CAA-2026-0007 Browser Ads Driving Engagement with Low-Reputation Software

Summary

Since July 2025, CyberAlberta Threat Intelligence identified at least four campaigns using browser ads to deliver Potentially Unwanted Programs (PUPs). Some of these PUPs come bundled with information stealer malware or a backdoor.

Organizations should implement protective measures to reduce exposure to PUPs and similar low reputation software. Recommended measures include a combination of deploying an organization-wide ad blocker, and restricting software installation to trustworthy and high-prevalence programs.

Details

Antivirus vendors use the classification of Potentially Unwanted Program (PUP)—also known as a Potentially Unwanted Application (PUA) or "bundleware"—to describe a seemingly legitimate software application that bundles either undesirable or malicious functionality. PUPs are commonly distributed through installers for productivity tools, browser extensions, and toolbars where they introduce adware or spyware as a monetization strategy.

Recent PUP campaigns have bundled information stealer malware or the application itself contains a malicious backdoor. Many PUP campaigns, such as TamperedChef,[1] leverage Google Ads or search engine optimization (SEO) poisoning to target users seeking productivity software. This activity highlights the risk posed by unrestricted software installation in enterprise environments.

Recent Campaigns

Figure 1. Timeline of Observed PUP Campaigns

Since early January 2026, CyberAlberta Threat Intelligence identified several PUP campaigns using a common tactic of presenting themselves as productivity software: PDF file editor, PDF converter, or an AI-enabled cooking assistant.

[1] https://www.acronis.com/en/tru/posts/cooking-up-trouble-how-tamperedchef-uses-signed-apps-to-deliver-stealthy-payloads/

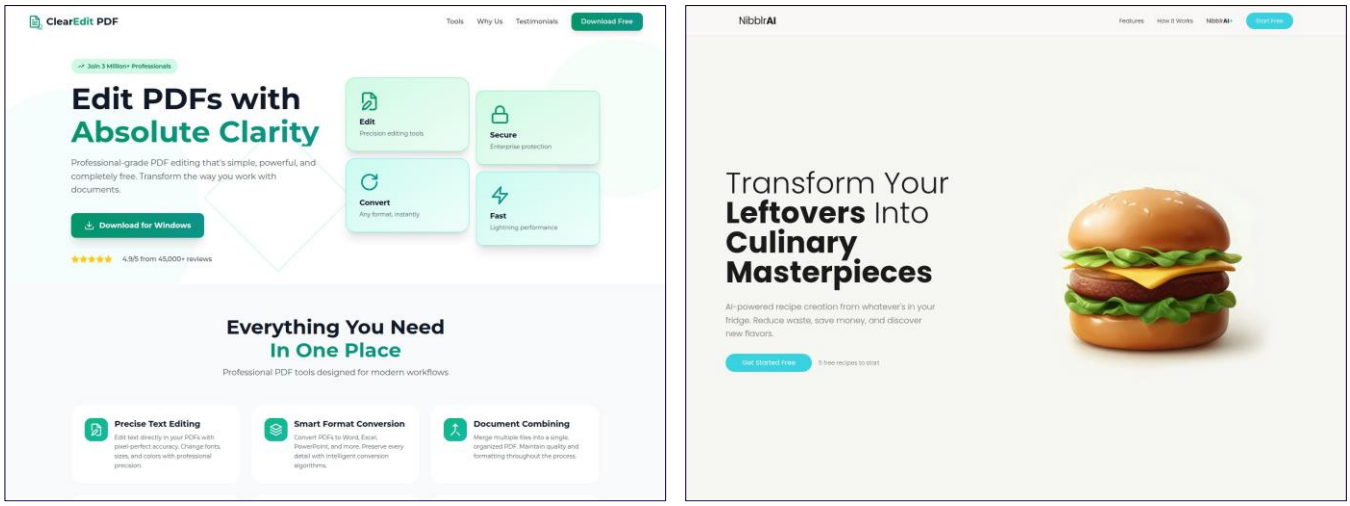

Figure 2. Websites Hosting PUP Downloads (Left: clearedítpdf[.]com, Right: nibblrai[.]com)

In one example, a PDF-themed PUP named ProfessionalConvert offers users ten free file conversions before requesting payment (Figure 3). However, the payment screen does not validate credit card information and accepts arbitrary input. Additionally, the PUP installs an illegitimate root Certificate Authority into the host operating system then gathers and exfiltrates system information over a TLS-encrypted channel on port 443 masquerading as HTTPS traffic.

