TIR-20260909 The PseudoTDS and PhantomJack Browser Hijacking Campaign

9/9/2026

Prepared for:

Aspire Technology Partners
25 James Way
Eatontown, NJ 07724

NOTICE:

This document is marked TLP: CLEAR, allowing recipients to share this information globally without any disclosure limitations.

This report is governed by the terms outlined in the Master Services Agreement (MSA) or any other master agreement between Aspire Technology Partners and the client receiving this report, along with the Statement of Work (SOW) or Order detailing the services that led to its creation.

Contributor(s)

Portia S. Cole
CTI Threat Researcher
Aspire Technology Partners
pcole@aspiretransforms.com

TABLE OF CONTENTS

Executive Summary

The chain begins with something ordinary - a mistyped web address. From there, PseudoTDS and PhantomJack work together to turn that small mistake into a browser compromise. PseudoTDS handles delivery, filtering visitors and steering selected users toward a fake security check. PhantomJack is the payload waiting at the end of that process. It is a browser hijacker typically disguised as a privacy or security tool, and in several cases it has been distributed through the Microsoft Store, which can make the download look more trustworthy than it is.

The campaign is similar to ClickFix, which also uses a fake CAPTCHA or security prompt to convince users that an unusual step is required. The difference is what happens next. ClickFix tells the user to paste and run a command. PseudoTDS tells the user to download a launcher and install a malicious MSIX application. Both attacks rely on the user completing that step.

Two recent security incidents, observed by Aspire's SOC, show what this looks like in a real environment. In the first, several suspicious MSIX files were found across multiple devices, and in the second, a PhantomJack-linked executable ran multiple times on one device. These cases show that a clean scan or an unidentified source website doesn't rule out risk on its own. However, confirming what actually happened, and that remediation was completed, is what closes the loop.

TIR SUMMARY

ASPIRE

TLDR;

- PseudoTDS filters and redirects mistyped-URL traffic toward a fake security check. PhantomJack is the browser hijacker waiting at the end of that chain.
- PhantomJack masquerades as a privacy, security, or file-sharing tool.
- PhantomJack can read browser bookmarks and history. It also replaces default search engines in Chrome, Edge, and Firefox/installs unauthorized extensions.
- The campaign shares tactics with ClickFix, including fake CAPTCHA and security prompts.
- Trinity Cyber disclosed the campaign on November 5, 2025. They had found 45 landing-page domains and 16 active PhantomJack apps on the Microsoft Store.
- Two security incidents from August show the pattern in practice. One involved several suspicious MSIX files across multiple devices. The other involved a PhantomJack-linked executable that ran repeatedly on a single device.
- MSIX or app downloads should be investigated. Confirm remediation even when scans come back clean or the source site can't be traced.

PseudoTDS and PhantomJack

As mentioned earlier, PseudoTDS and PhantomJack are two parts of the same operation. PseudoTDS controls how selected users reach the malicious application, while PhantomJack changes what happens inside the browser after installation. Understanding that division makes the attack much easier to follow.

PhantomJack

PhantomJack is a browser hijacker first documented and named by Trinity Cyber. It is not ransomware or a remote access trojan; its purpose is to alter browsing and profit from redirected traffic.

The applications are designed to look like legitimate software. Common themes include privacy tools, browser utilities, file-sharing programs, and security applications. They are packaged as MSIX files, and some were available through the Microsoft Store. Because users often associate official storefronts with safety, the applications may appear trustworthy even when they are not.

PhantomJack is built using NW.js, a framework commonly used to package web applications as desktop software. Researchers found that the applications interact directly with browsers and can modify settings such as the default search provider. Some variants were also observed accessing browser data and installing extensions without the user's knowledge.

