TRINITY CYBER

The Silent Watchers:

Revisiting EvilAI and TamperedChef Malware Campaigns

Author: Tyler Nist

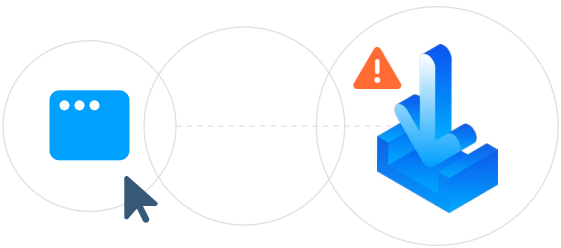
Executive Summary

Trinity Cyber has been tracking two broadly distributed malware campaigns, EvilAI and TamperedChef, since their discovery in 2025. Although TamperedChef slightly pre-dates the EvilAI umbrella, both refer to trojanized productivity applications that target victims via malvertising. Rather than exploiting software vulnerabilities, these campaigns rely on convincing users to install applications which silently masquerade as productivity tools, including PDF converters, recipe generators, calendars, document readers, browsers, and other utilities.

Operators behind these campaigns and clusters of activity are well-resourced. They combine malvertising, SEO poisoning, and professional download sites to drive victims toward digitally signed applications that perform their advertised functions while covertly installing backdoors to steal information and send system telemetry back to operators. Both families utilize advertising technology (AdTech) front companies who are likely involved in the creation, distribution, and sponsorship the code signing certificates used to digitally sign these applications—either knowingly or unknowingly.

Throughout 2026, multiple security vendors have documented the evolution of both campaigns, highlighting rapid infrastructure changes, resistance to digital signature revocation, and emerging clusters of similar activity. These campaigns illustrate how trusted software distribution mechanisms, legitimate code-signing certificates, and clever social engineering can combine to bypass traditional defensive controls, and trick users into becoming part of something much more nefarious.

It's become increasingly clear that EvilAI and TamperedChef are staging access to victim computers—racking up user installs and flying under the radar by being just enough of a productivity application that victims won't try to uninstall them.



Background

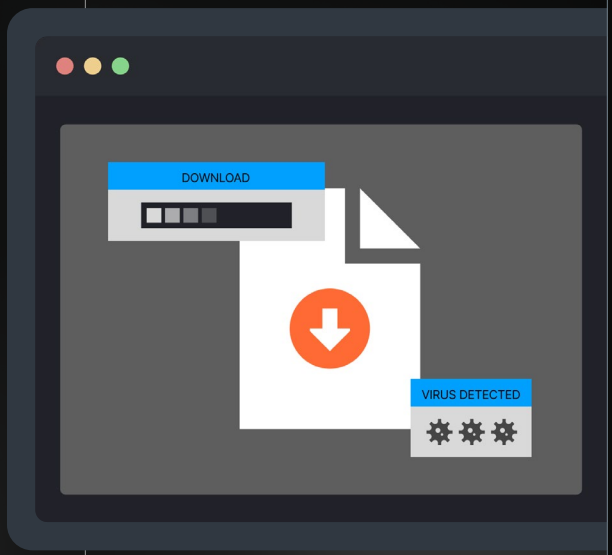
The origins of TamperedChef began in May 2025 with post from Blumira[1] for a suspicious “Recipe App”, were carried on through Luke Acha’s research in June 2025[2], and subsequent analyses by Truesec[3], Expel[4], and GDATA[5] in August 2025.

TrendMicro[6] coined the name “EvilAI” for activity that encompassed many of the same behaviors as TamperedChef before it. When comparing the two campaigns, it is useful to think of TamperedChef as a cluster of activity under the EvilAI umbrella. Both campaigns deliver productivity applications (or browsers, document viewers, recipe apps) that claim to do one thing, while quietly establishing persistence, sending system information to C2 servers, and opening victim computers up to further infection and malicious access in the future. In many ways EvilAI and TamperedChef are the same, yet technical nuances separate them into campaigns tracked by many researchers, including Palo Alto[7] in May 2026.

Peeling back the layers reveals undeniable similarities across both campaigns:

- Digitally signed executables to establish trust on Windows
- Post-install C2 for tracking victim installations
- Anti-reverse engineering techniques like VM/sandbox awareness
- Search and uninstall capability for legitimate browsers, document handlers, and productivity apps
- Dynamic packaging and compilation such as MSI files, Rust, Inno Setup, .NET, and Electron apps
- Promoted by AdTech networks and companies that rotate frequently

Perhaps the most important aspect of these campaigns, and one that Trinity Cyber tracks closely, is that operators are silently staging access to victim computers over long periods of time. Despite the “legitimate” functionality included, the job of both malware families is to facilitate access to victim machines, maintain persistence, and download additional payloads whenever actors choose to.



