The Hidden Threat of Free VPN Browser Plugins: A Cybersecurity Blind Spot in Enterprise Environments

Executive Summary

Free VPN browser extensions promise convenience and anonymity but often introduce significant risk into enterprise environments. These plugins frequently operate in the background, exfiltrate data, connect to blacklisted IP addresses, and potentially inject malicious code. This whitepaper presents real-world behavioral evidence, outlines the associated threats, and provides concrete recommendations to help organizations protect their networks.

Findings

During recent investigations, suspicious network behavior was identified originating from a browser process, specifically msedge.exe. Without any active user interaction, the system initiated multiple outbound connections to domains and IP addresses linked to known APT28 infrastructure. These connections included persistent communication with endpoints such as *.pipedream.net, a domain commonly used for dynamic payload delivery and telemetry exfiltration.

The activity occurred during off-hours, indicating that the connections were not user-driven but automated—likely the result of a browser plugin operating silently in the background. This behavior is consistent with botnet beaconing or data exfiltration patterns and clearly bypasses standard endpoint activity monitoring tied to active user sessions.

While no direct evidence of code injection was detected during this case, the context strongly suggests the possibility. The domains contacted are historically associated with credential harvesting, malicious JavaScript injection, and session token theft. This, coupled with the behavior of the browser plugin, supports the conclusion that code injection is a highly probable risk.

Case Study and Evidence: Background VPN Plugin Activity Linked to APT28

On June 11 and on 15, 2025, several endpoints triggered multiple alerts due to outbound communication with blacklisted IP addresses attributed to APT28. Over an 8-minute window, the device connected to at least seven different suspicious IPs and one dynamic domain. All traffic originated from the Edge browser, and the system was unattended at the time of activity.

ClientId	VeloFqdn	Identifier	MalCheck	CyberHavenIOC	Author	Name	Version
C.95e8ad239eb5c6da	[redacted]	fmdmnjcgegbabdefddkijefeadkhchcn	Unknown	False	__MSG_author__	Помощник диагностики	3.0.27_0
C.95e8ad239eb5c6da	[redacted]	nhbmmgegnhdhkcclaandbaipceebnckc	Unknown	False	__MSG_author__	Контур.Расширение	3.2.10_0
C.95e8ad239eb5c6da	[redacted]	kcijpkomlnpfpjmkbghnnmflfebimpfg	Unknown	False	null	3CX Click2Call	5.0.0.171_0
C.95e8ad239eb5c6da	[redacted]	aapbdbdomjkkjkaonfhkkikfgjllcleb	Malicious	False		Google Translate	2.0.16_0
C.95e8ad239eb5c6da	[redacted]	fjnehcbecaggobjholekjijaaekbnlgj	Unknown	False	null	Browsec VPN – Free VPN for Edge	3.92.0_1
C.95e8ad239eb5c6da	[redacted]	jlhmfgmfgeifomenelglieieghnjghma	Malicious	False	null	Cisco Webex Extension	2.0.4_0
C.95e8ad239eb5c6da	[redacted]	odfafepnkmbhccpbejgmiehpchacaeak	Unknown	False	Raymond Hill & contributors	uBlock Origin	1.64.0_0
C.95e8ad239eb5c6da	[redacted]	mkejgcgkdldbggjhhflekkondicpnop	Unknown	False	eff.software.projects@gmail.com	Privacy Badger	2025.5.30_0

Forensic Analysis with Velociraptor

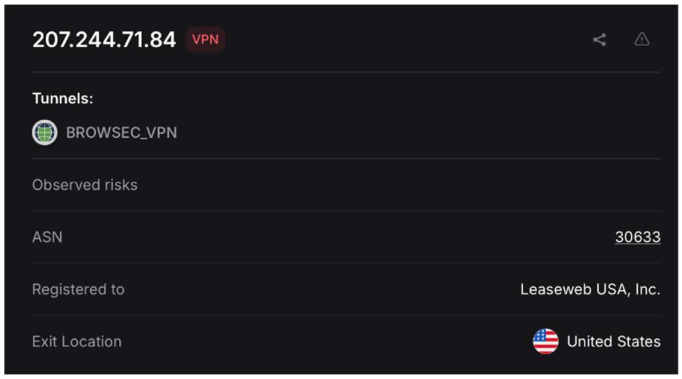
```
| where InitiatingProcessFileName in~ ("msedge.exe", "chrome.exe")
| project Timestamp, DeviceName, RemoteIP, RemoteUrl, InitiatingProcessFileName, InitiatingProcessCommandLine, ReportId
```

