Malicious Appsuite PDF Editor Spreads Tamperedchef Malware

By Simon Hertzberg

Published: 2025-08-27 · Archived: 2026-04-05 20:10:58 UTC

Threat Insight

Truesec has observed what appears to be a large cybercrime campaign, involving multiple fraudulent websites promoted through a Google advertising campaign. The objective is to lure victims into downloading and installing a trojanized PDF editor, which includes an information-stealing malware dubbed **TamperedChef**. The malware is designed to **harvest sensitive data**, including credentials and web cookies.

AppSuite PDF Editor

Truesec has observed what appears to be a large campaign aiming to spread the use of a malicious pdf editor. The campaign involved multiple sites promoting a free pdf editor called “AppSuite PDF Editor”. This activity overlaps with the findings reported by researchers at Expel.

The file PDF Editor was heavily obfuscated, and the malicious code might be generated by AI/LLM.

The file installed, PDF Editor.exe had the following properties:

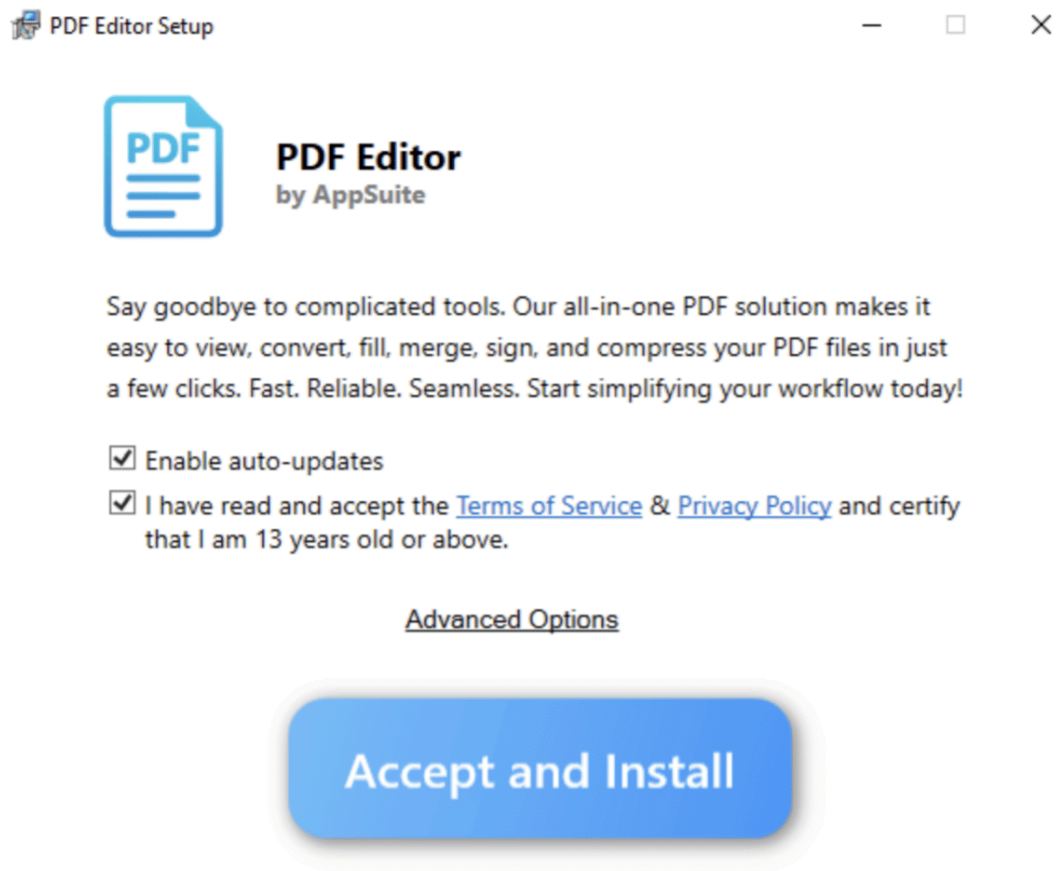
Filename: PDF Editor.exe

MD5: 6fd6c053f8fcf345efaa04f16ac0bffe

SHA1: 2ecd25269173890e04fe00ea23a585e4f0a206ad

SHA256: cb15e1ec1a472631c53378d54f2043ba57586e3a28329c9dbf40cb69d7c10d2c

When the user executes the installation file, a EULA is first prompted.



It then makes a HTTP GET request to indicate that the starting process is initiated to the following URL: hxxp[://]inst[.]productivity-tools[.]ai/status/InstallStart?v=1[.]0[.]28[.]0&p=PDFEditor&code=EN-US

It then continues to download the executable file that is the program that turns into a malware from the following URL: hxxp[://]vault[.]appsuites[.]ai/AppSuites-PDF-1[.]0[.]28[.]exe

When the installation is complete it makes two additional GET requests to confirm that all is set.

hxxp[://]inst[.]productivity-tools[.]ai/status/Download%20Complete?v=1[.]0[.]28[.]0&p=PDFEditor&code=

hxxp[://]inst[.]productivity-tools[.]ai/status/InstallDownloadComplete?v=1[.]0[.]28[.]0&p=PDFEditor&code

The following installation flow was also recorded in a network capture.

Time	Source	Destination	Protocol	Length	Request Method	Full request URI
.031074	127.0.0.1	18.64.79.24	HTTP	183	GET	http://inst.productivity-tools.ai/status/InstallStart?v=1.0.28.0&p=PDFEditor&code=EN-US
.155776	18.64.79.24	127.0.0.1	HTTP	399		
.163293	127.0.0.1	18.64.79.24	HTTP	154	GET	http://inst.productivity-tools.ai/status/InstallStart?v=1.0.28.0&p=PDFEditor&code=
.287762	18.64.79.24	127.0.0.1	HTTP	399		
.059337	127.0.0.1	18.64.79.24	HTTP	155	GET	http://inst.productivity-tools.ai/status/InstallAccept?v=1.0.28.0&p=PDFEditor&code=
.188347	18.64.79.24	127.0.0.1	HTTP	399		
.558917	127.0.0.1	3.168.217.9	HTTP	122	GET	http://vault.appsuites.ai/AppSuites-PDF-1.0.28.exe
5.452022	3.168.217.9	127.0.0.1	HTTP	1161		
5.454129	127.0.0.1	18.64.79.24	HTTP	161	GET	http://inst.productivity-tools.ai/status/Download%20Complete?v=1.0.28.0&p=PDFEditor&code=
5.576026	18.64.79.24	127.0.0.1	HTTP	399		
5.576642	127.0.0.1	18.64.79.24	HTTP	165	GET	http://inst.productivity-tools.ai/status/InstallDownloadComplete?v=1.0.28.0&p=PDFEditor&code=
5.801393	18.64.79.24	127.0.0.1	HTTP	399		
5.269260	127.0.0.1	18.64.79.24	HTTP	157	GET	http://inst.productivity-tools.ai/status/InstallComplete?v=1.0.28.0&p=PDFEditor&code=
5.422059	18.64.79.24	127.0.0.1	HTTP	399		

The Setup also adds a registry key for persistence that is executed on start-up. It contains a `--cm` arguments that gives the executable instructions how to behave.

Internet records suggests that this campaign begun on June 26, 2025, when a lot of the sites linked to the campaign were either first registered or first known to have promoted the AppSuites PDF Editor.

At first the pdf-editor appears to have behaved mostly harmless, but the code included instructions to regularly check back for potential updates in a .js file that includes the `--cm` arguments.

Records shows that PDF Editor has first been submitted to Virustotal on May 15th.

