

Wild Neutron – Economic espionage threat actor returns with new tricks

APT REPORTS

08 JUL 2015

10 minute read

Table of Contents

Older (2013) campaigns

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

Use necessary cookies only

Allow all cookies

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

Tweet

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

- Law firms

Table of Contents

Older (2013) campaigns

Known malicious IP's:

Known file names:

Named pipes:

Events & mutexes:

Page 1 of 13

- 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.iphonedevsdbk[.]com**, which is an iPhone developers forum.

The attackers injected a script into the forum that redirected visitors to another website

(**min.live**

day explo

fedoraf

http://er

additional

Other fo

Kaspers

- expa

- mygs

- forur

- emira

- forur

- comr

- ansa

In partic

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.



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 >

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

Back in 2010, a vulnerability was also discovered in the `http://erlang.org` website, which was a backdoor.

 Tweet

Some of
Microsof
issued s

The target
however
governm
state sp

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).

 **Tweet**

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

Cookiebot
by Usercentrics

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](#)

>

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

- 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

These features were removed from the newer backdoor versions that are used in recent attacks. Instead, backdoor developers started to focus on more sophisticated features and more different architectures.



In terms of Tools (RATs), the backdoor uses encryption to recover the attack.

According



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 >

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
0fa3657af06a8cc8ef14c445acd92c0f	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	RtlUpd.exe	253952

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

<

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.

The abus

Serial: 5
Thumbp

The drop
2015. It c
“app.clo



 [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



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](#) 

- Algeria
- United States

The victim
and in be
organiza
addition

Attribution

The targ
nation st
targets,
into finan



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

Tweet

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” ->



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 >

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

“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

[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.

Some of

- Use of
- Use of
- Use of
- Use of
- Use of
- Heavy
- Use of
- Simp
- Auxili

We cont

Kaspersky, ,
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

APT trends report Q2 2024

CloudSorcerer – A new APT targeting Russian government entities



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 >

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 *



Comments

ROLAND FINN

Posted on Jul 16, 2024

Please provide your comments in the context of the article. Do not use profanity, hate speech, or other inappropriate language. We reserve the right to remove any comments that violate these guidelines.

Group Profile Picture

Reply

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 >

- 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, 5:00PM60 MIN

Inside the Dark Web: exploring the human side of
- TECHNOLOGIES AND SERVICES

13 AUG 2024, 5:00PM60 MIN

The Cybersecurity Buyer's Dilemma: Hype vs (True)
- CYBERTHREAT TALKS

16 JUL 2024, 5:00PM60 MIN

Cybersecurity's human factor – more than an unpatched
- TRAININGS AND WORKSHOPS

09 JUL 2024, 4:00PM60 MIN

Building and prioritizing detection engineering backlogs

cybercriminals

ANNA PAVLOVSKAYA

Expertise

OLEG GOROBETS, ALEXANDER LISKIN

vulnerability

OLEG GOROBETS

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 NEWSLETTERS

The hottest

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 >

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