Statement for the Record

Richard Bejtlich

Chief Security Strategist

FireEye, Inc.

Before the

U.S. House of Representatives

Permanent Select Committee on Intelligence

The Growing Cyber Threat and its Impact on American Business

March 19, 2015

Chairman Nunes, Ranking Member Schiff, members of the Committee, thank you for the opportunity to testify. I am Richard Bejtlich, Chief Security Strategist at FireEye. I am also a nonresident senior fellow at the Brookings Institution, and I am pursuing a PhD in war studies from King's College London. I began my security career as a military intelligence officer in 1997 at the Air Force Information Warfare Center.

My employer, FireEye, provides software to stop digital intruders, with 3,100 customers in 67 countries, including 200 of the Fortune 500. Our Mandiant consulting service, known for its 2013 report on Chinese PLA Unit 61398, helps companies identify and recover from intrusions. In 2014, we conducted 226 investigations in 13 countries.

Today I will discuss digital threats, how to think about risk, and some strategies to address these challenges.

Who is the threat?

We have discovered and countered nation-state actors from China, Russia, Iran, North Korea, Syria, and other countries. The Chinese and Russians tend to hack for commercial and geopolitical gain. The Iranians and North Koreans extend these activities to include disruption via denial of service and sabotage using destructive malware. Activity from Syria relates to the regional civil war and sometimes affects Western news outlets and other victims. Eastern Europe continues to be a source of criminal operations, and we worry that the conflict between Ukraine and Russia will extend into the digital realm.

Threat attribution, or identifying responsibility for a breach, depends on the political stakes surrounding an incident.[1] For high-profile intrusions, such as those in the news over the last few months, attribution has been a priority. National technical means, law enforcement, and counter-intelligence can pierce anonymity. Some elements of the private sector have the right experience and evidence to assist with this process. Attribution is possible, but it is a function of what is at stake.

Who is being breached?

---

[1] Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," The Journal of Strategic Studies, 2014; http://bit.ly/attributing-cyber-attacks

In March 2014, the Washington Post reported that in 2013, federal agents, often the FBI, notified more than 3,000 U.S. companies that their computer systems had been hacked.[2] This count represents clearly identified breach victims. Many were likely compromised more than once.

Serious intruders target more than government, defense, and financial victims. No sector is immune. FireEye recently published two reports, showing that 96% of organizations we could observe had suffered compromise during two six-month periods.[3] The best performing sector was aerospace and defense, with "only" 76% of sampled organizations suffering a breach. All of the retail, automotive, transportation, healthcare, pharmaceutical, construction, and engineering clients we passively monitored over a six-month period were breached at least once.

In 2014, the top sectors assisted by our Mandiant consultants included business and professional services, finance, media and entertainment, and construction and engineering. Many of these attacks are driven by strategic national imperatives. For instance, we anticipate that certain foreign governments will continue to steal clean energy and biotechnology solutions, so long as their citizens suffer polluted cities and rising cancer rates. Some actors specifically target the healthcare sector. Criminal groups appear to steal data for financial gain, while nation-state hackers may steal data to improve the healthcare systems of their own countries, or to support national commercial champions.

How are victims breached?

Intruders use spear phishing, attacks against Internet-connected devices, and other methods to compromise victims. Last year we observed a rise in the proportion of phishing emails that impersonated IT staff, from 44% in 2013 to 78% in 2014.[4] The threat is going mobile as well. We recently completed a study of vulnerable mobile applications that can hijack entire devices, without the user's knowledge. We have seen malicious applications, pretending to offer banking services, harvest credentials and steal two-factor authentication codes and virtual private network passwords.

---

[2] Ellen Nakashima, "U.S. notified 3,000 companies in 2013 about cyberattacks," Washington Post, March 24, 2014; http://www.washingtonpost.com/world/national-security/2014/03/24/74aff686-aed9-11e3-96dc-d6ea14c099f9_story.html

[3] https://www.fireeye.com/blog/executive-perspective/2015/01/the_maginot_linedee.html

[4] https://www.fireeye.com/blog/threat-research/2015/02/get_a_view_from_the.html

How do victims learn of a breach?

In 70% of cases, someone else, likely the FBI, tells a victim about a serious compromise. Only 30% of the time do victims identify intrusions on their own. The median amount of time from an intruder's initial compromise, to the time when a victim learns of a breach, is currently 205 days, as reported in our 2015 M-Trends report. This number is better than our 229 day count for 2013, and the 243 day count for 2012.[5] Unfortunately, it means that, for nearly 7 months after gaining initial entry, intruders are free to roam within victim networks.

Why are intruders successful?

