Top 8 Security Predictions for 2014.

In 2014, you should expect attackers to focus more on psychology than technology, and target your weakest link—the user.

In 2014, you should expect attackers to focus more on psychology than technology, and target your weakest link—the user. After all the headline-grabbing cyber attacks last year, don't you wish you could gaze into future headlines and project the next big cyber threat for this year? While we may not have that superpower just yet, we can make our 2014 security predictions. At the end of every year, our Professional Partner WatchGuard Technologies reflects on the threat landscape and analyzes past information security incidents, in order to forecast this year's security trends and major threats. Their hope is to provide a little insight into the future, so you can prepare your defenses in advance.

Last year was quite eventful, from NSA leaks to a huge Adobe data breach, and we expect the fast pace of security incidents to continue to grow this year. Here's a quick high-level list of WatchGuard's eight security predictions. Want more detail… keep scrolling down to the bottom for a complete breakdown of each topic:

1. Hackers Harass U.S. Healthcare Hangout – WatchGuard anticipates that the U.S. HealthCare.gov site will suffer at least one data breach in 2014.
2. Increased Cyber Kidnappings Raise Attacker Profits – In 2014, WatchGuard expects many other cyber criminals will try to copy CryptoLocker's success by mimicking its techniques and capabilities.
3. A Hollywood Hack – In 2014 a major state-sponsored attack may bring a Hollywood movie hack to life that exploits a flaw against critical infrastructure.
4. Bad Guys Break the Internet of Things (IoT) – Next year, WatchGuard expects white and black hat hackers to spend more time cracking non-traditional computer devices such as cars, watches, toys and medical devices.
5. 2014 is the Year of Security Visibility – WatchGuard anticipates that in 2014 more organizations will deploy security visibility tools to help identify vulnerabilities and set stronger policies to protect crucial data.
6. A High-profile Target Suffers a Chain-of-Trust Hack – As advanced attackers go after harder targets, expect to see more "chain-of-trust" cyber breaches in 2014, where hackers hijack partners in order to gain access to high level organizations.
7. Malware Gets Meaner – Plan for an increase in destructive viruses, worms and Trojans in 2014.
8. Network Attackers Become Cyber Shrinks – In 2014, expect attackers to focus more on psychology than technology, with techniques like convincing phishing emails and leveraging pop culture, to target the weakest link – the user.

You can also download the entire predictions infographic or read the press release here.

In-Depth Review:

Hackers Harass U.S. Healthcare Hangout – WatchGuard anticipates that the U.S. HealthCare.gov site will suffer at least one data breach in 2014.Between its topical popularity, and the value in its data store, Healthcare.gov is an especially attractive cyber attack target. In fact, this has already happened to some extent. Security researchers have already pointed out minor security issues like evidence of web application vulnerabilities and an attempted Denial-of-Service (DDoS) attack.

The Deep Dive:The United States' (US) new Patient Protection and Affordable Care Act (PPACA), colloquially known as Obamacare, hinges on the use of online healthcare insurance exchanges, which are essentially cyber marketplaces where patients can purchase healthcare at discounted group rates. Healthcare.gov is the glue connecting US citizens to all the state exchanges and the oracle that helps you navigate your way through the new healthcare and health insurance process. Unfortunately, its key position also makes Healthcare.gov an especially attractive cyber attack target in 2014.

First, as the online cornerstone of the new US healthcare system, heathcare.gov will certainly garner a lot of attention over the next year. It is already the topic of heated political debate, which puts it in the news quite regularly. This increased media coverage will certainly draw the attention of white and black hat hackers alike. Imagine you're a hacktivist trying to make a big political message… what better place to capture the notice of millions?

Second, in order to do its job the site needs to ask citizens for some pretty personally identifying information (PII). For instance, you have to share your social security number with the site for identity purposes. This makes Healthcare.gov, and all the online exchanges under it, a pretty important overseer for some pretty sensitive data, which obviously also makes it an attractive target to malicious hackers.

Between its topical popularity, and the value in its data store, we believe both good and bad hackers will target Healthcare.gov in 2014. None of this is to say you should avoid healthcare.gov, or that it's any worse than any of the millions of other websites we share our valuable data with. In fact, its current high-profile means that the folks managing it will likely focus heavily on its defense. We'd argue that in time the Healthcare.gov will likely be more secure than the majority of sites out their. However, we also know things sometimes have to get a bit worse before they get better. That's why

we forecast that Healthcare.gov will suffer at least one data breach in 2014.

