Solutions for: Home Products | Small Business 1-50 employees | Medium Business 51-999 employees | Enterprise 1000+ employees

SECURELIST by Kaspersky

CompanyAccount | Get In Touch | Dark mode | English

Solutions | Industries | Products | Services | Resource Center | About Us | GDPR

Content menu | Search... | Subscribe

LuminousMoth APT: Sweeping attacks for the chosen few

APT REPORTS 14 JUL 2021 12 minute read

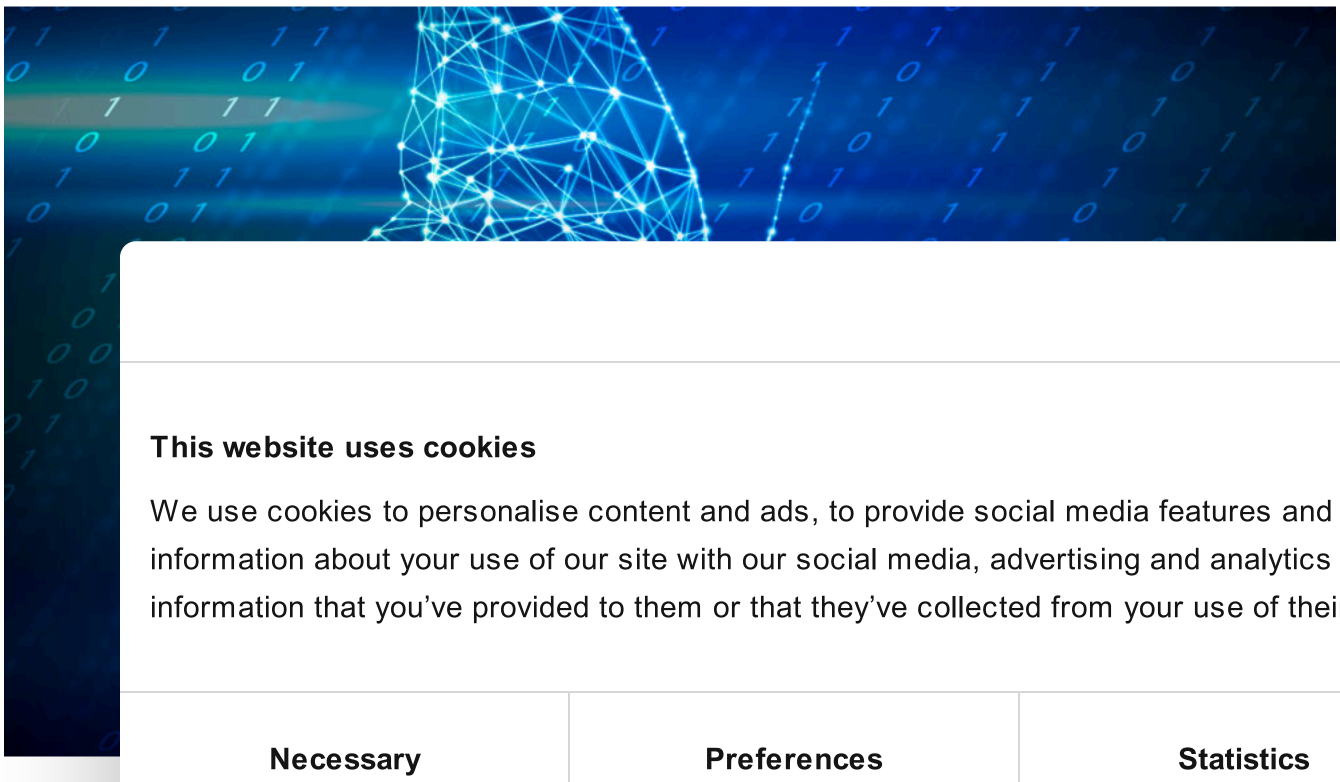


Table of Contents

What were the origins of the infections?

Older spreading mechanism

kies

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

// AU

MAI

APT act
handpick
vectors,
It's not o
due to such attacks being noisy, and thus putting the underlying operation at risk of being compromised by security products or researchers.

We recently came across unusual APT activity that exhibits the latter trait – it was detected in high volumes, albeit most likely aimed at a few targets of interest. This large-scale and highly active campaign was observed in South East Asia and dates back to at least October 2020, with the most recent attacks seen around the time of writing. Most of the early sightings were in Myanmar, but it now appears the attackers are much more active in the Philippines, where there are more than 10 times as many known targets.