Skilled adversaries take a campaign approach to their mission, with discrete, measurable objectives. They plan their approach, take the initiative, and enjoy freedom of maneuver. If they encounter obstacles, they adapt as necessary. If phishing fails, they exploit an Internet-facing computer. If their primary target resists compromise, the intruders attack a trusted third party. Once they have a foothold in the target's network, they apply anti-forensic tactics to obscure evidence that would reveal their activities. The actions of a small group of intruders can occupy the analysis and response time of hundreds or thousands of security professionals in dozens of companies. Finally, intruders enjoy concrete measures of success. They know they have accomplished their mission when they steal, change, or destroy the data they seek.

What is the answer?

Before talking about solutions to digital risk, we need to define it. Always ask "Risk of what?" Are we talking about the risk of a teenager committing suicide due to "cyber bullying," or the risk of a retiree's 401k being emptied due to electronic theft, or the risk of a week-long power outage due to state-sponsored attack?

---

[5] https://www.mandiant.com/resources/mandiant-reports/

Step one is to define the risk, and step two is to measure progress. This is exactly the role of strategic thinking, meaning the application of strategies, campaigns, tactics and tools to achieve organizational goals.

For example, a company may worry about the risk of losing intellectual property to foreign hackers. The board and management team works with the chief security officer (CSO) to define a company goal of minimizing loss due to digital intrusions. To accomplish the goal, they agree on a strategy of rapid incident detection and response. To achieve the strategy, the CSO develops a campaign to hunt for intruders in the company using network security monitoring (NSM) operations. To prosecute the campaign, the security team implements tactics to collect, analyze, escalate, and resolve intrusions based on NSM principles. Finally, the security team uses tools, or security software, to bring their tactics to life.[6]

To measure success, the security team should track the number of intrusions that occur per year, and the amount of time that elapses from the initial entry point to the time of discovery, and from the time of discovery to the removal of the threat. This strategic approach is the reason Mandiant calculates these metrics when helping breach victims.

Security professionals define Risk as the product of Threat, Vulnerability, and Cost, which is the impact of a security incident. We use a pseudo-equation where R = T x V x C. We're not trying to calculate a number. We're trying to show how Threat, Vulnerability, and Cost influence Risk. If any factor increases, Risk increases, and if any factor decreases, Risk decreases. We appear to live in an environment where Threat, Vulnerability, and Cost continue to rise, driving up Risk, but note that reducing any component -- Threat, Vulnerability, or Cost -- helps lower Risk.

Too often the more engineering-focused members of the security community fixate on Vulnerability. We hear of "game-changing technologies" promising to remove flaws, reduce attack surfaces, and so on. While I accept the need for more secure software, we must not neglect the role of reducing the Threat and the Cost they impose.

---

[6] http://taosecurity.blogspot.com/search/label/strategy

It is very expensive to fight tactical and tool-based battles, when intruders define the time, place, and nature of the engagement. Only a handful of organizations can attract, motivate, and retain the skilled individuals who know how to detect and respond to campaign-level intrusions. Even fewer security companies and government agencies can field teams to assist victims. We cannot win if we play to the enemy's strengths. We must harness broader forces at the strategic level and operate where we have advantages over the adversary.

Law enforcement and counter-intelligence operations are the primary means by which we can mitigate the Threat. In an editorial for the Brookings Institution titled "Target Malware Kingpins," I asked "what makes more sense: expecting the two billion Internet users worldwide to adequately secure their personal information, or reducing the threat posed by the roughly 100 top-tier malware authors?"[7] Along those lines, I applaud the FBI's recent announcement of a $3 million bounty for information leading to the arrest of a Russian hacking suspect who stole more than $100 million since 2011.[8]

Reducing the Cost of security incidents takes somewhat more creative approaches. One step in progress is the "tokenization" of the payment card system, whereby strings of numbers, or "tokens," replace traditional credit card numbers. A second step would be eliminating the value of Social Security numbers to identify thieves. I recommend reading the Electronic Privacy Information Center's suggestions on "effective SSN legislation" for policy changes.[9]

In brief, defenders win when they stop intruders from achieving their objectives. It's ideal to stop the adversary from entering the network, but that goal is increasingly difficult. If traditional defenses fail, you must quickly detect the intrusion, and respond to contain the adversary, before he steals, changes, or destroys the data or system under attack.

The time to find and remove intruders is now. If a company hired me to be their CSO, the first step I would take would be to hunt for intruders already in the network.

I look forward to your questions.

---

[7] Richard Bejtlich, "Target Malware Kingpins," The Brookings Institution; http://www.brookings.edu/research/opinions/2015/02/02-cybersecurity-target-malware-kingpins-bejtlich

[8] http://www.fbi.gov/wanted/cyber/evgeniy-mikhailovich-bogachev

[9] https://epic.org/privacy/ssn/