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

Key Group: another ransomware group using leaked builders

CRIMEWARE REPORTS 01 OCT 2024 11 minute read

Table of Contents

Timeline of Key Group's activity

Delivery and infection

Persistence methods

Victims

About the attackers

Takeaways

Indicators of compromise

// AUTHORS

Expert KASPERSKY

Key Group, or keygroup777, is a financially motivated ransomware group primarily targeting Russian users. The group is known for negotiating with victims on Telegram and using the Chaos ransomware builder.

The first public report on Key Group's activity was released in 2023 by BI.ZONE, a cybersecurity solutions vendor: the attackers drew attention when they left an ideological note during an attack on a Russian user, in which they did not demand money. However, according to our telemetry, the group was also active in 2022. Both before and after the attack covered in the BI.ZONE report, the attackers demanded that money be transferred to a Bitcoin wallet.

We tracked Key Group's activity from the start of their attacks and found that the group used not only Chaos but also other leaked ransomware builders. By analyzing the samples created with their help, we were able to find loaders and malicious URLs on GitHub that showed a connection between the group and previously unknown attackers.

Timeline of Key Group's activity

The first variants of ransomware from Key Group's arsenal were discovered in April 2022. At that time, the group was using the source code of Xorist.

In August 2022, Key Group added the Chaos builder to its toolkit. Notably, on June 30, 2022, the creator of Chaos announced the launch of a RaaS (Ransomware-as-a-Service) partnership program.

In the Chaos variant, a new extension `.huis_bn` was added to encrypted files, and in the ransom note, the attackers requested that victims send a message on Telegram. This note contained information in both Russian and English and went under the title "HOW TO DECRYPT FILES":

```
Attention! All your files are encrypted!
To restore your files and access them,
send an SMS with the text C32d4 to the User Telegram @[redacted]

You have 1 attempts to enter the code. If this
amount is exceeded, all data will irreversibly deteriorate. Be
careful when entering the code!

Glory @huis_bn
Ваши файлы зашифрованы!
Чтобы восстановить свои файлы и получить к ним доступ,
```

```
12  отправьте смс с текстом C32d4 Юзеру Телеграм @[redacted]
```

The next Key Group samples based on Chaos were discovered in January 2023. Throughout the year, the group used this ransomware, primarily changing only the content of the ransom note.

Starting in April 2023, the attackers were active on the DarkStore forum in the dark web. They targeted Telegram channels with spam raids and tested the publicly available remote access Trojan NjRat, which has keylogging, stealing, reverse shell, and USB propagation capabilities.

In the summer of 2023, a new sample of Chaos from Key Group was discovered, named `warnep.exe` (MD5: C2E1048E1E5130E36AF297C73A83AFF6).

The content of the note was significantly different from previous ones and was of an ideological nature. Key Group no longer provided contact information but declared its motives.

Note from Key Group

In August 2023, we discovered the group using the Annabelle ransomware (MD5: 05FD0124C42461EF553B4B17D18142F9).

This ransomware is named after the American horror film "Annabelle". The sample observed in Key Group's attacks encrypts files and includes an MBR locker (MD5: D06B72CEB10DFED5ECC736C85837F08E), as well as the following built-in evasion techniques.

1. Disabling Windows Firewall:

```
NetSh Advfirewall set allprofiles state off
```

2. Disabling Windows Defender:

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\
 "DisableAntiSpyware" = 1
 "DisableRealtimeMonitoring" = 1
```

3. Disabling UAC:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Syste
  "EnableLUA" = 0
```

4. Disabling the Registry Editor:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Syste
  "DisableRegistryTools" = 0
```

5. Disabling the Run command from the Windows Start menu:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explo
  "NoRun" = 1
```

6. Modifying Image File Execution Options by setting the `RIP` value instead of the debugger path for some processes, preventing them from launching correctly:

```
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
  "Debugger" = "RIP"
```

7. Deleting shadow copies:

```
"vssadmin delete shadows /all /quiet"
```

The ransomware adds the `.Keygroup777tg.EXE` extension to the encrypted files. After encryption, it restarts the computer and displays the following screens:

Screen from Annabelle (displayed immediately after encrypting files)

Screen from the MBR locker included in the Annabelle ransomware (displayed after reboot)

Around the same time, a sample of the Slam ransomware (MD5: 09CE91B4F137A4CBC1496D3791C6E75B) was detected in Key Group attacks. The Slam builder was also made publicly available back in 2021.