Here's what an EvilAI/TamperedChef campaign looks like from a victim perspective:

Delivery via Malicious Ads

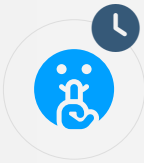
Actors register lookalike domains that mimic legitimate tools or documentation, and push them to the top of search results using Google Ads to achieve SEO poisoning. A user searching for a productivity app clicks an advertisement or sponsored result on an otherwise benign third-party site. They land on a convincing page with a download lure, which pulls down a software installer that's laced with malicious functionality.

Signed Installers

Installers are signed with valid code signing certificates—often issued to AdTech companies in countries such as Malaysia, Panama, Cyprus, or Isreal. Researchers have documented the operators cycling through at least 26 certificates over the past few years, generating new certificates after revocation. A valid signature bypasses Windows SmartScreen and earns trust on most endpoints, even with EDR installed.

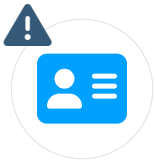
Trojanized Applications

Many EvilAI/TamperedChef packages are a NodeJS application: the main executable is a Chromium shell that runs bundled JavaScript. Malicious logic lives in a heavily obfuscated JavaScript file, which is generated with Artificial Intelligence (AI) models. This produces clean looking, dynamic code that circumvents signature-based detection methods. A native helper module handles registry edits, scheduled task creation, sandbox checks, and installation with user permissions.



Silently Waiting

Trojan applications sit idle for days or weeks before malicious activity starts. This is long enough to match the runtime of a typical Google ads buy, notably by design. In 2025, actors behind one of these campaigns pushed a **–fullupdate** command to victims over 56 days later, triggering infostealer capabilities. By delaying their operations, the actors gather a broad collection of victims to target with malicious payloads.



Persistence & Info-Stealing

Some infections enumerate installed security solutions and other applications via registry queries, terminate running browser processes, and use the Windows Data Protection API to steal credentials, cookies, and autofill data. They persist through autorun entries and scheduled tasks, and maintain an AES-encrypted command and control channel offers on-demand access to victims. In some builds, operators even go so far as to prompt victims to consent to having their machine used as a residential proxy in exchange for built-in functionlity.

With few exceptions, most EvilAI/TamperedChef campaigns in 2025 and 2026 follow the same campaign footprint noted above. Evolution in these campaigns has been mostly in packaging and digital signatures. Packaging started with NeutralinoJS[8] in 2025 and evolved into .NET, Rust, Inno Setup, and NSIS compiled applications in 2026. Operators behind the clusters of activity appear to rotate code signing certificates (and the subject names of certificates) every 2–4 weeks, along with the names and functions of the applications. This speaks to the dynamic nature of these campaigns: actors behind them know they're being tracked by the security community.

As it turns out, EvilAI and TamperedChef may have deeper roots in trojanized browsers and PDF editors. Researchers at Expel[9] documented that the operators behind the AppSuite/OneStart ecosystem rotated through multiple legitimate code-signing identities over time. OneStart installers were initially signed using certificates issued to Apollo Technologies Inc. After those certificates were revoked, the operators adopted certificates issued to Caerus Media LLC before later transitioning to OneStart Technologies LLC. This certificate churn appears to have been an operational tactic to maintain trust and evade reputation-based detection.

The purpose of this history lesson isn't to label OneStart's AI browser as malware. OneStart has denied the claim that their platforms are malware multiple times[10][11]. However, researchers have observed that OneStart-branded installers were associated with digital certificates that also signed AppSuite and other malicious applications within the EvilAI and TamperedChef universe.

Technical Details

Since the beginning of 2026, Trinity Cyber has prevented several hundred EvilAI and TamperedChef campaigns targeting customers. While the likes of **AppSuite** and **JustAskJacky**—precursors to modern EvilAI campaigns—have not surfaced in our telemetry, the evolution of clustered activity associated with both campaigns has. New obfuscated installers, clean websites serving malicious ads, and digital signatures signed by shell companies show the threat is moving full steam ahead, developing new methods to target unsuspecting victims via malvertising.

In a recent campaign of TamperedChef-style activity, the malicious website **tiprecipe[.]com** was used to deliver an AI-enhanced recipe helper application which claims to help users develop recipes. This activity closely aligns with the Google Threat Intelligence tracked UNC6468, an espionage campaign delivering DAYSHROUD malware via malicious calendar applications as far back as 2025[12]. This campaign also delivers food-centric executables, leveraging valid digital signatures and memory injection to obfuscate its malicious components.

Delivery Mechanism

Full Content Inspection (FCI)™ prevented the first step of the campaign—an outbound HTTP GET Request to **/static/js/main.9417d956.js**, presumably after clicking a Google Ad on another website.

