# Examining the Activities of the Turla APT Group

By Srivathsa Sharma ( words)

Published: 2023-09-22 · Archived: 2026-04-05 23:05:28 UTC

APT & Targeted Attacks

We examine the campaigns of the cyberespionage group known as Turla over the years, with a special focus on the key MITRE techniques and the corresponding IDs associated with the threat actor group.

By: Srivathsa Sharma Sep 22, 2023 Read time: 8 min (2043 words)

Save to Folio

---

In this blog entry, we examine the campaigns of the cyberespionage group known as Turlanews article over the years, with a special focus on the key MITRE techniques and the corresponding IDs associated with the threat actor group.

**An introduction to Turla**

Regarded as a highly sophisticated advanced persistent threat (APT) group, the Russian-based Turla has been suspected to be operational since at least 2004.

Turla's group names are infamously titled after its top-class rootkits such as Snake, Venomous Bear, WhiteBear, Uroburos, Group 88, and Waterbug, all known for targeting government entities, intelligence agencies, as well as the military, educational, research, and pharmaceutical industries around the world. Like other APT groups, Turla possesses its own specifically-designed, complex tools. However, it is the threat actor's satellite-based command-and-control (C&C) mechanism that it uses in the latter stages of an attack, coupled with its ability to fly under the radar, that makes Turla stand out from its contemporaries.

## Unravelling Turla's activities

Although Turla has been known to be active in the wild for several years now, its infection vector had been a question mark. Research conducted in 2014 indicated a sophisticated multi-stage attack using Epic (a malware family used by Turla), with the campaign being dubbed as Epic Turla. The attacks, which exploited the vulnerabilities CVE-2013-5065 and CVE-2013-3346, employed spear-phishing emails that used Adobe PDF exploits and watering-hole techniques that used Java exploits (CVE-2012-1723)

The major highlight of this campaign was Turla's use of more complex backdoors like Carbon/Cobra, with the group sometimes using both backdoors as a failover.


open on a new tab

Figure 1. The MITRE ATT&CK techniques used in the August 2014 campaigns

**Tactics and Techniques:**

- TA0001 (Initial Access)
- T1189 (Drive-by Compromise)
- T1566 (Phishing)
- TA0002 (Execution)
- T1204.002 (User Execution: Malicious File)

While the previous Turla campaigns were designed to target Windows-based machines, the campaign in August 2014 was the first instance where Turla targeted the Linux operating system. Dubbed as Penguin Turla, the group used a Linux Turla module with a C/C++ executable statically linked against multiple libraries, greatly increasing its file size for this campaign.

A group of threat actors named Waterbug (alleged to be a state-sponsored group) used variants of Trojan.Turla and Trojan.Wipbot to exploit a zero-day vulnerability, specifically the Windows Kernel *NDProxy.sys* local privilege escalation vulnerability CVE-2013-5065. A research entry suggested that the attackers used specially crafted emails with malicious attachments and a set of compromised websites to deliver malicious payloads.

In 2017, ESET published a research entry on a sophisticated variant of the Turla malware, a second-stage backdoor known as Carbon. A Carbon attack initially involves the victim either receiving a spear-phishing email or visiting a compromised website, also known as a watering hole.

This is then followed by the installation of a first-stage backdoor such as Tavdig or Skipper. The second-stage backdoor Carbon is then installed on key systems after renaissance activities are completed. The Carbon framework consists of a dropper to install its configuration file, a component to communicate with the C&C

server, an orchestrator to handle tasks and move them laterally over the network, and a loader to execute the orchestrator.

In May 2017, a new backdoor trojan by the name Kazuar was linked to the Turla group. Written using the Microsoft .NET Framework, Kazuar contains highly functional command sets that are capable of remotely loading additional plug-ins.

Kazuar gathers system and malware file name information and creates a mutex to ensure that only one instance of the malware executes on the system at a time. It then adds an LNK file to the Windows startup folder.

