WatchGuard®

2016 SECURITY PREDICTIONS

TABLE OF CONTENTS

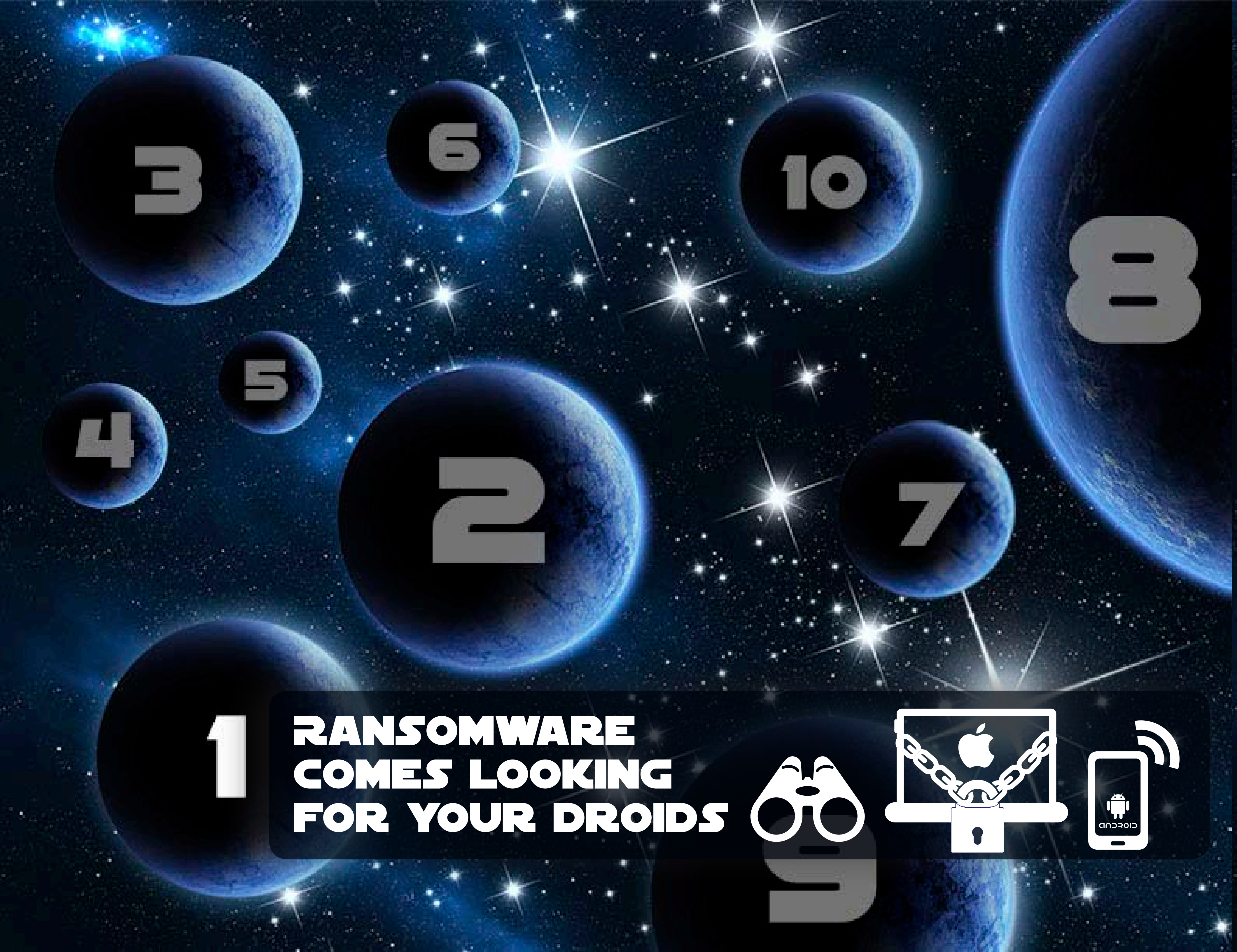
The start of the new year brings many exciting new opportunities, and as the past has proven, the security threat landscape will constantly change and present new information security challenges ahead.

