

INTRINSEC

Innovative by design

Malicious browser extensions ecosystem overview

Cyber Threat Intelligence

November 2026

@Intrinsec @Intrinsec Blog Website

2026 Intrinsec, Inc. All rights reserved.

Table of contents

1. Executive Summary 3
2. Recent campaigns 4
3. The malicious extension ecosystem 6
3.1 Threat actor: Kalen 6
3.2 Threat actor: Lupin 7
3.3 Threat actor: Nomix 8
3.4 Silent browser extensions 9
4. Incident investigated by our SOC 12
4.1 Suspicious extensions 12
5. Infrastructure 15
5.1 Needle 15
5.2 Lunex 18
5.3 Other 23
6. Actionable content 24
6.1 Indicators of compromise 24
6.2 Recommendations 26
6.3 Tactics, Techniques and Procedures 29
7. Sources 30

1. Executive Summary

This report provides an overview of the malicious browser extension ecosystem. We give details on:

- Recent public campaigns involving malicious browser extensions. Several common features were identified amongst the campaigns, such as the release of 'clean' extensions to gain trust, silent updates containing the malware, advanced evasion techniques and a focus on the theft of cryptocurrencies and authenticated sessions.
- Known threat actors that actively develop and manage malware masquerading as legitimate extensions. Discussions inside the forums highlight the quest for "silent" extension installation. We also noticed some talks about moderation and long-term stability for extensions on browser stores.
- Details on an incident investigated by our SOC and CTI related to malicious extensions. No evidence of malicious activity was evidenced at this time, but we managed to identify a list of "suspicious" browser extensions.
- Infrastructure analysis and pivots available to detect known malware that can be disguised as legitimate extensions, including Needle and Lunex. IP addresses exposing panels for these malwares were identified.

2. Recent campaigns

Campaigns involving malicious browser extensions (primarily for Chrome, Edge and Firefox) have become increasingly widespread and sophisticated in recent months, targeting users on a massive scale for data theft, ad fraud and cryptocurrency theft.

One of the most notable operations is StegoAd, which was dismantled by Microsoft in the spring and summer of 2026[1]. This campaign involved 119 malicious extensions that were downloaded up to 2.6 million times. They masqueraded as useful tools (ad blockers, VPNs, translators, video downloaders). The malware remained dormant for several days after installation to evade detection, then activated payloads concealed via steganography within PNG or WebP images or font files. Once activated, these extensions not only enabled ad fraud and the hijacking of Amazon affiliate programmes, but also provided a backdoor for remote code execution, the theft of Google passwords by bypassing 2FA, the retrieval of WordPress login credentials and the mass exfiltration of cookies.

Meanwhile, in August 2026, researchers at Socket[2] discovered 19 Chrome and Edge extensions (including one particularly popular one with around 80,000 users) that delivered an extensible malware framework. These extensions, which were often clean to begin with, were subsequently updated with malicious code. Some had even been purchased from legitimate developers. The malware established a persistent WebSocket connection with a command-and-control server, removed CSP headers to facilitate script injection, and loaded modules capable of draining multi-chain crypto wallets (EVM, Solana, Tron), phishing for Ledger and Trezor seed phrases, and stealing sessions on exchanges such as Binance, Coinbase or MetaMask.

Another campaign, reported by Malwarebytes in April 2026, demonstrated how a fake trading site (“TradingClaw”) distributed the Needle stealer[3]. This malware then installed malicious extensions that gave attackers almost total control of the browser: intercepting downloads, injecting scripts, monitoring activity and stealing wallet data.

[1] *https://microsoftedge.github.io/edgevr/assets/files/stego_ad/Microsoft_Edge_Security_StegoAd.pdf*

[2] *https://socket.dev/blog/chrome-edge-extension-wallet-drainer*

[3] *https://www.malwarebytes.com/blog/threat-intel/2026/04/malicious-trading-website-drop-malware-that-hands-over-your-browser-to-attackers*

Other recent operations, such as KREMLIN[4] (primarily targeting Brazil) or PEEP[5], confirm the trend: extensions have become a preferred vector for installing post-compromise backdoors, stealing session cookies and bypassing browser protections.

These campaigns share several common features:

- The release of 'clean' extensions to gain trust,
- Silent updates containing the malware,
- Advanced evasion techniques (steganography, polymorphism, activation delays),
- A focus on the theft of cryptocurrencies and authenticated sessions.

[4] *https://www.elastic.co/security-labs/threat-command/malicious-browser-extension-kremlin-banking-malware*

[5] *https://socradar.io/blog/peep-browser-rat-chrome-extension/*

3. The malicious extension ecosystem

Malicious extensions became an important intrusion vector, partly due to the evolution of the ecosystem and the enhancement of offers proposed to threat actors on cybercrime forums. As we regularly monitor cybercrime forums for the promotion of new tooling, malware and services, we wanted to show examples of recent malicious extensions promoted by threat actors.

3.1 Threat actor: Kalen

The threat actor “Kalen” is a developer of solutions related to browser extensions. One such malware is Lunex, designed as a versatile malware capable of various malicious activities, including acting as a stealer, clipper, dropper, and loader. Its core functionality involves injecting into bank and cryptocurrency-related browser extensions. It can steal cookies, passwords, and cryptocurrency wallet data, and has the capability to download and execute files on compromised systems. The malware also features a clipper function to substitute wallet addresses during transactions.

The malware is under continuous development, with frequent updates adding new features and improving existing ones. Recent updates include enhanced bot export, the ability to list installed browsers, improved deletion tracking, direct file execution from the extension, and the collection of various browser and desktop cryptocurrency wallet data.

Other threat actors consistently praise the 'Lunex' malware for its functionality and the developer's support. Feedback highlights that the software works as intended, is easy to set up and configure, and that the developer (“Kalen”) is responsive to questions and issues, often providing timely updates and adaptations.

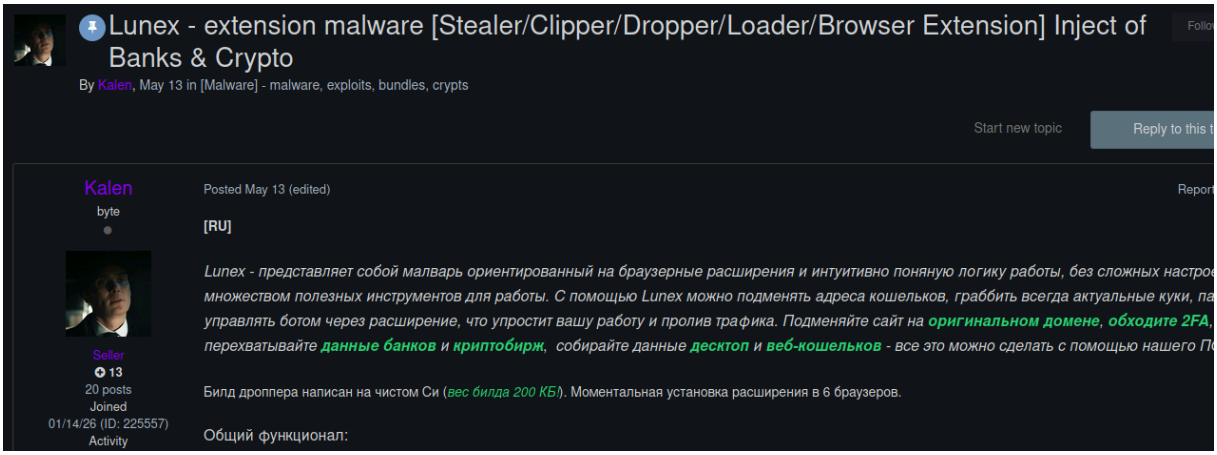


Figure 1: Lunex extension malware promotion on Exploit. Source: hxxps://forum.exploit.in/topic/282680/

Another example by the same developer is the "Lunex Dropper" tool designed for silently installing browser extensions across multiple Chromium-based browsers, including Chrome, Edge, Opera, Brave, Vivaldi, and ArcBrowser. The tool offers features such as optional Telegram notifications and automatic reinstallation of extensions if removed.

The primary technique discussed is the silent installation of browser extensions. A key tactic employed is bypassing security measures, specifically Chrome's developer mode, which typically requires user interaction to enable. This bypass can be achieved through technical means such as manipulating browser configuration files, and where necessary, handling or circumventing the integrity and data protection mechanisms associated with them, including protections involving HMAC and Windows DPAPI. The tool also implements persistence by offering an optional feature to automatically reinstall extensions if they are manually removed by the user. Furthermore, the dropper supports silent installation across multiple browsers, indicating a technique for widespread deployment.

The dropper tool is confirmed by other threat actors to bypass Chrome's developer mode. This capability is a key selling point for users seeking to deploy extensions without user interaction or explicit permission.



Figure 2: Extension dropper tool promotion on Exploit. Source: hxxps://forum.exploit.in/topic/277676/

3.2 Threat actor: Lupin

The threat actor 'Lupin' is the suspected developer of the 'NeedleExtension' service. The 'NeedleExtension' is being actively developed and marketed as a tool for creating and publishing malware browser extensions. This extension is designed to act as a dropper for Windows and macOS, with capabilities for publishing on the Google Chrome Store. It offers features such as a "bar to the site" for displaying custom content such as phishing or unwanted advertisements directly to users, the ability to execute PowerShell/CMD code on

a bot's machine, and file system management. The extension is designed to be adaptable to new browser versions, with ongoing development to maintain functionality and evade detection.



Figure 3: NeedleExtension promotion on Exploit. Source: hxxps://forum.exploit.in/topic/286109/

Messages from other users on the thread talk about the process of publishing extensions on the Google Store, including methods to bypass moderation and ensure persistence. Concerns are raised about the reliability of extensions staying online after publication, with suggestions of compromising legitimate developer accounts to push malicious updates. The data indicates that while initial moderation might be passed, the long-term stability is not guaranteed and depends on the developer's actions post-publication.