Getting started | Results | Query history

Export | Show empty columns | 1021 items | Search | 00:01.697 | Low | Chart type

Timestamp	DeviceName	RemoteIP	RemoteUrl	InitiatingProcessFileName	InitiatingProcessCommandL...	ReportId
Jun 11, 2025 12:37...	[redacted]	83.136.250.211	uk1.speedstream.live	msedge.exe	"msedge.exe" --type=ut...	2542
Jun 11, 2025 12:37...	[redacted]	217.12.210.35	ua3.fastfetch.info	msedge.exe	"msedge.exe" --type=ut...	2541
Jun 11, 2025 12:37...	[redacted]	185.123.100.161	tr1.datadispatch.xyz	msedge.exe	"msedge.exe" --type=ut...	2534
Jun 11, 2025 12:37...	[redacted]	192.71.244.113	si3.quickcache.click	msedge.exe	"msedge.exe" --type=ut...	2528
Jun 11, 2025 12:37...	[redacted]	23.106.248.251		msedge.exe	"msedge.exe" --type=ut...	2527
Jun 11, 2025 12:37...	[redacted]	23.108.96.79	sg5.datafrenzy.org	msedge.exe	"msedge.exe" --type=ut...	2524
Jun 11, 2025 12:37...	[redacted]	23.106.249.35		msedge.exe	"msedge.exe" --type=ut...	2523
Jun 11, 2025 12:37...	[redacted]	23.106.249.34	sg2.rapidcdn.xyz	msedge.exe	"msedge.exe" --type=ut...	2522
Jun 11, 2025 12:37...	[redacted]	167.71.199.232	sg13.cachequick.info	msedge.exe	"msedge.exe" --type=ut...	2521
Jun 11, 2025 12:37...	[redacted]	46.246.9.128		msedge.exe	"msedge.exe" --type=ut...	2518
Jun 11, 2025 12:37...	[redacted]	193.42.108.84	ru6.edgecache.xyz	msedge.exe	"msedge.exe" --type=ut...	2517
Jun 11, 2025 12:37...	[redacted]	89.46.236.111	rs11.speedstream.info	msedge.exe	"msedge.exe" --type=ut...	2516
Jun 11, 2025 12:37...	[redacted]	45.153.127.239		msedge.exe	"msedge.exe" --type=ut...	2515
Jun 11, 2025 12:37...	[redacted]	5.187.33.207	pl19.streamlineddata.space	msedge.exe	"msedge.exe" --type=ut...	2514
Jun 11, 2025 12:37...	[redacted]	194.68.32.50	no1.edgecache.online	msedge.exe	"msedge.exe" --type=ut...	2513
Jun 11, 2025 12:37...	[redacted]	51.158.253.114	nl34.speedcdn.pro	msedge.exe	"msedge.exe" --type=ut...	2511

Forensic Analysis with Advanced Hunting



Forensic Analysis with Velociraptor / No Risk detected but many connections created

Indicators of Compromise (IoCs):

- IPs: 3.229.250.76, 100.25.128.170, 54.243.253.130, 34.225.42.19, etc.
- Process: msedge.exe

The machine was automatically isolated through the organization's EDR solution, effectively containing the incident.

Recommendations for CISOs and IT Leaders

- Enforce strict extension control policies via GPO or MDM (e.g., block all but whitelisted browser plugins).
- Use behavioral analytics (via Defender or Sentinel) to monitor for unusual browser activity during non-working hours.
- Isolate machines that initiate communication with known malicious infrastructure.
- Train users to understand the risks of "free" browser extensions.
- Conduct regular browser extension audits across the environment.

