

Tracking TamperedChef Clusters via Certificate and Code Reuse

 unit42.paloaltonetworks.com/tracking-tampered-chef-clusters

Joseph Ganter

May 20, 2026

Executive Summary

This article documents novel activity clusters that have significant overlap with the publicly described threat known as TamperedChef (aka EvilAI). TamperedChef-style malware is trojanized productivity software, such as PDF editors or calendars, that deliver malicious payloads.

These campaigns typically employ malicious ads that direct users to sites hosting the applications. While this style of malware shares many similarities in technical operation, installation lures and distribution methods, we do not attribute it to a single author or group.

TamperedChef-style malware samples share characteristics with potentially unwanted programs (PUPs) and adware. These include robust mechanisms to remain persistent, and end-user licensing agreements (EULAs) that attempt to legally cover the software's questionable actions. However, TamperedChef-style malware is far more stealthy than PUPs or adware, remaining dormant for weeks to months before activating. This includes continuous command and control (C2) methods enabling adversaries to retrieve additional payloads, such as information stealers, proxy tooling or remote access Trojans (RATs).

We have been tracking several campaigns of TamperedChef-style activity starting in 2024, with three distinct clusters: CL-CRI-1089, CL-UNK-1090 and CL-UNK-1110. Between the three clusters of activity, we have identified over 4,000 samples across 100 unique variants.

Palo Alto Networks customers are better protected from TamperedChef activity discussed in this article through the following products and services:

- [Cortex XDR](#) and [XSIAM](#)
- [Prisma Browser](#)

If you think you might have been compromised or have an urgent matter, contact the [Unit 42 Incident Response team](#).

Related Unit 42 Topics [AI](#), [Malware](#), [Adware](#), [RATs](#), [Malvertising](#)

The Rise of Malicious Productivity Applications

Since early 2024, we have observed a sharp increase in information stealer-style incidents originating from software mimicking legitimate productivity tools (e.g., PDF editors, ZIP file extractors, GIF image makers). Upon deeper inspection, these applications generally contain code that enables the delivery of arbitrary binaries. These features are typically used to deploy stealer malware.

In 2025, our telemetry revealed over 100 unique variants of malware masquerading as productivity software. They all contained a malicious component, such as basic RAT capabilities, or delivering adware and infostealers.

Due to their legitimate functionality and tendency to remain dormant for long periods of time, these applications often go unnoticed by the victim. They are also commonly downplayed or miscategorized by defenders and security researchers as potentially unwanted programs (PUPs). Because these applications can execute arbitrary code on victims' machines, either directly or indirectly through module loads, these threats are more significant than mere background annoyances or adware.

We have been able to track over 4,000 file hashes and 81 unique code signing organisations through several methods, including:

- Reviewing code-signing certificates of the binaries
- Analyzing code reuse among the binaries
- Open-source intelligence (OSINT) on corporate structures for organizations distributing the binaries
- Leveraging ad transparency platforms to hunt for advertising overlaps that can identify additional organizations distributing the binaries

We have identified TamperedChef-style malware campaigns starting in 2023. These malicious productivity application campaigns include AppSuite PDF, Calendaromatic, JustAskJacky and CrystalPDF.

Masquerading in Plain Sight

The actors behind these campaigns take steps not commonly observed with other adware groups to remain undetected. In some cases, these attackers appear to diversify their revenue streams through more aggressive and malicious activities. This diversification includes deploying infostealers, establishing residential proxies and exhibiting behavior that resembles access brokers.

These applications avoid many of the common indicators that users are trained to associate with downloading malicious software, such as:

- Distributing via well-built, legitimate-looking websites
 - Without ads (as shown in Figure 1)
 - Appearing modern and credible
 - Containing common elements like descriptions, legal terms and contact pages
- Leveraging unique and contextually relevant domains for each campaign
- One-click download buttons distributed by large content distribution networks (CDNs) to minimize friction
- Providing promised functionality with minimal bloat, meaning victims are not likely to suspect anything is amiss

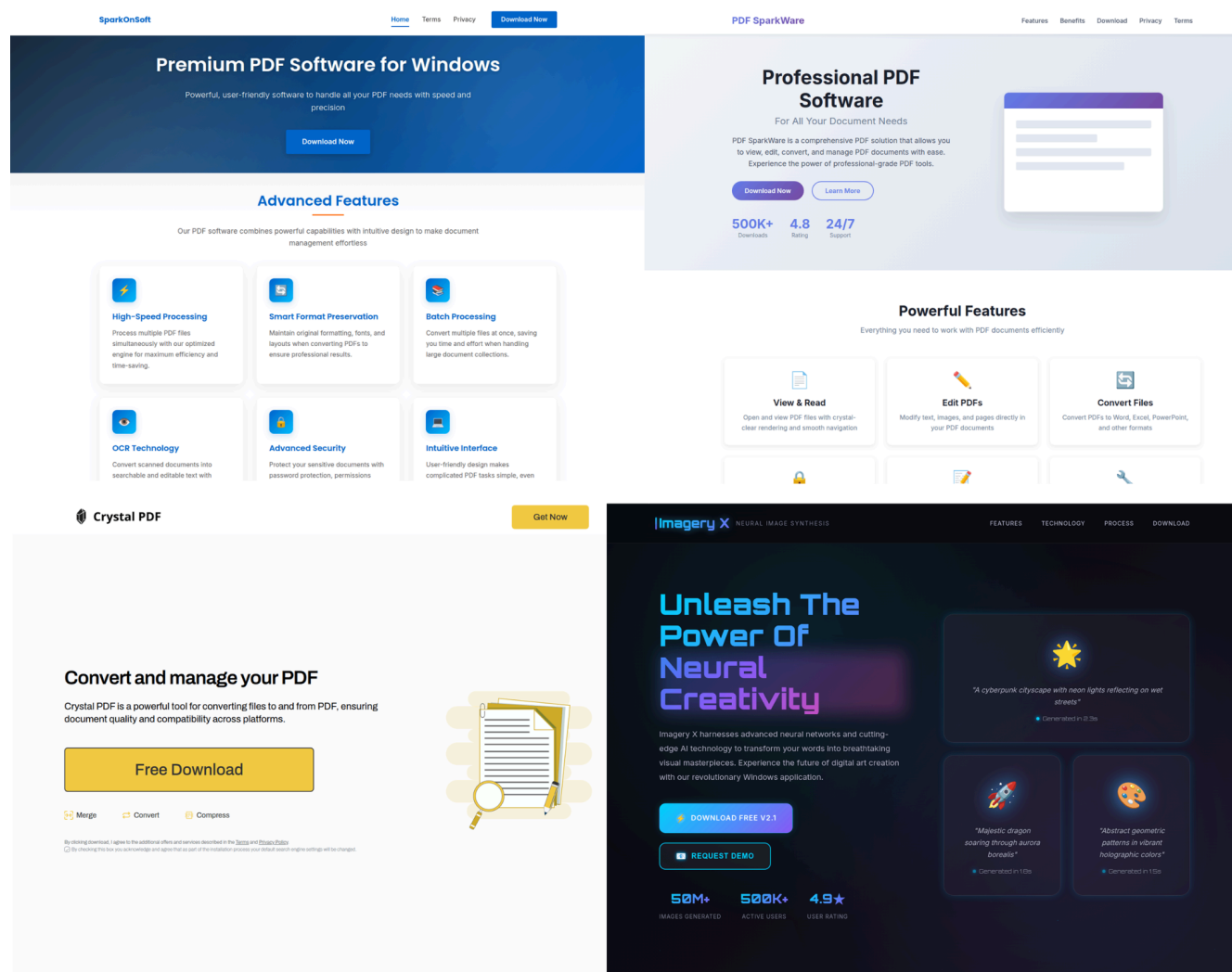


Figure 1. Examples of download pages for TamperedChef-style fake productivity applications.