- **Threat type -** Browser hijacker, adware, and potentially unwanted application.
- **Earliest documented activity -** PhantomJack applications were present in the Microsoft Store by April 2024, and the broader activity was underway by mid-2024.
- **Common disguises -** Privacy browsers, security utilities, file-sharing tools, PDF applications, and monitoring tools.
- **Delivery format -** MSIX applications containing NW.js-based executables.
- **Known capabilities -** Browser information collection, search-engine replacement, and unauthorized extension installation.
- **Attribution -** The operator, country of origin, targeted industries, and confirmed victim list is unknown.

PseudoTDS

PseudoTDS is not the malware installed on the device. It is the name given to the redirection and filtering system that delivers users to PhantomJack. It resembles a traffic distribution system (TDS) and uses the Trillion-advertising network during several stages of the operation.

The chain often begins when a user mistypes a web address and lands on a typosquatted domain. Instead of reaching the intended website, the visitor is routed through a series of redirects designed to identify legitimate users and filter out automated scanners and security tools. Selected visitors are then directed through advertising infrastructure and DGA-generated domains before arriving at a fake CAPTCHA or security verification page.

If the user completes the verification prompt, a small .NET launcher opens a PhantomJack application listing in the Microsoft Store. From there, the user is encouraged to download and install the application, which is delivered as an MSIX package.

- **Threat type -** Malicious traffic filtering and application-delivery system.
- **Observed since -** At least mid-2024, based on the earliest PhantomJack applications identified during the research.
- **Entry point -** Typosquatted domains capturing mistyped traffic.
- **Infrastructure and tools -** Trillion AdTech, JavaScript redirects, HTTP 302 redirects, Cloudflare-hosted infrastructure, DGA-generated domains, Google tracking IDs, and a .NET Store launcher.
- **Final payload -** PhantomJack applications delivered as MSIX packages.
- **Attribution -** No public source currently identifies the operator or its location.

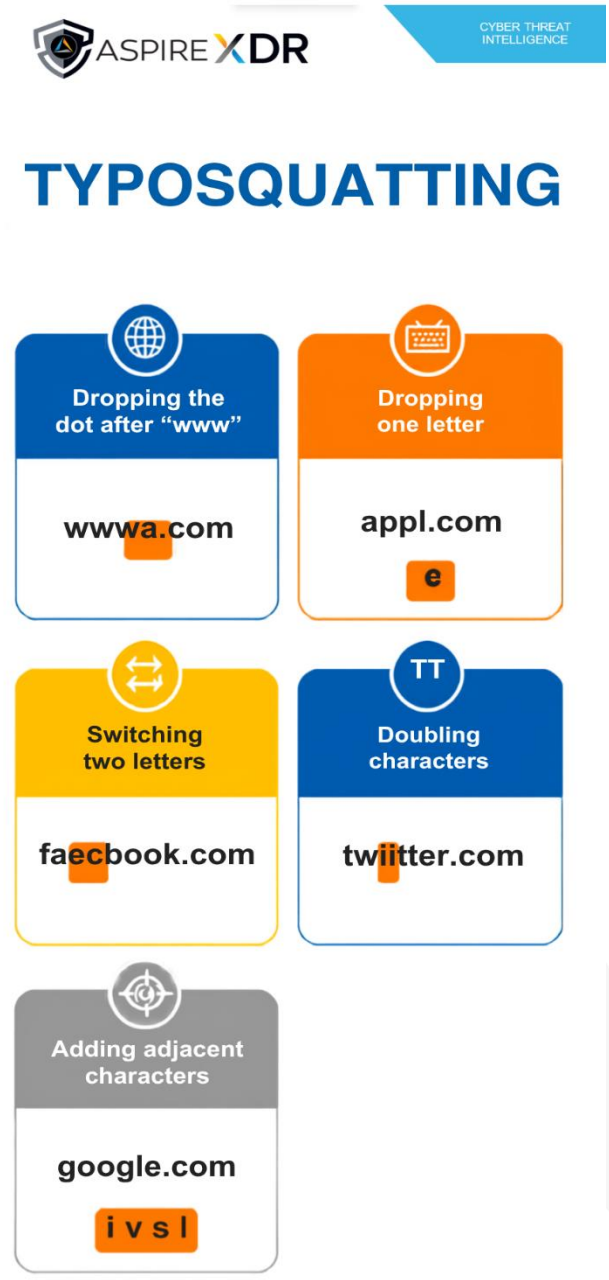
TYPOSQUATTING AND BROWSER HIJACKING

It's important to understand both techniques because one brings the user into this operation and the other explains the result.

