

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

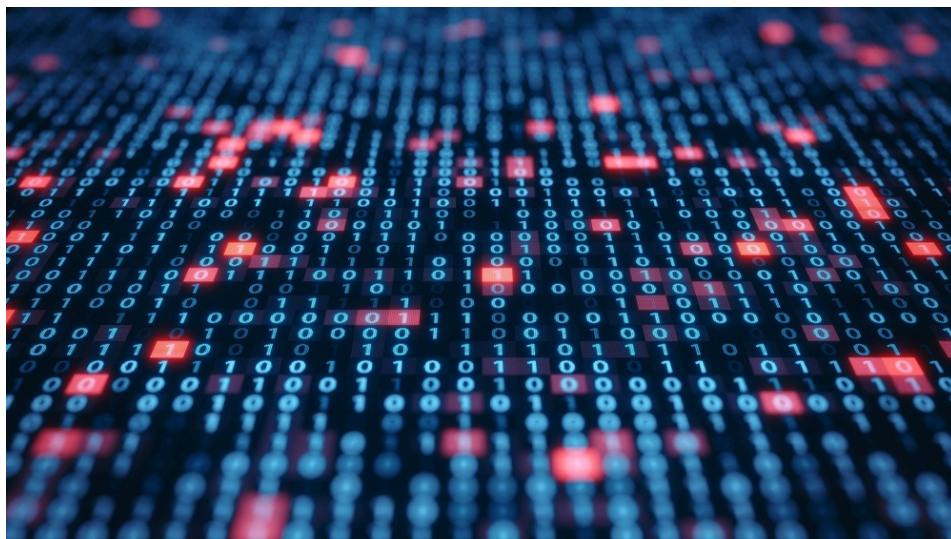


The Slingshot APT FAQ

APT REPORTS

09 MAR 2018

5 minute read



AUTHORS



ALEXEY SHULMIN

Expert

SERGEY YUNAKOVSKY

Expert

VASILY BERDNIKOV



Expert

ANDREY DOLGUSHEV

While analysing an incident which involved a suspected keylogger, we identified a malicious library able to interact with a virtual file system, which is usually the sign of an advanced [APT](#) actor. This turned out to be a malicious loader internally named 'Slingshot', part

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

of a new, and highly sophisticated attack platform that rivals Project Sauron and Regin in complexity.

The initial loader replaces the victim's legitimate Windows library 'scserv.dll' with a malicious one of exactly the same size. Not only that, it interacts with several other modules including a ring-0 loader, kernel-mode network sniffer, own base-independent packer, and virtual filesystem, among others.

While for most victims the infection vector for Slingshot remains unknown, we were able to find several cases where the attackers got access to Mikrotik routers and placed a component downloaded by Winbox Loader, a management suite for Mikrotik routers. In turn, this infected the administrator of the router.

We believe this cluster of activity started in at least 2012 and was still active at the time of this analysis (February 2018).

Why did you call the intruder Slingshot?

The name appears unencrypted in some of the malicious samples – it is the name of one of the threat actor's components, so we decided to extend it to the APT as a whole.

When was Slingshot active?

The earliest sample we found was compiled in 2012 and the threat was still active in February 2018.

How did the threat attack and infect its victims?

Slingshot is very complex and the developers behind it have clearly spent a great deal of time and money on its creation. Its infection vector is remarkable – and, to the best of our knowledge, unique.