The Slam ransomware uses the AES-CBC encryption algorithm. It also utilizes the IP Logger service to track infected victims.

Upon execution, the ransomware encoded file names using Base64 and added the `.keygroup777tg` extension.

In September 2023, a wiper based on the RuRansom builder (MD5: 1FED852D312031974BF5EB988904F64E) was found.

RuRansom is a wiper that emerged in 2022 and targets Russia. The malware is written in .NET and uses the AES-CBC encryption algorithm to encrypt files. The Key Group variant is distributed under the name "Россия-обновление.docs.exe" (Russia-update) with a note modified for the group's objectives:

Note from Key Group (RuRansom sample)

Around the same time as the Key Group-branded RuRansom instances, a sample of another ransomware, UX-Cryptor, was observed in the attackers' activities. It is also written in .NET (MD5: 6780495DAD7EB372F1A660811F4894A6).

Instead of encrypting files, this sample terminates the `explorer.exe` process.

FROM THE SAME AUTHORS

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

Awaken Likho is awake: new techniques of an APT group

```
taskkill.exe /im Explorer.exe /f
```

It sets the following text on the current screen using the .NET method `System.Windows.Forms.Label.set_Text`:

From 12 to 21: how we discovered connections between the Twelve and BlackJack groups

-=TWELVE=- is back

Head Mare: adventures of a unicorn in Russia and Belarus

Message from UX-Cryptor

After that, UX-Cryptor additionally saves the ransom note in a file named `info-0v92.txt`, using output redirection of the `echo` command:

```
cmd.exe /c cd "%systemdrive%\Users\Public\Desktop"&attrib +h +s +
Ooops! Your files are encrypted by the keygroup777tg hacker group
@[redacted] 1>info-0v92.txt & attrib -h +s +r info-0v92.txt
```

UX-Cryptor includes several methods for persistence and detection evasion. For example, it overwrites the registry key `Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU`:

```
"Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU\MRULis
```

The `RunMRU` key is used by incident response specialists to examine commands executed through the `Run` utility.

In February 2024, Key Group switched from Chaos to the Hakuna Matata ransomware (MD5: DA09FCF140D3AAD0390FB7FAF7260EB5). The Hakuna Matata builder was published on the dark web in July 2023.

The Hakuna Matata variant encrypts files using AES-CBC and adds an extension of five random characters. Below is a snippet of

Hakuna Matata running in our sandbox.

Snippet of the Hakuna Matata execution process

After encryption, the sample saves a file named `keygroup777.txt` in the system and refers to it in a message set as the desktop wallpaper:

Hakuna Matata message on the desktop

Contents of the note:

```
Your Files Have Been Locked With keygroup777 Ransomware
you have to pay Bitcoin for Unlock Process
you can send a little file (less than 1 or 2 mb) for Decryption t
Contact Us and Pay and get Decryption
Contact Our Email:******@yandex.ru
in Case of no reply from Email send message to my telegram id bel
Telegram ID:@[redacted]
Your ID:4062********
```

In early March 2024, we discovered a Key Group sample based on the Judge/NoCry ransomware (MD5: 56F5A95FFA6F89C24E0880C519A2AA50).

The NoCry variant encrypts files using AES-256-CBC and adds the `.Keygroup777tg` extension. The key used for encryption is generated based on the victim's system data and sent to a C2 server in plain text, allowing the files to be decrypted without the attackers' involvement.