Attackers also employ several tricks to avoid detection. These tricks include:

- Using code signing to increase the apparent legitimacy of the binaries

- Rebuilding binaries with only minor changes on a frequent basis to minimize the effectiveness of static or hash-based detection
 - The exact frequency varies, but is typically between one week and one month per rebuild
- Remaining dormant for periods of weeks to months before retrieving or running malicious components

This combination of technical and social masquerading enables these applications to remain undiscovered, unreported and free to operate without resistance for months — if not years — at a time.

What Is Adware vs. Malware?

Adware is a class of software designed to increase the number of ads a user observes. The more ads they observe, the more money for the distributor. This is typically done with some form of browser manipulation or additional free tooling bundled alongside downloads.

Adware sits in a middle zone between malware and legitimate software, often employing malware-like tactics to maintain persistence or display more ads to users. The distinction between malware and adware can be so fine that they are indistinguishable from each other when statically analyzed, only becoming clear after misuse occurs. Adware and malware are also often interlinked, with many seemingly legitimate adware developers overstepping into malware territory, either naively or intentionally.

Modern adware also walks the line between legal and illegal behavior. EULAs are ways that the groups behind adware and TamperedChef-style malware attempt to protect themselves legally. Examples of this are found on websites distributing TamperedChef-style software, such as one from `hxxps[:]//www.crystalpdf[.]com/conditions:`

“The Additional Services offer users enhanced, tailored features. Be aware that using these services may modify your browser’s new tab settings or installed features, possibly altering your browser configuration.”

However, TamperedChef-style programs execute commands remotely, exfiltrate users' credentials and deploy malware without consent. These actions firmly place them in the malware category.

A Historical Review of TamperedChef (Aka EvilAI)

The name TamperedChef was initially given to a cluster of activity that included several malicious recipe applications, PDF editors, manuals and search assistant applications. It

started to see widespread installation in June 2025, with some evidence suggesting these applications have been in the wild since February 2025.

As reporting on malicious productivity apps within the cybersecurity community grew, TamperedChef became a broad, informal term for several productivity software campaigns. These campaigns are likely not all operated by the same group.

The confusion in previous reporting is understandable, as many of the actors are leveraging extremely similar tactics, techniques and procedures (TTPs) and lures. The differences only become apparent when observing the infrastructure, code quality and organizations tied to the code signing. It is important to understand these differences to separate the attackers' motivations, capability and risks.

We identified and tracked three major clusters of activity that share many of the same operational traits, but we believe these represent three distinct groups. We track the three main activity clusters as CL-CRI-1089, CL-UNK-1090 and CL-UNK-1110.

The CL-UNK-1110 cluster is most commonly associated with the TamperedChef alias and includes campaigns distributing applications such as:

- JustAskJacky
- GoCookMate
- RocketPDFPro
- ManualReaderPro

[Acronis has researched and reported](#) on this cluster in detail. While this cluster remains active and significant, the primary focus of our analysis will be on the two other clusters, CL-CRI-1089 and CL-UNK-1090.

The CL-CRI-1089 cluster has been identified as active since early 2023. It includes several high-profile campaigns distributing applications such as:

- Calendaromatic
- DocuFlex
- AppSuite PDF

These campaigns leverage a diverse set of deployment methods and show the most change when it comes to the malware's techniques and tactics. This group leveraged infrastructure and code-signing certificates related to Ukrainian, Malaysian and British entities, which has remained consistent over the last two years of operation.

CL-UNK-1090 is unique in its clear evidence of vertical integration between marketing and malware creation. Similar to other clusters, the group behind this cluster distributes its malware via malicious advertisements (aka malvertisements).

A review of public records on corporate structures shows that, unlike the other groups, CL-UNK-1090 operators own both the code-signing companies and the ad agencies distributing the malware. This cluster used primarily Israeli infrastructure and code signing entities. It is responsible for several recent campaigns, including:

- CrystalPDF
- Easy2Convert
- PDF-Ezy

Victimology

We have observed approximately 12,000 unique instances of this fake productivity software across our customer base. Our analysis shows that this threat is global with no significant geographic or sector targeting within the Managed Threat Hunting customer base.

The data highlights that while Israel and the U.S. see slightly higher targeting than other countries, TamperedChef-style malware is seen globally in non-negligible volumes.

This is consistent across all three clusters, indicating that they all appear to operate globally.

Tracking TamperedChef-Style Samples

Understanding the capability of these threats is crucial to detection, response and disruption. Fortunately, the malware operators have made several design decisions that we can leverage to identify and link large portions of their operations.

Tracking via Code-Signing Certificates, Code Reuse and Infrastructure Overlaps

One unique attribute of the TamperedChef-style malware is that almost all the first-stage binaries are signed with legitimate code-signing certificates. Attackers used code-signing to add stealth to these payloads. However, a lack of proper certificate hygiene allowed us to follow these samples further than any one campaign.

We initially identified code signing reuse with the Calendaromatic campaign. This campaign involved a simple [Neutralinojs](#) framework-based calendar app, contained in a 7z self-

extracting archive (SFX). The calendar app would operate as expected, but it also contained a relatively basic RAT that enabled attackers to collect and install a second-stage payload.

This campaign gained some attention due to its novel use of homoglyphs to obfuscate the incoming command strings. The 7zSFX when extracted contains both a [calendaromatic-win_x64.exe](#) binary that is essentially just a wrapper for the real bulk of the code, a heavily obfuscated Neutralinojs resource file named resources.neu.

Public reporting highlighted that the 7zSFX file was signed by CROWN SKY LLC. Digging further through malware repositories, we identified four total files with the same core behavior of a 7zSFX file containing a calendaromatic-win_x64.exe binary and a resources.neu file. The resources.neu file varied across the samples. However, all appeared to contain similar functionality with differing C2 locations.

Of these four samples identified, we identified two unique signers. Samples [one](#) and [two](#) were signed by CROWN SKY LLC and sample [three](#) was signed by MARKET FUSION INNOVATIONS LLC. The final sample was found to not be signed and may not have been deployed widely.

