

Turla Cyber Campaign Targeting Pakistan's Critical Infrastructure

 socradar.io/turla-cyber-campaign-pakistans-critical-infrastructure/

January 7, 2025



[Home](#)
[Resources](#)

[Blog](#)

Jan 07, 2025

4 Mins Read

Among the most notorious cyber threat actors, the [Turla](#) group has garnered attention for its sophisticated and complex cyber attacks. Considered a state-sponsored actor, Turla has targeted governments, military institutions, and critical infrastructure across various regions. In its latest campaign, the group has focused its attention on Pakistan's [critical infrastructure](#).



“Turla Cyber Campaign Targeting Pakistan’s Critical Infrastructure” illustrated by DALL-E

These attacks pose significant threats not only to Pakistan but also to regional security and the global cyber threat landscape.

Campaign Details

Turla’s new campaign targeting Pakistan focuses on energy, telecommunications, and government networks. The group has employed methods like phishing and malware deployment to gain access to its targets.

By exploiting vulnerabilities such as [CVE-2022-38028](#), Turla has demonstrated advanced capabilities.

Techniques and Tools Used

Turla employs sophisticated techniques to maintain persistence and avoid detection within targeted systems. Key strategies include **DLL hijacking**, which allows them to remain undetected, and multi-layered encryption for secure communications. They frequently use periodic connections to **C2 servers** (Command and Control) and integrate malware into system startup points. The malware used in this campaign is tailored to exfiltrate sensitive data and disrupt target systems.

Espionage Tactics and Strategic Infrastructure Use

In late 2024, Microsoft reported that a threat group they track as **Secret Blizzard**, which overlaps with Turla, had compromised the infrastructure of **Storm-0156**, a Pakistan-based hacker group. By using Storm-0156's backdoors and tools, Secret Blizzard (Turla) could target entities like the Afghan government and the Indian Army. This method of leveraging third-party infrastructure allowed Turla to obfuscate its operations, complicating attribution efforts, and enhance its espionage capabilities.

This incident highlights the increasing complexity of cyber threats, where adversaries exploit each other's infrastructure to achieve strategic objectives. It underscores the importance of robust cybersecurity measures and vigilant monitoring to detect and mitigate such sophisticated attacks.

For organizations aiming to defend against advanced threats, SOCRadar's **Threat Hunting** module offers crucial insights. This module enables in-depth analysis of adversarial tactics and techniques, helping organizations detect potential compromises early and respond effectively to sophisticated cyber espionage campaigns like this one.

The screenshot displays the SOCRadar platform interface. On the left is a sidebar menu with various security modules. The main content area shows a campaign page for 'Turla Cyber Campaign: Targeting Pakistan's Critical Infrastructure'. The page includes a title, a brief description, and a detailed analysis section. A diagram illustrates the relationship between Secret Blizzard and Storm-0156. On the right, there is a world map showing observed countries and a history timeline of events.

SOCRadar Campaigns

Search...

Go back

Turla Cyber Campaign: Targeting Pakistan's Critical Infrastructure

TurlaAPT | RussianHackers | EspionageTactics | ShadowwareNetwork

The Russian-linked APT group Turla has been identified leveraging Pakistani infrastructure to conduct cyber-espionage operations. By hijacking servers and tools used by Pakistani hackers, Turla has masked its activities while targeting high-value entities for intelligence gathering.

DETAILS | IOC | APT GROUPS | **SUBSCRIBE** | **+**

ANALYSIS | MITIGATION | REMEDIATION | NOTES

Frequent reader: part 1: Secret Blizzard compromising Storm-0156 infrastructure for espionage

In December 2024, Microsoft reported that Secret Blizzard, a Russian state-sponsored threat actor, compromised the infrastructure of Storm-0156, a Pakistan-based hacking group, to conduct espionage operations. This tactic allowed Secret Blizzard to mask their activities and target entities such as the Afghan government and the Indian Army. By leveraging existing backdoors and tools from Storm-0156, Secret Blizzard effectively obscured their operations, complicating attribution efforts and enhancing their espionage capabilities.

