SOLUTION BRIEF

Reduce the Risk of Ransomware Incidents With Fortinet

Executive Summary

Today's enterprises have a lot going on. And the result is that organizations are more exposed to cyberattacks like ransomware than ever. Ongoing digital transformation, the quick switch from office to anywhere work, the acceleration of application and service delivery from the cloud, the diversity of connectivity on and off the corporate network and more, expand the attack surface. And while ransomware continues to enter organizations by email, it increasingly gains access via Remote Desktop Protocol (RDP) and vulnerability exploits.

Along with risk exposure, business impacts and consequences are growing. As the FBI noted in the Cyber Summit session, "Trends and Predictions in Ransomware," there has been an explosion in ransomware, with demands reaching the millions.[1] It is essential that organizations put the right mix of security controls in place (to balance acceptable risk with cost and effort) across the Cyber Kill Chain of these campaigns. Fortinet offers the broadest set of security products, services, and training to reduce the risk of a ransomware incident at multiple stages of that Cyber Kill Chain, before cyber criminals achieve their ultimate goal.

Ransomware activity jumped 7x from the start of the half to the end of 2020.[2]

Key Security Controls for Each Stage of Attack

In most respects, cyber criminals have the advantage. All they need is one target to bite to be on their way to reap rewards. But organizations do have the benefit of thwarting each campaign at any of its multiple attack stages to remain safe. This is why the Cyber Kill Chain concept remains a powerful cybersecurity strategy, especially in regard to ransomware.

Delivery Stage

Given that the majority of today's ransomware is typically delivered via email, followed by the web, strong threat prevention, detection, and response provided via a secure email gateway and next-generation firewall (NGFW) are key.

Fortinet FortiMail secure email gateway

FortiMail is a top-rated secure email gateway that stops volume-based and targeted cyber threats, prevents the loss of sensitive data, and helps maintain regulatory compliance. Of note, capabilities like click protection provide up-to-the-minute reputation checking for embedded URLs, while content disarm and reconstruction thwart malicious code embedded in attachments. Further, sandbox analysis can analyze both attached files and embedded URLs in an instrumented virtual environment. All of these capabilities can be enabled inline before emails are delivered, to protect end-users from messages designed to fool them into granting ransomware access to their system.

FortiGate next-generation firewall

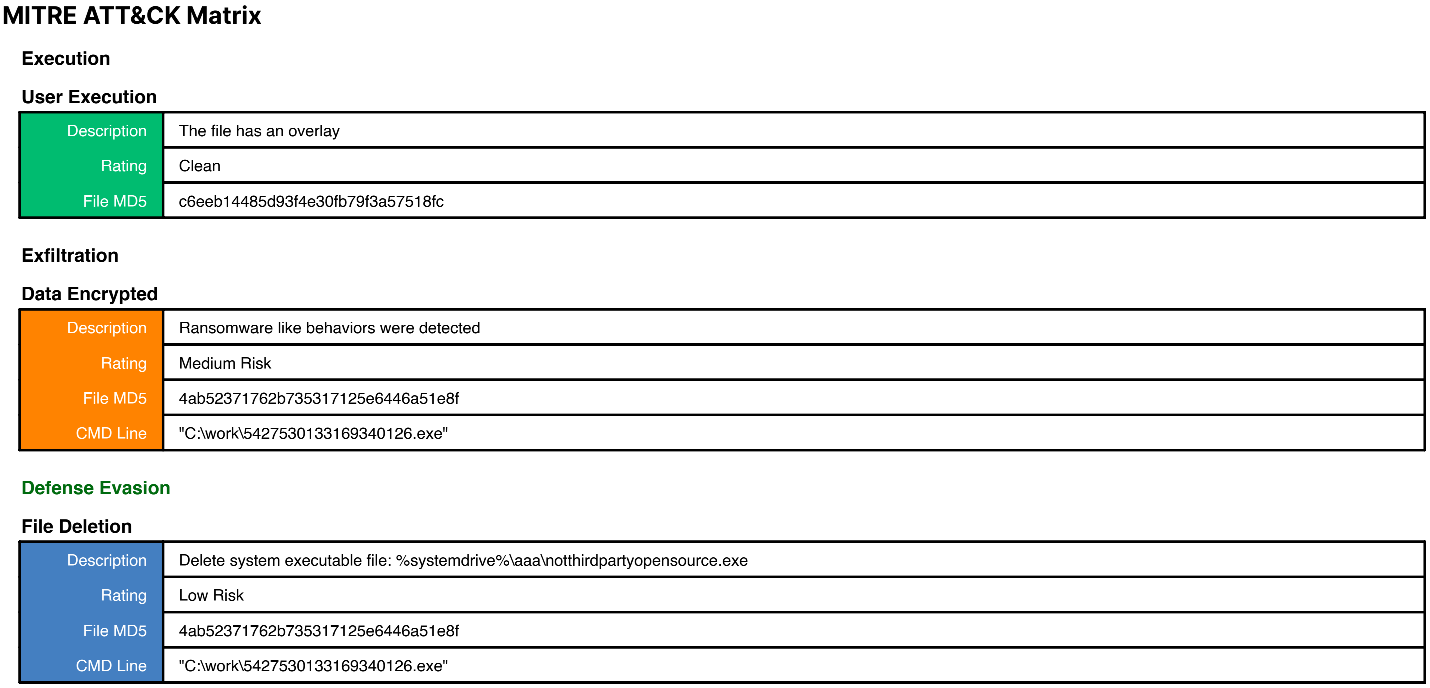
FortiGate NGFWs consolidate industry-leading security capabilities such as secure sockets layer (SSL) inspection including the latest TLS 1.3, web filtering, and intrusion prevention system (IPS) to provide full visibility and protect any network edge. With consistently top-rated security services from FortiGuard Labs, and integrating the dedicated advanced threat protection of FortiSandbox and FortiAI, FortiGates reduce the risk of ransomware delivered via the web.