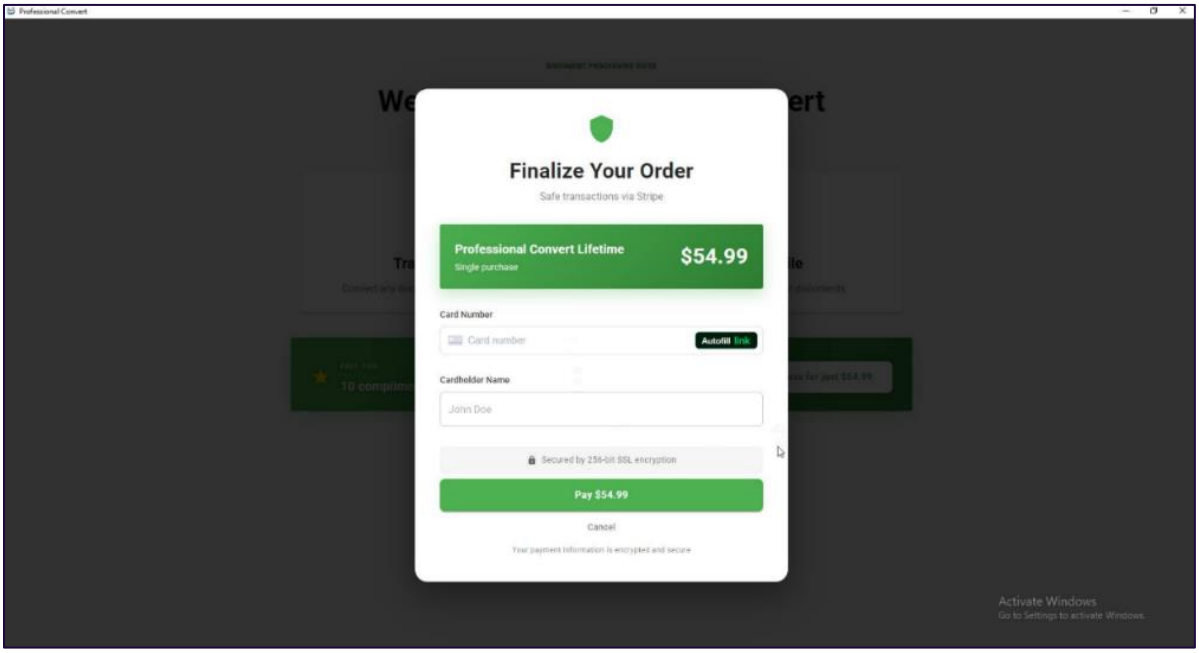

Figure 3. Professional Convert, a PDF-Themed PUP

Use of Google Ads to Drive Engagement

At least five of the observed PUPs from this recent campaign leveraged Google Ads to increase the likelihood of engagement and redirect users to a download page for the PUP's installer (Figure 4).