Code-signing certificates are considered private material and not commonly shared between entities. A single code base signed by two uniquely authored certificates generally indicates that a single entity or actor is in possession of both code-signing certificates. This can occur for several reasons, including certificate theft, a single entity with ownership of two or more organisations (e.g., shell corporations) or organisations providing code signing as a service.

Reviewing sample repositories for evidence of this new signer, we found two additional campaigns that we identified as related to the Calendaromatic operators: PDFPrime and ManualzPDF. Both PDFPrime and ManualzPDF campaigns share striking similarities and likely share a codebase.

Similarities between the samples include:

- The same C2 domain structures
- Shared code signing dates
- Shared embedded PDF editors

However, these samples are very distinct from the Calendaromatic campaign, sharing no code. This highlights attackers' preference to abandon codebases upon discovery rather than iterate and evolve. Figure 2 below shows a simplified view of these certificate chains.

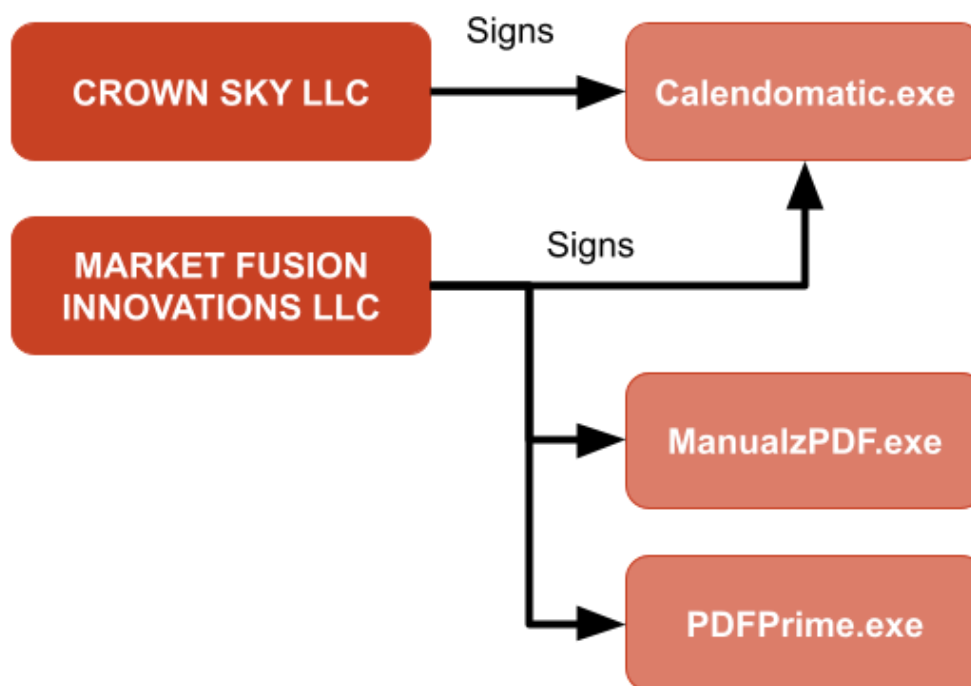


Figure 2. Simplified signature flow of reuse between samples.

The PDFPrime and ManualzPDF campaigns have several distinct variants, all with different code signers. Due to the high degree of code overlap, we clustered 34 samples to the PDFPrime/ManualzPDF codebase. We call these samples PixelCheck due to the C2 domains leveraging the format of `pixel.tool/name[.]com`. They represent some of the earliest evidence of the Calendaromatic operator's activity originating in late 2023.

Pivoting through sample repositories to identify other examples of the PixelCheck variant, seven additional signers were identified in the code of related malware:

- ADVANTAGE WEB MARKETING LLC
- Europae-Solutio Ltd
- SP Development and Solution Limited
- BUZZ BOOST ADVERTISERS LLC
- ADSMARKETO LLC
- LLC MATCH-TWO-USERS
- Monetize forward LLC

Tracking these samples via code signing overlaps involves:

- Identifying the code signers
- Mapping their certificate chains

- Pivoting to similar samples
- Repeating the steps with newly identified signers

This iterative approach uncovered an extensive network of seemingly disparate samples, all linked to a single group through certificate ownership.

While effective, this discovery method relies on lax operational security. True certificate isolation would prevent expanded identification and limit certificate burning.

Reusing code signing across variants also does not appear to be a cost-saving measure, as multiple campaigns often use unique signers rather than reusing a small set of certificates. If cost minimization was the primary goal, we would not see these cases of individual certificate use.

Certificate reuse most commonly appears to be a result of poor testing practice, where attackers use previous certificates on early samples of a new campaign before they can procure a dedicated certificate.

At the current cost of code-signing certificates, burning more than two certificates per campaign carries heavy financial costs. As a result of this research, we attributed a total of 34 unique code-signing certificates related to the Calendaromatic campaign to the CL-CRI-1089 cluster.

Based on the current cost of code-signing certificates, this inefficient approach likely cost the operators over \$10,000 in certificate expenses alone. This further highlights the scale of this operation, where this sum is likely considered a reasonable operational cost.

Tracking via Advertising

Much of the TamperedChef-style malware distribution is via ads, and as such it is subject to ad transparency. Ad transparency is a byproduct of regulation requiring players in the distribution of advertising to provide insights into ad content and owners. Many of the major platforms in the space have their own version of an ad transparency tool or dataset, and investigators can use these to map and track malvertising campaigns.

In most cases, ad transparency platforms enable searching either by the advertiser or the site being advertised. While the definition of an advertiser can be complicated, for the most part, the advertiser is the entity that sold or is selling an ad within the platform.