Further analysis revealed that the underlying actor, which we dubbed LuminousMoth, shows an affinity to the HoneyMyte group, otherwise known as Mustang Panda. This is evident in both network infrastructure connections, and the usage of similar TTPs to deploy the Cobalt Strike Beacon as a payload. In fact, our colleagues at ESET and Avast recently assessed that HoneyMyte was active in the same region. The proximity in time and common occurrence in Myanmar of both campaigns could suggest that various TTPs of HoneyMyte may have been borrowed for the activity of LuminousMoth.

Most notably though, we observed the capability of the culprit to spread to other hosts through the use of USB drives. In some cases, this was followed by deployment of a signed, but fake version of the popular application Zoom, which was in fact malware enabling the attackers to exfiltrate files from the compromised systems. The sheer volume of the attacks raises the question of whether this is caused by a rapid replication through removable devices or by an unknown infection vector, such as a watering hole or a supply chain attack.

In this publication we aim to profile LuminousMoth as a separate entity, outlining the infection chain and unique toolset it leverages, the scale and targeting in its campaigns as well as its connections to HoneyMyte through common TTPs and shared resources.

What were the origins of the infections?

We identified two infection vectors used by LuminousMoth: the first one provides the attackers with initial access to a system. It consists of sending a spear-phishing email to the victim containing a Dropbox download link. The link leads to a RAR archive that masquerades as a Word document by setting the “file_subpath” parameter to point to a filename with a .DOCX extension.

```
hxxps://www.dropbox[.]com/s/esh1ywo9irbexvd/COVID-19%20Case%2012-11-
2020.rar?dl=0&file_subpath=%2FCOVID-19+Case+12-11-2020%2FCOVID-19+Case+12-11-2020(2).docx
```

The archive contains two malicious DLL libraries as well as two legitimate executables that sideload the DLL files. We found multiple archives like this with file names of government entities in Myanmar, for example “COVID-19 Case 12-11-2020(MOTC).rar” or “DACU Projects.r01”
(MOTC i
Develop
(FERD) i

Infection chain

The second infection vector comes into play after the first one has successfully finished, whereby the malware tries to spread by infecting removable USB drives. This is made possible through the use of two components: the first is a malicious library called “version.dll” that gets sideloaded by “igfxem.exe”, a Microsoft Silverlight executable originally named “sllauncher.exe”. The second is “wwlib.dll”, another malicious library sideloaded by the legitimate binary of “winword.exe”. The purpose of “version.dll” is to spread to removable devices, while the purpose of “wwlib.dll” is to download a Cobalt Strike beacon.

The first malicious library “version.dll” has three execution branches, chosen depending on the provided arguments, which are: “assist”, “system” or no argument. If the provided argument is “assist”, the malware creates an event called “nfvlqfnlqwnlf” to avoid multiple executions and runs “winword.exe” in order to sideload the next stage (“wwlib.dll”). Afterwards, it modifies the registry by adding an “Opera Browser Assistant” entry as a run key, thus achieving persistence and executing the malware with the “assist” parameter upon system startup.

Registry value to run the malware at system startup

Then, the malware checks if there are any removable drives connected to the infected system. If any are found, it enumerates the files stored on the drive and saves the list to a file called "udisk.log". Lastly, the malware is executed once again with the "system" parameter.

If the provided argument is "system", a different event named "qjlfqwle21ljl" is created. The purpose of this execution branch is to deploy the malware on all connected removable devices, such as USB sticks or external drives. If a drive is found, the malware creates hidden directories carrying non ascii characters on the drive and moves all the victim's files there, in addition to the two malicious libraries and legitimate executables. The malware then renames the file "igfxem.exe" to "USB Driver.exe" and places it at the root of the drive along with "version.dll". As a result, the victims are no longer able to view their own drive files and are left with only

hidden fi

If no arg
launched
The malv
reposito
executes
the hidden files that were located on the drive before the compromise, and the user is able to view them.

The second library, "wwlib.dll", is a loader. It gets sideloaded by "winword.exe" and emerged two months prior to "version.dll", suggesting that earlier instances of the attack did not rely on replication through removable drives but were probably distributed using other methods such as the spear-phishing emails we observed.