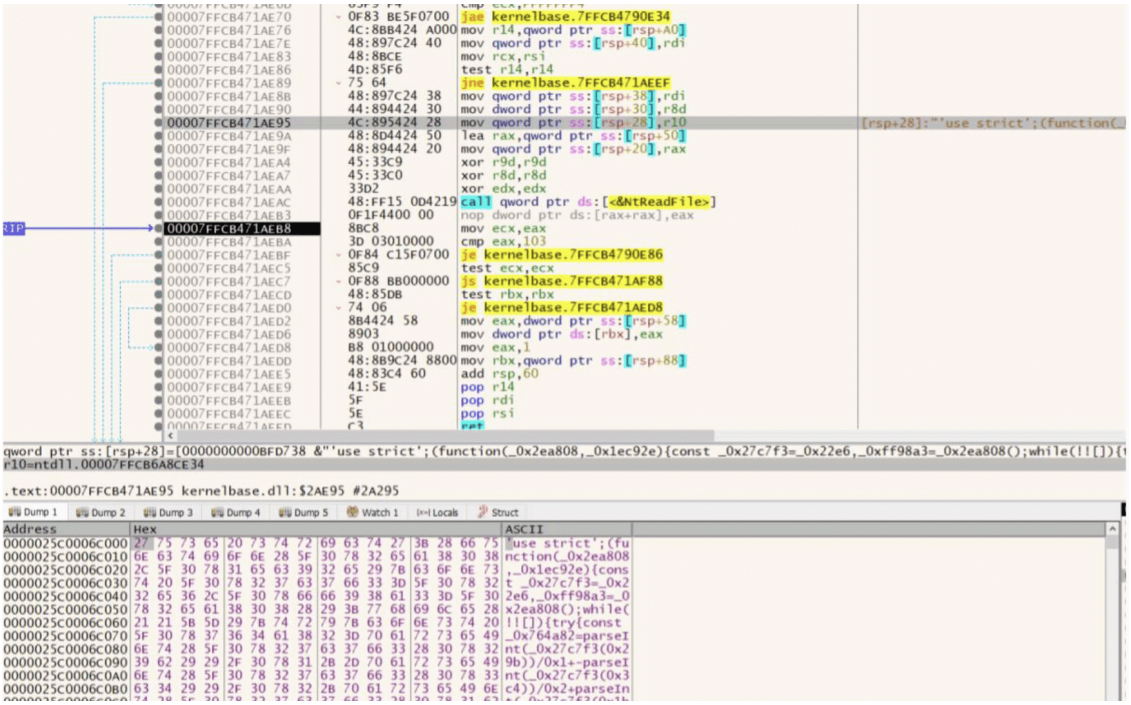
From August 21, 2025, machines that called back received instructions that activated the malicious capabilities, an information stealer, referred to as “Tamperedchef”.

When these malicious capabilities are activated, the following registry key is added:

Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\PDFEditorUpdater

With the arguments PDF Editor.exe `--cm=--fullupdate`

When the argument –fullupdate is set the executable loads an obfuscated file that is downloaded into /resources/app/w-electron/bun/releases/pdfeditor.js

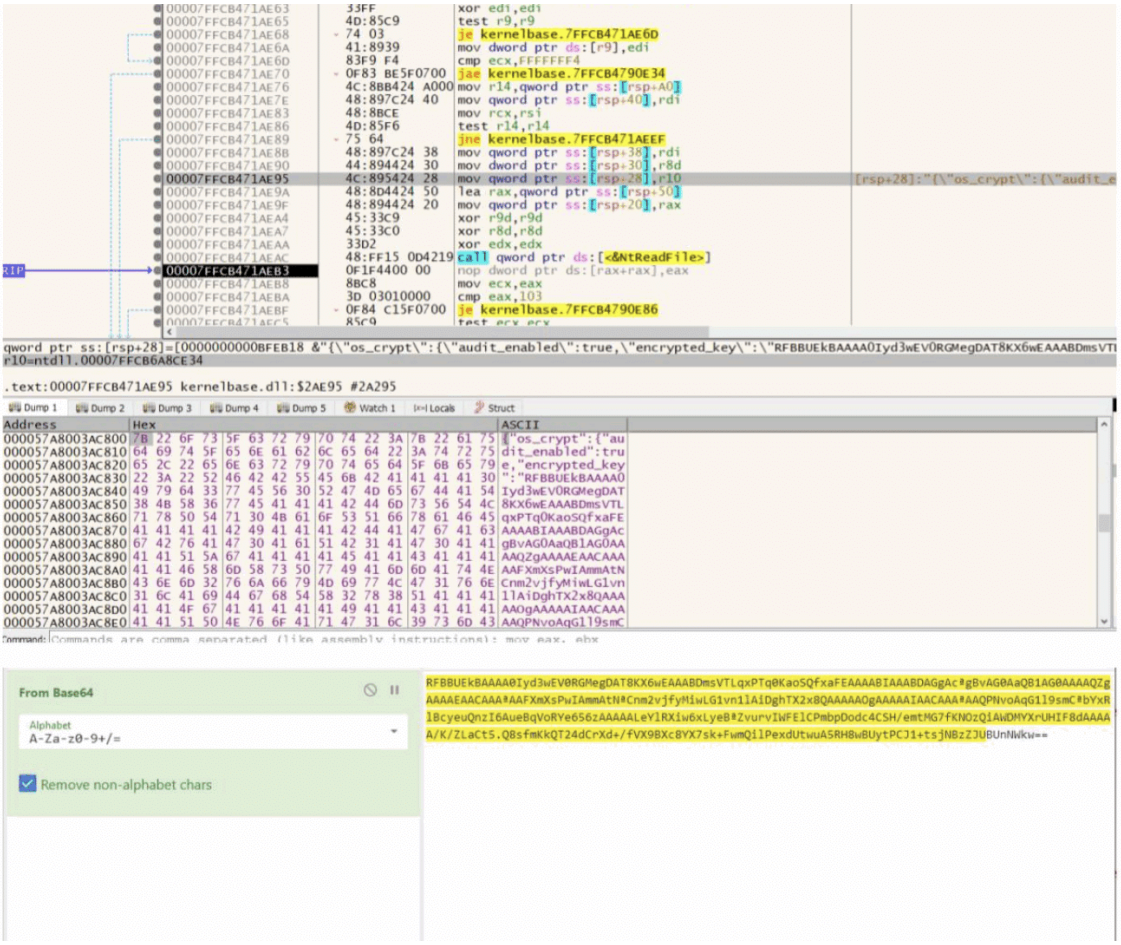


The –cm have the following different arguments.

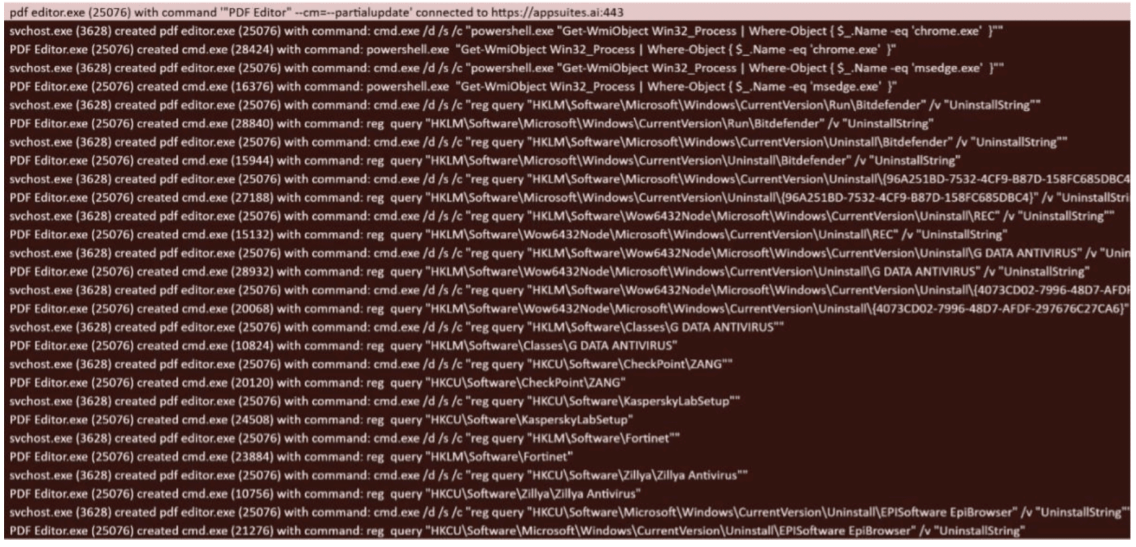
`--install`
`--enableupdate`
`--disableupdate`
`--fullupdate`
`--partialupdate`
`--backupupdate`
`--check`