Here's the first stage HTTP GET request for the campaign:

```
GET /static/js/main.9417d956.js HTTP/1.1
Host: tiprecipe.com
Connection: keep-alive
sec-ch-ua-platform: "Windows"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/148.0.0.0 Safari/537.36
sec-ch-ua: "Chromium";v="148", "Google Chrome";v="148", "Not/A)Brand";v="99"
sec-ch-ua-mobile: ?0
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://tiprecipe.com/recipe/download?campaign_id=23823772936&adgroup_id=203000169064&placement_id=solvethecube.com&creative_id=80
7859311968&spa=EAIaIQobChMIpdqL6be0lAMVgPNMAh2PIhmbEAEYASAAEgKJffD_BwE&gad_source=5&gad_campaignid=23823772936&gclid=EAIaIQobChMIpdqL6be0lA
MVgPNMAh2PIhmbEAEYASAAEgKJffD_BwE
Accept-Encoding: gzip, deflate, br, zstd
Accept-Language: en-US,en;q=0.9
```

Figure 1. Initial GET Request to **tiprecipe[.]com**

A wealth of information about this campaign can be found by examining the Google Analytics 4 (GA4) parameters in the request shown above:

- ✓ **campaign_id** – unique ID behind the ad campaign
- ✓ **adgroup_id** – unique ID of the ad within the campaign
- ✓ **placement_id** – origin site where the ad was located
- ✓ **gad_source** – source of the ad was Google Shopping
- ✓ **gad_campaignid** – aggregate ID behind the ad campaign
- ✓ **gclid** – unique click identifier behind the ad

While these fields are mostly opaque GA4 fields, they do offer some insight into the distribution of TamperedChef and EvilAI lure ads.

While tracking these fields for this research, our team observed similar advertisements on the following legitimate sites:

- ✓ **scribd[.]com**
- ✓ **soundboard[.]com**
- ✓ **manualslib[.]com**
- ✓ **themediterraneandish[.]com**
- ✓ **stripes[.]com**
- ✓ **zillow[.]com**
- ✓ **logtool[.]com**
- ✓ **nslookup[.]com**
- ✓ **calendarlabs[.]com**
- ✓ **realtor[.]com**
- ✓ **forbes[.]com**
- ✓ **allrecipes[.]com**

Each of these websites are benign (or in the very least, not inherently malicious)—yet all of them have served malicious advertisements using Google Ads for either TamperedChef or EvilAI. This shows how broad these campaigns are, appearing on well-known sites like Zillow, Forbes, and AllRecipes. In other words, users don't have to go far to be exposed to these malvertising campaigns.

These malicious ads are distributed in a way that indicates the developers of the malware and the ads themselves are vertically integrated.

In many cases the advertisers of the software are also responsible for developing, distributing, and signing the malware—meaning the entire operation exhibits some level of sophistication.This adds complexity to identifying the threat, as the operators are in control of every level of distribution and execution, down to code signing itself.

Upon arrival at **tiprecipe[.]com**, visitors see a modern webpage that lures victims into downloading TipRecipe (TamperedChef). To practitioners, the site raises red flags with its simplistic language and “Get Free App” buttons. But to the average person, it’s convincing enough to appear as just another program that can help them do something useful. These one-click buttons use various Content Delivery Networks (CDNs) to distribute TamperedChef and EvilAI, often relying on various JavaScript code to craft popups and make programs appear legitimate.

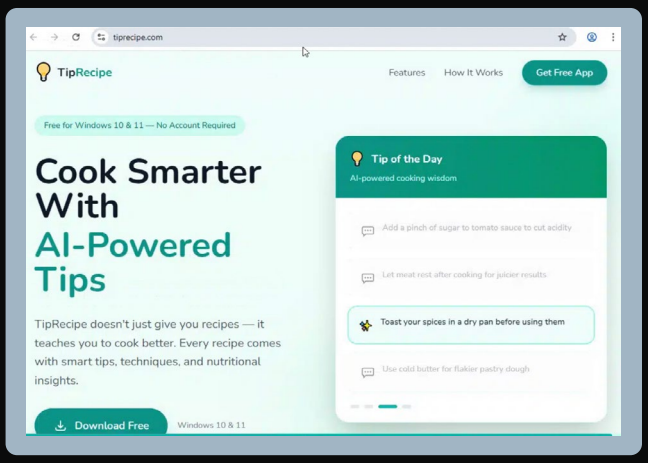


Figure 2. TipRecipe landing page

A closer look within the traffic of a website visit reveals the **main.9417d956.js** file observed in initial GET request. This file is built on React and likely AI-generated (based on overly verbose comments), serving as a conduit for filtering victims and retrieving the next stage. If the visitor passes these filtering checks, a request to an Amazon CloudFront CDN hosted domain is made when clicking the “Download Free” button. Within **main.9417d956.js**, the un-obfuscated CloudFront URL is present in the **URLSearchParams(window.location.search)** code. Additionally, this JavaScript contains visitor tracking logic for operators to track website visits and successful downloads.

```
 const[e, t] = (0, a.useState)("https://d1otg7p04d1sbe.cloudfront.net/TipRecipe.exe"),
[n, r] = (0, a.useState)(!1), [l, i] = (0, a.useState)(1), [o] = (0, a.useState)(Ae), s = (0, a.useRef)(!1), u = (0, a.useRef)(!1), c = Ue[o];
 (0, a.useEffect)(() = > {
     const e = new URLSearchParams(window.location.search);
```

