Okrum: Ke3chang group targets diplomatic missions

welivesecurity.com/2019/07/18/okrum-ke3chang-targets-diplomatic-missions/

July 18, 2019

Tracking the malicious activities of the elusive Ke3chang APT group, ESET researchers have discovered new versions of malware families linked to the group, and a previously unreported backdoor

Zuzana Hromcová
18 Jul 2019 - 11:30AM

Tracking the malicious activities of the elusive Ke3chang APT group, ESET researchers have discovered new versions of malware families linked to the group, and a previously unreported backdoor

In this blogpost, we will sum up the findings published in full in our white paper "Okrum and Ketrican: An overview of recent Ke3chang group activity".

The Ke3chang group, also known as APT15, is a threat group believed to be operating out of China. Its activities were traced back to 2010 in FireEye's 2013 report on operation Ke3chang – a cyberespionage campaign directed at diplomatic organizations in Europe.

We have been tracking the malicious activities related to this threat actor and discovered a previously undocumented malware family with strong links to the Ke3chang group – a backdoor we named Okrum. According to ESET telemetry, Okrum was first detected in December 2016, and targeted diplomatic missions in Slovakia, Belgium, Chile, Guatemala and Brazil throughout 2017.

Furthermore, from 2015 to 2019, we detected new versions of known malware families attributed to the Ke3chang group – BS2005 backdoors from operation Ke3chang and the RoyalDNS malware, reported by NCC Group in 2018.

Note: New versions of operation Ke3chang malware from 2015-2019 are detected by ESET systems as Win32/Ketrican and collectively referred to as Ketrican backdoors/samples, marked with the relevant year, across our white paper and this blogpost.

Okrum and Ketrican: An overview of recent Ke3chang group activity

Download Research Paper

Investigation timeline

2015: Ketrican

In 2015, we identified new suspicious activities in European countries. The group behind the attacks seemed to have a particular interest in Slovakia, where a big portion of the discovered malware samples was detected; Croatia, the Czech Republic and other countries were also affected.

Our technical analysis of the malware used in these attacks showed close ties to BS2005 backdoors from operation Ke3chang, and to a related TidePool malware family discovered by Palo Alto Networks in 2016 that targeted Indian embassies across the globe.

2016-2017: Okrum

The story continued in late 2016, when we discovered a new, previously unknown backdoor that we named Okrum. The malicious actors behind the Okrum malware were focused on the same targets in Slovakia that were previously targeted by Ketrican 2015 backdoors.

2017: Ketrican and RoyalDNS

We started connecting the dots when we discovered that the Okrum backdoor was used to drop a Ketrican backdoor, freshly compiled in 2017.

In 2017, the same entities that were affected by the Okrum malware (and by the 2015 Ketrican backdoors) again became targets of the malicious actors. This time, the attackers used new versions of the RoyalDNS malware and a Ketrican 2017 backdoor.

2018: Ketrican

In 2018, we discovered a new version of the Ketrican backdoor that featured some code improvements.

2019: Ketrican

The group continues to be active in 2019 – in March 2019, we detected a new Ketrican sample that has evolved from the 2018 Ketrican backdoor. It attacked the same targets as the backdoor from 2018.

This timeline of events shows that the attackers were focused on the same type of targets but were using different malicious toolsets to compromise them. In the process, they exposed Okrum, a formerly unknown project. Figure 1 shows ESET detections related to our investigation in the context of previously documented Ke3chang activity.

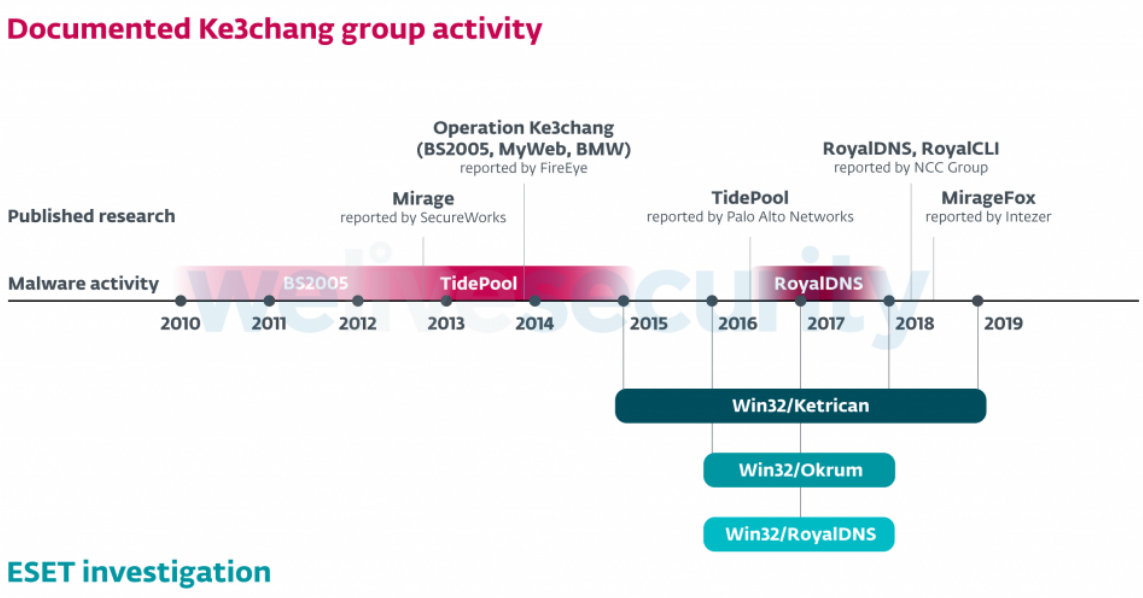

Figure 1. Timeline of previously documented Ke3chang group activity and ESET detections related to our investigation