--ping
--reboot

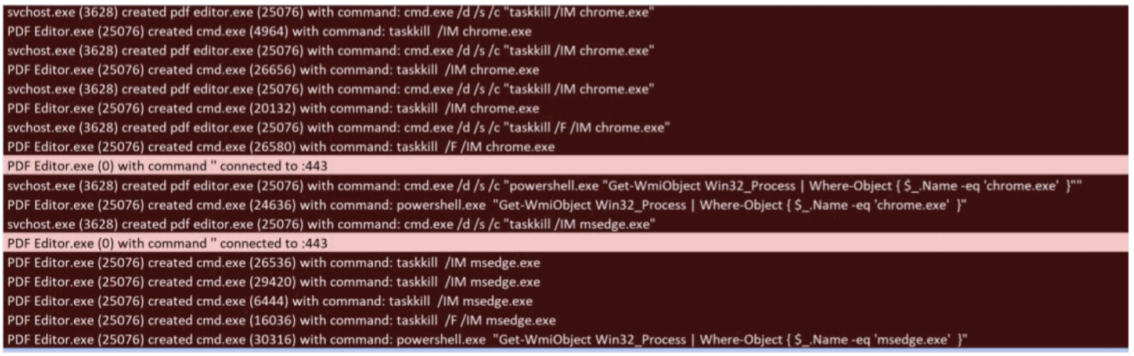
When initialized, Tamperedchef starts to query the web browsers database using DPAPI.



Upon starting it starts to query the system for different security products.



Then it terminates different browsers, likely to be able to accesses within them data that is locked if running.



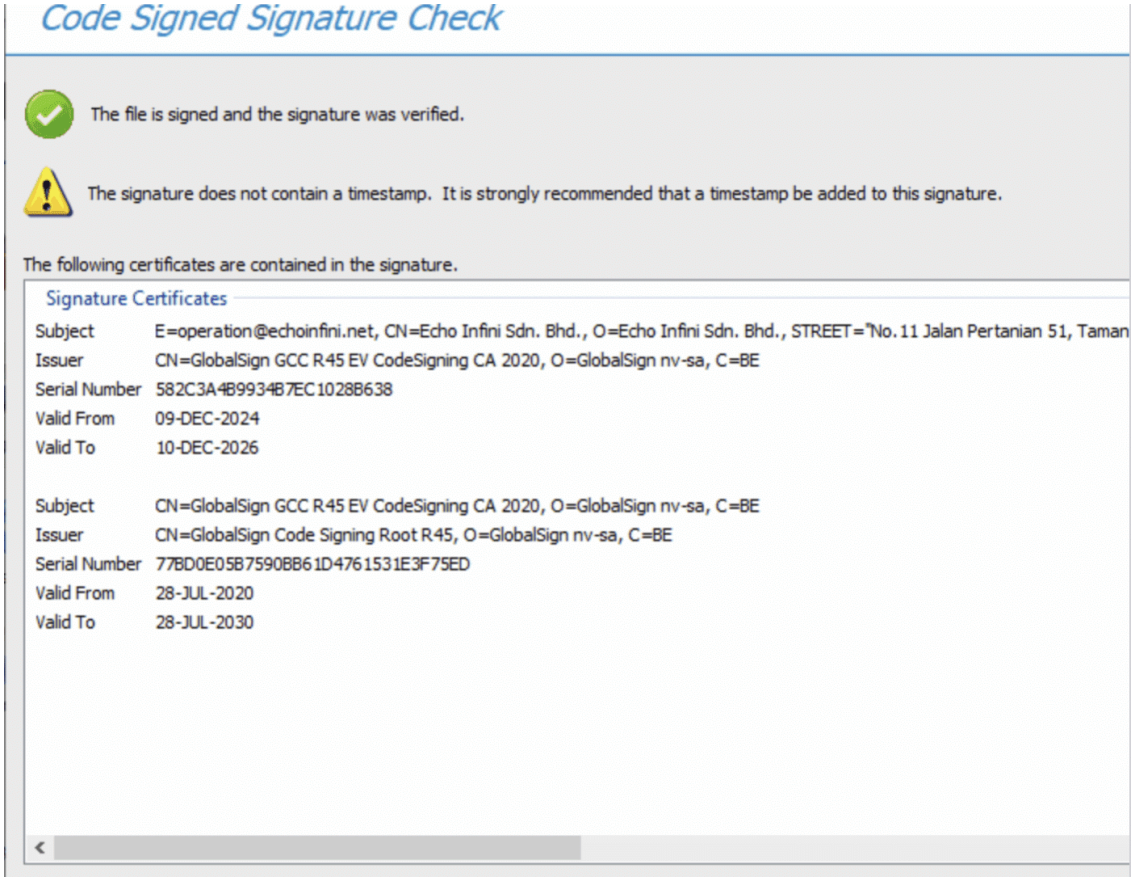
Data traffic with the sites that distributes AppSuites PDF Editor includes referrers to google ads campaign codes, suggesting that the threat actor behind this campaign used Google advertising to promote this pdf editor. Truesec has observed at least 5 different google campaign IDs which suggests a widespread campaign. The length from the start of the campaign until the malicious update was also 56 days, which is close to the 60 days length of a typical Google advertising campaign, suggesting the threat actor let the ad campaign run its course, maximizing downloads, before activating the malicious features.

Bad certificates

The threat actor has had different versions of the Appsuite PDF-editor app signed by certificates from to at least four different companies. The companies are:

