Emotet Malware

Emotet Malware is back

https://en.wikipedia.org/wiki/Emotet
CVEs: n/a

An Emotet spam campaigns is at large being distributed as an attached Excel document.

Background

The EuroPol has considered Emotet as one of the world's most dangerous malware. It was first discovered on year 2014 as a Banking Trojan. That malware was last seen for almost a year. This report focusses specifically on the Emotet malware protection and IOC detections by the Security Fabric products. ..

Announced

https://threatpost.com/emotet-resurfaces-trickbot/176362/

https://www.securityweek.com/emotet-using-trickbot-get-back-game

https://thehackernews.com/2021/11/notorious-emotet-botnet-makes-comeback.html

https://www.darkreading.com/threat-intelligence/emotet-returns

https://www.bleepingcomputer.com/news/security/here-are-the-new-emotet-spam-campaigns-hitting-mailboxes-worldwide/

Latest Developments

On November 16, 2021, hundreds of Malware samples were flagged as VB/Dloader.BLG!tr. At the same day, several security news article were published..

Fortinet Products Summary

Services	Version	Other Info
FortiGate		
AV	*89.06927*	FortiGuard AV detects the Emotet payload
FortiClient		
AV	*89.06927*	FortiGuard AV detects the Emotet payload
FortiEDR		
AV (Pre-Filter)	*89.06927*	FortiGuard AV detects the Emotet payload
FortiSandbox		
AV (Pre-Filter)	*89.06927*	FortiGuard AV detects the Emotet payload
	3.2+	FortiSandbox detects malware as medium risk.
FortiAI		
AV (Pre-Filter)	*89.06927*	FortiGuard AV detects the Emotet payload
FortiMail		
AV	*89.06927*	FortiGuard AV detects the Emotet payload
FortiCASB		
AV	*89.06927*	FortiGuard AV detects the Emotet payload
FortiCWP		
AV	*89.06927*	FortiGuard AV detects the Emotet payload
FortiADC		
AV	*89.06927*	FortiGuard AV detects the Emotet payload
FortiProxy		
AV	*89.06927*	FortiGuard AV detects the Emotet payload
FortiAnalyzer		
	6.4+	Detects indicators attributed to Emotet from Fabric products
FortiSIEM		
	6.2+	Detects indicators attributed to Emotet from Fabric products and 3rd party products

Cyber Kill Chain

Reconnaissance

Weaponization

Delivery

FortiGate
AV
Version Info: 89.06927
Link: https://www.fortiguard.com/encyclopedia/virus/10068309

FortiClient
AV
Version Info: 89.06927
Link: https://www.fortiguard.com/encyclopedia/virus/10068309

FortiEDR
AV (Pre-Filter)
Version Info: 89.06927
Link: https://www.fortiguard.com/encyclopedia/virus/10068309

FortiSandbox
AV (Pre-Filter)
Version Info: 89.06927
Link: https://www.fortiguard.com/encyclopedia/virus/10068309

FortiAI
AV (Pre-Filter)
Version Info: 89.06927
Link: https://www.fortiguard.com/encyclopedia/virus/10068309

FortiMail
AV
Version Info: 89.06927
Link: https://www.fortiguard.com/encyclopedia/virus/10068309

FortiCASB
AV
Version Info: 89.06927
Link: https://www.fortiguard.com/encyclopedia/virus/10068309

FortiCWP
AV
Version Info: 89.06927
Link: https://www.fortiguard.com/encyclopedia/virus/10068309

FortiADC
AV
Version Info: 89.06927
Link: https://www.fortiguard.com/encyclopedia/virus/10068309

FortiProxy
AV
Version Info: 89.06927
Link: https://www.fortiguard.com/encyclopedia/virus/10068309

Exploitation

Installation

C2

Action

Endpoint

Incident Response (Security Operations)

To help customers identify and protect vulnerable, FortiAnalyzer, FortiSIEM and FortiSOAR updates are available to raise alerts and escalate to incident response:

Analyzer / SIEM / SOAR Threat Hunting & Playbooks