We believe that most of the victims we observed appeared to have been initially infected through a Windows exploit or compromised Mikrotik routers.

fronts

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

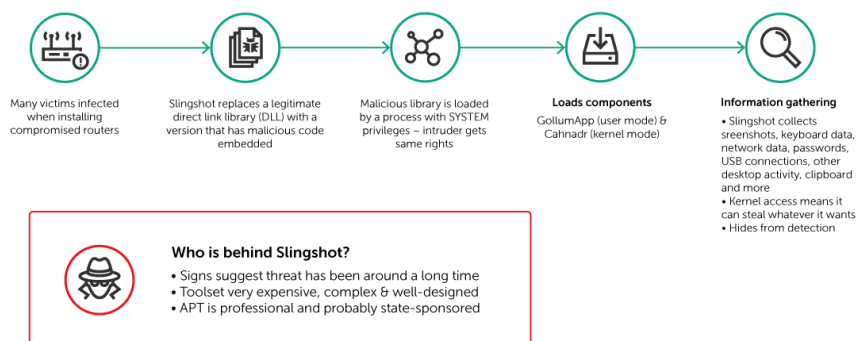
22 JUL 2020, 2:00PM

 **GReAT Ideas. Powered by SAS:**
threat hunting and new
techniques

DMITRY BESTUZHEV, COSTIN RAIU, PIERRE DELCHER,
BRIAN BARTHOLOMEW, BORIS LARIN,
ARIEL JUNGHEIT, FABIO ASSOLINI

Slingshot APT – how it attacks

Slingshot – an advanced, cyber-espionage threat actor targeting individuals and organizations in Africa and the Middle East, from at least 2012 until February 2018



KASPERSKY GREAT AMR

© 2018 AO Kaspersky Lab. All Rights Reserved

How exactly does infection happen?

The exact method used by Slingshot to exploit the routers in the first instance is not yet clear. When the target user runs Winbox Loader software (a utility used for Mikrotik router configuration), this connects to the router and downloads some DLLs (dynamic link libraries) from the router's file system.

One of them – ipv4.dll – has been placed by the APT with what is, in fact, a downloader for other malicious components. Winbox Loader downloads this ipv4.dll library to the target's computer, loads it in memory and runs it.

This DLL then connects to a hardcoded IP and port (in every cases we saw it was the router's IP address), downloads the other malicious components and runs them.

To run its code in kernel mode in the most recent versions of operating systems, that have Driver Signature Enforcement, Slingshot loads signed vulnerable drivers and runs its own code through their vulnerabilities. .

Following infection, Slingshot would load a number of modules onto the victim device, including two huge and powerful ones: Cahnadr, the kernel mode module, and GollumApp, a user mode module. The

FROM THE SAME AUTHORS

DarkUniverse – the mysterious APT framework #27

Platinum is back

New zero-day vulnerability CVE-2019-0859 in win32k.sys

The fourth horseman: CVE-2019-0797 vulnerability

DarkPulsar FAQ

two modules are connected and able to support each other in information gathering, persistence and data exfiltration.

The most sophisticated module is GollumApp. This contains nearly 1,500 user-code functions and provides most of the above described routines for persistence, file system control and C&C communications.

Canhadr, also known as NDriver, contains low-level routines for network, IO operations and so on. Its kernel-mode program is able to execute malicious code without crashing the whole file system or causing Blue Screen – a remarkable achievement. Written in pure C language, Canhadr/Ndriver provides full access to the hard drive and operating memory despite device security restrictions, and carries out integrity control of various system components to avoid debugging and security detection.

Are Mikrotik the only affected routers?

Some victims may have been infected through other routes. During our research we also found a component called KPWS that turned out to be another downloader for Slingshot components.

Did you inform the affected vendor?

Although the available intelligence is limited and we are not sure what kind of exploit was used to infect routers, we provided Mikrotik with all information available.

What can users of Mikrotik routers do to protect themselves?

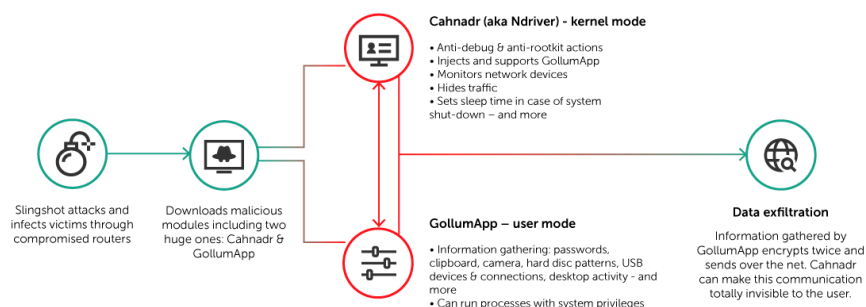
Users of Mikrotik routers should upgrade to the latest software version as soon as possible to ensure protection against known vulnerabilities. Further, Mikrotik Winbox no longer downloads anything from the router to the user's computer.