It's worth noting that instead of the C2 server address, Key Group provided a link to the Telegram channel `hxxps://t[.]me/s/SBUkr`, to which the victim's data and the encryption key were added in the following format:

```
hxxps://t[.]me/s/SBUkr?[username]_[generated_id]=[generated_key]
```

The channel's theme is not related to ransomware and consists of political news. This scheme does not involve the attackers obtaining the data.

Indicating the C2 server in code

Function for sending requests to C2 server

Detonation of Judge/NoCry

A complete timeline of Key Group's use of various ransomware families is presented below.

Use of leaked Key Group builders

Delivery and infection

To deliver the Chaos and Xorist ransomware to the victim's computer, Key Group used multi-stage loaders.

We discovered an LNK file that was likely distributed via phishing emails. The LNK file contained an obfuscated PowerShell command that downloaded an SFX archive (self-extracting archive) from a remote resource:

Deobfuscated command:

Upon extraction, the SFX archive saved another loader to the system. It downloaded another SFX archive containing a sample of the Chaos ransomware (MD5: C910DA0BAA2E08CEFCE079D1F7CB3469), as well as a separate

loader that downloaded a sample of the Xorist ransomware (MD5: E0C744162654352F5E048B7339920A76).

The contents of the notes from the two ransomware variants were identical.

In October 2022, we discovered another loader that delivered a variant of Chaos (MD5: F93695564B97F03CC95CA242EDCFB5F8). The loader uses the .NET method `WebClient.DownloadData` to download the ransomware (MD5: D655E77841CF6DB3008DCD60C9C5EB18) from a GitHub repository:

```
hxxps://raw.githubusercontent[.]com/max444432/RMS2/main/dfff.exe
```

While studying this repository, we found the already familiar RuRansom wiper, the Hakuna Matata ransomware, as well as a sample of J-Ransomware/LoveYou and the NjRat remote access Trojan.

Persistence methods

Xorist

The first discovered sample of Key Group, the Xorist ransomware, established persistence in the system by changing file extension associations. When a file with the `.huis_bn` extension, which was added to encrypted files, was opened, the ransomware would launch:

```
HKLM\SOFTWARE\Classes\.huis_bn = "LGDAGXRNCRZHPLD"

HKLM\SOFTWARE\Classes\LGDAGXRNCRZHPLD\shell\open\command =
 "C:\Users\[redacted]\AppData\Local\Temp\fj6qD14qWC1unS2.exe"
```

The ransomware also added itself to startup:

```
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run
  "Alcmeter" = "C:\Users\[redacted]\AppData\Local\Temp\fj6qD14qWC
```

Chaos

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.

Subscribe

The Chaos ransomware (MD5: C910DA0BAA2E08CEFCE079D1F7CB3469) copied itself to `$user\$appdata\cmd.exe` and executed this file as a new process. The new process, in turn, created a new file in the startup folder: `$user\$appdata\Microsoft\Windows\Start Menu\Programs\Startup\cmd.url`, containing the following:

```
URL=file:///$user\$appdata\cmd.exe
```

Annabelle

The Annabelle ransomware added itself to the `Run` and `Winlogon` registry keys.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
  "UpdateBackup" = "$selfpath"

HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
  "UpdateBackup" = "$selfpath"

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
  "Shell" = "$selfpath"
```

UX-Cryptor

UX-Cryptor added itself to the following registry keys to maintain persistence in the system:

```
HKU\$usersid\Software\Microsoft\Windows NT\CurrentVersion\Winlog
  "Shell" = "$selfpath"

HKU\$usersid\Software\Microsoft\Windows\CurrentVersion\Run
  "WindowsInstaller" = "$selfpath -startup"
  "MSEdgeUpdateX" = "$selfpath"

HKU\$usersid\Software\Microsoft\Windows\CurrentVersion\RunOnce
  "System3264Wow" = "$selfpath --init"
  "OneDrive10293" = "$selfpath /setup"
  "WINDOWS" = "$selfpath --wininit"
```

Additionally, it added the following executable file names to startup:

```
HKU\$usersid\Software\Microsoft\Windows\CurrentVersion\Run
  "WIN32_1" ="AWindowsService.exe"
  "WIN32_2" = "taskhost.exe"
  "WIN32_3" = "windowsx-c.exe"
  "WIN32_4" = "System.exe"
  "WIN32_5" = "_default64.exe"
  "WIN32_6" = "native.exe"
  "WIN32_7" = "ux-cryptor.exe"
  "WIN32_8" = "crypt0rsx.exe"
```

Judge/NoCry

The NoCry sample also has the ability to add itself to the startup folder:

```
1 $user\$appdata\Microsoft\Windows\Start Menu\Programs\Startup\sPo9
```

Victims

Key Group primarily targets Russian-speaking users. The ransom notes were often written in Russian or included a translation into Russian.

Message from Key Group

About the attackers

The `.huis_bn` extension added to encrypted files in the early versions of Key Group samples, Xorist and Chaos, refers to a Russian-speaking closed group “huis”, known in the shadow community. The group primarily conducted spam raids on Telegram channels. We suspect that Key Group is a subsidiary project of the “huis” group. The group is currently inactive and, according to the latest Telegram post, has been rebranded.

Logo of the huis group (source: tgstat.com)

We also checked the GitHub repository from which the ransomware and wipers were downloaded. The account max444432 is subscribed to the account `hxxps://github[.]com/json1c`. Its description contains the following contact on Telegram: `hxxps://t[.]me/json1c`.

Accounts subscribed to max444432 on GitHub

Description of the json1c account on GitHub

The Telegram user Bloody-Lord Destroyer-Crew, also known as “bloody” in the shadow community, was the owner of the “huis” group.

Preview of the @json1c account on Telegram

In the latest versions of the ransomware, the ransom notes listed the Telegram account `@[redacted]` (DarkZeus) as a contact, who is one of the administrators of the Key Group channel:

IN THE SAME CATEGORY

Stealer here, stealer there, stealers everywhere!

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

Awaken Likho is awake: new techniques of an APT group

From 12 to 21: how we discovered connections between the Twelve and BlackJack groups

-=TWELVE=- is back

Preview of the account on Telegram

This is a closed Telegram channel. Previously, the group also had an open channel `@[redacted]`, which the attackers used to communicate with victims; however, it is no longer available. In that channel, the group published news about Key Group, updates from other channels of both technical and ideological nature, leaks from other Telegram sources, and announcements about spam raids.

Invitation link to join the closed Key Group channel

In the GitHub repository used by the attackers to distribute malware, we also found samples of `telegram-raid-botnet.exe` (Hakuna Matata) and NoCry, uploaded in February 2024. The name of the first sample resonates with the activities of the “huis” group.

Commits for uploading samples to the RMS2 repository

In one of the ransom notes (MD5: 7E1577B6E42D47B30AE597EEE720D3B1), the attackers asked "not to touch Nikita's channels, bloody and nacha", which again indicates a connection to "huis":

