neustar // Blog

Cybersecurity & Performance Blog

The Shape of Cyberthreats to Come: Rodney Joffe Speaks on 2015

by Nikitas Magel January 08th, 2015

2014 was a year rife with news of large-scale security breaches of high-profile, global organizations. JPMorgan, eBay, Home Depot, the European Central Bank, and the U.S. Postal Service all appeared in headlines as targets of cyberattack. The most recent—and perhaps most prominent—victim was none other than Sony Pictures, whose breach precipitated both embarrassing publicity and scandalous fanfare befitting of the film industry through which it sent the deepest ripples. The event even created some diplomatic tension between the U.S. and North Korea, whose government is still being fingered for the attack. All told, the year certainly ended with a bang.

Which raises the question: after all that cyber scandal, what more could possibly be in store for 2015? To answer that, I turned to Neustar's resident expert, Senior Vice President and Fellow Rodney Joffe, who shared some intriguing assessments about the current landscape of cyberthreats. Setting the tone for our discussion was his sobering point that "at some point every company will be compromised" (even a company like Neustar, ironically and in spite of our expertise in cybersecurity).

From there, Joffe outlined several trends as being ones to watch in the coming year…

Currently covert compromises will surface as overt attacks.

One sobering reality Joffe shared is that "90 to 95 percent of companies have already been compromised." That's because before they launch an attack on a company, cyber criminals spend a great deal of time conducting reconnaissance, quietly burrowing into a firm's databases, patiently stealing sensitive information, and ultimately deciding which of it to expose and how. Many of these current compromises will come to the surface through media reports in 2015.

DDoS attacks will grow more common again.

Until recently, distributed denial of service (DDoS) as an attack technique was considered somewhat outdated. But against a carefully chosen victim, it can have tremendous impact. The attack on the gaming divisions of Sony and Microsoft, by a group now known as the Lizard Squad, is a prominent example of this strategy. Timed right at Christmas, it compromised the PlayStation and Xbox Live networks at the cusp of their prime selling season, causing significant damage to finance and reputation. The sheer volume of traffic in these attacks (1.2 Tbps of bandwidth), was unlikely to be mitigated, Joffe said, even for a company like Neustar.

Joffe stated that similar DDoS attacks will very likely occur throughout 2015, continuing to exact a high toll and actually increase in incidence. In addition, DDoS will be increasingly used as a foil and precursor to actual data breach, confirming that DDoS is actually a mainstream technique favored among hacktivists, cybercriminals, and perhaps even nation states with a political agenda.

Attacks will have smaller payload—but larger impact.

Cyberattackers are learning that large attacks, per se, aren't really necessary to exact the greatest damage. As deep and invasive as the attack on Sony's film network was, Joffe said, "it was the exposure of only a few private emails that caused the most damaging publicity"—both in and outside of the company. The result: a huge blow to the company's stock price. Attackers in the coming year will likely learn from this and launch more subtle forms of attack, choosing their payload for maximum damage at minimum effort. This also suggests that "cybercriminals are becoming increasingly sophisticated in their strategies, stealing what amounts to insider information from a company and leveraging it to manipulate and even benefit from the stock market."

The industrial Internet will be increasingly targeted.

The Internet of things is becoming a pervasive reality, linking more of the devices and systems we use on a daily basis. But while their interconnectivity makes these systems more effective, efficient, and convenient to operate, it also makes them more vulnerable. That may not be cause for concern, said Joffe, "when talking kitchen appliances, but it can be deeply troubling for critical infrastructure systems" such as utilities, aviation, or medicine. Core functions of nuclear power plants and turbines, major dams, or centralized water facilities, to take just a few examples, are increasingly controllable though portable wireless devices. When connected to a network, they become more vulnerable to a single attack that can affect millions of people.

Yet even as increasingly more of our everyday devices are connected, Joffe pointed out, an attack on an otherwise innocuous system could have an comparably devastating effect. He used the example of internet-connected private home thermostats (such as Nest), which if hacked to suddenly increase demand simultaneously over a large geographical area, could bring the power grid to its knees. While those devices in particular aren't ubiquitous (yet), there is plenty of opportunity for other systems to be affected, many of whose interconnectivity we're unaware. Ominously, Joffe speculated that 2015 is not at all too soon for us to experience the catastrophic result of such a breach: a massive explosion, an jetliner crash, a wide area traffic disaster, a sabotage of life-sustaining medical devices.

Nation states will aggressively target western companies for financial gain—or financial destruction.

It's no revelation that China has a behemoth workforce and economy but isn't so big on innovation. To fill that void, said Joffe, "the Chinese buy companies—and resort to stealing sensitive trade secrets." As a prime example, he cited last year's court case wherein a California engineer was convicted of stealing proprietary information from DuPont Company and selling it to a Chinese firm. "This industrial espionage occurs quite frequently," said Joffe, "but few companies are aware of it because much of it is conducted through surreptitious cyberattacks." The Obama administration itself, as reported in Bloomberg, has stated that "Chinese spy agencies are involved in a far-reaching industrial espionage campaign targeting biotechnology, telecommunications, clean energy and nanotechnology industries."

U.S. banks are another area where a hostile nation state may take advantage. Exploiting the industry's vulnerability of being almost entirely interconnected and online, a piece of malware unleashed into credit card systems, ATMs, inter-company transfers, or payment systems could bring the country's entire financial infrastructure to a grinding halt. Because the supply chains of every single industry depend on the smooth and rapid functioning of the financial sector, a disruption of that magnitude would unleash a cascade of interdependent events bringing the whole country into a catastrophic state from which it would be nearly impossible to get out. Even more chillingly, in modeling this scenario during an exercise recently with White House staff, Joffe was able to show that such an event could occur in only 72 hours.

Counterintuitively, this type of large-scale attack is unlikely to come from a high profile group like Al Qaeda, nor even from a country with whom we have discordant relations, such as China or Russia—quite simply because these entities depend heavily on western infrastructure and/or the U.S. economy to function. Rather, Joffe said, an attack of this magnitude "would come from a rogue group such as ISIS, or even a lone wolf, who seeks the wholesale destruction of western governments and economies."

In the end, any company or agency with an online presence is vulnerable. Exacerbating that vulnerability, Joffe pointed out, is the tendency for organizations to spend the majority, if not the entirety, of their cybersecurity resources on merely protecting themselves against attack, allocating very little to repairing the damage once it has happened. But mitigation is just as much about cure as it is about prevention. A savvy strategy is one that presumes that cyberattack will happen, minimizes opportunities for breach, and takes preemptive steps to control damage once it's done.

ddos protection, it security