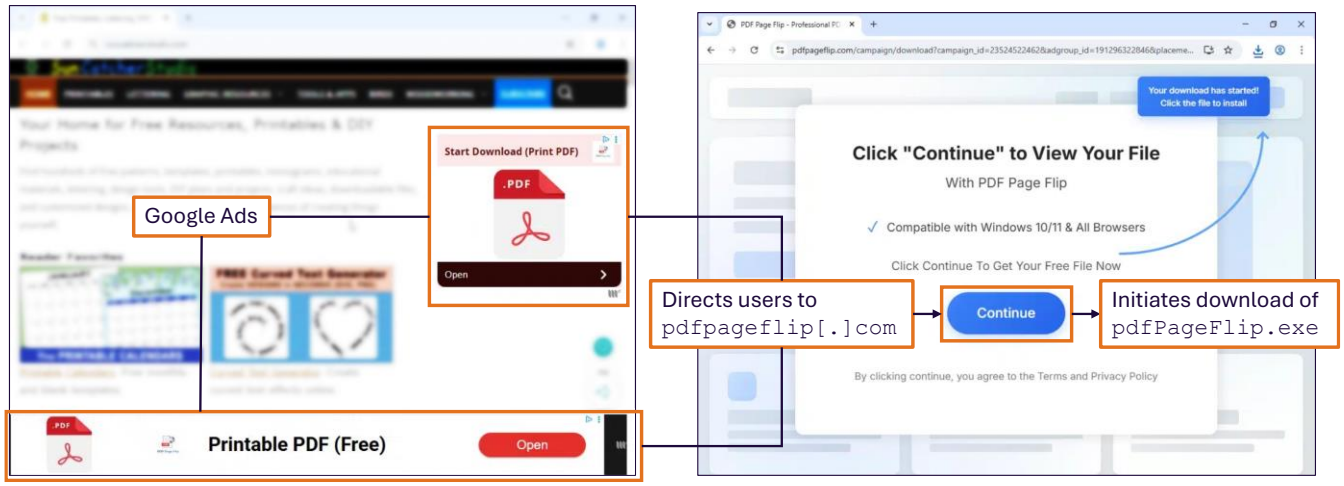

Figure 4. Google Ad Redirect to "PDF Page Flip" – A PDF Viewer PUP 'PDF

The file origin URL of `pdfPageFlip.exe` (Figure 5), and all other observed PUPs, contain the following URL parameters that are associated with Google Ads: `campaign_id`, `adgroup_id`, and `placement_id`.

```
https[:]//pdfpageflip-
cdn[.]com/pdfPageFlip.exe?campaign_id=[ID]&adgroup_id=[ID]&placement_id=suncatcher
studio.com&creative_id=[ID]&spa=EAIaIQobChMIvcKBhIK-
kgMVCAakBh3p8TdEEAEYASAAEgLJLfD_BwE&gad_source=5&gad_campaignid=23524510012&gclid=
EAIaIQobChMIvcKBhIK-kgMVCAakBh3p8TdEEAEYASAAEgLJLfD_BwE
```

Figure 5. File Origin URL of `pdfPageFlip.exe`

Owners of Google Ads

Analysis of the domains in the Google Ads Transparency Center revealed four distributors of Google Ads redirecting users to PUP installers:

- Brain Faculty LLC
- Binary Wave Innovations LLC
- AdsRoad Pass Limited
- Byte Blaze Pro LLC

Between November 2025 and March 2026, these four entities distributed a combined total of over 600 Google Ads in Canada. All four distributors had achieved verification by Google.[2][3]

[2] https://support.google.com/adspolicy/answer/15577076
[3] https://support.google.com/adspolicy/answer/9872280

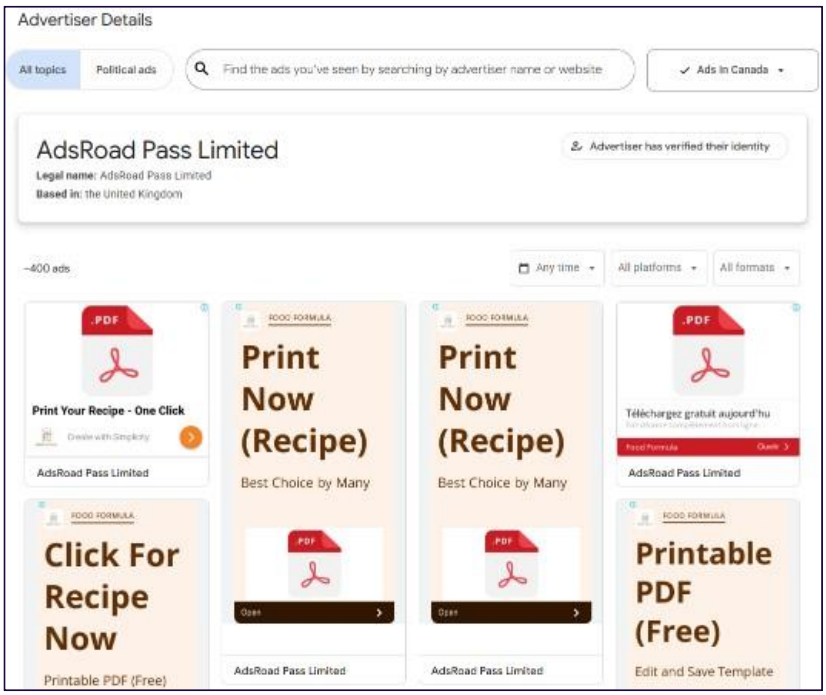

Figure 6. Google Ads for PUPs Distributed by 'AdsRoad Pass Limited'

Further analysis of the Google Ads revealed three previously unidentified distribution domains: `readslickpdf[.]com`, `readslickpdf-ddl[.]com`, and `mypdfswitch[.]com`.

