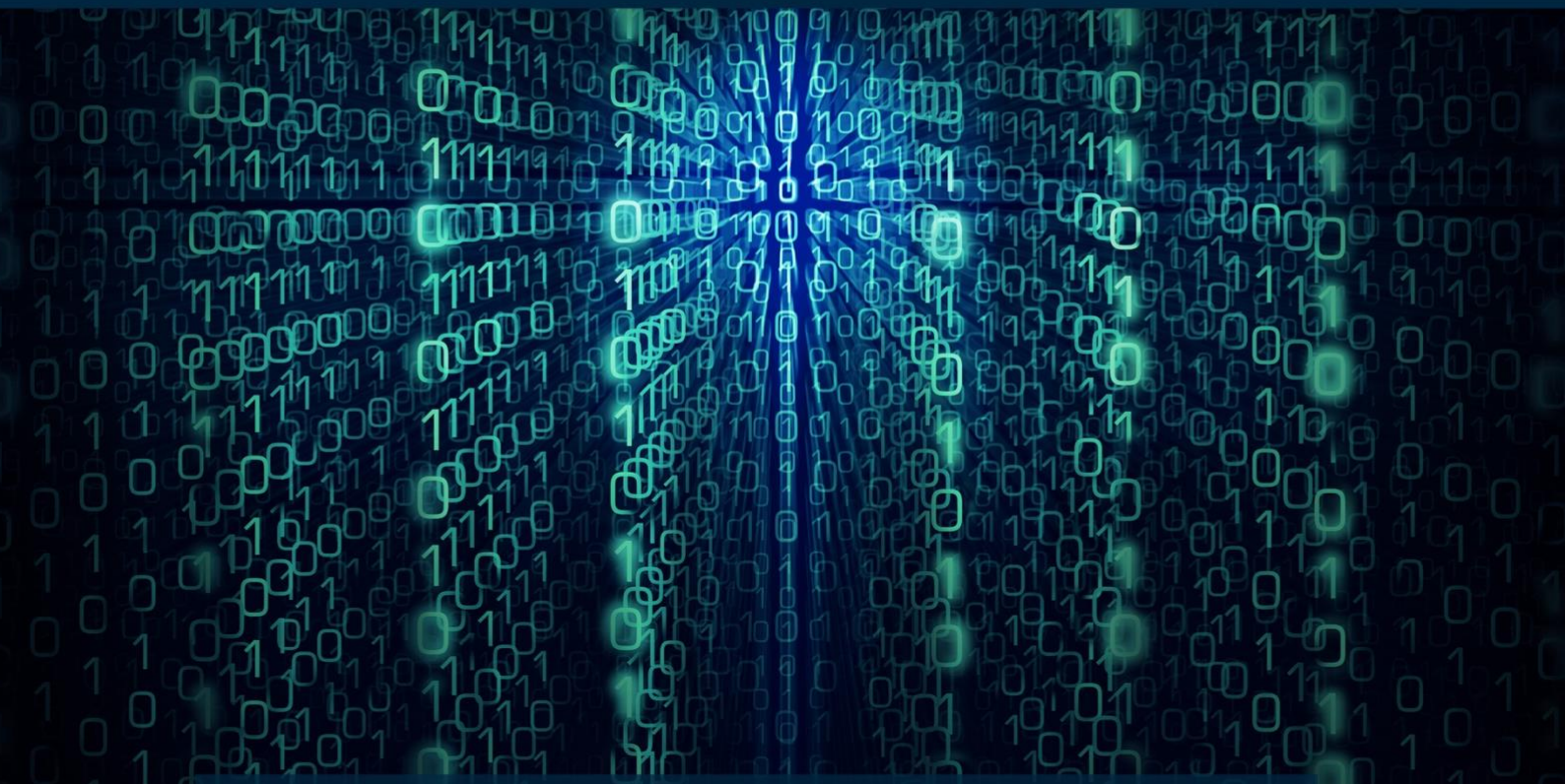
Cyberint



RUSSIAN BACKED TURLA RESURFACES WITH A SOPHISTICATED RAT

Kazuar Remote Access Trojan Revealed

By Cyberint | 2019

Table of Contents

Executive Summary

CyberInt Research has recently detected a potential resurgence of Kazuar, a Remote Access Trojan (RAT), previously linked to Turla, an advanced persistent threat (APT) group widely attributed as Russian-state sponsored.