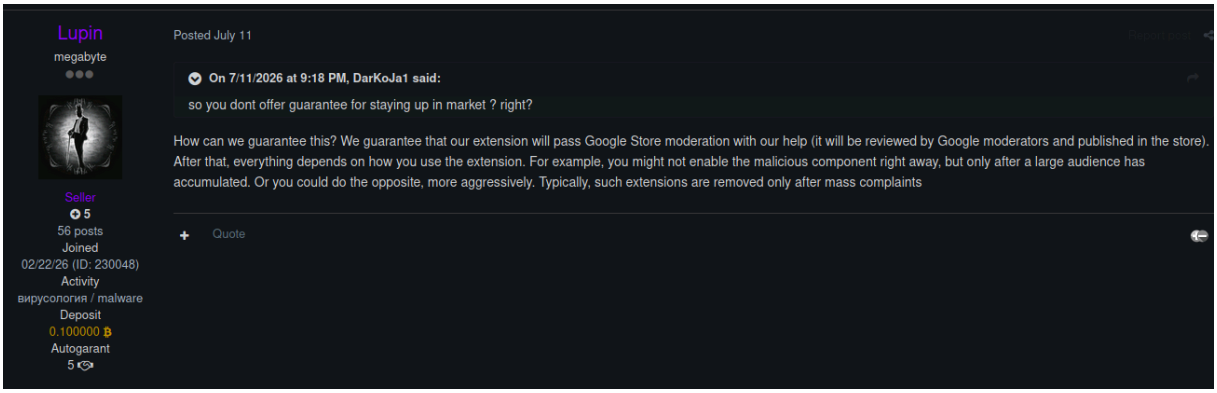


Figure 4: Discussion about Google Store moderation and "silent" extension.

3.3 Threat actor: Nomix

The threat actor "Nomix" was identified as a seller and developer of a ScreenConnect tool enhanced with custom extensions and an RPacker crypter. The tool is advertised with

advanced evasion capabilities, including UAC bypass, AV/EDR bypass, and browser warnings bypass, making it a potent threat for initial access and persistence. The tool can generate payloads with PDF icons and .cmd/.lnk formats, capable of opening decoy PDF documents to mask malicious activity.

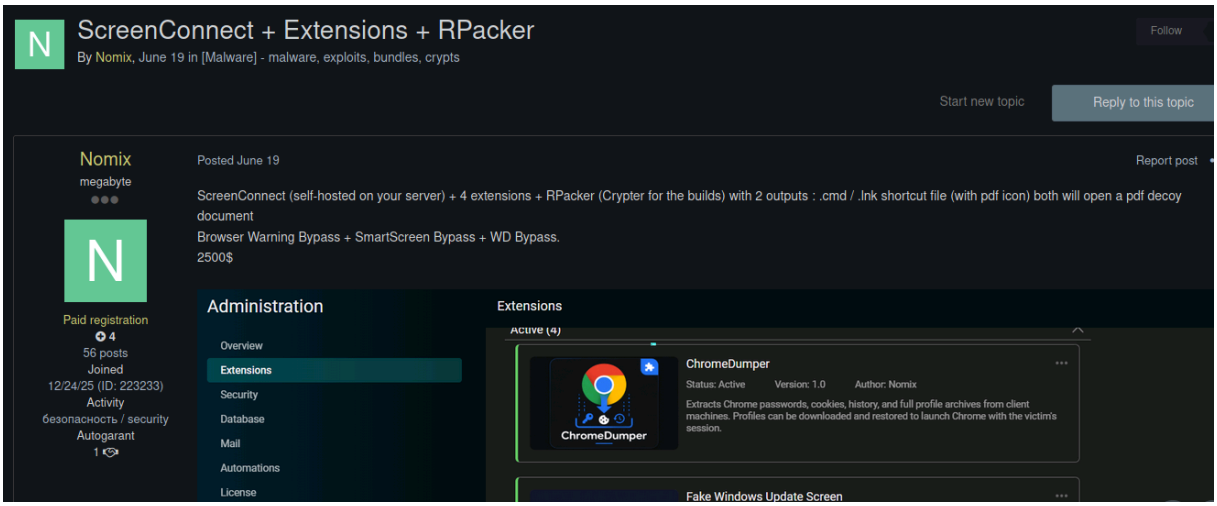


Figure 5: Extensions sold inside a package. Source: hxxps://forum.exploit.in/topic/285440/

“Nomix” is actively updating the tool and engaging with potential buyers. However, there are indications of seller unreliability and potential scamming, with some users reporting disappearing sellers and delayed responses. The tool's capabilities suggest a high risk for organizations relying on ScreenConnect for legitimate remote access, as it can be weaponized for malicious purposes. Recent additions include Telegram, Trezor, and Ledger extensions, which can forward captured data to Telegram or replace user applications for persistence. 'Nomix' also claims to have patched public CVEs related to ScreenConnect and offers support and escrow services, though some users have reported issues with seller responsiveness and product availability.

There are significant concerns regarding the seller's reliability and potential for fraudulent activity. Multiple users have reported issues such as the seller disappearing after initial contact, delayed responses, and unfulfilled promises for demonstrations or product delivery.

3.4 Silent browser extensions

We identified various services related to “silent” browser extensions. One threat actor, “vuvum”, appears to be the developer or main seller of a “Silent Browser Extension Installer”. The silent installation of browser extensions is achieved through direct manipulation of browser configuration files and potentially employing techniques to remain undetected by security software ('FUD' status, evasion of Windows Defender). The tool supports multiple

browsers and versions, indicating adaptability. Distribution methods discussed include direct download of executables, and the installer is offered as part of broader malware kits, suggesting its use in phishing campaigns, drive-by downloads, or as a component in more sophisticated attacks to steal credentials, inject ads, or establish persistent access.

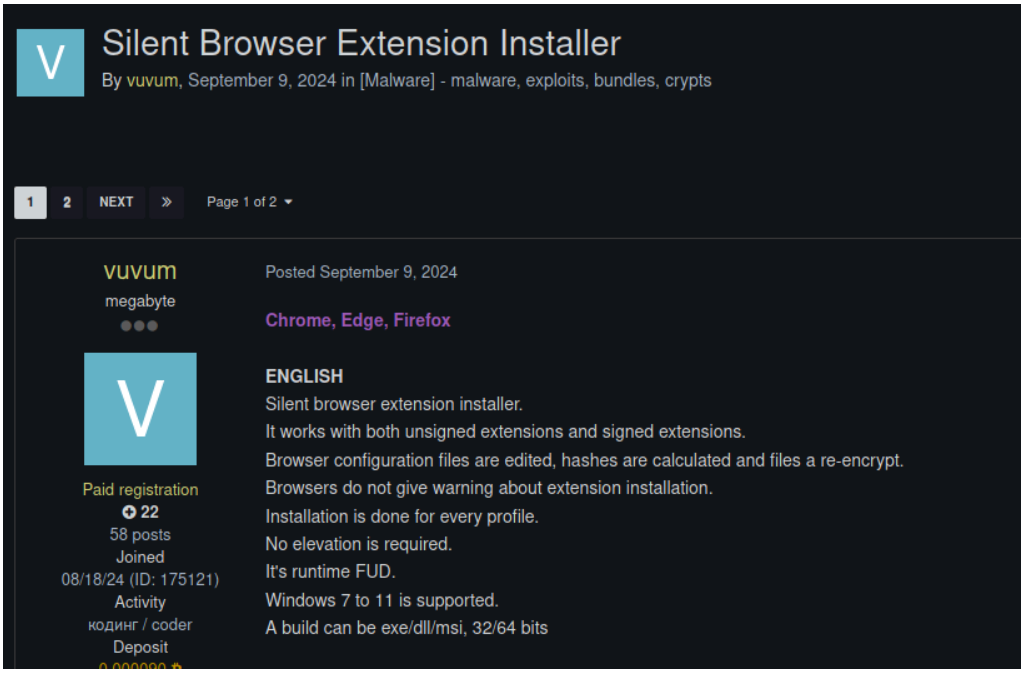


Figure 6: Silent Browser Extension installer. Source: hxxps://forum.exploit.in/topic/247096/

The tool supports silent installation across major browsers including Chrome, Firefox, and Edge. Discussions indicate compatibility with the latest versions of these browsers. The installer operates without requiring administrative privileges or closing the browser.

Other threat actors are inquiring about bypassing security measures such as Windows Defender and achieving 'FUD' status for the installer. There is also discussion about how Chrome handles silent extension installations and potential user warnings. The tool's developers claim it is designed to be stealthy and avoid detection.

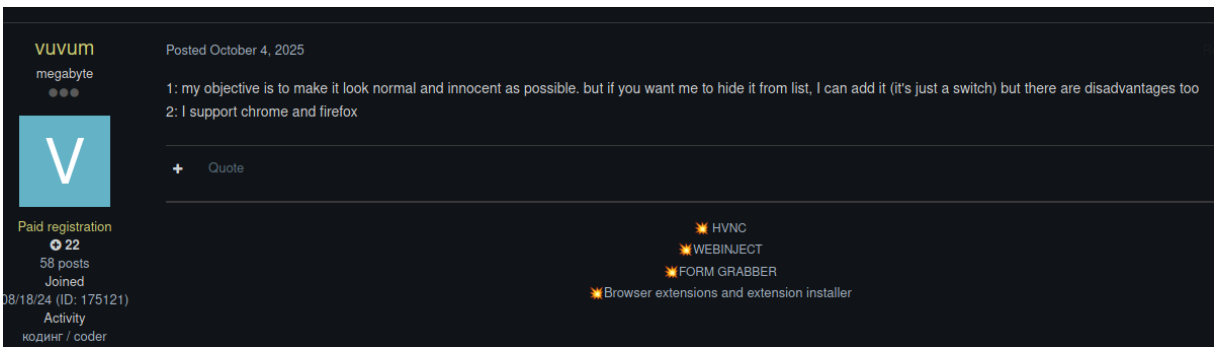


Figure 7: Discussion about evasion techniques.