Observed Countries

History Timeline

- 17:12 - DECEMBER 17, 2024
New IOC's Added
Total 36 IOC's added.
- 17:12 - DECEMBER 17, 2024
New Apt Groups Added
New APT Groups added.
- 17:12 - DECEMBER 17, 2024
Created!
New Campaign created.
- 03:12 - DECEMBER 04, 2024
Publish
Microsoft publishes a comprehensive blog detailing Secret Blizzard's tactics.

Turla Cyber Campaign Targeting Pakistan's Critical Infrastructure (SOCRadAr platform, Campaigns page)

To gain deeper insights into the tactics and techniques employed by advanced threat actors like Turla, explore **SOCRadar LABS' Campaigns** page. Here, you can find detailed reports on various cyber espionage operations, track ongoing trends, and access actionable intelligence to enhance your organization's defense strategies.

Analysis of Indicators of Compromise (IOCs)

The campaign's Indicators of Compromise (IOCs) include various IP addresses, domain names, and malware components. Notable IOCs include:

IP Addresses:

- 130.185.119[.]198
- 94.177.198[.]94
- 162.213.195[.]129

Domains:

- connectotels[.]net
- hostelhotels[.]net
- pentestlab[.]blog

These IOCs indicate the use of multiple Command and Control (C2) servers to facilitate communication between malware and the attackers. This infrastructure enables the attackers to maintain the campaign's longevity.

Mitigation and Remediation


The tables below outline the key techniques used by threat actors and provide recommended mitigation and remediation actions to protect your systems and data against such techniques.

ID	Technique	Recommended Mitigation
T1189	Drive-by Compromise	Use browser sandboxes and modern security features to prevent drive-by exploitation.
T1105	Ingress Tool Transfer	Detect malicious content through network monitoring and behavioral analytics.
T1036	Masquerading	Prevent masquerading with antivirus tools and file signature checks.
T1566	Phishing	Educate users and implement email authentication mechanisms.

ID	Technique	Recommended Remediation
T1059	Command and Scripting Interpreter	Monitor and block suspicious commands, modules, or functionalities.
T1102	Web Service	Enforce secure traffic policies using web proxies to detect unsafe data flow.

SOCRadar's **Cyber Threat Intelligence** platform is critical in mitigating complex cyber campaigns. Its advanced modules provide proactive tracking of Indicators of Compromise (IOCs), in-depth threat actor analysis, and targeted threat reporting.

Notably, the **Advanced Dark Web Monitoring** and **Threat Hunting** modules are highly effective in identifying and responding to emerging threats. For more detailed insights and other cybersecurity strategies, explore our platform.



**Every second,
a dark web threat
makes a move**

Act before them

Start Dark Web Monitoring Trial

© 2025 [SOC Radar](#). All rights reserved.



PROTECTION OF PERSONAL DATA COOKIE POLICY FOR THE INTERNET SITE

Protecting your personal data is one of the core principles of our organization, SOCRadar, which operates the internet site (www.socradar.com). This Cookie Usage Policy (“Policy”) explains the types of cookies used and the conditions under which they are used to all website visitors and users.

Cookies are small text files stored on your computer or mobile device by the websites you visit.

Cookies are commonly used to provide you with a personalized experience while using a website, enhance the services offered, and improve your overall browsing experience, contributing to ease of use while navigating a website. If you prefer not to use cookies, you

can delete or block them through your browser settings. However, please be aware that this may affect your usage of our website. Unless you change your cookie settings in your browser, we will assume that you accept the use of cookies on this site.

1. WHAT KIND OF DATA IS PROCESSED IN COOKIES?

Cookies on websites collect data related to your browsing and usage preferences on the device you use to visit the site, depending on their type. This data includes information about the pages you access, the services and products you explore, your preferred language choice, and other preferences.