"Wwlib.dll" fetches a payload by sending a GET request to the C2 address at "103.15.28[.]195". The payload is a Cobalt Strike beacon that uses the Gmail malleable profile to blend with benign traffic.

GREAT WEBINARS

13 MAY 2021, 1:00PM

GReAT Ideas. Balalaika Edition

BORIS LARIN, DENIS LEGEZO

n

SHIMARU,

:
IoT

MELEV

: threat

BAB,

GReAT Ideas. Powered by SAS: threat hunting and new techniques

DMITRY BESTUZHEV, COSTIN RAIU, PIERRE DELCHER, BRIAN BARTHOLOMEW, BORIS LARIN, ARIEL JUNGHEIT, FABIO ASSOLINI

Downloading a Cobalt Strike beacon from 103.15.28[.]195

Older spreading mechanism

We discovered an older version of the LuminousMoth infection chain that was used briefly before the introduction of “version.dll”. Instead of the usual combination of “version.dll” and “wwlib.dll”, a different library called “wwlib.dll” is in fact the first loader in this variant and is in charge of spreading to removable drives, while a second “DkAr.dll” library is in charge of downloading a Cobalt Strike beacon from the C2 server. This variant’s “wwlib.dll” offers two execution branches: one triggered by the argument “Assistant” and a second one with no arguments given. When this library is sideloaded by “winword.exe”, it creates an event called “fjsakljflwqlqewq”, adds a registry value for persistence, and runs “PrvDisk.exe” that then sideloads “DkAr.dll”.

The final step taken by “wwlib.dll” is to copy itself to any removable USB device. To do so, the malware checks if there are any files carrying a .DOC or .DOCX extension stored on the connected devices. If such a document is found, the malware replaces it with the “winword.exe” binary, keeping the document’s file name but appending “.exe” to the end. The original document is then moved to a hidden directory. The “wwlib.dll” library is copied to the same directory containing the fake document and the four samples (two legitimate PE files, two DLL libraries) are copied to “[*USB_Drive_letter*]:\System Volume Information\en-AU\Qantas”.

If the ma
started
malware
of the vi
“C:\User
the “Ass

Since th
attacker
which ra
means t
them, an
regardle

Post

The atta
Myanma
exfiltrate them to a C2 server. Interestingly, this stealer impersonates the popular Zoom video telephony software. One measure to make it seem benign is a valid digital signature provided with the binary along with a certificate that is owned by Founder Technology, a subsidiary of Peking University’s Founder Group, located in Shanghai.

FROM THE SAME AUTHORS

Operation TunnelSnake

king in

To facilit
"zVideoU
vital that
The con

Paramete	
meeting	
ssb_sdk	
zAutoUp	
XmppDll	
zKBCrypt	
zCrashReport	Suffix string appended to the name of the staging directory used to host exfiltrated files before they are archived.
zWebService	Path prefix for the exfiltration staging directory.
zzhost	Path to the file that will hold a list of hashes corresponding to the files collected for exfiltration.
ArgName	AES key for configuration string encryption.
Version	AES IV for configuration string encryption.
zDocConverter	Path #1 to a directory to look for files with the extension intended for exfiltration
zTscoder	Path #2 to a directory to look for files with the extension intended for exfiltration
zOutLooklMutil	Path #3 to a directory to look for files with the extension intended for exfiltration

Each field in the configuration file (with the exception of Version, ArgName and zCrashReport) is encoded with Base64. While the authors incorporated logic and parameters that allow the decryption of some of the fields specified above with the AES algorithm, it remains unused.

The stealer uses the parameters in order to scan the three specified directories (along with root paths of fixed and removable drives) and search for files with the extensions given in the zKBCrypto parameter. Matching files will then be copied to a staging directory created by the malware in a path constructed with the following structure: "<zWebService>\%Y-%m-%d %H-%M-%S<zCrashReport>". The string format in the directory's name represents the time and date of the malware's execution.

In addition, the malware collects the metadata of the stolen files. One piece of data can be found as a list of original paths corresponding to the exfiltrated files that is written to a file named 'VideoCoingLog.txt'. This file resides in the aforementioned staging directory. Likewise, a second file is used to hold the list of hashes corresponding to the exfiltrated files and placed in the path specified in the zzhost parameter.

