski.c
a legit w
compro

BOTNET

- MALWARE TECHNOLOGIES
- RANSOMWARE
- TARGETED ATTACKS
- VHD RANSOMWARE

BlindEagle flying high in Latin America

EastWind campaign: new CloudSorcerer attacks on government organizations in Russia

APT trends report Q2 2024

CloudSorcerer – A new APT targeting Russian government entities



This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

Necessary



Preferences



Statistics



Marketing



Show details >

Lazarus on the hunt for big game

Your email address will not be published. Required fields are marked *

Type your comment here

Name *

Email *

Comment

// LATEST POSTS

SAS

The Crypto Game of Lazarus APT: Investors vs. Zero-days

BORIS LARIN, VASILY BERDNIKOV

MALWARE DESCRIPTIONS

Grandoreiro, the global trojan with grandiose goals

GREAT

CRIMEWARE REPORTS

Stealer here, stealer there, stealers everywhere!

GREAT

New product

Get your business' security to the Next level

Kaspersky Next

KASPERSKY

// LATEST

04 SEP 2024
Inside the hum
the hum
cybercr
ANNA PAVLOVA

Beyond
expansi

Kaspersky analyzes SideWinder APT's recent activity: new targets in the MiddleEast and Africa, post-exploitation tools and techniques.

EastWind campaign: new CloudSorcerer attacks on government organizations in Russia

Kaspersky has identified a new EastWind campaign targeting Russian organizations and using CloudSorcerer as well as APT31 and APT27 tools.

TTPs of the BlindEagle APT, which targets organizations and individuals in Colombia, Ecuador, Chile, Panama and other Latin American countries.

APT trends report Q2 2024

The report features the most significant developments relating to APT groups in Q2 2024, including the new backdoor in Linux utility XZ, a new RAT called SalmonQT, and hacktivist activity.


Let's go Next: redefine your business's cybersecurity

Kaspersky Next

// SUBSCRIBE TO OUR WEEKLY E-MAILS

The hottest research right in your inbox

Email

Subscribe

☐ 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.

kaspersky

THREATS

- APT (Targeted attacks)
- Secure environment (IoT)
- Mobile threats
- Financial threats
- Spam and phishing

CATEGORIES

- APT reports
- Malware descriptions
- Security Bulletin
- Malware reports
- Spam and phishing reports

OTHER SECTIONS

- Archive
- All tags
- Webinars
- APT Logbook
- Statistics



This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services.

Necessary



Preferences



Statistics



Marketing



Show details >