At the end of each year, WatchGuard's security team spends some time imagining what the threat landscape might look like in the coming year. This gives us the opportunity to analyze the security trends we've followed over the past year, and allows us to creatively extrapolate what might happen next. Though our predictions don't always hit dead on – they are based on very real security trends, which means they can help you prepare your defenses for 2016's upcoming threats.

This year, I've come up with ten predictions covering a wide variety of security threats and trends that will impact many organizations. As 2015 comes to a close, let's explore some of the new security threats we may see in the coming year. New and emerging trends that criminals may deploy, using old and new methods to expand reach, exploit users and gain access to valuable data.

– **Corey Nachreiner**, CTO, WatchGuard

For more in-depth security news and analysis, please visit the **WatchGuard Security Center blog**



1 RANSOMWARE COMES LOOKING FOR YOUR DROIDS

1. RANSOMWARE COMES LOOKING FOR YOUR DROIDS

PREDICTION 1
RANSOMWARE COMES LOOKING FOR YOUR DROIDS
CYBER CRIMINALS REACH NEW PLATFORMS

Cyber Criminals Reach New Platforms:

The first prediction focuses on **ransomware**, which has really taken off over the past three years. Ransomware has evolved from relatively feeble policeware variants like Reveton to extremely effective cryptoware samples like Cryptolocker and Cryptowall.

Unfortunately, these new strains of file encrypting malware are so good at their evil jobs that many victims have paid the ransoms. FBI agents have even **gone on record** recommending victims pay up. Our acquiescence to this cyber ransom will only ensure that victims continue paying up in 2016. Proving to cyber criminals that this practice works, so expect them to up the stakes and continue refining their cryptoware techniques next year.

We expect the evolution in two main categories:

- **Targeting of wider platforms** – Right now, ransomware primarily targets Windows victims. We've seen Mac, Linux, and Android samples, but those haven't had much success yet. Next year, we expect this will change, and that cyber criminals will make very effective ransomware for alternate platforms; especially for Android mobile devices and Mac laptops.

- **Refinement of the extortion techniques** – Now that cybercriminals have figured out victims are willing to pay for lost files, we suspect they'll start to develop nasty new methods to tighten the screws on victims. Next year, expect them to target specific business files or other critical information. For instance, in the past they've encrypted web server files to temporarily take down a web server. Yet, imagine if they targeted password managers, thus preventing you from logging on to anything, or worse yet, if they targeted the SCADA systems used to run critical infrastructure. We also think they'll up their psychological pressure by threatening to release your embarrassing files to the public or by harming your reputation in some other way.

In short, Crypto ransomware will get even worse in 2016, and will become more effective at stealing millions from Android and Mac users as well.

2. IT'S A TRAP!

Social Engineering Keeps People as Your Biggest Threat:

Security professionals spend a lot of time trying to plug the technical security gaps in their organization's IT infrastructure. We find and fix software vulnerabilities, tighten our network security controls, and monitor the latest malware samples and exploits to try and ensure a hacker can't leverage them against our systems. However, if you look at most of the advanced network breaches over the past few years, they have one thing in common –and it's not technical. They all started with spear phishing, which is a social, user issue.

Let's hypothetically assume you could fix every technical security problem a network faces. Your software is perfect, your network only allows the things you want, and your access controls only let people you know access the things they need. Would this prevent all attacks? No. Rather, bad guys would simply change their focus and instead try to trick one of your trusted users into doing something they shouldn't, in hopes of gaining that user's privileges.

Cyber criminals have realized this over the last few years, as our defenses have gotten more advanced. To counter our technical defense, they have increased the reconnaissance capabilities and started to target our specific users with very convincing and customized social engineering. Next year, we believe this trend will grow; and many of the breaches will start with a targeted attack on your organization's users.