Decoy Payloads

Occasionally, victims of these campaigns received a benign, decoy payload. Typically, this decoy was a legitimate installer for WinRAR or Okular—a document viewer. When a user receives a malicious PUP, the filename contains five to six random numbers, for example `ConverKit_474317.exe`. However, when a user received a decoy file, the numerical string was absent, for example `ConverKit.exe`. It is unclear why these decoy files were delivered, but is likely the result of conditional filtering to evade detection by automated malware analysis systems, such as a sandbox.

Historic Campaigns

Crystal PDF

In December 2025, multiple interactions were observed with domains hosting an information stealer masquerading as an installer for a PDF file converter dubbed Crystal PDF (Figure 7). Microsoft Threat Intelligence noted this malicious installer establishes persistence via scheduled tasks and hijacks browser sessions, extracting sensitive files and session data to command and control (C2) servers.[4]

[4] https://www.microsoft.com/en-us/security/blog/2026/02/02/infostealers-without-borders-macos-python-stealers-and-platform-abuse/

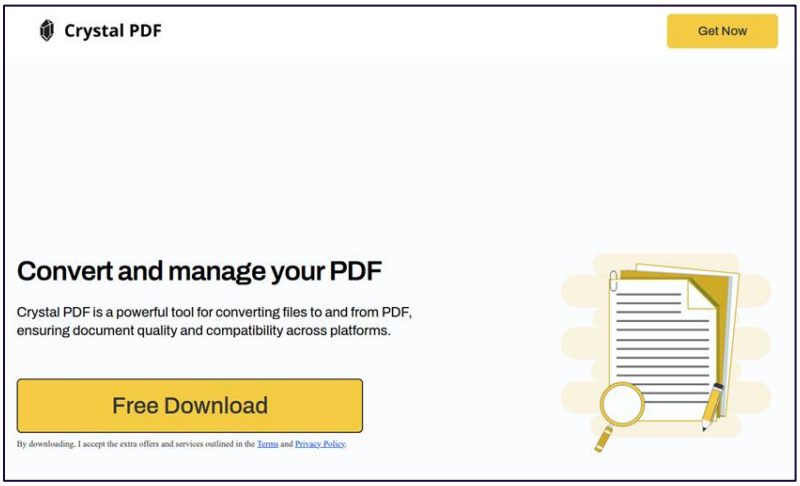

Figure 7. Website crystalpdf[.]com

CrystalPDF also leveraged Google Ads to increase engagement with users, with similar parameters present in the file's origin URL (Figure 8).

```
https[:]//smartdwn[.]com/download?v=<GUID>&campaign_id=<ID#>&utm_source=google_b2b
&subid=<domainSource>&kw=true&gad_source=5&gad_campaignid=<ID#>&gclid=<>
```

Figure 8. Crystal PDF File Origin URL

Calendaromatic

In September 2025, multiple public reports identified malicious productivity-themed calendar software, named Calendaromatic (Figure 9), hijacking browser sessions and exfiltrating sensitive information.[5][6]

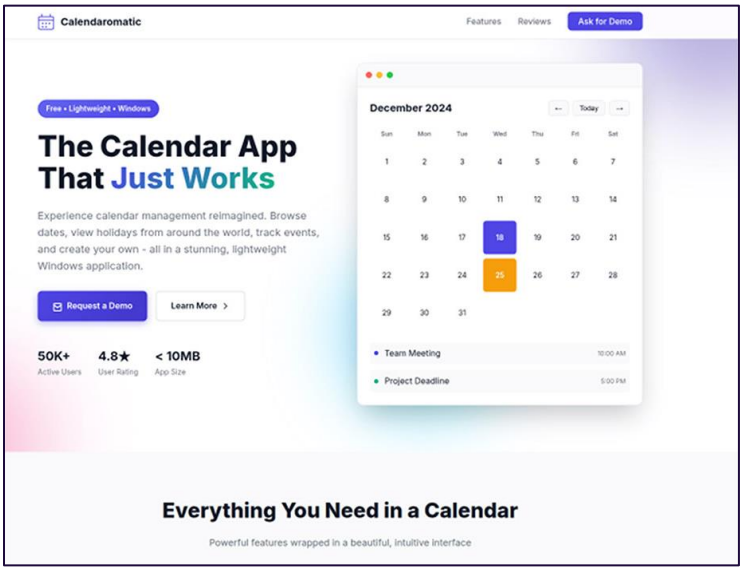

Figure 9. Website for calendaromatic[.]com

[5] https://fieldeffect.com/blog/potentially-unwanted-applications
[6] https://www.kroll.com/en/publications/cyber/widespread-installation-calendaromatic-adware-homoglyph-channel