Another service is offered by the threat actor “rabiidd”. He advertised a “private” offering on the Exploit forum concerning a Windows malware infrastructure, which includes a silent browser extension installer, a Remote Access Trojan (RAT), and a browser stealer. The service is priced at $3500/year or $500/month, with ongoing support, feature updates, bug fixes, and patches. The limited availability, indicated by 'Spots' updates, implies a controlled or exclusive access model.

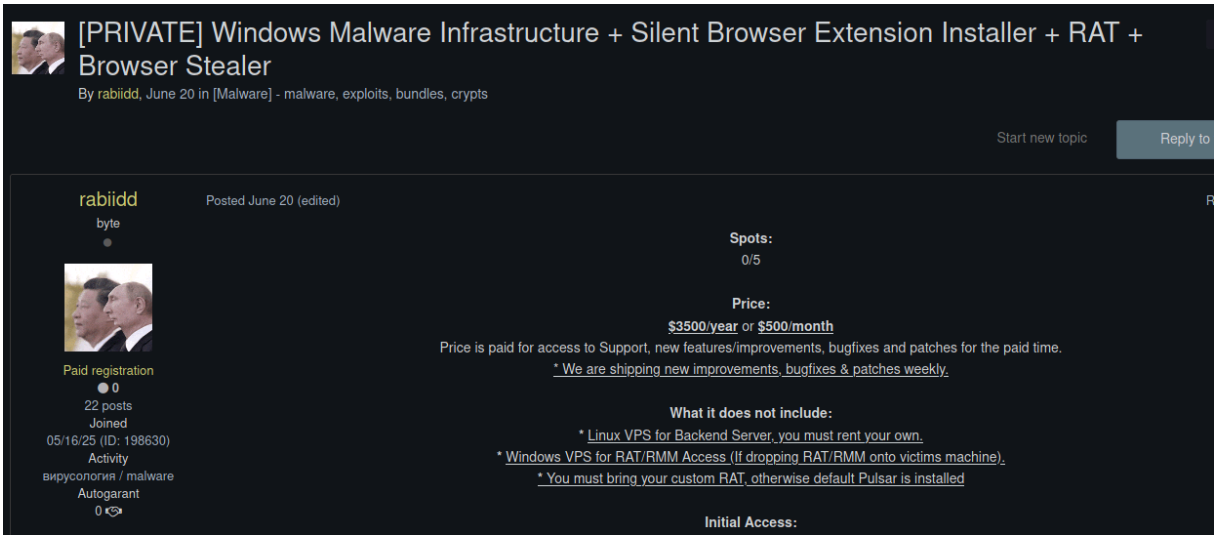


Figure 8: Silent Browser Extension Installer sold inside a package. Source: hxxps://forum.exploit.in/topic/285514/

4. Incident investigated by our SOC

Our SOC team received an alert on a client's SIEM based on domain names mentioned in the Microsoft report related to the StegoAD threat[6]. The notification popped in the end of August, so the extensions mentioned inside Microsoft's report were not found on the Chrome Web Store as they probably were taken down since then. The SOC team asked for our help to identify additional information and the potential origin of the alert.

4.1 Suspicious extensions

We noticed that the subdomain commerce-js[.sovrn[.co was linked to several Google Chrome extensions. While sovrn[.co is a legitimate affiliate marketing website, the low number of files communicating with this subdomain and the fact that some of them are malicious is suspicious.

Communicating Files (38)

Scanned	Detections	Type	Name
2026-07-26	0 / 61	Google Chrome Extension	jfjlaojhifbpfjimnfbleohlcfbdblmm.1.0.crx
2026-05-14	0 / 61	Google Chrome Extension	libgdijhcidhkeigehfhnpoiiehjfcbe.0.0.0.1.crx
2026-06-02	0 / 60	INI	Elliot Institute.url
2026-01-10	1 / 65	Android	3380caf74ec34a3362c3f5bcffd717b9.apk
2026-05-11	0 / 61	Email	AMAZON Final Reminder Govind Prasad.. Your Application has
2025-12-15	0 / 64	PDF	DMCA takedown notice - Advanced Whispers Dec 2025.pdf
2026-01-10	2 / 65	Android	2313770ff9b3e1094cdc4ee252c3a355.apk
2025-11-01	0 / 56	Android	com.fxp.fxpapp_5.1.apk
2026-08-29	0 / 60	Email	Re Correction RE Invoices 196185 196462 196186 196245 1963
2026-01-08	56 / 71	Win32 EXE	395131e2166aca1e712d9f732106aa268749748f485d67728977
2026-07-03	0 / 61	Windows shortcut	Chromium.lnk
2026-05-23	0 / 60	Google Chrome Extension	pbmmdmbfgfoimnofdclpocoelhbcmleb.1.0.crx
2026-02-02	15 / 65	RAR	5566a4cd2373ac9e8a6d3b2f05f8c4ba3d911e911c32c17ad6b2
2025-12-31	47 / 72	Win32 EXE	Special Amoyme
2026-01-08	0 / 66	Android	iu6ra4e.exe
2025-12-29	6 / 67	Android	Aerohokkey Vyzov.apk

Figure 9: Google Chrome Extension communicating with the domain. Source: https://www.virustotal.com/gui/domain/commerce-js.sovrn.co/relations

The extensions identified can be found on the Chrome Web Store as the extension ID is available in the name. For example, searching for "**libgdijhcidhkeigehfhnpoiiehjfcbe**" on the Web Store returns the extension "**Canvas Tab Shield**".

[6] https://microsoftedge.github.io/edgevr/assets/files/stego_ad/Microsoft_Edge_Security_StegoAd.pdf

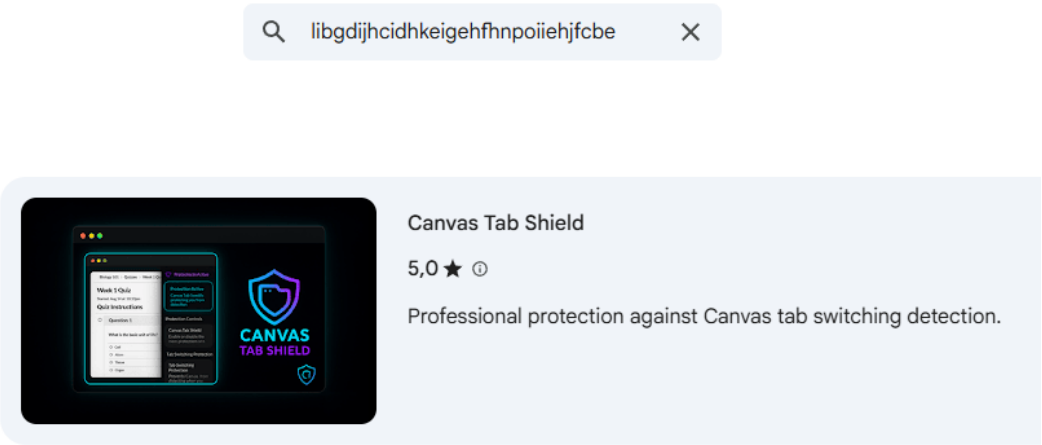


Figure 10: Extension on the Chrome Store. Source: https://chromewebstore.google.com/search/libgdijhcidhkeigehfhnpoiiehjfcbe

We could not confirm malicious behaviour associated with these extensions, but we cannot rule out the fact that these extensions could be compromised or created by threat actors and stay "silent" to attract users before a malicious update. This is a common behaviour observed in recent campaigns and evoked by threat actors on cybercrime forums. As such, we mapped all the extensions linked to this subdomain and detailed them in the table below. We do not recommend blocking them, but we will continue to monitor this cluster for potential future developments. In total these extensions were downloaded by at least 11 702 users.

Extension ID	Extension name	Number of users
mfpoeklkcdchkgklmaekfnocmihcegdj	**Screenly: Coupons & Price Comparison**	28
klhkhgekdhfcbbckbhhbmimfdmnkaika	**CleverReply**	21
eneoaclnonpfdlbdhbkcdljbaecmkblc	**AI Test Solver**	41
dammfdepmngjjoidfdbhkjboecgceamb	**Permanent Progress Bar for YouTube**	+ 10 000
mfegjohngebecpnmclfmjcpodhainlon	**Deal Analyzer**	442
ojebkaibnikkejjkedhfembnkcjebali	**CID拼多多拓展工具**	38
ljbnmcpgoakfbggfgmgidmimpdeolhaa	**Vistack.io: SaaS Management Platform**	4
njkdmfabiidfloejcpjfoeoclpiohmje	**Crimson Leaves Under Blue Sky**	0
jfkcdnlmhjbhacbpbhojpgohcodjpkjj	**Tab Closer Pro**	4
pbmmdmbfgfoimnofdclpocoelhbcmleb	**GPT prompt engineering**	13
libgdijhcidhkeigehfhnpoiiehjfcbe	**Canvas Tab Shield**	759

eboalegbolmfnmnhiojlejdihbapbnoc	**QuizCloak**	352

5. Infrastructure

We were able to map infrastructure associated with the different malicious extensions malware promoted by threat actors on cybercrime forums that we evoked earlier in this analysis.

5.1 Needle

As exposed previously, **Needle** is a malware which can be deployed in the form of malicious extensions but is not limited to such methods. By leveraging information visible on the thread promoting the service on Exploit, we can identify an IP address exposing a Needle panel (62.238.113[.106, on port 80)



Figure 11: Needle panel exposed on port 80. Source: https://www.shodan.io/host/62.238.113.106

The panel exposes a basic authentication page.