Links to Ke3chang group

Our research has shown that the Ketrican, Okrum, and RoyalDNS backdoors detected by ESET after 2015 are linked to previously documented Ke3chang group activity, and to each other, in a number of ways. These are the most important connections:

- Ketrican backdoors from 2015, 2017, 2018 and 2019 have all evolved from malware used in Operation Ke3chang
- The RoyalDNS backdoor detected by ESET in 2017 is similar to the RoyalDNS backdoor used in previously reported attacks
- Okrum is linked to Ketrican backdoors in that it was used to drop a Ketrican backdoor compiled in 2017
- Okrum, Ketrican and RoyalDNS target the same type of organizations; some of the entities affected by Okrum were also targeted with one or more of Ketrican/RoyalDNS backdoors
- Okrum has a similar modus operandi as previously documented Ke3chang malware – it is equipped with a basic set of backdoor commands and relies on manually typing shell commands and executing external tools for most of its malicious activity

Okrum

Distribution and targets

According to our telemetry, Okrum was used to target diplomatic missions in Slovakia, Belgium, Chile, Guatemala, and Brazil, with the attackers showing a particular interest in Slovakia.

The operators of the malware tried to hide malicious traffic with its C&C server within regular network traffic by registering seemingly legitimate domain names. For example, the samples used against Slovak targets communicated with a domain name mimicking a Slovak map portal (support.slovakmaps[.]com). A similar masquerade was used in a sample detected in a Spanish speaking country in South America – the operators used a domain name that translates as “missions support” in Spanish (misiones.soportesisco[.]com).

How the Okrum malware was distributed to the targeted machines is a question that remains to be answered.

Technical details

The Okrum backdoor is a dynamic-link library that is installed and loaded by two earlier-stage components. During our investigation, the implementation of these two components was being changed frequently. Every few months, the authors actively changed implementation of the Okrum loader and installer components to avoid detection. By the time of publication, ESET systems have detected seven different versions of the loader component and two versions of the installer, although the functionality remained the same.

The payload of Okrum is hidden in a PNG file. When the file is viewed in an image viewer, a familiar image is displayed, as seen in Figure 2, but the Okrum loaders are able to locate an extra encrypted file that the user cannot see. This steganography technique is an attempt by the malicious actors to stay unnoticed and evade detection.

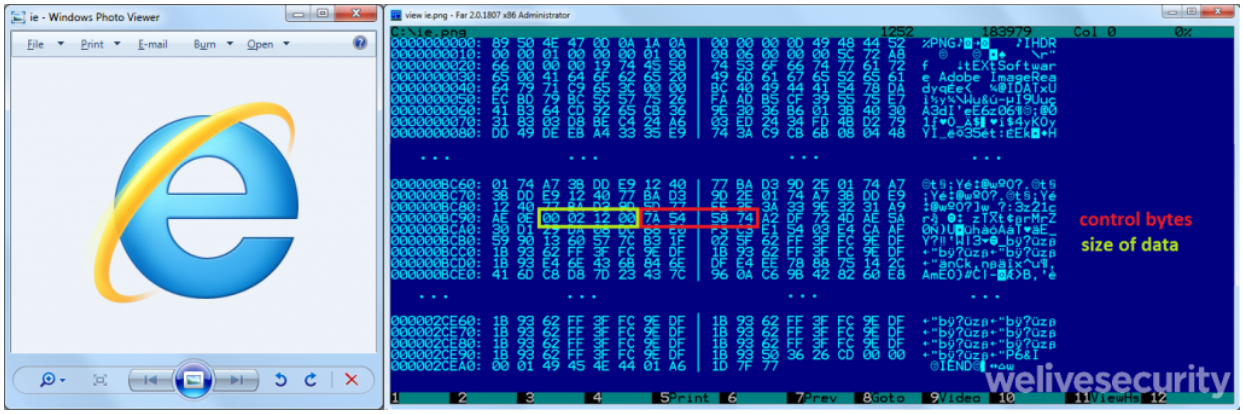

Figure 2. An innocuous-looking PNG image with an encrypted malicious DLL embedded inside

As for functionality, Okrum is only equipped with basic backdoor commands, such as downloading and uploading files, executing files and shell commands. Most of the malicious activity has to be performed by typing shell commands manually, or by executing other tools and software. This is a common practice of the Ke3chang group, which had also been pointed out previously in the Intezer and NCC Group reports monitoring Ke3chang group activity.

