The history of AppSuite: the certs of the BaoLoader developer

By Aaron Walton

Published: 2025-09-11 · Archived: 2026-04-05 21:35:53 UTC

This blog was created through a collaboration between Expel and the folks maintaining CertGraveyard.org.

TL;DR

- We demonstrate that the developers behind the recent AppSuite-PDF and PDF Editor campaigns have used at least 26 code-signing certificates over the last seven years to make their software appear legitimate.
- We track the malware under the name BaoLoader. Their software has generally been regarded as “potentially unwanted programs” (PUPs). However, recent analysis of the software and the actors’ connections to fraud suggest we should re-consider how we think about them.
- This analysis primarily focuses on code-signing certificate abuse. This gives us a high-level overview of the actors to define their history of behavior, but not a complete picture.
- We clarify how this malware is different from Chromeloader and TamperedChef. These names have been mistakenly applied to this malware, but the distinction is important for research and law enforcement.

What we’re tracking and why

Our analysis focuses on years of tracking a team of threat actors through mapping the actors’ use of code-signing certificates. These actors register new businesses for receiving authorization to generate code-signing certificates. Code-signing is a critical component used to validate the legitimacy of software. They then use these certificates to sign their own malware, often disguised as potentially unwanted programs (PUPs).

This particular analysis will focus on our research into the code-signing activity of the actors involved, connecting the threads between the businesses the actors have propped up to create certificates, the certificate authorities they’ve used to authorize them, and the pieces of software signed by these certificates.

Background on code-signing certificate abuse

To set the scene, it’s important to know how threat actors abuse code-signing certificates. These certificates have a unique ecosystem of exploitation, typically beginning with threat actors impersonating legitimate businesses to obtain them. Think of this impersonation as being similar to corporate identity theft, as the organizations listed on the fraudulent certificates are often victims themselves.

The purpose of code-signing is to grant trust to programs after their providers are vetted. The vetting process creates a chain of trust, starting with Microsoft trusting a certificate authority to vet software providers and determine whether they are

trustworthy. Through the chain of trust, Microsoft then trusts the software provider's certificate once the certificate authority signs it.This allows validation processes to trust software signed by that software provider's certificate as well.

The certificate also contains a hash of the signed file, which is compared against a computed file hash. If the hashes match, the certificate is considered valid, indicating that the file hasn't been tampered with. (See the articles from the following authors to learn more about code-signing and abuse: Axelarator, Expel.)

In most cases, cybercriminals abuse this system by impersonating businesses to receive a certificate. This impersonation may include creating domains imitating a company and using it to apply, modifying government databases to include their names and contact information, or other methods. In the case of BaoLoader, the actors registered legitimate businesses.

We believe with high confidence the malware "AppSuite-PDF," "PDF Editor," "ManualFinder," "PDFTools," "PDFProSuite," and "OneStart" are distributed by the same team that buys certificates directly. Our data shows this team has been active over the last seven years. During this time, they've consistently maintained software that antiviruses have generally flagged as PUPs.

This analysis lays the groundwork for understanding and documenting their activity and exposes the threat actors' code-signing certificate use over the last seven years.

The data

Expel is grateful for the opportunity to collaborate with CertGraveyard.org and relied heavily on its database for the creation of this analysis. Cert Graveyard has documented more than 1,500 unique organizations with at least one abused code-signing certificate. Cert Graveyard identifies certificates used to sign malware and reports them to their issuers for review and revocation.

Identifying BaoLoader as unique malware via certificates

When reviewing the abused certificates, we observed a high level of consistency which causes the actors to stand out:

- The actors used 15 code-signing certificates issued for companies in Panama. Out of ~1,500 entries, no other actors in the database use certificates from Panama.
- The actors used five certificates for companies in Malaysia. No other actors in the database use certificates from Malaysia.
- The actors are capable of getting certificates from other countries as well. After some certificates used to sign OneStart were revoked, they obtained certificates for the company "Onestart Technologies LLC," which they registered in the US.
- The certificates are consistently obtained for media companies.

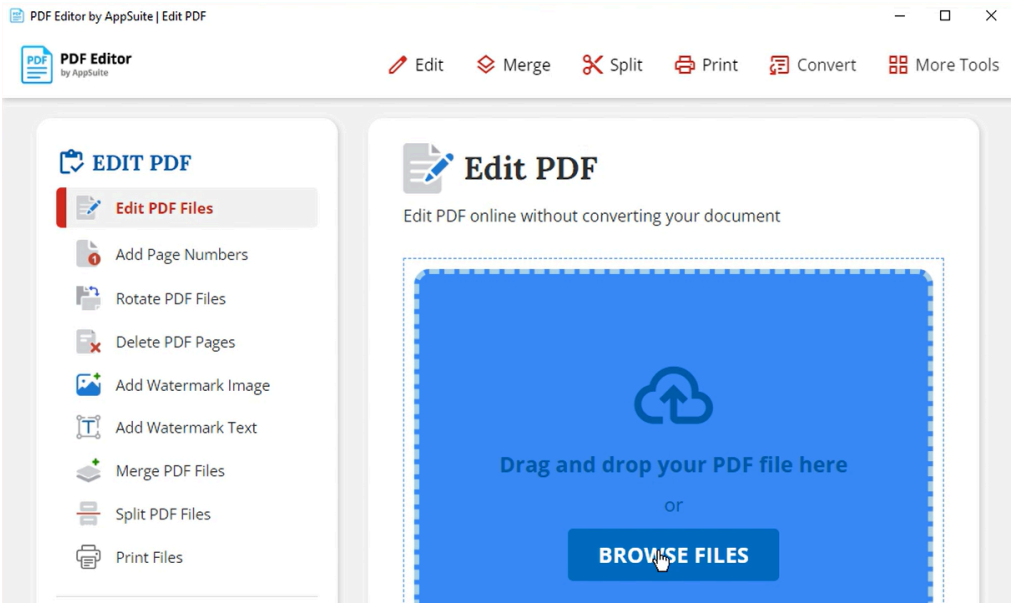
In most cases when a certificate is resold, the signer name is insignificant—a buyer is simply handed a certificate. However, these actors regularly use multiple certificates with the same signer name, but from different certificate authorities. This is highly unusual within Cert Graveyard's database of abused certificates. The Cert Graveyard database shows only one other documented instance where one actor used certificates for the same company but from two different certificate issuers. It also has only four cases where multiple providers issued certificates for the same organization, but each were sold to distinct actors. However, the actors responsible for this malware obtained certificates for unique organizations from multiple providers 11 times. This leads us to conclude that the actors acquire the certificates themselves—buying the certificates from providers rather than buying them from resellers.The malware signed with these certificates and named "BaoLoader" by RussianPanda, was initially misidentified. Some sources mistakenly referred to it as "Chromeloader" due to perceived similarities, while others incorrectly labeled it "TamperedChef." From our analysis, we believe that BaoLoader is distinct from both Chromeloader and TamperedChef, due to its different behavior and characteristic certificate patterns. We'll dive into these differences in depth in a bit, but first we'll discuss what we can learn about their campaigns by looking at their history of abusing code-signing certificates.

A history of abuse

In the following analysis, we first share information on the most recent abuse leveragingOneStart and the files it drops. Then we review software and malware campaigns from over the years, including files going as far back as 2018.

AppSuite-PDF and its relations

AppSuite-PDF is a simple app whose main functionality is to download and install the PDF Editor app that allows users to edit PDFs. But it also comes with a backdoor.



