JONES DAY

COMMENTARY

MAY 2017

IN SHORT

The Situation: Detected on the morning of May 12, 2017, "WannaCry," a widespread ransomware attack, is impacting institutions in at least 150 nation around the world.

The Response: Specific actions, including the application of the Microsoft patch for the MS17-010 SMB vulnerability, are recommended.

Looking Ahead: Given the risks involved, companies should ensure that their insurance policies supply adequate coverage for ransomware attacks.

A new and widespread ransomware attack is affecting institutions around the world, with reports of hundreds of thousands of infections in nearly 150 countries, including the United States, United Kingdom, Spain, Russia, Taiwan, France, and Japan. The impact is expected to expand. Reports indicate that the software can run in 27 different languages. The latest version of this ransomware, known as WannaCry, WCry, or Wanna Decryptor, was just discovered on the morning of May 12, 2017, and spread rapidly and widely in a matter of hours. The ransom demanded is reported to be .1781 bitcoins, or roughly US$300.

Among the organizations affected are large transportation firms in the United States, telecommunications firms in Europe, a global automaker, universities in China, Germany's federal railway system, and Russia's Interior Ministry. The most dangerous and disruptive attacks were to Britain's public health system, which resulted in surgeries being rescheduled and patients being turned away from emergency rooms.

The Need to Patch Systems

Ransomware spreads easily when it encounters unpatched or outdated software. This risk may only be exacerbated given recent reports that NSA tools designed to exploit compromised systems have been leaked and are falling into the hands of cyber criminals. If more NSA tools are released, the need to patch known vulnerabilities proactively will grow.

> We recommend that systems be patched immediately.

We recommend that systems be patched immediately. Reports indicate the hackers behind the WannaCry campaign are accessing enterprise servers either through a Remote Desktop Protocol ("RDP") compromise or through the exploitation of a critical Windows SMB vulnerability. Microsoft released a security update for that vulnerability (MS17-010) on March 14, 2017, more than two months ago.

What Steps to Take

What to Do If Infected with Ransomware

- Apply the Microsoft patch for the MS17-010 SMB vulnerability dated March 14, 2017.
- Isolate the infected computers immediately. Infected systems should be removed from the network as soon as possible to prevent ransomware from attacking network or share drives.
- Isolate or power-off affected devices that have not yet been completely corrupted. This may afford more time to clean and recover data, contain damage, and prevent worsening conditions.
- Secure backup data immediately by taking it offline.

- Inspect backups for malware.

- Systems infected with ransomware are often also infected with other malware. Thus, responding to a ransomware attack should include an evaluation of relevant systems for the presence of other malware.

- Forensics typically will be unable to decrypt files once they are infected with ransomware. But, on occasion, the encryption key may be recovered from memory or the executable payload.

- Once infected, you should remove the infected system from the network, but do not power off.

- Separately, a good provider can assist you in determining (i) how malware was introduced into the IT environment; (ii) the scope of the compromise; and (iii) the malware's functionality, if not a documented variant with known functionality. Consider engaging outside counsel to retain and direct the forensic investigation to maximize privilege protection.

Business Continuity

- Backups are critical in ransomware recovery and response. If an infection occurs, a backup may be the best way to recover your critical data.

- Back up data regularly. Verify the integrity of those backups, as well as restoration systems to ensure they are working.

- Conduct an annual penetration test and vulnerability assessment and address identified vulnerabilities.

- Secure your backups. Ensure backups are not permanently connected to the computers and networks they are backing up.

Should You Pay the Ransom?

Law enforcement advises against payment of ransom. At the same time, they recognize that these determinations need to be made on a case-by-case basis. For instance, a ransomware victim must evaluate the technical feasibility, timeliness, and cost of restarting systems from backup—if a backup is even available. If mission-critical data is involved, or time is of the essence, paying a ransom may be the only viable recourse.

However, you should consider that with payment of ransom, the following outcomes are possible: (i) you do not get the decryption key; (ii) you get a decryption key that does not work; (iii) you are asked to pay a second ransom to get the decryption key; and/or (iv) you get the decryption key, it works, but you are immediately targeted again.

Insurance Considerations

We recommend that companies review their insurance programs to make sure they have adequate coverage for ransomware attacks. Coverage is available for investigative costs, ransom payments, and data restoration under cyber policies, property policies, and kidnap and ransom policies. However, such coverage is typically not part of the standard policy form and must be added by endorsement or coverage extension. Companies that fall victim to an attack should immediately assess their insurance as coverage may be impaired if the policyholder fails to notify the insurer and/or obtain consent before making payments.

THREE KEY TAKEAWAYS

1. Since ransomware spreads easily when it encounters unpatched or outdated software, it is critical that systems be patched immediately.
2. In order to minimize the impact of a ransomware infection, back up data regularly. If an infection occurs, secure the backup data by taking it offline.
3. If faced with a situation where a ransom must be paid, it is important to remember that payment does not guarantee the end of the situation. The attackers may not provide a working decryption key or you may be immediately targeted again.

AUTHORS


Richard M. Martinez
Minneapolis


Mauricio F. Paez
New York


Lisa M. Ropple
Boston


Richard J. Johnson
Dallas

ALL CONTACTS >>

YOU MIGHT BE INTERESTED IN: Go To All Recommendations >>

- Personal Data Held by Government Agencies Now Heavily Protected in Mexico
- China's New Cybersecurity Law and Draft Data Localization Measures Expected to Burden Multinational Companies
- $2.5 Million Settlement Reached as HIPAA Crackdown Continues on Unsecured Portable Devices
- Data Breach Risks for 401 (k) and Retirement Plans

SUBSCRIBE SUBSCRIBE TO RSS

Jones Day is a legal institution with more than 2,500 lawyers on five continents. We are One Firm Worldwide℠.