Based on malware samples observed, components of this RAT appear to have been discovered in Argentina, Canada, the Czech Republic, Germany and Malaysia, potentially indicating that Turla is conducting operations in these regions.

Believed active since 2004, Turla, also known as Krypton, Snake, Uroburos and Venomous Bear, is a cyber-espionage group that has previously targeted government institutions, the military-industrial complex (MIC), education and research organisations as well as the pharmaceutical industry. These attacks typically employ similar tactics, techniques and procedures (TTP) and often commence with a watering hole (supply-chain compromise) or spear-phishing campaign followed by the deployment of bespoke malware that communicates with a tiered command and control (C2) infrastructure.

After the initial compromise, additional tools are uploaded to the victim and are used to move laterally within the target organisation. Additionally, modular malware has allowed Turla to tailor their attacks against specific targets.

Of the various malware threats used by Turla over the last decade and a half, the Kazuar RAT was analysed by Palo Alto's Unit 42 in 2017[1] and is believed to have a code lineage that could be traced back to at least 2005, consistent with early indications of the group. This RAT, built using Microsoft .NET Framework, targets Windows-based systems although analysis of the code has also identified 'Unix' command references and therefore potentially indicates that the RAT may also target *nix platforms such as Apple MacOS or Linux.

Utilising common protocols for communications, previously observed C2 infrastructure appears to be hosted on compromised websites, a common tactic used to complicate take-down activity.

This analysis reveals the new strain of Kazuar RAT linked to Russian nexus nation state threat Actor Turla.

[1] https://unit42.paloaltonetworks.com/unit42-kazuar-multiplatform-espionage-backdoor-api-access/

Kazaur RAT

INITIALISATION

Upon execution, Kazaur first gathers information about the victim system and itself in addition to ensuring that only one instance of the RAT is running through the creation of a unique 'mutual exclusion object' (mutex).

Subsequently, a folder and file structure is created, using an encoded process that generates hexadecimal-looking names, in '%LOCALAPPDATA%'. This structure contains the RAT's configuration, commands, plugins and logs in addition to the output of any successful task.

Additionally, the RAT has four execution paths, based on the environment or arguments provided when started, and these determine how the malware will function:

- When executed with an 'install' command-line argument, or starting within a non-interactive environment, the RAT is installed as a Service;
- When executed on Windows without command-line arguments, a dynamic-link library (DLL) is dropped and injected into the 'explorer.exe' process (Figure 1) to launch the RAT within a legitimate process' memory;
- When executed with a 'single' command-line argument, or starting on a MacOS or Linux system, Windows-specific functionality is limited.

```
LoadLibraryW (lpLibFileName="C:\\Users\\<USERNAME>\\AppData\\Local\\<ENCODED_PATH>\\<ENCODED_FILENAME>.dll") returned 0x62480000
GetModuleFileNameA (in: hModule=0x0, lpFilename=0x29e12c, nSize=0x104 | out: lpFilename="C:\\Users\\<USERNAME>\\Desktop\\<KAZUAR_RAT>.exe"
                                                                            (normalized: "c:\\users\\<USERNAME>\\desktop\\<KAZUAR_RAT>.exe")) returned 0x25
PathFindFileNameA (pszPath="C:\\Users\\<USERNAME>\\Desktop\\<KAZUAR_RAT>.exe") returned="<KAZUAR_RAT>.exe"
lstrcmpiA (lpString1="<KAZUAR_RAT>.exe", lpString2="explorer.exe") returned 1
CoTaskMemAlloc (cb=0xa) returned 0x21f3840
GetProcAddress (hModule=0x62480000, lpProcName="HookProc") returned 0x624830f4
CoTaskMemFree (pv=0x21f3840)
SetWindowsHookExA (idHook=4, lpfn=0x624830f4, hmod=0x62480000, dwThreadId=0x60c) returned 0x60193
```

Figure 1 – Process injection of DLL file '%LOCALAPPDATA%\[a-f0-9]{32}\[a-f0-9]{32}.dll' (Encoded path/filename)

The DLL files identified in this recent resurgence of Kazuar are those that would be dropped in the case of execution, without command-line arguments, on a Windows-based systems.