After collection of the targeted files and their metadata, the malware executes an external utility in order to archive the staging directory into a .rar file that will be placed in the path specified in the zWebService parameter. The malware assumes the existence of the utility in a path specified under the XmppDll parameter, suggesting the attackers have prior knowledge of the infected system and its pre-installed applications.

Finally, th
should b
linked CU
transact

CURL logic used to issue the archive of exfiltrated files to the C&C

Post exploitation tool: Chrome Cookies Stealer

The attackers deployed another tool on some infected systems that steals cookies from the Chrome browser. This tool requires the local username as an argument, as it is needed to access two files containing the data to be stolen:

```
C:\Users\[USERNAME]\AppData\Local\Google\Chrome\User Data\Default\Cookies
C:\Users\[USERNAME]\AppData\Local\Google\Chrome\User Data\Local State
```

The stealer starts by extracting the encrypted_key value stored in the “Local State” file. This key is base64 encoded and used to decode the cookies stored in the “Cookies” file. The stealer uses the CryptUnprotectData API function to decrypt the cookies and looks for eight specific cookie values: SID, OSID, HSID, SSID, LSID, APISID, SAPISID and ACCOUNT_CHOOSER:

Cookie values the stealer looks for

Once found, the malware simply displays the values of those cookies in the terminal. The Google policy available here explains that these cookies are used to authenticate users:

During o
using the
hijacking

Com

For C2 c
whereas

- 103.15.28[.]195
- 202.59.10[.]253

Infrastructure ties from those C2 servers helped reveal additional domains related to this attack that impersonate known news outlets in Myanmar, such as MMTimes, 7Day News and The Irrawaddy. Another domain “mopfi-ferd[.]com” also impersonated the Foreign Economic Relations Department (FERD) of the Ministry of Planning, Finance and Industry (MOPFI) in Myanmar.

- mmtimes[.]net
- mmtimes[.]org
- 7daydai1y[.]com
- irrawddy[.]com
- mopfi-ferd[.]com

“Mopfi-ferd[.]com” resolved to an IP address that was associated with a domain masquerading as the Zoom API. Since we have seen the attackers deploying a fake Zoom application, it is possible this look-alike domain was used to hide malicious Zoom traffic, although we have no evidence of this.

Who

We were
which ar
Myanma
It seems
organiza

It is likely
its sprea
connect
activity i
solely in the Philippines. It could, however, simply be that the attackers are more interested in going after targets from this region.

Connections to HoneyMyte

Over the course of our analysis, we noticed that LuminousMoth shares multiple similarities with the HoneyMyte threat group. Both groups have been covered extensively in our private reports, and further details and analysis of their activity are available to customers of our private APT reporting service. For more information, contact: intelreports@kaspersky.com.

LuminousMoth and HoneyMyte have similar targeting and TTPs, such as the usage of DLL side-loading and Cobalt Strike loaders, and a similar component to LuminousMoth's Chrome cookie stealer was also seen in previous HoneyMyte activity. Lastly, we found infrastructure overlaps between the C2 servers used in the LuminousMoth campaign and an older one that has been attributed to HoneyMyte.

Some of LuminousMoth's malicious artifacts communicate with "updatecatalogs[.]com", which resolves to the same IP address behind "webmail.mmtimes[.]net". This domain was observed in a campaign that dates back to early 2020, and was even found on some of the systems that were later infected with LuminousMoth. In this campaign, a legitimate binary ("FmtOptions.exe") sideloads a malicious DLL called “FmtOptions.dll”, which then decodes and executes the contents of the file “work.dat”. This infection flow also involves a service called “yerodns.dll” that implements the same functionality as “FmtOptions.dll”.

The domain “webmail.mmtimes[.]net” previously resolved to the IP “45.204.9[.]70”. This address is associated with another MMTimes look-alike domain used in a HoneyMyte campaign during 2020: “mmtimes[.]org”. In this case, the legitimate executable “mcf.exe” loads “mcutil.dll”. The purpose of “mcutil.dll” is to decode and execute “mfc.ep”, a PlugX backdoor that communicates with “mmtimes[.]org”. Parts of this campaign were also covered in one of our private reports discussing HoneyMyte’s usage of a watering hole to infect its victims.

Therefore, based on the above findings, we can assess with medium to high confidence that the LuminousMoth activity is indeed connected to HoneyMyte.