Over time, the actors obtained the following code-signing certificates to sign the files:

- GLINT SOFTWARE SDN. BHD.
- ECHO INFINI SDN. BHD. (from two different providers)
- Summit Nexus Holdings LLC

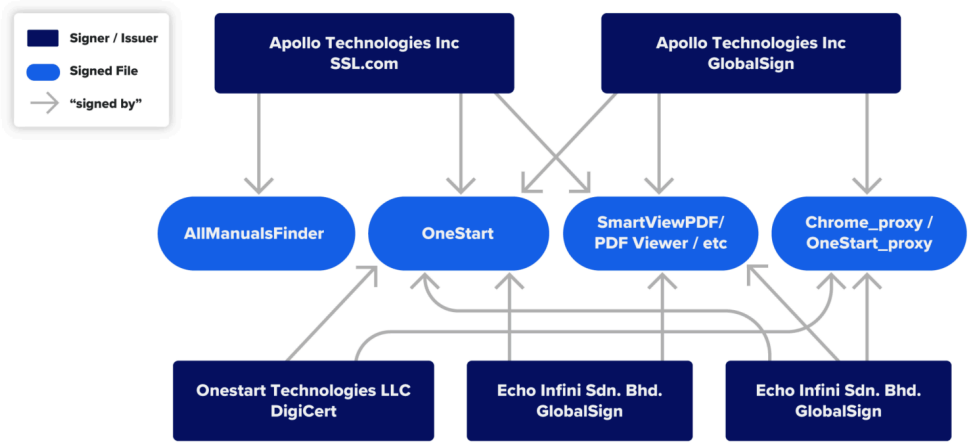
In our review of these organizations and websites, we found they offered minimal to no basic information about the businesses. This is characteristic of sites used in obtaining and abusing code-signing certificates. We were able to cluster the applications together because of the overlaps in code-signing certificates as displayed in the table and graph below.

Table 1: Representative sample of files using these certificates

File name	Example file hash	Signer (x509 CN)	Issuer	First VirusTotal Submission date
PDFEditor-1.0.0.8.exe	9dc1b05b8fc53c84839164e82200c5d484b65eeba25b246777fa324869487140	GLINT SOFTWARE SDN. BHD.	SSL.com	2025-08-05
ManualFinder (1).msi	d0838244e7ebd0b4bd7d7486745346af6b9b3509e9a79b2526dcfea9d83c6b74	GLINT SOFTWARE SDN. BHD.	SSL.com	2025-07-21
AppSuites-PDF-1.0.37.exe	98bb0ab170efdf98414114d6c14a047d2144730f3552bb4aea36198fc49083ac	Summit Nexus Holdings LLC	DigiCert	2025-08-23
PDF Editor.msi	c4f0b51308eb02c20e9bb33df80442b85b0cc0ad3ccf2598546d67c49242d506	Summit Nexus Holdings LLC	DigiCert	2025-08-22
AppSuites-PDF-1.0.8.2.msi	3c702aa9c7e0f2e6557f3f4ac129afd2ad4cfa2b027d6f4a357c02d4185359c4	ECHO INFINI SDN. BHD.	SSL.com	2025-07-16

PDF Editor.exe	66334de2175a0b85e2cba42189312af23497605489607e3952121ed223b2c0af	ECHO INFINI SDN. BHD.	SSL.com	2025-08-23
PDF Editor	b0c321d6e2fc5d4e819cb871319c70d253c3bf6f9a9966a5d0f95600a19c0983	Echo Infini Sdn. Bhd.	GlobalSign	2025-07-16
AppSuites-PDF-1.0.29.0.msi	fbc7ffc5bdda978afe0f20910210752d91762b97d6d7719a5b3a1e352a4717c3	Echo Infini Sdn. Bhd.	GlobalSign	2025-07-16

Figure: Diagram showing how signers and issuers relate to signed files. Squares represent signers/issuers, pills represent the files they sign, and arrows indicate 'signed by' relationships. Entity names are shown in their official casing.



OneStart and its relations

Users generally download OneStart unintentionally, commonly from PDF editor advertisements or bundled with other software. The application is primarily treated as a PUP, but also appears to use the same covert network communication mechanisms as AppSuite.

The developer signed OneStart with multiple code-signing certificates for Apollo Technologies Inc. They obtained certificates from SSL.com and GlobalSign. The certificates were used to sign OneStartInstaller, which was uploaded to VirusTotal with other names, such as “AllManualsFinder” or “PDF Viewer”. In some cases, the internal name for OneStartInstaller was “chrome_proxy” or “OneStart_proxy”.

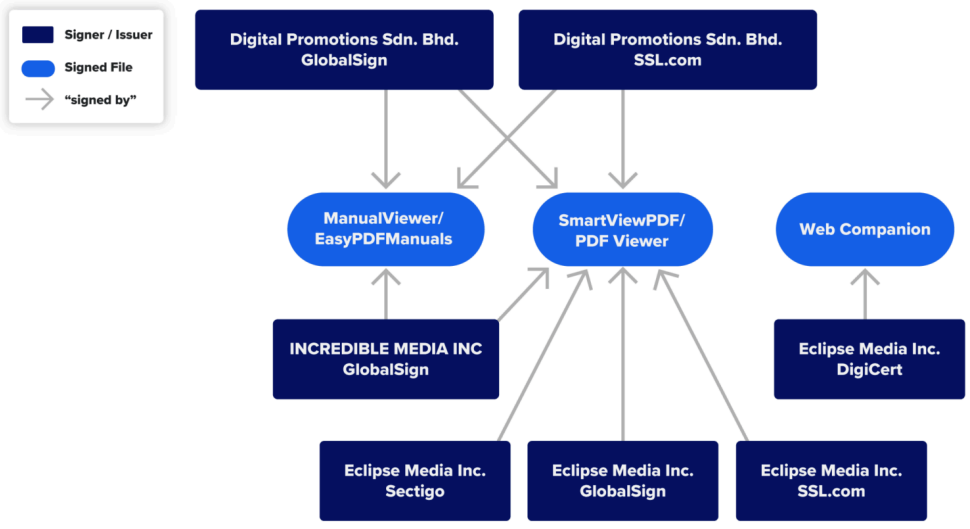
After the Apollo Technologies certificates were revoked by the certificate issuers, the actors used a certificate for Caerus Media LLC, issued by SSL.com, to sign copies of OneStart, Chrome_proxy, and EasySmart PDF. Following its revocation, they obtained certificates for “Onestart Technologies LLC” from both SSL.com and DigiCert. This may have been an attempt to appear legitimate, however, due to the history of abuse documented within this report, these were also reported and revoked.

Table 2: Representative sample using another set of certificates

File name	Example file hash	Signer (x509 CN)	Issuer	First Virus Subm date
AllManualsFinder.msi	469960964daf6666231f379604cb0cbd536b277bdb595c7ded9e8147278ba5ea	Apollo Technologies Inc.	SSL.com	2024