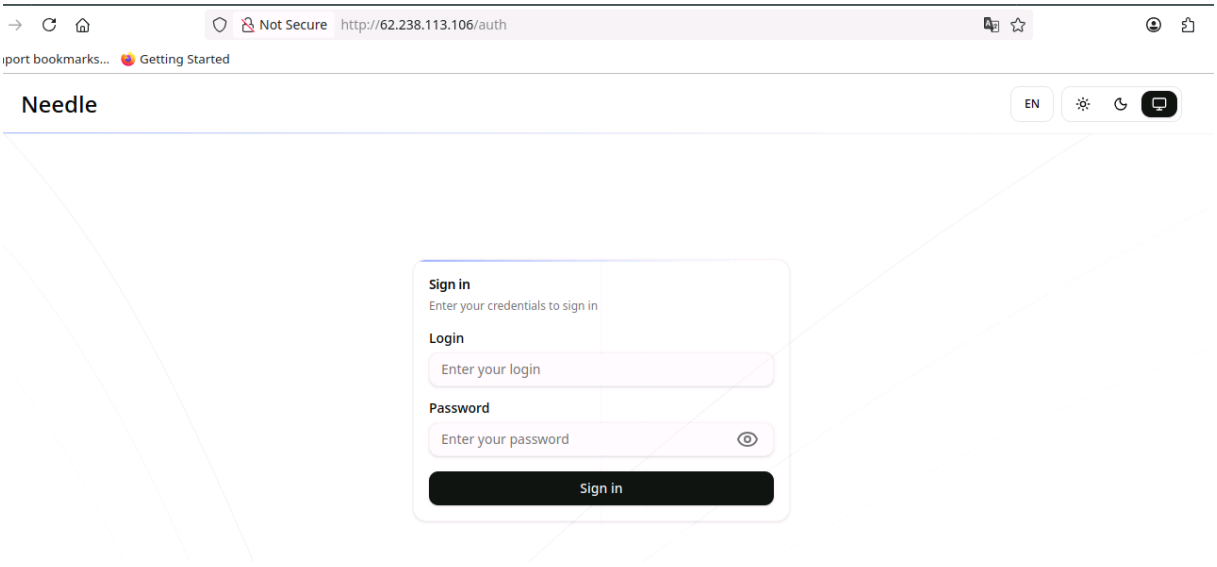


Figure 12: Needle authentication panel.

Searching for the favicon hash returns a list of IP addresses exposing the Needle panel. The list can be found in the Indicators of compromise section.

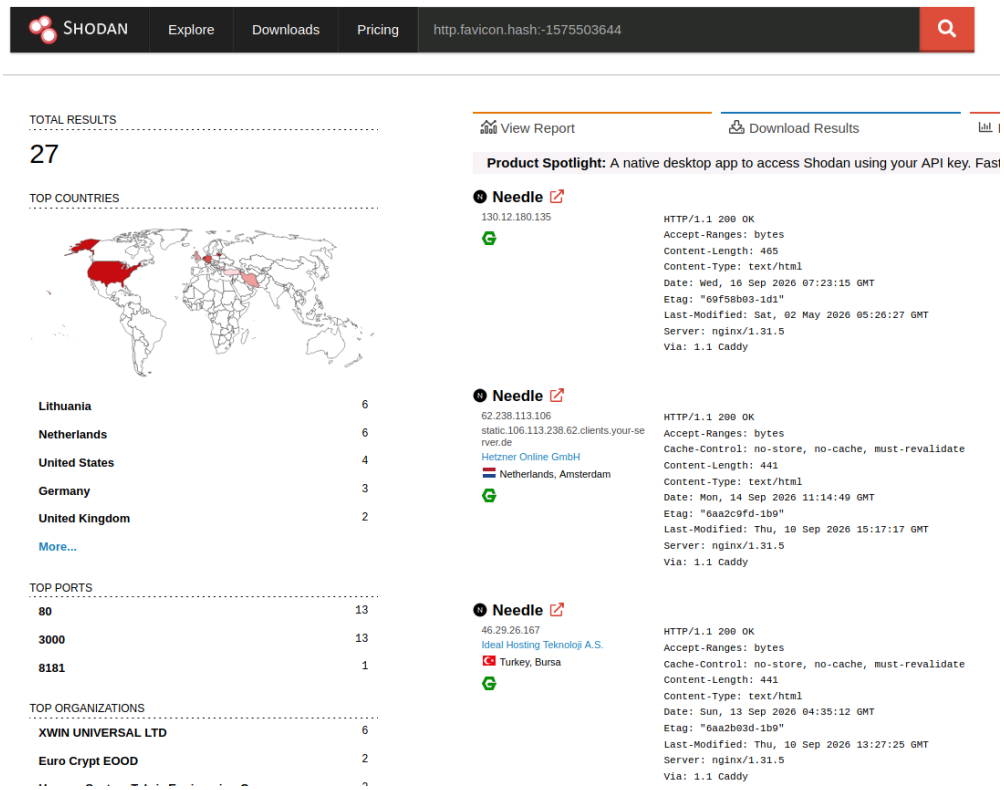


Figure 13: Other IP addresses exposing the Needle panel. Source: https://www.shodan.io/search?query=http.favicon.hash%3A-1575503644

Additionally, we found a Needle Stealer sample which reveals that the malware communicates with its C2 using endpoints hosted on "**/api/v2/needle-core**", which can be an interesting behavior for detection.

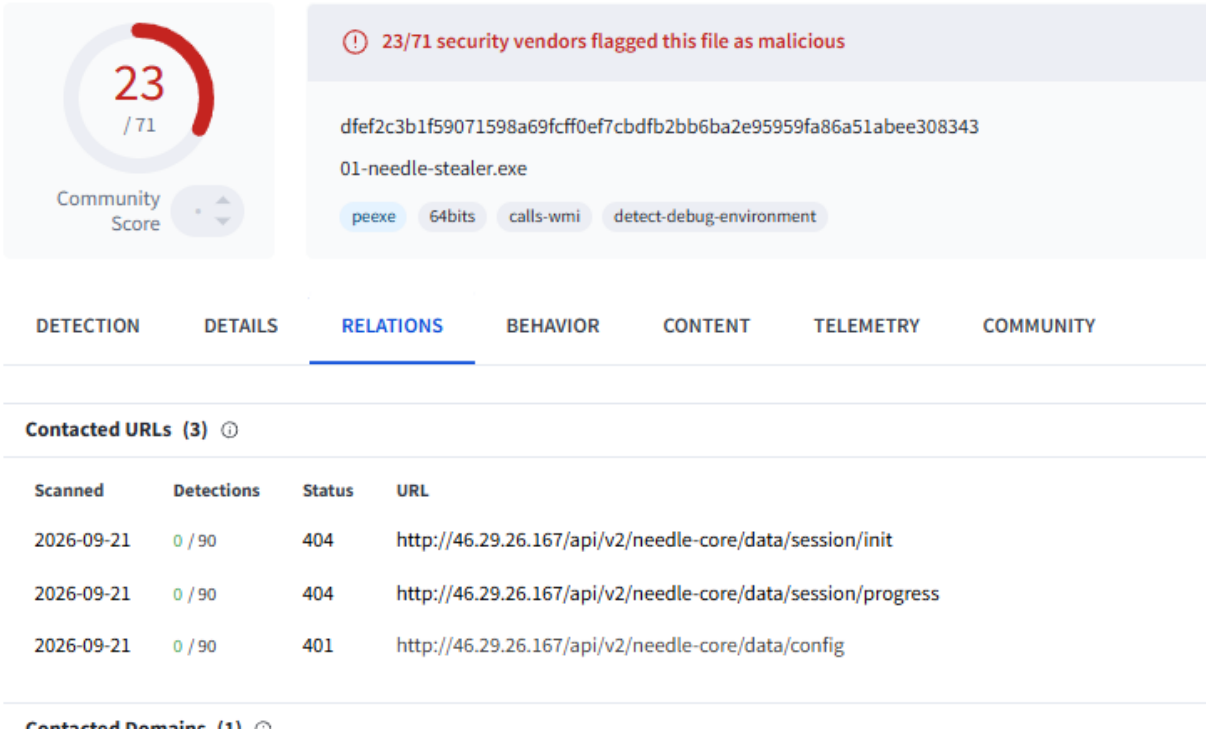


Figure 14: Needle Stealer sample communication with its C2. Source: https://www.virustotal.com/gui/file/dfef2c3b1f59071598a69fcff0ef7cbdfb2bb6ba2e95959fa86a51abee308343/relations

There are several endpoints visible on VirusTotal, including "/data/upload", "/data/session/event", "data/config", "data/session/init", "data/session/progress".