Figure 3. TamperedChef download URL

```
const t = setInterval(() = > {
    s(e = > (e + 1)%4)
}, 3500), n = new URLSearchParams(window.location.search);
if (!u.current)  {
    const e = {};
    n.forEach((t, n) = > {
        e[n] = t
    }

    ), e.type = "landing", e.lp_url = window.location.pathname, e.flow = "node", e.doc_ref = document.referrer;
    const t = JSON.stringify(e), r = btoa(t);
    navigator.sendBeacon("https://tiprecipe.com/report", r), u.current = !0
}

return() = > {
    window.removeEventListener("scroll", e), clearInterval(t)
}
```

Figure 4. Visitor tracking via JavaScript to the **/report** URI

Dynamically Named Campaigns

TamperedChef operators use randomly generated pseudonyms that correlate between domains and filenames of delivered installers. **TipRecipe, MealFormula, KitchenCanvas, GiveMeRecipe,** and others can be reliably found on VirusTotal. Here's two examples from the campaign:

Installer Name	SHA256 Hash
`KitchenCanvas-Setup-2.8_780442.exe`	`3c1dbc3f56e91cc79f0014850e773a7f12bbfef06680f08f883b2bf12873eccc`
`TipRecipe_26467.exe`	`5d687b0466bbaf61d703046a8e8768f8b8c60686f5cc9c1ec6bcf0364d5c2ef9`

The first two files—**KitchenCanvas-Setup-2.8_780442.exe** and **TipRecipe_26467.exe –** are structurally similar, both 6.73MB and packaged with NSIS installer. WinRAR.exe is just that—the official (and benign) WinRAR installer. Malware from this campaign is delivered from domains that match the filename of the executable that a victim downloads, along with six random digits before the file extension. This supports the theory that these applications are being generated programmatically, at a rapid rate.

Here are several known filenames and their delivery websites:

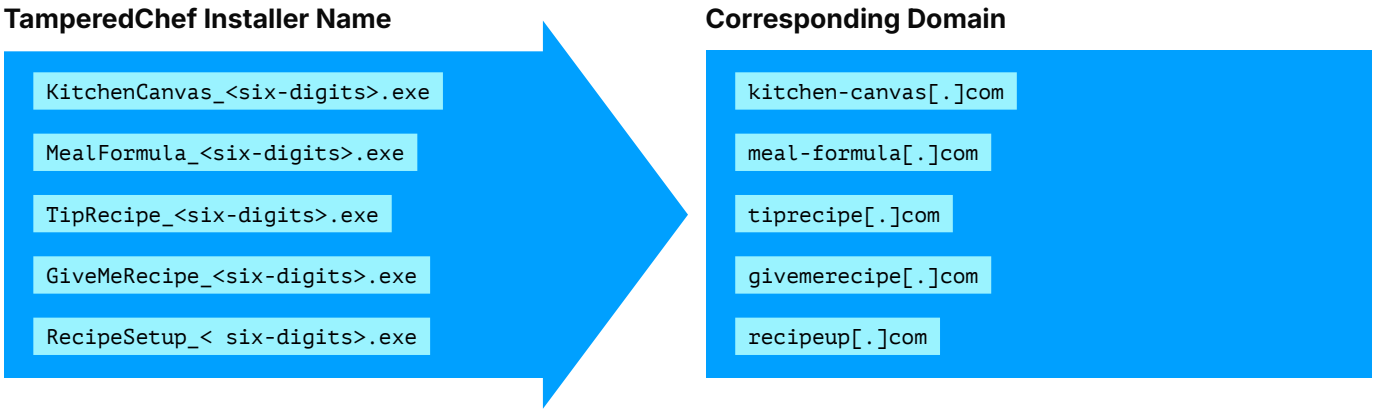


Figure 5. TamperedChef filename to domain crosswalk

The delivery websites for this campaign are structurally similar. They mimic each other with minor wording and theme changes, but the same visual look and feel. The use of identical websites implies the use of website templates, which operators use to deliver new TamperedChef and EvilAI campaigns quickly.