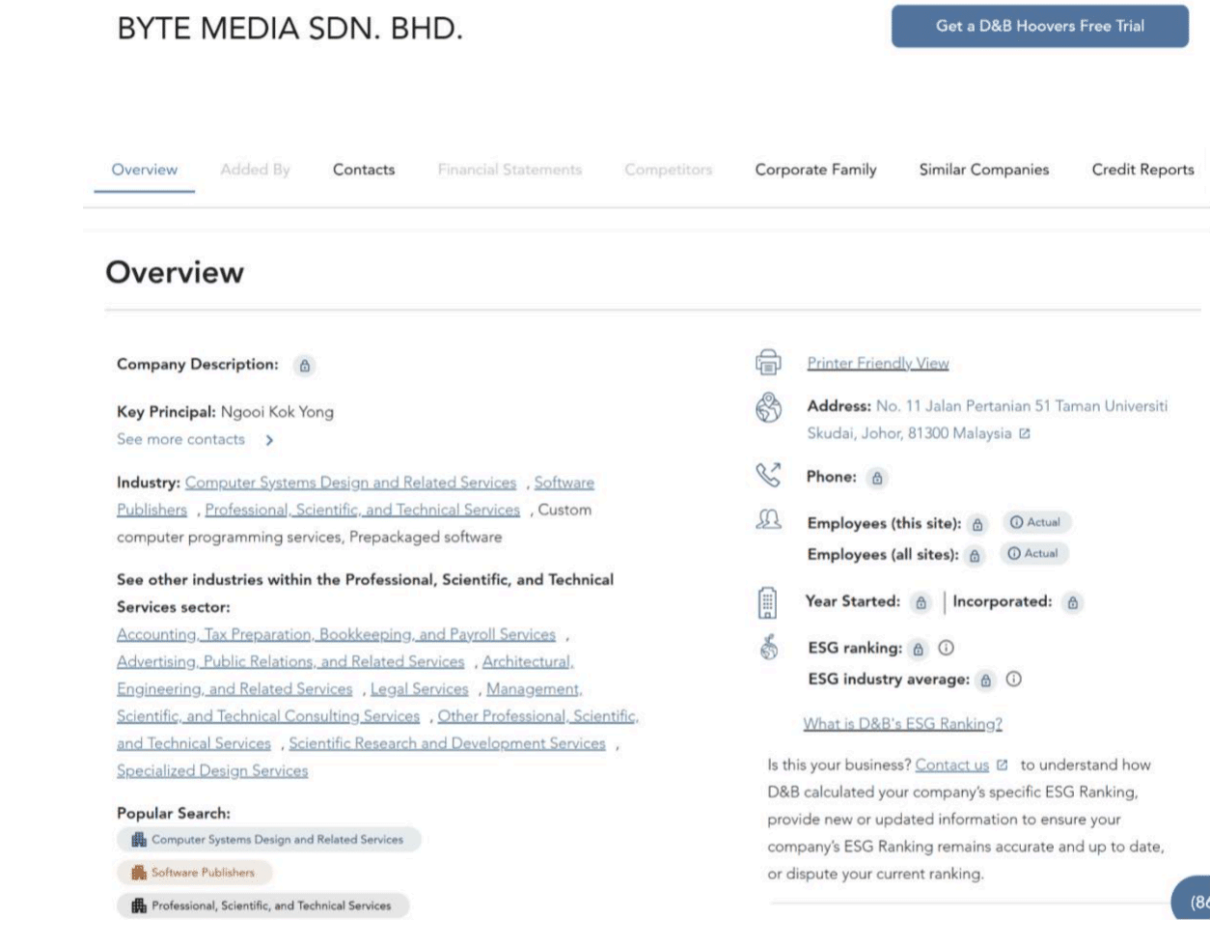
- ECHO Infini SDN BHD
- GLINT By J SDN. BHD
- SUMMIT NEXUS Holdings LLC, BHD

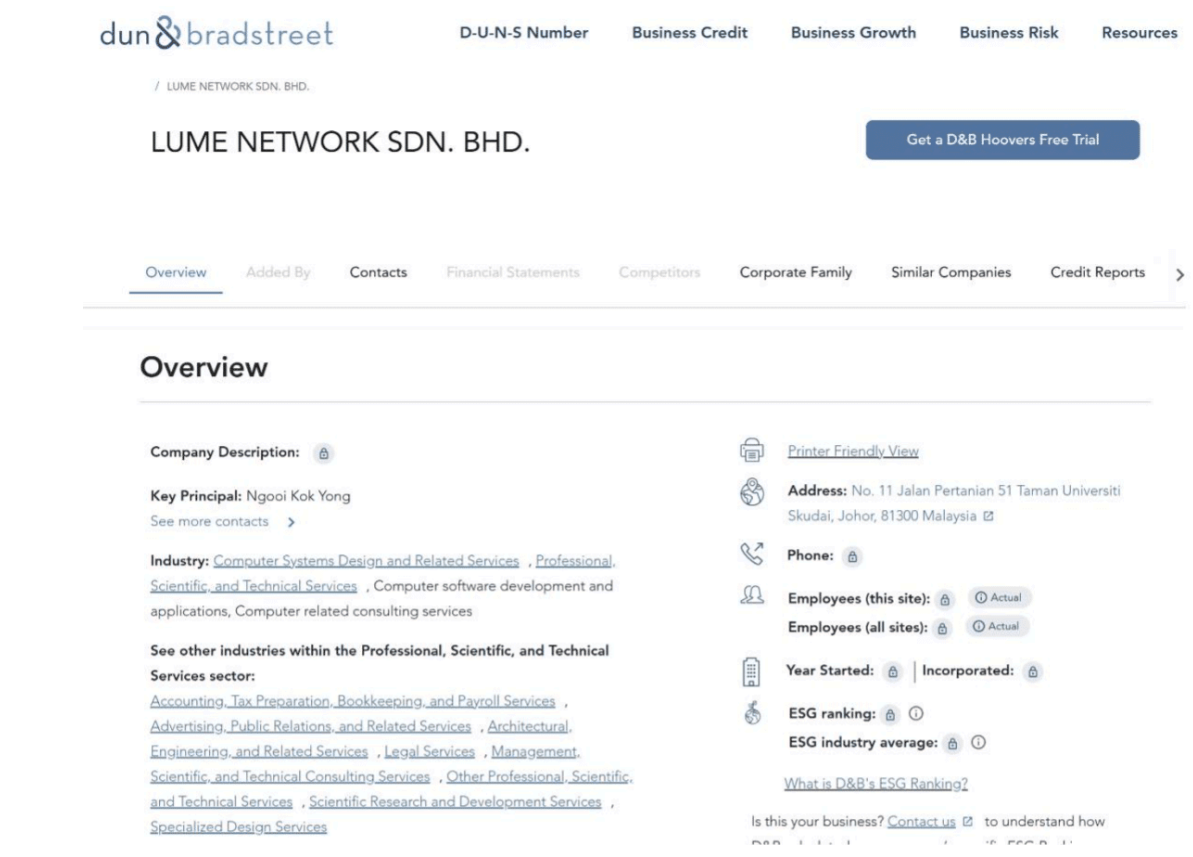
Below is the digital certificate of ECHO Infini:



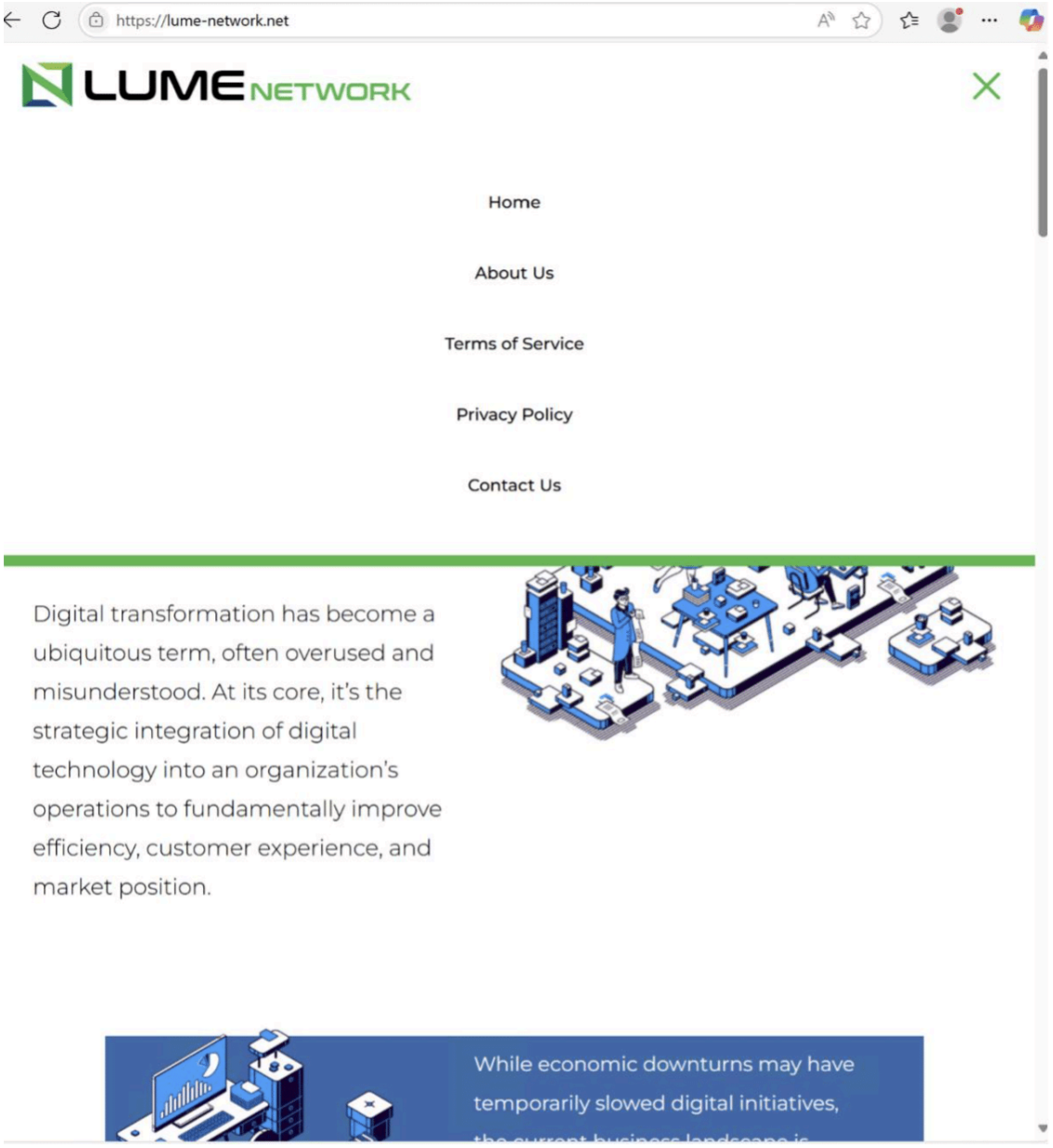
The web page of ECHO Infini SDN appears highly generic and possibly AI generated.