Typosquatting

Typosquatting uses a domain that is a small variation of a legitimate address. It may omit or reverse letters, add a hyphen, or use a look-alike character. A user typing quickly may not notice the difference.

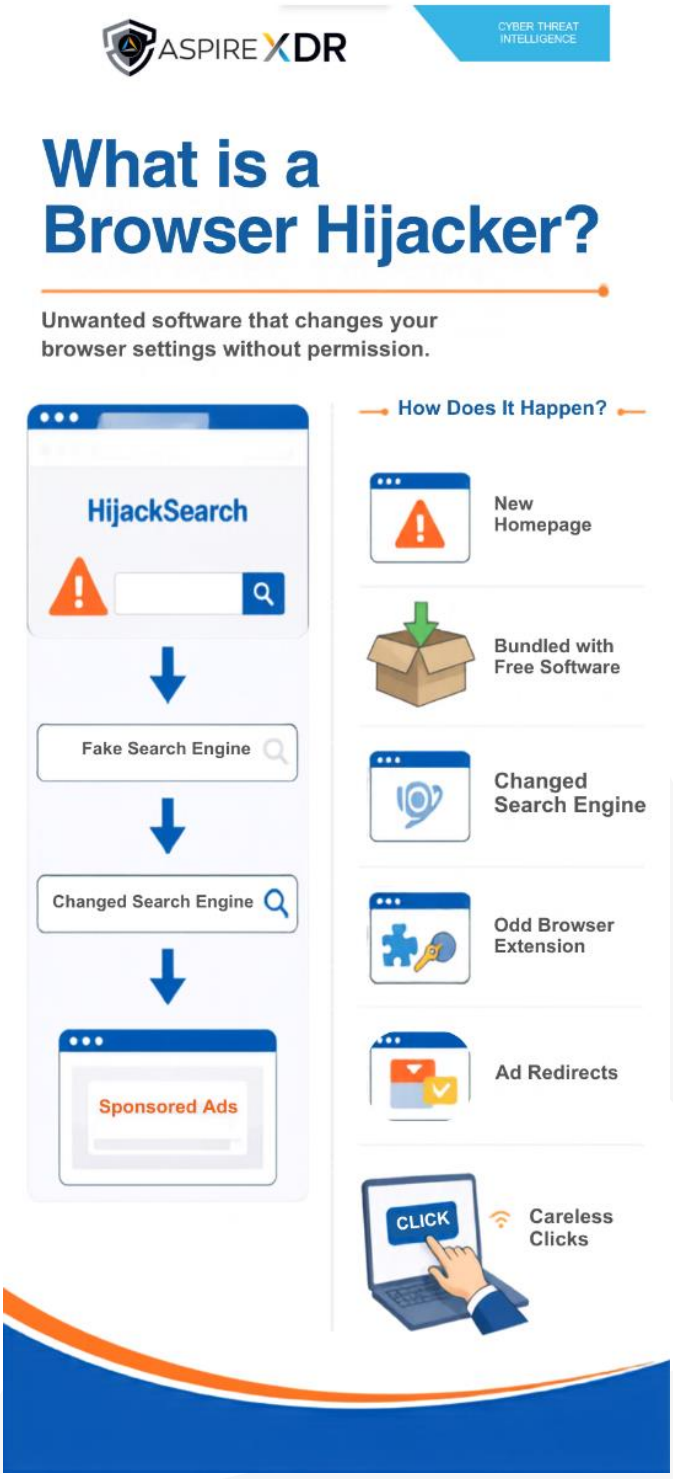
Here, the false domain is the doorway rather than the destination. It can route visitors through advertising infrastructure, show harmless content to scanners, and reserve the malicious path for selected users. A padlock, CAPTCHA, or polished page does not make the address legitimate.



