STORMSHIELD

MALWARE

POSeidon malware

COMPROMISES POINT OF SALE TERMINALS.

Information

Also known as “FindPOS”.

Created in November 2014 and ever since, several variants have started spreading.

Attack type

Theft of banking data through point-of-sale (POS) terminals

Target

All types of businesses

Risks

Exfiltration of stolen information in order to exploit it (resale, misuse)

Step 1

The malware deploys in the operating system (OS)

Step 2

It creates a registry key so that it is executed each time the POS terminal starts running

Step 3

It records information that has been entered (keylogging)

Step 4

The malware then reads memory from all processes to find banking data

THREATS

THEFT OF BANKING DATA

More information on threats: Thisissecurity.net

PROTECTION OF COMPUTERS

Endpoint Full Protect

THE ONLY SOLUTION THAT PROVIDES PROVEN PROTECTION AGAINST TARGETED ATTACKS AND APTS.

Stormshield Endpoint Security Full Protect offers protection against the creation of executable files

POSeidon is neutralized

Stormshield Endpoint Security Full Protect protects the Windows registry base

The malicious recording of information through the POS terminal is blocked by the keylogging module on Stormshield Endpoint Security Full Protect

Stormshield Endpoint Security Full Protect prevents the malware from being injected into the operating system’s processes

In a few words

The Full Protect product utilizes a unique proactive signature-less technology which protects efficiently against unknown and sophisticated attacks.

Protection from known threats

Protection against the exploitation of vulnerabilities on the operating system

Protection against the exploitation of vulnerabilities on third-party applications

Monitors integrity of the system’s memory

Protection for workstations

Detection of malicious programs through behavioral analysis

Reinforcement of the operating system

Application control (whitelisting or blacklisting)

Granular control over user privileges

Granular control over the exfiltration of sensitive data

Intrusion prevention

Firewall

Network intrusion detection

IMMEDIATE TOTAL PROTECTION

PROACTIVE PROTECTION

More information on the security solution: www.stormshield.eu/endpoint-protection/