Published on *The National Law Review* https://natlawreview.com

Global Ransomware Attack: What Your Organization Needs to Know Now

Article By:

Kenneth K. Dort

Anand Raj Shah

Katherine E. Armstrong

Beginning on Friday, May 12, 2017, organizations across the world were hit by a cyberattack called WannaCry. This malware—a type of ransomware—operates by encrypting an organization's data and demanding a Bitcoin payment (nearly $300 per attack) before it will restore the affected files. So far approximately 200,000 computers in over 150 countries have been impacted, making this the largest international ransomware attack to date. Victims of the attack range in size—from Fortune 500 to small/medium-sized businesses—and industry—from academic institutions to large banks, health care providers, and transportation networks.

I. What Happened?

The ransomware culprit, WannaCry, spreads via a computer virus known as a "worm." Unlike many other similar types of malware, this one has the ability to move around a network by itself. What makes WannaCry particularly insidious is that once inside an organization's network it will hunt down vulnerable machines and infect them too. This may explain why WannaCry's impact has been so massive, because large numbers of machines at each victim organization are being compromised. Currently, the perpetrators behind the attack are not known.

The WannaCry malware has been found throughout Europe, North and South America, and Asia. The UK's National Health Service (NHS) was among the hardest hit and it has been reported that the IT systems of about 40 NHS organizations have been affected by this ransomware attack. As a result, non-emergency operations were suspended and ambulances were being diverted to other hospitals. It appears that these NHS systems were vulnerable because they used older versions of Microsoft operating systems that are no longer updated.

II. Understanding the Code

Besides WannaCry, the ransomware goes by several other names, including WCry, WannaCrypt0r, WannaCrypt, and Wana Decrypt0r, all of which are version 2.0 of the original WCry ransomware

code first introduced in March 2017. This ransomware appears to attack older Microsoft operating systems such as Windows XP, Windows 8 and Windows Server 2003.

The most popular infection vector reported has been via phishing emails. According to experts, the initial spread of WannaCry came through spam, in which fake invoices, job offers, and other lures are sent out to random email addresses. Within the emails is a .zip file, and clicking on the file initiates the WannaCry payload.

Experts are concluding that WannaCry appears to exploit a bug found earlier this year by the U.S. National Security Agency (NSA), as well as a weakness in certain Microsoft operating systems. However, the NSA has neither confirmed nor denied this fact. News organizations have reported that when details of the bug were initially leaked in March by a group calling itself the “Shadow Brokers,” many security researchers predicted it would lead to the creation of self-starting ransomware worms. It appears that it only took a couple of months for malicious hackers to make good on that prediction.

The number of infections may have been slowed somewhat after a so-called "kill-switch" appears to have been triggered by a UK-based cyber-security researcher tweeting as @MalwareTechBlog. The researcher discovered that the web address that WannaCry was searching for had not been registered. As soon as he registered the domain, the ransomware appeared to stop spreading. Nevertheless the researcher is urging computer users to still immediately patch their systems and update their Windows operating systems because the attackers are likely to introduce new variants of the ransomware code.

III. Potential System Risks

The WannaCry virus has only been known to infect computers running Windows. Your organization is at risk if you do not update your Windows operating system. The NHS, for example, was particularly vulnerable because of its heavy reliance on Windows XP, an operating system that is no longer supported by Microsoft. Anti-virus signatures for known ransomware variants, including WannaCry, may need to be updated as well. Furthermore, the risks of ransomware compound when organizations lose valuable data that has not been backed up and that cannot be properly restored.

IV. Possible Solutions and Best Practices

Patching and System Updates. Older unsupported Microsoft systems such as Windows Server 2003 and Windows XP are particularly vulnerable. In what some are calling an unusual step, Microsoft announced that it would roll out updates to users of older operating systems "that no longer receive mainstream support," such as Windows XP, Windows 8 and Windows Server 2003. In the meantime, experts are recommending that organizations harden against this threat and ensure that all systems are fully patched with the "MS17-010" security update.

Data Backups. Organizations should regularly back up important data. As a precaution, backups should be stored apart from your system, thereby insulating it from potential malware, and rendering it available for a system restoration when necessary. Ransomware cannot encrypt what it cannot access.

User Vigilance and Training. Your organization should not only use firewalls and update its anti-virus software, but also instruct users to be careful in their use of the internet and emails—including being wary of any unfamiliar emails and refraining from clicking on any suspicious links or attachments. Employees and users should be reminded to “think before they click” when they

receive any out-of-the-ordinary emails.

V. Best Practices

The WannaCry attack provides another in a long series of “red flags.” Data security policies and procedures should be reviewed and revised in light of the vulnerabilities identified by the WannaCry ransomware.

1. If you have not conducted a comprehensive security assessment, now would be a good time to begin. Indeed, this assessment should be commenced as soon as possible. Once an assessment has been conducted, it is important to have it incorporated into an incident response plan for your organization to use going forward.

2. For those organizations having comprehensive security protocols in place, take this opportunity to conduct your regular re-assessments and threat analyses now. Ensure that your current defenses are properly configured to address your current risk profile and that all appropriate updates and patches have not only been installed, but are also functioning. As noted above, a patch to close the vulnerability in question has been available since March 2017 but, unfortunately, many organizations simply failed to apply it in time.

3. Ensure that the backups to your data are current and properly secured to enable their implementation when necessary.

4. Continually train and remind employees and network users to be aware of and on the lookout for suspicious emails and to “think before they click” on any attachments.

5. As part of a comprehensive information governance program, ensure that you have a thorough incident response plan in place that contemplates the occurrence of a ransomware attack.

National Law Review, Volume VII, Number 135