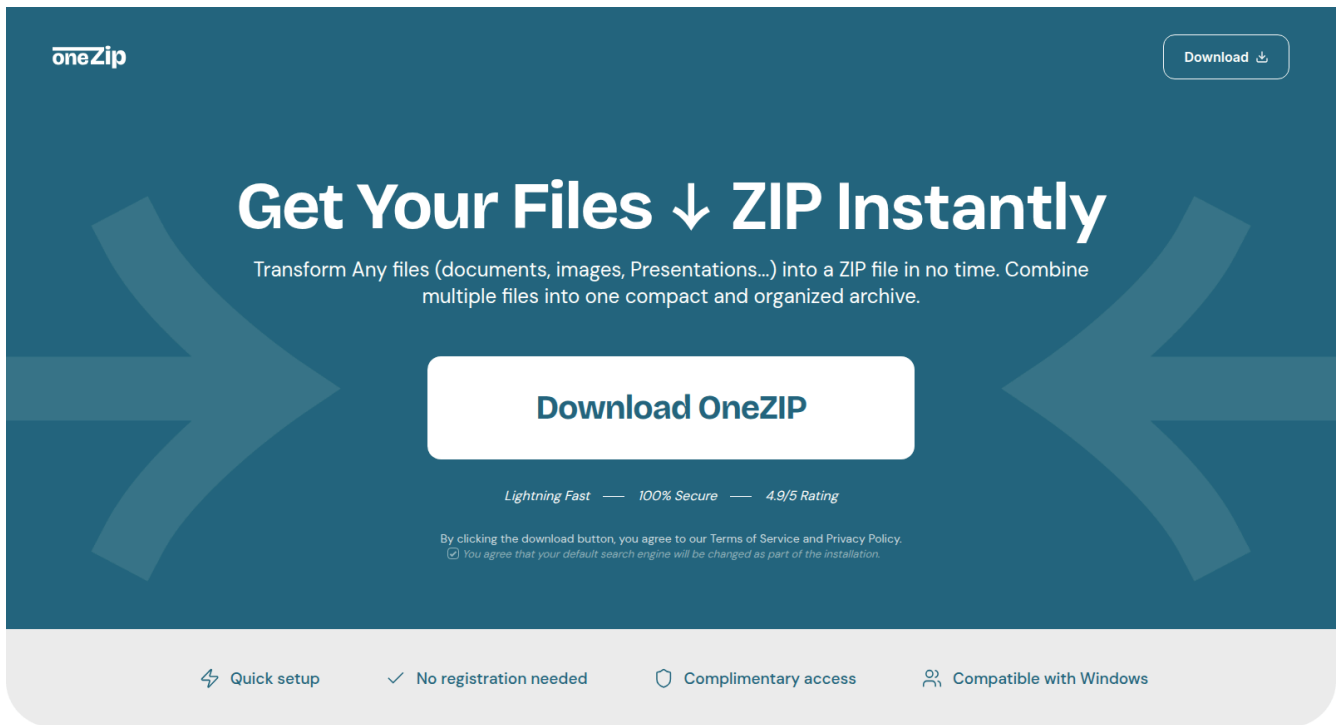
This means there is no guarantee that the malware operator and the ad seller are the same or related entities. However, it implies that the malware operator has interacted with the advertiser in some capacity (e.g., exchanging funds or ad details). Advertisers using these

advertising marketplaces are held to certain standards by the platforms and must abide by the terms of service, which distribution of malware would typically breach.

TamperedChef-style campaigns are different from many other malvertising campaigns, as the malware creators and advertisers are generally vertically integrated. This vertical integration means advertisers also create the malware and, on occasion, sign the code. This direct link between code signers and advertisers implies a strong relationship between malware operators and distributors. This link can provide a starting point to map the wider network distributing this malware.

This is particularly evident with activity in CL-UNK-1090 being run by attackers that are clearly well versed in using ad marketplaces to distribute their malware. For CL-UNK-1090, we identified more than 20,000 unique ads deployed over several years via ad transparency platforms. This volume of ads is unlikely to originate from an individual. The OneZip campaign belonging to the CL-UNK-1090 cluster provides a real-world illustration of how tracking these clusters through advertising commonality and agencies works.

OneZip is a malicious compression tool with binaries signed by TAU CENTAURI LTD observed in the wild in early 2025. OneZip was distributed via the site [onezipapp\[.\]com](http://onezipapp[.]com) (Figure 3 shows the landing page).



Why Choose OneZIP?

The fastest, most secure and powerfull way to manage your files

Figure 3. OneZip landing page.

By leveraging ad transparency platforms, we find that a single advertiser (CANDY TECH LTD) creates and distributes ads for onezipapp[.]com. Based on information from these platforms, CANDY TECH LTD has distributed approximately 4,000 ads that appear related to malicious productivity applications starting in June 2024.

Figure 4 below shows an example of the ads distributed. While not the most innovative, attackers have taken care with these ads to consider language, format, logo and branding. This indicates an actor well-versed in the AdTech space.

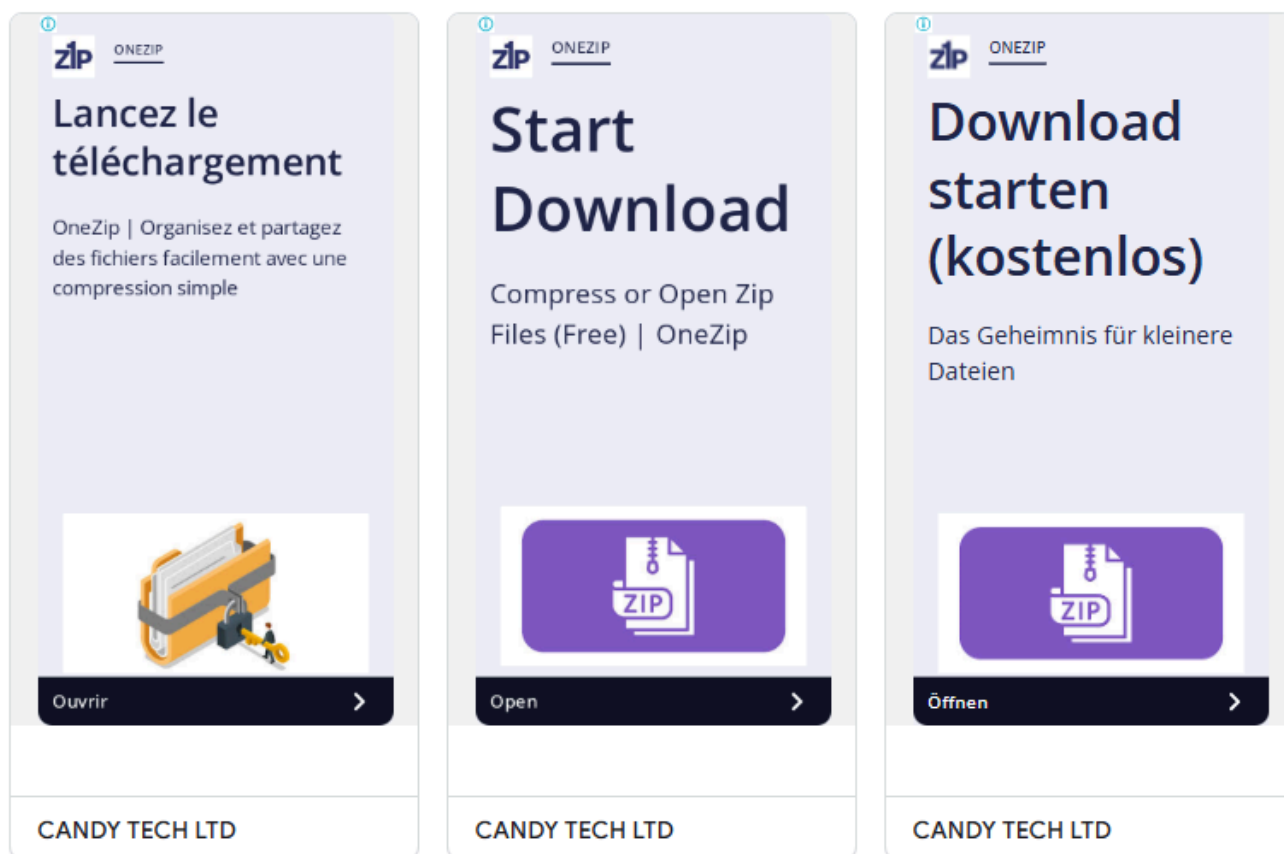


Figure 4. Example OneZip ads run by CANDY TECH LTD.

