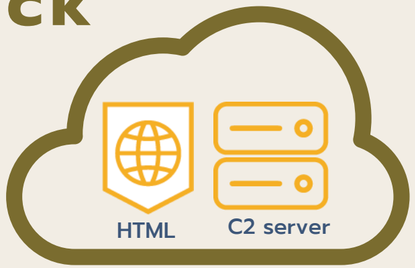
Emotet Lifecycle Attack & Protection



MAED prevents the Powershell command from reaching malicious sites to download file that leverages Emotet.

MAED prevents the download of Emotet from malicious sites and further leverages that may be attempted after, due to Emotet being a part of a MaaS (Malware as a Service) scheme.

KEY

SNPR
Secure Network Perimeter Response

SCUD
Secure cloud Unified Defense

MAED
Managed Advanced Endpoint Protection

01

If SCUD security engines are enabled the file will be contained and prevented.

SCUD

MAED

MAED prevents the malicious PowerShell in the file from executing.

The infected file is commonly delivered by email and other collaboration apps. The attack lifecycle begins here whenever a malicious document is clicked on or a file embedded with macros is enabled.

02

When enabling Macros the malicious files will auto execute PowerShell commands connecting to malicious sites.

03

MAED

SNPR

If the links are on a threat intelligence blacklist the firewall will block it, zero-day file sandboxing can prevent malicious files.

The Powershell commands reach out to the attacker's C2 servers or malicious sites for the download of Emotet and further attacks.

04

MAED

SNPR

SNPR will detect command and control traffic, and stop the transaction.

Emotet is then downloaded and utilizes other ransomware and malware to leverage further attacks.

BLOKWORX