Browser Hijacking

A browser hijacker changes browser behavior without meaningful consent. It may replace the homepage or search provider, add extensions, insert advertisements, or redirect searches.

The damage goes beyond an annoying search page. History and bookmarks can reveal services an employee uses, internal portals, and business relationships. Unauthorized extensions can also support tracking, further redirects, or later data collection.



ASPIRE CASE STUDY

Case Study 1: Suspicious MSIX Files Found Across Multiple Devices

In late August 2026, Aspire's SOC investigated multiple PhantomJack-related installers discovered throughout a user's environment. NetGuard[.]msix was found on 14 devices, HushBrowse[.]msix on 18 devices, and PrivateBrowsing2 (1)[.]msix on two devices, with some overlap between affected systems. Analysts also reviewed PrivacyShield[.]msix and SecurePass[.]msix during the investigation.

During the investigation, SOC analysts conducted a detailed review of installed software, browser extensions, execution artifacts, DNS activity, and PowerShell history across affected systems. The analysis found no evidence that the identified MSIX files had been installed or executed. One PowerShell event initially flagged for review was determined to be a command used to inspect Mark-of-the-Web metadata associated with PrivateBrowsing2 (1)[.]msix rather than execute the installer. Analysts also evaluated reports of a "Confirm you're human" prompt and subsequent redirects but were unable to collect sufficient evidence to conclusively identify the original download source.

As additional detections appeared, affected systems were isolated and scanned for signs of follow-on activity. Analysts found no suspicious processes, browser modifications, or DNS requests associated with PhantomJack. The files were quarantined, related hashes were blocked, and copies stored within roaming profiles were removed. During the investigation, Talos updated its classification of PrivacyShield[.]msix and reversed a previous false-positive determination. Although several PhantomJack-related files were identified, investigators found no evidence that the applications had executed or resulted in browser compromise.

Lessons Learned

- Close any CAPTCHA, verification page, or "Confirm you're human" prompt that requests a software download instead of granting access to a website.
- Install browser, privacy, security, and productivity applications only through your organization's approved process.

- Report unexpected downloads, redirects, or verification prompts to IT or security teams, even if the file was never opened.
- A file appearing in the Microsoft Store or using a security-related name does not **automatically make it safe**.

Case Study 2: PhantomJack-Linked Application Executes on One Device

On August 31, 2026, SentinelOne detected SafeDomainGuardian[.]exe on a user's device. The file was located within Program Files\WindowsApps, and its SHA-256 hash matched a publicly reported PhantomJack executable. The application's security-themed name and installation location allowed it to blend in with legitimate software on the system.

During the investigation, SOC analysts reviewed endpoint telemetry and confirmed that SafeDomainGuardian[.]exe had executed multiple times on the device. No additional PhantomJack-related files were identified elsewhere in the environment, and a review of DNS activity found no evidence of suspicious domain communications associated with the campaign. Although investigators were unable to determine how the file was originally delivered, the execution activity increased confidence that the application had been installed and used on the system.

The SOC immediately initiated containment measures, including device isolation, a full-disk scan, and validation that the file's hash had been added to blocklists. Because the executable remained present on the system despite detection, analysts recommended reimaging the device to ensure complete removal and eliminate any remaining risk.