Between June 2024 and December 2024, ad transparency platforms report that CANDY TECH LTD pushed ads for JustConvertFiles, a similar TamperedChef-style campaign. JustConvertFiles is a malicious file conversion tool similar in operation to all other TamperedChef-style samples.

JustConvertFiles binaries are signed by B.L.A ASPIRE LTD and PASTEL CONCEPTION LTD, and entities with these names are both observed reusing certificates. These entities appear to be responsible for several other campaigns, including:

- PDFPilot
- SwiftNav
- ShinyPDF
- FileEase

Based on advertising transparency data, we have not observed CANDY TECH LTD representing any campaigns other than TamperedChef-style malware.

CANDY TECH LTD is also observed in the malware creation stages, too. Several TamperedChef-style binaries are signed by CANDY TECH LTD or have other links to an entity with this name. These include:

- ZipMakerPro
- GifsMakerPro
- ScreensRecorder
- RapiDoc (contained a copyright stub with CANDY TECH LTD, but not signed)

We then performed the following activities to substantially flesh out CL-UNK-1090 and CL-CRI-1089, and to identify additional campaigns:

- Leveraging known TamperedChef download URLs
- Identifying the advertiser
- Pivoting around the public information on these advertisers

These advertising pivots are not without limitations, and many malvertising actors do not have the expertise to set up the AdTech infrastructure, instead relying on established entities for distribution. This makes any sensible linking through public sources much more difficult, as most of the time, the malware advertising only accounts for a small percentage of the advertisers' overall ad presence. In these cases, other methods are likely to be more effective. However, when possible, investigating the distributor can provide more information.

Tracking via Co-location and Corporate Structures

The TamperedChef-style malware footprint is large and well-organised, with hundreds of campaigns and large sums of money invested. All TamperedChef certificates are validated by an organization, which means certificate authorities require a corporate entity to fulfill [OV/EV](#) requirements to be granted certificates.

Certificate issuers impose these validation requirements to aid in maintaining the reputation of signed code. There is a cost, of both money and time, for adversaries to establish a corporation for the sole purpose of signing code.

Corporate structures tend to leave traces, particularly in countries where data is publicly available. This opens new avenues for discovery.

OSINT sources such as private and government-run corporate search engines can be used to gain rapid insights into corporate entities. Our primary focus areas when tracking code-signing entities were:

- Co-location, especially in residential dwellings
- Companies with a handful of employees and minimal presence, especially when owned by much larger corporations, can indicate possible shell corporations
- Shared ownership structures, particularly when shared ownership is by an individual and not a corporate entity

- History of company renames (especially renames that are potentially aligned with malware campaigns)

With the CL-UNK-1090 cluster, we can use CANDY TECH LTD as an example again. Ad transparency data indicates that CANDY TECH LTD is registered in Israel. Leveraging Israeli company search engines, we found CANDY TECH LTD with a listed phone number, website, address and ownership structure.

Figure 5 below shows the webpage for CANDY TECH LTD.

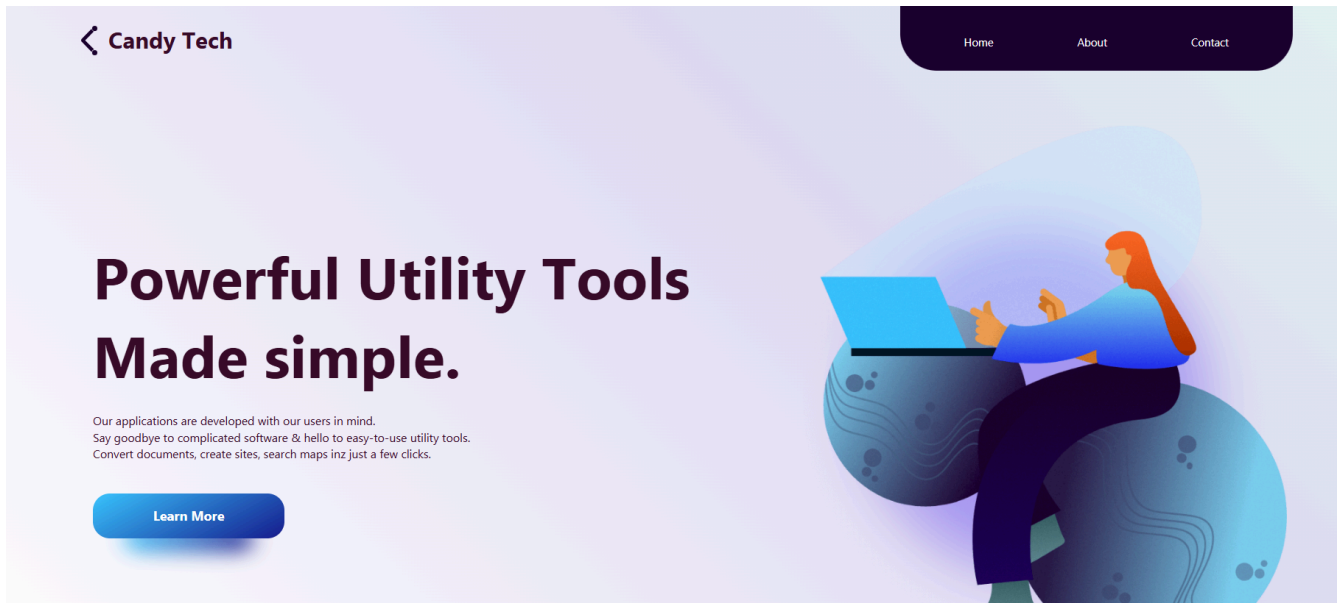


Figure 5. CANDY TECH LTD webpage.

From public records, Zizik with me is the director of CANDY TECH LTD and Fairark Systems Ltd. consists of option holders for the company.

Zizik with me and Fairark Systems Ltd. are listed as having sole ownership stakes in several companies in Israel, such as:

- AMARYLLIS SIGNAL LTD
- TAU CENTAURI LTD
- RED ROOT LTD
- BITTERN SKY LTD
- TOGO NETWORKS LTD

The list of companies that we mined from the Zizik with me and Fairark Systems Ltd. ownership structures — as well as some minor variations and co-location checks — match the names of companies that signed significant volumes of TamperedChef-style code. With high confidence, we believe these ownership structures link all cases to a single group.

Additionally, many of these companies have undergone several name changes in the past three years. Many of the old names match names that were used to sign TamperedChef-style malware.

Fairark Systems Ltd. is the registered name of FireArc, an Israeli advertising company. It states it creates games, connected TV applications, eCommerce solutions and, notably, utility applications. Figure 6 shows this statement on its website.

