SentinelOne eBook

SentinelOne® INFO EXCHANGE

7 Common Ways Ransomware Can Infect Your Organization

Table of Contents

Introduction

Understanding how ransomware infects a device and spreads across a network is crucial to ensuring that your organization does not become the next victim of an attack.

As recent trends have shown, the danger of losing access to your data, devices and services is compounded by threat actors that are now exfiltrating data and threatening to leak it on public sites if victims don't pay up. Ransomware operators have become wise to the threat to their business model from their own success: increased public attention of the ransomware threat has pushed (at least some) businesses to invest in backup and recovery. But those techniques become redundant when the perpetrators are holding your most sensitive customer and corporate data over your head.

Post infection, ransomware can spread to other machines or encrypt shared filers in the organization's network. In some cases, it can spread across organizational boundaries to infect supply chains, customers and other organizations, and indeed, some malware campaigns have specifically targeted MSPs. The real answer to ransomware lies in prevention rather than cure. So just how does this devastating malware commonly infect devices?

01
Breaches Through Phishing & Social Engineering

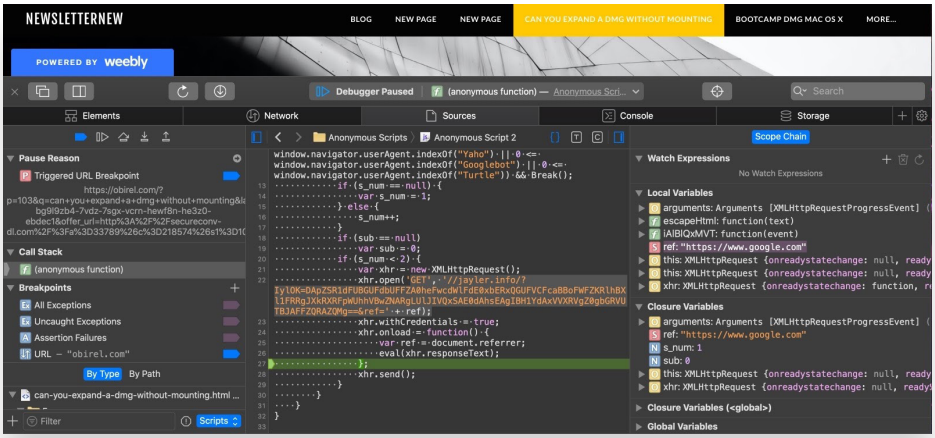
Still the most common method for hackers to initially infect an endpoint with ransomware is through phishing emails. Increasingly targeted, personalised and specific information is used to craft emails to gain trust and trick potential victims into opening attachments or clicking on links to download malicious PDF and other document files. These can look indistinguishable to normal files, and attackers may take advantage of a default Windows configuration that hides the file's true extension. For example, an attachment may appear to be called 'filename.pdf', but revealing the full extension shows it to be an executable, 'filename.pdf.exe'.

Files can take the form of standard formats like MS Office attachments, PDF files or JavaScript. Clicking on these files or enabling macros allows the file to execute, starting the process of encrypting data on the victim's machine.

Also See: Phishing | Revealing The Most Vulnerable Targets

02
Infection via Compromised Websites

Not all ransomware attacks have to be packaged in a maliciously-crafted email. Compromised websites are easy places to insert malicious code. All it takes is for an unsuspecting victim to visit the site, perhaps one they frequent often. The compromised site then reroutes to a page that prompts the user to download a newer version of some software, such as the web browser, plugin, or media player. Web redirections like this are particularly difficult for users to spot without digging into the code underneath every site they visit.



If the site has been primed to deliver ransomware, the malware could be either activated directly or more commonly run an installer that downloads and drops the ransomware.

03
Malvertising & Breaching The Browser

If a user has an unpatched vulnerability in his or her browser, a malvertising attack can occur. Using common advertisements on websites, cybercriminals can insert malicious code that will download the ransomware once an advertisement is displayed. While this is a less common ransomware vector, it still poses a danger since it doesn't require the victim to take any overt action such as downloading a file and enabling macros.

Also See: macOS Security | So How Do Macs Get Infected With Malware?

04
Exploit Kits That Deliver Custom Malware

Angler, Neutrino, and Nuclear are exploit kits that have been widely used in ransomware attacks. These frameworks are a type of malicious toolkit with pre-written exploits that target vulnerabilities in browser plugins like Java and Adobe Flash. Microsoft Internet Explorer and Microsoft Silverlight are also common targets. Ransomware like Locky and CryptoWall have been delivered through exploit kits on booby-trapped sites and through malvertising campaigns.

05
Infected Files and Application Downloads

Any file or application that can be downloaded can also be used for ransomware. Cracked software on illegal file-sharing sites are ripe for compromise, and such software is as often as not laden with malware. Recent cases of MBRLocker, for example, took this route. There is also potential for hackers to exploit legitimate websites to deliver an infected executable. All it takes is for the victim to download the file or application and then the ransomware is injected.

06
Messaging Applications As Infection Vectors

Through messaging apps like WhatsApp and Facebook Messenger, ransomware can be disguised as scalable vector graphics (SVG) to load a file that bypasses traditional extension filters. Since SVG is based on XML, cybercriminals are able to embed any kind of content they please. Once accessed, the infected image file directs victims to a seemingly legitimate site. After loading, the victim is prompted to accept an install, which if completed distributes the payload and goes on to the victim's contacts to continue the impact.

Also See: Hiding Code Inside Images: How Malware Uses Steganography

07

Brute Force Through RDP

Attackers use ransomware like SamSam to directly compromise endpoints using a brute force attack through Internet-facing Remote Desktop Protocol (RDP) servers. RDP enables IT admins to access and control a user's device remotely, but this also presents an opportunity for attackers to exploit it for malicious purposes.

Hackers can search for vulnerable machines using tools like Shodan and port scanners like Nmap and Zenmap. Once target machines are identified, attackers may gain access by brute-forcing the password to log on as an administrator. A combination of default or weak password credentials and open source password-cracking tools such as Aircrack-ng, John The Ripper, and DaveGrohl help achieve this objective. Once logged on as a trusted admin, attackers have full command of the machine and are able to drop ransomware and encrypt data. They may also be able to disable endpoint protection, delete backups to increase likelihood of payment or pivot to achieve other objectives.

Also See: 7 Ways Hackers Steal Your Passwords

Conclusion

Ransomware continues to evolve, with ransomware-as-a-service now growing in popularity. Malware authors sell custom-built ransomware to cybercriminals in exchange for a percentage of the profit. The buyer of the service decides on the targets and the delivery methods. This division of labor and risk is leading to increasingly targeted malware, innovation in delivery methods and ultimately a higher frequency of ransomware attacks.

Along with the threat of extortion through data leakage, these recent trends make it vital for organizations to invest in securing endpoints and networks and preventing breaches from occurring in the first place through AI-powered behavioral detection engines that do not rely on reputation nor rely on cloud-connectivity. If you would like to see how SentinelOne can help protect your business from ransomware and other threats, contact us today or request a free demo.

We would like to thank Daniel Card and Chris Roberts for their assistance with this post.

SentinelOne®

INFO EXCHANGE

Info Exchange, Ltd.
7 - 9 Ardenne Road
Unit 26, Kingston 10
+1 876.931.9552
www.infoexchangeja.com