3 SMBS CAN'T LET BASIC SHIELDS DOWN

3. SMBS CAN'T LET BASIC SHIELDS DOWN

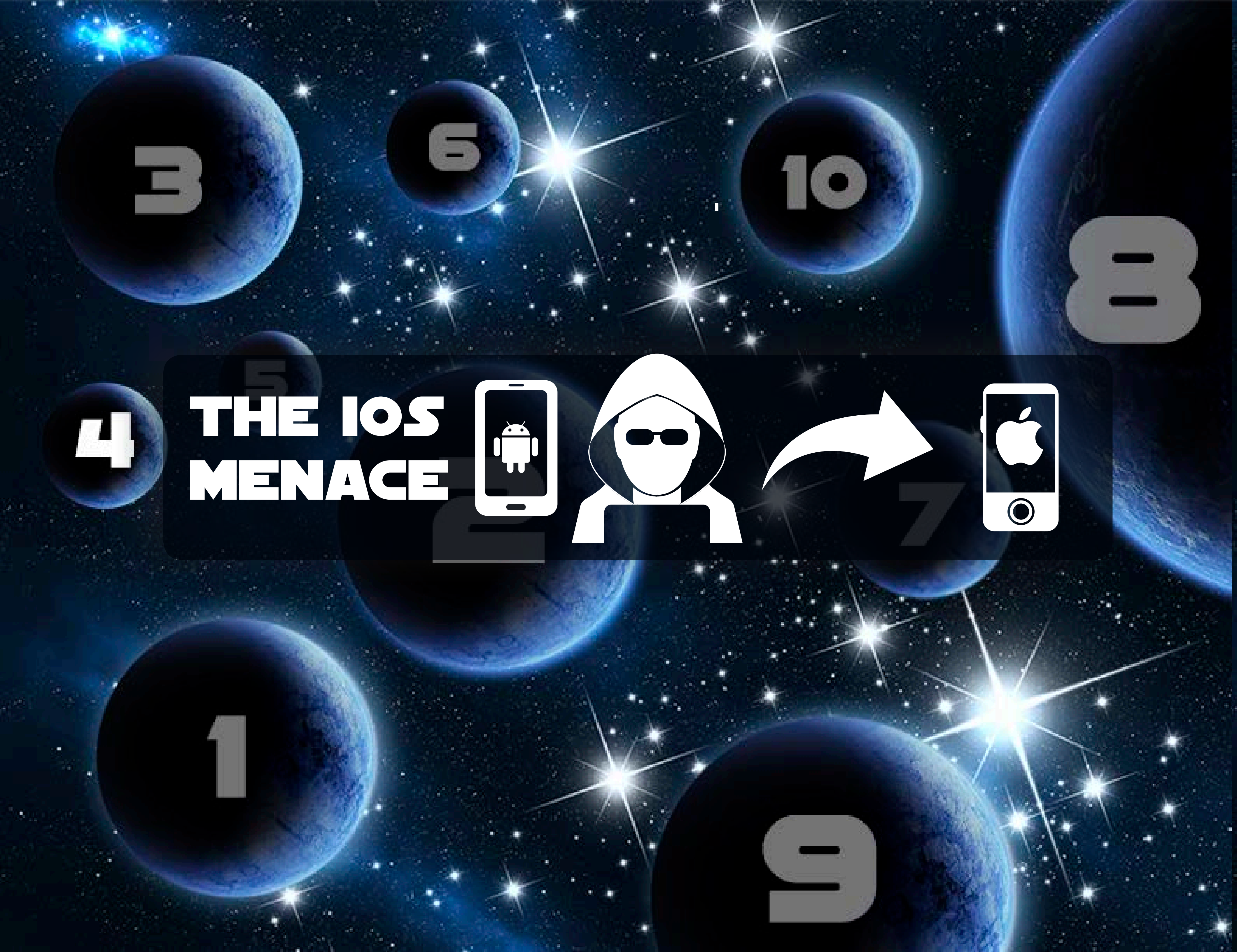
PREDICTION 3
SMBS CAN'T LET BASIC SHIELDS DOWN
SECURITY BREACHES GO BACK TO BASICS

Security Breaches Go Back to Basics:

Security experts often focus on the latest and greatest progressions of the threat landscape. They're most interested in sharing how threat actors have become more sophisticated and how attack technology, malware, and techniques have evolved significantly. They warn that the latest attacks bypass or evade many of the industry's original information security defenses.