PDF Viewer/OneStart installer	2eace7cf97b21c58dc7dc731911c5258479661275e9a6f43870a6117694b0c82	Apollo Technologies Inc	SSL.com	2024
OneStartInstaller-v5.5.244.0.msi	c826b208e30168a7ccf9fb34a18927d60c6a4686bc5e84076216217ee9d7d3fb	Apollo Technologies Inc.	GlobalSign	2024
chrome_proxy	046d27a6097283c2619ead410201807eb5b85c4b48b50a9e49eef422a8c3b865	Apollo Technologies Inc.	GlobalSign	2024
SmartViewPDF	c0dea5039c67a46462116a345b39e3953f89b87f395b537b2a8be0e3f2b4f8bd	Apollo Technologies Inc.	GlobalSign	2024
onestart.exe	db4d49ca1adca1248124c20c0762875cafa8a6ce85a19332b17aff9c5200a291	Caerus Media LLC	SSL.com	2025
chrome_proxy	7025ec177a7df0ceca69d9e1f145c1889e39c0d7c32feeda4cb9c3a6a47e33f9	Caerus Media LLC	SSL.com	2025
EasySmartPDF	6adbdd262a335eb59c55ca1c8b21efc1cc5a8bf0f8f5662e78fd9f00141feed1	Caerus Media LLC	SSL.com	2025
PDF Editor	e27d911a785d3c22a2c023cc41b2862f15d08d2301856b33fe9a51e39398d418	Onestart Technologies LLC	SSL.com	2025
OneStart.exe	430c783801d2e30c314c76f379ed28f98c540f530f309a95c542ae68043d78b1	Onestart Technologies LLC	DigiCert	2025
OneStart_proxy	6dfd5793fa84f54be855ad4bd16bf561e6c80699527ba40e9d50ca6cd27b7768	Onestart Technologies LLC	DigiCert	2025

Figure: Diagram showing how signers and issuers relate to signed files. Squares represent signers/issuers, pills represent the files they sign, and arrows indicate 'signed by' relationships. Entity names are shown in their official casing.



Before AppSuite

Before AppSuite, the actors also had other products with the same manual finding and PDF viewing themes. Note (in the table above) that they seem to use a consistent version naming system over time for their software ("-vX.X.XXXX.X). This version numbering was used in OneStart, AppSuite, *and* the applications that came before it. Reviewing these certificates,

we see that they are clearly making iterations on the same product. Most prominent is their PDF Pro Suite, which became AppSuite-PDF.

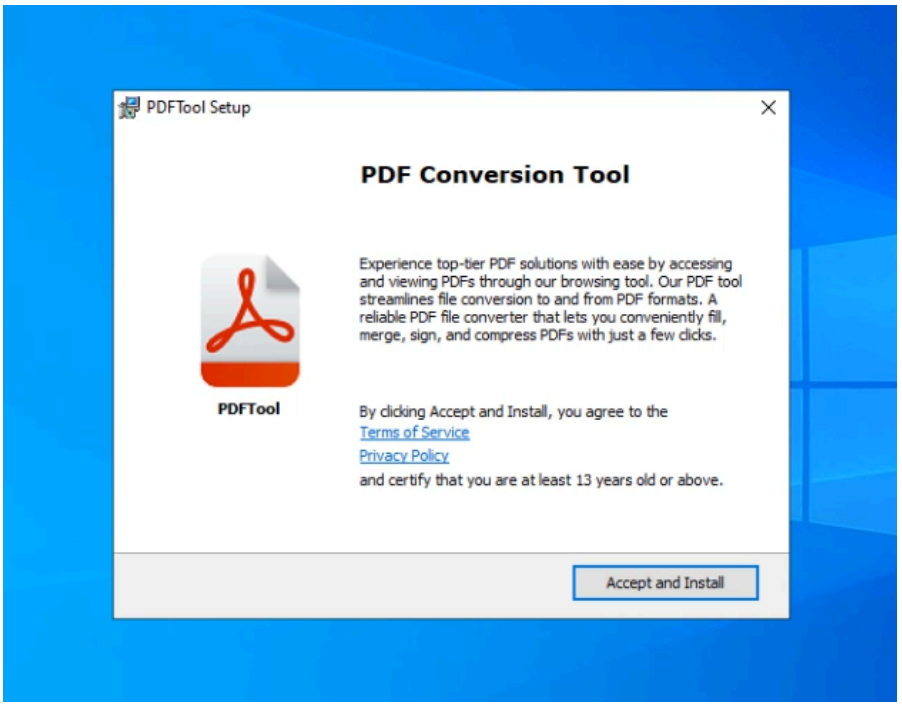


Image: Installer message from file submitted to VirusTotal on 2024-02-29. (8dfb2197e19e9dfa09cd38bc039702cf4ea7df0c4f7c16fa5df80ba2e8267b92)

Image: Installer message from file submitted to VirusTotal on 2024-08-02. (099c77409d23507d65ee7783575c77c4eeee86cd35b9338ac6fcdfef894ad472)

Image: Installer message from file submitted to VirusTotal on 2024-11-08. (84781fa57f2c01eee0e0160734019bde86c212bbaab7fce9241f84e07cee11d6)

During this time, they also acquired code-signing certificates for "Digital Promotions Sdn. Bhd." from both GlobalSign and SSL.com and many other certs from additional code authorities.

One notable certificate signer is "Eclipse Media Inc.," which was issued by GlobalSign, SSL.com, Sectigo, and DigiCert. The first three were primarily used in the PDF campaign; however, the DigiCert-issued certificate was used with another software often considered a PUP: Web Companion. The files from Eclipse Media Inc., issued by DigiCert, are important in that they show a strong connection between different campaigns. The DigiCert issued cert was issued two years earlier to the same business as indicated by the business' serial number specified in the certificate (see Appendix for a table of the business serial numbers for all the certificates.)

The files using this certificate represent a much earlier behavior of the developer: dropping files with many names, but only installing one application. In this case—as well as many earlier cases—the app installs Web Companion. In one example file, VirusTotal flags the file's primary name as "ZoomSetup_40356044.msi", but the "Names" category on the details page (pictured below), VirusTotal show that the file was uploaded with many other names, such as "TinyTaskSetup…", "WinRarSetup", and "MinecraftSetup…". Reviewing these names gives us a glimpse into the lures used to trick users into downloading the files.

