KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | OriginLogger replaces Agent Tesla in newer campaigns

Tracker ID: TN0920 **Date:** 20/Sept/2022 **Category:** Threat Actor **Industry:** All **Region**: All

Background

OriginLogger, a new malware program, is being utilized as a variation of Agent Tesla, a prominent information stealer and remote access trojan (RAT). Agent Tesla is a keylogger and remote access tool built on the .NET framework, that enables malicious actors to get remote access to target systems and beacon sensitive data to a domain controlled by them. It has been in use since 2014 and is advertised for sale on dark Web forums. It is typically distributed as an attachment in malicious spam emails. In February 2021, two new versions of the generic malware (versions 2 and 3) appeared, with the capacity to steal login information from online browsers, email clients, and VPN clients, as well as use the Telegram API for C&C.

OriginLogger, aka Agent Tesla version 3, is said to have sprouted up to fill the vacancy left by the former after its operators closed business on March 4, 2019, due to legal concerns. On May 17, 2022, the first malware sample for "OriginLogger.exe" was added to the VirusTotal. The new executable now allows a customer to specify the type of data to be captured, such as clipboards, screenshots, and a list of the other services and apps (browsers, email clients, etc.) from which the credentials are to be retrieved. Based on the two builder artifacts produced on September 6, 2020, and June 29, 2022, it achieves user authentication by sending a request to an OriginLogger server, which resolves to the domain names 0xfd3[.]com and its more modern counterpart, originpro[.]me.

Two source code repositories were also identified on a GitHub profile with the username "0xfd3," which is maintined for gathering credentials from Google Chrome and Microsoft Outlook, utilized in OriginLogger. Similar to Agent Tesla, it is transmitted via a fake Microsoft Word document that, when opened, is intended to display a picture of a German passport, a credit card, and several Excel worksheets. The worksheets themselves include a VBA macro that uses MSHTA to access an HTML page hosted on a remote server. In turn, the HTML page contains obfuscated JavaScript code, which calls two encoded binaries hosted on Bitbucket.

The first of the two malicious components is a loader that injects the second executable, the OriginLogger payload, into the trusted aspnet_compiler.exe process, which is used to precompile ASP.NET programs. The malware leverages well-known mechanisms to keylog, steal passwords, grab screenshots, download additional payloads, post data in a variety of methods, and avoid detection. In addition, an examination of over 1900 samples found that the most commonly used exfiltration techniques for delivering data to the attacker are 181 distinct bots, SMTP, FTP, web uploads to the OriginLogger panel, and Telegram.

OriginLogger and its predecessor, Agent Tesla, are both commoditized keyloggers in terms of similarities and code, but distinguishing them is critical for tracking and comprehension. Commercial keyloggers have generally catered to less competent attackers, but as evidenced by the first lure documents, attackers are nonetheless capable of obfuscating and complicating the investigation. As a result, commercial keyloggers should be used with the same caution as any malware.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | OriginLogger replaces Agent Tesla in newer campaigns

Tracker ID: TN0920 **Date:** 20/Sept/2022 **Category:** Threat Actor **Industry:** All **Region**: All

MITRE ATT&CK Tactics

Initial access, Defense Evasion, Exfiltration and Command and Control.

Indicators of Compromise *

Please refer to the attached sheet for IOCs.

Recommendations

- Validate the IOCs attached and implement the detection & prevention accordingly. Check with your existing AV/EDR vendor to validate the detection scope of identified samples.
- Keep systems and products updated as soon as possible after the patches are released.
- Deploy Multi Factor Authentication for all services. Ensure strong password policies, where strong, unique passwords are required for all services.
- Keyloggers and most malware are often distributed via phishing emails. Thus, it's essential that users are educated on the importance of not clicking on hyperlinks or attachments from untrusted sources.
- Restrict network connections, including VPN, to the critical systems on the network. Disable unused or unnecessary network services, ports, protocols, and devices.

References

- Jeff White, OriginLogger: A Look at Agent Tesla's Successor, Unit 42 PaloAlto, 13th September 2022, External Link (unit42.paloaltonetworks.com)
- Ravie Lakshmanan, Researchers Detail OriginLogger RAT — Successor to Agent Tesla Malware, The Hacker News, 14th September 2022, External Link (thehackernews.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 Cyber Threat Intelligence Platform

Cyber Threat Notification | OriginLogger replaces Agent Tesla in newer campaigns

Tracker ID: TN0920 **Date:** 20/Sept/2022 **Category:** Threat Actor **Industry:** All **Region**: All

*

SHA-256	Domains	URLS	IPs
595a7ea981a3948c4f387a5a6af54a70a41dd604685c72cbd2a55880c2b702ed	originpro[.]me	hxxp://www.asianexportglass[.]shop/p/25.html	23.106.223[.]46
b22a0dd33d957f6da3f1cd9687b9b00d0ff2bdf02d28356c1462f3dbfb8708dd	originproducts[.]xyz	hxxps://bitbucket[.]org/!api/2.0/snippets/12sds/pEEggp/8cb4e7aef7a46445b9885381da074c86ad0d01d6/files/snippet.txt	204.16.247[.]26
ccc8d5aa5d1a682c20b0806948bf06d1b5d11961887df70c8902d2146c6d1481	origindproducts[.]pw	hxxp://www.coalminners[.]shop/p/25.html	31.170.160[.]61
dc8b81e2f3ea59735eb1887128720dab292f73dfc3a96b5bc50824c1201d97cf	originlogger[.]com	hxxps://agusanplantation[.]com/new/new/inc/7a5c36cee88e6b.php.	74.118.138[.]76
23fcaad34d06f748452d04b003b78eb701c1ab9bf2dd5503cf75ac0387f4e4f8	0xfd3[.]com		23.106.223[.]47
cddca3371378d545e5e4c032951db0e000e2dfc901b5a5e390679adc524e7d9c	mail.originlogger[.]com		
c2a4cf56a675b913d8ee0cb2db3864d66990e940566f57cb97a9161bd262f271			