PERSISTENCE

Kazuar attempts to gain persistence on Windows using registry keys added to the 'HKEY_CURRENT_USER' hive:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\load
- HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell

Additionally, a shortcut to the malicious executable is added to the Windows 'Startup' folder, typically located in '%APPDATA% \Microsoft\Windows\Start Menu\Programs\Startup'.

COMMAND AND CONTROL (C2)

Kazuar's C2 infrastructure allows those behind the campaign to interact with the RAT which, based on commands observed, includes the following functionality:

- Information gathering;
- File system interaction (find, copy, move and delete);
- File upload and download;
- Remote command execution;
- Screen and webcam image capture;
- Process interaction (list and kill);
- RAT management (logs, sleep, upgrade, C2 configuration and persistence);
- Plugin management (installation and removal of additional functionality);

The initial beacon to the C2 is sent from the compromised system as a HTTP GET request that contains an 'AuthToken' cookie value that uniquely identifies the victim. Subsequent responses sent from the C2 to the victim are in the form of XML 'tasks', corresponding to the features available within the RAT, which are then executed.

Additionally, the RAT can be instructed to listen for inbound HTTP requests containing tasks, effectively reversing the communication channel, and could potentially allow the threat actor to configure a particular victim system as a staging point for data exfiltration from others.

New Campaign

Recent samples of the Kazuar DLL file, dropped when the RAT is executed without command-line arguments on Windows-based systems, were first observed during the last week of January 2019:

SHA-256	Country	Date Observed
05176162c0ee6686c3e904ff2ecd6c1cf60be6748b37f0039da44f40d83fdf35	CA	2019-01-31
115a28656df83393eeef49e3bada3f1f779941d61867813ca7496eaf07858101	CA	2019-01-28
1cf1b34d77b877505a61b598aa2a93bd8a1bac70bea7492154e310ade1c7076d	DE	2019-01-28
2ad4fbe8ca3cd82f8e37ff7dbcf07c925321defc52e80117f49613b1b8209479	DE	2019-01-28
9c661cf8fcb8be0ee7ce7833770ef3a758cf0fb5d931f49670b0a9fe56bf687c	AR	2019-01-28

Pivoting on these samples, such as identifying files based on similarity and function, identified a further three samples, one detected in two countries, also first observed during the last week of January 2019:

SHA-256	Country	Date Observed
26010b29d08075c94943a21cd73189524743be739e4fa5019ace5e12d6219d5c	DE	2019-01-28
4fb50173ea192ef5aba04779114ae3616175232229b4437b4f179451b5501797	MY	2019-01-29
cf0c37d865ed0aea7d7cc8678990068f7b0e2c2b5684d386f6a6460775763159	CZ	2019-01-27
	UA	2019-01-31

In addition to providing an indication of potential target regions, including Argentina, Canada, the Czech Republic, Germany and Malaysia, the identification of these samples within a few days of each other appears to suggest a resurgence or renewal of potential Turla Kazuar activity.

MISSING LINK

Whilst the above identified DLL files were linked based on similarity, the associated Kazuar RAT executable initially remained elusive. Pivots on strings present within these malicious DLL samples identified that all shared the string '**tcHcI<L**', potentially suggesting that they were generated by the same process, and subsequently this string was found in Kazuar RAT executables.

The most recent Kazuar RAT executable, found through the string pivot, appears to have been identified in the Czech Republic and was observed as using the filenames 'Agent.exe' and 'dbgsview.exe'.