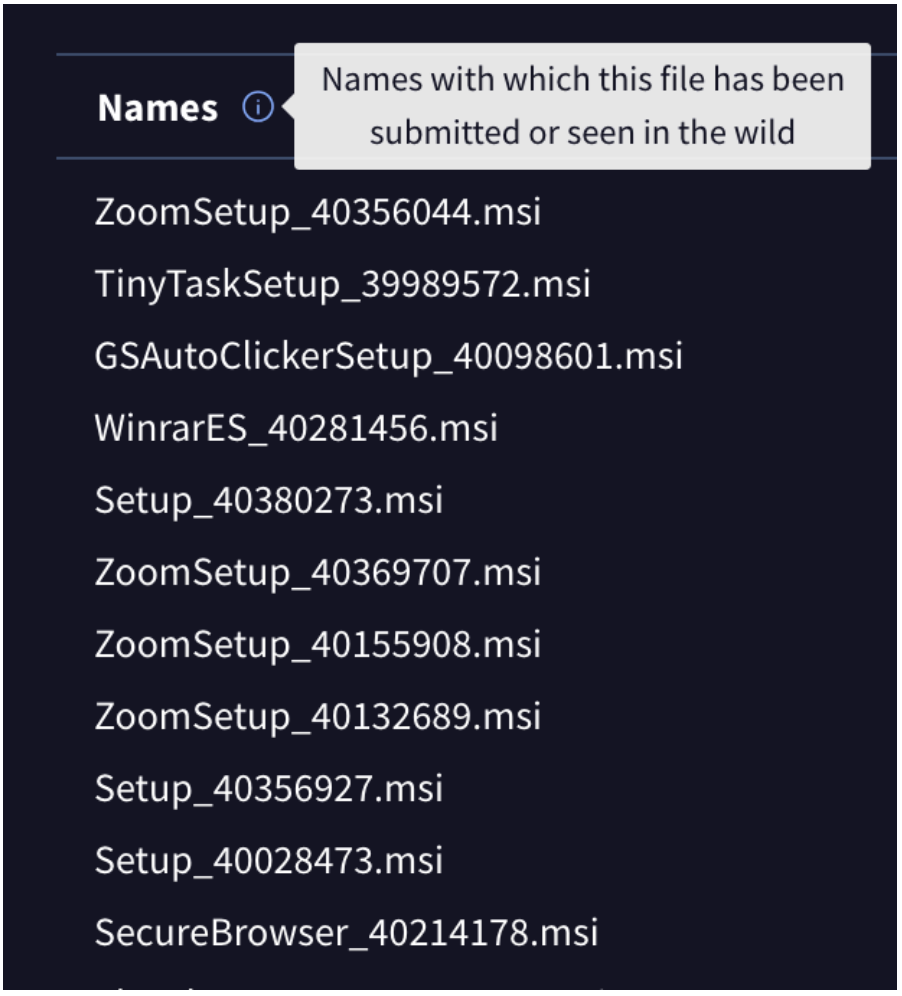
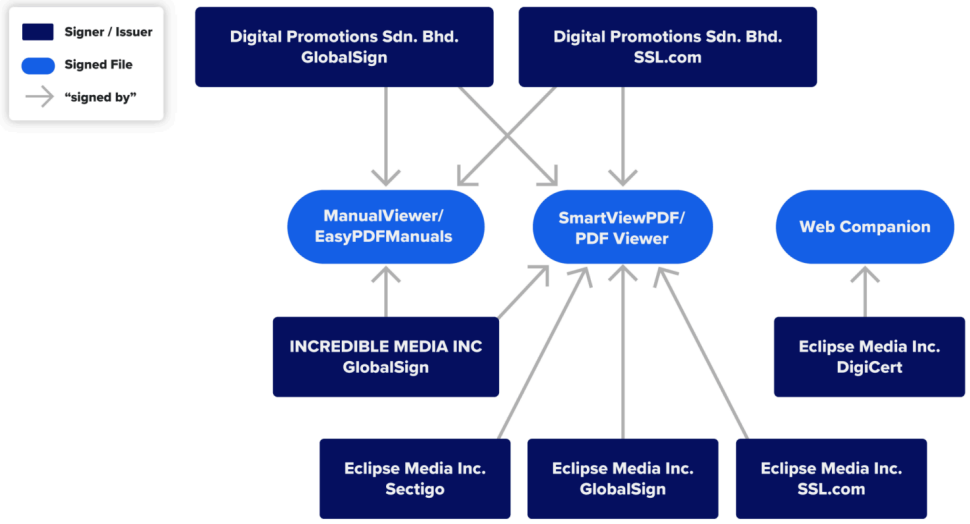


Table 3: Representative sample using another set of certificates

File name	Example SHA256	Signer (x509 CN)	Issuer
ManualsViewer-v3.3.1233.0.msi	7857a4020d08ec40f254847a9768da0432b0da6c90c7f18c68c05e0cfd0cec0b	Digital Promotions Sdn. Bhd.	GlobalSign
PDFTool-v3.2.1210.0_PDFTool.exe	fd7912de8df0ae262d77df294db71a5fcd7abeb2895214fa4f06edd6f54cce42	Digital Promotions Sdn. Bhd.	GlobalSign
PDFViewer_47171210.msi	8dfb2197e19e9dfa09cd38bc039702cf4ea7df0c4f7c16fa5df80ba2e8267b92	Digital Promotions Sdn. Bhd.	SSL.com
PDFProSuite-Patch-v10.1.2103.0.msi	a1a42a82e51d2278d38370f23524d2a715bb511312722428b4bc7f817a5532ea	Digital Promotions Sdn. Bhd.	SSL.com
PDFProSuite-v10.1.2020.0.msi	099c77409d23507d65ee7783575c77c4eeee86cd35b9338ac6fcdfef894ad472	INCREDIBLE MEDIA INC	GlobalSign
EasyPDFManuals.msi	84781fa57f2c01eee0e0160734019bde86c212bbaab7fce9241f84e07cee11d6	INCREDIBLE MEDIA INC	GlobalSign

PDFFlex-v3.202.1115.0.msi	bbee7d6beb0b1fc2f19bbda5a0765c00af7ec16642f7b4ad6f7bc8f6d43a2cc7	Eclipse Media Inc.	GlobalSign
PDFFlex-v4.110.1239.13.msi	7022b6b2caa7ecfc1a9575b74cce793336fc5fe4571955b1240716d9ab4b9e84	Eclipse Media Inc.	SSL.com
PDFFlex-v3.410.1238.10.msi	e06c05b3e19e78108a4f4174219862c4680dd1ee4b5dbef18b9295fc846eda98	ECLIPSE MEDIA INC.	Sectigo
ZoomSetup_40356044.msi (file is an installer for WebCompanion)	fe30b6b149d8a7e5da77faa6a6f36ce78132b682fde4f48fc77939de870bbabc	Eclipse Media Inc.	DigiCert

Figure: Diagram showing how signers and issuers relate to signed files. Squares represent signers/issuers, pills represent the files they sign, and arrows indicate 'signed by' relationships. Entity names are shown in their official casing.



Footnote: The Digicert-issued certificate for Eclipse Media Inc. uses the same RDN number as the same company name certificates issued by Sectigo, GlobalSign, and SSL.com.

Web companion

As we saw in the above graph and table, certificates associated with BaoLoader are also being used to load a version of Browser Assistant/Web Companion. The official Web Companion product is signed by "7270356 Canada Inc." and is a product of LavaSoft (also known as Adaware and/or Avanquest). The actors had a *much* longer history of loading the Web Companion software onto hosts and the actors re-sign some Web Companion dynamic link libraries (DLL) that are deployed. These require additional analysis to understand if or how they were manipulated. (See table 4 below for a sample of the signed DLL observed.)

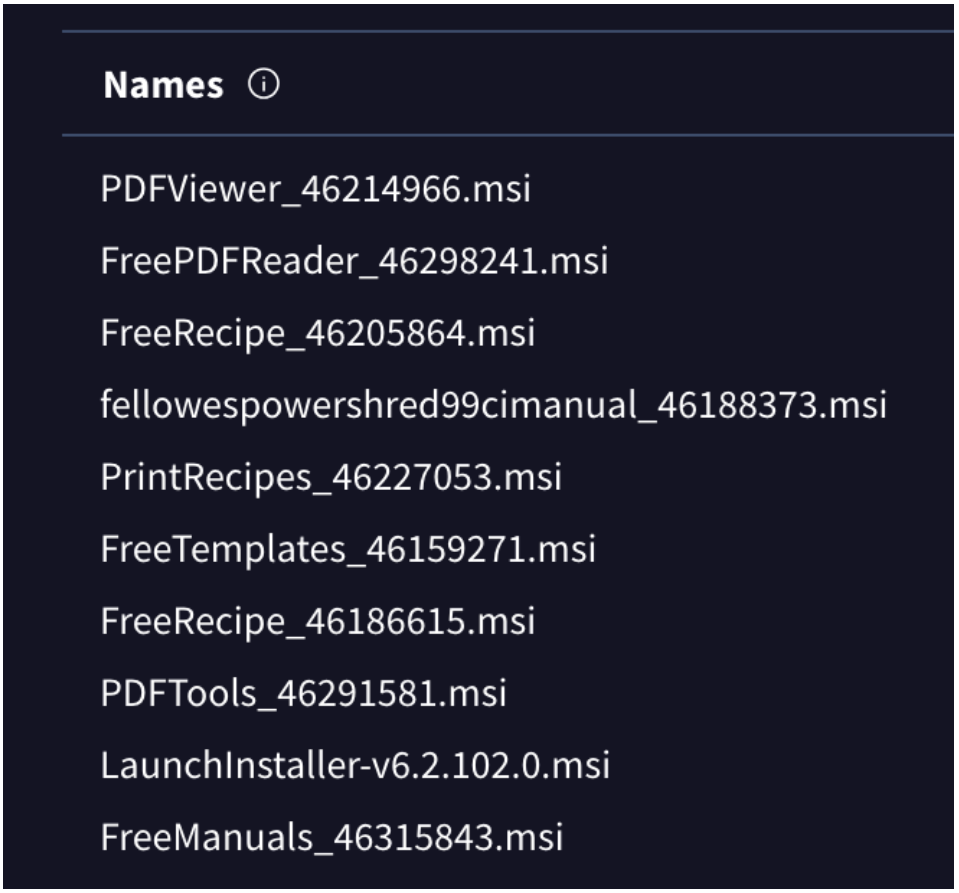
These files—and the ones mentioned below—exhibit behavior that most SOC analysts will recognize as known and/or expected Web Companion behavior, executing the following PowerShell:

"C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" -noninteractive -ExecutionPolicy bypass -c "$w="$env:APPDATA"+'/BBWC/';
[Reflection.Assembly]::Load([System.IO.File]::ReadAllBytes($w+'Newtonsoft.Json.dll'));
[Reflection.Assembly]::Load([System.IO.File]::ReadAllBytes($w+'System.Data.SQLite.dll'));
[Reflection.Assembly]::Load([System.IO.File]::ReadAllBytes($w+'ICSharpCode.SharpZipLib.dll'));
[Reflection.Assembly]::Load([System.IO.File]::ReadAllBytes($w+'LZ4.dll'));$f=$w+'WC.txt';$h=Get-Content -Path $f -Raw;$h=Get-Content -Path $f -Raw;[byte[]]$bytes=($h -split '(.{2})' -ne '' -replace '^','0X');
[Reflection.Assembly]::Load($bytes);[WebCompanion.StartUp]::Start()"

This behavior is noteworthy in that it clearly identifies it as Web Companion installation. It's also noteworthy because the behavior exhibited by this PowerShell is generally treated as highly suspicious, but is considered acceptable because many consider Web Companion as standard adware. This borderline-acceptable behavior seemed to play well with the actors using Web Companion.

As in other cases, we see the actors leverage certificates with the same certificate signer provided by multiple issuers: “Astral Media Inc” was issued by GlobalSign, SSL.com, and DigiCert. And “Interlink Media Inc.” was issued both by GlobalSign and SSL.com.

With many of the certificates discussed here, files using them have been uploaded to VirusTotal with a wide range of names associated with the same file. One example is “e1d6ea166a0a09b4af4f697a0a88ff8b638f7f1738b0a5fa14f43bdf8e85739e”, which was uploaded under many names, including “PDFViewer”, “FreeRecipe”, “FreeManuals”, and others.



Other signed files during this period include applications such as “Launch Browser” (Interlink Media Inc./SSL.com), which was an alternative version of the OneStart Browser.

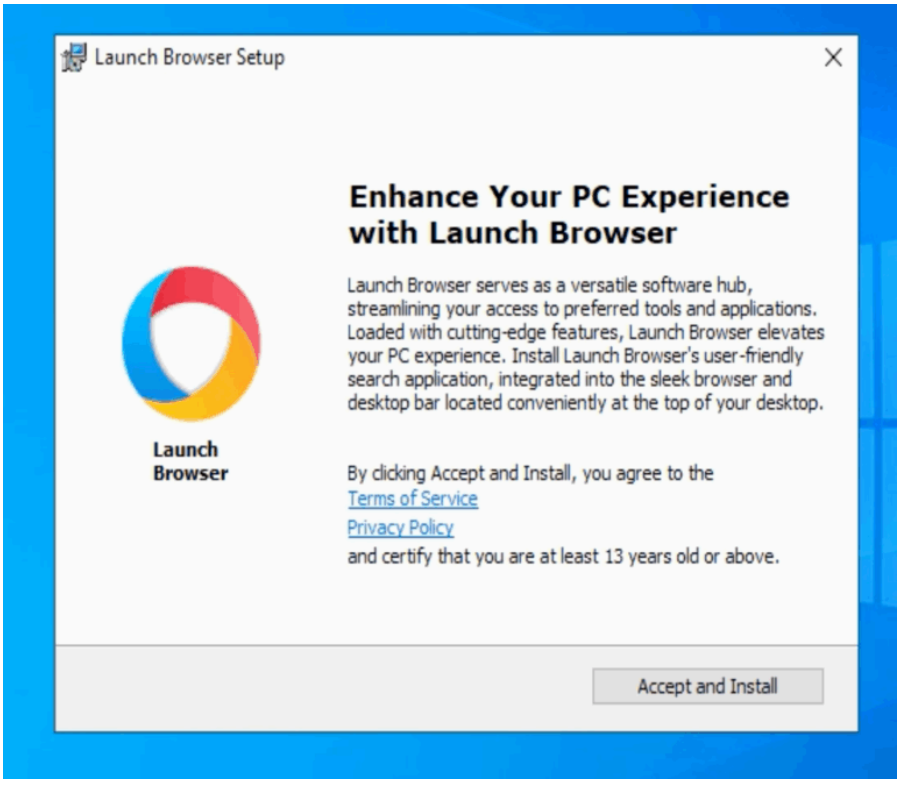


Image: Launch Browser installer prompt. This file was uploaded as PDFViewer, FreeRecipe, FreeManuals, etc. First submitted to VirusTotal on 2024-01-15 (e1d6ea166a0a09b4af4f697a0a88ff8b638f7f1738b0a5fa14f43bdf8e85739e)

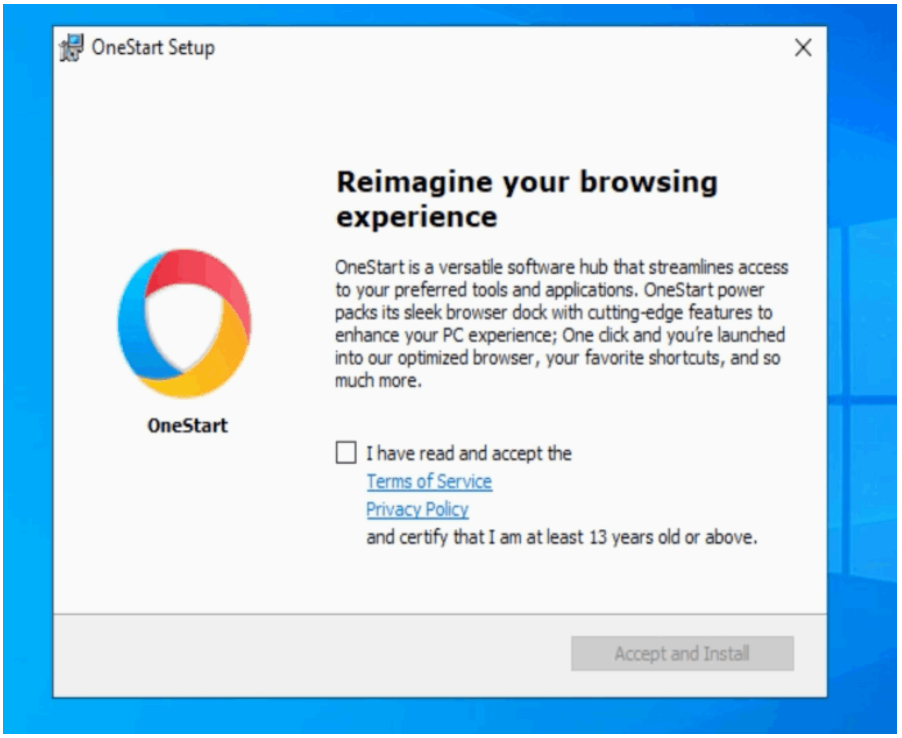


Image: OneStart installer prompt. This file was uploaded to VirusTotal as "PDFViewer". First uploaded to VirusTotal on 2023-09-18. (a704398d2446d297938d773f22e3a703b8e8b9a411edcf0f821dff6e975f2724)