IN THE SAME CATEGORY

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

BlindEagle flying high in Latin

ew
s on
ions in

2024

w APT

Connection between HoneyMyte and LuminousMoth C2s

Conclusions

LuminousMoth represents a formerly unknown cluster of activity that is affiliated to a Chinese-speaking actor. As described in this report, there are multiple overlaps between resources used by LuminousMoth and those sighted in previous activity of HoneyMyte. Both groups, whether related or not, have conducted activity of the same nature – large-scale attacks that affect a wide perimeter of targets with the aim of hitting a few that are of interest.

On the same note, this group’s activity and the apparent connections may hint at a wider phenomenon observed during 2021 among Chinese-speaking actors, whereby many are re-tooling and producing new and unknown malware implants. This allows them to obscure any ties to their former activities and blur their attribution to known groups. With this challenge in mind, we continue to track the activity described in this publication with an eye to understanding its evolution and connection to previous attacks.

Indicators of Compromise

Version.dll payloads

Hashes	Compilation Date
0f8b7a64336b4315cc0a2e6171ab027e 2d0296ac56db3298163bf3f6b622fdc319a9be23 59b8167afba63b9b4fa4369e6664f274c4e2760a4e2ae4ee12d43c07c9655e0f	Dec 24 09:20:16 2020
37054e2e8699b0bdb0e19be8988093cd 5e45e6e113a52ba420a35c15fbaa7856acc03ab4 a934ae0274dc1fc9763f7aa51c3a2ce1a52270a47dcdd80bd5b9afbc3a23c82b	Dec 24 09:19:51 2020
c05cdf3a29d6fbe4e3e8621ae3173f08 75cd21217264c3163c800e3e59af3d7db14d76f8 869e7da2357c673dab14e9a64fb69691002af5b39368e6d1a3d7fda242797622	Dec 29 11:45:41 2020
5ba1384b4edfe7a93d6f1166da05ff6f 6d18970811821125fd402cfa90210044424e223a 857c676102ea5dda05899d4e386340f6e7517be2d2623437582acbe0d46b19d2	Jan 07 11:18:38 2021
afb777236f1e089c9e1d33fce46a704c cf3582a6cdac3e254c017c8ce36240130d67834a 1ec88831b67e3f0d41057ba38ccca707cb508fe63d39116a02b7080384ed0303	Jan 14 11:18:50 2021

wwlib.

Hashes
4fbc4835 b43d7317 95bcc8c3

Relate

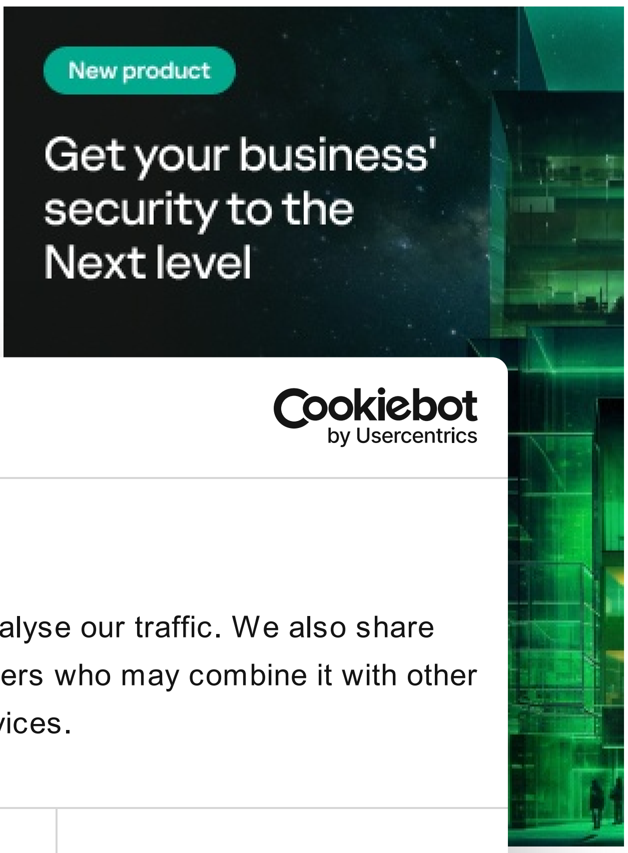
Hashes		
b31008f6 c1945fd976836ba2f3fbeafa276f60c3f0e9a51c 4a4b976991112b47b6a3d6ce19cc1c4f89984635ed16aea9f88275805b005461		10:00:42 2021
ac29cb9c702d9359ade1b8a5571dce7d 577ad54e965f7a21ba63ca4a361a3de86f02e925 d8de88e518460ee7ffdffaa4599ccc415e105fc318b36bc8fe998300ee5ad984	yerodns.dll	Oct 29 10:33:20 2019
afe30b5dd18a114a9372b5133768151c 9a6f97300017a09eb4ea70317c65a18ea9ac49bd cf757b243133feab2714bc0da534ba21cbcdde485fbda3d39fb20db3a6aa6dee	mcutil.dll	Jun 13 16:35:46 2019
95991f445d846455b58d203dac530b0b cee6afa1c0c8183900b76c785d2989bd1a904ffb f27715b932fb83d44357dc7793470b28f6802c2dc47076e1bc539553a8bfa8e0	mcutil.dll	Feb 21 09:41:11 2020