```
I am the owner of keygroup777 and I was enraged by the work of th
and I ask you not to touch Nikita's channels, bloody and nacha wi
time goes by, hello from Root)
and quote Durov, Everything is just beginning - knees will become
```

Takeaways

As we can see, Key Group, like many hacktivists, does not develop its own malware but actively uses leaked ransomware builders, and the primary C2 channel is a GitHub repository, which makes it easy to track their activities. It's also important to note that ransomware source code is increasingly becoming publicly available, and the number of groups using leaked builders or ransomware source code is on the rise. In the future, it is likely that there will be even more such groups.

Indicators of compromise

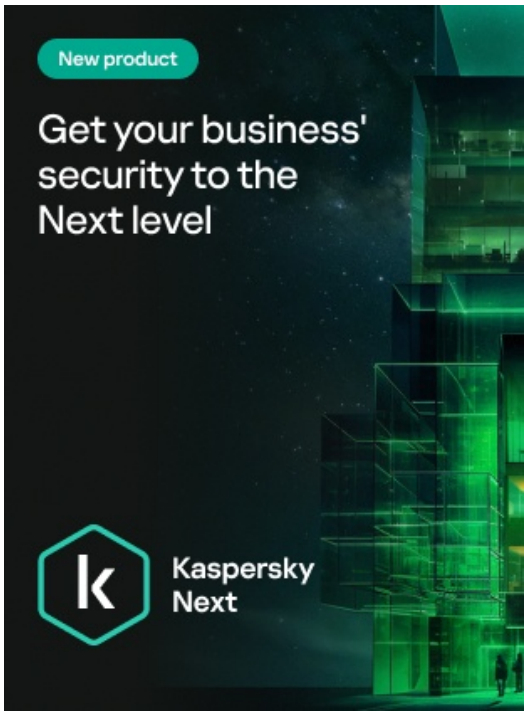
D2FFADEC5AA0A5CDD5E5CF1A7901EB29	Ransomware 1-st stage downloader
5AA991C89A6564A3C6351052E157F9D8	Ransomware 2-nd stage dropper (SFX archive) – RegAsm.exe
BC9B44D8E5EB1543A26C16C2D45F8AB7	Xorist ransomware – 1.exe
ACEA7E35F8878AEA046A7EB35D0B8330	Chaos ransomware – 2.exe
2737B1B3835242989F544A18D2DBAEFF	PowerShell LNK downloader
843F24AFDA0E1B375F00A00B39CF4A6E	Ransomware 1-st stage dropper (SFX archive)
636E1A7083439E77920C5C902DE8E2AE	Ransomware 2-nd stage downloader
1113BFBC7F3A62C87F1E090C57FA5D14	Ransomware 3-rd stage dropper (SFX archive)
C910DA0BAA2E08CEFCE079D1F7CB3469	Chaos ransomware – 1.exe
A0165523B0CB1A3AD28B995F100CC3C3	Xorist ransomware downloader – 2.exe
E0C744162654352F5E048B7339920A76	Xorist ransomware – RegAsm.exe
F93695564B97F03CC95CA242EDCFB5F8	Chaos ransomware downloader
D655E77841CF6DB3008DCD60C9C5EB18	Chaos ransomware – RegAsm.exe
BC9B44D8E5EB1543A26C16C2D45F8AB7	Xorist ransomware
CE9D5037EF8AB5C5677263E88E87464B	Xorist ransomware
A7ED00A3B0F827A3DCCC69D8908F5A22	Xorist ransomware
604FD6351A04B871DC77B6C7AD24FF3C	Chaos ransomware

C2E1048E1E5130E36AF297C73A83AFF6	Chaos ransomware
7E1577B6E42D47B30AE597EEE720D3B1	Chaos ransomware
D655E77841CF6DB3008DCD60C9C5EB18	Chaos ransomware
C910DA0BAA2E08CEFCE079D1F7CB3469	Chaos ransomware
FBD7E50091E64349827D1A62947CE042	Chaos ransomware
B404ACD8CFCE28DE0FCF5D2B0BE04989	Chaos ransomware
7237881AF3C17426FA262EA362C2D50F	Chaos ransomware
0889B78C02C338DF9394D913866E540C	Chaos ransomware
ACEA7E35F8878AEA046A7EB35D0B8330	Chaos ransomware
B1097F0A2B5B4B82E28CBD9953DD8B7C	Chaos ransomware
1FED852D312031974BF5EB988904F64E	RuRansom
6170BF1741D344C7D9B4384BF0771135	RuRansom
65CD0E68B4B5803064C6CA8BE9B05B89	RuRansom
3F224ADB6164F9A9C9E39E437FD0874C	RuRansom
291F9902534C323E2093D0FEE37B5187	RuRansom
EDAD568267A1D83403A8A55E557C8554	RuRansom
6780495DAD7EB372F1A660811F4894A6	UX-Cryptor
D2B80AC7CFCB075C5BDC637A75493E47	UX-Cryptor
44913214A6F04604E1B688524D9C419B	UX-Cryptor
DA09FCF140D3AAD0390FB7FAF7260EB5	Hakuna Matata ransomware
BA2108E9C3BF810F8B59E19C0D8DE310	Hakuna Matata ransomware

7249F2373BB6ADFC60DB971B4F7A1D20	Hakuna Matata ransomware