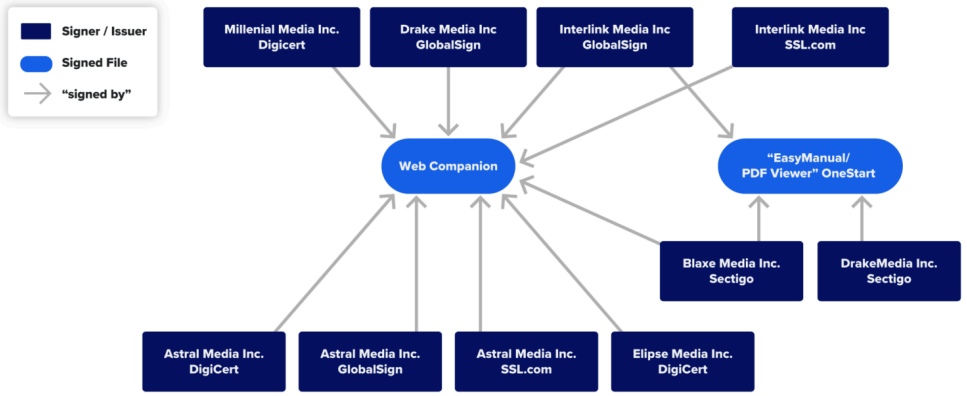
Table 4: Representative sample using another set of certificates

File name	Example SHA256	Signer (x509 CN)	Issuer

IEBrowserAssistantSetup.msi	10acb7208a455b07940336a489f7c3cf34904f887b1f8904f5bff54569963f0b	ASTRAL MEDIA INC.	GlobalSigı
BAv1411302.msi	3276154a7f2ea64e43cf6dbec33bfb20ee0d46b2ca03d5d0c7f51ec803f7101d	Astral Media Inc	SSL.com
BAv1403298.msi	35ab1c46e0341e6cda9ba1db61e8d8c0496df90ee758ed02d15f564a62b35da8	Astral Media Inc.	DigiCert
EasyQuickManuals_46736718.msi / PDFViewer_46586326.msi	45fb5807dc1f88cb65dbfe611028ad09f1e85ab0ab244a1f691408c063851cc1	Interlink Media Inc.	GlobalSigı
LaunchBrowserInstaller-v5.2.153.0.msi / PDFViewer_45578527.msi	34c12da57921ab46ae9f06b321b3d47cc41d7bcb66d6635e3db58d3f6e7c4156	Interlink Media Inc.	SSL.com
PDFViewer_46214966.msi	e1d6ea166a0a09b4af4f697a0a88ff8b638f7f1738b0a5fa14f43bdf8e85739e	Blaze Media Inc	Sectigo
PDFTools_12345678.msi	e505e4bc6c76f8ccd1d626832d1d5d5d2852a5c78016c43bdc2f502af6e40396	Drake Media Inc	Entrust
CSharpDLL.dll	5bff84ba6e59086ca5ae880f0f299b59bc222a1e85f57ef620d5f725fc398ff8	Blaze Media Inc	Sectigo
DarkNet.dll	162e65e8e74ed4637184a827629636f0c687c008e0937537fe32ca85ab21bd71	Blaze Media Inc	Sectigo
WindowsDisplayAPI.dll	492193072be8c959112abd720360cedb24f564f27c375bf57346030b78b4db96	Blaze Media Inc	Sectigo
OperaSharpDLL.dll	7ba95a9470697f33c5bd4e047253c2df035aedb96856126642af89c348bf3652	Interlink Media Inc.	GlobalSigı
WebCompanion.dll	3a3511aa0c7e42daa2b6467bdd6fd2006605c6a72667300ee3740df930be51d2	Millennial Media Inc.*	DigiCert

**This cert was used only to sign Web Companion DLL. However, due to the actors' use of certificates issued to similarly-named companies — namely, the ones seen in this table, which are all registered in Panama — we're highly confident the certificate was theirs as well.*

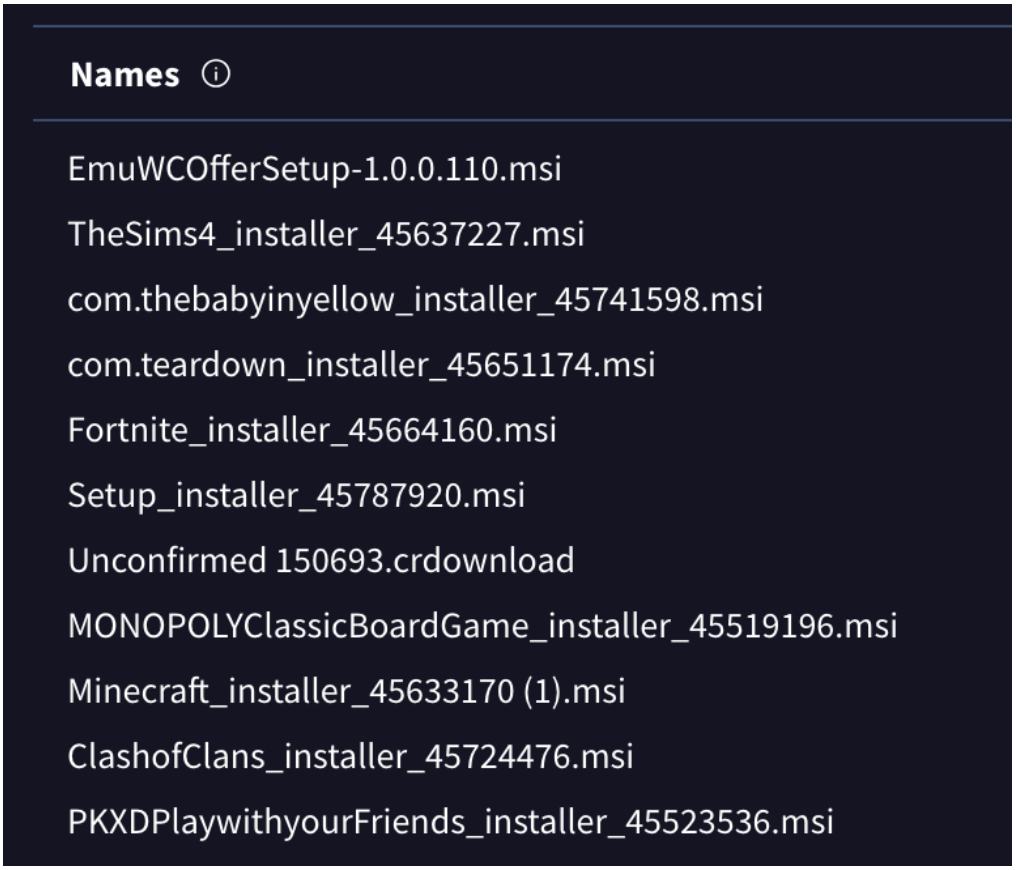
Figure: Diagram showing how signers and issuers relate to signed files. Squares represent signers/issuers, pills represent the files they sign, and arrows indicate 'signed by' relationships. Entity names are shown in their official casing.



Not only PDF editors

While the above analysis focused on PDF editors, manual finders, and OneStart, the actor team didn't just target users looking for this help. They also targeted broader audiences looking for games, wallpapers, and other software (note the re-use of "Drake Media Inc"). This time, it uses a certificate from GlobalSign, whereas above, Entrust issued it.