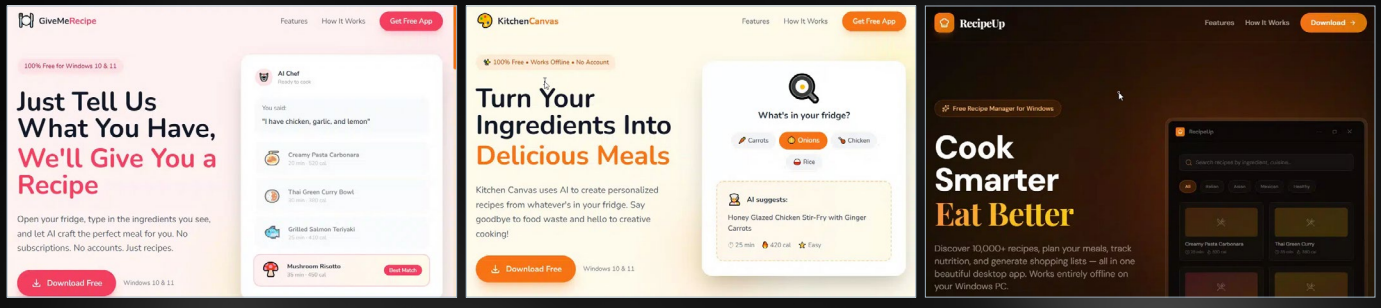


Figure 6. Similar landing pages used in TamperedChef campaigns

Code Signing Certificates

A code signing certificate is a digital certificate which is typically issued by a trusted Certificate Authority (CA) to cryptographically verify a software publisher's identity and provide anti-tampering proof. Despite the protections offered by Extended Validation (EV) and Organization Validation (OV) certificates, malicious actors still manage to sign malware with them. Many TamperedChef installers are signed with EV certificates trusted by GlobalSign and other trusted identity providers:

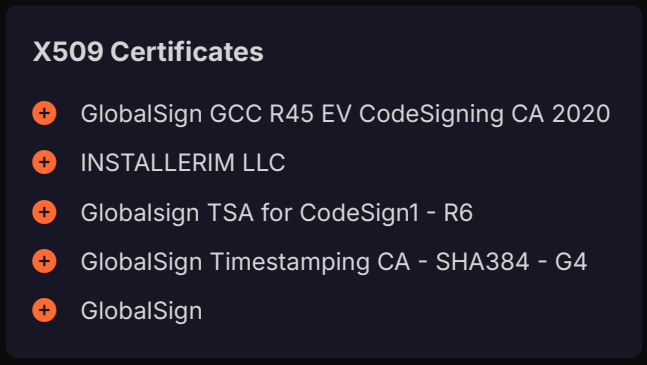


Figure 7. EV Certificate chain on TamperedChef installer

In a similar campaign, installers drop two similar files when executed: **FoodFormula_885414.exe** and **Food Formula.exe**. Both files list their File Version as 2.6.8.3. Digging into both installers, both are signed by certificates from the company **INSTALLERIM LLC** with a GlobalSign EV certificate chain.

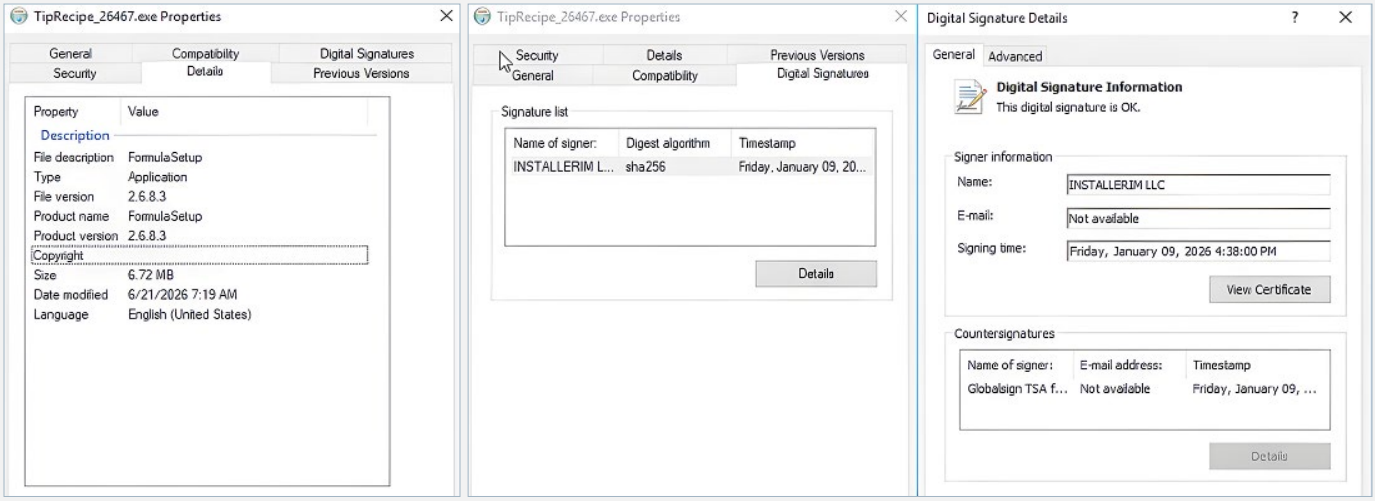


Figure 8. Certificate subject **INSTALLERIM LLC**

Multiple vendors[13] have shown how TamperedChef campaigns operate by reusing code signing certificates. Clusters and overlaps between filenames and these code signing certificates show clear associations and minor changes to installers at rapid pace. The use and reuse of EV certificates, shell companies for certificate subjects, and dynamic changes to installers suggest a wide and elaborate ecosystem, which most likely relies on AI generated code and workflows to avoid detection and establish trust on victim endpoints.

