# TEAM46 (TAXOFF) EXPLOITS GOOGLE CHROME ZERO-DAY (CVE-2025-2783) IN HIGHLY TARGETED PHISHING CAMPAIGN

## Vairav Security News Report

**Date: June 17, 2025**

**Vairav Cyber Threat Intelligence Team**


## Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

## EXECUTIVE SUMMARY

The APT group **Team46**, also operating under the alias **TaxOff**, has launched a highly sophisticated phishing campaign leveraging **CVE-2025-2783**, a Google Chrome zero-day vulnerability that enables **sandbox escape**. The attack, uncovered by Positive Technologies Expert Security Center (PT ESC), employs advanced delivery and evasion mechanisms, including **multi-layered malware loaders**, decoy emails, and obfuscated PowerShell chains. Analysis of infrastructure and TTPs confirms that Team46 and TaxOff are the same threat group. The campaign has been active since at least **September 2024**, with targets across high-profile forums and digital services.

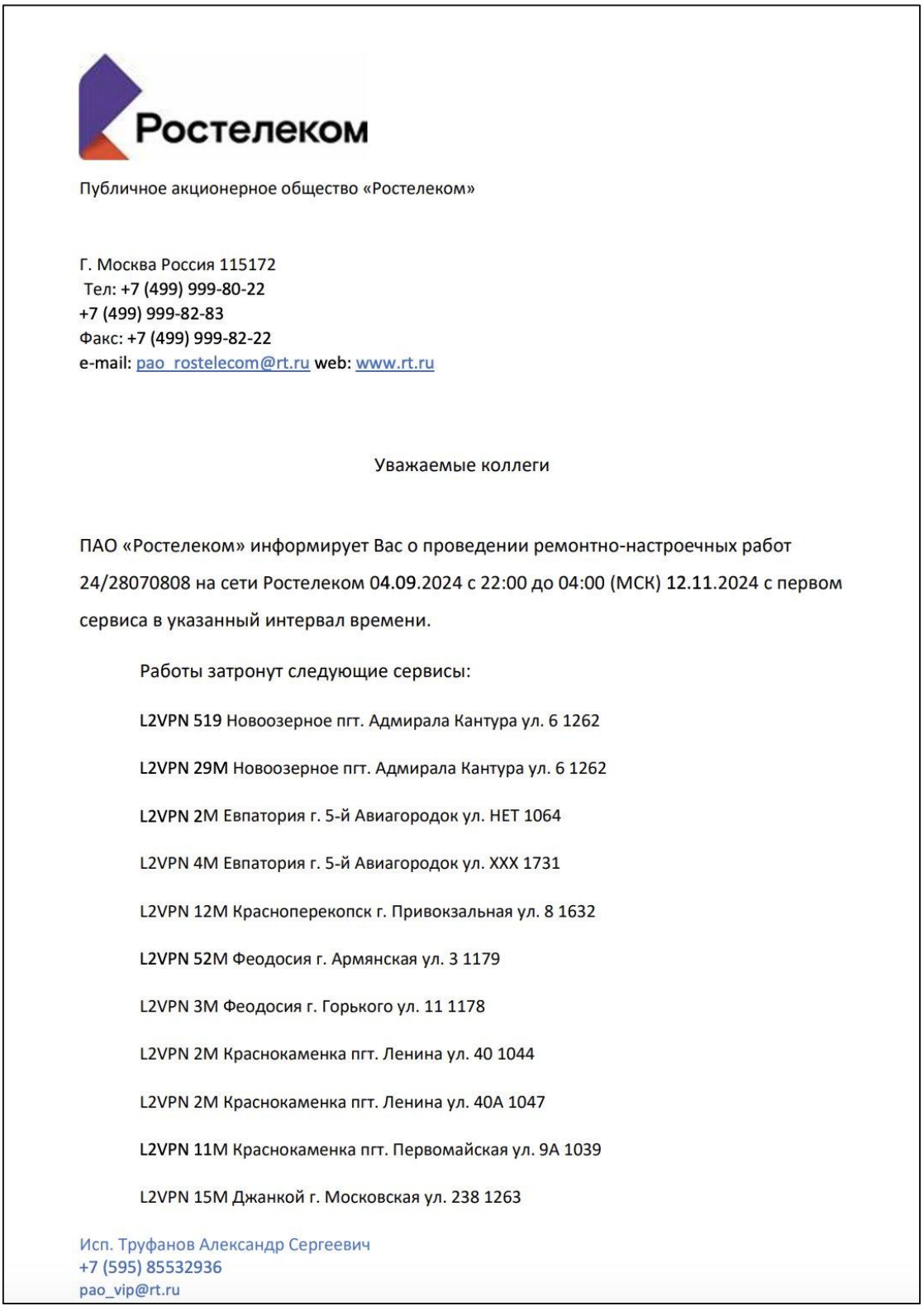
## CAMPAIGN DETAILS

The campaign begins with **phishing emails** disguised as invitations to events like the **Primakov Readings** and the "Security of the Union State" forum. When victims click the embedded links, it triggers a **one-click Chrome exploit** (CVE-2025-2783), automatically bypassing the browser's sandbox and delivering the **Trinper backdoor**.

The Trinper malware is a **multi-stage, obfuscated loader** that:

- Derives decryption keys using **firmware UUIDs**, **process paths**, and **modified ChaCha20** algorithms.
- Aborts or stalls if executed outside predefined processes or environments (anti-analysis features).
- Communicates via **named pipes** and **mimicry C2 domains** (e.g., common-rdp-front.global.ssl.fastly.net).

The payload chain uses **LOLBins** (e.g., rdpclip.exe, AdobeARM.exe) and disguised files (e.g., PDFs or updater executables). Reconnaissance tools like dirlist.exe, ProcessList.exe, and ScreenShot.exe are also deployed post-infection, all written in **.NET**.



Ростелеком

Публичное акционерное общество «Ростелеком»

Г. Москва Россия 115172
Тел: +7 (499) 999-80-22
+7 (499) 999-82-83
Факс: +7 (499) 999-82-22
e-mail: pao_rostelecom@rt.ru web: www.rt.ru

Уважаемые коллеги

ПАО «Ростелеком» информирует Вас о проведении ремонтно-настроечных работ 24/28070808 на сети Ростелеком 04.09.2024 с 22:00 до 04:00 (МСК) 12.11.2024 с первом сервиса в указанный интервал времени.

Работы затронут следующие сервисы:

