STORMSHIELD

MALWARE

About

Targeted attacks in 2016 and 2017 in the Middle East aimed at destroying data on the infected computer. First instance of Shamoon was in 2012.

Attack type

Malware spreads via credential theft (lateral propagation) within the organization

Target

Some Saudi Arabian Ministries and several engineering and manufacturing companies in the Middle East

Risks

Data destruction, loss of sensitive data, loss of productivity

Shamoon 2 malware

TARGETED ATTACKS IN THE MIDDLE EAST THAT DESTROY DATA ON INFECTED MACHINES

Step 1

Malware copies executable files and driver onto the hard disk.

Step 2

Malware runs executable files.

Step 3

Malware steals credential information and propagates laterally.

Step 4

Data on the hard disk is destroyed.

THREATS

TARGETED ATTACK

More information on threats: Thisissecurity.net

PROTECTION OF COMPUTERS

Endpoint Full Protect

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

Protection against the creation of executable files. The malware is neutralized

The application control module prevents the execution of the program thanks to whitelisting.

Stormshield Endpoint Security is able to block credential theft if the right policy is applied (privilege escalation, application control)

Impossible for data to be destroyed.

In a few words

The Full Protect product utilizes a unique proactive signature-less technology which efficiently protects 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/