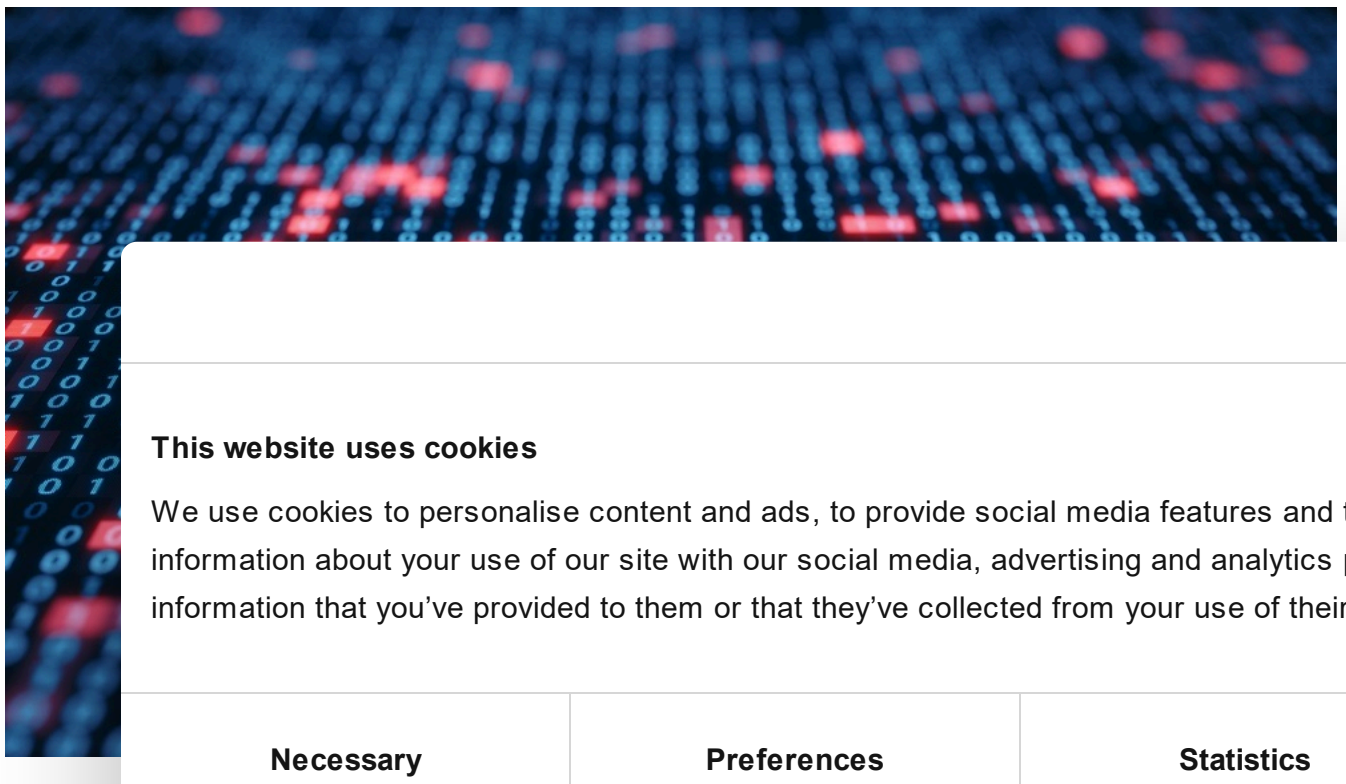
The Slingshot APT FAQ

APT REPORTS 09 MAR 2018 5 minute read



// AU

ALE

While an
library ab
actor. Th
highly sc

The initial loader replaces the victim´s legitimate Windows library 'scesrv.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.

