Teneo®

Vision

Edition 5 | 2018

Where Is The World Going? How Do We Get There First?

Editor | James Hoge

The New World of Cyber

What You Need to Know

Max Kelly, Senior Advisor, Teneo

Imagine you are CEO of a Fortune 500 company, and the year is 2016. Your Chief Security Officer (CSO) is about to give a presentation of your security posture. He is delivering a little bit of theater to convince you to fully fund his 2016 budget, plus a little more for 2017. Security budgets are hard to quantify because, at the end of the year, it's hard to show a return on investment. The CSO can't prove that the money you spent in the previous year actually prevented disasters from happening. Every year, you leave this meeting thinking "what is this money buying me?"

Your CSO starts his presentation showing how many attacks your Security Operations Center has prevented over the last year. It seems like a lot. Your CSO also touts the creation of a broad security policy compliance framework. You are now compliant with a wide variety of industry standards that you have never heard of. This was one of your CSO's bonus measures, so it's no surprise that he focused so much attention on it.

Then, here comes the money pitch. Your CSO needs a budget increase to continue this stellar performance. The IT department is not able to keep up with the aggressive operating system patch schedule that your company's aging infrastructure requires. So, that responsibility will have to move to the security operations center. It will cost a few more headcount and some migration funds, not to mention the political maneuvering that you will have to support. The Chief Technology Officer is already grumbling.

After all of this set-up, the number finally lands. The CSO announces that he can accomplish his goals next year with only a "modest" budget increase of 20 percent. This is needed to grow and to remain competitive in the salaries of your security staff. They are always being recruited away. Your CSO concludes with the confident pitch that this will protect us from everything – except, of course, Nation State actors.

For context, a Nation State actor is a hacker that works directly for, or on behalf of, a sovereign government. They are usually given significant training and support by their host government, and in some cases, are allowed to undertake criminal hacking activity in exchange for their services. In short, Nation State actors have the best training, tools and techniques and are expected to produce results; and they almost always do.

A New Era of Leaks

On August 13, 2016, a previously unknown hacking group calling themselves "ShadowBrokers" released an archive of sophisticated hacking tools, and, over the next six months, continued to release additional tools and techniques to the public. Anyone could, and still can, download the archive for free and use the tools.

Although the origin of the tools and techniques released by the ShadowBrokers can never be definitively proven, their effectiveness has been. By May 2017, code from those releases had been

used to infect hundreds of thousands of computers and had been integrated into the WannaCry ransomware, which encrypted files on companies' computers and would not release them until ransoms had been paid to criminal hackers.

On March 7, 2017, Wikileaks began publishing a series of documents and tools that it attributed to the CIA's Center for Cyber Intelligence. As of July 2017, it has released 17 archives, each containing documentation, techniques, and in some cases source code. The capabilities leaked include such things as document tracking, hacking iPhones, and using smart TVs as video and audio listening devices.

These two leaks alone, containing not just tools and documentation, but also techniques and protocols for operation, will empower a wide array of unsophisticated adversaries. Those now have access to a roadmap on how world-class hacking systems evade key security measures. What your CSO told you last year – that the company was protected from anything except Nation State actors – remains true. Then you wake up in the middle of the night realizing that everyone is now a Nation State.

How do you defend against this? You can't. Better tools and techniques are now available to prevent breaches, but system upgrades are costly and disruptive. In reality, one should question the industry's focus on the breach, which tends to ignore the full process of hacking. The very terminology, 'breaching' implies that you have to build firewalls around your company that cannot be breached. As your adversaries get better and better, you have to build higher walls to keep the 'bad' packets out. But, in the past, this has not worked well, so why continue?

A new approach would invoke a step-by-step process in which the firewalls serve as first contact with the adversary, alerting to signs of trouble – not as the ultimate line of defense. When you understand the steps a serious adversary will have to undertake before they can breach your defenses, you discover weaknesses in their process that you can exploit. The following offers a brief guide to the steps in the process of hacking and proposes a handful of important counter-measures to thwart attackers and minimize the damage from breaches.

Targeting
Hackers monitor press reporting and closely observe certain corporate activities – such as negotiations with a foreign country. Avoid press releases that divulge too much information (e.g., dates, locations, identity of key personnel) that could prompt attacks. Work with communications and public relations firms who are familiar with this sort of risk.

