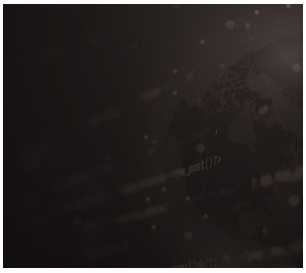
Rewterz Threat Alert – Widely Abused MSIX App Installer Disabled by Microsoft – Active IOCs

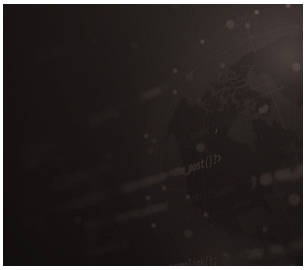
rewterz.com/rewterz-news/rewterz-threat-alert-widely-abused-msix-app-installer-disabled-by-microsoft-active-iocs/

December 30, 2023



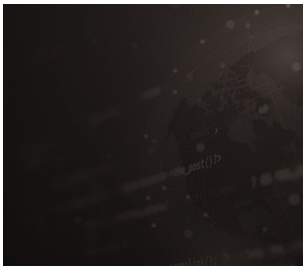
Rewterz Threat Advisory – CVE-2023-44362 – Adobe Prelude Vulnerability

December 31, 2023



Rewterz Threat Alert – SideWinder APT Group aka Rattlesnake – Active IOCs

December 30, 2023



Rewterz Threat Advisory – CVE-2023-44362 – Adobe Prelude Vulnerability

December 31, 2023

Severity

High

Analysis Summary

Microsoft stated that it is disabling the ms-appinstaller protocol handler again after various threat actors exploited it as an initial access vector to distribute malware. It was discovered that many cybercriminals are selling a malware kit that uses the ms-appinstaller protocol handler and MSIX file format.

The attacks utilize signed malicious MSIX application packages spread through Microsoft Teams or malvertising of legitimate popular software on Google Search. At least four financially motivated threat groups have been detected leveraging the App Installer service since November 2023 and using it for initial access for further ransomware operations. These groups are:

- Storm-0569 is an initial access broker that distributes BATLOADER using search engine optimization (SEO) poisoning with websites that spoof Zoom, TeamViewer, Tableau, and AnyDesk. It uses the loader malware to inject the Cobalt Strike payload and transfers access to Storm-0506 for the deployment of the Black Basta ransomware.
- Storm-1113 is an initial access broker that uses fake MSIX installers pretending to be Zoom to spread EugenLoader (aka FakeBat), acting as a conduit for several remote access trojans and stealer malware.
- Sangria Tempest (aka FIN7 and Carbon Spider) uses Storm-1113's EugenLoader to distribute Carbanak which delivers an implant named Gracewire. The group also relied on Google ads as a lure so victims downloaded malicious MSIX application packages from rogue landing pages to inject POWERTRASH which is used to load Gracewire and NetSupport RAT.
- Storm-1674 is an initial access broker that uses Teams messages to send fake landing pages that look like Microsoft OneDrive and SharePoint by using the TeamsPhisher tool. It urges the users to open PDF files that prompt them to update their Adobe Acrobat Reader. It downloads a malicious MSIX installer that has DarkGate or SectopRAT payloads.

In October 2023, another campaign was discovered in which fake MSIX Windows app package files for Microsoft Edge, Google Chrome, Grammarly, Brave, and Cisco Webex were used to propagate a malware called GHOSTPULSE. This is not the first time Microsoft has disabled the MSIX ms-appinstaller protocol handler in Windows as in February 2022, the company did it to prevent attackers from leveraging it to spread Emotet, Bazaloader, and TrickBot.

The reason cyber criminals choose to abuse the ms-appinstaller protocol handler is that it is capable of bypassing security mechanisms that are designed to keep users safe from malware, like Microsoft Defender SmartScreen and built-in browser warnings for downloads of executable file formats.

Impact

- Security Bypass
- Financial Loss
- Sensitive Information Theft

Indicators of Compromise

Domain Name

- amydeks.ithr.org
- scheta.site
- gertefin.com
- septcntr.com
- info-zoomapp.com
- storageplace.pro
- sun1.space

MD5

- dd131870c45342afdd00f314730481ca
- a2a868e6a1f660b8349a9083ccd44565
- 7d27ed94ba01dc9c2761af0ed84c616f
- 2ac5924081c7976cd114def3e603a178
- 140aa1b7d3ca8ba8c525624165c86b49

SHA-256

- 48aa2393ef590bab4ff2fd1e7d95af36e5b6911348d7674347626c9aaafa255e
- 11b71429869f29122236a44a292fde3f0269cde8eb76a52c89139f79f4b97e63
- 44cac5bf0bab56b0840bd1c7b95f9c7f5078ff417705eeaaf5ea5a2167a81dd5
- 2ba527fb8e31cb209df8d1890a63cda9cd4433aa0b841ed8b86fa801aff4ccbd
- 06b4aebbc3cd62e0aadd1852102645f9a00cc7eea492c0939675efba7566a6de

SHA-1

- e915271b74704df25dca82a291330b14d36d4788
- 2a067ae967fe4035baccbbb5e1c38da31a09ab5b
- c2d9ecb9e0496dd21e636a77fac370325b8ae6ef
- 55ccec9cafca2b3680e898d5fe7614d4807ff176
- 6a688c406f72a4f6892c80f221c222705299db10

URL

- https://scheta.site/api.store/ZoomInstaller.msix
- https://scheta.site/api.store/Setup.msix

Remediation

- Block all threat indicators at your respective controls.
- Search for Indicators of compromise (IOCs) in your environment utilizing your respective security controls
- Ensure that all systems, software, and applications are up-to-date with the latest security patches. Regularly check for and apply updates to eliminate known vulnerabilities that attackers could exploit.
- Educate employees about phishing emails, social engineering tactics, and safe online behavior. Effective training can reduce the likelihood of users inadvertently initiating an attack.
- Regularly back up critical data and systems to offline or isolated storage. Test the backup restoration process to ensure that it is effective in case of an attack.
- Implement a web application firewall to filter out malicious traffic and protect against common web-based threats.
- Implement strong access controls, including limiting login attempts and using two-factor authentication (2FA) to enhance login security.
- Deploy strong endpoint protection solutions that include advanced threat detection, behavior monitoring, and real-time protection against malware and ransomware.
- Employ robust email filtering and anti-phishing solutions to detect and prevent malicious attachments and links from reaching user inboxes.
- Thoroughly assess third-party vendors and software before integrating them into your environment. Ensure they have strong security practices and adhere to cybersecurity standards.