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.

January 6, 2021 — Earliest Vulnerability Detection

Earliest detection of the MS Exchange vulnerability is covered in the Outbreak report:
https://fndn.fortinet.net/FortiGuard-Alert-Outbreaks/Hafnium-full/

March 11, 2021 — MSFT Annoucement

On March 11, Microsoft released the following announcement referring to the ransomware:
https://twitter.com/MsftSecIntel/status/1370236539427459076

March 12, 2021 — Latest Developments

*FortiGuard Labs released the **Threat Signal** report:*
https://www.fortiguard.com/threat-signal-report/3685/observed-in-the-wild-campaigns-leveraging-recent-microsoft-exchange-server-vulnerabilities-to-install-doejocrypt-dearcry-ransomware

Fortinet Products Summary	Services	Version	Other info
FortiGate NGFW	Anti-Virus	*84.00634*	NGAV Detects & Blocks malware file transfers
FortiClient	Anti-Virus	*84.00634*	FortiClient AV real-time protection blocks ransomware file
	Anti-Ransomware	*6.4*	Detects & defuses the ransomware based on suspicious process behaviour.
FortiEDR	EDR	*SaaS*	Existing behaviour detection & blocking of DoejoCrypt/DearCry ransomware activity out of the box.
FortiSandbox	Sandboxing	*3.x*	Existing behaviour detection of the ransomware (launching files, visible windows, etc.).
	Pre-filter	*84.00634*	Detected by pre-filter or scan engines, as this is a known ransomware.
FortiAI	ANN	*1.066*	FortiAI detects the sample as Ransomware, please see FortiAI VSA.
FortiMail FortiCASB FortiCWP	Anti-Virus	*84.00634*	Detected by pre-filter or scan engines, as this is a known ransomware.
FortiDeceptor	Decoy	*3.x*	A Deception Decoy that acts as a file server will detect the ransomware while encrypting the fake network drive share on the infected endpoint.
FortiAnalyzer	Event Handler Threat Hunting Report	*6.2, 6.4*	Detects indicators attributed to DearCry from Fabric products.
FortiSIEM	Rules & Threat Hunting Report	*5.x, 6.x*	Detects indicators attributed to DearCry from Fabric products and 3rd parties.

Cyber Kill Chain

Reconnaissance

Weaponization

Delivery

FortiGuard Anti-Malware Protection

FortiGate
FortiClient
FortiEDR
FortiMail
FortiSandbox
FortiAI
FortiCASB
FortiCWP
Version Info: 84.00634
Link: https://www.fortiguard.com/encyclopedia/virus/10009650/w32-dearcry-oge-tr-ransom

FortiSandbox

Behavior Detection
Version Info: 3.2
Link: https://filestore.fortinet.com/fortiguard/downloads/FortiSandbox_DearCry_Behaviour_Report.pdf
Other Info: FortiSandbox detects the ransomware behaviours of this malware, including (1) The file tries to launch the original file, and (2) The executable had visible window(s).

FortiAI

Artificial Neural Networks (ANN)
Version Info: 1.066
Link: https://filestore.fortinet.com/fortiguard/downloads/FortiAI_dearCry_c6eeb14485d93f4e30fb79f3a57518fc.pdf
Other Info: FortiAI detects as Ransomware, please see FortiAI VSA.

Exploitation

Installation

FortiEDR

Behavior Detection
Version Info: SaaS
Link: https://kb.fortinet.com/kb/microsites/microsite.do?cmd=displayKC&docType=kc&externalId=FD51764
Other Info: Default FortiEDR and FortiXDR deployments detect and block DoejoCrypt/DearCry ransomware activity out of the box.

FortiClient

Anti-Ransomware
Version Info: 6.4.3
Link: https://kb.fortinet.com/kb/microsites/microsite.do?cmd=displayKC&docType=kc&externalId=FD51766
Other Info: FortiClient Anti-ransomware engine identifies and defuses DearCry ransomware.

FortiDeceptor

Deception Lure (SMB) + Deception Decoy (file server)
Version Info: 3.x
Link: https://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FD52010
Other Info: A Deception Decoy that acts as a file server will detect the ransomware while encrypting the fake network drive share on the infected endpoint.

C2

Action

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

FortiAnalyzer Event Hanlders & Reports
Version Info: 6.2, 6.4
Link: https://kb.fortinet.com/kb/microsites/microsite.do?cmd=displayKC&docType=kc&externalId=FD51762
Other Info: Detects indicators attributed to DearCry from across the Security Fabric products.

FortiSIEM Rules & Reports

SIEM Rules & Reports