Clients&FriendsMemo

WannaCry Ransomware Attacks Should Be a Wake-Up Call for Cybersecurity Diligence

May 17, 2017

Last week's massive ransomware attack should serve as a wake-up call that companies across all industries and regions must take the threat of global cyber attacks seriously. Although investigators are still uncovering details, three key lessons have emerged for businesses seeking to protect themselves. First, ransomware attacks are going to become much more common. Second, the attack might have been prevented if companies had been more diligent about implementing basic cybersecurity practices, such as patching software vulnerabilities and training staff to detect phishing emails, *i.e.*, emails that appear legitimate but contain links or files that deploy computer viruses if opened. And, third, companies that fail to take reasonable measures to prevent attacks might find themselves to be the subject of costly regulatory enforcement actions or private litigation.

What Is Ransomware?

Ransomware is a form of malevolent software, or "malware," that typically encrypts or deletes data stored on computer networks, trapping the data and making it unavailable and unusable. Hackers responsible for installing ransomware on victims' computer networks frequently demand payment (the "ransom" in ransomware) to have the data restored.

Ransomware attacks can be tremendously costly. Even in the best-case scenario, where victims are prepared for an attack and have maintained up-to-date archives, there are still significant remedial costs and business disruptions that come in the wake of an attack. However, in the worst-case scenario, where victims do not have access to backup copies of their data, they find themselves in the no-win position of having to decide whether to pay the hackers or potentially lose their data forever. Each option is unappealing – by paying the hackers, victims only encourage future attacks and there is no guarantee that the hackers will even restore the victims' data. However, by refusing to pay, victims could effectively find themselves out of business.

Ransomware has grown in popularity in recent years because it can be very profitable. In a traditional data breach, financially-motivated hackers typically steal personal data such as bank or credit card information; however, that is only the first of several steps they must take before they can profit from their efforts. They must then find buyers for the stolen data or themselves exploit the

information through an identity-theft or other fraudulent scheme, each of which imposes additional risks and costs.

By contrast, in a ransomware attack, hackers need not worry about dealing with a middleman or finding a way to exploit the stolen data themselves. They simply hold a victim's data hostage and demand payment.

What Happened in the WannaCry Attack?

Last week's attack focused on a vulnerability in computer networks running Microsoft Windows.[1] The vulnerability at issue appears to have been originally identified by the National Security Agency ("NSA") and was leaked online earlier this year by a group known as "The Shadow Brokers." Several weeks later, an unknown group of hackers – possibly backed by North Korea[2] – used a combination of the NSA exploit coupled with phishing attacks to infect computers with a type of ransomware known as "WannaCry" or "WannaCrypt." Once a victim's network became infected, the ransomware quickly spread to other computers throughout the network, encrypting data and demanding approximately $300 in bitcoin in exchange for decrypting the data.

Initially, the attack appeared to be focused on the computer network of the United Kingdom's National Health Service, which was forced to close emergency rooms and cancel patient appointments due to the temporary inability to access patient records. The attack quickly spread to computers around the world, reaching at least 200,000 computers in 150 countries, including networks used by the Russian Interior Ministry and by thousands of schools in China. Researchers estimate that victims have paid approximately $70,000 thus far to the hackers.[3] The attack was effectively halted when a computer researcher reportedly discovered a "kill switch" in the ransomware's computer code and was able to prevent additional attacks.[4] However, by then it was too late to rescue computers that had already been infected. Even though the ransomware's continued spread appears to have been slowed or even stopped, and no significant follow-up attacks have emerged thus far, the damage is still being felt by victims who are struggling to restore their operations.

---

[1] *See* Nicole Perlroth and David E. Sanger, *Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool*, The New York Times (May 12, 2017), *available at* https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html?action=click&contentCollection=U.S.&module=RelatedCoverage&region=Marginalia&pgtype=article.

[2] *See* Nicole Perlroth and David E. Sanger, *In Computer Attacks, Clues Point to Frequent Culprit: North Korea*, The New York Times (May 15, 2017), *available at* https://www.nytimes.com/2017/05/15/us/nsa-hacking-shadow-brokers.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=first-column-region&region=top-news&WT.nav=top-news.

[3] *See* Sean Gallagher, *WCry ransomware worm's Bitcoin take tops $70k as its spread continues*, Ars Technica (May 16, 2017), *available at* https://arstechnica.com/security/2017/05/wcry-ransomware-worms-bitcoin-take-tops-70k-as-its-spread-continues/.

[4] *See* Malwaretech, *How I accidentally stopped a global Wanna Decryptor ransomware attack*, Ars Technica (May 15, 2017), *available at* https://arstechnica.com/information-technology/2017/05/wanna-decryptor-kill-switch-analysis/.

What Lessons Should Be Learned?

