Aon Benfield
Cyber Analytics

Cyber Event Briefing: WannaCry Ransomware Attack

May 22, 2017

What happened: A global ransomware attack infected more than 300,000 computers in approximately 150 countries across the globe. As of May 22, the "second wave" of attacks that was expected on Monday, May 15 has not materialized, and the immediate threat of WannaCry appears to be abating.

Details: On Friday, May 12, 2017, tens of thousands of users' machines around the world were infected with the "WannaCry" malware, a form of ransomware. More computers continued to be infected over the weekend and into Monday, May 15 with over 300,000 machines across 30,000 institutions now estimated to have been affected.

Ransomware is designed to encrypt well-known file extensions on a host computer, in the hopes the victim will pay a ransom to decrypt their most important files. In this case, the average ransom requested was the equivalent of USD 300, payable in bitcoin. The initial reports indicated widespread business interruption at hospitals, universities, telecommunications firms, and government institutions.

Ransomware is nothing new, but what we've witnessed since Friday, May 12 is much more prolific. This iteration of WannaCry ransomware exploited a Microsoft Windows-based vulnerability MS17-010 that allowed it to promulgate within a compromised network. MS17-010 is a Server Message Block (SMB) network file-sharing protocol vulnerability first exploited by the United States National Security Agency (NSA)—known as ETERNALBLUE—and subsequently leaked by the hacker group, the Shadow Brokers. By exploiting MS17-010, the perpetrators gained remote access with system privileges. Additionally, WannaCry would use the protocol to locate and exploit adjacent, vulnerable hosts. In other words, **WannaCry can infect new hosts without requiring user interaction.** This is more pernicious than many varieties of ransomware which are distributed through phishing e-mails, which require users to click to trigger the malware. The initial vector into a host network remains a mystery, as "patient zero" has yet to be identified. Another feature of this iteration of WannaCry was the presence of a built-in "kill switch"—activated when the malware communicated with a specific domain. The subsequent activation of this specific domain eventually decelerated WannaCry's spread.

The most high-profile infections have been against the United Kingdom's National Health Service (NHS), FedEx, Telefonica, Nissan and Renault. However, the vast majority of successful attacks were in Russia, followed by other states in CEE, Asia, and Africa.

The spread of WannaCry and potential fallout was so great Microsoft pushed out a patch for Windows XP—what Microsoft referred to as a "highly unusual step" as it does not offer updates of this legacy version of Microsoft's OS.

Who is responsible? Attribution of cyber attacks is extremely difficult, and it could be weeks or months before any official charges are made—if they are made at all.

What are the loss estimates?

Economic losses

The extent of infection and associated costs are still being determined; some businesses have several more days to decide whether to pay the ransoms.

The cyber modeling firm Cyence, with whom Aon Benfield has a model license, has made an initial estimate of approximately USD 8 billion in economic losses from this event.

Aon Benfield also licenses the RMS cyber accumulation model. While RMS have not yet published a loss estimate, our estimation of economic losses using the RMS model for the UK NHS locations is *much* lower, at approximately USD 32,000. Our experience with the RMS model to date suggests that the RMS numbers are lower than reality—perhaps meaningfully so. For example, the RMS model makes the default assumption that large companies do not become victims of ransomware.

While demand for ransom payments gets the attention in ransomware cases, the ransom payments can in fact be a fairly small expense relative to total costs. Cybercriminals typically set the ransoms to be small amounts—in this case, about USD 300 equivalent in bitcoin—so that it is easier for infected institutions to pay the ransom than to try to recoup their data (even so, USD 300 is curiously low). The cost of business interruption to an institution can quickly dwarf the ransom payments. In addition, businesses will often run forensics to make sure that no further threats are affecting their networks. In the Cyence loss estimate, the bulk of the USD 8 billion loss estimate comes from incident response costs and lost income due to business interruption.

As of 22 May, security analysts only estimated a bitcoin total equivalent to USD 99,000 in ransoms has been paid.

Insurance and reinsurance losses

Some large businesses with cyber cover will most likely have incurred some costs for incident response such as rectification, restoration and forensics, and potentially a business interruption loss, subject to their deductible / time retention. Generally, we expect losses will most likely arise from the incident response costs, rather than ransom payments or business interruption.

That said, we expect the impact on insurers and reinsurers to be minimal, for several reasons. Most cyber insurance policies—approximately 85 percent—are for US companies, and US companies were fortunate not to be greatly impacted by WannaCry. US companies may have been better prepared to mitigate the risks posed by WannaCry by implementing proper cyber security controls - such as patch management - compared to their counterparts around the world. . A large number of infections took place in geographies where cyber insurance take-up is extremely low, such as Eastern Europe, Russia, and Asia. Even in the UK, the most affected institution was the National Health Service, which being a government-supported entity, is unlikely to have had much cyber insurance in place.

How has the insurance industry reacted to this event? For the most part, insurers have seen the WannaCry attack as good for business. This was an event that a cyber policy is designed to cover, and is seen as likely to stimulate demand for cyber insurance—particularly in countries where current take-up rates are extremely low.

Could we have seen this coming? Yes and no. Once the NSA exploits were leaked one could assume that some group would use them in some way. But anticipating the timing and nature of this attack would have been difficult.

The specific Windows vulnerability that was used in WannaCry could not be seen from outside a company's firewall—this means that outside-in security raters could not see this vulnerability on company systems, which constrained their ability to anticipate this specific scenario. What these vendors can do is look at the software patching cadence for organizations – the discipline and regularity with which an organization adheres to a patching regime: any company up to date on its patching should not have been hit by this attack.

Could this have been worse? Absolutely. The SMB exploit could have been used in conjunction with a much more potent piece of malware. However, the concentrations in specific territories seem to suggest that good risk management measures, including IT security, business continuity planning and employee training, can drastically reduce an organization's vulnerability to such an attack. Nonetheless, that large, sophisticated businesses did fall victim underlines the residual risk and, hence, the relevance of the product.

Sources

Anomali, Cyence, Malware Tech, McAfee, New York Times, Reuters, Twitter, Wall Street Journal.

Further reading

http://www.reuters.com/article/us-cyber-attack-insurance-idUSKCN18B00H

https://www.nytimes.com/2017/05/13/world/asia/cyberattacks-online-security-.html?mabReward=R2&recp=0&action=click&pgtype=Homepage&region=CColumn&module=Recommendation&src=rechp&WT.nav=RecEngine&_r=0

https://www.strozfriedberg.com/blog/were-you-ready-for-wannacry/

http://www.theonebrief.com/lessons-learned-questions-posed-by-wannacry-ransomware-attack/

Contact Information

Authors

Jon Laux, FCAS
Head of Cyber Analytics
Aon Benfield
+1 312 381 5370
jonathan.laux@aonbenfield.com

Craig Guiliano, CISSP
Associate Director, Global Cyber Practice Group
Aon Benfield
+1 212 441 1568
craig.kerman@aonbenfield.com

Aon Benfield Cyber Practice Group Leadership

Bill Henriques
Global Cyber Practice Group Co-Leader
Aon Benfield
+1 973 966 3565
william.henriques@aonbenfield.com

Luke Foord-Kelcey
Global Cyber Practice Group Co-Leader
Aon Benfield | Global Re Specialty
+44 (0)20 7086 2067
luke.foord-kelcey@aonbenfield.com

About Aon Benfield

Aon Benfield, a division of Aon plc (NYSE: AON), is the world's leading reinsurance intermediary and full-service capital advisor. We empower our clients to better understand, manage and transfer risk through innovative solutions and personalized access to all forms of global reinsurance capital across treaty, facultative and capital markets. As a trusted advocate, we deliver local reach to the world's markets, an unparalleled investment in innovative analytics, including catastrophe management, actuarial and rating agency advisory. Through our professionals' expertise and experience, we advise clients in making optimal capital choices that will empower results and improve operational effectiveness for their business. With more than 80 offices in 50 countries, our worldwide client base has access to the broadest portfolio of integrated capital solutions and services. To learn how Aon Benfield helps empower results, please visit aonbenfield.com.