Global Cyber Attack Highlights Need for President Trump's Executive Order

05.19.2017

Many companies from around the globe are continuing their recovery efforts after a massive ransomware attack affected hundreds of thousands of computers across various industries and throughout several nations. Ransomware is a type of malware that encrypts files on infected networks, rendering them useless, and then issues a ransom demand, often in Bitcoin, for the decryption of the data.[i] On Friday, a ransomware variant known as "WannaCry," which was purportedly generated and disseminated using a stolen National Security Agency toolkit, spread rapidly throughout approximately 150 countries, affecting organizations such as the British National Health Service, Federal Express, and Nissan.[ii] The National Health Service in Britain was particularly hard hit with at least 40 organizations affected, leaving critical data such as patient and scheduling data and email unavailable.[iii]

The ransom demanded with these attacks has been relatively small, around $300 per computer on Friday and doubling to $600 after several days. The hackers threatened to lock the files permanently after a week.[iv] Although these are low dollar figures even for many ransomware attacks, typically ransomware demands are modest in order to encourage the victims to pay. As of the morning of Monday, May 15, 2017, roughly $50,000 in bitcoin had been paid.[v] Microsoft has issued a security patch which can help prevent an infection, and cybersecurity experts encourage victims to download the Microsoft patch rather than pay the ransom, as paying only encourages the hackers to continue their attacks.[vi] There is also no guarantee that paying the ransom will result in the unlocking of one's encrypted data.

As a temporary reprieve, a British researcher uncovered and utilized the "kill switch" the hackers had installed in the event that they had chosen to stop the attack from spreading, and it was for this reason that a number of United States' companies initially were left untouched. However, the researcher's actions to stop the malware's spread are believed to have only a temporary benefit, and it has been reported that new variants on the WannaCry ransomware have been released.[vii]

Already likely the largest ransomware attack to date, the potential for additional repercussions from the Friday WannaCry attack, as well as subsequent variations, are a significant and continuing cybersecurity threat worldwide.

The cyber attacks came one day after President Trump issued his long-awaited executive order, "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" (the "Executive Order"). The Executive Order sets forth the administration's efforts to strengthen cybersecurity to protect federal government assets as well as critical infrastructure by having government agencies focus more on the government from a connected enterprise perspective rather than on each agency as a separate, unconnected entity. Federal agency heads are held responsible under the Executive Order for managing cybersecurity risk and are directed to use the National Institute of Standards and Technology's (NIST) "Framework for Improving Critical Infrastructure Cybersecurity" (the "Framework") to manage their respective agency's cybersecurity risk. The Framework initially was published in February, 2014. However, earlier this year NIST circulated a version 1.1 draft of the Framework; comments to the draft were due on April 10th.

Each agency head is directed to provide a risk management report to the Department of Homeland Security and the Office of Management and Budget (OMB) within 90 days. Agency heads also are directed to show preference for shared IT services, such as the cloud, in federal procurements. In addition, the Executive Order calls for various federal agencies to prepare a number of government studies and reviews. Issues to be addressed, include:

- Modernization of federal IT systems;
- The potential and consequences of a prolonged power outage associated with a cyber event; and,
- Future training needs for cybersecurity professionals.

The proposed studies and their outcomes may have significant consequences and present opportunities for government contractors. The government relies heavily on contractors to develop and maintain their information systems. In addition, contractors often interact directly with government information systems while providing needed services. As a result, as the President seeks to hold agency heads accountable for the security of their systems, such agencies may begin to hold contractors to a higher standard of accountability. On the other hand, the government's reliance on industry presents opportunities for the contractors to be creative in addressing the government's ever growing need for connected and secure Information services.

It is increasingly clear that a well-crafted cyber protection program needs to include a technical, operational and a policy/procedure component. There does not appear to be a connection between the timing of the WannaCry attacks and the Executive Order. However, they highlight the growing pressure that organizations of all sizes and types will face to strengthen their cyber protection program.

[i] "Ransomware," *Microsoft*, https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx (last visited May

15, 2017).

[ii]David E. Sanger, et al., “Ransomware’s Aftershocks Feared as U.S. Warns of Complexity”, The New York Times, May 17, 2017, available at https://www.nytimes.com/2017/05/14/world/europe/cyberattacks-hack-computers-monday.html?_r=0 ; Saphora Smith, et al., “Huge Cyberattack Hits Nearly 100 Countries with ‘Wanna Decryptor’ Malware”, NBCNews, May 13, 2017, available at http://www.nbcnews.com/news/world/national-health-service-cyberattack-hits-english-hospitals-hackers-demand-bitcoin-n758516.

[iii] Damien Gayle, et al., “NHS Seeks to Recover from Global Cyber-attack as Security Concerns Resurface”, The Guardian, May 13, 2017, available at https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack.

[iv]Arjun Kharpal, “Hackers Who Infected 200,000 Machines Have Only Made $50,000 Worth of Bitcoin”, CNBC, May 15, 2017, available at http://www.cnbc.com/2017/05/15/wannacry-ransomware-hackers-have-only-made-50000-worth-of-bitcoin.html.

[v] *Supra* note iv.

[vi] *Supra* note v; Alex Johnson, *‘WannaCry’ Malware Attack Could Just Be Getting Started: Experts*, NBCNews, May 15, 2017, available at http://www.nbcnews.com/news/us-news/blockbuster-wannacry-malware-could-just-be-getting-started-experts-n759356.

[vii] *Supra* note ii.

Related People

- Anthony H. Anikeeff – 703.760.5206 – aanikeeff@williamsmullen.com
- Kevin D. Pomfret – 703.760.5204 – kpomfret@williamsmullen.com

Related Services

- Data Protection & Cybersecurity