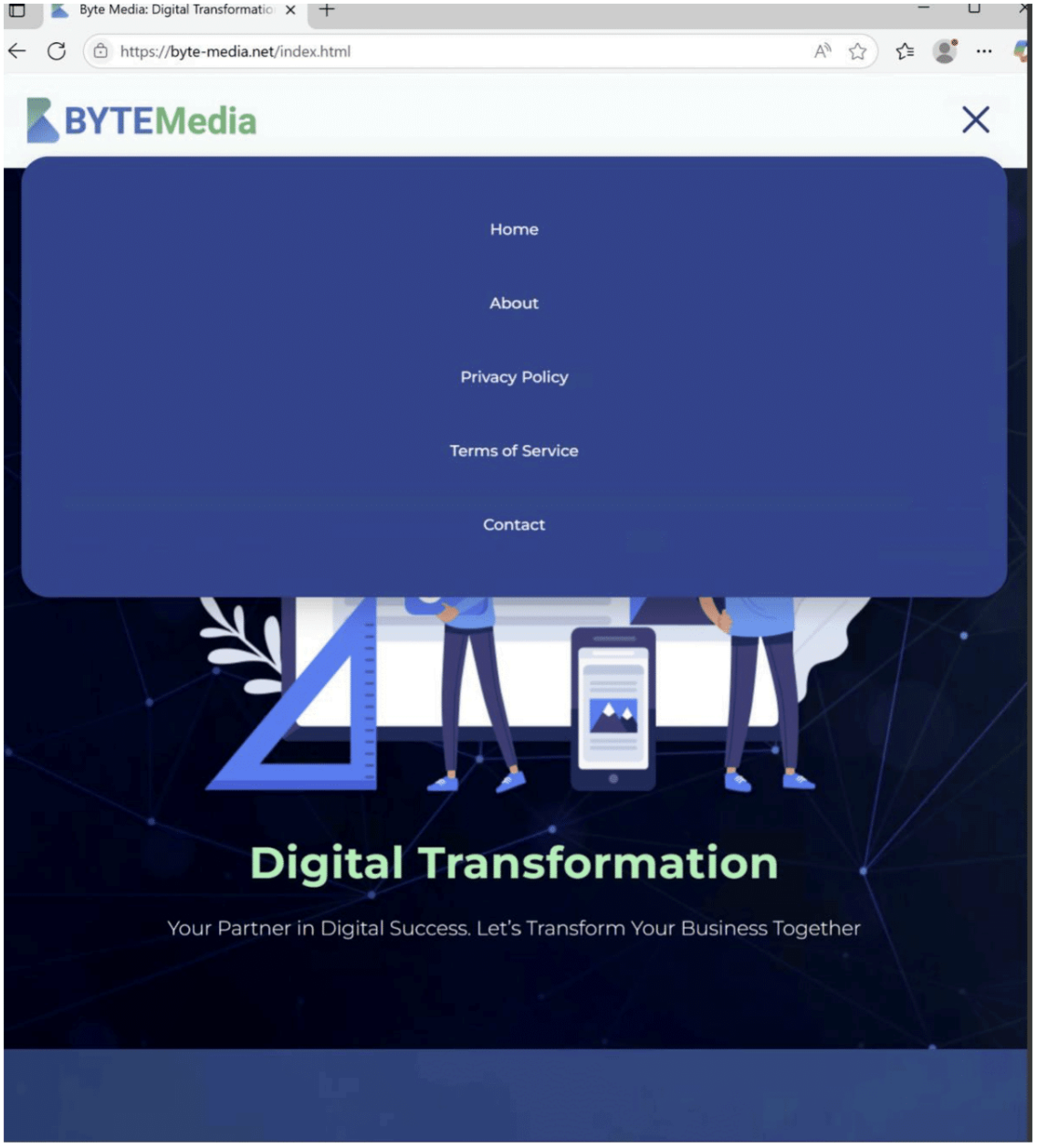
Searching for more information regarding the company reveals that there are several companies located at the same address.


BYTE MEDIA SDN. BHD.
Get a D&B Hoovers Free Trial
Overview
Added By
Contacts
Financial Statements
Competitors
Corporate Family
Similar Companies
Credit Reports
Overview
Company Description:
Key Principal: Ngooi Kok Yong
See more contacts
Industry: Computer Systems Design and Related Services , Software Publishers , Professional, Scientific, and Technical Services , Custom computer programming services, Prepackaged software
See other industries within the Professional, Scientific, and Technical Services sector:
Accounting, Tax Preparation, Bookkeeping, and Payroll Services , Advertising, Public Relations, and Related Services , Architectural, Engineering, and Related Services , Legal Services , Management, Scientific, and Technical Consulting Services , Other Professional, Scientific, and Technical Services , Scientific Research and Development Services , Specialized Design Services
Popular Search:
Computer Systems Design and Related Services
Software Publishers
Professional, Scientific, and Technical Services
Printer Friendly View
Address: No. 11 Jalan Pertanian 51 Taman Universiti Skudai, Johor, 81300 Malaysia
Phone:
Employees (this site): Actual
Employees (all sites): Actual
Year Started: | Incorporated:
ESG ranking:
ESG industry average:
What is D&B's ESG Ranking?
Is this your business? Contact us to understand how D&B calculated your company's specific ESG Ranking, provide new or updated information to ensure your company's ESG Ranking remains accurate and up to date, or dispute your current ranking.

