SOLUTION BRIEF

Ransomware: How Fortinet Helps Prevent the Most Irritating Yet Effective Malware

Executive Overview

With 71% of ransomware attacks targeting small-to-medium sized businesses (SMBs),[1] it continues to be the prevailing form of malware used by attackers to disrupt organizations. The rapid adoption of new digital innovations often introduces new security gaps and makes it easier for attacks to spread across the flat and open internal network. For many, the loss of critical business cycles and revenues from systems that have ground to a halt far outweighs the price of the ransom itself. The Fortinet Security Fabric provides comprehensive network security and advanced threat-intelligence sharing to help SMBs detect and protect against ransomware attacks.

Do not be fooled by scareware and other social engineering scams

Scareware attempts to trick a user into believing their device has been compromised. There are two main ways this is traditionally accomplished using pop-up displays and soliciting payment for removal or blackmail:

1. Stating the device is infected with malware
2. Stating the device has or is being used for an illegal act, such as part of a botnet or child pornography

How Ransomware Gets In

The pressing need for speed and agility across business's of all sizes has led to the rapid adoption of innovations (e.g., cloud-based tools, Software-as-a-Service [Saas], smart devices) that bring convenience along with complexity—quickly creating vulnerabilities and making it easier for even basic threats to get past outdated defenses at various points of entry.

Ransomware-as-a-Service (RaaS) that enables attackers to merely invest in an attack carried out by others and the natural IT knowledge of younger generations have made it easier for low-level hackers to easily blast a wide target base and expose one of those holes and is one reason that has led to such high rates of SMBs being hit with ransomware.

Email Vulnerabilities

Email is the primary way that ransomware gets inside a business's network. Many users still unintentionally open a malicious attachment or URL that slips by consumer-grade email filters. More often these days, attackers rely on social engineering and business email compromise (BEC) scams where users unknowingly give attackers the information they seek to set off a series of events—like getting the victim's phone number and replicating known sites to obtain user credentials. For SMBs that often rely on consumer-based email solutions that lack advanced email security checks, recognizing threats and avoiding social engineering schemes rely on a user's individual judgment to identify the threat and avoid infection.

Exposed Ports and Default or Weak Passwords

With so much to do and the security implications of new technologies not being fully understood before implementation, it is common for organizations to simply forget or be unaware of potential security holes. Remote Desktop Protocol (RDP) is often used as an initial entry point for attackers. RDP is used by IT staff to troubleshoot problems with an employee's device via remote control, but that same remote access can be exploited by attackers without the proper protections in place. By detecting public-facing ports, attackers can use brute-force tactics and stolen credentials to gain entry into an organization's systems and ultimately inject their malware. For SMBs, this is even more of a risk as they adopt new technologies (such as smart devices and cloud-based applications) without dedicated staff resources and tools to ensure proper visibility and control of everything on the network.

Malicious URLs

Accidentally going to a website that has been hacked or that has been falsely replicated offers attackers a variety of tactics to infect unknowing users. They can scan the user's machine for application vulnerabilities and inject code directly via drive-by download, or they can capture credentials and other information for later use. Hackers are able to control these sites by exploiting application vulnerabilities in the website itself and copy the look, feel, and interaction—otherwise known as "spoofing" the site. Users believe they are inputting information into a valid site interface while unsuspectingly sending information straight to their attackers. Often, users accidentally end up on these sites through mobile devices that are used for both work and personal use—clicking on links embedded in social media and unknowingly exposing themselves and their organization at the same time.

Challenges with Resetting to a Point Before the Attack

Perhaps the most common way of dealing with a ransomware attack is acknowledging that—despite best efforts—attackers have the advantage. Thanks to business system integrations, the smallest hole in outdated security defenses (ones that lack effective network segmentation controls inside the network) can result in an organizationwide infection.

The only remedy to an effective ransomware attack, other than making the payoff and hoping to receive decryption codes, is to restore the business's systems to a state prior to the attack. However, a number of factors should be checked:

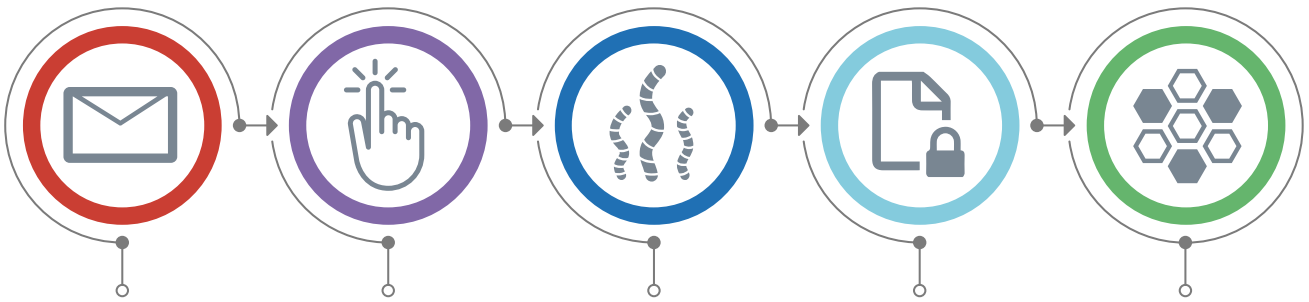
- When was the last time backup and recovery was tested to ensure it worked as planned?
- Have new systems and information been added to the backup process and tested accordingly?
- How long does it take to restore information and is this an affordable delay?

