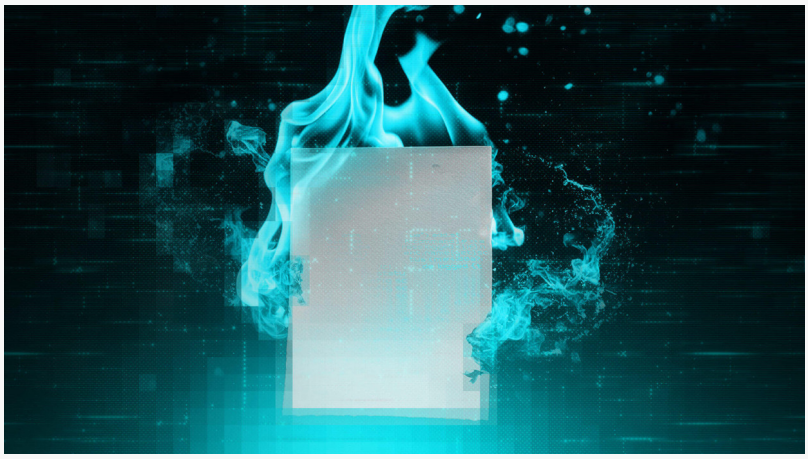
Chinese HotPage browser injector is capable of replacing web content and opens the system to other vulnerabilities, ESET



DUBAI, DUBAI, UNITED ARAB EMIRATES, July 19, 2024 /EINPresswire.com/ -- ESET Research has discovered a sophisticated Chinese browser injector: a signed, vulnerable, ad-injecting driver from a mysterious Chinese company. This threat, which ESET dubbed HotPage, comes self-contained in an executable file that installs its main driver and injects libraries into Chromium-based browsers. Posing as a security product capable of blocking advertisements, it actually introduces new ads. Additionally, the malware can replace the content of the current page, redirect the user, or simply open a new tab to a website full of other ads. The malware introduces more vulnerabilities and leaves the system open to even more dangerous threats. An attacker with a non-privileged account could leverage the vulnerable driver to obtain SYSTEM privileges or inject libraries into remote processes to cause further damage, all while using a legitimate and signed driver.

At the end of 2023, ESET researchers stumbled upon an installer named “HotPage.exe” that deploys a driver capable of injecting code into remote processes, and two libraries capable of intercepting and tampering with browsers’ network traffic. The installer was detected by most security products as an adware component. What really stood out to ESET researchers was the embedded driver signed by Microsoft. According to its signature, it was developed by a Chinese company named Hubei Dunwang Network Technology Co., Ltd.

“The lack of information about the company was intriguing. The distribution method is still unclear, but according to our research, this software was advertised as an internet café security solution aimed at Chinese-speaking individuals. It purports to improve the web browsing experience by blocking ads and malicious websites, but the reality is quite different — it leverages its browser traffic interception and filtering capabilities to display game-related ads. It also sends some information about the computer to the company’s server, most likely to gather

installation statistics," explains ESET researcher Romain Dumont, who discovered the threat.

According to available information, the business scope of the company includes technology-related activities such as development, services, and consulting – but also advertising activities. The principal shareholder is currently Wuhan Yishun Baishun Culture Media Co., Ltd., a very small company that looks to be specialized in advertising and marketing. Due to the level of privileges needed to install the driver, the malware might have been bundled with other software packages or advertised as a security product.

Using Windows' notification callbacks, the driver component monitors new browsers or tabs being opened. Under certain conditions, the adware will use various techniques to inject shellcode into browser processes to load its network-tampering libraries. Using Microsoft's Detours hooking library, the injected code filters HTTP(S) requests and responses. The malware can replace the content of the current page, redirect the user, or simply open a new tab to a website full of gaming ads. On top of its obvious mischievous behavior, this kernel component leaves the door open for other threats to run code at the highest privilege level available in the Windows operating system: the SYSTEM account. Due to improper access restrictions to this kernel component, any process can communicate with it and leverage its code injection capability to target any non-protected processes.

"The HotPage driver reminds us that abusing Extended Verification certificates is still a thing. As a lot of security models are at some point based on trust, threat actors are inclined to play along the line between legitimate and shady. Whether such software is advertised as a security solution or simply bundled with other software, the capabilities granted thanks to this trust expose users to security risks," adds Romain.
ESET reported this driver to Microsoft in March 2024 and followed their coordinated vulnerability disclosure process. ESET technologies detect this threat — which Microsoft removed from the Windows Server Catalog on May 1, 2024 — as Win{32|64}/HotPage.A and Win{32|64}/HotPage.B.

For more technical information about HotPage, read the blogpost "HotPage: Story of a signed, vulnerable, ad-injecting driver" on WeLiveSecurity.com. Make sure to follow ESET Research on Twitter (today known as X) for the latest news from ESET Research.

About ESET
ESET® provides cutting-edge digital security to prevent attacks before they happen. By combining the power of AI and human expertise, ESET stays ahead of known and emerging cyberthreats — securing businesses, critical infrastructure, and individuals. Whether it's endpoint, cloud or mobile protection, our AI-native, cloud-first solutions and services remain highly effective and easy to use. ESET technology includes robust detection and response, ultra-secure encryption, and multifactor authentication. With 24/7 real-time defense and strong local support, we keep users safe and businesses running without interruption. An ever-evolving digital landscape demands a progressive approach to security: ESET is committed to world-class research and

powerful threat intelligence, backed by R&D centers and a strong global partner network. For more information, visit www.eset.com or follow us on LinkedIn, Facebook, and X.

Sanjeev Kant
Vistar Communications
0559724623
email us here