Serianu Cyber Security Advisory

Ransomware Distribution Methods

Serianu SOC Advisory Number:
TA – 2020/0011

Date(s) issued:
8th September 2020

OVERVIEW

Ransomware is a growing threat to organizations around the world. Not only is it one of the biggest security problems on the internet but also one of the biggest forms of cybercrime that organizations face today. Ransomware infections such as WannaCry, Bad Rabbit, CryptoLocker and Locky are a growing problem that is now affecting many users and organizations.

Ransomware uses different techniques, the most common being to encrypt the victim's files, making them inaccessible and demanding a ransom payment to decrypt them. Victims are often left with limited choices; they can either regain access to their encrypted network by paying a ransom to the criminals behind the ransomware or crack the ransomware encryption. When ransomware successfully attacks an organization's critical assets, this has the potential to halt all business functions in the organizations.

This advisory covers how ransomware can affect a user, be distributed and be prevented against.

1. Email Attachments

Malicious email attachments are an increasingly dangerous threat to corporate security. This is because email is one of the most important means of communication in corporate environments. Ransomware is commonly distributed via emails. Attackers send email attachments and provide email content that is sufficient enough to convince the user that it is legitimate.

Since many email systems automatically block obvious malicious programs, attackers conceal a piece of software, called an exploit, inside files. The file can be delivered in a variety of formats including a ZIP file, PDF, Word document and Excel spreadsheet. Once the attachment is opened, the ransomware may be deployed immediately. In other situations, attackers may wait days, weeks or even months after the infection to encrypt the victim's files.

Recommendation

1. Check that the sender's email address is correct. Remember that domain names and display names can easily be spoofed.
2. Do not open attachments from unknown sources. Users should immediately alert IT security when they observe unsolicited emails containing attachments.
3. Install endpoint and server-based antivirus scanners.
4. Make sure spam filtering is enabled on your email account.

2. Malicious URLs

Malicious URLs that often look legitimate are widely used to propagate ransomware attacks. Attackers use emails and social media platforms to distribute ransomware by inserting malicious links into messages. To encourage users to click on the malicious links, the messages are usually worded in a way that evokes a sense of urgency or intrigue. Clicking on the link triggers the download of ransomware which encrypts the system and locks data for ransom.

Recommendation

1. Be wary of all links embedded in emails and direct messages.
2. Double check URLs by hovering over the link before clicking.
3. Use CheckShortURL to expand shortened URLs.
4. Manually enter links into your browser to avoid clicking on phishing links.

3. Remote Desktop Protocol

Remote Desktop Protocol (RDP) is a communication protocol that allows users to connect and control another computer over a network connection. By default, RDP receives connection requests through port 3389. Cybercriminals take advantage of this by using port scanners to scan for open ports. Attackers then attempt to gain access to the machine by exploiting security vulnerabilities or use a brute force attack to crack the machine's login credentials.

Once the attacker has gained access to the machine, they disable user's antivirus software and other security solutions, delete accessible backups and deploy the ransomware. Attackers may also leave a backdoor so that they can use it in the future. Some examples of ransomware that spread via RDP include SamSam, Dharma and GandCrab.

Recommendation

1. Use strong passwords.
2. Only enable RDP if necessary.

3. Enable 2FA for remote sessions.

4. Managed Service Providers

Hackers are increasingly finding ways to target several organizations at once through attacking Managed Service Providers (MSPs) that often provide IT services to organizations. Cybercriminals frequently target them with phishing attacks and exploit the remote monitoring and management (RMM) software commonly used by MSPs.

Attackers have exploited remote monitoring and management software that organizations download to install systems updates, patches and configuration changes. Remote management is often used to install updates and solve users' problems but it can also serve as an entry point to ransomware distribution. Hackers largely prey on MSPs that have weak passwords or do not use two-factor authentication.

Recommendation

1. Enable 2FA on RMM software.
2. MSPs should be hyper-vigilant regarding phishing scams.

5. Malvertising

Malvertising (malicious advertising) is becoming an increasingly popular method of ransomware delivery. Malvertising takes advantage of the tools used to display legitimate ads on the web. Attackers purchase ad space which is linked to an exploit kit. The ad might be a provocative image, a message notification or an offer for free software.

When a user clicks on the ad, the exploit kit scans the system for information about its software, operating system and browser details. If the exploit kit detects a vulnerability, it attempts to install ransomware on the user's machine. Ransomware attacks that spread through malvertising, include CryptoWall ransomware and Sodinokibi ransomware.

Recommendation

1. Keep systems, applications and web browsers up to date.
2. Disable plugins that are not in use.
3. Use ad blocker to block ads.

6. Drive-by Downloads

A drive-by download is any download that occurs without your knowledge. Ransomware distributors make use of drive-by downloads by either hosting the malicious content on their own site or injecting it into legitimate websites by exploiting known vulnerabilities.

When a user visits the infected website, the malicious content analyzes their device for specific vulnerabilities and automatically executes the ransomware in the background. Unlike many other attack vectors, drive-by downloads don't require any input from the user. Users don't have to click, install or open a malicious attachment. Visiting an infected website is all it takes to become infected.

Recommendation

1. Always install the latest software security patches.
2. Remove unnecessary browser plugins.
3. Install an ad-blocker.

7. Pirated Software

Ransomware is known to spread through pirated software. Some cracked software also comes bundled with adware, which may be hiding ransomware. In addition, websites that host pirated software may be more susceptible to malvertising or drive-by downloads.

The use of pirated software may also indirectly increase the risk of ransomware infection. Unlicensed software doesn't receive official updates from the developer, which means that users may miss out on critical security patches that can be exploited by attackers.

Recommendation

1. Avoid using pirated software.
2. Do not visit websites that host pirated software, cracks, activators or key generators.
3. Be careful of software deals that are too good to be true.

8. USB Drives and Portable Computers

USB drives and portable computers are a common delivery vehicle for ransomware. Connecting an infected device can lead to ransomware encrypting the local machine and potentially spreading across the network.

Recommendation

1. Never plug in unknown devices to your computer.
2. Do not plug in USB drives to a shared public system such as printers at cafes.
3. Organizations should implement and maintain robust BYOD security policies.

4. Where portable device storage is needed for business functions, a sheep-dip computer should be implemented to scan these devices. This computer is not connected to the organization network, and is equipped with multiple anti-malware scanners and file integrity verifiers.
5. Use reputable antivirus software that can scan and protect removable drives.

Measures to take when your system has been infected with ransomware:

1. Disconnect from Networks.

- Unplug Ethernet cables and disable wifi or any other network adapters.
- Put your device in Airplane Mode.
- Turn off Wi-Fi and Bluetooth.

2. Disconnect External Devices.

- USB drives or memory sticks.
- Attached phones or cameras.
- External hard drives.
- Or any other devices that could also become compromised.

3. Report the Incident

It is important that incidents are reported as early as possible so as to limit the damage and cost of recovery.

Conclusion

Regardless of how ransomware propagates, there are many ways organizations can reduce the risk of ransomware infection and mitigate the effects of an attack. Investing in proven antivirus software, maintaining backups and being cautious with clicking links can go a long way towards protecting the data and keeping systems safe from ransomware. In addition, user training on the risks of ransomware is important to improve information security hygiene in the organization.

Information Sharing

As a means of preventing such attacks from occurring, we encourage any organization or individual that has access to ransomware attacks share it with us through our email: info@serianu.com.