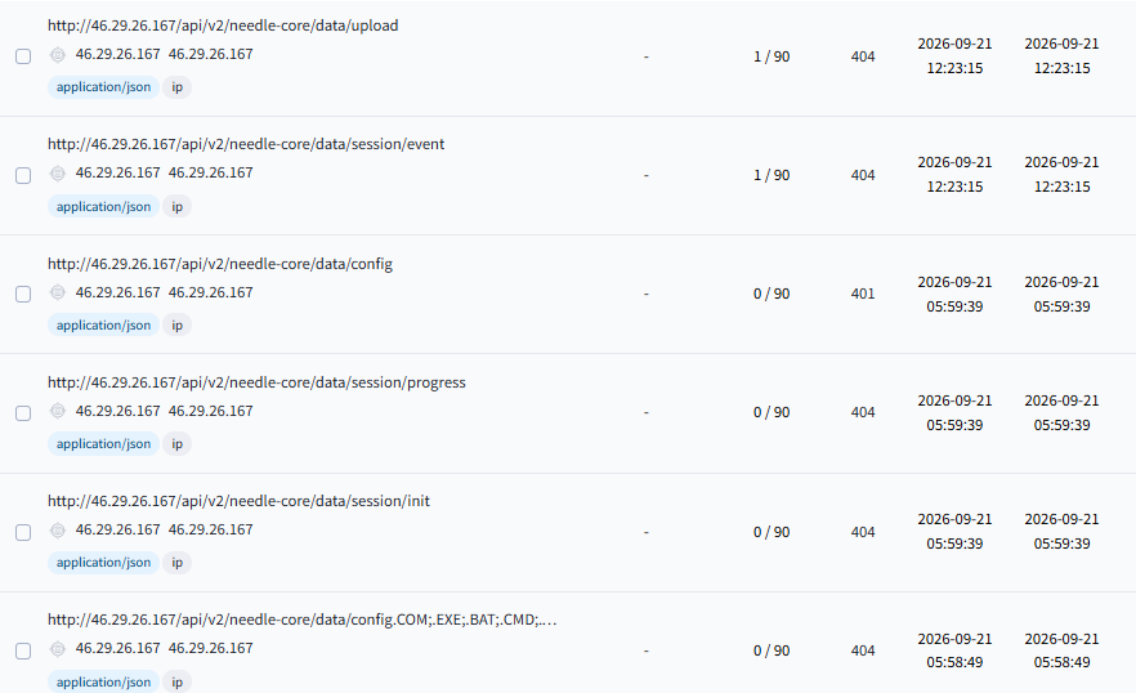


Figure 15: Other C2 endpoints identified. Source: https://www.virustotal.com/gui/search?query=entity%3Aurl+url%3Aapi%2Fv2%2Fneedle-core&type=urls

This specific endpoint shows potential file extensions available for Needle.

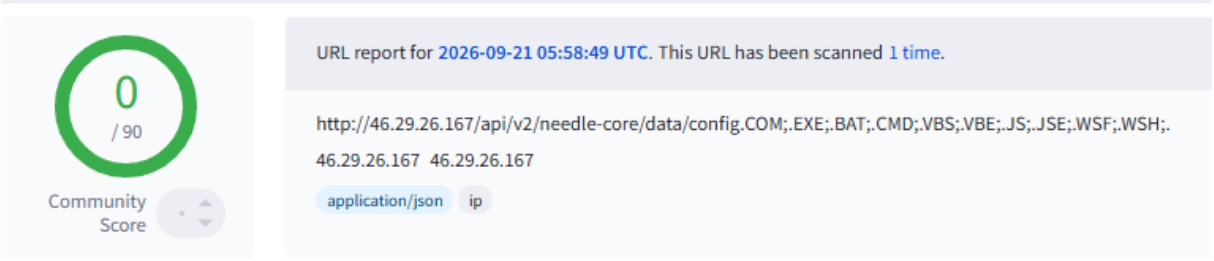


Figure 16: C2 endpoint showing file extensions. Source: https://www.virustotal.com/gui/url/d36f3d8b88328c0af8914c7905b3da963b611bdbcc98c266e64fabb9f9335591/details

5.2 Lunex

We can also identify panels associated with the **Lunex** malware.

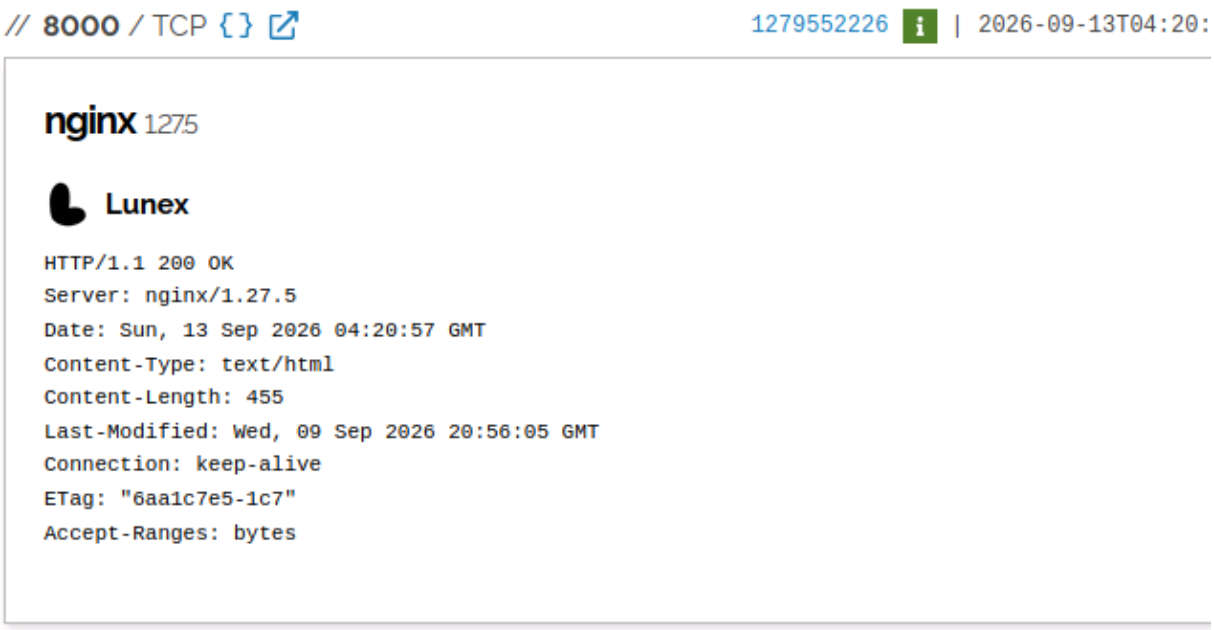


Figure 17: Lunex panel exposed on port 8000. Source: https://www.shodan.io/host/95.179.159.159

The panel is locked behind an authentication wall.

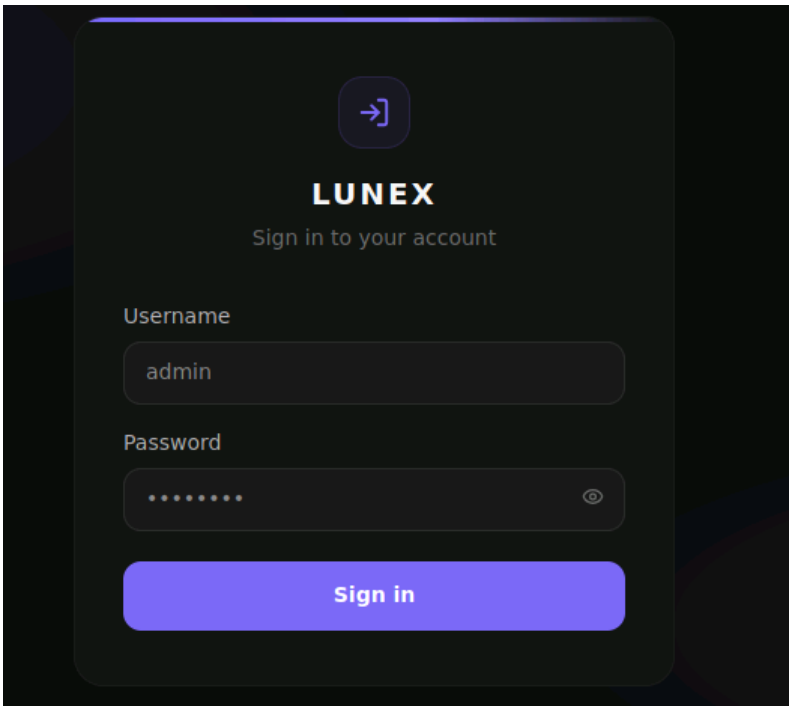


Figure 18: Lunex authentication page. Source: hxxp://95.179.159.159:8000/login

The favicon hash also returns a list of IP addresses exposing the Lunex panel. These IP addresses are available in the IOC section.

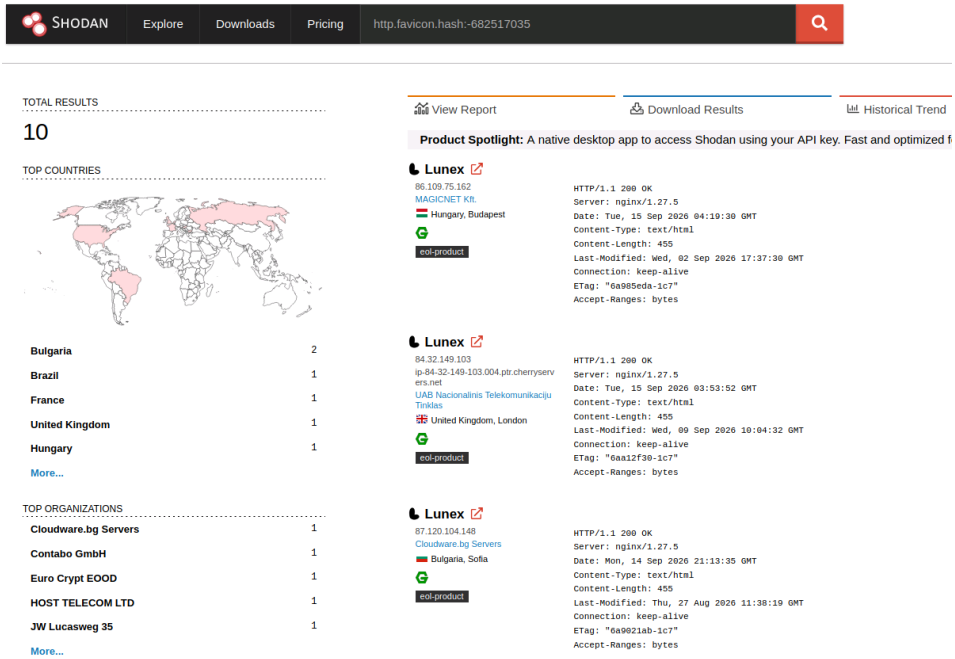


Figure 19: Other IP addresses exposing the Lunex panel. Source: https://www.shodan.io/search?query=http.favicon.hash%3A-682517035

Using those IP addresses, we were able to find one malicious Lunex sample **masquerading as a Google Translate extension**. The extension could not be found on the Chrome Store as it was probably already taken down or is installed directly on the victim's browser.