Majority of the commands set in Kazuar share similar attributes with other backdoor Trojans. For example, the *tasklist* command uses a Windows Management Instrumentation (WMI) query to obtain running process from Windows while the *info* command is used to gather information about opened windows. Meanwhile, Kazuar's *cmd* command will run commands using *cmd.exe* for Windows systems and */bin/bash* for Unix systems. These commands strongly suggests that Kazuar was built to be a cross-platform malware targeting both Windows and Unix systems.

Research conducted in early 2021 revealed several similarities between the Sunburst and Kazuar backdoors.

**Tactics and Techniques:**

- TA0002 (Execution)
- T1047 (Windows Management Instrumentation)
- TA0003 (Persistence)
- T1547.009 (Boot or Logon Autostart Execution: Shortcut Modification)
- TA0007 (Discovery)
- T1010 (Application Window Discovery)

In August, Turla unveiled a new second-stage backdoor written in C++ known as Gazer, which relied on watering-hole attacks and spear-phishing campaigns for more precise targeting of victims.

Aside from being stealthier, Gazer was found to have plenty of similarities with the previously used second-stage backdoors such as Carbon and Kazuar. The defining characteristic of this campaign was the insertion of "video-game-relate" sentences throughout the code. Turla encrypts Gazer's C&C server using its own library for 3DES and RSA.

**Tactics and Techniques:**

- TA0011 (Command and Control)
- T1573 (Encrypted Channel)

An intelligence reportnews article from 2018 suggested that Turla used new malicious tools known as Neuron and Nautilus in conjunction with the Snake rootkit to target Windows machines, focusing on mail and web servers in particular. Turla made use of existing Snake victims to scan for ASPX shell, with the commands being passed using encrypted HTTP cookie values. The entry also mentioned that Turla used ASPX shells to gain a foothold into the target system to deploy additional tools.

Turla targeted the foreign offices of European governments via a backdoor, with the intention of accessing highly sensitive information. The campaign targeted Microsoft Outlook and The Bat! (a popular mail client primarily used in Eastern Europe) by forwarding all outgoing emails to the attackers. The backdoor used email messages to exfiltrate data, employing specially crafted PDF documents. It also used email messages as a transport layer for its C&C server.

OilRig is an Iran-linked APT group that usually targets government agencies and organizations in the Middle East. Previous research suggests that the Turla group compromised a target using OilRig's infrastructure. The campaign saw the use of a heavily modified, custom variant of the Mimikatz toolnews- cybercrime-and-digital-threats, plus a  new set of tools involving several new backdoors. In the later stages of the campaign, Turla group used a different remote procedure call (RPC) backdoor, which included code from the publicly available PowerShell Runner tool to execute PowerShell scripts (without using *powershell.exe*).

In March 2020, security researchers observed Turla targeted multiple Armenian websites using watering-hole attacks. These websites were implanted with malicious JavaScript code, although the access methods used in attack are unknown.

The compromised webpage then delivered the second-stage malicious JavaScript code to fingerprint victim browser and trick them into installing a malicious flash installer. Turla then used NetFlash (a .NET downloader) and PyFlash for its second-stage malware.

| Tactic | ID |
|---|---|
| Initial Access | T1189 |
| Execution | T1204 |
| Persistence | T1053 |
| Discovery | T1016 |
| | T1057 |
| | T1082 |
| Command and Control | T1071 |
| | T1573 |
| | T1571 |
| Exfiltration | T1041 |



open on a new tab

Figure 4. The MITRE ATT&CK techniques used in the March 2020 campaigns

**Tactics and Techniques:**

- TA0001 (Initial Access)
- T1189 (Drive-by Compromise)

- TA0002 (Execution)
- T1204 (User Execution)
- T0003 (Persistence)
- T1053 (Scheduled Task/Job)
- T0007 (Discovery)
- T1016 (System Network Configuration Discovery)
- T1057 (Process Discovery)
- T1082 (System Information Discovery)
- TA0011 (Command and Control)
- T1071 (Application Layer Protocol)
- T1573 (Encrypted Channel)
- T1571 (Non-Standard Port)
- TA0010 (Exfiltration)
- T1041 (Exfiltration Over C2 Channel)

ComRAT v4, also known as Agent.BTZ, is a remote access trojan (RAT) used by Turla and developed using C++ and employing a virtual FAT16 file system that is often used to exfiltrate sensitive documents. It is deployed using existing access methods, such as the PowerStallion PowerShell backdoor. Furthermore, it uses HTTP and emails as C&C channels.