Reconnaissance
Attackers will unearth or purchase all manner of information – tax filings, technical data, internet traffic, and investor relations reports. Once they know all about you, they will act. Remember, the company can control what technology data is released publicly or made available by third-party vendors. Information flows can also be seeded with decoy data that detect if an attacker is researching.

Planning
Hackers will collect information to determine the easiest way to attack your company. Once they discover your vulnerabilities, they may reach out to friends who specialize in exploiting those particular vulnerabilities. Develop relationships with business partners who know how these actors communicate with one another and can identify when someone is 'asking around' about your company.

Building
Once an attacker has determined the best way to victimize your company, they will buy the appropriate servers and software to penetrate your information infrastructure. The attacker will try to obfuscate these purchases, perhaps by using stolen credit cards. Your company's security department can work with partners to gather information about the creation of infrastructure that could be used in an attack.

Experimenting
Hackers will employ various tools and techniques to determine the best way to attack. An attacker is likely to make repeated attempts with known exploits to test your company's defenses and see how your security team reacts. This is where firewalls can act as cameras to alert your personnel and begin the process of assessing the attackers' plans and true intent. The firewall will block the 'easy' attacks, but by carefully monitoring traffic across the firewall, your security team may be able to see all of the attacker's probes, even the ones the firewall can't stop.

Attack
Once an adversary has identified the company's blind spots, an attack can begin. This is the most dangerous phase for the attacker, since he has invested so much time, effort, and other resources that could all be lost if the attack is detected. To reduce that risk, attackers will often mount a simultaneous distraction (such as denial of service or known malware attacks) to divert attention from the real threat. Expect decoy attacks and persistent probes; monitor the firewall to observe these correlated attacks. The company's security forces must stay alert to diversions.

Breach
Successful attackers may gain access to one or more computers in a company's network. The security industry blankly labels this a 'breach' and encourages a panicked response. However, without expansion or lateral movement, such a breach likely only constitutes a small foothold in your network, warranting a calmer approach. If you can detect the breach, you may be able to see where it might go from there and take measures to contain it before the attacker is able to access any sensitive information. Partnering with a highly-skilled operational security partner can help a great deal, as they can help you see the initial breach, understand how the attackers are likely to move laterally, and take steps to extricate the attackers from your network.

Exploration

When one machine in your network has been compromised, it will be used to compromise others. Expanding the infection to move laterally in your network, an attacker will explore and identify your company's most valuable data and resources. Very often, an attacker's assessment of what data is most valuable will differ considerably from the conclusions your company reached in its own risk assessment. Knowing what an attacker considers valuable will help focus your security team's attention and effort on the direction the lateral movement is most likely to follow.

Exfiltration

Once the attackers find valuable data, they will work to get it out of your control. This can mean copying it in bulk out of your network, setting up services to replicate and send it to them automatically, or using your compromised machines to attack your trusted partners. This is where your 'camera' is your best asset. Every attempt to move laterally in your network will generate network traffic that is easily identifiable. The attackers are on your turf at this point, and you can generate substantive disinformation to manipulate their activities to your defensive benefit.

Loss

When hackers succeed, the innocuous breach turns into actual damage. The data or network is out of your control, and, thus, your business is out of your control. This is when you're allowed to panic. However, if you take the right steps, you should never get to this point. Working with sophisticated partners in the communications and operational security space means you should never have to contend with the damage a breach can lead to. Mitigating loss at this stage is challenging but not impossible, if you can find the right partners to work with.

The Way Forward

It is not possible to stop all hacker threats, particularly ones from Nation States. But each of the steps outlined here can produce results that change the odds in your favor and significantly reduce the risk that you will suffer serious loss.

280 Park Avenue, 4th Floor
New York, NY 10017

Teneo is a global advisory firm that works exclusively with the CEOs and leaders of the world's largest and most complex companies providing strategic counsel across their full range of key objectives and issues. Comprised of the most senior talent, we work collaboratively to solve the most complex issues. Our teams integrate the disciplines of strategic communications, investment banking, management consulting, political risk analysis, talent development, risk management, digital analytics, corporate governance, government affairs and corporate restructuring to solve for the most complex business and reputational challenges and opportunities. The Firm was founded in June 2011 by Declan Kelly, Doug Band and Paul Keary and now has more than 700 employees located in 17 offices around the world.

For more information contact teneoinsights@teneoholdings.com or visit teneoholdings.com