Lessons Learned

- Security-themed names such as browser, privacy, or security tools should not be trusted without verification.
- Report unexpected software installations and browser changes as soon as they are noticed.
- Stop using the affected device and contact IT if an unapproved application was installed

TACTICS, TECHNIQUES. AND PROCEDURES (TTPS)

The campaign abuses legitimate services and familiar prompts to make each step look routine:

- **Domain impersonation -** Typosquatted domains capture users who mistype common addresses.
- **Target filtering -** Browser scripts collect display, window, and graphics information to separate real users from bots or sandboxes.
- **Redirect chain -** Trillion advertising infrastructure, Cloudflare-hosted services, HTTP redirects, and DGA domains move selected users toward the landing page. These services are abused infrastructure; their use does not make the providers participants in the campaign.
- **Fake verification -** A CAPTCHA or security check gives the next action a familiar reason.
- **Store launcher -** A .NET executable opens the corresponding Microsoft Store listing.
- **Application execution -** The user installs or opens an MSIX application containing the NW.js-based PhantomJack component.
- **Browser modification -** PhantomJack can read browser information, replace search engines, and add unauthorized extensions.
- **Tracking and control -** Shared Google tracking IDs link landing pages, while published domains support redirection and command-and-control activity.

HOW PSEUDOTDS AND PHANTOMJACK COMPARE TO CLICKFIX

ClickFix, PseudoTDS, and PhantomJack all rely on social engineering to convince users that an action is necessary to continue. In each case, the victim is presented with what appears to be a routine security check, verification prompt, or troubleshooting step. The objective is to create enough trust that the user willingly performs the next action, whether that involves running a command or installing an application

Similarities

ClickFix and the PseudoTDS-PhantomJack campaign both disguise malicious activity as a normal security process. Users are commonly directed to fake CAPTCHA or verification pages that make the next step appear legitimate. Both campaigns can reach victims through malicious advertising, redirects, and compromised websites, and both depend on user interaction rather than exploiting a software vulnerability.

Differences

ClickFix directs users to run commands through Windows or macOS system tools and can deliver malware. PseudoTDS begins with a typosquatted domain and fingerprints visitors. It then uses an AdTech redirect chain before a .NET launcher opens a Microsoft Store listing for the MSIX-packaged PhantomJack browser hijacker.

Aspire's CTI team has already published threat intelligence reports on FakeCaptcha and FileFix. Emergency Flash Notices have also covered the ClickFix technique in ClickLock for macOS and a Fortinet-themed FileFix campaign. This report builds on that work by covering a separate campaign that uses a familiar verification lure but ends with a malicious application installation.

Conclusion

The success of the PseudoTDS and PhantomJack campaign depends on trust. Users are presented with familiar prompts and legitimate-looking applications that make the activity appear normal. Recognizing those tactics and responding quickly to suspicious downloads or verification requests can help prevent a simple browsing mistake from becoming a larger security incident.

Recommendations

These incidents show that browser threats may look like ordinary downloads and receive changing security classifications. Users and organizations both have a role in stopping the chain.

For Users

- Check the full domain before continuing, especially after typing an address manually.
- Close any CAPTCHA or security page that asks you to download software, install an app, open the Run dialog, or paste a command.
- Install applications only through the process approved by your organization. Do not rely on the application's name or store placement alone.
- Confirm the developer and publisher with IT before installing privacy, browser, PDF, or security utilities.
- Report unexpected MSIX downloads even if you did not open them. Include the website address and a screenshot when possible.
- If an application was installed, stop using the browser and contact IT. Do not attempt to "clean" the device by deleting files before responders collect evidence.

For Organizations

- Restrict Microsoft Store and MSIX installation to approved applications and publishers through application-control policy.
- Alert on unapproved MSIX downloads, installations from user-writable directories, and execution from WindowsApps by unfamiliar publishers.
- Block the published hashes and domains, then search historical endpoint, DNS, proxy, and browser telemetry for prior contact.
- Monitor for changes to browser search providers, new extensions, and access to browser history or bookmark databases by unexpected processes.
- Review roaming profiles and synchronized folders so quarantined files do not return to other devices.
- Treat a detection that was not quarantined as unresolved until removal or reimaging is verified.
- Revisit files when vendors change a disposition. Case Study 1 shows why a previous false-positive ruling should not end future review.
- Teach employees the difference between a normal CAPTCHA and one that requests a download or system action. Include both PseudoTDS and ClickFix examples in awareness training.