Conclusion

- Free VPN browser plugins represent a growing attack vector. Enterprises must treat browser extensions as part of their endpoint attack surface and enforce corresponding controls. Behavioral evidence shows that such plugins are not just a privacy risk—they can act as a launchpad for advanced persistent threats.

Further Reading and References

1. **Ars Technica – "Hola VPN used to perform DDoS attacks, violate user privacy"**
   https://arstechnica.com/information-technology/2015/06/hola-vpn-used-to-perform-ddos-attacks-violate-user-privacy/ cisomag.com
2. **McAfee – "Attention Android Users: This Free VPN App Leaked the Data of 21 Million Users"**
   https://www.mcafee.com/blogs/privacy-identity-protection/attention-android-users-this-free-vpn-app-leaked-the-data-of-21-million-users/
   techradar.com+9mcafee.com+9cybernews.com+9
3. **TechRadar – "This free VPN leaked data from millions of users online"**
   https://www.techradar.com/news/this-free-vpn-leaked-data-from-millions-of-users-online-find-out-if-youre-affected adguard.com+14techradar.com+14techradar.com+14
4. **Cybernews – "One of the biggest Android VPNs hacked? Data of 21 million users from 3 Android VPNs put for sale"**
   https://cybernews.com/security/one-of-the-biggest-android-vpns-hacked-data-of-21-million-users/ cybernews.com+4cybernews.com+4adguard.com+4
5. **Kaspersky – "Fake VPN apps on Google Play"**
   https://www.kaspersky.com/blog/fake-vpn-apps-google-play/45679/
   cybernews.com+13cybernews.com+13mcafee.com+13
6. **ZDNet – "Google removed 500 malicious Chrome extensions"**
   https://www.zdnet.com/article/google-removed-500-malicious-chrome-extensions/
7. **CISA – Malicious browser extensions advisories**
   https://www.cisa.gov/news-events/cybersecurity-advisories

Blacklisted Domains

webhook.site
mocky.io
pipedream.net
frge.io
dynu.com
mockbin.org
ngrok.io
urlbae.com
rf.gd
000.pe
1cooldns.com
42web.io
4cloud.click
accesscan.org
bumbleshrimp.com
camdvr.org
casacam.net
ddnsfree.com
ddnsgeek.com
ddnsguru.com
dynuddns.com
dynuddns.net
free.nf
freeddns.org
glize.com
great-site.net
infinityfreeapp.com
kesug.com
loseyourip.com
lovestoblog.com
mockbin.io
mybiolink.io
mysynology.net
mywire.org
ooguy.com
webhookapp.com
webredirect.org
wuaze.com
lopeid.com

Blacklisted IPs

207.244.71.84
31.135.199.145
79.184.25.198
91.149.253.204
103.97.203.29
162.210.194.2
31.42.4.138
79.185.5.142
91.149.254.75
209.14.71.127
46.112.70.252
83.10.46.174
91.149.255.122
109.95.151.207
46.248.185.236
83.168.66.145
91.149.255.19
64.176.67.117
83.168.78.27
91.149.255.195
64.176.69.196
83.168.78.31
91.221.88.76
64.176.70.18
83.168.78.55
93.105.185.139
64.176.70.238
83.23.130.49
95.215.76.209
64.176.71.201
83.29.138.115
138.199.59.43
70.34.242.220
89.64.70.69
147.135.209.245
70.34.243.226
90.156.4.204
178.235.191.182
70.34.244.100
91.149.202.215
178.37.97.243
70.34.245.215
91.149.203.73
185.234.235.69
70.34.252.168
91.149.219.158

70.34.252.186
91.149.219.23
194.187.180.20
70.34.252.222
91.149.223.130
212.127.78.170
70.34.253.13
91.149.253.118
213.134.184.167
70.34.253.247
91.149.253.198
70.34.254.245
91.149.253.20