FortiWeb web application firewall, FortiCASB cloud access security broker, and FortiCWP cloud workload protection

Fortinet offers a range of ransomware detection and protection capabilities for web applications, cloud services, and cloud infrastructure. Notably, sandboxing is also an integrated capability to identify and thwart the latest attacks.

FortiSandbox advanced threat protection

Top-rated FortiSandbox provides both automated analysis of files and URLs in an instrumented virtual runtime environment and static artificial intelligence (AI)-based inspection to address the rapidly evolving and more targeted threats. These include ransomware, cryptomalware, and others across a broad digital attack surface. Specifically, it classifies previously unknown attack components and delivers real-time actionable intelligence as an integrated component of Fortinet and third-party security infrastructures.



MITRE ATT&CK Matrix

Execution

User Execution

Description	The file has an overlay
Rating	Clean
File MD5	c6eeb14485d93f4e30fb79f3a57518fc

Exfiltration

Data Encrypted

Description	Ransomware like behaviors were detected
Rating	Medium Risk
File MD5	4ab52371762b735317125e6446a51e8f
CMD Line	"C:\work\5427530133169340126.exe"

Defense Evasion

File Deletion

Description	Delete system executable file: %systemdrive%\aaa\notthirdpartyopensource.exe
Rating	Low Risk
File MD5	4ab52371762b735317125e6446a51e8f
CMD Line	"C:\work\5427530133169340126.exe"

Figure 1: FortiSandbox scan job report in the MITRE ATT&CK Matrix.

FortiAI Virtual Security Analyst

FortiAI is the first solution of its kind that embeds a sophisticated and mature deep learning model via deep neural networks (DNN). Its patent-pending DNN approach learns about new threats by itself and helps organizations adapt threat protection to new attacks instantaneously. In addition, FortiAI comes pre-trained with more than 6 million malware features. These can identify IT- and OT-based threats and classify them into malware categories, including ransomware. These features can also accurately pinpoint patient zero and lateral spread of a malware and its variants by analyzing the entire threat movement.

Exploitation/Installation Stage

Even the strongest preventive security controls applied to delivery vectors can be bypassed by cyber criminals, especially in light of sophisticated techniques like exploitation of zero-day vulnerabilities and compromise of authorized supply chains. That's why robust endpoint security is also required.

FortiEDR endpoint protection platform

FortiEDR is a cloud-native unified endpoint security solution that combines behavior-based pre-execution and post-execution protection with ongoing detection and response for devices of all kinds. FortiEDR is arguably the most important security control to combat ransomware given technology effectiveness and deployment on the devices ransomware tries to lock. Patented code tracing enables deep insight into system activity, as well as granular options to block and even roll back malicious activity such as the encryption of files by ransomware.

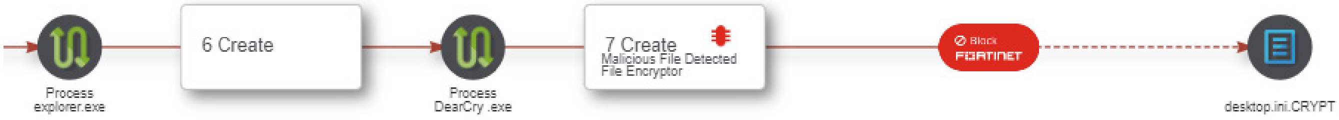


Figure 2: FortiEDR post-execution blocking process flow.