**Tactics and Techniques:**

- TA0002 (Execution)
- T1059 (Command and Scripting Interpreter)
- T0003 (Persistence)
- T1053 (Scheduled Task/Job)
- TA0005 (Defense Evasion)
- T1055 (Process Injection)
- T1112 (Modify Registry)
- T1027 (Obfuscated Files or Information)
- TA0007 (Discovery)
- T1069 (Permission Groups Discovery)
- T1033 (System Owner/User Discovery)
- T1082 (System Information Discovery)
- T1083 (File and Directory Discovery)
- T1087 (Account Discovery)
- T1120 (Peripheral Device Discovery)
- T1135 (Network Share Discovery)
- T1016 (System Network Configuration Discovery)
- TA0009 (Collection)
- T1213 (Data from Information Repositories)
- TA0011 (Command and Control)
- T1573 (Encrypted Channel)

- T1071 (Application Layer Protocol)
- T1102 (Web Service)
- TA0010 (Exfiltration)
- T1048 (Exfiltration Over Alternative Protocol)

In December 2020, a previously undocumented backdoor and document stealer named Crutch was attributed to the Turla group. Apparently, older versions of Crutch included a backdoor that communicated with a hard-coded Dropbox account using the official HTTP API.

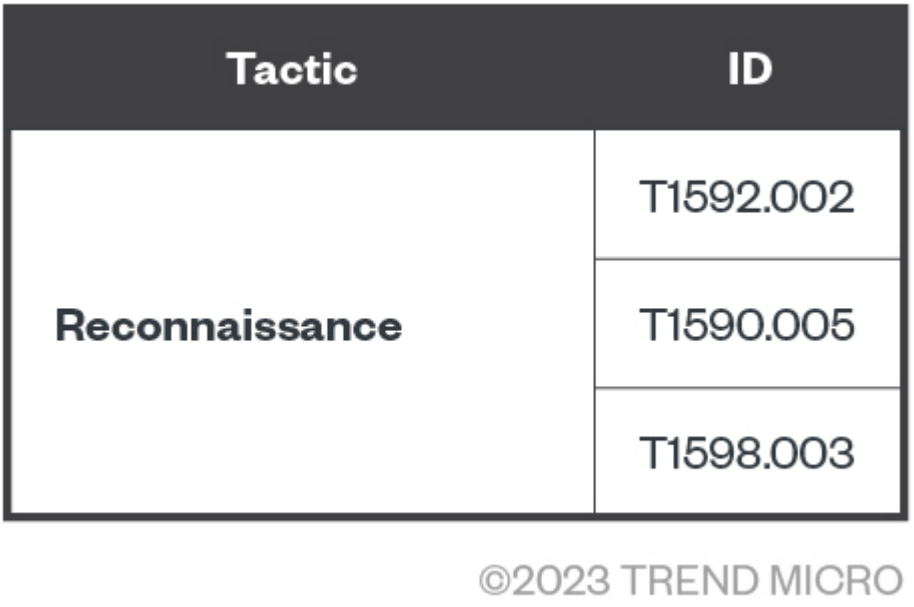
It had the ability to execute commands related to the reading and writing of files, executing additional processes, and setting persistence via DLL hijacking on Google Chrome, Mozilla Firefox, or Microsoft OneDrive. One major feature of Crutch v4 is that it can automatically upload the files found on local and removable drives to Dropbox storage by using the Windows version of the Wget utility (unlike the previous versions that relied on the backdoor commands).