SHA-256	Country	Date Observed
44cc7f6c2b664f15b499c7d07c78c110861d2cc82787ddaad28a5af8efc3daac	CZ	2019-01-27

The use of these filenames, in addition to file version information, may be an attempt to masquerade as the Microsoft Windows Sysinternals 'Debug Output Viewer' tool, legitimately named 'dbgview.exe'.

Furthermore, this sample was observed as attempting to communicate with 'www.northviewcanada.com', a seemingly legitimate Canadian website (Figure 2). This behaviour would be consistent with Turla's preference for using compromised websites to host their C2 infrastructure to thwart take-down activity initiated by the cyber security community or law enforcement agencies.

Figure 2 – C2 hosted on a seemingly legitimate website

LEGACY SAMPLES

Based on the consistent string pivot, the following legacy Kazuar RAT executables were identified and, when combined with dates that the DLL files were observed, provide an indication of periods when Turla were active:

SHA-256	Country	Date Observed
2d8151dabf891cf743e67c6f9765ee79884d024b10d265119873b0967a09b20f	ES	2018-03-21
b51105c56d1bf8f98b7e924aa5caded8322d037745a128781fa0bc23841d1e70	IT	2016-10-10
	KR	2016-10-17
cd4c2e85213c96f79ddda564242efec3b970eded8c59f1f6f4d9a420eb8f1858	IT	2016-10-04
	KR	2016-10-17

In addition to the following legacy DLL files used by Kazuar RAT for the Windows Explorer process injection:

SHA-256	Country	Date Observed
1e72f465d9fe490eed2fddb9275aac3be0e94b25a3aa480d2b5e2032462acc2a	US	2018-04-26
49e0356272b9f8a30ec24a6e271f94e11668d7a48704bb9aed64f61b4b9b343c	US	2018-04-28
508e65769a57882549ed4831138579d1b70146e679836035b06fe3f5ba0a73ab	US	2018-04-26
	RU	2018-04-27
6b5d9fca6f49a044fd94c816e258bf50b1e90305d7dab2e0480349e80ed2a0fa	GB	2018-03-09
	MY	2018-03-11
743b3347dc86b4a4aa6510648076eeca9eec0ff23c1294b3931263c990bcb5e6	US	2018-04-08
	RU	2018-04-09
	RU	2018-05-05
	CN	2018-11-07
890d750cd90cfba284981db3c8bb5b525ebfc2af4d223c48ad67b1b7463b1829	US	2018-04-28
c20323170b19903527097ca3f9378e3f904efd243f112df3d56e87a55054fd73	US	2018-04-18
	IS	2018-04-19
f7de721a276135d08dcc12ede3cc1dd1c1484c90d74a6e44bb4a1e2669e5caa6	US	2018-04-15
	ES	2018-04-16
fe60f90cdcfa4ec82c02d1e179ecd35f4d17bef1e7a68161fbb8b8c3cf928361	UA	2018-01-21

Furthermore, legacy C2 domains and URLs, again utilising seemingly compromised websites, were identified:

- 2d8151dabf891cf743e67c6f9765ee79884d024b10d265119873b0967a09b20f
  - www.weauthenticate.co.uk
  - jaireve.co
- b51105c56d1bf8f98b7e924aa5caded8322d037745a128781fa0bc23841d1e70
  - hxxp://www.**gallen.fi**/wp-content/gallery/
  - hxxp://**gaismustudija.lv**/wp-includes/pomo/kontakti.php
- cd4c2e85213c96f79ddda564242efec3b970eded8c59f1f6f4d9a420eb8f1858
  - hxxp://**hcdh-tunisie.org**/wp-includes/SimplePie/gzencode.php

Notably, the two Kazuar RAT executable samples first observed in 2016, along with their associated C2 domains/URLs, are detailed in Palo Alto Unit 42's research[2] from May 2017.