FortiClient Fabric Agent

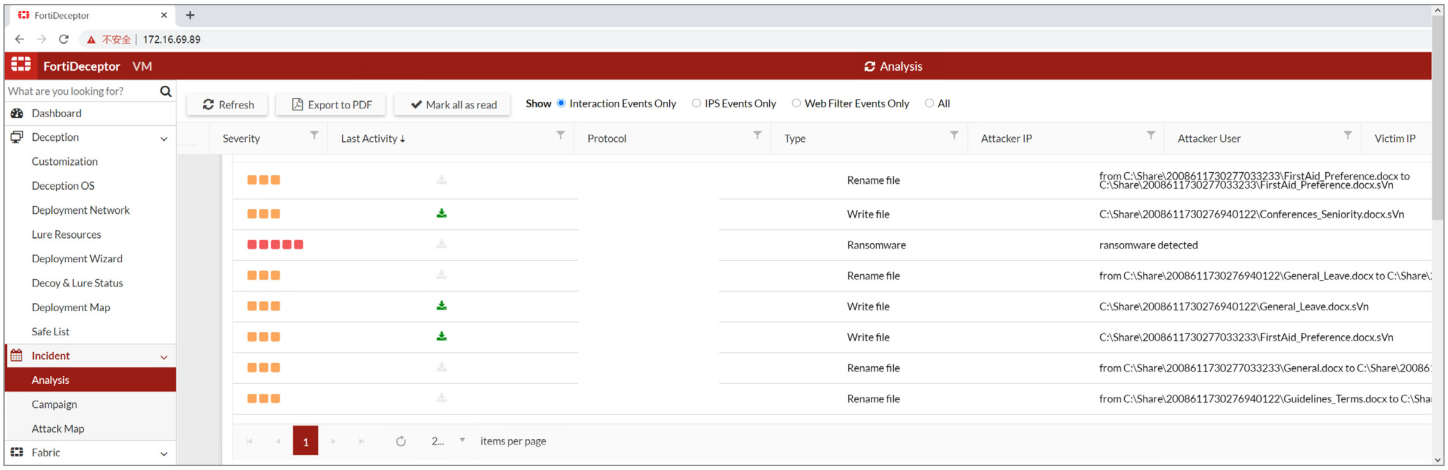
Among other capabilities, FortiClient provides important visibility about device configuration, as well as vulnerability management to reduce the endpoint attack surface. Integration with FortiSandbox also enables the detection of previously unknown malware.

Action on Objectives Stage

While many of the above controls like FortiGate, FortiEDR, and FortiAI are also able to contain attempts of ransomware to move laterally, there is an innovative use case for deception at this stage as well.

FortiDeceptor deception-based breach protection

FortiDeceptor is a deception-based technology intended to deceive, expose, and eliminate both external and internal threats before any significant damage is done. It creates a network of decoy virtual machines (VMs) that appear ripe for attack. FortiDeceptor then analyzes any threat activity and shares information via the Fortinet Security Fabric across all security components to protect the entire network. In the case of ransomware, FortiDeceptor infrastructure is smart enough to engage the ransomware code as it seeks to move laterally, slowing it down long enough for containment intelligence to be shared with the rest of the Fortinet Security Fabric.



Show ● Interaction Events Only ○ IPS Events Only ○ Web Filter Events Only ○ All

Severity	Last Activity ↓	Protocol	Type	Attacker IP	Attacker User	Victim IP
🟧🟧🟧			Rename file	from C:\Share\20086117302770332333\FirstAid_Preference.docx to C:\Share\20086117302770332333\FirstAid_Preference.docx.sVn		
🟧🟧🟧	⬇		Write file	C:\Share\2008611730276940122\Conferences_Seniority.docx.sVn		
🟥🟥🟥🟥🟥			Ransomware	ransomware detected		
🟧🟧🟧			Rename file	from C:\Share\2008611730276940122\General_Leave.docx to C:\Share\		
🟧🟧🟧	⬇		Write file	C:\Share\2008611730276940122\General_Leave.docx.sVn		
🟧🟧🟧	⬇		Write file	C:\Share\2008611730277033233\FirstAid_Preference.docx.sVn		
🟧🟧🟧			Rename file	from C:\Share\2008611730277033233\General.docx to C:\Share\20086		
🟧🟧🟧			Rename file	from C:\Share\2008611730276940122\Guidelines_Terms.docx to C:\Sha		

1 · 2... items per page

Figure 3: FortiDeceptor detecting ransonmware engaging its activity.

FortiAnalyzer fabric analytics and FortSIEM security information and event management

Both FortiAnalyzer and FortiSIEM collect telemetry from across the Fortinet Security Fabric, giving security teams insight into potential ransomware activity throughout the organization. Both are also able to ingest threat feeds from FortiGuard Labs and other sources to identify indicators of compromise (IOCs) associated with various ransomware campaigns.

