STORMSHIELD

Threat advisory

Stormshield Endpoint Security Evolution

Your **company** With Stormshield Endpoint Security Evolution
is protected against ransomware

LockBit 2.0

DATA EXFILTRATION AND ENCRYPTION ON INFECTED MACHINES

LockBit is a group of cyberattackers operating under a Ransomware-as-a-Service (RaaS) model, as a turnkey product.

LockBit offers its ransomware platform to other entities or individuals who use it on an affiliate model.

LockBit is said to be the most active ransomware group, with an impressive list of 203 victims in Q3 2021 alone.

Initial access
Social engineering to gain elevated privileges to encrypt files and demand a ransom.

Target
Businesses of any size without effective protection against ransomware. Especially in the US, Canada and Europe.

Risks
Encryption of data (integrity impact), theft of sensitive information (confidentiality impact), loss of productivity (availability impact), etc.

Find out about our ransomware protection solution

LOCKBIT 2.0

#1

Primary infection

Phase 1

The cyberattacker **gains access to the target company** either by purchasing an exploit from another group, or via his own phishing campaign.

*Stormshield Endpoint Security Evolution gives you **effective protection against various attack techniques** (buffer overflow, packed malware and process hollowing).*

#2

Lateral movement and value search (expansion)

Phase 2

The cyberattacker **infiltrates deep** into the network. They then **move laterally** as they seek to identify the machines containing valuable information.

*Stormshield Endpoint Security Evolution **detects and neutralises discovery operations** (e.g. running commands to obtain IP addresses, user accounts, DNS servers, network shares, etc.).*

#3

Impact

Phase 3

Exfiltration of data to the LockBit Group infrastructure

*Stormshield Endpoint Security Evolution **blocks access to sensitive files** such as passwords, private keys, digital vaults, credentials, etc.*

Encryption of files and publication of a ransom note

***This step is never performed.** Stormshield Endpoint Security Evolution neutralizes malware that behaves like ransomware, avoiding data encryption.*

Destruction of Shadow Copies restore points

*It **detects and blocks Shadow Copy tampering attempts**, stopping ransomware from running.*