websense®

WEBSENSE® SECURITY LABS™

2015 SECURITY PREDICTIONS

websense®

2015 SECURITY PREDICTIONS

CONTENTS

HELP! CALL THE IT DOCTOR. MY HOSPITAL IS UNDER ATTACK – AGAIN!

Healthcare will see a substantial increase of data stealing attack campaigns.

According to the Identity Theft Resource Center, healthcare data accounted for 43 percent of major data breaches reported in 2013[1]. Medical records and patient data are logical targets for cybercriminals. Healthcare records hold a treasure trove of data that is valuable to an attacker. No other single type of record contains as much Personally Identifiable Information (PII) that can be used in a multitude of different follow-up attacks and various types of fraud. Healthcare records not only contain vital information on the identity of an individual (name, address, social security) but also often link to financial and insurance information. Access to PII allows an attacker to commit identity fraud, while the financial information can lead to financial exploitation. This is a logical and profitable secondary attack area for cybercriminals who have already dealt in stolen credit card data.

Healthcare professionals are also at risk. Often, they have an increased tendency to try and get around IT security policies in order to better serve their patients. In a medical emergency, the stakes couldn't be higher. When a doctor or nurse needs access to computing resources or data because a patient's health is at risk, IT policy takes a back seat to the patient's health. In the heat of the moment, such behavior can lead to increased risk to cyber threats or insecure access and storage of sensitive information.

This is also occurring in a healthcare environment that is still undergoing a transformation to digital and electronic records. While there has been a huge political push to move to electronic health care records, hospital and medical care security (especially in smaller offices) has not yet caught up to the challenge of protecting this valuable patient data.

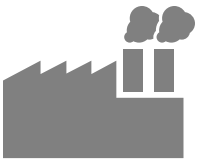
As a result, targeted cyber-attacks against healthcare organizations will continue their rapid rise in frequency and success.

"The healthcare industry is a prime target for cybercriminals. With millions of patient records now in digital form, healthcare's biggest security challenge in 2015 will be keeping personally identifiable information from falling through security cracks and into the hands of hackers."

– Carl Leonard, Principal Security Analyst
Websense Security Labs

1. www.idtheftcenter.org/ITRC-Surveys-Studies/2013-data-breaches.html

PREDICTION 2



YOUR REFRIGERATOR IS NOT AN IT SECURITY THREAT. INDUSTRIAL SENSORS ARE.

Attacks on the Internet of Things will focus on business use cases, not consumer products.

There will be at least one major breach of an organization via a newly introduced internet-connected device, most likely through a programmable logic controller, or similar connected device, in a manufacturing environment.

While many hacks of refrigerators, home thermostats and cars have found their way to the headlines, the likelihood of a major attack campaign via connected household items in the age of the Internet of Things is minimal. There often is not a lot of sophistication in these "smart" devices and using these items to create a viable attack would be very challenging given the current state of the technology.

While you may have to worry about cybercriminals successfully melting your butter or spoiling the milk in your refrigerator, there is little reward in attacks against your connected domestic devices. The criminal element has set its sights elsewhere.

The Internet of Things will change the security landscape significantly in other ways, with the primary IoT security challenges resulting from business use. Every internet-connected device greatly increases the number of attack surfaces in the business. The Internet of Things is set to explode and be one of the main sources of headaches for CSOs this year, inheriting the title from the bring-your-own-devices (BYOD) initiatives of the past.

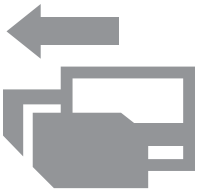
"The Internet of Things means consumer products from TVs to refrigerators are now digitally connected. While the enterprise need not fear the implications of an interconnected home appliance, every new employee's internet-connected device, app and upgrade is a potential threat vector." – Charles Renert, VP, Websense Security Labs

For example, whole new processes are evolving rapidly to add to the IoT architecture. However, the strong likelihood will be that at least one of these areas will see attack traffic, especially when security is not a priority for most innovations, and because not everyone will get it right.

Many of the new network-connected devices in business IOT deployment include machine-assisted or machine-determined sharing of information. These devices automate large industries to ensure that major operational sites such as power plants, factories and oil rigs are all operating smoothly.

When you attach a new device to these existing, highly complex networks, they may have a different sort of communications protocol. Once you have turned on the flow of amplified communications in an organization, it's a challenge to identify which traffic is legitimate and which may be a data-stealing attack. As a result, this communication may also go unmonitored.

Furthermore, downtime of these systems can mean millions in lost revenue, so business leaders are not willing to tolerate this possibility. Any interruption due to a false positive of a security solution will be loathed in the C-suite, meaning that much of these machine-to-machine communications will remain also unsecured.



CREDIT CARD BREACHES ARE THE LEAST OF YOUR WORRIES

Credit card thieves will morph into information dealers.