The team of malicious actors used the "Drake Media Inc" certificate to sign the file "EmuWCOfferSetup-1.0.0.110.msi" to VirusTotal, which was later distributed disguised as games. We suspect that the "EmuWCOfferSetup-1.0.0.110.msi" file was uploaded by the actors themselves; the name differs from the other uploads, follows the same version naming convention, and contains the acronym "WC", which likely means "Web Companion," as it also installs Web Companion.



We've seen these dynamically-named applications used by the Baoloader developers before. However, with the Baoloader malware specifically, the lures are normally productivity apps (PDF Editors and popular collaboration tools). And yet this time, there are also versions of the malware disguised as game installers.

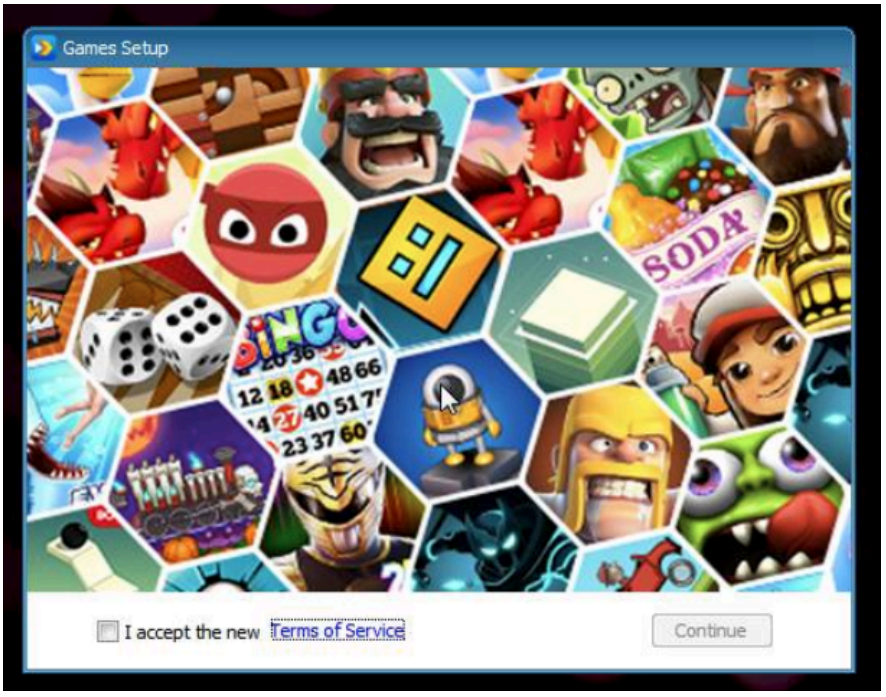


Table 5: Representative sample using another set of certificates uploaded imitating game installers

File name	Example SHA256	Signer	Issuer	First VirusTotal Submission date
EmuWCOfferSetup-1.0.0.110.msi	aad5be480738f546f7538f70463f4144bb5654cf74bbf99aa9b5b2917164cbb4	Drake Media Inc.	GlobalSign	2023-11-06
games_1329303.exe	6b6fc62a294d5ef1c619d623f1cf6d735d9f191df9ef5c745b0881b1e01b8565	Realistic Media Inc.	DigiCert	2018-12-06

Chromeloader, is that you?

The early deviation into deploying games is interesting because this behavior is *remarkably* close to what we've seen of the malware "Chromeloader." In fact, the malware shares many similarities, such as

- Heavy certificate abuse, including certificates for organizations with multiple issuers
- During lifetime, using payload to load Chrome extensions
- During lifetime, using node.exe to execute malicious JavaScript
- Use cloudfront domains in the first stage of the malware
- Use DGA or random domain names for second-stage command and control
- Use scheduled tasks for persistence mechanism
- Target both Windows and MacOS*

*BaoLoader's MacOS targeting hasn't been thoroughly explored. From what we identified, this was only found recently (the first submission was uploaded to VirusTotal on 2025-06-24). They recreated a ManualFinder app which received a developer ID that's since been revoked. The developer ID is for "IENGINEERING PRIVATE LIMITED".

However, our research leads us to believe that BaoLoader and Chromeloader are either completely unrelated *or* separate teams that work independently based on their certificate abuse trends. BaoLoader often uses certificates from Panama, Malaysia, and the US. Chromeloader often uses certificates from Israel, Germany, Great Britain, and Slovenia. Further, we didn't observe the same certificates used across the two different malware.

For certificates used by Chromeloader, see certgraveyard.org/lookup?detail_type=malware&query=Chromeloader (requires GitHub login).

Not Chromeloader, but maybe TamperedChef?

The name TamperedChef became associated with BaoLoader after a tweet by Karsten Hahn. The tweet followed research from GDATA where TamperedChef was grouped into some other apps that have functional capabilities but fit the concept of a trojan. Like TamperedChef, AppSuite-PDF and other apps have been functional (for the most part). GDATA argues that this is due to AI enabling cybercriminals to create more convincing applications. The name TamperedChef started being applied to the campaign by accident and has now stuck. The original TamperedChef name was a joke name given to a different malware—a malware which offered a recipe app, but had covert means of communication, including hidden characters.

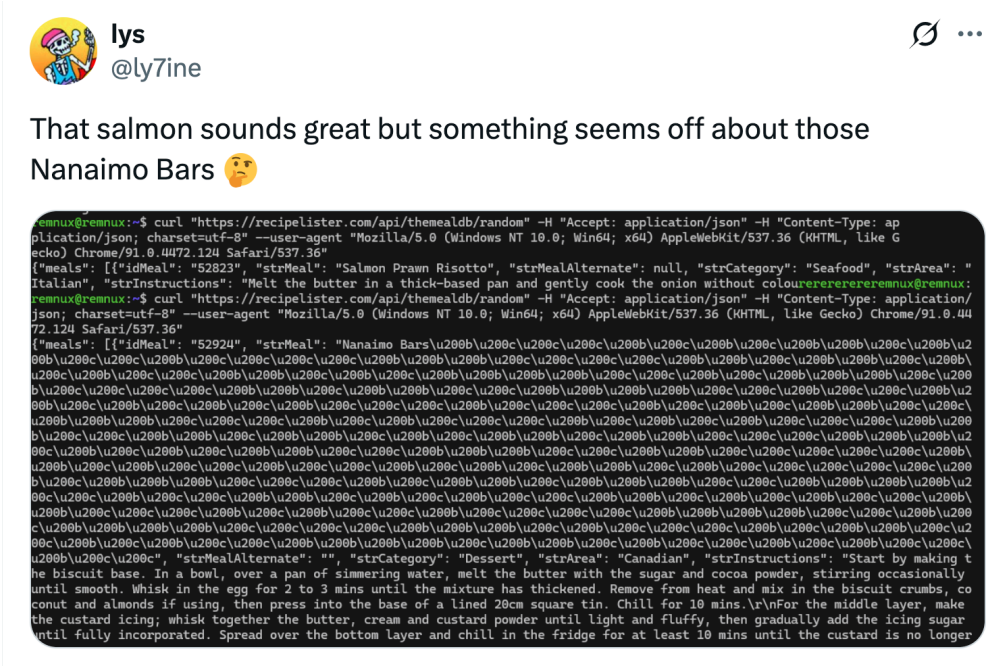


Image: Twitter user @ly7ine showing an example of hidden characters in a recipe.

