Issued 3/28/18

How On Earth Did Russia Hack Our Energy Systems?

Last July, DHS and FBI officials revealed that Russian hackers were behind cyber intrusions into the U.S. energy power grid. The intrusion illustrated the severe threat that hackers pose to our most critical industries - energy, finance, healthcare, manufacturing and transportation. The DHS and FBI issued a joint statement saying, 'There is no indication of a threat to public safety, as any potential impact appears to be limited to administrative and business networks.' When DHS and FBI dissected the hackers' tradecraft, it turned out to be very clever indeed. One of the attackers' main strategies is to divide targets into suppliers, even trade journals and industry websites. Instead of going straight to the larger and better-protected targets, like a $60 billion Energy Company with a cyber security department, the hackers worked their way into the smaller and less secure companies' networks like those that supply the big ones with smaller equipment. Or the local utilities that are partnered with them. Local regulators may also have good access. There is even an Electric Utility Industry Sustainable Supply Chain Alliance that many of the large energy companies use. When the hackers get into those systems, they use that access to gather intelligence and set traps for the larger company. This targeting of the supply chain partners is brilliant. The manufacturer of natural gas turbines that supply a gas power plant would have great access to the plant's systems and management, would probably have password access, and would not be questioned very hard. This is a long-term strategy that takes patience – just the kind of thing traditional espionage has perfected over the last century. America seems to be getting the message. A recent survey from Raytheon and Ponemon showed that two-thirds of cyber security executives and chief information security officers in

America, Europe and the Middle East believe cyber extortion, such as ransomware and data breaches, will increase in frequency and payout. The traps themselves are pretty imaginative. Many are based in social media. No one would suspect a cute kitten video of hiding malware. But they do. And if your co-worker is a kitten-nut, they may not hesitate to download that video without thinking that it is a trap. ‘The weakness in cybersecurity are the users themselves, those that are not necessarily computer-savvy,’ says Quinn Mockler, a young cyber security researcher at Columbia Basin College near Hanford, Washington. ‘People overall need better awareness of cyber security. Otherwise, we will be open to constant attack.’ In one example discussed by Orlando, the attackers found a harmless-looking photo on one company’s human resources site that contained valuable information - the manufacturer and model of a certain piece of control-systems equipment. That provided critical information on how the plant runs and set up the next phase of the attack - spear phishing – which is the use of customized, highly deceptive emails designed to deliver malware. Using resumés, curricula vitae, policy documents and other common messages, the hackers made reference to these control systems creating plausible, well-informed emails likely to fool someone into opening a malware-laced attachment. One was an invitation to a company New Year’s Eve party. Another common method used to infiltrate is called a watering-hole attack which plants malicious code in a place the targets trust, then waits for them to come pick it up. In the energy-sector attack, DHS and FBI found that watering holes included trade publications and informational websites that dealt with matters specific to the energy industry. The hackers corrupted those sites and altered them to contain malicious content. The targets saw no reason to suspect anything was wrong when they visited them. Fake Office Christmas Party invitations are a great way to spear phish which is the use of customized deceptive emails designed to deliver malware. Fortunately, when I responded to this invitation last December, it was real. ‘It’s a low-complexity, low-effort, high-yield attack,’ Orlando says. ‘With relatively little effort, you can target lots and lots of users.’ The best defense, he says, is for a company to monitor its own networks for signs that a user may have unwittingly stumbled into a watering-hole. Much of the malware in the energy-sector attack was designed to capture user credentials, or the digital identity of someone authorized to use a target network. Credential harvesting includes usernames and passwords, hashes or a

computer’s digital signature, often stolen through tricking someone at a false login page for a familiar site. The hackers’ spear phishing emails contained documents that ordered the target's computer to retrieve data from a server – one the hackers either owned themselves, or had commandeered. Once the hackers had the target’s credentials, they could apply techniques to reveal the password in plain text. Hackers imitated login pages themselves, planting a link that redirected users to a page whose ‘username’ and ‘password’ fields fed credentials straight to them. Orlando notes, ‘If I can come into your environment using authorized credentials, detecting that just became exponentially more difficult.’ ‘Your network isn’t just your network. It’s your network, plus your trusted partners, plus your suppliers,’ he says. ‘If you’re not mitigating risk across the entire cyber ecosystem, you’re potentially missing a very large exposure to your business.’ Since smaller companies are the hacker's first stop on the way to the bigger targets, Orlando recommends monitoring computer networks for unusual activity, installing security patches regularly, developing a response plan to disclose breaches and limit damage, and communicate up and down the supply chain on cyber security.