This campaign was assessed by multiple teams to have leveraged sponsored search results and Google Ads to promote the domains delivering Calendaromatic (and a related malware known as ImageLooker) to the top of search results for users seeking this type of software.

TamperedChef - AppSuite PDF Editor Backdoor

In July 2025, a malware campaign dubbed TamperedChef leveraged Google Ads to direct users to a Windows Installer file (.MSI) for a PDF-themed software named AppSuite PDF Editor that contained a backdoor.[7]

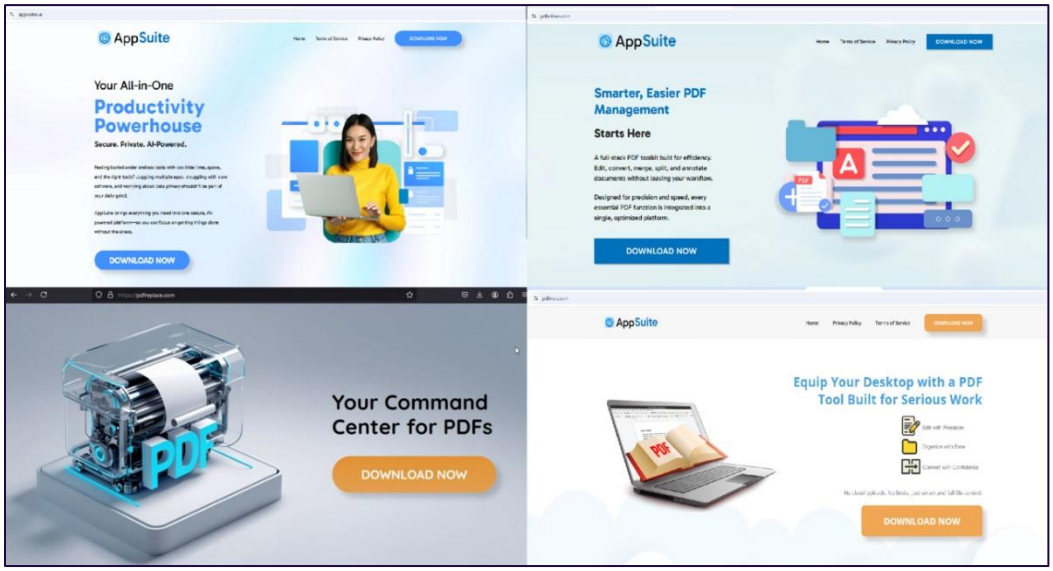

Figure 10. Multiple Websites Distributing the AppSuite PDF Editor (source: @struppigel.bsky.social[8])

Analysts at G DATA Security Lab noted that the developers of this trojanized PDF editor submitted samples of their malware as a false positive to antivirus companies, requesting their detections to be removed. As a result, AppSuite PDF Editor was incorrectly assessed as a PUP.[9] However, researchers from Truesec and WithSecure observed devices with AppSuite PDF Editor later received a malicious update on 21 August 2025 that contained an information stealer.[10][11]

Assessment

CyberAlberta Threat Intelligence assesses that PUPs and trojanized software will likely continue to victimize unsuspecting users and increase the risk of additional malware, such as information stealers and remote access trojans. As the reported events demonstrate, end users frequently install unapproved software to complete routine tasks. This risk is amplified by threat actors using paid advertisement space for increased exposure and submitting samples as false positives to evade detection. As a result, robust controls and policies are needed to mitigate the risk of PUPs quicker, freeing up incident responders from what is becoming a routine event.