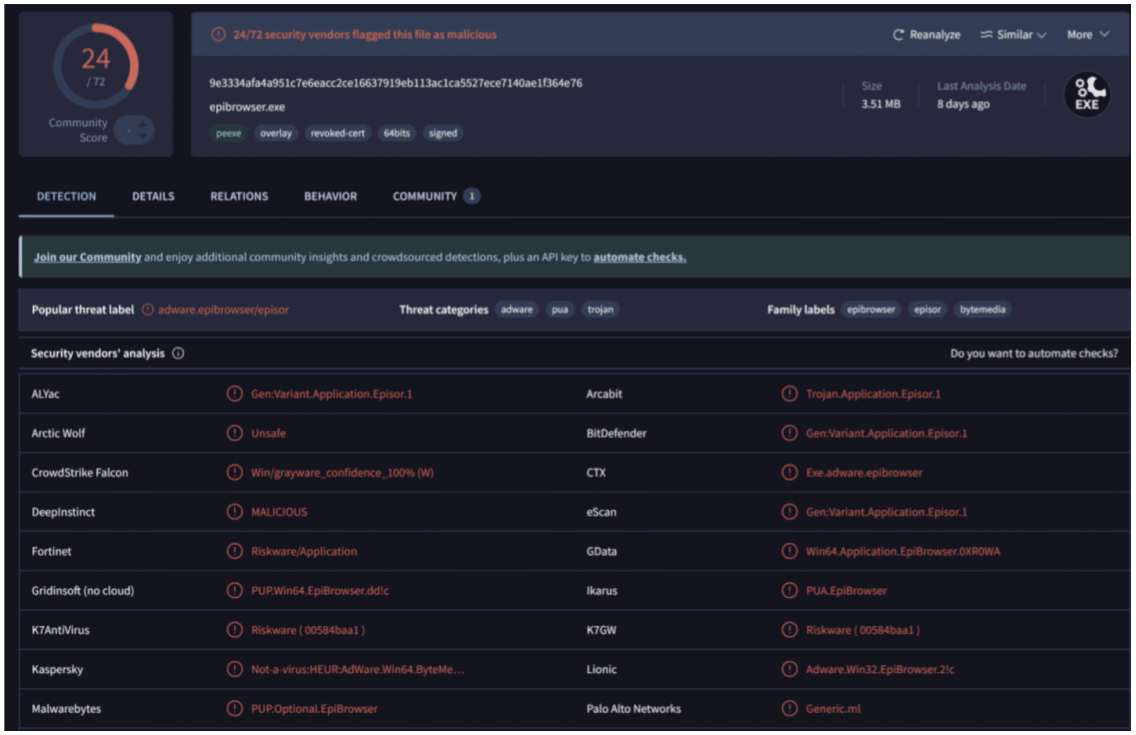

dun & bradstreet
D-U-N-S Number
Business Credit
Business Growth
Business Risk
Resources
/ LUME NETWORK SDN. BHD.
LUME NETWORK SDN. BHD.
Get a D&B Hoovers Free Trial
Overview
Added By
Contacts
Financial Statements
Competitors
Corporate Family
Similar Companies
Credit Reports
Overview
Company Description:
Key Principal: Ngooi Kok Yong
See more contacts
Industry: Computer Systems Design and Related Services , Professional, Scientific, and Technical Services , Computer software development and applications, Computer related consulting services
See other industries within the Professional, Scientific, and Technical Services sector:
Accounting, Tax Preparation, Bookkeeping, and Payroll Services , Advertising, Public Relations, and Related Services , Architectural, Engineering, and Related Services , Legal Services , Management, Scientific, and Technical Consulting Services , Other Professional, Scientific, and Technical Services , Scientific Research and Development Services , Specialized Design Services
Printer Friendly View
Address: No. 11 Jalan Pertanian 51 Taman Universiti Skudai, Johor, 81300 Malaysia
Phone:
Employees (this site): Actual
Employees (all sites): Actual
Year Started: | Incorporated:
ESG ranking:
ESG industry average:
What is D&B's ESG Ranking?
Is this your business? Contact us to understand how

Looking at the information on their website it also tells they all work with digital transformation.





For the company BYTE Media there are also digital certificates used for to sign malware, but another one called Epibrowser.



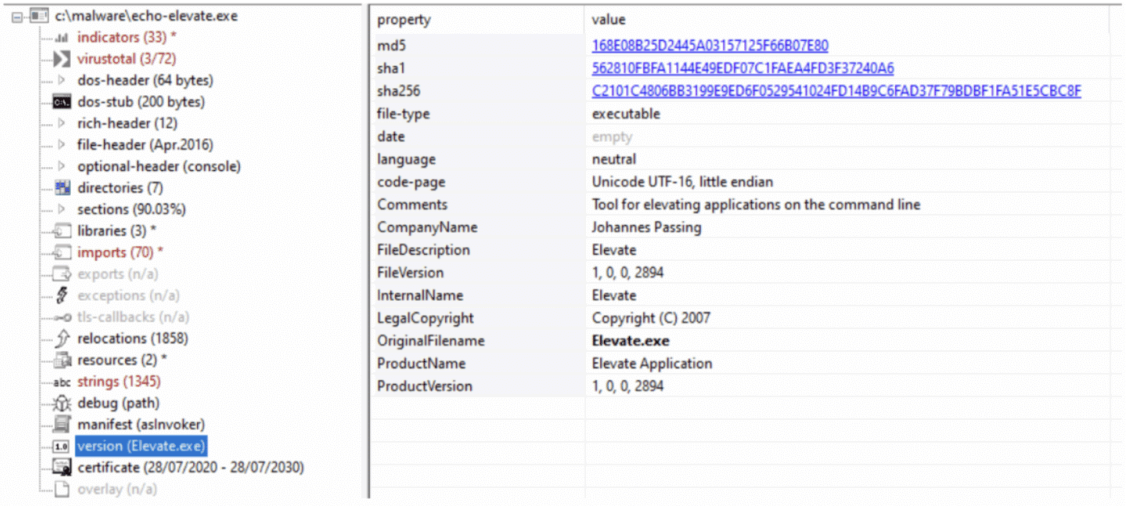
[Virustotal]

Further investigation has revealed that the threat actor behind this campaign has been active at least as early as August 2024, and possibly earlier, promoting a plethora of tools including the OneStart and Epibrowser browsers, that both have been distributed as a potentially unwanted program (PUP) in code bundles.

Samples of the OneStart browser has also contacted the same C2 domains as the Tamperedchef malware associated with the AppSuites PDF-editor, suggesting it exhibits malicious behaviour too.

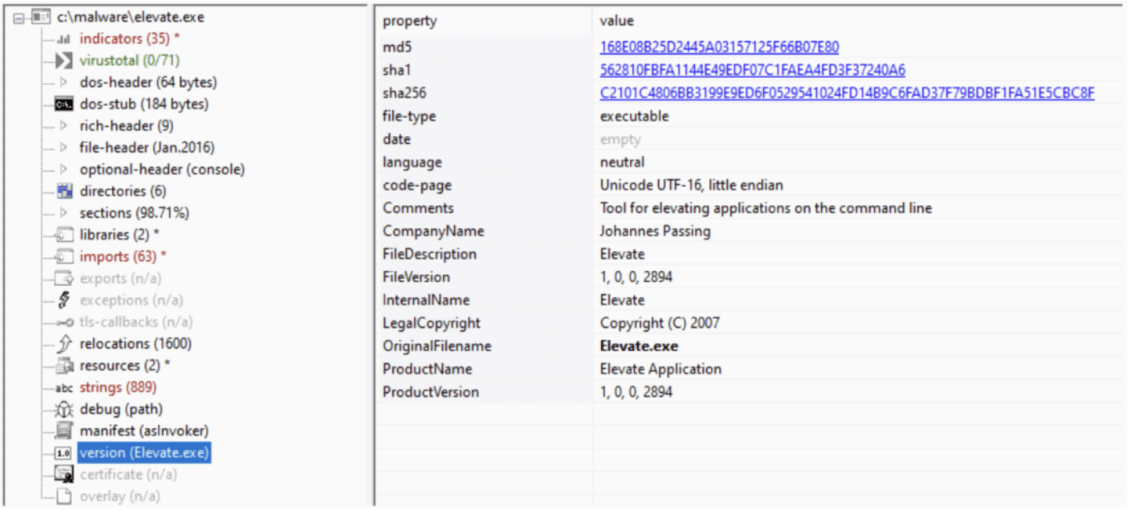
Other binaries

In several cases we have observed a file called elevate.exe being installed together with the PDF Editor bundle. This file is also signed by Echo Infini but looking at the company name this file is created by Johannes Passing.



Elevate is an open source project that can be used to give a program higher privileges upon running, but is has been recompiled and digitally signed.