This malware was distributed under a few different names, such as "RecipeLister," "LookUpKitchen," and "Fast-Forks" of which, "RecipeLister.exe" was the most common. After they were exposed by certificate revocation and public blogs, the actor moved onto a different theme: apps allowing users to search for pictures (see image below).

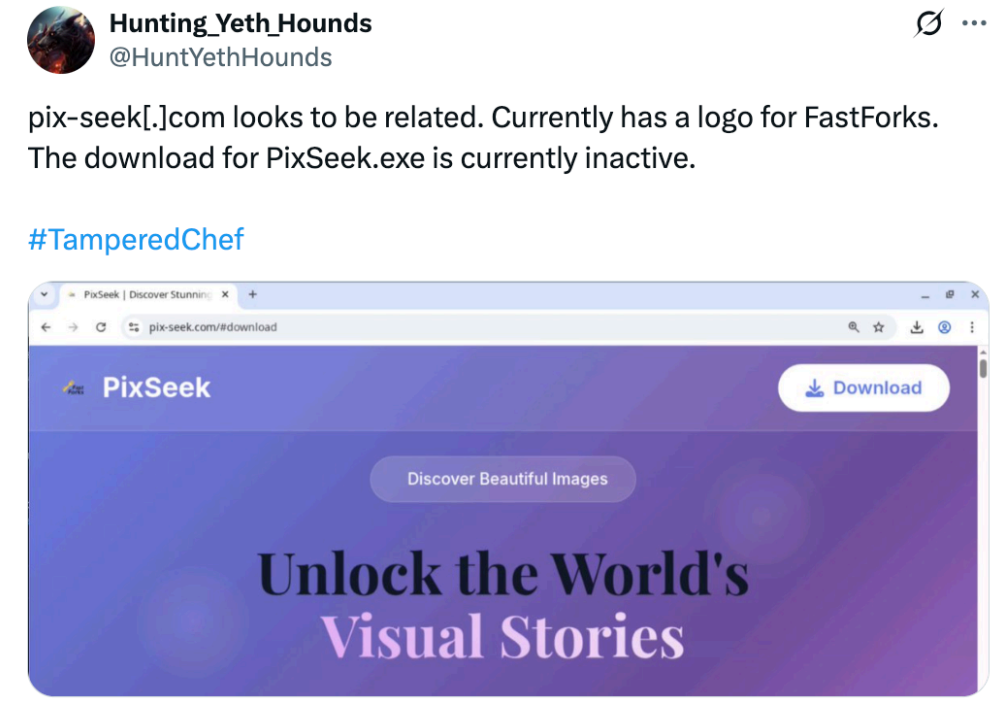


Image: Twitter user @HuntYethHounds shows the owner of Fast-Forks re-used the template of their website for a new website. The icon and favicon still show “Fast-Forks”.

TamperedChef’s use of hidden content in webpages differs significantly tactics used by BaoLoader. The two also differ in their use of code-signing certificates: TamperedChef used code-signing certificates issued to companies in Ukraine and Great Britain while BaoLoader consistently used certificates from Panama and Malaysia as mentioned above. We don’t see any connection linking the original TamperedChef and BaoLoader.

File name	SHA256 hash	Signer	Issuer	First VirusTotal Submission date
RecipeLister.exe	1619bcad3785be31ac2fdee0ab91392d08d9392032246e42673c3cb8964d4cb7	Global Tech Allies ltd	SSL.com	2025-05-06
Forks.exe	d8bff72de51213510004a2652b9e31b48a25e2eb0d7184fab4ef9014fc85e145	IT BRIDGE CONNECT LLC	GlobalSign	2025-06-11

Why it matters

Code-signing certificates are intended to validate that software is from a known provider (and is likely safe). When software is signed and distributed by dozens of providers, it should raise suspicion. BaoLoader is an example of this, but went relatively unnoticed for years. It’s only the recent changes to their behavior that’s put their infrastructure and malware in the spotlight. However, their abuse of code-signing certificates has been a known issue, as evidenced by certificate providers revoking the certificates over the years.

Analysis of irregularities around code-signing can provide defenders early warning that something’s wrong. The clearest indicator is when the software, the metadata about the application, and the application itself don’t line up. This can help defenders identify malicious programs even when antivirus or other tools haven’t identified suspicious indicators. Code-signing certificates can also be used for threat hunting to identify files already known to be malicious by the security community.

Organizations should consider controls available to them to prevent unwanted and malicious software in their environment. Such unwanted software may be downloaded for many reasons—by accident from phishing emails, users attempting to download a PDF editing tool to help them do their job, or many other situations. However, many controls exist to help prevent these software—such as AppLocker for Windows—and application whitelisting. These tools play a vital part in keeping known (and stealthy) malicious files off systems.

Questions or additional insights regarding BaoLoader or any of the analysis detailed here? We’d love to hear from you. Reach out anytime at intel@expel.com.

Appendix

The following are the company details extracted from the code-signing certificates. In most certificates, the signer’s state, country, locality (region), and business serial number are available. Some columns have been removed for readability, but the full data can be viewed here: https://certgraveyard.org/lookup?detail_type=malware&query=BaoLoader and https://certgraveyard.org/lookup?detail_type=malware&query=OneStart.

Signer	Issuer short	Valid start date	Country	Locality	RDN serial number
Apollo Technologies Inc	SSL.com	7/28/23	PA	Panama City	155722923
Astral Media Inc	SSL.com	4/11/23	PA	Panama City	155704413
Astral Media Inc.	DigiCert	5/10/21	PA	Panama City	155704413
ASTRAL MEDIA INC.	GlobalSign	5/3/23	PA	Panama City	155704413

Blaze Media Inc.	DigiCert	9/19/22	PA	Panama City	155704406
Caerus Media LLC	SSL.com	9/04/24	US	Delaware	6125248
Digital Promotions Sdn. Bhd.	GlobalSign	3/6/24	MY	Skudai	1505433-P
Digital Promotions Sdn. Bhd.	SSL.com	4/3/24	MY	Skudai	202301011511
Digital Promotions Sdn. Bhd.	SSL.com	6/15/23	MY	Skudai	202301011511
Drake Media Inc	Entrust	4/12/23	PA	Panama City	155704428
Drake Media Inc	GlobalSign	3/24/23	PA	Cuidad de Panama	155704428
ECHO INFINI SDN. BHD.	SSL.com	1/13/25	MY	Skudai	202401031184
ECHO INFINI SDN. BHD.	SSL.com	1/13/25	MY	Skudai	202401031184
Echo Infini Sdn. Bhd.	GlobalSign	12/9/24	MY	Johor Bahru	1577033-U
Eclipse Media Inc	SSL.com	7/2/24	PA	Panama City	155704432
Eclipse Media Inc.	DigiCert	1/21/22	PA	Panama City	155704432
ECLIPSE MEDIA INC.	Sectigo	6/20/24	PA	?Not specified?	155704432
Eclipse Media Inc.	GlobalSign	1/17/24	PA	Panama City	155704432-2-2021
GLINT SOFTWARE SDN. BHD.	SSL.com	4/24/25	MY	Skudai	202401011747
INCREDIBLE MEDIA INC	GlobalSign	4/18/24	PA	Cuidad de Panama	155722937
Interlink Media Inc.	GlobalSign	11/2/23	PA	Cuidad de Panama	155704402
Interlink Media Inc.	SSL.com	5/24/23	PA	Panama City	155704402
Millennial Media Inc.	DigiCert	2/28/22	PA	Panama City	155704409
Onestart Technologies LLC	SSL.com	3/6/25	US	Delaware	10070121
Onestart Technologies LLC	DigiCert	5/16/25	US	Delaware	10070121
Realistic Media Inc.	DigiCert	8/2/18	VG	Road Town	1817807