EB74803E3F3396E076517A8BE727AE0D	Hakuna Matata ransomware
63D8D813BC214B6F13F5EB3EE93B950A	Hakuna Matata ransomware
B3BF4F7CA0BB97F68CFE61136C8F26D1	Hakuna Matata ransomware
E46330807AFA8A023324E01F9B9C98BF	Hakuna Matata dropper
46F8DE68E5348E1042461629B0B634A2	Hakuna Matata ransomware
DA8419165BCC5014114B1D1934DB5DC0	Hakuna Matata ransomware
56F5A95FFA6F89C24E0880C519A2AA50	Judge/NoCry
09F95167104B8CCEECB7969CD5399E11	Judge/NoCry
05FD0124C42461EF553B4B17D18142F9	Annabelle
09CE91B4F137A4CBC1496D3791C6E75B	Slam ransomware

from repository hxxps://raw.githubusercontent[.]com/max444432/RMS2/main/:

75F46171E81D6C5C81929AE6E3996257	RuRansom – dlldata.exe ()
3BA80C2F430FAC5DEEC03788E5A438C3	J-Ransomware/LoveYou ransomware – l.exe
8EFCF0FA4EB05EFE76A3AE28FB193606	J-Ransomware/LoveYou ransomware – lLove.exe
46F8DE68E5348E1042461629B0B634A2	Hakuna Matata ransomware – telegram-raid-botnet.exe
C2EDCC9211872B82475CB0EE3ADFED5D	XWorm V2.2 – cheat.exe
A095507117B229ECBC53D5F3B5F35ADF	NjRat – Server.exe



404D831747E7713F2EA6D859B52CE9B3	NjRat – Plugin cmd.sfx.exe
5AA991C89A6564A3C6351052E157F9D8	SFX archive (Xorist + Chaos) – bater.exe

URLs

hxxp://fastxstreamz.herokuapp[.]com/913915/ndp462-kb3151800-x86-x64-allos-rus.scr?hash=AgADzh
hxxp://fastxstreamz.herokuapp[.]com/913034/setupdjprog-i0w0w04g8gww4ock.exe?hash=agadox
hxxp://fastxstreamz.herokuapp[.]com/912974/3.exe?hash=agadob
hxxps://raw.githubusercontent[.]com/max444432/RMS2/main/*
make-catherine.at.ply[.]gg – C2 XWorm V2.2

HACKTIVISTS MALWARE MALWARE DESCRIPTIONS MALWARE TECHNOLOGIES MBR MICROSOFT WINDOWS RAAS RANSOMWARE RAT RAT TROJAN TARGETED ATTACKS TELEGRAM WIPER

Key Group: another ransomware group using leaked builders

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

CRIMEWARE REPORTS

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

KASPERSKY

// LATEST WEBINARS

THREAT INTELLIGENCE AND IR

04 SEP 2024, 5:00PM 60 MIN

Inside the Dark Web: exploring the human side of cybercriminals

ANNA PAVLOVSKAYA

TECHNOLOGIES AND SERVICES

13 AUG 2024, 5:00PM 60 MIN

The Cybersecurity Buyer's Dilemma: Hype vs (True) Expertise

OLEG GOROBETS, ALEXANDER LISKIN

CYBERTHREAT TALKS

16 JUL 2024, 5:00PM 60 MIN

Cybersecurity's human factor – more than an unpatched vulnerability

OLEG GOROBETS

TRAININGS AND WORKSHOPS

09 JUL 2024, 4:00PM 60 MIN

Building and prioritizing detection engineering backlogs with MITRE ATT&CK

ANDREY TAMOYKIN

// REPORTS

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

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

BlindEagle flying high in Latin America

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

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.

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.

// 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

© 2024 AO Kaspersky Lab. All Rights Reserved.
Registered trademarks and service marks are the property of their respective owners.