L2VPN 519 Новоозерное пгт. Адмирала Кантура ул. 6 1262

L2VPN 29M Новоозерное пгт. Адмирала Кантура ул. 6 1262

L2VPN 2M Евпатория г. 5-й Авиагородок ул. НЕТ 1064

L2VPN 4M Евпатория г. 5-й Авиагородок ул. XXX 1731

L2VPN 12M Краснoперекопск г. Привокзальная ул. 8 1632

L2VPN 52M Феодосия г. Армянская ул. 3 1179

L2VPN 3M Феодосия г. Горького ул. 11 1178

L2VPN 2M Краснокаменка пгт. Ленина ул. 40 1044

L2VPN 2M Краснокаменка пгт. Ленина ул. 40А 1047

L2VPN 11M Краснокаменка пгт. Первомайская ул. 9А 1039

L2VPN 15M Джанкой г. Московская ул. 238 1263

Исп. Труфанов Александр Сергеевич
+7 (595) 85532936
pao_vip@rt.ru

*Figure 1: Decoy document used in the September 2024 attack*

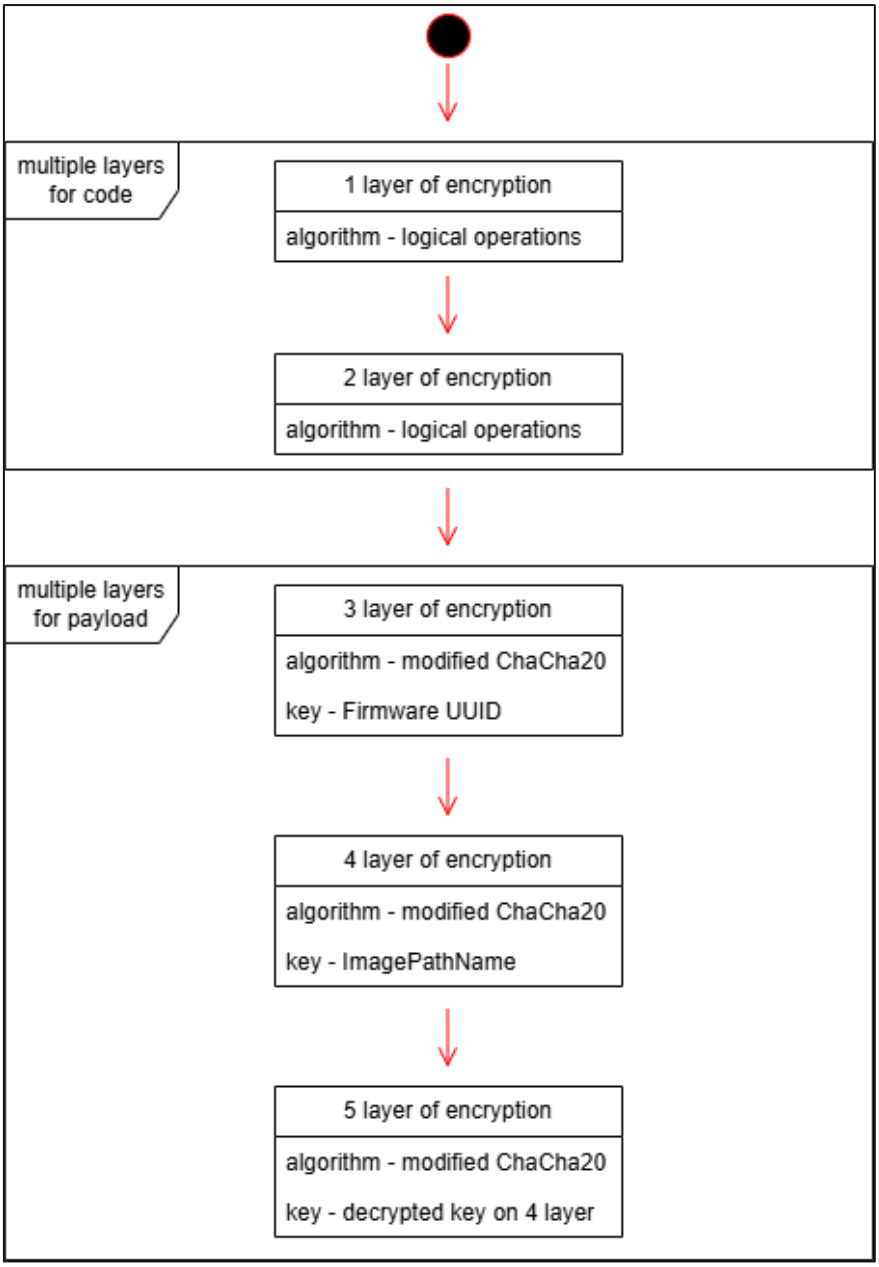



*Figure 2: Layers of encryption*

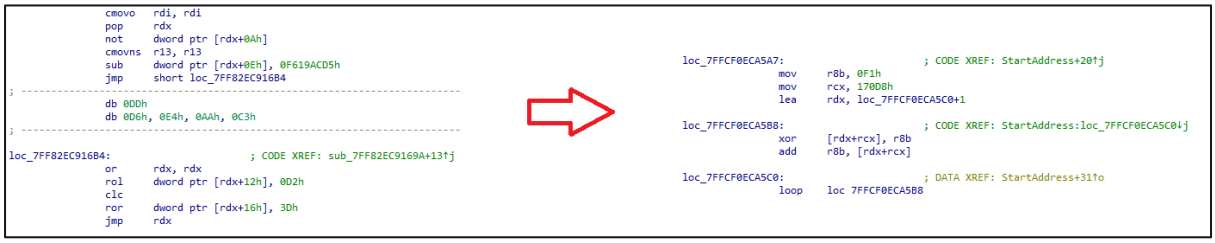



*Figure 3: Decryption of the first and second layers*

## THREAT ACTOR PROFILE

| Threat Actor Profile: Team46 | |
|---|---|
| **Aliases** | Team46, TaxOff |
| **Type** | Advanced Persistent Threat (APT) |
| **Target Sectors** | Government entities**,** Defense organizations**,** Diplomacy, and international policy institutions. |
| **Activity Timeline** | At least since February 2024 – Ongoing |
| **Motivation** | Espionage, intelligence gathering |
| **Target Regions** | Primarily Russia, potentially broader Eurasia region |
| **Delivery Mechanism** | Phishing emails with malicious archive/shortcut links or decoy documents. |

## CVE DETAILS

**CVE-2025-2783: Chrome sandbox escape vulnerability**

**Description:** A vulnerability in the Mojo component of Google Chrome for Windows, before version 134.0.6998.177, allowed a remote attacker to escape the browser sandbox by leveraging a malicious file. This issue occurred due to using an incorrect handle under certain unspecified conditions.