Despite these checks, restoring back to a prior "safe point" does not fix how the attack was initially successful. Also, if users have file synchronization turned on, encrypted files are automatically copied to SaaS clouds, and more advanced ransomware (such as the recent SamSam and Ryuk attacks) makes a point to delete shadow volumes and backup files—even in the cloud—to prevent recovery efforts.

Was It Only Ransomware?

If ransomware was introduced into the network, then attackers gained access. While ransomware may have been the primary motive, other nefarious tools—such as monitoring software, command-and-control (C&C) code, or assimilation into botnets—may have also been introduced to launch additional attacks or siphon data at a later date. Therefore, any ransomware-compromised business must do further investigation into logs and systems for full and effective remediation.

How Ransomware Attacks



Step 01

Email

Given the volume of email, even a small percent of evasion translates to malicious email getting through to users

Step 02

User Clicks and Attack Begins

Without URL filtering to prevent users going to malicious sites or proper endpoint protection to prevent malicious file detection and execution, an attack is unsuspectingly launched

Step 03

Worms Network

Without anomaly or heuristic detection and prevention, attack hunts for key data, folders and disables backup and recovery mechanisms

Step 04

Command & Control and Encrypts

When ready, establishes command and control to communicate back to the attacker and encrypts files

Step 05

Lateral Movement

Without segmentation in place to isolate systems, encryption spreads laterally and hunts for other connected networks

Ransomware Prevention and Remediation: Fortinet Security Fabric

The Fortinet Security Fabric enables organizations to stop known and unknown ransomware across their environment through automated sharing of actionable intelligence.

Phishing—FortiMail

FortiMail brings powerful antispam and anti-malware capabilities. These are complemented by advanced techniques like outbreak protection, content disarm and reconstruction, sandbox analysis, and impersonation detection to stop unwanted bulk email, ransomware, phishing, business email compromise, and targeted attacks.

Malicious URLs—FortiGuard Web Filtering

The FortiGuard Web Filtering Service enhances the core web filtering capabilities of FortiGate next-generation firewalls (NGFWs) by sorting billions of webpages into a wide range of categories that users can allow or block. It includes over 45 million individual ratings of websites that apply to more than 2 billion pages.

Endpoint Execution—FortiEDR

FortiEDR real time endpoint security solutions proactively reduces the attack surface, and protects endpoint devices using machine learning anti-malware and behavior-based detection technology.

Lateral Movement—FortiGate Intent-based Segmentation

Fortinet intent-based segmentation provides end-to-end protection across the network. It intelligently segments network and infrastructure assets, whether on-premises or across multiple clouds. Policy-based access controls continuously monitor the trust level of users and devices to keep sensitive data and assets safe. Analytics and automation capabilities ensure quick detection and neutralization of threats.

Recover and Reset—Fabric-Ready Integration

Fortinet's Open Fabric Ecosystem was designed to connect traditionally disparate security solutions into an integrated framework. This enables evolving IT infrastructures to stay connected across the entire organization, share information in real time, and defend against a rapidly changing attack surface. Fabric-Ready Partners (such as Rubrik and BackBox) offer organizations quick recovery of lost data and device configurations to ensure minimal downtime with little to no integration effort.

Detection and Response

FortiEDR delivers threat protection both pre- and post-infection in real time. It detects and defuses potential threats in real time to stop breaches and prevents ransomware damage. It automates response and remediation procedures with customizable playbooks.

Helping SMBs Put Ransomware in Its Place

As long as smaller businesses present an easy target for cyber criminals, the threat of ransomware will not go away on its own. The Fortinet Security Fabric architecture offers SMBs advanced capabilities and threat-intelligence sharing to help them prevent, detect, and remediate ransomware and other sophisticated modes of attack.

[1] "Beazley Breach Briefing – 2019," Beazley, March 21, 2019.

FORTINET

www.fortinet.com

February 27, 2020 9:00 AM

608059-0-0-EN

Mac:Users:susiehwang:Desktop:Egnyte:Egnyte:Shared:Creative Services:Team:Susie-Hwang:Egnyte:Shared:CREATIVE SERVICES:Team:Susie-Hwang:2020:SB-Ransomware-SMB:sb-ransomware-smb-022720-900am