KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Hackers Exploited Google Search Ads to Spread “BatLoader” Malware

Tracker ID: TN2340 **Date:** March 20, 2023 **Category:** Malware **Industry:** All **Region**: All

Background

Researchers discovered “BatLoader” activity in December, in which Google Search Ads were exploited to imitate products such as WinRAR to send malicious Windows Installer packages. The installation files contained bespoke action instructions that leveraged PowerShell to download and execute payloads hosted on legitimate websites (Redline Stealer, Ursnif, and so on). Malicious adverts promoting malware have recently become more prevalent in Google search results. In one such campaign, threat actors created new websites mimicking various legitimate products and businesses, including ChatGPT, Zoom, Spotify, AnyDesk, Microsoft Teams, Java, Tableau, and Adobe, and used Google Adwords to disseminate the BatLoader.

These phony websites host and distribute malicious Windows installer files that contain custom action commands which enable an embedded batch file (InstallPython[.]bat or PythonFramework[.]bat) with admin rights to be executed in a hidden window. The batch file unwraps two PyArmor-protected Python files. The files run Python code containing the BatLoader payload to obtain next-stage malware housed on a remote server, such as Vidar Stealer and Ursnif.

The malware strains changed throughout the campaign, which began in February. The most recent BatLoader samples cannot establish persistent access to business networks; nevertheless, this capability has been included in the most recent version. The batch file in the mid-February version had a third Python file, obfuscated using PyArmor, that contained an identical set of commands to handle payload retrieval, decryption, and execution. That Python file assists in the curation of payloads for domain-joined computers with more than two IP neighbors in the ARP table. BatLoader probably employed Cobalt Strike alongside conventional payloads like Vidar Stealer and Ursnif.

BatLoader is continually changing, employing more plausible trickery such as imitating well-known corporate programs and spreading via Google advertisements. A range of new malware has lately employed the same impersonation tactics. Thus, employers are advised to educate employees on how to protect themselves against malware disguised as legitimate programs and implement measures to safegaurd enterprise from such threats.

MITRE ATT&CK Tactics

Initial Access, Execution, Persistence, Defense Evasion, Command and Control, Exfiltration and Impact.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Hackers Exploited Google Search Ads to Spread "BatLoader" Malware

Tracker ID: TN2340 **Date:** March 20, 2023 **Category:** Malware **Industry:** All **Region**: All

Indicators of Compromise *

Please refer to the attached sheet for IOCs.

Recommendations

- Check with your existing AV/EDR vendor to validate the detection scope of identified samples.
- Raise awareness of malware masquerading as legitimate applications and include relevant examples within Phishing and Security Awareness Training (PSAT) program to educate the employees on how to protect themselves against similar cyber threats.
- Protect endpoints against malware and ensure antivirus signatures are up-to-date.
- Check the URL the one is visiting to ensure the site is legitimate before clicking on it or downloading software. The intended URL may be like a legitimate domain name, but it may have errors like a misplaced letter.
- Implement email restriction on downloading suspicious files from unknown sources.
- Block users from connecting to dangerous domains, IP addresses, and URLs, regardless of whether they are on or off the business network.
- Use a Next-Gen AV (NGAV) or Endpoint Detection and Response (EDR) product to detect and contain threats.
- Monitor and control the execution of applications and their dependencies, including DLLs, to detect and prevent malicious activities.
- Use complex passwords and enforce multi-factor authentication wherever possible and follow multilayered defense solutions and active monitoring to detect threats before operators can launch their attacks.

References

- Blog, BatLoader Abuse Google Search Ads to Deliver Vidar Stealer and Ursnif, March 09, 2023, External Link (www.esentire.com).
- Cyware Alerts, Hackers Push BatLoader via Google Search Ads, March 13, 2023, External Link (ww.cyware.com).

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176471471

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Hackers Exploited Google Search Ads to Spread “BatLoader” Malware

Tracker ID: TN2340 **Date:** March 20, 2023 **Category:** Malware **Industry:** All **Region**: All

*	MD5	URL	Domain
	3db1edc5b5550f54abdcb5520cf91d75	shvarcnegerhistory[.]com	chatgpt-t[.]com
	0cb75b1192b23b8e03d955f1156ad19e	Pixelarmada[.]su	zoomvideor[.]com
	85fbc743bb686688ce05cf3289507bf7	uelcoskdi[.]ru	adobe-l[.]com
	11ae3dabdb2d2458da43558f36114acb	iujdhsndjfks[.]ru	freecad-l[.]com
	9ebbe0a1b79e6f13bfca014f878ddeec	isoridkf[.]ru	microso-t[.]com
		gameindikdowd[.]ru	spotify-uss[.]com
		jhgfdlkjhaoiu[.]su	quickbooks-q[.]com
		reggy506[.]ru	freecad-f[.]com2
		reggy914[.]ru	java-s[.]com
			adobe-e[.]com
			anydesk-o[.]com
			anydesk-r[.]com
			java-r[.]com
			tableau-r[.]com
			java-a[.]com
			basecamp-a[.]com
			adobe-a[.]com
			visualstudio-t[.]com
			openoffice-a[.]com
			bitwarden-t[.]com
			gimp-t[.]com
			figma-t[.]com6