**Impact:** Remote Code Execution outside the sandbox

**CVSS Score:** 8.3 (High)

**Affected Product:** Google Chrome (latest versions as of March 2025)

**Exploit Vector:** Phishing link → malicious site → automatic payload drops

## NOTABLE CAMPAIGNS

**March 2025 - Chrome 0-Day Campaign**

- **Exploit Used**: CVE-2025-2783 (Chrome sandbox escape)
- **Delivery: P**hishing email disguised as an invitation to the *Primakov Readings* forum
- **Payload:** Trinper backdoor via PowerShell script
- **Infrastructure:** ms-appdata-query.global.ssl.fastly.net, fake forum site hosting exploit
- **Key Indicators:** Edge User-Agent for decoys, obfuscated PowerShell scripts, use of system UUID in decryption

**October 2024 - "Union State Security" Campaign**

- **Lure:** Conference invitation decoy
- **Phishing URL:** https://mil-by[.]info/#/i?id=[REDACTED]
- **Execution:** PowerShell downloading DLL-hijacking payload targeting rdpclip.exe and replacing winsta.dll
- **Final Payload:** Trinper

**September 2024 - Rostelecom Campaign**

- **Lure:** Maintenance alert from Rostelecom
- **Payload:** AdobeARM.exe (Trinper loader variant)
- **Style Clues:** Random fake phone numbers, matching Team46 pattern
- **PowerShell Delivery:** Download of scan_3824.pdf and a second-stage payload from a C2 domain

**February 2024 - Early Team46 Campaign**

- **Indicators:** infosecteam.info, similar PowerShell script format
- **Similarities:** Use of obfuscation, BLAKE2b hashes, and decoy PDFs

## IMPACTS

- **Zero-Click Malware Deployment:** Exploitation of Google Chrome zero-day (CVE-2025-2783) enables automatic malware installation upon clicking a phishing link, requiring no further user action, boosting infection success, especially among high-value targets.
- **Targeted Government & Defense Entities:** The campaign targets individuals tied to government and defense, using phishing emails disguised as official conference invitations, indicating a likely espionage objective.
- **Persistent Surveillance with .NET Tools:** Following infection, custom .NET tools (e.g., dirlist.exe, ProcessList.exe, ScreenShot.exe) are used for reconnaissance and data collection, maintaining covert system monitoring via named pipes.
- **Evasion of Sandbox Analysis:** The Trinper loader incorporates anti-analysis checks using environment-specific identifiers (firmware UUIDs, ImagePathName). In unapproved environments (e.g., sandboxes), it triggers an infinite decryption loop to avoid detection.

## MITRE ATT&CK TECHNIQUES

| Tactics | Techniques (ID) |
|---|---|
| Resource Development | Obtain Capabilities (T1588)<br>• Exploits (T1588.005) |
| Initial Access | Phishing (T1566)<br>• Spearphishing Link (T1566.002) |
| Execution | Command and Scripting Interpreter (T1059)<br>• PowerShell (T1059.001)<br>Native API (T1106)<br>User Execution (T1204)<br>• Malicious Link (T1204.001)<br>• Malicious File (T1204.002) |
| Privilege Escalation | Process Injection (T1055) |
| Defense Evasion | Obfuscated Files or Information (T1027)<br>Process Injection (T1055)<br>• Process Hollowing (T1055.012)<br>Indicator Removal (T1070)<br>• File Deletion (T1070.004)<br>• Clear Persistence (T1070.009)<br>Execution Guardrails (T1480)<br>• Environmental Keying (T1480.001)<br>Virtualization/Sandbox Evasion (T1497)<br>• System Checks (T1497.001)<br>Impair Defenses (T1562)<br>• Disable or Modify Tools (T1562.001)<br>Debugger Evasion (T1622) |

| Tactics | Techniques (ID) |
|---|---|
| Credential Access | Input Capture (T1056)<br>• Keylogging (T1056.001)<br>Steal or Forge Kerberos Tickets (T1558)<br>• Kerberoasting (T1558.003)<br>• AS-REP Roasting (T1558.004)<br>Steal or Forge Authentication Certificates (T1649) |
| Discovery | Process Discovery (T1057)<br>File and Directory Discovery (T1083)<br>System Owner/User Discovery (T1033) |
| Collection | Input Capture (T1056)<br>• Keylogging (T1056.001)<br>Clipboard Data (T1115) |
| Command and control | Application Layer Protocol (T1071)<br>Proxy (T1090)<br>• Domain Fronting (T1090.004)<br>Data Encoding (T1132)<br>• Standard Encoding (T1132.001)<br>Protocol Tunneling (T1572)<br>Encrypted Channel (T1573)<br>• Symmetric (T1573.001)<br>• Asymmetric (T1573.002)<br>Remote Access Software (T1219) |
| Exfiltration | Exfiltration Over C2 Channel (T1041) |