With billions of dollars just there for the taking, retail cyber-attacks seeking credit card data are likely to continue in 2015. However, as those within retail security escalate their defenses (and security measures such as Chip and PIN technology are mandated), we will see a morphing of the manner in which these thefts are committed.

For example, as cards are hacked and then put up for sale on carding sites worldwide, the value of the stolen cards decreases as cards get flagged or cancelled by the issuing bank. The window of time for maximizing profit from these endeavors continues to shrink even as criminals find more ways to steal them. Because of this decline in value, it's likely that criminals will look to gather even more credit card numbers than they currently do, while also attempting to maintain the value of the information they hold for a longer duration.

We believe that we will see the data thieves begin to tune their malware to gather other information available besides just relevant credit card details. With a tiny code modification, that credit card stealing malware can now also steal credentials or any information associated with that terminal, including the user's identity, customer loyalty programs or other store-related data. If they can collate their massive data collection efforts, they can begin to assemble the individual pieces of data and collect whole profiles of individual users, consisting of multiple credit cards, regional and geographic data, personal information and behavior. This personal information, pulled from the criminal Cloud, will then be worth considerably more than the simple credit card number they have stolen.

Thus, those that are now selling credit card accounts are likely to adapt their illegal craft to selling complete personal identity dossiers.

YOU ARE ONLY WHO YOUR PHONE SAYS YOU ARE

Authentication consolidation on the phone will trigger data-specific exploits, but not for stealing data on the phone.

Despite ongoing hype, mobile devices will continue to be a non-factor for the overwhelming majority of malware attacks against enterprises. While it is true that the number of variants and incidents of mobile malware has exploded year-over-year (remember, we essentially started at zero), they still do not constitute even a single percentage point of overall attacks or of Advanced Attacks.

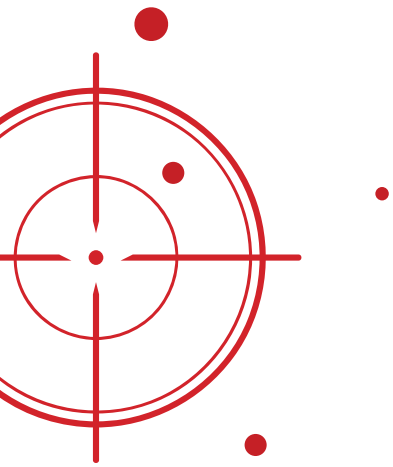
However, mobile devices will increasingly be targeted for broader credential-stealing or authentication attacks to be used at a later date.

To get a more complete understanding of the problem, we really have to think of mobile devices as conduits to the Cloud. As the Cloud gains more data, organizations facilitate the access of this data through various kinds of devices, whether desktop, tablet or mobile. Because of this, we will see criminals going after the mobile device – not to simply crack a phone code and steal data from the device itself – but as a vector into the growing data resources that the devices can freely access in the Cloud.

Mobility also creates possible vulnerabilities in the area of user authentication. Many online services looked to defer authentication to major social networks so that to access their services, users had to login using their Facebook account information, for example. The thinking was that Facebook's security was much more sophisticated than theirs. It's a bit ironic, however, that security professionals advise using different passwords for each site, yet we now can use the same "master account" (e.g. Facebook) to authenticate login to many services.

This single-point-of-failure problem will extend to phones this year, as smartphones are increasingly being used as a primary out-of-band authentication measure, particularly for business-critical applications. Authentication will become an even hotter security issue as the transition to new broad deployments of out-of-band mobile and social authentications develop. Attacks seeking to compromise social credentials and out-of-band devices will increase on a massive scale.

Criminals will take advantage of the increasing reliance on the smartphone as an authentication measure. This is likely to manifest itself as malicious code designed to either intercept the text or code generation authentication elements built into mobile programs, or clone or mimic a mobile device itself to take over other accounts in a variation of man-in-the-middle attacks. With this information, criminals can use the device as a key to access a broad range of information available to the user, including valuable corporate data.



OPEN SOURCE OR OPEN DOOR?

New vulnerabilities will emerge from decades-old source code.

Huge vulnerabilities such as OpenSSL, Heartlbeed and Shellshock have existed within open source code for years, only to be revealed when scrutinized for weaknesses with a fresh pair of eyes. Although these vulnerabilities were only recently revealed, we should not assume that they have not already been used as exploitation vectors for years before they were made public.

"Old source code is the new Trojan horse waiting to be exploited, and open-source code is only the beginning. With so much code written and in use, it's impossible to catch every dormant exposure point until they've been executed. Because of this, any time source code is altered or integrated as part of an application or service upgrade, these unknown systemic vulnerabilities have the potential to expose networks to attack." – Carl Leonard, Principal Security Analyst

It's quite likely that each of these vulnerabilities was probably already in the quiver of sophisticated cyber attackers for a very long time. Combine that with the challenges of hiccups in certificate management, HTTPS and SSL protocols by certain cloud services, and we may face a real challenge this year. Attackers will make use of the vulnerabilities in old code to target new applications.