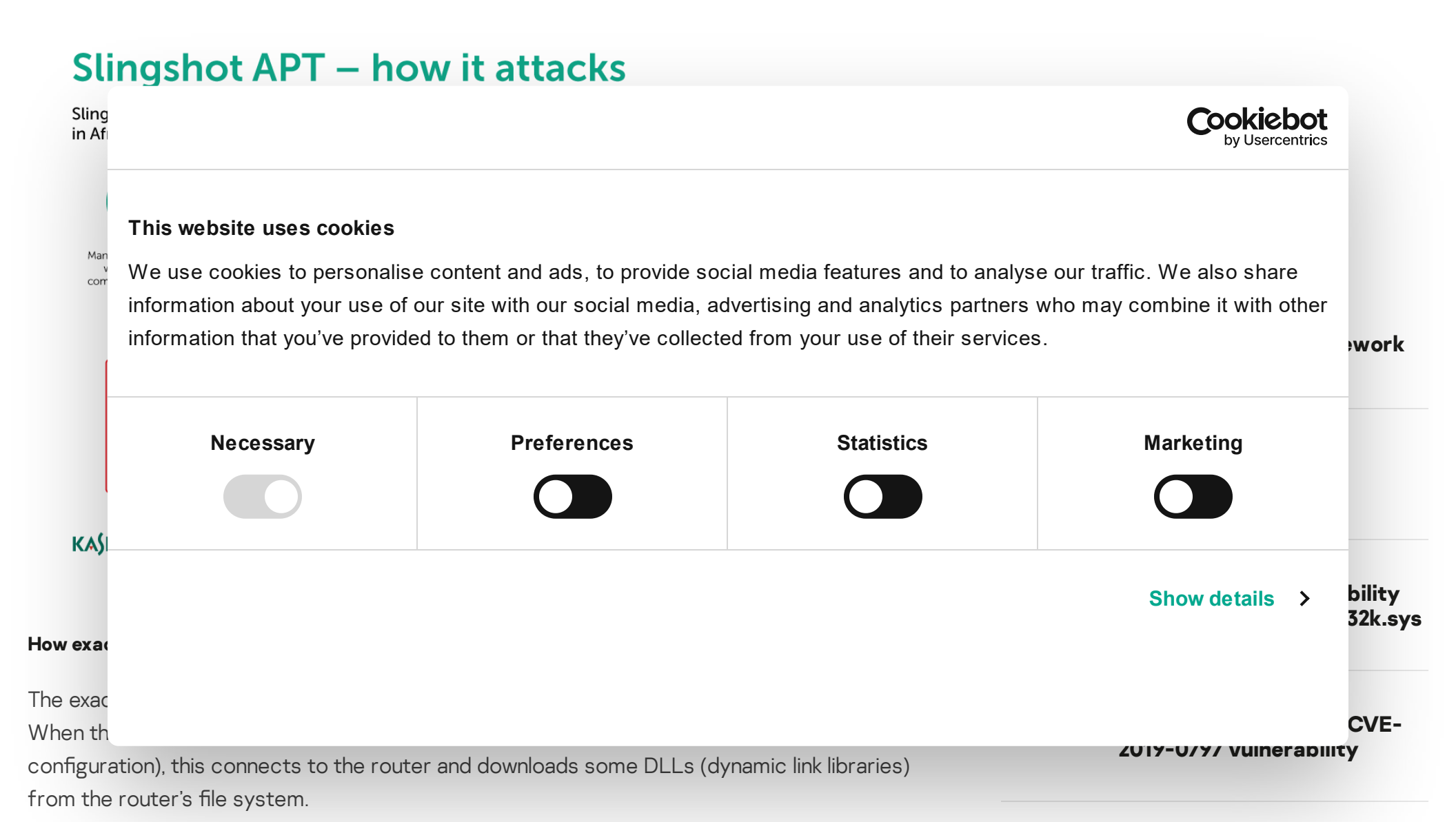
When was Slingshot active?

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.



The exact
When th
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 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?

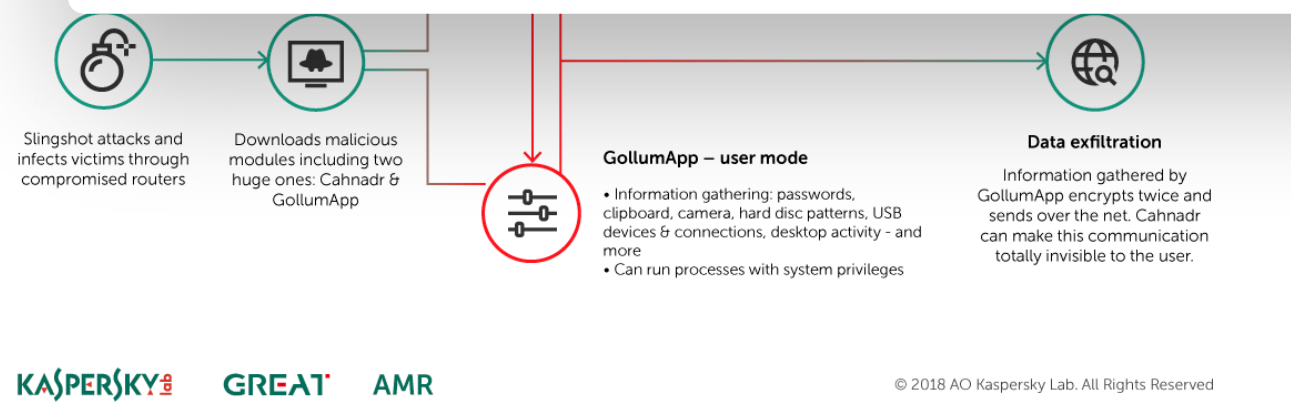
Although the available intelligence is limited and we are not sure what kind of exploit was used to infect routers, we provided Mikrotik with all information available.