Increased Cyber Kidnappings Raise Attacker Profits – Ransomware, a class of malicious software that tries to take a computer hostage, has grown steadily over the past few years, but a particularly nasty variant emerged in 2013: CryptoLocker. This year, it has affected millions and it is suspected that the authors have made a high return in their criminal investment. In 2014, WatchGuard expects many other cyber criminals will try to copy CryptoLocker's success by mimicking its techniques and capabilities. Plan for a surge of ransomware in 2014.

Criminal hackers are always looking for surprising new ways to increase their profits. Ransomware is a class of malicious software that tries to take your computer hostage, or "kidnaps" your important files; making it so you can't access your data or use your computer. Criminals then try to extort you for a relatively small sum of money in order for you to regain access to your computer or its files.

But, a particularly nasty variant emerged in 2013 – Cryptolocker. It arrives in various ways, including as an attachment to a phishing email, or through websites hosting malicious drive-by downloads. It encrypts many of your important files, including Office documents, pictures, and digital certifications. Then it tries to get you to pay $300 to get them back.

However, Cryptolocker is much smarter and much more aggressive in its techniques. It uses industry-standard encryption to ensure you can't reclaim your files; it uses domain generation algorithms (DGA) to make sure it can always reach its master, and it uses Bitcoin to make it harder for authorities to track these illegal payments. In short, Cryptolocker has affected millions and we suspect its authors have made quite the return in their criminal investment.

A Hollywood Hack – In 2014 a major state-sponsored attack may bring a Hollywood movie hack to life that exploits a flaw against critical infrastructure. Even if these systems are kept offline, the often-cited Stuxnet proved that motivated cyber attackers could infect non-networked infrastructure, with some potentially disastrous results.

You've seen it in the movies. A big hack that drains the Federal Reserve Bank, shuts down power in all the big cities, or causes a critical dam to fail and flood a town downstream. These types of cyber attacks sound like science fiction, and so far they have mostly stayed in that realm. However, our critical infrastructure really does rely on computers and—despite best practices saying otherwise—we are slowly putting some of this infrastructure online.

As a result, researchers have spent the past few years discovering and studying the vulnerabilities in industrial control systems (ICS) and supervisory control and data acquisition (SCADA) solutions, and their findings aren't great… These systems have many holes.

We think a malicious actor or nation-state might realize a Hollywood-like hack next year, by exploiting a flaw against critical infrastructure.

Bad Guys Break the Internet of Things (IoT) – There are computers in everything!

Ok… Not literally, but some days it sure seems that way. We have computers in our cars, pace makers, televisions, watches, kids toys, cameras, baby monitors, and we are even trying to strap them to our head inside a pair of eyeglasses. Furthermore, most of these non-traditional computers include all kinds of interesting, information gathering sensors, including GPS, accelerometers, altimeters, photodetectors, and good old fashion cameras (video and still). Finally, most of them can connect wirelessly, and they treat security like an afterthought.

When you add this all up, it's like Christmas for hackers – white hat and black hat alike. The Internet of Things (IoT) provides a playground of connected devices for curious and malicious computer experts to have fun with. Want to make a car think it's flying? You can! How about trolling a baby over the Internet? It's been done. However, things can also take a dark turn as well, with an ex-vice president disabling his implanted defibrillator's wireless feature to avoid assassination.

Security experts have warned about securing the IoT for a while now. However, the market is just now catching up with the expectation, with more and more embedded computing devices showing up in stores everyday. Next year, WatchGuard expects white and black hat hackers to spend more time cracking non-traditional computer devices such as cars, watches, toys and medical devices. While security experts have warned about securing these devices for the past few years, the market is just now catching up with the expectation. WatchGuard suspects that good and bad hackers will focus heavily on finding holes in these IoT devices in 2014.

A High-profile Target Suffers a Chain-of-Trust Hack – Cyber attackers have clearly gotten more sophisticated over the years; especially those associated with state-sponsored hacking. These advanced hackers also target a higher level of victim, regularly going after government and military organizations, critical infrastructure providers, and Fortune 500 businesses.

These top-level victims tend to have a higher security pedigree, and do NOT pose soft targets. Yet, they still can fall to the persistent, advanced attacker who preys on the weakest link in a victim's chain of trust—your partners and contractors.