2. WHAT ARE COOKIES AND WHAT ARE THEIR PURPOSES?

Cookies are small text files stored on your device or web server by the websites you visit through your browsers. These small text files, containing your preferred language and other settings, help us remember your preferences on your next visit and assist us in making improvements to our services to enhance your experience on the site. This way, you can have a better and more personalized user experience on your next visit.

The main purposes of using cookies on our Internet Site are as follows:

- Improve the functionality and performance of the website to enhance the services provided to you,
- Enhance and introduce new features to the Internet Site and customize the provided features based on your preferences,
- Ensure legal and commercial security for the Internet Site, yourself, and the Organization, and prevent fraudulent transactions through the Site,
- Fulfill legal and contractual obligations, including those arising from Law No. 5651 on the Regulation of Publications on the Internet and the Fight Against Crimes Committed Through These Publications, as well as the Regulation on the Procedures and Principles Regarding the Regulation of Publications on the Internet.

3. TYPES OF COOKIES USED ON OUR INTERNET SITE

3.1. Session Cookies

Session cookies ensure the smooth operation of the internet site during your visit. They are used for purposes such as ensuring the security and continuity of our sites and your visits. Session cookies are temporary cookies and are deleted when you close your browser; they are not permanent.

3.2. Persistent Cookies

These cookies are used to remember your preferences and are stored on your device through browsers. Persistent cookies remain stored on your device even after you close your browser or restart your computer. These cookies are stored in your browser's subfolders until

deleted from your browser's settings. Some types of persistent cookies can be used to provide personalized recommendations based on your usage purposes.

With persistent cookies, when you revisit our website with the same device, the website checks if a cookie created by our website exists on your device. If so, it is understood that you have visited the site before, and the content to be presented to you is determined accordingly, offering you a better service.

3.3. Mandatory/Technical Cookies

Mandatory cookies are essential for the proper functioning of the visited internet site. The purpose of these cookies is to provide necessary services by ensuring the operation of the site. For example, they allow access to secure sections of the internet site, use of its features, and navigation.

3.4. Analytical Cookies

These cookies gather information about how the website is used, the frequency and number of visits, and show how visitors navigate to the site. The purpose of using these cookies is to improve the operation of the site, increase its performance, and determine general trend directions. They do not contain data that can identify visitors. For example, they show the number of error messages displayed or the most visited pages.

3.5. Functional Cookies

Functional cookies remember the choices made by visitors within the site and recall them during the next visit. The purpose of these cookies is to provide ease of use to visitors. For example, they prevent the need to re-enter the user's password on each page visited by the site user.

3.6. Targeting/Advertising Cookies

They measure the effectiveness of advertisements shown to visitors and calculate how many times ads are displayed. The purpose of these cookies is to present personalized advertisements to visitors based on their interests.

Similarly, they determine the specific interests of visitors' navigation and present appropriate content. For example, they prevent the same advertisement from being shown again to the visitor in a short period.

4. HOW TO MANAGE COOKIE PREFERENCES?

To change your preferences regarding the use of cookies, block or delete cookies, you only need to change your browser settings.

Many browsers offer options to accept or reject cookies, only accept certain types of cookies, or receive notifications from the browser when a website requests to store cookies on your device.

Also, it is possible to delete previously saved cookies from your browser.

If you disable or reject cookies, you may need to manually adjust some preferences, and certain features and services on the website may not work properly as we will not be able to recognize and associate with your account. You can change your browser settings by clicking on the relevant link from the table below.

5. EFFECTIVE DATE OF THE INTERNET SITE PRIVACY POLICY

The Internet Site Privacy Policy is dated The effective date of the Policy will be updated if the entire Policy or specific sections are renewed. The Privacy Policy is published on the Organization's website (www.socradar.com) and made accessible to relevant individuals upon request.

SOCRadar

Address: 651 N Broad St, Suite 205 Middletown, DE 19709 USA

Phone: +1 (571) 249-4598

Email: [\[email protected\]](#)

Website: www.socradar.com