Comparing it to the open source it is identical and have the same functionality.



```
C:\Malware>Elevate.exe
(c) 2007 - Johannes Passing - http://int3.de/

Execute a process on the command line with elevated rights on Vista

Usage: Elevate [-?|-wait|-k] prog [args]
-?    - Shows this help
-wait - Waits until prog terminates
-k    - Starts the the %COMSPEC% environment variable value and
                executes prog in it (CMD.EXE, 4NT.EXE, etc.)
prog  - The program to execute
args  - Optional command line arguments to prog

C:\Malware>echo-elevate.exe
(c) 2007 - Johannes Passing - http://int3.de/

Execute a process on the command line with elevated rights on Vista

Usage: Elevate [-?|-wait|-k] prog [args]
-?    - Shows this help
-wait - Waits until prog terminates
-k    - Starts the the %COMSPEC% environment variable value and
                executes prog in it (CMD.EXE, 4NT.EXE, etc.)
prog  - The program to execute
args  - Optional command line arguments to prog
```

We have not seen any sign of Elevate has been executed, so might be a file that is dropped to be used at a later stage for privilege escalation.

Summary

The threat actor behind this malicious activity apparently has a long record of distributing malicious code disguised as free utility tools. Our findings suggest, however, that the threat actor may have elevated this activity with the latest ad campaign.

We have observed several organizations in Europe being affected as employees have downloaded the malicious app, suggesting this latest campaign has been highly successful in tricking individuals to download the app.

This activity highlights the importance of vetting any software introduced into your environment. Seemingly harmless utility tools from unknown sources can overnight transform into a security nightmare.

When alerted about this activity, Google has apparently been very helpful, so we encourage anyone to report similar activity to both their local CERT and to Google, if and when such activity is observed in the future.

Detection and prevention of weaponized software

When creating a detection the Truesec Detection Engineering strategy revolves around the TTP layer, avoiding static patterns and IOCs whenever possible.
This ensures that instead of detecting a specific attack that might change its static values at any time, our Detections trigger on holistic behaviors.

In this case we'll try to break down the software into Points of Detection by considering what telemetry is available and the signal value of said telemetry.

The first clearly detectable event through an EDR-perspective comes when the software adds a registry key for persistence, the purpose of which is to execute a command on startup indicating that the software is checking for updates.

This is not entirely uncommon among PUAs (Potentially Unwanted Applications) and similar software and will likely be difficult to alert on without creating too much noise, likely drowning out any True Positives and creating alert fatigue for any analysts investigating such alerts.
As such the Signal Value of these events are low and can likely not be used without further context, but for example the RegistryKey Value Data might however indicate an execution from an unprotected folder which is of more interest as a starting block for building a solid foundation of a detection rule.
Similar behavior with PUAs adding scheduled tasks relating to their own execution is not entirely uncommon either and would likely produce similar results of alert fatigue and therefore as a standalone indicator serves no purpose.

The second identified Point of Detection where signal value is high comes at the point where the software is weaponized. At this stage the software touches the web data and kills the browsers for further enumeration. While the signal value of these events are high the telemetry is often lacking relating to File Reads, and the attack is already underway.

With this in mind there are detections that might be employed at the earlier stages when the malware (at this stage identified as PUA) is establishing persistence by querying for Registry keys under ***/Run** with a value pointing towards ***:/Users/*** and similar unprotected folders, but this does require a certain control of the environment in order to strengthen the Signal Value of the detection to mitigate the risk of alert fatigue.

At this point we've established that creating detections for weaponized malware utilizing the telemetry available to most EDRs will be difficult on it's own, so what measures can be taken to enable these types of detection as to prevent similar attacks in the future?

A few key prevention tools come to mind off the bat; AppLocker and AdBlockers.
AppLocker and similar solutions are key to gaining control of your organizations endpoints and creates an environment where it's easily discernable what applications are supposed to exist where, which in turn enables detections as described above.
AdBlockers on the other hand will help mitigate the rising threat of malicious ads, an attack vector that Truesec Detect has seen being employed increasingly during the last few years.

With these measures in place the Signal Value of the Detection Points described above is greatly increased, enabling detections that more easily stops evasive threats such as the trojanized software of TamperedChef.

The file hashes are not all inclusive and new versions of PDF Editor appears continuously.

IOC

Hosting Domains

apdft[.]net
mypdfonestart[.]com
ltdpdf[.]com
pdfreplace[.]com
pdf-tool[.]appsuites[.]ai7
pdfsmartkit[.]com
fastonestartpdf[.]com
pdfhubspot[.]com
pdfhubspot[.]com
businesspdf[.]com
pdfdoccentral[.]com
pdffilehub[.]net
pdfonestarthub[.]com
pdfonestartlive[.]com
download04[.]pdfgj[.]com
pdfappsuite[.]com
pdffacts[.]net
pdftraining[.]com
smarteasypdf[.]com
pdffacts[.]com
pdfonestart[.]com
pdf-kiosk[.]net
pdfmeta[.]com
download04[.]internetdownloadhub[.]biz
download05[.]masterlifemastermind[.]net
pdf-kiosk[.]com
easyonestartpdf[.]com

ltdpdf[.]net
fileconverterdownload[.]com
download02[.]pdfgj[.]com
pdfworker[.]com
getsmartpdf[.]com
proonestartpdf[.]com
cdasynergy[.]net
pdfscraper[.]com
appsuites[.]ai
pdfts[.]site
micromacrotechbase[.]com
pdfartisan[.]com
apdft[.]com
itpdf[.]net
9mdp5f[.]com
proonestarthub[.]com
advancedtransmitart[.]net
click4pdf[.]com
convertpdfplus[.]com
onestartbrowser[.]com
vault[.]appsuites[.]ai
download02[.]apdft[.]online
download04[.]masterlifemastermind[.]net
itpdf[.]com
transmitcdnzion[.]com
smartmanualspdf[.]com
pdfonestarttoday[.]com

C2 Domains

y2iax5[.]com
abf26u[.]com
mka3e8[.]com
5b7crp[.]com

SHA256

Hash	Application / Library
da3c6ec20a006ec4b289a90488f824f0f72098a2f5c2d3f37d7a2d4a83b344a0	PDF Editor
956f7e8e156205b8cbf9b9f16bae0e43404641ad8feaaf5f59f8ba7c54f15e24	PDF Editor
f97c7edb0d8d9b65bf23df76412b6d2bbfbab6e3614e035789e4e1a30e40b7f1	PDF Editor

