APT/MALWARE

Carbanak malware

LARGE-SCALE APT CAMPAIGN TARGETING BANKS.

Step 1
Malware targets banks via spearphishing attack using infected Word document

Step 2
Viral strain gets copied onto the hard disk

Step 3
File is executed

Step 4
Malware injected into legitimate 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

Stromshield Endpoint Full Protect proactively blocks the exploitation of vulnerabilities (CVE-2012-0158 et CVE-2013-3906)
Carbanak malware neutralized

Full Protect offers protection against creation of executable files

Application control module prevents execution thanks to its whitelisting approach

Stormshield Endpoint Full Protect secures access to legitimate processes

More information on threats: Thisissecurity.net