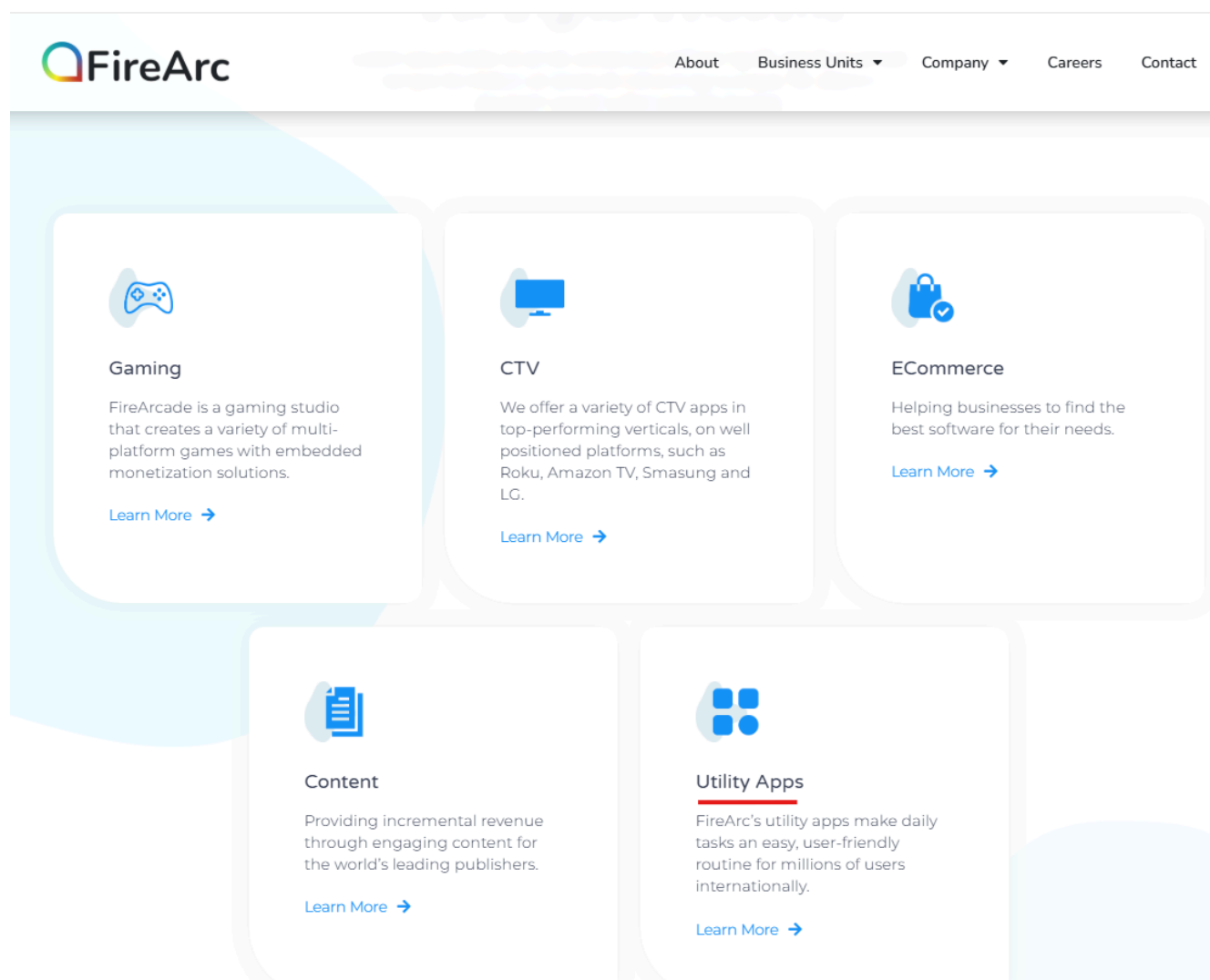


Figure 6. FireArc marketing pages stating they create utility applications.

Additionally, the RapiDoc campaign created by CANDY TECH LTD has a program database (PDB) (D:\\!Work\\Clients\\<user>\\Projects\\RapiDoc\\SrcForTests\\RapiDoc\\x64\\Release\\RapiDoc\\RapiDoc.pdb). This could have been left by mistake in the RapiDoc binaries installed during execution.

PDBs are created during the build process for binaries and contain useful symbol and debug information. Binaries that are productionized tend to remove the PDB, as it can provide reverse engineers a head start when analyzing a binary, which is not desirable for either

legitimate software or malware. PDBs, where applicable, were for the most part removed from other TamperedChef-style samples, indicating that this was likely an error.

The SHA256 hashes for the binaries containing the PDB are:

- 248de1470771904462c91f146074e49b3d7416844ec143ade53f4ac0487fdb44
- 2231bfa7c7bd4a8ff12568074f83de8e4ec95c226230cccc6616a1a4416de268

The Wide-Reaching Web of TamperedChef

Leveraging several linking methods, we broadly identified significant portions of these activity clusters' operations, mapping several networks of TamperedChef-style malware. While this may not represent their entire infrastructure, it highlights the pervasive nature of this threat. We supply all identified samples, domains, signers and any other relevant details in the Indicators of Compromise section.

CL-CRI-1089

Using Calendaromatic as a starting point, we mapped out the CL-CRI-1089 cluster to include 34 unique code-signing entities. Our primary method of identification was code and certificate reuse. We observed some evidence of shared corporate addresses with code signers. However, generally, each entity was separately created and operated.

The CL-CRI-1089 cluster included malvertisements generated through self-created and likely dedicated companies. This cluster did not appear to cross-contaminate advertising entities with code-signing entities. This cluster primarily leveraged companies based out of Ukraine, Malaysia, Singapore, the U.S. and the UK to perform operations. In cases where the owner's place of birth was recorded by the UK government, all owners were of Ukrainian origin.

We identified over 3,300 samples related to CL-CRI-1089 across Palo Alto Networks and public sample databases, with the vast majority related to productivity software.

CL-UNK-1090

We mapped out CL-UNK-1090 primarily through a combination of real-world incidents, OSINT on the FireArc corporate structures and advertising network links. Certificate and code reuse were present but formed less of a basis for discovery.

We found CL-UNK-1090 used 39 Israeli corporations for certificate generation. This cluster included changed organization names to mine these structures for multiple certificates, so the real number of organizations is likely less than 39. We identified approximately 750 samples related to CL-UNK-1090, all with productivity application themes.

Malvertising as a Service: How Did the Threat Scale?

The scale of TamperedChef-style malware is immense. We found evidence of the two tracked clusters (CL-CRI-1089 and CL-UNK-1090) across more than 50% of Managed Threat Hunting customers. If this number is an accurate representation of the wider community, it shows an operation on a scale rarely observed.

The distribution and scale of these campaigns come with high monetary and labor costs. TamperedChef-style actors are likely to have bought much of their success. They have positioned themselves less as malware experts than as advertising and logistics specialists.

Buying Legitimacy: Purchasing Code-Signing Certificates

Code signing as a practice provides authenticity and integrity validation to binaries, but it can be misused by malicious actors. Purchasing code-signing certificates offers a marginal increase in binary trustworthiness. However, they come with strict identity validation and cost, which can deter many malware developers.