What car

Users of
ensure p
anything

What are

It gives i
everythi
the malw



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 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.

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 extracte
the user

Does it u

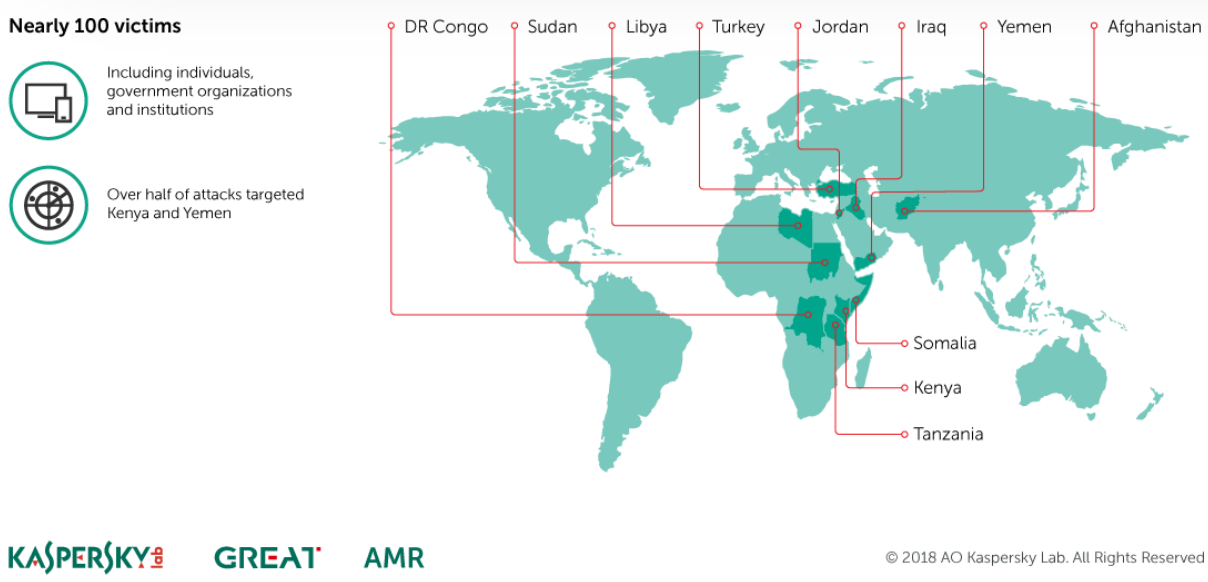
We have
part of a
executab
1592, CV

What is t

So far, r
in Kenya,
Most of
some go
victims c

Slingshot – global attack geography

Countries targeted by the Slingshot APT from at least 2012 until Feb 2018, according to Kaspersky Lab detection data



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

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.

APT | MALWARE DESCRIPTIONS | VULNERABILITIES AND EXPLOITS

CloudSorcerer – A new APT targeting Russian government entities

The Slingshot APT FAQ

Your email address will not be published.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

Type your comment here

Name *

Com

MICHAEL JC
Posted on Ma

I know th
comes w
personal
personal
compror
that wou

Reply

FKUC
Poste

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!

Interesing! 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 Cry… houls APT: Inv… es of

BORIS LARIN…

// LA…

THR… PS

04 SEP 20… 60 MIN

Inside th… the human side of cybercriminals

ANNA PAVLOVSKAYA

Dilemma: Hype vs (True) Expertise

OLEG GOROBETS, ALEXANDER LISKIN

more than an unpatched vulnerability

OLEG GOROBETS

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.

// SU
MAILS

The hott

cribe

kaspe

Industrial threats
Web threats
Vulnerabilities and exploits
All threats

Security technologies
Research
Publications
All categories

Encyclopedia
Threats descriptions
KSB 2023

Privacy Policy | License Agreement | Cookies