VISA Payment Fraud Disruption Technical Analysis

JULY 2016

POSEIDON MALWARE PERSISTENCE MONITORING

Distribution: Visa Merchants, Acquirers

Summary: In March 2016, the PoSeidon (point-of-sale) PoS malware was modified with the incorporation of a persistence monitoring capability. PoSeidon malware now actively monitors the PoS system processes in order to maintain the infection and malware functionality. If the malware is removed from the system, the monitor process waits two (2) minutes and re-infects the system.

1. Threat and Risk Description

PoSeidon malware actively monitors the PoS system processes in order to maintain the infection and malware functionality (this is referred to as the persistence or immortality mechanism).

- The process monitoring functionality works by injecting itself into a new instance of svchost.exe.
- Once the monitoring process is executed, it will then enter into an infinite loop which ensures the malware maintains full functionality on the target system.
- Additionally, to ensure that no other monitor threads are running, it creates a mutex named "WinHostWD".

The monitoring process will check the system32 directory or User Profile directory for the malware executable (WinHost32.exe). The monitoring process will then reach back and check every five (5) seconds for this executable to be present on the system. If the malware cannot find the file after two minutes it will then reinitiate the installation process to infect the target system.

This functionality ensures the persistent reinstallation of the malware on the targeted system as well as the ability to verify that the persistence is maintained with the least possible down time.

2. Best practices, mitigation measures or action required

Check for the monitoring process:

To identify if the monitoring process is running, a search should be done for a process named svchost.exe using the mutex “WinHostWD”.

PoSeidon clean-up and removal:

There are two options for malware clean-up and removal.

1. Rebuild the infected system, making sure to not restore from an infected backup.

2. Follow the normal PoSeidon clean-up procedure, with the additional step of killing the monitoring process identified by the mutex above.

3. Sources

https://www.trustwave.com/Resources/SpiderLabs-Blog/PoSeidon-Completionist/

For information please contact, **paymentintelligence@visa.com**.