These requirements did not impede any of the TamperedChef actors, and one of their key strengths comes from a deep understanding of the business side of advertising. The development of several shell companies appeared minimally impactful and provided a reusable pool of code-signing certificates. In the case of CL-UNK-1090, it appeared that renaming existing companies was enough to be granted new, valid certificates, further lowering the barrier for entry.

In recent months, we've identified a trend of these clusters moving away from code signing. This shift could be occurring because these binaries are becoming better understood and researched. The damage done by identifying an entire campaign through tracking code signers may now outweigh the benefits gained through signing binaries.

Buying Speed: The Influence of Distributed Development and AI

The rate and scale at which the TamperedChef-style actors deploy new campaigns is incredibly fast. Attackers run tens of campaigns simultaneously, with new ones being developed constantly.

The CL-CRI-1089 cluster, in particular, demonstrates a high degree of variation. Each campaign features an entirely new set of TTPs, delivery methods, languages, functionality and C2 structures. This suggests a new codebase for each campaign, and potentially even different developers.

The code quality also shows a lack of mature development practices and teams likely inexperienced with malware development. This does somewhat work in favor of TamperedChef binaries, as upon first glance, the C2 methods are not always obvious.

In the case of CL-CRI-1089, the codebases are highly variant. However, they share common certificates, demonstrating limited code reuse between campaigns. This may indicate they were created by several development teams or that generative AI was at least partially responsible for the set of campaigns.

Distribution infrastructure setup appears to be largely driven using generative AI. This is particularly evident with the distribution websites where the content of pages for different campaigns appears visually similar. However, they have distinct Document Object Model (DOM) structures. This is indicative of a non-deterministic development practice, which is characteristic of content generated by large language models (LLMs).

Buying Visibility: Hijacking the Advertising Pipeline and Search Engine Optimization (SEO)

TamperedChef-style samples for all clusters are distributed primarily through malvertisements, sponsored results and [search engine marketing](#) techniques. Our telemetry for real-world infection chains commonly shows victims browsing terms like “free calendar prints” or “document formatting” before being served the malvertisements.

TamperedChef-style malware establishes a distribution-first approach. Getting installed by the masses is far more important to the operators than managing persistent and reliable C2.

Technical Analysis of TamperedChef Malware Samples

Operational Commonalities Across All Samples

While none of the identified TamperedChef malware samples are technically complex, they vary significantly between campaigns. All samples tend to share a common set of TTPs and second-stage payloads, which only serves to further highlight the motivations and risks these TamperedChef-style malware samples pose.

These universal TTPs include:

- Leveraging code signing for the first-stage payloads
- Implementing a robust persistence mechanism, almost always through scheduled tasks or registry Run keys

- Initial information gathering and exfiltration typically occurring on install
 - This usually involves simple data collection, like system version, hostname and active browsers.
 - However, we have seen more targeted information gathered, including patch levels, user details, domain information, geolocation and screen size.
- Employing a delayed activation technique to evade detection
 - Initially, the samples mimic legitimate applications, remaining dormant for days or even weeks.
 - Upon activation, they trigger the next stage, which typically involves downloading and executing an additional payload delivered via an upstream API.
- Obfuscating the malicious components
 - This is the clearest evidence to suggest that these binaries are not just simple adware.
 - Most of the campaigns we observed used some form of obfuscation or defense evasion techniques for their loader or stealer components.
 - While obfuscation is used for intellectual property (IP) protection, in this case, the routines were primarily for de-obfuscating incoming payloads within the loader components.
 - Since no other parts of the binaries were obfuscated, IP protection was likely not the main reason for these methods.

Delivering Second Stage Malware

TamperedChef-style malware, when activated, can deliver arbitrary payloads, but in practice sticks to two primary categories: adware and browser hijackers or RATs and stealer malware. Which payload it delivers depends on the campaign specifics. TamperedChef rarely deploys both simultaneously.

Adware and Browser Hijacking

The primary objective of the majority of the TamperedChef-style binaries is to distribute ads or gain some form of control over the user's browser. This has been achieved via either:

- Installing a new adversary-controlled default search engine in the user's primary browser
- Installing an entirely new adversary-controlled browser (e.g., OneBrowser)

Both these methods enable adversaries to control the content searched, ads displayed to victims and, in the case of the browser installation, full control over user cookies and credentials.

Stealers and RATs

While adware can be disruptive and undesirable, it does not generally pose a major organizational risk. TamperedChef-style binaries, on the other hand, display a level of stealth, defense evasion and persistence that is unusual and excessive for adware.

This likely further indicates that the true threat of the TamperedChef-style malware goes beyond adware and into more insidious use cases. This is backed by real-world cases where attackers have consistently deployed active C2 and stealer-style malware as second stages targeting victims' browser credentials or for information gathering.

These second-stage stealers range in capability, targets and formats but are almost always deployed after a dormancy period of weeks. Evidence of more exotic payloads has been observed too, but far less frequently and not en masse. An example of this was the AppSuite campaign that saw the sporadic installation of proxy-style malware.

Distilling the Motivations

Our analysis shows that CL-CRI-1089 activity focuses on criminal-style activity targeting credentials, deploying adware and in some cases proxy-style payloads. Based on sample and corporate analysis, the operators of CL-CRI-1089 are globally distributed but centrally operated.

In contrast, the motivations behind CL-UNK-1090 activity are far less clear. This activity appears to be solely managed by a much smaller group of entities related, at least in part, to a seemingly successful advertising agency.

These samples are all designed to look like adware. However, the samples do not operate like adware, housing RATs with .NET loader-style capabilities that legitimate adware or productivity software do not require.

In real world cases, we have not observed the same volume of malicious second stage deployments from samples tracked as CL-UNK-1090 as we have with the CL-CRI-1089 samples. However, second stages deployed by CL-UNK-1090 are more stealthy, existing primarily in memory and include RAT deployments, browser hijackers and adware.

Detection, Prevention and Response to Future Threats

Preventive Recommendations

Some key preventive steps to combat this threat are:

- **Education:** Ensure users are aware of this style of threat and know that even legitimate looking software can carry risks
- **Endpoint/extended detection and response (EDR/XDR):** Ensure updated EDRs/XDRs are in place on all hosts within an environment
- **Enterprise browsers:** Enterprise browsers can help protect against this threat and ensure that in the event of compromise, saved credentials remain secure
- **Device hardening:** Consider hardening user endpoints to prevent the installation of software from untrusted sources

Detection and Response

Due to the prevalence of these threats, continuous active monitoring and hunting can have a very high return on investments however due to the varied nature of these threats hunting queries vary in effectiveness.

If these threats are identified, our general remediation advice is to:

- Remove and/or quarantine all files associated with the malicious software
These are generally located in the installation folder
- Ensure that persistence mechanisms such as the created scheduled tasks are removed to prevent reinfection
Consider running a full malware scan of the host as it may identify any second-stage components
- Consider revoking active tokens for the impacted users and resetting their credentials
It is likely that any browser-based credentials are potentially compromised
- Review access logs to ensure that the impacted users' credentials are not actively being misused

Conclusion

TamperedChef-style campaigns are likely to continue to misuse advertising pipelines to deliver malware, developing and adapting new lures and evasion methods. The prevalence of the CL-CRI-1089, CL-UNK-1090 and CL-UNK-1100 clusters will likely serve as a blueprint for future malvertising campaigns.