[2] https://unit42.paloaltonetworks.com/unit42-kazuar-multiplatform-espionage-backdoor-api-access/

Indicators of Compromise (IOC)

RECENT IOC

DLL Files (SHA-256)

05176162c0ee6686c3e904ff2ecd6c1cf60be6748b37f0039da44f40d83fdf35

115a28656df83393eeef49e3bada3f1f779941d61867813ca7496eaf07858101

1cf1b34d77b877505a61b598aa2a93bd8a1bac70bea7492154e310ade1c7076d

26010b29d08075c94943a21cd73189524743be739e4fa5019ace5e12d6219d5c

2ad4fbe8ca3cd82f8e37ff7dbcf07c925321defc52e80117f49613b1b8209479

4fb50173ea192ef5aba04779114ae3616175232229b4437b4f179451b5501797

9c661cf8fcb8be0ee7ce7833770ef3a758cf0fb5d931f49670b0a9fe56bf687c

cf0c37d865ed0aea7d7cc8678990068f7b0e2c2b5684d386f6a6460775763159

Executable Files (SHA-256)

Agent.exe/dbgsview.exe: 44cc7f6c2b664f15b499c7d07c78c110861d2cc82787ddaad28a5af8efc3daac

C2 Domains (Compromised)

northviewcanada.com

LEGACY IOC

DLL Files (SHA-256)

1e72f465d9fe490eed2fddb9275aac3be0e94b25a3aa480d2b5e2032462acc2a

49e0356272b9f8a30ec24a6e271f94e11668d7a48704bb9aed64f61b4b9b343c

508e65769a57882549ed4831138579d1b70146e679836035b06fe3f5ba0a73ab

6b5d9fca6f49a044fd94c816e258bf50b1e90305d7dab2e0480349e80ed2a0fa

743b3347dc86b4a4aa6510648076eeca9eec0ff23c1294b3931263c990bcb5e6

890d750cd90cfba284981db3c8bb5b525ebfc2af4d223c48ad67b1b7463b1829

c20323170b19903527097ca3f9378e3f904efd243f112df3d56e87a55054fd73

f7de721a276135d08dcc12ede3cc1dd1c1484c90d74a6e44bb4a1e2669e5caa6

fe60f90cdcfa4ec82c02d1e179ecd35f4d17bef1e7a68161fbb8b8c3cf928361

Executable Files (SHA-256)

2d8151dabf891cf743e67c6f9765ee79884d024b10d265119873b0967a09b20f

b51105c56d1bf8f98b7e924aa5caded8322d037745a128781fa0bc23841d1e70

cd4c2e85213c96f79ddda564242efec3b970eded8c59f1f6f4d9a420eb8f1858

C2 Domains/URLs (Compromised)

hxxp://gaismustudija.lv/wp-includes/pomo/kontakti.php

hxxp://hcdh-tunisie.org/wp-includes/SimplePie/gzencode.php

hxxp://www.gallen.fi/wp-content/gallery/

jaireve.co

www.weauthenticate.co.uk

KAZUAR RAT FILE SYSTEM ARTEFACTS

Configuration files and the DLL used for process injection:

%LOCALAPPDATA%\[a-f0-9]{32}\[a-f0-9]{32}

%LOCALAPPDATA%\[a-f0-9]{32}\[a-f0-9]{32}.dll

KAZUAR RAT PERSISTENCE ARTEFACTS

Registry keys, used for persistence may be created in the following locations:

HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run

HKCU\Software\Microsoft\Windows\CurrentVersion\Run

HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce

HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\load

HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell

Additionally, files may be created in the Windows Startup folder:

%APPDATA% \Microsoft\Windows\Start Menu\Programs\Startup

United Kingdom
Tel: +442035141515
25 Old Broad Street | EC2N 1HN | London | United Kingdom

USA
Tel: +1-646-568-7813
214W 29th Street, Suite 06A-104 | New York, NY 10001 | USA

Israel
Tel:+972-3-7286777 Fax:+972-3-7286777
Ha-Mefalsim 17 St | 4951447 | Kiriat Arie Petah Tikva | Israel

Singapore
Tel: +65-3163-5760
10 Anson Road | #33-04A International Plaza 079903 | Singapore

sales@cyberint.com