Indeed, we have detected various external tools being abused by Okrum, such as a keylogger, tools for dumping passwords, or enumerating network sessions. The Ketrican backdoors we detected from 2015 to 2019 used similar utilities. We can only guess why the Ke3chang actor uses this technique – maybe the combination of a simple backdoor and external tools fully accommodates their needs, while being easier to develop; but it may also be an attempt to evade behavioral detection.

The detection evasion techniques we observed in the Okrum malware include embedding the malicious payload within a legitimate PNG image, employing several anti-emulation and anti-sandbox tricks, as well as making frequent changes in implementation.

Conclusion

Our analysis of the links between previously documented Ke3chang malware and the newly discovered Okrum backdoor lets us claim with high confidence that Okrum is operated by the Ke3chang group. Having documented Ke3chang group activity from 2015 to 2019, we conclude that the group continues to be active and works on improving its code over time.

ESET detection names and other Indicators of Compromise for these campaigns can be found in the full white paper: "Okrum and Ketrican: An overview of recent Ke3chang group activity".

MITRE ATT&CK techniques

Tactic	ID	Name	Description
Execution	T1059	Command-Line Interface	Okrum's backdoor uses cmd.exe to execute arbitrary commands.
T1064	Scripting	The backdoor uses batch scripts to update itself to a newer version.	
T1035	Service Execution	The Stage 1 loader creates a new service named NtmsSvc to execute the payload.	
Persistence	T1050	New Service	To establish persistence, Okrum installs itself as a new service named NtmSsvc.
T1060	Registry Run Keys / Startup Folder	Okrum establishes persistence by creating a .lnk shortcut to itself in the Startup folder.	
T1053	Scheduled Task	The installer component tries to achieve persistence by creating a scheduled task.	

Tactic	ID	Name	Description
	T1023	Shortcut Modification	Okrum establishes persistence by creating a .lnk shortcut to itself in the Startup folder.
Privilege Escalation	T1134	Access Token Manipulation	Okrum can impersonate a logged on user's security context using a call to the ImpersonateLoggedOnUser API.
Defense Evasion	T1140	Deobfuscate/Decode Files or Information	The Stage 1 loader decrypts the backdoor code, embedded within the loader or within a legitimate PNG file. A custom XOR cipher or RC4 is used for decryption.
	T1107	File Deletion	Okrum’s backdoor deletes files after they have been successfully uploaded to C&C servers.
	T1158	Hidden Files and Directories	Before exfiltration, Okrum’s backdoor uses hidden files to store logs and outputs from backdoor commands.
	T1066	Indicator Removal from Tools	Okrum underwent regular technical improvements to evade antivirus detection.

Tactic	ID	Name	Description
	T1036	Masquerading	Okrum establishes persistence by adding a new service NtmsSvc with the display name Removable Storage in an attempt to masquerade as a legitimate Removable Storage Manager.
	T1027	Obfuscated Files or Information	Okrum's payload is encrypted and embedded within the Stage 1 loader, or within a legitimate PNG file.
	T1497	Virtualization/Sandbox Evasion	The Stage 1 loader performs several checks on the victim's machine to avoid being emulated or executed in a sandbox.
Credential Access	T1003	Credential Dumping	Okrum was seen using MimikatzLite and modified Quarks PwDump to perform credential dumping.
Discovery	T1083	File and Directory Discovery	Okrum was seen using DriveLetterView to enumerate drive information.
	T1082	System Information Discovery	Okrum collects computer name, locale information, and information about the OS and architecture.

Tactic	ID	Name	Description
	T1016	System Network Configuration Discovery	Okrum collects network information, including host IP address, DNS and proxy information.
	T1049	System Network Connections Discovery	Okrum used NetSess to discover NetBIOS sessions.
	T1033	System Owner/User Discovery	Okrum collects the victim user name.
	T1124	System Time Discovery	Okrum can obtain the date and time of the compromised system.
Collection	T1056	Input Capture	Okrum was seen using a keylogger tool to capture keystrokes.
Exfiltration	T1002	Data Compressed	Okrum was seen using a RAR archiver tool to compress data.
	T1022	Data Encrypted	Okrum uses AES encryption and base64 encoding of files before exfiltration.
	T1041	Exfiltration Over Command and Control Channel	Data exfiltration is done using the already opened channel with the C&C server.
Command And Control	T1043	Commonly Used Port	Okrum uses port 80 for C&C.
	T1090	Connection Proxy	Okrum identifies a proxy server if it exists and uses it to make HTTP requests.

Tactic	ID	Name	Description
	T1132	Data Encoding	The communication with the C&C server is base64 encoded.
	T1001	Data Obfuscation	The communication with the C&C server is hidden in the Cookie and Set-Cookie headers of HTTP requests.
	T1071	Standard Application Layer Protocol	Okrum uses HTTP for communication with its C&C.
	T1032	Standard Cryptographic Protocol	Okrum uses AES to encrypt network traffic. The key can be hardcoded or negotiated with the C&C server in the registration phase.

18 Jul 2019 - 11:30AM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion