Global ransomware attacks—the impact and the response

May 16 2017

Credit: Northeastern University

A global cyberattack unleashed Friday has reportedly affected more than 200,000 computers across more than 150 countries. The "ransomware," called "WannaCry," exploits a vulnerability in the Windows operating

system. The attacks hit companies and governments, encrypting users' computers and demanding bitcoin payments in exchange for unlocking the files. Asia was hit particularly hard Monday, because many businesses there had closed when the attack first struck on Friday.

We asked four faculty members—professors Engin Kirda and Alina Oprea, experts in cybersecurity, and professors Jeffrey Born and Martin Dias, of the D'Amore-McKim School of Business—to assess the nature of the cyberattack and what it means for the businesses and other affected institutions going forward.

How would you characterize the significance of the scale and scope of these attacks?

Kirda: The scale was large, but I would not say that it was surprising. "Ransomware" has been a problem for a while, and many different organizations have been hit in the past. In this specific case, the interesting issue was that a specific "ransomware" campaign managed to infect many organizations in a very short period of time. Looking at this historically, however, we have seen this type of thing before. For example, in the 90s and early 2000s, internet worms used to spread this quickly as well. The main difference today, though, is that the attackers are aiming to make money.

Oprea: One interesting aspect of this attack was the synchronization across different countries and continents and the variety of targeted organizations, which ranged from hospitals to academic institutions. Clearly, this was a well-organized attack with a larger scale than previous campaigns.

As The Washington Post notes, "The attack was notable because it took advantage of a security flaw in

Microsoft software found by the National Security Agency for its surveillance tool kit" and that flaw was leaked online. Should the NSA or any other entity be partially blamed for this cyberattack?

Oprea: We could not blame a single entity for this attack, as cybersecurity is a complex ecosystem. But this attack shows that intelligence and government agencies need to work closely with vendors and industry to patch vulnerable software and prevent large-scale catastrophic effects such as the ones we just experienced.

In light of these "ransomware" attacks, what would you identify as critical cybersecurity priorities going forward? Where should more resources be dedicated?

Oprea: Cybersecurity should become a priority for all organizations across various sectors, and this incident demonstrates this one more time. Organizations need to develop basic security programs that involve patching their software, deploying various defenses, and having clear plans for incident response. They should try to become more proactive about preventing these incidents, rather than trying to recover after the fact.

Various news outlets reported that an expert stopped the spread of attack by activating the software's "kill switch." What is a kill switch, and why would something like this be built into a cyberattack?

Kirda: A kill switch in any system is a mechanism that would deactivate that system right away. In this specific case, the malware, apparently, was contacting a domain name that hadn't been registered yet. Whenever the domain was available, the malware would stop spreading. We can

only speculate on why the authors of the malware would choose to have a kill switch like this. Anything is possible.

The attackers demanded bitcoin in exchange for unlocking users' files. Why they would want to be paid in this currency, and does this situation raise concerns over its use going forward?

Born: I think the ransom demand for bitcoins has a lot more to do with the perceived cybersecurity of the "currency" rather than the recent price strength in bitcoins. Bitcoins are not issued by countries, and their transfer has become even more difficult to trace. This provides the criminal element an opportunity to conduct transportation in virtual secrecy. Bitcoins have always been popular with those looking to cover their financial tracks. The development of the block-chain technology has made them even more stealthy, which has helped drive their market prices up substantially. It may not be an ideal endorsement in a marketing sense, but this use as a ransom will no doubt drive bitcoin popularity even higher.

What do these attacks mean for how businesses—and perhaps consumers—approach their information systems going forward? What lessons, if any, can be learned?

Dias: When considering cybersecurity for businesses, we tend to break out three goals for what is called "information assurance"—confidentiality, integrity, and accessibility. If our information systems were water systems, we might say our goals are no leaks, no pollution, and no blockage. "Ransomware" attacks hurt organizations by creating a blockage. On some accounts, "ransomware"

attacks have doubled in frequency from 2015 to 2016, and these attacks are gaining in publicity.

Going forward, more resources will be allocated to data backups. Companies and consumers are already moving toward more cloud-based storage platforms, which generally should improve recoverability from "ransomware" attacks. In addition, more attention will be given to upgrading existing systems to at least update security patches. I also think you will see more businesses attempting to make more effective business use of the cybersecurity monitoring and alerting tools they invest in. Artificial intelligence is currently used in many organizations to identify anomalies in customer and employee online behavior. When Big Data analysis makes more effective use of cybersecurity monitoring tools, then you will see even more attention and resource given to protecting the information assets of firms.

Provided by Northeastern University