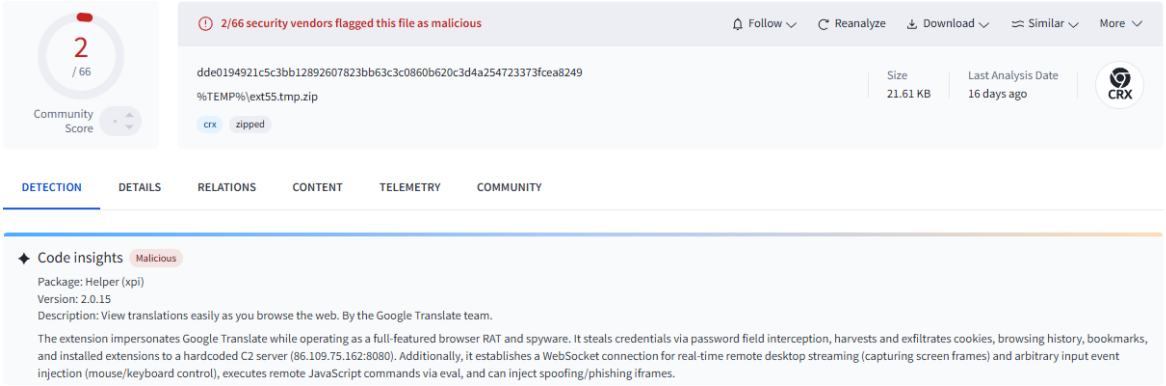


Figure 20: Malicious extension associated with Lunex. Source: https://www.virustotal.com/gui/file/dde0194921c5c3bb12892607823bb63c3c0860b620c3d4a254723373fcea8249/detection

The main malicious component of the extension is a JavaScript named "**background.ts-UeeP6rC3.js**", which contains the hardcoded C2 IP address.

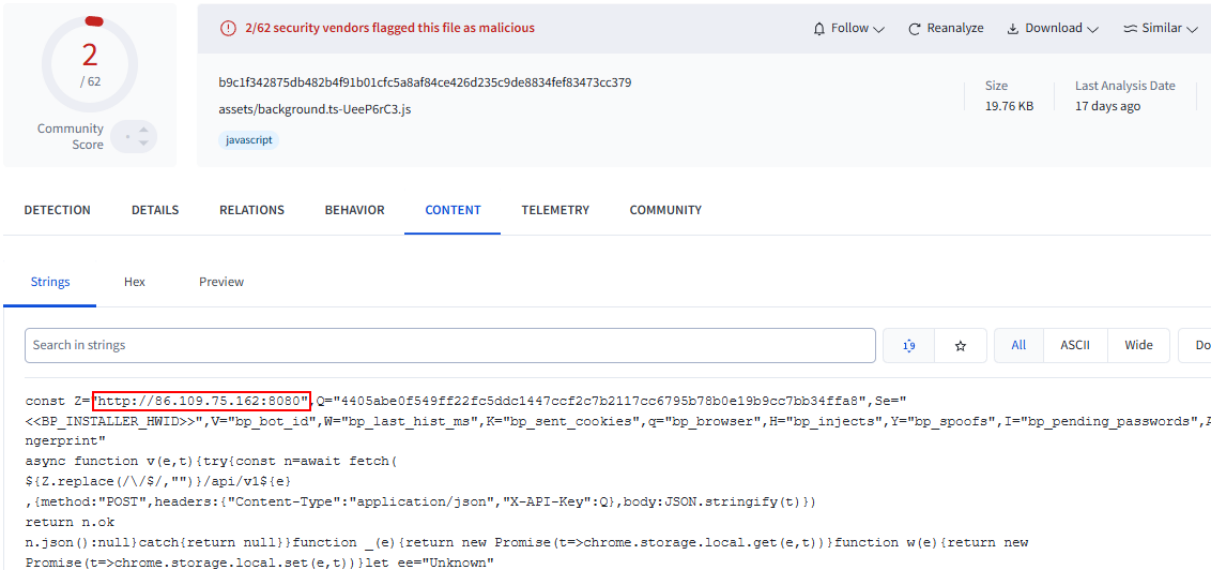


Figure 21: Malicious JavaScript inside the extension showing a hardcoded C2. Source: https://www.virustotal.com/gui/file/b9c1f342875db482b4f91b01cfc5a8af84ce426d235c9de8834fef83473cc379/content

Knowing this naming convention, we can find other malicious JavaScript components of disguised Lunex extensions.

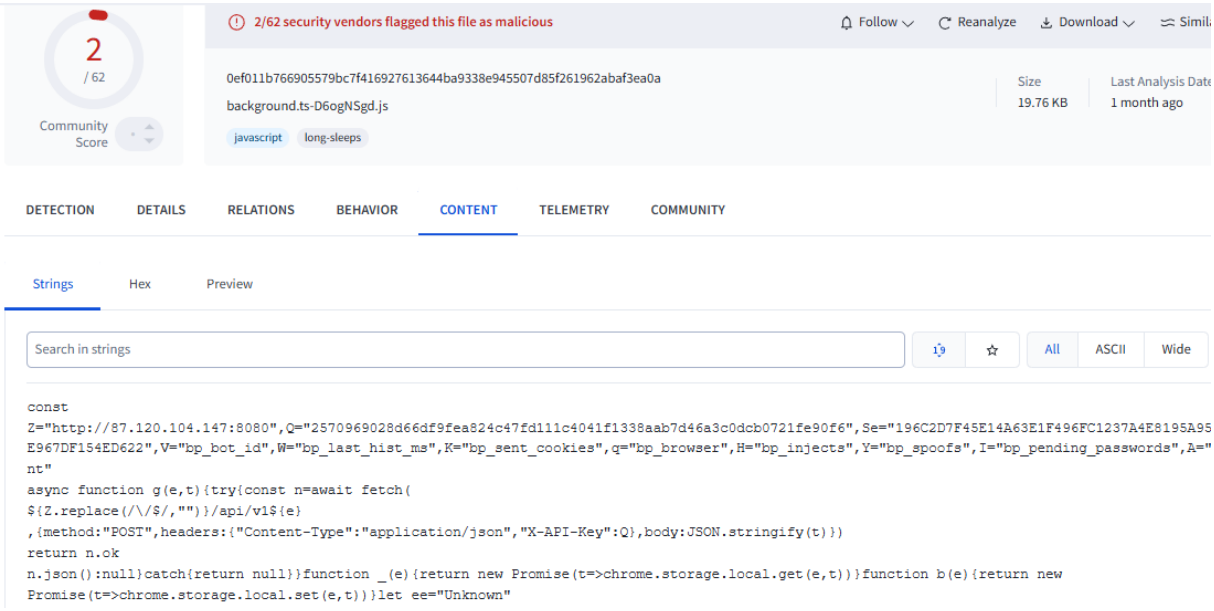


Figure 22: Another malicious JavaScript. Source: https://www.virustotal.com/gui/file/b9c1f342875db482b4f91b01cfc5a8af84ce426d235c9de8834fef83473cc379/content

The files can be searched on VirusTotal using the query depicted on the following figure.

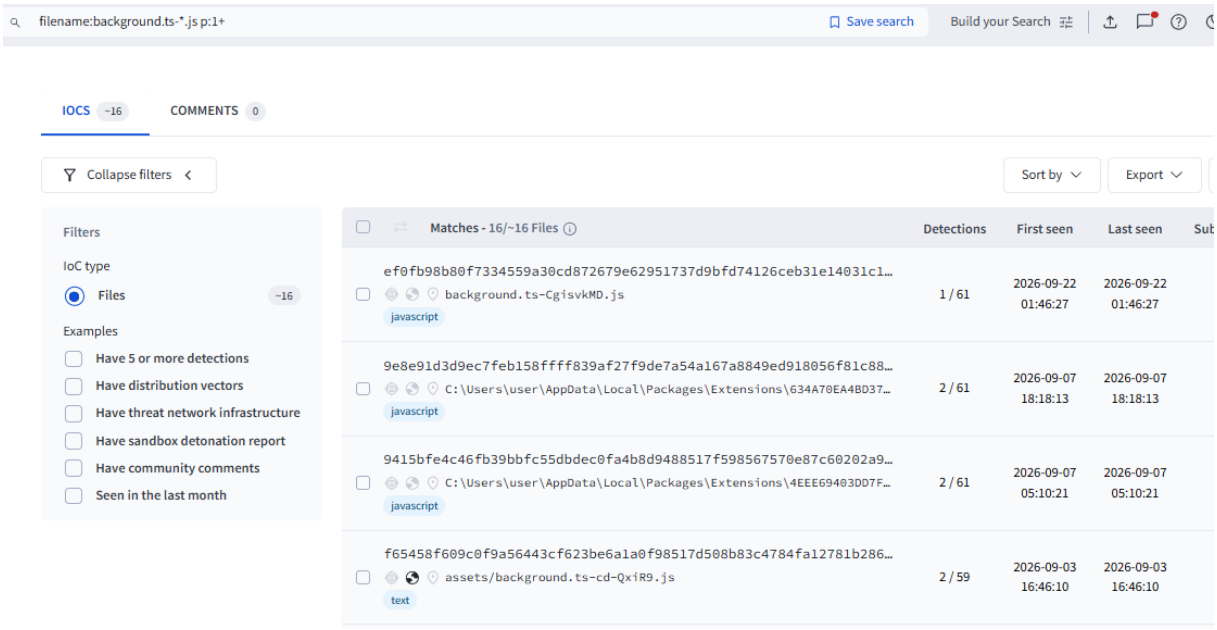


Figure 23: VirusTotal query to find other Lunex extension malicious JavaScript. Source: https://www.virustotal.com/gui/search?query=filename%3Abackground.ts-.js+p%3A1%2B&type=files*

We also noticed that the engine detection query below (**rising:"Stealer.BPRemote/JS!1.14543 (CLASSIC)"**) can return samples associated with Lunex, and additional malicious extensions.