MITRE MAP

***Note**: The following TTPs are based on Aspire's SOC findings during investigations.*

Initial Access	T1189 – Drive by Compromise
Execution	T1204.002 – User Execution: Malicious File
Stealth	T1036 – Masquerading

***Note**: The following TTPs are based on public reporting.*

Reconnaissance	T1592 – Gather Victim Host Information
Resource Development	T1583.001 – Acquire Infrastructure: Domains T1608.001 – Stage Capabilities: Upload Malware
Initial Access	T1189 – Drive-by Compromise:
Stealth	T1497 – Virtualization/Sandbox Evasion T1036 – Masquerading
Discovery	T1217 – Browser Information Discovery
Command and Control	T1071.001 – Application Layer Protocol: Web Protocols T1568.002 – Dynamic Resolution: Domain Generation Algorithms
Impact	T1176 – Browser Extensions

ASPIRE PROTECTS

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.

  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all

threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.

- **Aspire Managed Detection and Response (MDR)**
  - Accelerate the maturity of your security operations and reduce risk with faster threat detection and response capabilities. Aspire MDR delivers around-the-clock protection across cloud, network, and endpoints in one integrated solution.
  - Our team of experts act as an extension of your IT operations to quickly identify and mitigate security threats before they impact your business.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

INDICATORS OF COMPROMISE (IOCS)

Customer-Observed Indicators

Customer Case 1 — SHA-256 (MSIX packages)

- NetGuard[.]msix — 24ec63f3976d04f5e7a7f229ae76301bd1ca6099016d65a727d1c33459853847
- HushBrowse[.]msix — 2632787e4b1661cb73e313e8d93e6d8981bb6cafe6daada5d6ffa44d850999af
- PrivateBrowsing2 (1)[.]msix — bba03fe757280615ed3a1aee037ecefd3e4434ac17edc59838bb7b28e58c99b6

- PrivacyShield[.]msix — d36c8f2dc20938345bb5969995472ddb02b47590fb0a32613659026912447b1e
- SecurePass[.]msix — 9855d798465baf8b24e09a718846749a0dc9e462b07bc75b4a0806f1a46f6632
- SecuriGuard[.]msix — c054e260401d7b203382752666b03f334312eb019a1483fc04d348e5acbcdb5b

Customer Case 2 — SHA-256 (Executable)

- SafeDomainGuardian[.]exe — 8625846616d0c21e4624e238f2919f17f5d435f98f13bd84ee72bdb61435aa2b

Additional Anonymized Customer Detections — SHA-256 (Executables)

- NetGuard[.]exe — 228c316455d5ed69232adcbe9acd033092f200014cfa7ed40d6c382f07b19b82
- LeakGuard[.]exe — 67e8f51957b39bb3193a211161f6332e5320f1c31754d903b8822e2c1061b1a4
- SafeDrop[.]exe — 06245bdbc4b8ea1c2ec57da25cee8e4f8617ee5b0769de570fab6433c7be579e
- PrivateBrowsing[.]exe — a6023a1eb13286242318383783cb09ca702e40d086403a1521f377aed088d927
- SafeMail[.]exe — ce77601f50bc5a69110d01cf0c0b4f43be7a3df89e28f8617af8fe3a7df24ddc

Public Campaign Indicators (Trinity Cyber)

Typosquatted Entry Domains

- citymanager[.]com
- urlscanner[.]io
- lastpas[.]com
- turkishairline[.]com
- walksandiego[.]org

PhantomJack Landing Page Domains

- pgaurdroute[.]me
- pdfroute[.]app
- cool-pdf[.]app
- stealth-browse[.]app
- net-guard[.]app
- securepass[.]info
- safe-mail[.]app
- private-browsing[.]app
- watchitonline[.]app
- safe-drop[.]app
- safe-watch[.]app
- leak-guard[.]app
- safedomain-guardian[.]app
- safe-scan[.]info
- leakmonitor-live[.]app
- call-guard[.]app