What are the advantages of achieving kernel mode?

It gives intruders complete control over the victim computer. In kernel mode malware can do everything. There are no restrictions, no limitations, and no protection for the user (or none that the malware can't easily bypass).

Slingshot APT – the main malicious modules

Slingshot – an advanced, cyber-espionage threat actor targeting individuals and organizations in Africa and the Middle East, from at least 2012 until February 2018



KASPERSKY GREAT AMR

© 2018 AO Kaspersky Lab. All Rights Reserved

What kind of information does Slingshot appear to be looking for?

Slingshot's main purpose seems to be cyber-espionage. Analysis suggests it collects screenshots, keyboard data, network data, passwords, USB connections, other desktop activity, clipboard and more. But with full access to the kernel part of the system, it can steal whatever it wants – credit card numbers, password hashes, social security account numbers – any type of data.

How did Slingshot avoid detection?

The threat actor combined a number of known approaches to protect it very effectively from detection: including encrypting all strings in its modules, calling system services directly in order to bypass security-product hooks, using a number of Anti-bug techniques, and more.

Further, it can shut down its components, but ensure they complete their tasks before closing. This process is triggered when there are

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.

signs of an imminent in-system event, such as a system shutdown, and is probably implemented to allow user-mode components of the malware to complete their tasks properly to avoid detection during any forensic research.

 [Subscribe](#)

You said that it disables disk defragmentation module in Windows OS. Why?

This APT uses its own encrypted file system and this can be located among others in an unused part of a hard drive. During defragmentation, the defrag tool relocates data on disk and this tool can write something to sectors where Slingshot keeps its file systems (because the operating system thinks these sectors are free). This will damage the encrypted file system. We suspect that Slingshot tries to disable defragmentation of these specific areas of the hard drive in order to prevent this from happening.

How does it exfiltrate data?

The malware exfiltrates data through standard networks channels, hiding the traffic being extracted by hooking legitimate call-backs, checking for Slingshot data packages and showing the user (and users' programs like sniffers and so on) clear traffic without exfiltrated data.

Does it use exploits to zero-day vulnerabilities? Any other exploits?

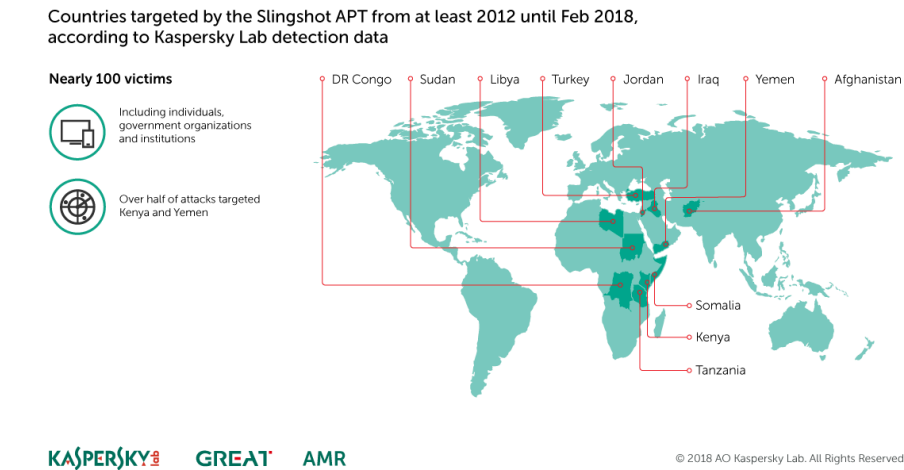
We haven't seen Slingshot exploit any zero-days, but that doesn't mean that it doesn't – that part of a story is still unclear for us. But it does exploit known vulnerabilities in drivers to pass executable code into kernel mode. These vulnerabilities include CVE-2007-5633; CVE-2010-1592, CVE-2009-0824.

