ModPipe Malware has a new module that siphons Credit Card Data

foregenix.com/blog/modpipe-malware-has-a-new-module-that-siphons-payment-card-data

23/03/21 11:58

By Mark Shelhart

Cybersecurity researchers at Foregenix have discovered what appears to be a new module for the *ModPipe* malware, previously reported by ESET in November 2020. Alarmingly, this new module has the ability to siphon sensitive Track1 and Track2 data from payment

systems, a featureset that had not previously been disclosed. Like the originally analysed and documented *ModPipe*, this module is most prevalent in the hospitality sector. This malware should be considered a high risk.

The *CCSiphon* (aka "*JHook*") module was observed in the wild targeting the CCS.exe application which is at the core of the RES 3700 POS management system, made by Oracle's Micros (Oracle Food and Beverage and Oracle Hospitality). What's fascinating about the module is that it strategically inserts itself between the Micros application and the decryption mechanism used by the system. This "app in the middle" listens when the Micros application needs to decrypt the payment card data. While Micros thinks it's talking to the official Microsoft DPAPI decryption routine, it is actually passing data that requires decryption directly to the malware. The siphon then leverages the actual crypto routines, quietly examining the data returned for evidence that it contains Track data. If Track data is found, the *CCSiphon* malware quietly writes the data to a buffered communications channel to be harvested later.

Foregenix researchers point out that while this sample of the new module is targeting the Micros RES 3700 system specifically, it's dynamic mode of operation, (controlled by a configuration string presented to the malware module) enables it to attack any payment processing application. This "configuration string" defines the details of how the application hook should be implemented and which payment process should be targeted.

The malware even has a fallback mechanism that could be used where a similar hooking approach is applied to the fundamental mechanism the system uses to move memory contents around. Should a more specific approach be unsuitable, this backup will provide access to the target data.

This siphon module is basically "file-less" in its design. The module is inserted into memory directly from the C2 channel. The siphoned data is also written to a location in memory so it leaves little-or-no footprint on the system to be detected. At the time of this article, none of the antivirus companies seem to have detected this code.

While the original *ModPipe* malware was not attributed to any particular attack group, Foregenix identified similarities comparing *CCSiphon* to the RDFScanner module in the *Boostwrite* malware reported by Mandiant in 2019. That attack was attributed to Fin7, and targeted NCR's Aloha Point of Sale system. Additional research performed by Foregenix suggests that *ModPipe* may have passed unnoticed for a considerable period of time, with similar variants being available on VirusTotal also going back to 2019.

"Attackers are certainly getting more sophisticated", says Chris Hague, Global Manager Digital Forensics & Incident Response at Foregenix. "...This may be a game changer for PCI SSF (formerly PA-DSS) and other security standards.". It was also pointed out that the approach taken by this malware differs significantly from traditional "memory scrapers". The latter generally scan memory on some form of timed cycle, leaving small windows of

opportunity where payment details are “missed” by the malware. With the approach implemented by this variant of *ModPipe* every payment card processed can and would be intercepted by the malware. Coupled with it’s stealthy operation, this could pose a significant risk to retailers.

Foregenix is a cybersecurity company; specializing in Incident Response and Digital Forensics.

Contact: info@foregenix.com.

Research/Authors: Niall Newman and Mark Shelhart
Forensics and Incident Response