While none of that is false, the truth is a huge majority of successful attacks—especially ones against smaller targets—still rely on the basics. Many successful cyber-attacks last year exploited software flaws that had been fixed for months, took advantage of bad or default passwords or bad password practices, or just tricked users into doing something basic that they shouldn't do. Despite the fact that some threat actors really are using very sophisticated techniques, we predict the majority of small to medium businesses (SMBs) will experience security breaches next year that will succeed due to a basic security best practice failure, such as not keeping your software up to date or not using very basic security controls like Gateway Antivirus (GAV) or Intrusion Prevention Services (IPS).

There is a silver lining to this prediction, though. If you concentrate on following basic security best practices, your organization can avoid a majority of the attacks that will launch in 2016.



4. THE IOS MENACE

Malware on iOS Will Rise:

Experts have been predicting the growth of mobile malware for years. We've covered how the increase in mobile device usage has led to an increase in criminal attention. We've predicted how the inclusion of mobile wallets, using NFV and RFID technology, would lead to attackers targeting the mobile payment vector. We've even talked about how Google's open developer and consumer strategy translates to more threats against Android devices, since it's an easier platform for criminals to infiltrate. However, through all these trends one thing has remained the same—Apple iOS has not seen that many threats. Next year, we expect this to begin to change, and for attackers to launch more attacks against iOS users.

Underneath the surface, iOS devices are not technically more secure than their Android brethren. They're still just mini computers running software. Researchers and black hat hackers have found plenty of vulnerabilities in iOS software before, including the **recent zero day** that can easily root an iOS device via the Web. . The difference is that Apple has retained a much tighter control of their app community than Google, making it much harder for users to install non-sanctioned apps and thus making it harder for attackers to get malware on an iOS device.

However, last year smart cyber criminals found a way around this challenge: they infected the Apple development platform by releasing a **maliciously hijacked version of Xcode called XcodeGhost**. . If Apple's own development kit builds malicious code that seems legitimate, it makes it much harder for Apple to keep it off their official App store. Though Apple has since fixed the issue that led to XcodeGhost, and has tried to educate developers about it, we believe cyber criminals will continue to exploit this attack vector to sneak malware onto Apple's official marketplaces. iOS users should prepare for more threats in 2016.

JAR JAR CAN'T RESIST ADS FROM THE DARK SIDE

5. JAR JAR CAN'T RESIST ADS FROM THE DARK SIDE

PREDICTION 5
JAR JAR CAN'T RESIST ADS FROM THE DARK SIDE
MALVERTISING INCREASES BY LEVERAGING ENCRYPTION

Malvertising Increases by Leveraging Encryption:

Malvertising, the combination of the words malware and advertising, is an attack where criminals booby-trap a legitimate, trusted website with a malicious code by sneaking it in through a third party advertising network. Unfortunately, legitimate web advertising services haven't been very discerning with the ads they allow their "customers" to upload to their networks.

As a result, criminals have paid for advertising services in order to sneak malicious code onto all the legitimate web sites that use that service. Over the past two years, this has been a very successful technique for cyber criminals to redirect innocent users browsing the web to their malicious drive-by download sites.

The good news is a number of reputation services and security products have become better at detecting malicious advertisements, and preventing your users from getting redirected to these evil sites. However, the criminals are fighting back. They have started to implement a number of techniques to obfuscate their malicious web code, including encoding their malicious JavaScript or by burying their attack in a Shockwave video file. The most recent obfuscation technique is the simplest—they serve their malicious advertisement over HTTPS.

In 2016, expect malvertising attempts to triple and for it to succeed more regularly due to its use of HTTPS. Criminals know that security products and companies are keeping on the look out for malicious ads. They also know that many security controls cannot see into HTTPS traffic. By encrypting their malvertising campaigns, they hope to bypass most detections next year.

If you don't have security controls that can monitor HTTPS, you should update as soon as you can.

JANGO FETT AND THE CLONE ARMY ARE COMING

6. JANGO FETT AND THE CLONE ARMY ARE COMING

PREDICTION 6:
JANGO FETT AND THE CLONE ARMY ARE COMING
AUTOMATION BRINGS SECURITY TO THE NEXT LEVEL

Automation Brings Security to the Next Level:

Security experts have always realized that information security is a constant arms race. Attackers discover new methods to evade defenses, we update our defenses, and the cycle continues and repeats. In fact, much of our legacy defense is reactive. It relies on us having seen a particular attack, and creating a specific defense for that particular attack. The problem is, reactive defenses do little good for new attacks.

Today's attackers have automated their attacks, ensuring they constantly evade our reactive defenses. Signature-based protection is no longer effective. While human analysts can identify new threats by monitoring for suspicious behaviors, cyber criminals release new threats in such volume that humans can't keep up. The solution? Artificial Intelligence (AI) and machine learning that can automatically recognize malicious behavior.

At a very high level, statisticians and mathematicians have begun to develop big data algorithms that can identify very complex behaviors and trends. The security industry is starting to see a new level of security controls that can proactively find new threats in real time, without human interaction. We'll always be one step behind the latest attack, so these more proactive security technologies are the only way we might stop the newest threat.

Expect 2016 to be the year of machine learning and behavioral detection security controls. Look for defenses that are proactive, technologies like APT Blocker that automatically identify malware and threats based on behaviors and not just on static patterns.

7. STARFLEET ACADEMY TARGETED

PREDICTION 7
STARFLEET ACADEMY TARGETED
CYBER CRIMINALS GO BACK TO SCHOOL TO GET DATA

Cyber Criminals Go Back to School to Get Data:

Information security is all about protecting data, because at the end of the day, stolen data is what makes the cyber criminals rich. Criminals started with the basics. Monetizing stolen credit card (CC) information was easy. You just needed the basic CC information and a few personal details to make a purchase with a stolen card. We saw this in 2014—the Year of the Retail Breach—as cyber criminals stole millions of CC records through point-of-sale systems.

However, as fraud systems got better, making false CC purchases became harder and today stolen CC information is barely worth the effort to steal it. Meanwhile, the personally identifying information (PII) required to steal a full identity has become much more valuable. PII value in the underground directly increases in relation to how many individual pieces of data you have in a corresponding set. As you can imagine: a name, email, address, CC, date of birth, and social security number (SSN) is much more valuable than just a name and email address. That's why CCs may only fetch 50 cents to a dollar on the underground, while a full set PII (which the underground calls a fullz) can bring in 10 to 20 dollars, especially since it includes an SSN. That's also why healthcare records are so valuable—they're rich in PII data and include SSNs. In 2015, we saw many attacks targeting healthcare data.

So what's even better than a healthcare record? Apparently, student records! We are learning that the amount of **data collected about our kids over their lifetime** as a student is staggering. It even includes some of their health records to boot, which is already one of the richest PII datasets. This, combined with the more open network environment found in educational facilities is why we expect cyber criminals to target student data systems in 2016.

If you manage IT for an educational facility, we recommend hardening the database server and review the web applications that tie to student data.

BREACHES COME TO THE IOT FRONTIER

8

8. BREACHES COME TO THE IOT FRONTIER

PREDICTION 8
BREACHES COME TO THE IOT FRONTIER
HIJACKED FIRMWARE ATTACKS THE INTERNET OF THINGS

Hijacked Firmware Attacks the Internet of Things:

When a hacker hijacks a computer, gaining persistence (or making sure his malicious trojan stays on the computer) is easy. The attacker just has to load malware onto the computer's hard drive and make sure it runs when the computer reboots. However, hijacking the Internet of Things (IoT) is a different story. Many IoT devices don't have local storage, and are often small embedded systems with low resources. Gaining persistence on these devices is much more difficult and may actually involve modifying the software these devices use to boot, which we call *firmware*.

Next year, we expect to see more researchers release proof-of-concept attacks that permanently modify and hijack the firmware of IoT devices. It's not enough to just find a vulnerability in these devices, you also have to figure out how to inject malicious code that can stick around.

We expect to see vendors start to harden the security of their IoT devices by implementing secure boot mechanisms that makes it more difficult for attackers to modify firmware.

9. SPIES SLIP INTO WIRELESS ALLIANCES

PREDICTION 9
SPIES SLIP INTO WIRELESS ALLIANCES
WIRELESS "EASE-OF-USE" FEATURES EXPOSE THE NEXT BIG WIRELESS FLAW

Wireless "Ease-of-Use" Features Expose the Next Big Wireless Flaw:

To be honest, wireless security hasn't changed too much in the last few years. That's not to say it's perfectly secure. There are still plenty of folks using legacy WEP encryption standards, and organizations that use WPA2-PSK with a horrible password. There are also many wireless networks that don't segment clients, so attackers can sniff plenty of private connections by hanging out on public hotspots. Furthermore, many SMB organizations haven't solved the problem of rogue hotspots or evil twin hotspots. That said, there hasn't been a huge, industry-wide wireless standard vulnerability in quite a while.

While we don't know exactly what it'll be, we suspect the next big wireless vulnerability will have to do with an "ease-of-use" feature. The **Wi-Fi Protected Setup (WPS)** standard was a great example of this possibility. WPS was designed to make it easier for new users to join a secure wireless network without having to remember a complex password. Unfortunately, it suffered from a flaw that made it easy for attackers to brute-force a WPS pin and gain access to the wireless network quickly. Unfortunately, usability features can sometimes clash with real security.

Recently, Windows included a new wireless feature **called Sense**. This feature is intended to allow you to automatically connect to secure wireless networks that your friends or acquaintances have used. While no one has found any issue with this feature yet, this is the type of feature that may introduce new wireless problems.

We expect the next wireless vulnerability to involve an ease of use feature that enables users, and hackers, to easily join a wireless network. Take this potential security issue into consideration when accessing and using wireless networks.

ALIEN ATTACKERS HIJACK OUR BROADCAST SIGNALS FROM SPACE

10. ALIEN ATTACKERS HIJACK OUR BROADCAST SIGNALS FROM SPACE

Hacktivists Take Over Broadcast Media:

Unlike cyber criminals, who want to stay under the radar, Hacktivists like to make big splashy messages. The whole point of "cyber" activism is to use technology to get as many people as possible to notice your message, whatever it may be.

Anonymous is a great example of this, with their well-known videos containing a man in a suit wearing a Guy Fawkes mask and speaking with a distorted voice over theatrical music. All of theAnonymous "operations" are designed to get noticed. Whether they're trolling the Church of Scientology, DDoSing credit card providers, defacing websites, or doxing someone they disagree with, the goal is getting attention for their cause. What better way to get attention than to hijack a live TV signal or big event?

While hacktivists are known for their attention-grabbing videos, so far they've never taken over live TV or radio, and really gotten their message across to a wider audience. Movies and TV would have us expect "l33t h@x0rs" to take over the airwaves, but so far their strange hacktivist videos have been relegated to YouTube posts anyone can do. Hacking TV broadcasts may sound like sci-fi, but there is precedent. Back in the 80s, a weird, masked man (sound familiar?) **took over a few Chicago TV stations** for a few minutes at a time. While our TV broadcast have become more protected today, the **breach to TV5Monde**—a French broadcast network—shows that attackers still have the potential to take over the airwaves.

Next year, I expect cyber attackers to pull off some hack that gets broadcast to the world live. Perhaps they'll take over a big stadium screen during the Super Bowl or World Cup; they might hijack all of the big TVs in Times Square; or perhaps they pull off the ultimate hacktivist's dream, and hijack a major TV network's live broadcast. Whatever it is, expect hacktivists to do something big that televises their revolution to the world live.

FOR MORE SECURITY NEWS, VISIT THE WATCHGUARD BLOG:

www.watchguardsecuritycenter.com

WatchGuard®