HOME CYBER DEFENSE
ARE YOU SAFE FROM CYBER CRIME?
ALERT

Issued 7/6/18

This Password-Stealing Malware Just Added a New Way to Infect your PC

Distributed in spam email phishing campaigns, Smoke Loader has been sporadically active since 2011 but has continually evolved. The malware has been particularly busy throughout 2018, with campaigns including the distribution of Smoke Loader via fake patches for the Meltdown and Spectre vulnerabilities which emerged earlier this year. Like many malware campaigns, the initial attack is conducted via a malicious Microsoft Word attachment which tricks users into allowing macros, enabling Smoke Loader to be installed on the compromised system and allowing the Trojan to deliver additional malicious software. Researchers at Cisco Talos have been tracking Smoke Loader for some time and have seen its latest campaigns in action. One of the current preferred payloads is TrickBot -- a banking Trojan designed to steal credentials, passwords and other sensitive information. Phishing emails distributing the malware are designed to look like invoice requests from a software firm. What intrigued researchers is how Smoke Loader is now using an injection technique which hadn't been used to distribute malware until just days ago. The code injection technique is known as PROPagate and was first described as a potential means of compromise late last year. This technique abuses the SetWindowsSubclass function -- a process used to install or update subclass windows running on the system -- and can be used to modify the properties of windows running in the same session. This can be used to inject code and drop files while also hiding the fact it has happened, making it a useful, stealthy attack. Those behind this process have also added anti-analysis techniques to complicate forensics, runtime AV scanners, tracing, and debugging that any researchers may attempt to conduct on the malware. Each of these plugins are designed to steal sensitive information, specifically stored credentials or sensitive information transferred over a browser -- the likes of Firefox, Internet Explorer, Chrome, Opera, QQ Browser, Outlook, and Thunderbird can all be used to steal data. The malware can even be injected into applications like TeamViewer, potentially putting the credentials of others on the same network as the infected machine at risk too. It's possible that Smoke Loader has been equipped with these tasks because its operators aren't currently getting much business in response to adverts on dark web forums advertising their ability to install other types of malware onto their compromised network of machines. It could also just be a means of taking advantage of the botnet for their own purposes.