Recommendations

To mitigate the risks presented by PUPs, organizations should adopt:

[7] https://www.sophos.com/en-us/blog/tamperedchef-serves-bad-ads-with-infostealers-as-the-main-course
[8] https://bsky.app/profile/struppigel.bsky.social/post/3lwtpsng4hc2p
[9] https://www.gdatasoftware.com/blog/2025/08/38257-appsuite-pdf-editor-backdoor-analysis
[10] https://labs.withsecure.com/publications/tamperedchef
[11] https://www.truesec.com/hub/blog/tamperedchef-the-bad-pdf-editor

- An organization-wide browser-based ad blocker, as per CCCS guidance, to protect organizations from malware:[12]
  - The ad blocker should be supported by a risk assessment and appropriate patch management.
  - Alternatively, DNS filtering, also known as Protective DNS (PDNS), can also be implemented to further mitigate interactions with malicious infrastructure.[13]
- Vendor-specific security controls such as:
  - Microsoft Defender SmartScreen policy for blocking PUPs.[14]
  - Microsoft Defender for Enterprise (MDE) Attack Surface Reduction (ASR) rule “Block executable files from running unless they meet a prevalence, age, or trusted list criterion.”[15]
- CCCS guidance for application control by restricting what software is permitted. [16][17]

Detection Opportunities

```
// Detect PUPs downloaded via Google Ads
let Google_Ad_URL_Parameters = dynamic(["campaign_id=", "adgroup_id=",
"placement_id="]);
DeviceFileEvents
| where
    FileOriginReferrerUrl has_all(Google_Ad_URL_Parameters)
    or
    FileOriginUrl has_all(Google_Ad_URL_Parameters)
| where ActionType == "FileCreated" and FolderPath !contains "Recycle.Bin"
| sort by Timestamp desc
```

Figure 11. - KQL Query for detecting PUPs downloaded via Google Ads.

Indicators of Compromise (IOCs)

The following Indicators of Compromise (IOCs) characterize the PUP campaigns described in this report.

Description	Indicator
Unattributed PUPs - Domains	cleareditpdf[.]com
	cleareditpdfdd[.]com
	readslickpdf[.]com
	readslickpdf-ddl[.]com
	myeditorpdf[.]com
	mypdfswitch[.]com
	sparkeditpdf[.]com
	sparkonsoft[.]com
	docflares[.]com
	nibblr-ai[.]com
	ainibblrusa[.]com

[12] https://www.cyber.gc.ca/en/guidance/protect-your-organization-malware-itsap00057
[13] https://www.cyber.gc.ca/en/guidance/protective-domain-name-system-itsap40019
[14] https://learn.microsoft.com/en-us/deployedge/microsoft-edge-browser-policies/smartscreenpuaenabled
[15] https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#block-executable-files-from-running-unless-they-meet-a-prevalence-age-or-trusted-list-criterion
[16] https://www.cyber.gc.ca/en/guidance/top-10-security-actions-number-4-harden-operating-systems-and-applications-itsm10090
[17] https://learn.microsoft.com/en-us/windows/security/application-security/application-control/app-control-for-business/appcontrol