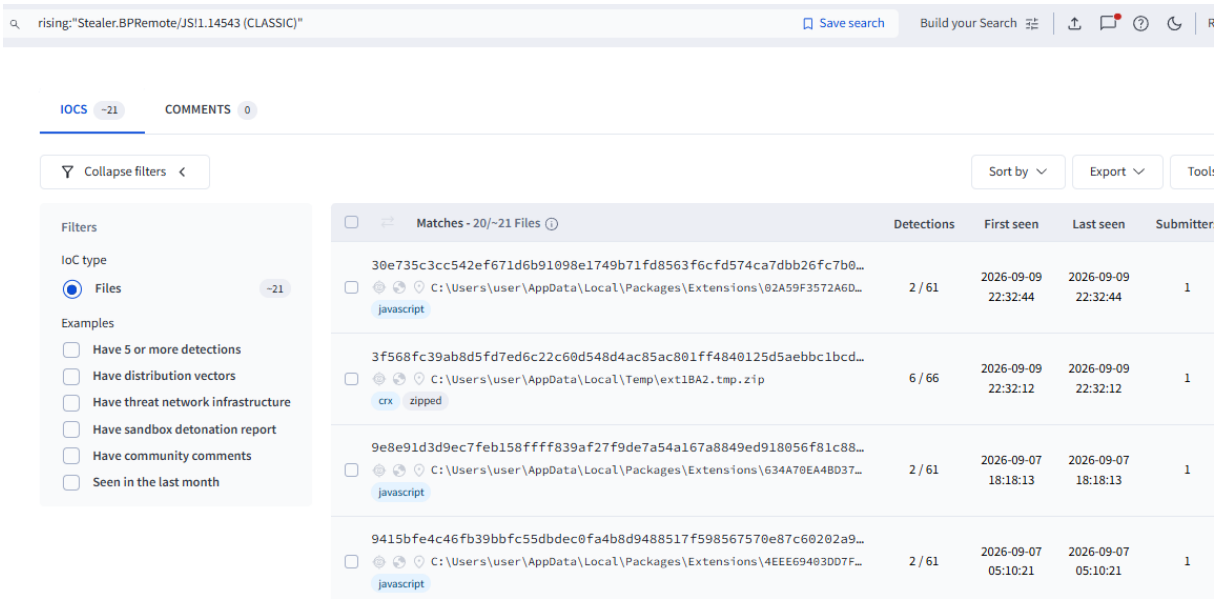


Figure 24: Another VirusTotal query. Source: https://www.virustotal.com/gui/search?query=rising%3A%22Stealer.BPRemote%2FJS%211.14543+%28CLASSIC%29%22&type=files

Interestingly, we found an extension in Cyrillic masquerading as a **Redactor for Microsoft Office Word.** The fact that it is in Cyrillic may not directly mean that it targets Russian users, as threat actors usually restrict their tools against Russia and its partners, but it may

however target Ukrainian users. The description of the tool is “Work with Word, Excel and PowerPoint files in Google Docs, Google Sheets and Google Slides.”

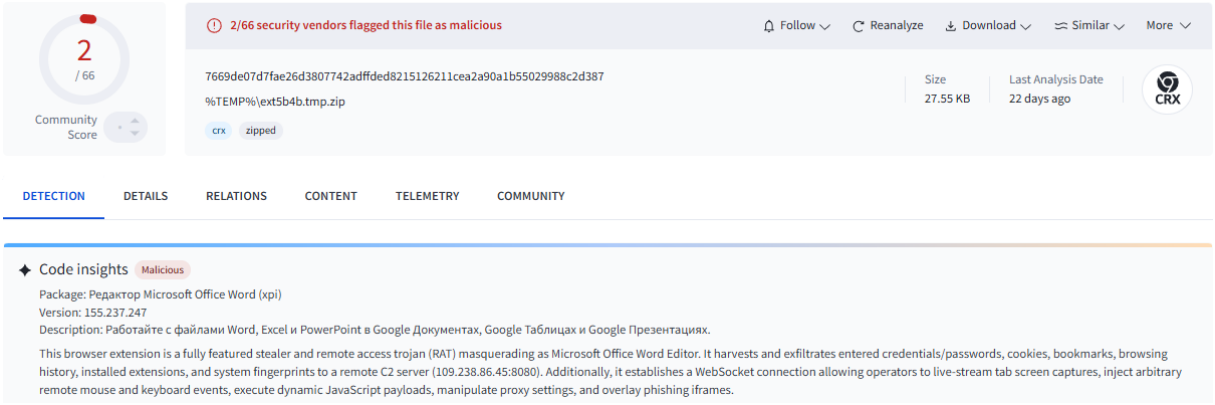


Figure 25: Malicious extension. Source: https://www.virustotal.com/gui/file/7669de07d7fae26d3807742adffded8215126211cea2a90a1b55029988c2d387/detection

5.3 Other

Other tools identified on cybercrime forums also showcase malicious extensions on browsers. This specific screenshot of the thread by “rabiidd” ([PRIVATE] Windows Malware Infrastructure + Silent Browser Extension Installer + RAT + Browser Stealer) shows an Edge extension named “**Stream Player Inc V5.4.20**”. We did not find this extension on the Edge store, which can either mean that it was taken down since the screenshot was uploaded, or that it is an extension that is installed directly on the victim’s browser.

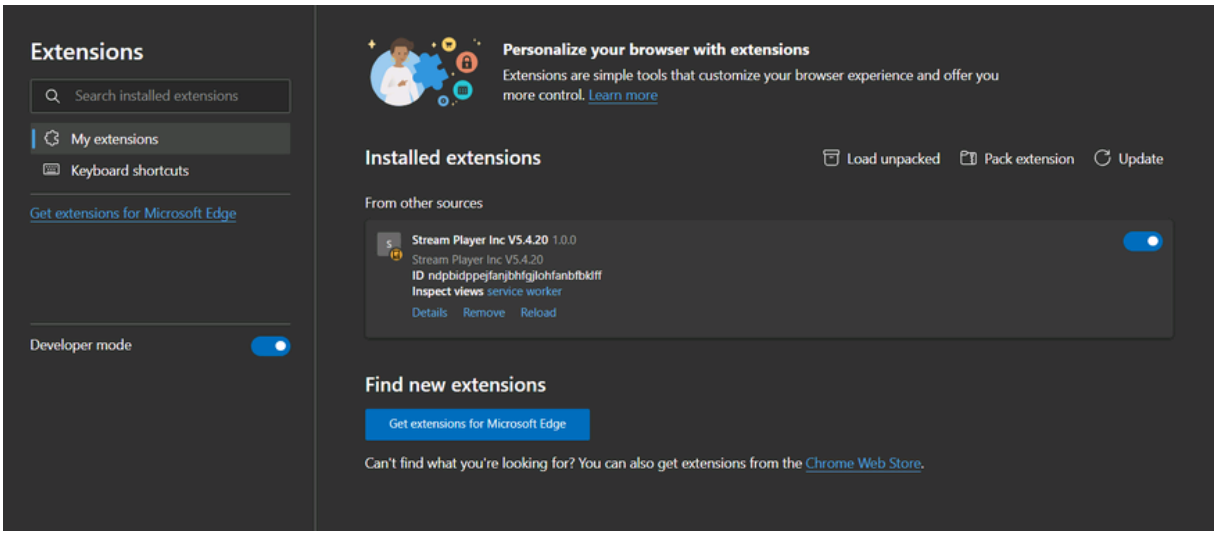


Figure 26: Malicious extension from the “Silent Browser Extension Installer” tool. Source: hxxps://forum.exploit.in/topic/285514/

6. Actionable content

6.1 Indicators of compromise

Value	Type	Description
62.60.226[.103	Ipv4	Lunex panel
84.32.149[.103	Ipv4	Lunex panel
86.109.75[.162	Ipv4	Lunex panel
87.58.201[.224	Ipv4	Lunex panel
87.120.104[.147	Ipv4	Lunex panel
87.129.104[.148	Ipv4	Lunex panel
91.92.34[.243	Ipv4	Lunex panel
95.179.159[.159	Ipv4	Lunex panel
103.101.85[.123	Ipv4	Lunex panel
109.238.86[.45	Ipv4	Lunex panel
109.238.86[.48	Ipv4	Lunex panel
109.238.87[.205	Ipv4	Lunex panel
130.12.180[.187	Ipv4	Lunex panel
132.243.235[.195	Ipv4	Lunex panel
152.232.132[.254	Ipv4	Lunex panel
176.53.159[.98	Ipv4	Lunex panel
193.178.159[.128	Ipv4	Lunex panel
194.165.16[.55	Ipv4	Lunex panel
217.77.15[.181	Ipv4	Lunex panel
45.227.254[.53	Ipv4	Needle panel
45.227.254[.161	Ipv4	Needle panel
45.227.254[.162	Ipv4	Needle panel
46.29.26[.167	Ipv4	Needle panel
62.238.113[.106	Ipv4	Needle panel
84.201.6[.21	Ipv4	Needle panel
87.120.104[.213	Ipv4	Needle panel
89.34.90[.31	Ipv4	Needle panel
93.152.223[.154	Ipv4	Needle panel
93.152.223[.199	Ipv4	Needle panel
95.81.77[.88	Ipv4	Needle panel
95.179.181[.208	Ipv4	Needle panel
104.251.181[.138	Ipv4	Needle panel
130.12.180[.135	Ipv4	Needle panel
136.244.100[.54	Ipv4	Needle panel
158.94.209[.204	Ipv4	Needle panel
178.16.52[.194	Ipv4	Needle panel
209.99.189[.205	Ipv4	Needle panel