Lesson #1. Ransomware attacks are going to become much more common. As hackers realize that it is faster and more profitable to extort money directly from victims, rather than steal data and then engage in identify theft and money laundering schemes to profit from it, they will be encouraged to pursue attacks similar to what we saw last week. The U.S. Department of Justice reported that there was an average of about 4,000 ransomware attacks each day in 2016, a 300 percent increase over the prior year.[5] Some experts believe that ransomware may be one of the most profitable cybercrime tactics in history.[6]

Lesson #2. Companies must take certain basic steps to protect their networks, including regularly updating their software and training employees to better recognize phishing emails. In this case, Microsoft issued a "critical" patch for its Windows operating systems in March 2017 that resolved the vulnerability that was exploited during the attack.[7] Yet countless organizations remained vulnerable either because they were not diligent about installing software updates, were running older versions of Windows (such as Windows XP) for which Microsoft no longer issues updates, or were running pirated versions of Windows that are unable to receive security updates.[8] Further, as it appears that phishing emails were used to deliver the ransomware, it is vital that companies train employees to recognize phishing emails and respond appropriately. According to one study, nearly half of adults in the United States cannot identify a phishing email.[9]

Lesson #3. Victims of future cyber attacks will face not only the time and monetary disruption caused by a successful breach, but also possible enforcement actions and civil litigation. Indeed, last fall the former Chairwoman of the Federal Trade Commission warned U.S. businesses that "a company's unreasonable failure to patch vulnerabilities known to be exploited by ransomware might violate the [Federal Trade Commission] Act."[10] Other regulators, such as the Securities and Exchange Commission ("SEC") and the New York Department of Financial Services, might also consider a company's failure to timely implement updates or train employees as failing to take

---

[5] *See* Department of Justice, *Protecting Your Networks from Ransomware*, *available at* https://www.justice.gov/criminal-ccips/file/872771/download.

[6] *See* Tom Risen, *Ransomware Is the Most Profitable Hacker Scam Ever*, U.S. News & World Report (July 27, 2016), *available at* https://www.usnews.com/news/articles/2016-07-27/cisco-reports-ransomware-is-the-most-profitable-malware-scam-ever.

[7] *See* Microsoft Security Bulletin MS17-010 – Critical (Mar 14, 2017), *available at* https://technet.microsoft.com/en-us/library/security/ms17-010.aspx.

[8] *See* Dan Goodin, *Wanna Decryptor ransomware: What is it, and how does it work*, Ars Technica (May 15, 2017), *available at* https://arstechnica.co.uk/security/2017/05/what-is-wanna-decryptor-wcry-ransomware-nsa-eternalblue/.

[9] *See* Angus Loten, *Employee 'Weak Link' in Cybersecurity Efforts: Analysts*, The Wall Street Journal (Apr 3, 2017), *available at* https://blogs.wsj.com/cio/2017/04/03/employees-weak-link-in-cybersecurity-efforts-analysts/.

[10] Opening Remarks of FTC Chairwoman Edith Ramirez, Fall Technology Series, Ransomware (Sept 7, 2016), *available at* https://www.ftc.gov/system/files/documents/public_statements/983593/ramirez_-_ransomware_remarks_9-7-16.pdf.

reasonable measures to safeguard customer data, prompting regulatory action. And the Office of Civil Rights ("OCR") of the Department of Health and Human Services, which is responsible for bringing enforcement actions under the Health Insurance Portability and Accountability Act ("HIPAA") when health care companies fail to safeguard confidential patient data, issued guidance in July 2016 that stated that OCR would consider a ransomware attack to be a HIPAA breach if private patient data was compromised.[11] OCR issued this guidance after a series of high-profile ransomware attacks on hospitals in the U.S. in early 2016, including one attack in which a California hospital was required to pay hackers $17,000 in bitcoin to restore access to its patient medical records.[12] Further, publicly traded companies need to consider whether a ransomware attack is material and whether disclosure is appropriate. The acting director of enforcement at the SEC recently stated that the agency would "absolutely" pursue an enforcement action for insufficient disclosure of cyber incidents and risks if circumstances warranted.[13] Finally, the possibility of harm to consumers – particularly those who are harmed by the loss of sensitive medical or financial data – raises the possibility of costly customer class action litigation against companies that are the victims of ransomware attacks.

Conclusion

Most public companies and financial institutions are already subject to a host of regulations governing how they safeguard customer data. However, last week's attack illustrates the importance of taking simple steps to protect data from ransomware. In response to the WannaCry attack, the Federal Bureau of Investigation has posted a bulletin listing ways for companies to protect their data.[14] Basic steps to protect data include:

- Maintaining backups of critical data that are maintained separately from the organization's internal computer network and regularly testing the backups to ensure they work correctly.
- Promptly installing software updates that are intended to address security vulnerabilities.
- Screening incoming email traffic for potential phishing attacks and ensuring that employees are trained to detect and report them.

In addition, companies should consider consulting with legal counsel regarding the adequacy of their cybersecurity programs or, if they have been the victims of a cyber attack, to mitigate their potential liability.

---

[11] *See* FACT SHEET: Ransomware and HIPAA, *available at* https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf.

[12] *See* Richard Winton, *Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating*, Los Angeles Times (Feb 18, 2016), *available at* http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html.

[13] *See* Jimmy Hoover, *SEC Suits Over Cyber Reporting Could Be On Horizon*, Law360 (Apr 20, 2017), *available at* https://www.law360.com/articles/915377/sec-suits-over-cyber-reporting-could-be-on-horizon.

[14] *See* FBI Flash, *Indicators Associated With WannaCry Ransomware*, MC-000081-MW (May 13, 2017), *available at* http://www.himss.org/sites/himssorg/files/flash-fbi-wannacry.pdf.

If you have questions, please contact any of the following attorneys or your Cadwalader contact:

Joseph Moreno	+1 202 862 2262 +1 212 504 6262	joseph.moreno@cwt.com
Joseph Facciponti	+1 212 504 6313	joseph.facciponti@cwt.com