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

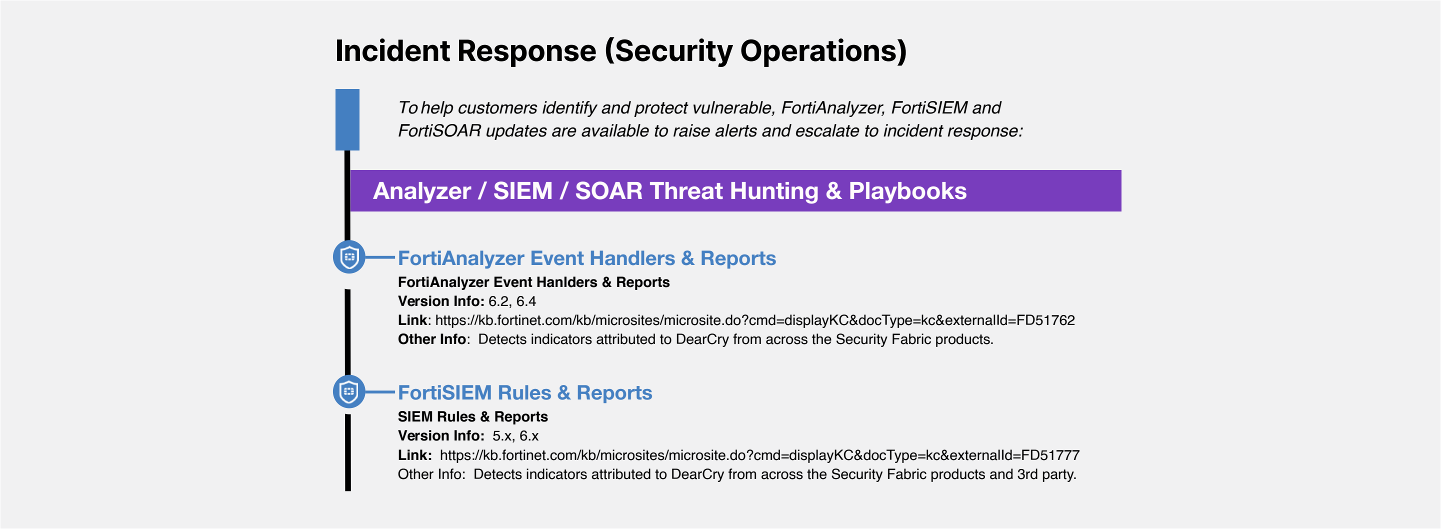
Anti-Ransomware
Version Info: 6.4.3
Link: https://kb.fortinet.com/kb/microsites/microsite.do?cmd=displayKC&docType=kc&externalId=FD51766
Other Info: FortiClient Anti-ransomware engine identifies and defuses DearCry ransomware.

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
Version Info: 5.x, 6.x
Link: https://kb.fortinet.com/kb/microsites/microsite.do?cmd=displayKC&docType=kc&externalId=FD51777
Other Info: Detects indicators attributed to DearCry from across the Security Fabric products and 3rd party.

Figure 4: DearCry’s mapping technologies to Cyber Kill Chain.

Staff Augmentation

In addition to the security controls above, Fortinet offers a range of information and expert resources from both trusted partners and FortiGuard Labs. These resources include our weekly threat intelligence newsletter, ad hoc Outbreak Alerts, and more, to help keep organizations abreast of the latest ransomware campaigns.

Managed detection and response services to supplement an organization’s in-house staff, skills, and tools are also available. Plus, incident response professionals are on-call to help contain incidents in progress.

It’s Time to Thoroughly Prepare for Ransomware

Tracking global activity over time makes it clear that ransomware is going to continue to be more prevalent and more difficult to stop. Fortinet has technologies to address ransomware at multiple attack stages, in addition to security awareness training, staff augmentation, and other services.

Organizations should assess their current strength of security, concern about exposure, and best solution fit at each stage of the Cyber Kill Chain. This should complement broader efforts to prepare for potential ransomware incidents such as:

- Segmenting the network
- Hardening devices
- Establishing and testing backups
- Determining monitoring and response processes
- Augmenting in-house technologies, tools, and processes with expert outsourced services

[1] Jonathan Holmes, et al., “Cyber Summit 2020: Trends and Predictions in Ransomware,” Federal Bureau of Investigation, 2020.

[2] “Global Threat Landscape Report: A Semiannual Report by FortiGuard Labs,” Fortinet, February 2021.

May 1, 2021 6:59 AM

D:\Fortinet\2021 Rebranded templates\Solution Briefs\April\Refresh\Ransomware\sb-FA-reduce-the-risk-of-ransomware-4302021\sb-FA-reduce-the-risk-of-ransomware-4302021

996100-0-0-EN