The speed of development using third party tools is astounding. Nobody builds from scratch. The rate of adoption for open source programing as a basic component of new software and services greatly exceeds the vetting of the code of these applications. Unfortunately, security is still not built into most development cycles. As the source code gets used and altered into a new application or service, every integration is another opportunity for risk.

Flaws in the old code, including legacy proprietary code, not just open-source code, will open up major data breaches in divergent applications because the code was never properly vetted by third parties before or after integration. If you threat model the internet, the results show that the underlying protocols used are broken or will be.

In 2015, at least one major breach of data, a veritable treasure trove, will trace its origins to confidential company data improperly transmitted or secured on publicly available cloud storage sites based on these old code foundations.

EMAIL THREATS ARE EVOLVING

Email threats will take on a new level of sophistication and evasiveness.

While the Web remains the single largest attack vector for attacks against businesses, email will play an increasingly integral role in data compromises. Massively polymorphic Domain Generation Algorithms and evolving evasion techniques will test the limits of most current email security solutions.

Cybercriminals upping their game are perfecting their campaign abilities previously associated only with advanced, targeted attacks. These advanced tactics designed to evade most modern email security solutions are quickly becoming the new norm as more sophisticated email threats increase.

As a result, although spam volumes are decreasing, most users will begin to witness an increase in the amount of spam they receive in their inbox, because most email security measures will be incapable of detecting them in the Cloud scrubbing prior to passing to a user's inbox.

While usually associated with the Lure stage in the 7-Stage Kill Chain[2], we have seen a growing trend toward emails that do not contain a link or spam message, but are actually the first Reconnaissance steps of an advanced attack. Because the sender and text is sufficiently randomized, and the body of the email hosts neither malware nor links for analysis, the emails are typically getting through most security solutions. However, by automating the process across an organization, attackers can still use this method to validate credentials and prepare more effectively for other penetrating aspects of an attack.

"Over the years, we've seen email take a back seat to the Web as the preferred entry point for data theft. With all eyes primarily focused on the more advanced and obvious threats, we expect email threats to increase as attackers evolve their techniques and reconnaissance operations to bypass the limits of current email security solutions."

– Carl Leonard, Principal Security Analyst
Websense Security Labs

2. www.websense.com/sevenstages

GOOGLE DOCS CONTROLS THE BOT

As companies increase access to cloud and social media tools, Command and Control instructions will increasingly be hosted on legitimate sites.

As companies open up access to more cloud, collaboration and social tools, criminals will migrate their Command and Control infrastructure to hide in these approved channels.

In today's business world, network administrators monitoring internet activity will flag traffic moving to suspicious sites, but will not think twice if network traffic shows a user visiting Twitter every few hours, or going to Google docs. Criminals will take advantage of this and increasingly place malware Command and Control infrastructure onto these sites.

Further, we will see the compromise of legitimate sites that are prominent in an industry, to instruct rather than distribute malware. In this way, "waterhole" sites may be modified and instead of delivering malware (and risk a dropper being detected), they may simply be used to control malware already present on a device.

In the same manner, we anticipate that exfiltration will be perpetuated via these company-approved channels to hide data-stealing attacks from scrutiny.

NEW CYBER WAR PLAYERS TAKE A SEAT AT THE TABLE

There will be the new (or newly revealed) players on the global cyber espionage/cyber war battlefield.

Last year, the release of classified documents underscored that nation-states are actively engaging in cyber war planning, tactics and attacks. For the most part, these gambits have defined a model that is primarily successful. This will undoubtedly elicit new recruits to the global cyber war table.

Unlike past measures to limit access to strategic weapons of war (such as nuclear non-proliferation treaties), there is currently nothing to limit the ability of countries, government factions, rebel groups and those with nationalist interests to engage in cyber war activities.

Cyber war treaties may be on the horizon in a few years, but in the interim, nation-state hacking will continue and the adversaries wielding computers as weapons in these battles will multiply tremendously.

Because it does not require nation-state funding to take advantage of current tools to create destructive malware, we will see an increase in loosely affiliated "cells" that conduct cyber-terrorist or cyberwarfare initiatives independent from, but in support of, nation-state causes.

In addition, watch for increasing cyber espionage activities from countries with high forecasted global economic growth. These countries are more likely to be the next to engage in cyberwarfare and espionage activities to protect and advance their growing affluence.

websense
SECURITY LABS™

2015 SECURITY PREDICTIONS

For more information, visit:
www.websense.com/securitylabs

[WSL-2015PREDICTIONS-ENUS-18NOV14]