**Tactics and Techniques:**

- TA0001 (Initial Access)
- T1078.003 (Valid Accounts: Local Accounts)
- TA0003 (Persistence)
- T1053.005 (Scheduled Task/Job: Scheduled Task)
- T1574.001 (Hijack Execution Flow: DLL Search Order Hijacking)
- TA0005 (Defense Evasion)
- T1036.004 (Masquerading: Masquerade Task or Service)
- TA0007 (Discovery)
- T1120 (Peripheral Device Discovery)
- TA0009 (Collection)
- T1025 (Data from Removable Media)
- T1074.001 (Data Staged: Local Data Staging)
- T1119 (Automated Collection)
- 1560.001 (Archive Collected Data: Archive via Utility)
- TA0011 (Command and Control)
- T1008 (Fallback Channels)
- T1071.001 (Application Layer Protocol: Web Protocols)
- T1102.002 (Web Service: Bidirectional Communication)
- **TA0010 (Exfiltration)**
- T1020 (Automated Exfiltration)
- T1041 (Exfiltration Over C2 Channel)
- T1567.002 (Exfiltration Over Web Service: Exfiltration to Cloud Storage)

The new Turla backdoor known as TinyTurla was likely used as a failover option to maintain access to the system even when the primary malware is removed. The backdoor is installed using a batch file and comes in the form of a service DLL called *w64time.dll* that tries to impersonate the legitimate *w32time.dll* file on Windows systems.

Turla's May 2022 campaign was used for the sole purpose of reconnaissance and did not involve any use of malicious code. Security researchers discovered a document that performed requests via HTTP to its own controlled server, with the purpose of capturing the version and type of Microsoft Word application used by the victim. The information can later be used to craft a specific exploit based on the Microsoft Word version.




open on a new tab

Figure 7. The MITRE ATT&CK techniques used in the May 2022 reconnaissance campaign

**Tactics and Techniques:**

- TA0043 (Reconaissance)
- T1592.002 (Gather Victim Host Information: Software)
- T1590.005 (Gather Victim Network Information: IP Addresses)
- T1598.003 (Phishing for Information: Spearphishing Link)

A July 2023 announcement from the Computer Emergency Response Team of Ukraine (CERT-UA) revealed that Turla was using the Capibar malware and Kazuar backdoor for espionage attacks on Ukrainian defensive assets. In this campaign, Capibar was used for intelligence gathering while Kazuar performed credential theft. This attack targeted diplomatic and military organizations by leveraging phishing attacks.

| Tactic | ID |
| --- | --- |
| Defense Evasion | T1027 |
| Execution | T1059 |
| | T1053 |
| Command and Control | T1105 |
| Exfiltration | T1567 |
| Persistence | T1546 |



open on a new tab

Figure 8. The MITRE ATT&CK techniques used in the July 2023 Capibar/Kazuar attacks

**Tactics and Techniques:**

- TA0005 (Defense Evasion)
- T1027 (Obfuscated Files or Information)
- TA0002 (Execution)
- T1059 (Command and Scripting Interpreter)
- TA0011 (Command and Control)
- T1053 (Scheduled Task/Job)
- T1105 (Ingress Tool Transfer)
- TA0010 (Exfiltration)
- T1567 (Exfiltration Over Web Service)
- TA0003 (Persistence)
- T1546 (Event Triggered Execution)
-

## Conclusion

The Turla group is a persistent adversary with a long history of activities. Their origins, tactics, and targets all indicate a well-funded operation with highly skilled operatives. Turla has continuously developed its tools and techniques over years and will likely keep on refining them.

The threat posed by groups such as Turla underscores the importance for organizations and governments to remain vigilant by staying informed, sharing intelligence, and implementing security measures that can allow both groups and individuals to better protect themselves against these kinds of threat actors.

## Indicators of Compromise

The indicators of compromise for the various Turla campaigns can be found here.

Tags

---