## INDICATORS OF COMPROMISE (IOCs)

| File Hashes |
|---|
| *2e39800df1cafbebfa22b437744d80f1b38111b471fa3eb42f2214a5ac7e1f13* |
| *f062681125a93a364618da3126c42b6e7c8f27910e954a7b8afd72455ddce328* |
| *b159534cd3bf2fa350edf18969ea4b07cb3cded49c40d927bac19ff390589504* |
| *ab42a3c6ff062147fa7bbf527f7b0b106c1514872bd1a90c8868423fa0485038* |
| *f15d8c58d8edb2ec17d35fe9d65062a767067760896eb425fc0de0d4536cc666* |
| *d622119cd68ad24f3498c54136242776d69ffe1f6b382a984616a667849c08b2* |
| *99786a04acc05254dd35b511c4b3af34c88251f926c4ef91c215a9fce6ba8f96* |
| *fde9725923e15ca4f790c0ad4766fe7d60e6e3dae75ea8ccf04ff42f2458b4b1* |
| *7975d287b07454b68455dd7e052eb741b5bf81712596ea00ddda2b103a99d037* |
| *185cdfd1eeef2a4063e5134653c53058f91050de8c9234740a7ddd215a2aeaed* |
| *2997647affa42eff41a27c5db54b126087a36f789c8cfc66d24a21fe7212badc* |

| ***IP Address*** |
|---|
| *185.81.114.15* |

| ***Domains*** | |
|---|---|
| *mil-by.info* | *2025primakovreadings.info* |
| *primakovreadings.info* | *primakovreadings2025.info* |

| ***URLs*** | |
|---|---|
| *ads-stream-api-v2.global.ssl.fastly.net* | *common-rdp-front.global.ssl.fastly.net* |
| *fast-telemetry-api.global.ssl.fastly.net* | *front-static-api.global.ssl.fastly.net* |
| *browser-time-stats.global.ssl.fastly.net* | *main-front-api.global.ssl.fastly.net* |
| *rdp-query-api.global.ssl.fastly.net* | *ms-appdata-fonts.global.ssl.fastly.net* |
| *rdp-statistics-api.global.ssl.fastly.net* | *ms-appdata-main.global.ssl.fastly.net* |
| *clip-rdp-api.global.ssl.fastly.net* | *ms-appdata-query.global.ssl.fastly.net* |
| *rdp-api-front.global.ssl.fastly.net* | |

## RECOMMENDATIONS

1. **Patch Chrome Immediately**

   Apply updates as soon as Google releases patches for CVE-2025-2783. Disable JavaScript and limit browser extension permissions where feasible.

2. **Monitor PowerShell Behavior**

   Implement PowerShell logging and monitor for suspicious, encoded, or LOLBin-related execution patterns.

3. **DNS and Network Monitoring**

   Block or alert on outbound traffic to known C2 domains (e.g., *.fastly.net) and named pipe communication patterns indicative of Trinper activity.

4. **Harden Endpoint Detection**

   Enable EDR solutions capable of behavior-based detection, especially those that track memory injections, UUID-based decryptors, or .NET tool usage.

5. **Phishing Awareness**

   Train employees to identify lures tied to political or event-related themes. Warn against clicking on unsolicited invitations or downloading unknown PDFs.

## REFERENCES

https://securityonline.info/team46-taxoff-exploits-google-chrome-zero-day-cve-2025-2783-in-sophisticated-phishing-campaign/

https://global.ptsecurity.com/analytics/pt-esc-threat-intelligence/team46-and-taxoff-two-sides-of-the-same-coin

https://nvd.nist.gov/vuln/detail/CVE-2025-2783

https://chromereleases.googleblog.com/2025/03/stable-channel-update-for-desktop_25.html

**Vairav Technology Security Pvt. Ltd.**

**Cyber Defender from the land of Gurkha**

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com