Included in the IOC section of this report are hashes for 24 binaries signed with **INSTALLERIM LLC** certificates. Since EvilAI and TamperedChef actors rotate them frequently, this is only the tip of the iceberg when it comes to certificate tracking within both campaigns.

There is not much reliable, public information behind **INSTALLERIM LLC**. Previous analysis points to a business entity registered in Ukraine[14]. Additional variants have been observed with obvious shell company names across multiple continents, making geographical attribution unreliable. INSTALLERIM LLC, like hundreds of other obvious shell companies, is part of the dynamic infrastructure of TamperedChef and EvilAI.

Different Outcomes, Same Website

Some TamperedChef and EvilAI campaigns utilize a decoy technique involving WinRAR, the common archiving software for Windows. During a visit to the lure website, potential victims are filtered using JavaScript and delivered a legitimate copy of WinRAR (SHA256: cfca124c2141b4171cebad48cc286751910b408aec69767db2bc3af38f277a06) instead of the utility advertised within the lure. While it's not uncommon for malware campaigns to provide decoy files to users as an anti-analysis technique, the use of WinRAR is unique among TamperedChef and EvilAI.

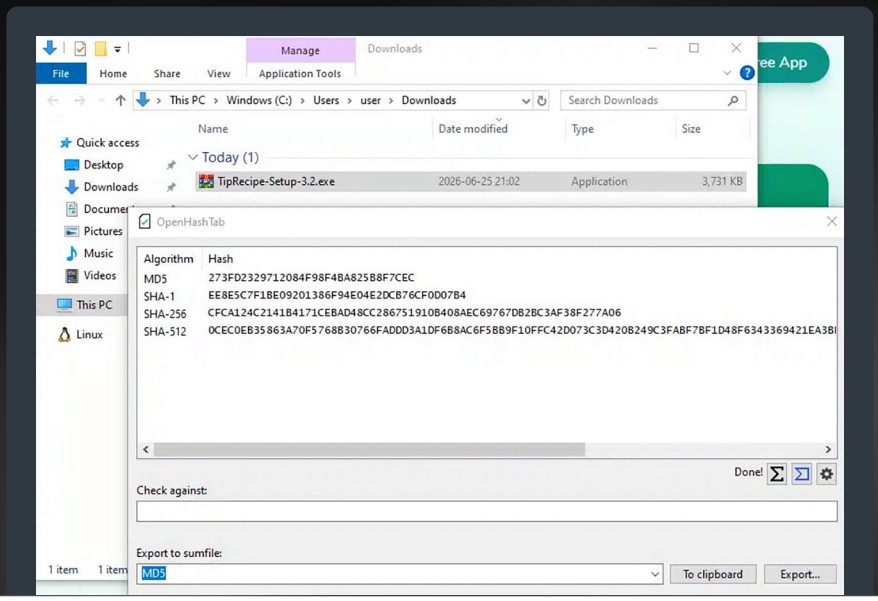


Figure 9. TipRecipe Decoy WinRAR Installer

The image to the right shows WinRAR installer aliases found on VirusTotal—showing many of the TamperedChef filenames.

```
WinRAR
WinRAR.exe
PDFSnap-2.23.exe
PDFSnap-2.3 (2).exe
PDFGrip-Install-2.2.1.exe
PDFFlows-Setup-v2.8.0 (1).exe
winrar-x64-720.exe
$TEMP/Setupko/winrar-x64-720 exe
PDFDocu-Setup-2.D.exe
PDFDocu-Setup-1.9.exe
PDFSnap-2.22.exe
clusers\GAIN BD\AppData\Local \Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000079
KitchenCanvas-Setup-2.8.exe
PDFSnap-2.21.exe
PDFDocu-Setup-1.8.exe
PDFDocu-Setup.exe
PDFFlows-Setup-v2.8.0.exe
PDFGrip-Setup-2.1.2.exe
PDFSnap-2.20.exe
FlipGrip.exe
tOegwBuyj.exe
PDFGrip-Setup-1.9.D.exe
PDFGrip-Setup-1.9.0 (1). exe
PDFGrip.exe
KitchenCanvas-Setup-3.6.exe
c:\users Administrator\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\f_00002e
PDFSnap-2.19.exe
TipRecipe-Setup-2.7.exe
PDFDocu-Setup-1.6.exe
PDFFlows-Setup-v2.5.0.exe
PDFSnap-2.7.exe
PDFGrip-Setup-2.0.4.exe
PDFSnap-2.18.exe
EasyDish-Setup-2.4.exe
PDFDocu-Setup-1.5.exe
PDFSnap-2.17.exe
```