Hash	Application / Library
cf5194e7f63de52903b5d61109fd0d898b73dd3a07512e151077fba23cdf4800	PDF Editor
189b0ba8c61740d5ad1c802649718958a86f5b7a8c8e795dc2e990909a9ab88a	Elevate Application
57c92ed1e87dda6091903e1360c065e594576e2125f5d45f159269b0bef47f32	PDF Editor
cb15e1ec1a472631c53378d54f2043ba57586e3a28329c9dbf40cb69d7c10d2c	PDF Editor
71edb9f9f757616fe62a49f2d5b55441f91618904517337abd9d0725b07c2a51	ManualFinder
ce0019424497040351c9054aa2ee6b07fc610024cc2cb2cc810de80f838c7a14	PDF Editor
7e0d909c934620140db7d53e2caefdd58866484cb049f876f8a8428e6334618a	Elevate Application
abbb3e96b910c9d1e2074dc05fd51e78984941f03bcb7d443714838849a7a928	PDF Editor
a3fc5447a9638a3469bab591d6f94ee2bc9c61fc12fd367317eec60f46955859	PDF Editor
13698b05960edbda52fa8f4836526f27e8fc519ca0f4a7bc776990568523113e	PDF Editor
bdb0e1f2582547fdc64a656a813b0e67f8819f96918050f6114b159d7ca7fd69	Elevate Application
10640dcc67b3e2e4a6dbbfdb2fab981de4676d57f9f093af3cfb6f4f8351baf6	PDF Editor
2e4de114ad10967f1807f317f476290dc0045bdfa9395553d1b443ef9f905018	EpiBrowser
9e3334afa4a951c7e6eacc2ce16637919eb113ac1ca5527ece7140ae1f364e76	EpiBrowser
2e06a801c4bdfca8061c04dea3a43b0fd3b883b96f32dd901a076be786d466e6	EpiBrowser
3b32696ebac176a898f277bb662099deebecf7216dae942e610dc8b7b3dd4c48	EpiBrowser
ce1a6009f013eafecbe13d72bee044c546654dad3805b7d2744d453e6544ecc8	ANGLE libGLESv2 Dynamic Link Library
3a2b1f97a47e63d48f8955311f18664aa2c5e5a865ec6f43d8943b81eefd5a65	ANGLE libEGL Dynamic Link Library
ab376fbec6ca90c8cac2fd4ec92c564638bde0e6737a48f687b5367c51f49a0b	SwiftShader Vulkan Dynamic Link Library
5c839e560530a7a4077baa16294cc9dc404f98a42c004f2013903543383af669	Microsoft(r) DirectX for Windows(r) – Google Dawn Custom Build
458ef97817fa4537ff9a4b73844260e4a9951ec4e7e4b4d3c13240bb8675764b	EpiBrowser
9bbe83ec13fc6397ddb69c47a3266ae39b3204d68674b529170bc6b56bcbdfcc	EpiBrowser

Hash	Application / Library
9fa4d8a68d6f231577d62d560d110a66fd3f311cc8dcb1b4b10a50632d03ad1d	EpiBrowser
987a94fbe252da32dfb83daeb52d5636bd61d4b88fb45e9a97b79df3c03edcb8	ANGLE libGLESv2 Dynamic Link Library
76cf960146bf07ad8b459ceb401a35ed37c98cb4e84ace329595b5b0f3955d3a	ANGLE libEGL Dynamic Link Library
2f66690072dae1ca203e8c93330fccb8b5ccf8b8c9cce747250a11096d551794	SwiftShader Vulkan Dynamic Link Library
5adc11546db45ab8e57f9bc2808b46898dc7eef179ccbf963552b694f0ec61b6	Microsoft(r) DirectX for Windows(r) – Google Dawn Custom Build
f4bc13b8b76656e4e4b7306d2dc6a5be4e19e752b015bcefbfdcc885a8bb122f	EpiBrowser Installer
b0c321d6e2fc5d4e819cb871319c70d253c3bf6f9a9966a5d0f95600a19c0983	PDF Editor
42222692739edf910e1e25310923ddfbbea465a69b6d9e5ec01091c5aa0aee0f	EpiBrowser
031682d2f69322a68cd13d0e380cf149199b20755c6e08f4fb7b41d27a5378f0	EpiBrowser
5cbd51bbd10008b92fe490a6fa87339dd3d0f57fce82d10dc4fa0566133ac94d	ANGLE libGLESv2 Dynamic Link Library
b07ffbd8eed8dc989db1c58d84d3f8b9d57fb6a7b5f30af6d982e2bd4da0e696	ANGLE libEGL Dynamic Link Library
232006ef149a2dcc150d765a3b330317d5e62f21391c1f355fba4a833a9dd49f	SwiftShader Vulkan Dynamic Link Library
b7f63771d24f07f5ce30f2a9f8895b815e47ab01a1e3c09322f55c16f140e041	Microsoft(r) DirectX for Windows(r) – Google Dawn Custom Build
3c702aa9c7e0f2e6557f3f4ac129afd2ad4cfa2b027d6f4a357c02d4185359c4	PDF Editor
14fb07941492c7f014435633a02bf14761d91d1df3023fa0dd4c3210e80554b7	PDF Editor
f6e323d4741baf047445a13bb9587acfb79cc2b16737b91df18a8a9bf5b307f4	PDF Editor
3b32696ebac176a898f277bb662099deebecf7216dae942e610dc8b7b3dd4c48	EpiBrowser
0a15e90c062bf6137336beba0ec480af8f370ceaedca3e1ff76cd131f2e54927	EpiBrowser Installer
0faaec07a598784fc76caa5254307a01383b229397e271020f319be84c7b8bf9	EpiBrowser

Hash	Application / Library
2ce20ceb2aaa24de8d3d7714bf87cef90b9cc90a21234d0b7cc78f22d9d5d5c1	Elevate Application
cebe0ce89e4622118371f60cd82a9d0a7659e0916edf522cacba6b308bded8de	Vulkan Runtime
bd21360149904ce42c6927d9c3fb482316f2537a4a7bce8b64990428e27a54ac	PDF Editor
e08cc90e738e7e5f275d220b3914c2860a388e7ada67ed34fda1a01a23bf42bc	PDF Editor
69b373084e47cbb54a9003ae2435adb49f184bfa11989a2800700da22a153dff	PDF Editor
5485bafd43f2f3865f18e74a14a00a433971cdc5b50c357bd0307179e0187e3d	PDF Editor
5964e5c15ea512ea3208109d7175e6b43c5f85a77de95f44d3dc81e1940f94e3	Elevate Application
5c21b5d1eb58367cb1ac189d383a7f0eb1e8d00d6722712897eb2efdbc670d1d	PDF Editor
6ec07c1d2dc566d59a7576cc4a89c605bcfc8abd414c77338c940fb8e3ed5f1a	EpiBrowser Installer
aaf6e40848b904e664cdfbefa1e42870c3e42387471a03361e4fd0781943a032	Elevate Application
5d3a41e2c6b854d12b70cea9000cafe1f3877bbccc51ca20f29da2e47f79a088	EpiBrowser
2221b218ad03b615683941d11bd8085ca87b7b576bc5d1a6c720a0eb223d4405	ANGLE libGLESv2 Dynamic Link Library
aefab9c1959c5cb86fd656d9ea2148c584cae543ac203dd2ae4467a36382586a	ANGLE libEGL Dynamic Link Library
8f1960939eee8d0689cc07613189f27054beff96e8740045de88fa1b6764b5b5	SwiftShader Vulkan Dynamic Link Library
95176fc574f3d707e68965690826759260c5867e865b19a000bebb20a01a2e0a	Microsoft(r) DirectX for Windows(r) – Google Dawn Custom Build
fc4d1107958f70bd553d824224fc74b3b5ad2365f3599bfda795e0b718f3c76a	EpiBrowser
6aa61426d77da6674efdf6f7d139b4ccd9eebf4afb86831b79da0b8913ba89d8	EpiBrowser
88450ae2c0c19d2a3a54e7b2c029998ed3daf68e78fbd664aea50c7ed582f544	EpiBrowser Installer
2fe2d16e51488337de25bb02c7ca4a06e2b7e3229cd2af9903db7c9efdf88e31	EpiBrowser
6ec7acd0ff0980b88801d5eed7dfe69d6349f2044bd5e1768f6d1ed7f403e43e	EpiBrowser
e6286f5f4c7cdde39c9300d1204ff504499c760bbffa56fc7e3830796537f71b	EpiBrowser
6c6cde420ea1b48c2f070ae139a71294b3c4c6c768da4279e4fe3bd2a9ff1885	ANGLE libGLESv2 Dynamic Link Library

Hash	Application / Library
d7315bbccff2899c1751c7f7e0e0b48d561366771699f48c90d9b448418856c2	ANGLE libEGL Dynamic Link Library
25d1fd2706c39edeb453a30fbca7561142978468d3e94efa0982504d60b06757	SwiftShader Vulkan Dynamic Link Library
5f52dc64c6d56287abcdd16d1e2a42db1a4bccc43263cbc259d881fc709242b9	Microsoft(r) DirectX for Windows(r) – Google Dawn Custom Build

Edit 1, 2025-08-29, added recommendations for detecting and preventing weaponized software.