New trends, such as moving away from using code signing, will require new tracking methods to be developed to remain ahead of these actors' operations.

Palo Alto Networks Protection and Mitigation

Palo Alto Networks customers are better protected from the threats discussed above through the following products:

[Cortex XDR](#) and [XSIAM](#) help to prevent the threats described in this blog, by employing the Malware Prevention Engine. This approach combines several layers of protection, including Advanced WildFire, Behavioral Threat Protection and the Local Analysis module, designed to prevent both known and unknown malware from causing harm to endpoints.

Prisma Browser helps to prevent access to known malicious campaigns using [Advanced URL Filtering](#), [Advanced Web Protection](#) (Live Page Scanning) which runs AI models within the browser to detect and block attack patterns, file download scanning and protection on the default search engine.

If you think you may have been compromised or have an urgent matter, get in touch with the [Unit 42 Incident Response team](#) or call:

- North America: Toll Free: +1 (866) 486-4842 (866.4.UNIT42)
- UK: +44.20.3743.3660
- Europe and Middle East: +31.20.299.3130
- Asia: +65.6983.8730
- Japan: +81.50.1790.0200
- Australia: +61.2.4062.7950
- India: 000 800 050 45107

Palo Alto Networks has shared these findings with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the [Cyber Threat Alliance](#).

Indicators of Compromise

Table 1 lists the signers' organization noted in code-signing certificates used in the TamperedChef-Style malware samples we found in our research.

Signer	Related Cluster
CANDY TECH LTD	CL-UNK-1090
G.R.CIGAR. LTD	CL-UNK-1090

TAU CENTAURI LTD	CL-UNK-1090
AMARYLLIS SIGNAL LTD	CL-UNK-1090
METROPOLITAN DESIGN LLC	CL-UNK-1090
BLACK INDIGO LTD	CL-UNK-1090
Red Root LTD	CL-UNK-1090
A1A Marketing Ltd.	CL-UNK-1090
GOLD HARMONY LTD	CL-UNK-1090
BEGONIA LIFE LTD	CL-UNK-1090
SAMBUSAK LLC	CL-UNK-1090
ACTIVE INTELLECT AI LLC	CL-UNK-1090
VAST LAKE LTD	CL-UNK-1090
LONG SOUND LTD	CL-UNK-1090
B.L.A ASPIRE LTD	CL-UNK-1090
VANILLA FORCE LTD	CL-UNK-1090
SELA LINES LTD	CL-UNK-1090
WIND TRUST LTD	CL-UNK-1090
BLUE TAKIN LTD	CL-UNK-1090
ORCHID MARS LTD	CL-UNK-1090
ENIGMATIC SAOLA LTD	CL-UNK-1090
TROPICAL RIFF LTD	CL-UNK-1090
BITTERN SKY LTD	CL-UNK-1090
astro bright ltd	CL-UNK-1090
my tech media ltd	CL-UNK-1090

LIGHTNER TOK LTD	CL-UNK-1090
TOGO NETWORKS LTD	CL-UNK-1090
CHRONO ORION LTD	CL-UNK-1090
LOGOS AQUA LTD	CL-UNK-1090
Impresan Solutions OÜ	CL-UNK-1090
Shopcut LLC	CL-UNK-1090
Judy Wanjiru	CL-UNK-1090
Keen Internet Technologies Ltd	CL-UNK-1090
ROYAL STEP LTD	CL-UNK-1090
Smart Contract LLC	CL-UNK-1090
DORNOVI LTD	CL-UNK-1090
Green Topaz Ltd	CL-UNK-1090
LOGOS AQUA LTD	CL-UNK-1090
SPARROW TIDE LTD	CL-UNK-1090
mania tech ltd	CL-UNK-1090
PASTEL CONCEPTION LTD	CL-UNK-1090
Mainstay Crypto LLC	OneBrowser Signers
Crowd Sync LLC	OneBrowser Signers
WORK PRODUCT, INC.	OneBrowser Signers
Chickadee Digital	OneBrowser Signers
Riya Software	OneBrowser Signers
Eman Group, LLC	OneBrowser Signers
MATCH-TWO-USERS LLC	CL-CRI-1089

TWEAKSCODE LLC	CL-CRI-1089
AFFILIDADOS	CL-CRI-1089
MARKET FUSION INNOVATIONS LLC	CL-CRI-1089
BUZZ BOOST ADVERTISERS LLC	CL-CRI-1089
ADSMARKETO LLC	CL-CRI-1089
CROWN SKY LLC	CL-CRI-1089
Summit Nexus Holdings LLC	CL-CRI-1089
Europae-Solutio Ltd	CL-CRI-1089
SP Development and Solution Limited	CL-CRI-1089
Echo Infini SDN BHD	CL-CRI-1089
COMMERCE GROUP TECHNOLOGY LTD	CL-CRI-1089
ALGORYTHM TECH LTD	CL-CRI-1089
Byte Media Sdn Bhd	CL-CRI-1089
GLINT SOFTWARE SDN. BHD	CL-CRI-1089
Global Tech Allies Ltd	CL-CRI-1089
SOFT SOLUTIONS HUB	CL-CRI-1089
Monetize forward LLC	CL-CRI-1089
ADVANTAGE WEB MARKETING LLC	CL-CRI-1089
Incredimarket	CL-CRI-1089
ILLUSION MEDIA SOLUTIONS	CL-CRI-1089
Virtual Media App Ltd	CL-CRI-1089
DEV SPOTS LLC	CL-CRI-1089
Digit Consult	CL-CRI-1089

Outsource Genius LLC	CL-CRI-1089
OneStart Technologies LLC	CL-CRI-1089
Apollo Technologies Inc	CL-CRI-1089
Caerus Media LLC	CL-CRI-1089
Digital Promotions Sdn. Bhd.	CL-CRI-1089
Eclipse Media Inc.	CL-CRI-1089
Astral Media Inc	CL-CRI-1089
Incredible Media Inc	CL-CRI-1089
STYLE SOLUTION LIMITED	CL-CRI-1089

Table 1. Signers of code-signing certificates from the TamperedChef-style malware samples.

Additional Resources

- [Cooking up trouble: How TamperedChef uses signed apps to deliver stealthy payloads](#) – Acronis
- [When the Dash Hits the Fan: Artificial Intelligence Exposes the Homoglyph Hustle](#) – GuidePoint Security
- [EvilAI Operators Use AI-Generated Code and Fake Apps for Far-Reaching Attacks](#) – TrendMicro
- [Malicious Appsuite PDF Editor Spreads Tamperedchef Malware](#) – Truesec
- [The history of AppSuite: the certs of the BaoLoader developer](#) – Expel