Stage-One DGA Domains (Trillion AdTech Redirect Chain)

- fyabyq[.]com
- zutebo[.]com
- jyagit[.]com
- fajuez[.]com
- hodeoc[.]com
- gifowy[.]com
- kiylox[.]com
- idysuk[.]com
- jyroda[.]com

- iviqag[.]com
- hyakio[.]com
- cuyuzu[.]com

PhantomJack Command-and-Control Domains

- dislp[.]dropitsafe[.]online
- cint[.]browsingit[.]online
- cint[.]prvtbrws[.]online
- cint[.]privitosurfo[.]online
- cint[.]sfwtch[.]online
- cint[.]ntgrdnw[.]online
- cint[.]cablegaurdian[.]online
- cint[.]mailingit[.]online
- cint[.]sfml[.]online
- results[.]streamio[.]site
- chres[.]streamio[.]site
- ffres[.]streamio[.]site
- sder[.]collectitnow[.]net
- sdcr[.]collectitnow[.]net
- sdfr[.]collectitnow[.]net
- eaed[.]collectitnow[.]net
- each[.]collectitnow[.]net
- eaff[.]collectitnow[.]net

Google Campaign Tracking IDs

- G-4RGNVF5QCG
- AW-11009830956

Public PhantomJack SHA-256 — MSIX Packages

- 24ec63f3976d04f5e7a7f229ae76301bd1ca6099016d65a727d1c33459853847
- 3316a4a24270ec8b268ea07635c66de2dd0c24776b834f60529f2d9b1104479f
- d66895d8da6d5eb1d8658647c80f66dce40236c06bb600f1c62a44a657f923b3
- e9cfdcb18bb4c54802b7214a226d983c0015bb37e41a39a4d293d4e674fa94c8
- abb9c26f58962a19ea1362c859dca5b7dd59216858e38ec6c15258d1489cda38
- 0a0b6d419aa7520ff29ac5cec8d1a4a89096319774cf481127a92048566eeb91
- 961b50c8419d220d479a7e029f0cf4aeb1233ed3b21ff9f8b3bca8f23adfd434
- 06a044644b0b896c72800c9dfc1ec1770b46001a8f8a21fb3ba28949e52120ef
- c96fcb15d8fbcf555fa2f1e7502610348caa3220dd9c29fdab4d05625f0fa5e9
- bebd647687d3f57b4f1077eba829ae0353546179f2d7170faab769fae7e61c15
- bba03fe757280615ed3a1aee037ecefd3e4434ac17edc59838bb7b28e58c99b6
- afa2250fb08d3c47b09ee5dca817fd686f4196e22d834993dc8a9ac36630c22e
- ea2d72cb87c93f447be6502690328f441fdf2fa665d12938bb294bbd18855aeb
- 63f043de4e769f46838e4891e2fc96b247ebeee2806240874867ca5d343d5e33
- ff5b9aa8094e962b1803d011730c9278afbfb42aa3dac9f71ebe78449218728a
- 8ed91cb0478f21a23bbf6ca23b9577c90fe9eedff6cb3fe4effbf90a52564b9c

Public PhantomJack SHA-256 — Executable Files

- 67e8f51957b39bb3193a211161f6332e5320f1c31754d903b8822e2c1061b1a4
- 58388c8efbee568b805a80078b789e9c39b4af6d97c1029da902897e77b5ec58
- a6023a1eb13286242318383783cb09ca702e40d086403a1521f377aed088d927
- 8625846616d0c21e4624e238f2919f17f5d435f98f13bd84ee72bdb61435aa2b
- ce77601f50bc5a69110d01cf0c0b4f43be7a3df89e28f8617af8fe3a7df24ddc
- bdb67859951a4078187b8c9fdb6bd7f8e94c6ce5cf03a70c9ad96c8ef261355c
- 228c316455d5ed69232adcbe9acd033092f200014cfa7ed40d6c382f07b19b82
- 14da6bdc694a5e9106afd8e3ac46855c8a87c521eb567e76bac2d87bf6c644b8
- e0b54f6586f85d2902fde5b052e6591f6f5a9fd70319d82483e6656bf3466124

