2017-11-19

Russia and Ransomware: Stop the Act, Not the Actor

Jasper, Scott

S. Jasper, Russia and Ransomware: Stop the Act, Not the Actor, The National Interest, November 20, 2017
http://hdl.handle.net/10945/57094

Russia and Ransomware: Stop the Act, Not the Actor

nationalinterest.org/feature/russia-ransomware-stop-the-act-not-the-actor-23263

The problem with defeating cyberattacks is that speed and number of threats outpace human-centered cyber defense. That is why a new approach to cyber defense is needed.

Reports have surfaced that the U.S. government hasevidence linking hackers working for the Main Intelligence Directorate of the Russian military with stolen emails that harmed the Democratic National Committee during the presidential campaign. While arrests are unlikely, bringing charges that name and shame the hackers might influence the malefactors in the Kremlin. Barack Obama responded by placing sanctions on Russia as well as expelling officials and closing facilities, which led Vladimir Putin to laugh and eventually counter with similar measures. Perhaps it is time to admit that imposing costs on Russia isn't working and to stop the act, not the actor.

An official report on the hacking that took place during the 2016 elections identified the Main Intelligence Directorate operatives as APT28. Ukraine blamed this group for the outbreak of BadRabbit ransomware in Eastern Europe at the end of last October, but the incident received little attention in the mainstream press except for a few technology columns. That lack of attention was probably because the target was Ukraine, including the Kiev Metro and Odessa Airport. The APT28 ransomware encrypted files and demanded 0.05 Bitcoin (worth roughly $280) as ransom for a key to unlock computers.

BadRabbit appeared not long after the NotPetya Ransomware struck computers in more than one hundred countries in June 2017. It differed in extorting money, while NotPetya wiped out data. Researchers determined that BadRabbit was compiled from NotPetya source code with additions. That meant the same authors, namely Russian hackers, most likely committed both of the attacks, though their incentives vary. The obvious BadRabbit strike could have been

a smokescreen for quiet attacks to obtain financial and proprietary information, where NotPetya disrupted energy, telecom and commercial industries in Ukraine to spread panic among the people, which also caught other nations in the crossfire.

Large companies outside Ukraine were hard hit by NotPetya. The shipping giant Maersk and FedEx TNT Express experienced falls in their volume of business of almost three hundred million dollars each. Maersk was forced to use WhatsApp on personal telephones once email services went down and Merck also incurred costs because of shutting down production of adult and pediatric vaccines, which may cause loss of innocent life. The decision to conduct ransomware attacks might have been aimed at achieving regional goals, but their indiscriminate impact had global repercussions. If Russia continues to make such choices sole based on internal benefits, then clearly a more effective way is needed to deny the benefit of the act.

The problem with defeating cyberattacks is that speed and number of threats outpace human-centered cyber defense. In fact, most ransomware completes encryption in under one minute after intrusion, too quick for manual intervention to counter it. Thus, organizations must automate cyber defenses to reduce the time needed to detect and respond to attacks. Moreover, these defenses must be capable of obstructing or interfering with multiple phases in an attack to guarantee success. The cybersecurity marketplace has responded with a number of solutions.

One example is the advanced endpoint device, which protects any type of Internet-capable computer hardware. In the WannaCry global ransomware attack, this device blocked processes from retrieving injected malicious code and forwarded a sample to a threat intelligence cloud to run in a confined environment. Once confirmed as mischievous, additional signatures were sent to the perimeter firewall and shared with the public. WannaCry devastated unprotected health trusts in the United Kingdom and prompted the cancellation of hundreds of surgical procedures because it hijacked screens and shut down X-ray machines and blood refrigeration units.

One example is the advanced endpoint device, which protects any type of Internet-capable computer hardware. In the WannaCry global ransomware attack, this device blocked processes from retrieving injected malicious code and forwarded a sample to a threat intelligence cloud to run in a confined environment. Once confirmed as mischievous, additional signatures were sent to the perimeter firewall and shared with the public. WannaCry devastated unprotected health trusts in the United Kingdom and prompted the cancellation of hundreds of surgical procedures because it hijacked screens and shut down X-ray machines and blood refrigeration units.

One example is the advanced endpoint device, which protects any type of Internet-capable computer hardware. In the WannaCry global ransomware attack, this device blocked processes from retrieving injected malicious code and forwarded a sample to a threat intelligence cloud to run in a confined environment. Once confirmed as mischievous, additional signatures were sent to the perimeter firewall and shared with the public. WannaCry devastated unprotected health trusts in the United Kingdom and prompted the cancellation of hundreds of surgical procedures because it hijacked screens and shut down X-ray machines and blood refrigeration units.

Automatic responses isolate or eradicate malicious software, such as ransomware, without regard for the identity or motivation of the actors. They simply halt attacks before damage is inflicted. Yet the hackers are constantly adjusting their tactics, including their type of tools they use for evasion after breaking into a system. For example, Russian hackers in the NotPetya case used the Mimikatz tool to steal login credentials, which gave them access to the typical Windows administration tools they needed to enter local systems. That is why it is important to test breach detection and mitigation capabilities that can correlate indicators of compromise in order to prove they are capable of working at the speed of cyberattacks.

The adoption of proven automated cyber defenses can thwart the objectives of attackers. And by doing so, those defenses would deny attackers any reward. The use of methods such as economic sanctions and legal indictments by the U.S. government to change behavior should continue, but to date they have not deterred Russia or hostile states

like North Korea, which do not fear failure, risk or consequences. A new approach to cyber defense is needed in order to change the cost-benefit analysis of hackers. That analysis can be altered through the introduction of automated cyber defenses, which aim to stop the act, not the actor.

Scott Jasper teaches at the Naval Postgraduate School and is the author of Strategic Cyber Deterrence: The Active Cyber Defense Option. *You can follow him @ScotJasper.*

Image: A projection of cyber code on a hooded man is pictured in this illustration picture taken on May 13, 2017. Capitalizing on spying tools believed to have been developed by the U.S. National Security Agency, hackers staged a cyber assault with a self-spreading malware that has infected tens of thousands of computers in nearly 100 countries. REUTERS/Kacper Pempel/Illustration