Post exploitation tools

Hashes	Name	Compilation Date
c727a8fc56cedc69f0cfd2f2f5796797 75d38bf8b0053d52bd5068adf078545ccdac563f 361ccc35f7ff405eb904910de126a5775de831b4229a4fdebfbacdd941ad3c56	ZoomVideoApp.exe	Mar 02 10:51:31 2021

Domains and IPs

103.15.28[.]195
202.59.10[.]253
updatecatalogs[.]com
mopfi-ferd[.]com
mmtimes[.]net
mmtimes[.]org
7daydai1y[.]com
irrawddy[.]com



APT

GOOGL

MICRO

Lumi

Your em

Type y

Name *

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

CRIMEWARE REPORTS

Analysis of the Crypt Ghouls group: continuing the investigation into a series of attacks on Russia

KASPERSKY

// LATEST WEBINARS

THR

04 SEP 20

Inside tl the hum cybercr

ANNA PAVLC

PS

60 MIN

acklogs

// RE

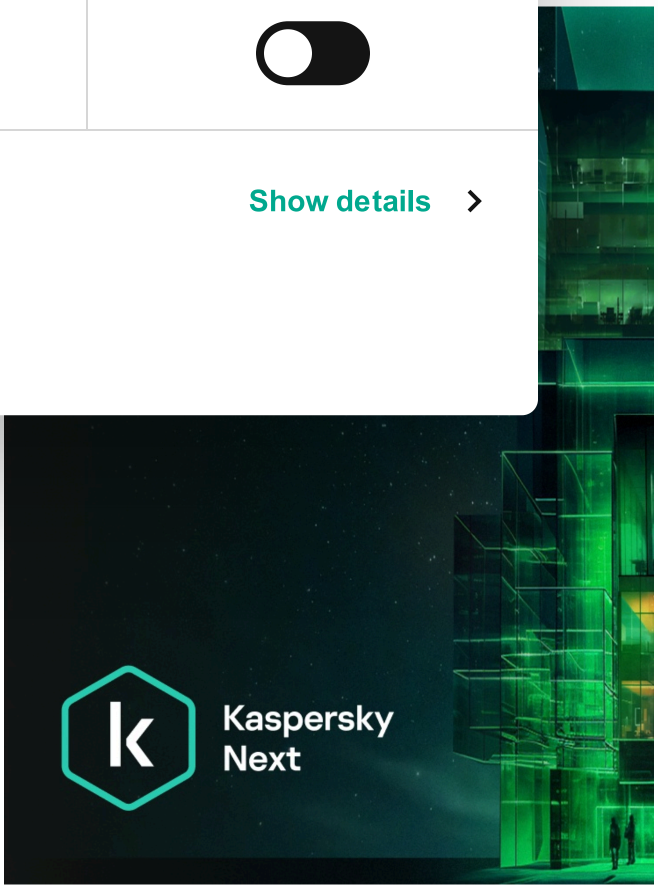
Beyond expansi

Kaspers activity: Africa, p

EastWin attacks Russia

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

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.



// 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
- Industrial threats
- Web threats
- Vulnerabilities and exploits
- All threats

CATEGORIES

- APT reports
- Malware descriptions
- Security Bulletin
- Malware reports
- Spam and phishing reports
- Security technologies
- Research
- Publications
- All categories

OTHER SECTIONS

- Archive
- All tags
- Webinars
- APT Logbook
- Statistics
- Encyclopedia
- Threats descriptions
- KSB 2023

Privacy Policy | License Agreement | Cookies