67.205.42[.190	Ipv4	Associated with StegoAD campaign
ef0fb98b80f7334559a30cd872679e62951737d9bfd74126ceb31e14031c17a1	Sha-256	Malicious Js linked to Lunex extension
9e8e91d3d9ec7feb158ffff839af27f9de7a54a167a8849ed918056f81c88489	Sha-256	Malicious Js linked to Lunex extension
9415bfe4c46fb39bbfc55dbdec0fa4b8d9488517f598567570e87c60202a9d2a	Sha-256	Malicious Js linked to Lunex extension
f65458f609c0f9a56443cf623be6a1a0f98517d508b83c4784fa12781b286dbf	Sha-256	Malicious Js linked to Lunex extension
1478eb5c762d9aa9a6f43af72e2f55503a4efd7dd2ddce653564a294a6ecd0d4	Sha-256	Malicious Js linked to Lunex extension
380ab9440c58659408c49b966bf471ae310da75fb67d654b4932d4b19dc34096	Sha-256	Malicious Js linked to Lunex extension
e0d7be05ed053324d828bc829ae62bf409ca0582fd82a8f8c7d12529e8271910	Sha-256	Malicious Js linked to Lunex extension
3c0e59896bc2b7c1f30844fc8c6859bd92fc973628b5819d75f71910367b45b9	Sha-256	Malicious Js linked to Lunex extension
cf95da087df12e998dc295b25f371bb7ebfb96596cc26b023c974ca58d5cb99f	Sha-256	Malicious Js linked to Lunex extension
ab513e760c7b6bdbdc8920ea8d046b071586d9b66cf25aeb8f932aafb3b3af04	Sha-256	Malicious Js linked to Lunex extension
60d7b83983650fc092d17fd0b8794da975b430c19b819fb0ecde6dadd64ecc91	Sha-256	Malicious Js linked to Lunex extension
93f6c72cb21e3ea97bae9e5a43295bffdd980ebf9ecd54b8ff444e768ddcd9e9	Sha-256	Malicious Js linked to Lunex extension
1b760aa6d49d58a781de4752aa860e8cade86a2736262f1c2f548f07c4a77fc5	Sha-256	Malicious Js linked to Lunex extension
9bb59653b716e8d9f4a4c56cace5eb853dc14da7b1aabfd34a80cd4c327cc2ab	Sha-256	Malicious Js linked to Lunex extension
0ef011b766905579bc7f416927613644ba9338e945507d85f261962abaf3ea0a	Sha-256	Malicious Js linked to Lunex extension
9bee0cb99f7c8cf978469c9a1850b8e9ce738355cc4881f40a69339e2b585787	Sha-256	Malicious Js linked to Lunex extension
30e735c3cc542ef671d6b91098e1749b71fd8563f6cfd574ca7dbb26fc7b0f47	Sha-256	Malicious Js linked to Lunex extension
549b9875eee9d87d2df668ad465d7eaf89bd8f05b1c72018d88309a0e4594ea4	Sha-256	Malicious Js linked to Lunex extension
dfef2c3b1f59071598a69fcff0ef7cbdfb2bb6ba2e95959fa86a51abee308343	Sha-256	Needle stealer sample

6.2 Recommendations

- **Block the IOCs** provided in the "Indicators of compromise" section of this analysis and subscribe to a CTI feed to obtain fresh IOCs related to cyber threats. Intrinsec offers its own **CTI feed** to enhance your detection and response capabilities: https://www.intrinsec.com/en/cyber-threat-intelligence-feeds/
- **Use a threat intelligence service** to be alerted on relevant evolution surrounding this ecosystem and other threats.
- **Use a credentials leak service** to monitor and renew leaked valid corporate accesses to your assets.
- **User Training**: Educating employees and contractors on recognizing, reporting, and preventing cyber threats that rely on human interaction, such as phishing, social engineering, and other manipulative techniques. Comprehensive training programs create a human firewall by empowering users to be an active component of the organization's cybersecurity defenses.
- **User Account Management**: Implementing and enforcing policies for the lifecycle of user accounts, including creation, modification, and deactivation. Proper account management reduces the attack surface by limiting unauthorized access, managing account privileges, and ensuring accounts are used according to organizational policies.
- **Restricting web-based content**: Enforcing policies and technologies that limit access to potentially malicious websites, unsafe downloads, and unauthorized browser behaviors. This can include URL filtering, download restrictions, script blocking, and extension control to protect against exploitation, phishing, and malware delivery.
- **Restricting file and directory permissions**: Setting access controls at the file system level to limit which users, groups, or processes can read, write, or execute files. By configuring permissions appropriately, organizations can reduce the attack surface for adversaries seeking to access sensitive data, plant malicious code, or tamper with system files.
- **Password policies:** Set and enforce secure password policies for accounts to reduce the likelihood of unauthorized access. Strong password policies include enforcing password complexity, preventing password reuse.
- **Network Intrusion Prevention**: Use intrusion detection signatures to block traffic at network boundaries.
- **Multi-Factor Authentication (MFA)**: Enhances security by requiring users to provide at least two forms of verification to prove their identity before granting access. These

factors typically include passwords, PINs, physical tokens, smartphone authenticator apps, biometric data (fingerprints, facial recognition, or retinal scans).

- **Limit Software Installation**: Prevent users or groups from installing unauthorized or unapproved software to reduce the risk of introducing malicious or vulnerable applications. This can be achieved through allowlists, software restriction policies, endpoint management tools, and least privilege access principles.
- **Filter Network Traffic**: Employ network appliances and endpoint software to filter ingress, egress, and lateral network traffic. This includes protocol-based filtering, enforcing firewall rules, and blocking or restricting traffic based on predefined conditions to limit adversary movement and data exfiltration.
- **Execution Prevention**: Prevent the execution of unauthorized or malicious code on systems by implementing application control, script blocking, and other execution prevention mechanisms. This ensures that only trusted and authorized code is executed, reducing the risk of malware and unauthorized actions.
- **Behavior Prevention on Endpoint**: Use of technologies and strategies to detect and block potentially malicious activities by analyzing the behavior of processes, files, API calls, and other endpoint events. Rather than relying solely on known signatures, this approach leverages heuristics, machine learning, and real-time monitoring to identify anomalous patterns indicative of an attack.
- **Code Signing**: Ensures the authenticity and integrity of software by digitally signing executables, scripts, and other code artifacts. It prevents untrusted or malicious code from executing by verifying the digital signatures against trusted sources.
- **Audit**: Auditing is the process of recording activity and systematically reviewing and analyzing the activity and system configurations. The primary purpose of auditing is to detect anomalies and identify potential threats or weaknesses in the environment.
- **Software updates**: Ensure systems are protected against known vulnerabilities by applying patches and upgrades provided by vendors. Regular updates reduce the attack surface and prevent adversaries from exploiting known security gaps.
- **Software configuration**: Making security-focused adjustments to the settings of applications, middleware, databases, or other software to mitigate potential threats. These changes help reduce the attack surface, enforce best practices, and protect sensitive data.
- **Pre-compromise mitigations**: Proactive measures and defenses implemented to prevent adversaries from successfully identifying and exploiting weaknesses during the Reconnaissance and Resource Development phases of an attack. These activities focus on reducing an organization's attack surface, identify adversarial

preparation efforts, and increase the difficulty for attackers to conduct successful operations.

- **Data Loss Prevention**: Implementing strategies and technologies to identify, categorize, monitor, and control the movement of sensitive data within an organization. This includes protecting data formats indicative of Personally Identifiable Information (PII), intellectual property, or financial data from unauthorized access, transmission, or exfiltration.

6.3 Tactics, Techniques and Procedures

ID	Tactic	Detail
T1583.003	Acquire Infrastructure: Virtual Private Server	Threat actors have bought IP addresses from known bulletproof and not bulletproof hosting providers
T1587.001	Develop Capabilities: Malware	Threat actors have developed malware disguised as browser extensions
T1588.001	Obtain Capabilities: Malware	Customers of malicious extension have bought the service and malware.
T1204.002	User Execution: Malicious File	Victims need to install the browser extension from browser stores, or execute a file that will install the extension in the background, to launch the kill-chain
T1036.005	Masquerading: Match Legitimate Resource Name or Location	Malicious browser extensions can masquerade as legitimate extensions from renown providers
T1678	Delay Execution	The extensions are usually legitimate before a malicious update is dropped.
T1176.001	Software Extensions: Browser Extensions	Malware can be dropped by extensions or disguised as legitimate extensions to enable malicious activity
T1005	Data from Local System	The malicious extensions can collect data from the compromised system.
T1185	Browser Session Hijacking	The malicious extensions can interact with the compromised browser, to inject content, display ads, phishing pages, intercept and modify clipboard pasted content (clipper module).
T1539	Steal Web Session Cookie	The malicious extensions can steal web session cookies.
T1555.003	Credentials from Password Stores: Credentials from Web Browsers	The malicious extensions can steal credentials stored on web Browsers.
T1071.001	Application Layer Protocol: Web Protocols	Malicious browser extensions communicate with their C2 using HTTP.
T1041	Exfiltration Over C2 Channel	Malicious browser extensions can exfiltrate data using C2 channel.
T1105	Ingress Tool Transfer	The malicious extensions can act as a dropper for other malware.
T1657	Financial Theft	The main goal of threat actors is to steal credentials for theft or to resell them.

7. Sources

- *https://microsoftedge.github.io/edgevr/assets/files/stego_ad/Microsoft_Edge_Security_StegoAd.pdf*
- *https://socket.dev/blog/chrome-edge-extension-wallet-drainer*
- *https://www.malwarebytes.com/blog/threat-intel/2026/04/malicious-trading-website-drop-malware-that-hands-over-your-browser-to-attackers*
- *https://www.elastic.co/security-labs/threat-command/malicious-browser-extension-kremlin-banking-malware*
- *https://socradar.io/blog/peep-browser-rat-chrome-extension/*