What is the victim profile and target geography?

So far, researchers have seen around 100 victims of Slingshot and its related modules, located in Kenya, Yemen, Afghanistan, Libya,

Congo, Jordan, Turkey, Iraq, Sudan, Somalia and Tanzania. Most of the victims appear to be targeted individuals rather than organizations, but there are some government organizations and institutions. Kenya and the Yemen account for most of the victims observed to date.

Slingshot – global attack geography



IN THE SAME CATEGORY

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

What do we know about the group behind Slingshot?

The malicious samples investigated by the researchers were marked as ‘version 6.x’, which suggests the threat has existed for a considerable length of time. The development time, skill and cost involved in creating Slingshot’s complex toolset is likely to have been extremely high. Taken together, these clues suggest that the group behind Slingshot is likely to be highly organized and professional and probably state-sponsored.

Text clues in the code suggest it is English-speaking. Some of the techniques used by Slingshot, such as the exploitation of legitimate, yet vulnerable drivers has been seen before in other malware, such as White and Grey Lambert. However, accurate attribution is always hard, if not impossible to determine, and increasingly prone to manipulation and error.

Read more in our [technical paper](#).

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

- APT
- MALWARE DESCRIPTIONS
- VULNERABILITIES AND EXPLOITS

The Slingshot APT FAQ

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

Type your comment here

Name *

Email *

Comment

MICHAEL JORDAN
Posted on March 12, 2018. 12:11 pm

I know the Technicolor TC8717T Wireless Telephony DOCSIS 3.0 Modem, 4 Port Router which comes with ISP Xfinity, has been harnessed this attack. The malicious code has infected my personal network. I have logs and other detailed in-depth information gathered from my personal analysis. The ISP Xfinity (Comcast) would eventually confirm that my network had been compromised, but would not go as far as to agree to the nature of the attack and/or anything that would show incompetence on their end.

Reply

FKUCTARD5000
Posted on March 13, 2018. 3:41 pm

You expect your ISP to admit they have a large scale problem on their hands?
I think not.

Reply

ALEXEY SHULMIN

Posted on March 16, 2018. 11:09 am

Hi, Michael!

Interesting! Do you think you could share all collected information with us? We need it to continue our research. If yes, please contact me via Alexey[dot]Shulmin[at]kaspersky[dot]com

Thank you!

Reply

ALBERT STEIN

Posted on March 19, 2018. 10:13 am

That strange: The infection goes router->management app in computer and since the TC8717T has NO management app (is managed via WEB interface) I can't see how your network has been infected.

The vulnerability analysis clearly states that "When the target user runs Winbox Loader software (a utility used for Mikrotik router configuration), this connects to the router and downloads some DLLs (dynamic link libraries) from the router's file system."

Theres NO Winbox-equivalent app for the TC8717T, so this exploit DOES NOT applies to you. Maybe your network is compromised, but by other means. Please, be precise with your sayings.

Please note: I'm not affiliated in any way to Xfinity and/or Comcast. Feel free to answer since I've leaved my email in case of reply.

Reply



// LATEST POSTS

SAS

The Crypto Game of Lazarus APT: Investors

MALWARE DESCRIPTIONS

Grandoreiro, the global trojan with grandiose

CRIMEWARE REPORTS

Stealer here, stealer there, stealers

CRIMEWARE REPORTS

Analysis of the Crypt Ghouls group:

vs. Zero-days	goals	everywhere!	continuing the investigation into a series of attacks on Russia
BORIS LARIN, VASILY BERDNIKOV	GREAT	GREAT	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.

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

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

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