- 06245bdbc4b8ea1c2ec57da25cee8e4f8617ee5b0769de570fab6433c7be579e
- 7a2076172068d44a699ccc0e597382a05cc3a0da9b5620c9fbb6eddd1e6faf5f
- 1ee688c763ce39fce2c8e814ff18420529717d35eba6d16a73633786a134acf3
- de4980ee96d968420d3897d861a1a5cde7c3d27704a68d0067b398cbef86e6e7
- 31af13993756db91d90e3c0d8bc1904cb776eb47162000eaa0a85182b9485418
- 08bac051af00724dd688a35ae4973a82c4d7157b34ddba935dab830c62ae54dd
- d0b0aaf3bf2a21c6b5b1a899da311f400bbc8fcaa9290e1d2811a5addd5941e9
- 640088274eee03faab19c4296764a66a3c2efd9023fcf8be677a117d7725df00
- 59579af118faca431f7b464ad3a8592c467314274ccea7547153ed8d00667d40
- f71ea2a3edcd39983f7069e38bba42c13f4038607236ae73e923c841b381d1ec
- e6b69a432c63b6268acffae22125cb0a1000cb83b080f75f6072537ac7b51d58
- 4aefe15a6285587755fcae1dfb1af7b9eb8f81c512b625223fc21580115455d3
- b16f478f1469155707b7a899735d96e26be548acb5d863852533decbb4eba05f
- f80e1bbc93d645c47ea53b44f6e9917a26f5d2eab3f22b030518092ab9b5ebc0
- f9af137fc8c0232d7b52557f4276ded47f000566231617a0f6955bc28b7b1ebc
- 930f0039cbc94d9aa39311b4c2f533dc6de67f433ea3f07091b051fab145b3f9
- 84da4be52c1e1f6729b2dfcd05d84d9f9dc5fef3e906ef38dd88749f2dde9dec
- 2f025b7e289b87f6aebbc4b3264754408f11308fd6a849c0142ef4870b90990b
- f961a74f27ccb4a300d37f3546a3e8833d63fd9a32ad8ccc2252fe3a2306d439
- d046ab9588433b8009fe2185088b081dd20e21952a999221809a525712af69f1
- 296c3bdc102ce337aeeec7382e0b759bed05dd935662a58ef4ed102e5caadd14

Supporting Documentation

AdTech Abuse Delivers Hijackers Through the Microsoft Store

VirusTotalPrivacyShield

PrivacyBrowse.Msix - Resolved Malware Removal Logs - Malwarebytes Forums

What is MSIX? - MSIX | Microsoft Learn

Think before you Click(Fix): Analyzing the ClickFix social engineering technique | Microsoft Security Blog

The Art of Deception: Typosquatting to Bypass Detection

VirusTotalNetGuaurd

What Is Typosquatting? - Definition & More on Attacks | Proofpoint US

Browser Hijackers | What is a Browser Hijacker & how to remove it? | Malwarebytes Labs

SafeGuardBrowser.Msix downloaded to my computer without my knowledge - how can I tell if it installed on my pc (windows 10) - Microsoft Q&A

APPENDIX II: DISCLAIMER

This document and its contents are not intended to serve as legal advice and should not be used as a substitute for it. The results of a Security Risk Assessment are intended to guide the implementation of diligent measures to reduce the risk of potential vulnerabilities being exploited to compromise data.

While the Services and this report may offer information that the Client can use to support its compliance efforts, the responsibility for evaluating and fulfilling compliance obligations rests solely with the Client, not Aspire. This report does not guarantee or assure the Client's compliance with any law, regulation, or standard.