Figure 10. Alternate filenames for WinRAR

Command & Control

Dynamic analysis of TipRecipe when executed shows connections to two domains: **foodformulaai[.]com** and **foodformulasetup[.]com**. Both domains resolve to a series of related Cloudflare IP Addresses. The resolved IP addresses have re-used by previous TamperedChef binaries. Command & Control (C2) domains are almost always related to the filename of the specific binary (ie. recipe = food, PDF = document) and are rotated frequently as new campaigns emerge:

Host	IP Address

`foodformulasetup[.]com`	`104.26.4.123`
	`104.26.5.123`
	`172.67.73.218`

`formulas[.]foodformulasetup[.]com`	`104.26.5.123`
	`172.67.73.218`
	`104.26.4.123`

Nearly all TamperedChef and EvilAI binaries have a check-in mechanism that involves a POST request with JSON sent back to the C2 server. These domains are hardcoded into the configuration of each binary and do not (at the time of this writing) appear to be dynamic. While Trinity Cyber has never observed follow on C2 traffic due to preventing earlier stages, our overall hypothesis is that TamperedChef and EvilAI operators are staging access to victim computers for malicious attacks in the future. They can achieve this remotely with C2 sent to infected endpoints.

Summary

EvilAI has demonstrated an agile malware distribution model built around rapidly generated infrastructure with both AdTech and shell companies behind registrations. The operators repeatedly deploy trojanized productivity applications through professionally presented lure websites that require relatively little customization beyond branding and basic functionality. By combining reusable installer logic, disposable domains, and frequently rotated code-signing certificates, the campaign can quickly replace disrupted infrastructure with new variants while preserving the same distribution pipeline. This operational model reduces the cost of rebuilding campaigns after detection and complicates reputation-based defenses, allowing the operators to continually introduce new lure applications—such as the recently observed food-themed TipRecipe site—without significantly changing their underlying tradecraft. Rather than relying on sophisticated exploitation, TamperedChef and EvilAI succeed through scale, convincing social engineering, and dynamic infrastructure designed for rapid iteration and staging for future malicious activity.

IOCs

INSTALLERIM LLC Binaries:

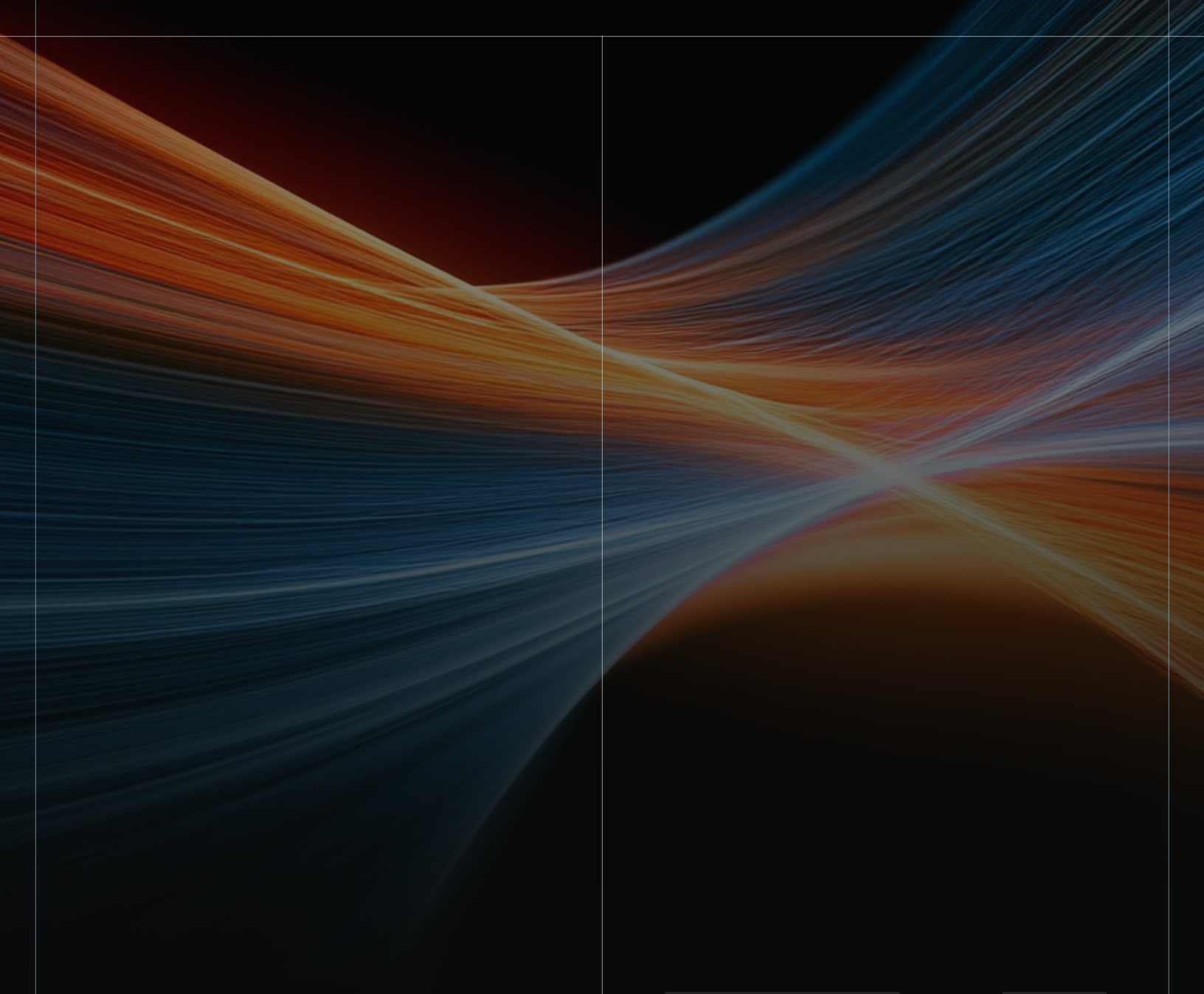
- dfd1251da5da673223fc362f9ea82f9f536ef04c95c70435b7d5a1b7b9106396
- 3c1dbc3f56e91cc79f0014850e773a7f12bbfef06680f08f883b2bf12873eccc
- e7bc36c7345b3894bc1da3d18ff3dbf0a20713d17b93a585ac0da65776d29027
- 2d4472be94023a83a60935345d38f24c378fabe60c66c26926749d65475c9eca
- e00abc28acca6ed100dc18f852c84a945d12c59767c7407ecbca46970b719c4c
- b04964c52417ab34551210f0cc419348da48bcd1a8d7c97ba90762a6d39f42ff
- 74e113427fb5809f295e14ceb25f3281a6903e999de8f0f0b59f174ebabc82be
- 29b425116eaf07d66a6909ba5911fc7dc0cd4954692022339eb6b0784310a0ef
- c98bab0254f37aa2688da1457e4b5c089f0b53d0ac8b111c3385ab90058b43ad
- 355171c1e1192e74701526e507a21d153197e1f3edb8da8196dc2b25cb6116c4
- 7cc2eb3998505ddd4180feb8266c93336a567f2c8e855686a2432a7c7db0648f
- c4c257deded93f62a7fe3e15586f9e450889aa568a21013ecf1accd050a90b66
- 6e7543ce7a240325d5448b9c921e08f829abb5babf8c678108bb26140eeca2b2
- b179bec73efe194bffb69eeedc8c136b5e7506a10b3589d223b1e6f8a8fbfb53
- 988f1a65f10dde8ed8e3b6793e1dc226f96911b507e21fae98a7abb88a6a0bd1
- 5d687b0466bbaf61d703046a8e8768f8b8c60686f5cc9c1ec6bcf0364d5c2ef9
- ad13b4f55f02156a6ce8f91546f67cf7128180a565555391a4ff5c23814d8058
- dca696a3404705a46e09bf32f37550d911db7248a35c84726299f604af7da8dd
- 23f979c14ab14b7832a4251686e111c3ed654d2222835725b9818819f36d6b7c
- d997c735883c0a190a34ad0540c48234b024f8dfcb9b01ff30ac93c9a4a5c572

TamperedChef Domains:

- **tiprecipe[.]com**
- **kitchen-canvas[.]com**
- **givemerecipe[.]com**
- **recipeup[.]com**
- **meal-formula[.]com**
- **dish-desk[.]com**
- **foodformulaai[.]com**
- **foodformulasetup[.]com**
- **formulas.foodformulasetup[.]com**

Sources

1. https://www.blumira.com/blog/suspicious-code-spike-fraudulent-recipe-application
2. https://blog.lukeacha.com/2025/06/suspicious-recipe-app.html
3. https://www.truesec.com/hub/blog/tamperedchef-the-bad-pdf-editor
4. https://expel.com/blog/you-dont-find-manualfinder-manualfinder-finds-you/
5. https://blog.gdatasoftware.com/2025/08/38257-appsuite-pdf-editor-backdoor-analysis
6. https://www.trendmicro.com/en_us/research/25/i/evilai.html
7. https://unit42.paloaltonetworks.com/tracking-tampered-chef-clusters/
8. https://www.guidepointsecurity.com/blog/ai-exposes-homoglyph-hustle/
9. https://expel.com/blog/the-history-of-appsuite-the-certs-of-the-baoloader-developer/
10. https://onestart.ai/blog/onestart-ai-is-not-malware/
11. https://onestart.ai/blog/onestart-malware-or-misunderstood/
12. https://security.googlecloudcommunity.com/security-validation-5/vhr20251126-november-26-2025-release-6359
13. https://unit42.paloaltonetworks.com/tracking-tampered-chef-clusters/
14. https://compassmsp.com/resources/articles/how-adversaries-leverage-advertisement-networks-to-breach-your-network



TRINITY CYBER

Take the Next Step

Contact us today to see the Trinity Cyber Platform in action.

trinitycyber.com