In many of the most sophisticated attacks, bad actors had to first infiltrate secondary or tertiary targets in order to gain access to some asset needed

to compromise the intended victim. For instance, hackers targeting Lockheed Martin first needed to steal SecureID seed data from RSA (and their ultimate target may have been the US military, a customer of Lockheed Martin). We're also seeing more and more cases where attackers hijack digital certificate providers, or steal the certificates from smaller companies, for use in a more specific targeted attack.

As advanced attackers go after harder targets, expect to see more "chain-of-trust" cyber breaches in 2014, where hackers hijack partners in order to gain access to high level organizations.

Malware Gets Meaner – Whether it's because we are more paranoid than the average bear, or just plain tinfoil hats, security professionals often like to imagine worst-case scenarios. You know, scenarios like some doomsday malware that deletes everyone's hard drives, launches the world's complete arsenal of nuclear weapons, and evolves into an evil, self-aware "Skynet" to enslave humankind.

While often amusing to imagine, and sometimes even theoretically possible, these worst-case scenarios are rarely seen in the real world. Most cyber attacks and malware are not purposely destructive. If you think about it from the attacker's perspective, it typically just doesn't make sense to destroy your victim's resources. If you destroy your victim's computer, you can't spy on them and gain access to other resources. Not to mention, you also give yourself away.

However, changes in hacker profiles have resulted in more cases where cyber destruction might become a valid goal for network attackers. For instance, hacktivists or nation-states actors who want to send a brash message, or to disable an adversary's systems, may turn to destructive attacks; like the case of the disk wiper malware seen in a South Korean attack. Cyber criminals may also realize the threat of imminent destruction could help increase cyber extortion success rates, as seemed to be the case with the countdown timer Cryptolocker used scare victims into compliance.

Whatever the reason, we think malware will get meaner in 2014, and you can expect to see more cases of destructive malware and attacks.

Network Attackers Become Cyber Shrinks – The information security battle has always been like a pendulum, with the technical advantage swinging back and forth between the attacker and defender. As defenders develop new security technologies to get the leg up, attackers develop new evasion techniques and reclaim advantage—the cycle goes on ad infinitum.

Over the last few years, the attackers have had the advantage; leveraging more sophisticated attack techniques and using advanced evasion tactics to get past legacy defenses. However, the tide is turning. Next year, defenders will have more access to next generation security solutions and new advanced threat protection capabilities, swinging the technological security pendulum back in our direction.

While that's good news, don't expect cyber criminals to give up that easily; rather expect them to change their strategy. There are two ways attackers can compromise our networks; they can exploit technical weaknesses or they can prey on sociological ones. As we regain the technical advantage, expect cyber criminals to refine their social engineering skills, and concentrate more on attacking flaws in human nature. In fact, they've already done a good job in this area. Their phishing emails are better written and more convincing, they're masters at leveraging pop culture, and they know our worst habits.

2014 is the Year of Security Visibility – In the past few years, cyber attackers have successfully breached many big companies, despite the victims having common security defenses, like firewalls and antivirus. Furthermore, many of these victims didn't even realize they were compromised until it was much too late.

So what's the problem? Do our cyber security controls not work or are we doing something wrong? We think the issue is threefold:

Most businesses still rely on legacy defenses, such as stateful packet filtering firewalls, which don't help against today's threats. They don't configure their security controls properly, and often don't enable their best defenses, or accidentally bypass them. (In fact, Gartner says 95% of firewall breaches are due to misconfigurations), And they are drowning in oceans of security logs, making it impossible for them to recognize the important security events that they need to react too. WatchGuard anticipates that in 2014 more organizations will deploy security visibility tools to help identify vulnerabilities and set stronger policies to protect crucial data. Expect 2014 to be the year of security visibility.

In 2014, you should expect attackers to focus more on psychology than technology, and target your weakest link—the user.

LogicalTech is one of the leading Professional Partner with WatchGuard Technologies in Australia. Find out more by contacting an authorized WatchGuard reseller, LogicalTech today. This Top 8 Security Predictions for 2014 information release is submitted by Cassidy Poon, National Marketing Manager for LogicalTech Group and on behalf of our Professional Partner, WatrchGuard Technologies. Cassidy Poon is one of Australia's leading technology media publicist for B2B Enterprise Technology Media.

Contacts

Cassidy Poon
0386436448
mailto: cassidyp@logicaltech.com.au