DearCry Ransomware

Targeting the MS Exchange Exploit

https://twitter.com/MsftSecIntel/status/1370236539427459076

Following initial compromise of the MS Exchange system, the attacker can execute the primary objective. From monitoring these incidents, a new family of ransomware has been detected. The threat is known as DoejoCrypt or DearCry.

Background

Earliest detection of the MS Exchange vulnerability is covered in the MS Exchange Outbreak report.

Announced

On March 11, Microsoft released the following announcement referring to the ransomware:

https://twitter.com/MsftSecIntel/status/1370236539427459076

Latest Developments

Refer to the FortiGuard Labs released the Threat Signal report:

https://www.fortiguard.com/threat-signal-report/3885/observed-in-the-wild-campaigns-leveraging-recent-microsoft-exchange-server-vulnerabilities-to-install-doejocrypt-dearcry-ransomware

Fortinet Products Summary

	Services	Version	Other Info
FortiGate	**AV**	*84.00634*	NGAV Detects & Blocks malware file transfers
FortiClient	**AV**	*84.00634*	FortiClient AV real-time protection blocks ransomware file
	Anti-Ransomware	*6.4.3*	FortiClient Anti-ransomware blocks suspicious process behaviour that matches ransomware activity.
FortiEDR	**EDR**	*4.0 - 5.0*	Default FortiEDR and FortiXDR deployments detect and block DoejoCrypt/DearCry ransomware activity out of the box.
FortiSandbox	**AV (Pre-Filter)**	*84.00634*	Detected by FortiSandbox pre-filter, as this is a known malware.
	Behavior Detection	*3.2 - 4.0*	Pre-existing behaviour detection of the ransomware behaviours (launching files, visible windows, etc.).
FortiAI	**AV (Pre-Filter)**	*84.00634*	Detected by FortiSandbox pre-filter, as this is a known malware.
	ANN	*1.066*	FortiAI detects the sample as Ransomware, please see FortiAI VSA.
FortiDeceptor	**Lure**	*3*	A Deception Decoy that acts as a file server will detect the ransomware while encrypting the fake network drive share on the infected endpoint.
	Decoy VM	*3*	A Deception Decoy that acts as a file server will detect the ransomware while encrypting the fake network drive share on the infected endpoint.
FortiMail	**AV**	*84.00634*	Detected by pre-filter or scan engines, as this is a known ransomware.
FortiCASB	**AV**	*84.00634*	Detected by pre-filter or scan engines, as this is a known ransomware.
FortiCWP	**AV**	*84.00634*	Detected by pre-filter or scan engines, as this is a known ransomware.
FortiAnalyzer	**Event Handlers & Reports**	*6.2 - 7.0*	Detects indicators attributed to DearCry from across the Security Fabric products
FortiSIEM	**Rules & Reports**	*5.0 - 6.0*	Detects indicators attributed to DearCry from across the Security Fabric products & 3rd party devices.

Cyber Kill Chain

Reconnaissance

Weaponization

Delivery

FortiGate
AV
Version Info: 84.00634
Link: https://www.fortiguard.com/encyclopedia/virus/100096650/w32-dearcry-oge-tr-ransom

FortiClient
AV
Version Info: 84.00634
Link: https://www.fortiguard.com/encyclopedia/virus/100096650/w32-dearcry-oge-tr-ransom

FortiSandbox
AV (Pre-Filter)
Version Info: 84.00634
Link: https://www.fortiguard.com/encyclopedia/virus/100096650/w32-dearcry-oge-tr-ransom

Behavior Detection
Version Info: 3.2 - 4.0
Link: https://www.fortiguard.com/encyclopedia/virus/100096650/w32-dearcry-oge-tr-ransom

FortiAI
AV (Pre-Filter)
Version Info: 84.00634
Link: https://www.fortiguard.com/encyclopedia/virus/100096650/w32-dearcry-oge-tr-ransom

ANN
Version Info: 1.066
Link: https://filestore.fortinet.com/fortiguard/downloads/FortiAI_dearCry_c6eeb1448f5d993f4e30fb79f3a5751f8c.pdf

FortiMail
AV
Version Info: 84.00634
Link: https://www.fortiguard.com/encyclopedia/virus/100096650/w32-dearcry-oge-tr-ransom

FortiCASB
AV
Version Info: 84.00634
Link: https://www.fortiguard.com/encyclopedia/virus/100096650/w32-dearcry-oge-tr-ransom

FortiCWP
AV
Version Info: 84.00634
Link: https://www.fortiguard.com/encyclopedia/virus/100096650/w32-dearcry-oge-tr-ransom

Exploitation

Installation

FortiClient
Anti-Ransomware
Version Info: 6.4.3
Link: https://kb.fortinet.com/kb/microsites/microsite.do?cmd=displayKC&docType=kc&externalId=FDS1766

FortiEDR
EDR
Version Info: 4.0 - 5.0
Link: https://kb.fortinet.com/kb/microsites/microsite.do?cmd=displayKC&docType=kc&externalId=FDS1764

FortiDeceptor
Lure
Version Info: 3
Link: https://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FDS2010

Decoy VM
Version Info: 3
Link: https://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FDS2010

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

FortiAnalyzer
Event Handlers & Reports
Version Info: 6.2 - 7.0
Link: https://kb.fortinet.com/kb/microsites/microsite.do?cmd=displayKC&docType=kc&externalId=FDS1762

FortiSIEM
Rules & Reports
Version Info: 5.0 - 6.0
Link: https://kb.fortinet.com/kb/microsites/microsite.do?cmd=displayKC&docType=kc&externalId=FDS1777