	dish-desk[.]com
	dish-deskcdn[.]com
	kitchen-canvas[.]com
Unattributed PUPs - SHA256 Hashes	11d342f01a9deb1d8dbeb8030255fdd5ec4ba4f5c9029d38e0c71d3e885f6ddf
	17e58940134e52257987399e55812858586702e79a0d70b568d71cb7ae632897
	5e3b16a08257951e5e5bda8b5c9414a1f35c354d312e6ded7bdad2d39a47829a
	2e3136adaf91f431cf6cacb303a52011eb29e383db216e00c0c49d41ca8f5e52
	5e67ea6ea287fd68492c520d188b13996126ea0d4f4e10c1f0c89d3bc3c77c50
	686d018c86c03165925ebd3773c622f182c93f54b98db9616bae86f5e8684e4c
	87f4b996f0ca6b937577109cb4b74ea7c6bd32bea76f38d938153176af5174a5
	92bbfe8572c148b95f2cd9581718377fadcdfd075bdde32b961f726e31e0aa7b
	9776f251353c7d1376635a84919ea8472e98f3821845c0a51e3298e8e945104e
	a81169ff82c030f88a2d70de160027f22619126465f6f3051462ee7ebad9c88c
	b00b77ec01df64677a7efa571a4a920e8167ed039d4f3fe4e95fa130d2b3e844
	b389375aca18cc65063aa96b94824b4c218ddf6b6f2866cd33b6677a9576b76f
	b5dc803aa9f35ab89b52b64b8c1a657a7759e5035eb94027d126761faa4af57b
	d5332a30dabb3df8d8f875911f1a98ab1a223815e65f58df7bd1a04ab11f2e40
	5861bfe3fe17cac44241715d2b9c383cef3bea165de2cf2ebac6ec69f51dce6c
	ded96ce9c1eb032cdb0ef9f116b26c6321e66fefbd68075a0a9f34cda8153e35
	f764da7d36536de6f050e93317a90823af4c24d4e5a9b5fdd756a158666c766f
Unattributed PUPs - Code Signers	New Mexico Star Networks LLC
	Hawk Integrated Inc
	Mainstay Crypto LLC 2025
	Financial Opportunities, Inc.
	International Holdings, LLC
	K Desktop Environment e. V.
	Monetize forward LLC
Crystal PDF – C2 Domains	negmari[.]com
	ramiort[.]com
	strongdwn[.]com
	crystalpdf[.]com
	smartdwn[.]com
	seranlo[.]com
	novarion[.]net
Crystal PDF – SHA256 Hashes	598da788600747cf3fa1f25cb4fa1e029eca1442316709c137690e645a0872bb
	3bc62aca7b4f778dabb9ff7a90fdb43a4fdd4e0deec7917df58a18eb036fac6e
	c72f8207ce7aebf78c5b672b65aebc6e1b09d00a85100738aabb03d95d0e6a95
	176cdfdb775d909ddb14cc5c3e7e035d1dd6ea7a36efe37e663f840fa75b9500
	0f76f6a9f7c2575f9312953d37b51a8e1a7cc38a0758e272deef25bd6593306e
Calendaromatic – Domains	calendaromatic[.]com
	theworldwhoisquite[.]com
	ovementxview[.]com

	lovetravellinga[.]com
Calendaromatic – SAH256 Hashes	69934dc1d4fdb552037774ee7a75c20608c09680128c9840b508551dbcf463ad
	e32d6b2b38b11db56ae5bce0d5e5413578a62960aa3fab48553f048c4d5f91f0
	497ed5bca59fa6c01f80d55c5f528a40daff4e4afddfbe58dbd452c45d4866a3
	c24774d9b3455b47a41c218d404ae6b702da0d2e3e8ad3d2a353ffddd62239c2
Calendaromatic – Code Signers	CROWN SKY LLC
AppSuite PDF Editor Backdoor - Domains	pdfmeta[.]com
	pdfartisan[.]com
	appsuites[.]ai
	pdfreplace[.]com
AppSuite PDF Editor Backdoor – SHA256 Hashes	fde67ba523b2c1e517d679ad4eaf87925c6bbf2f171b9212462dc9a855faa34b
	b3ef2e11c855f4812e64230632f125db5e7da1df3e9e34fdb2f088ebe5e16603
	6022fd372dca7d6d366d9df894e8313b7f0bd821035dd9fa7c860b14e8c414f2
	da3c6ec20a006ec4b289a90488f824f0f72098a2f5c2d3f37d7a2d4a83b344a0
	cb15e1ec1a472631c53378d54f2043ba57586e3a28329c9dbf40cb69d7c10d2c
	956f7e8e156205b8cbf9b9f16bae0e43404641ad8feaaf5f59f8ba7c54f15e24
	104428a78aa75b4b0bc945a2067c0e42c8dfd5d0baf3cb18e0f6e4686bdc0755
AppSuite PDF Editor Backdoor – Code Signers	ECHO Infini SDN BHD
	GLINT By J SDN. BHD
	SUMMIT NEXUS Holdings LLC, BHD

Table 1. PUP Campaign Indicators of Compromise

MITRE ATT&CK

The following table maps tactics, techniques, and procedures (TTPs) described in this report to the MITRE ATT&CK Framework.

Tactic	Technique	Observable
Resource Development	T1583.008 - Acquire Infrastructure: Malvertising	Threat actors used Google Ads to increase visibility and engagement with PUP campaigns.
	T1587.002 - Develop Capabilities: Code Signing Certificates	Threat actors acquired code signing certificates to sign PUP installers.
Initial Access	T1189 - Drive-by Compromise	Victims are compromised during normal browser activity, with Google Ads providing the lure to their own domains delivering PUPs.
Execution	T1204.002 - User Execution: Malicious File	Users must download and execute the PUP installers.

Table 2. Unattributed PUP Campaign TTPs