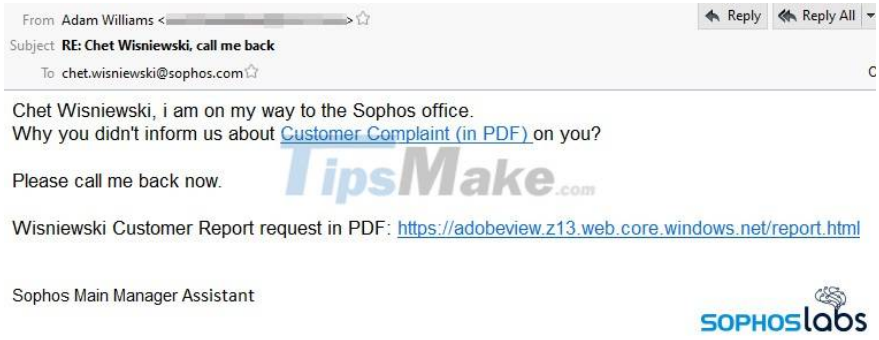
App Installer on Windows 10 was used to install BazarLoarder malware

The TrickBot hacker group is said to be taking advantage of Windows 10's App Installer to spread their BazarLoader malicious code on the systems they target.

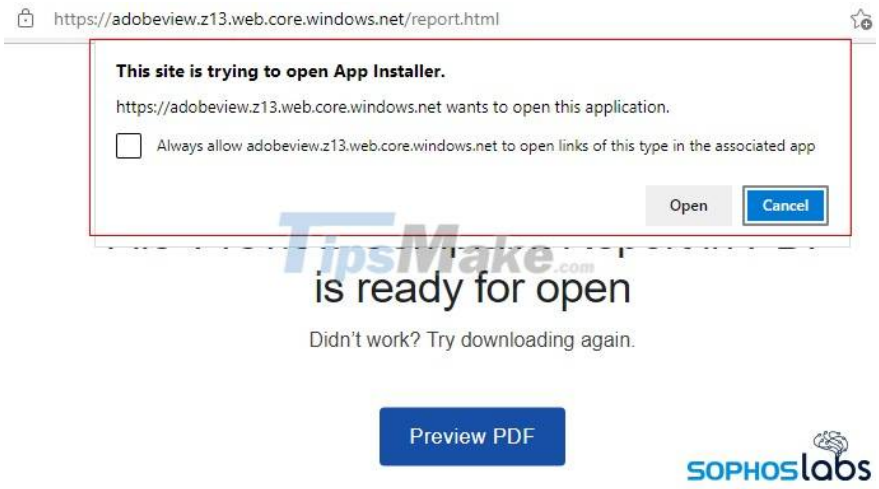
BazarLoader (also known as BazarBackdoor, BEERBOT, KEGTAP, and Team9Backdoor) is a type of Trojan that silently infiltrates the networks of high-value targets. Then, the people behind BazarLoader will exploit the assets they compromised or resell access to other cybercriminals.

BazarLoader also carries other malicious code such as Cobalt Strike. In this way, they can help attackers install additional malicious software, such as the Ryuk ransomware.

In the most recent campaign, BazarLoader terrorized victims with phishing emails. The emails contain urgent and urgent content to trick the victim into clicking on the malicious link in the email. The link is also edited by cybercriminals and assigned to reputable domains such as Microsoft, Adobe.



After clicking the link, the "Preview PDF" button will open a URL with the prefix appinstaller. When this button is clicked, the browser will display a warning whether the victim allows the page to open the App Installer. Most people will ignore this warning when looking at the adobeview.*.*.web.core.windows.net domain name in the address bar.



Next, the victim clicks "Open", the Windows 11 App Installer will be deployed and the malware will be installed on the victim's machine in the form of a fake Adobe PDF Component. This component is distributed as an AppX application package.

A series of components, other files will be downloaded to complete the installation of BazarLoader.

After the deployment is complete, BazarLoader will start collecting information such as storage drive, processor, motherboard, RAM and IP address. These information will be sent to the hacker's server. The longer it lives on the victim's machine, the more dangerous BazarLoader is with its ability to attack and steal information that is constantly being upgraded.

After receiving the notice from Sophos, Microsoft removed the sites that hackers used to store malicious files for the BazarLoader attack campaign.