CYREN 2015 CYBERTHREAT YEARBOOK

Table of Contents

Content providers

Sigurður A. Stefnisson
VP & GM AntiMalware

Magni Reynir Sigurðsson
AV Analyst

Michael Taranov
Software Engineer

Ohad Arnon
Director,URLF R&D and Detection

Michael Peick
Software Engineer

Eyal Matzkel
Lead Researcher

Editors

Avi Turiel
Director of Threat Research

Christopher Taylor
Senior Director, Product Marketing

Foreword

Lior Kohavi
Chief Technical Officer,
CYREN, Inc.

Looking back on 2014, it has been an incredibly dynamic year in the world of cyberthreats. It takes only two names to sum up the impact the cybercriminal had on the 2014 headlines: Home Depot and Sony. The Home Depot breach yielded about 110 million stolen pieces of sensitive information, including social security numbers and email addresses. And, in a classic case of hacktivism, Sony lost more than just emails and employee social security numbers; it suffered significant brand damage.

For some, these headlines say everything that needs to be said about cyberthreats in 2014. The headlines lead you to believe that cybercriminals are only targeting the "big guys" for their money and profile, and that everyone else is safe because the criminals aren't going to bother unless you're a Fortune 1000 corporation.

Well, not quite. Enterprises of all sizes are now besieged by cybercrime at an alarming rate. In fact, during the four-year period between 2010 and 2014:

- The number of successful cyberattacks on businesses of all sizes increased by 144%.
- The cost of cybercrime per company increased by 95%.
- The average time to resolve incidents increased by 221%.

The problem with making companies like Home Depot and Sony the poster-children for cybercrime is that it gives the vast majority of businesses in the world the false impression that they won't be targeted. But this perception couldn't be further from the truth. When it comes to cybercrime, businesses regularly misjudge their risk profile because they misunderstand what is valuable to the cybercriminal. The game is money-driven and value can be extracted from many different types of data. In fact, stealing personally identifiable information (PII)—such as email addresses and social security numbers—is actually more lucrative than

When it comes to cybercrime, companies regularly miscalculate their risk profile because they misunderstand what is valuable to the cybercriminal.

CYREN

CYREN CYBER SECURITY BY THE NUMBERS

CYBER **1** Cyber Platform

19 Data Centers

200 Countries

500,000 Points of Presence

600,000,000 Users

17,000,000,000 Daily Transactions

144%

The number of successful attacks on businesses is up by 144% in four years.

credit card number theft. Social security numbers can yield criminals millions of dollars. Email address lists can be sold to spammers and malware distributors. And, ultimately *every enterprise holds some amount of PII data*.

At the same time, cybercriminals are getting more creative in their approach. Today's cybercriminals are well-educated, sophisticated "crime professionals" with highly developed business networks that focus their efforts on threat innovation geared towards penetrating corporate systems.

> Cybercriminals can sell personally identifiable information (PII), such as that stolen from Blue Cross Blue Shield Anthem, for 10 times more than credit card data on the black market.

So, as threats continue to evolve, the challenge for businesses isn't the massive volume of known threats, it is the smaller volume of unknown threats, like the malicious socially engineered phishing email, designed to look like it came from the HR department and sent to a handful of select employees to test the corporate defenses.

But ultimately, protecting the business enterprise is about more than just algorithms or software. It's about the data that powers the solution. With rapidly evolving distribution and attack methods, to be effective security solutions must employ a detection-based methodology that combines high-quality threat data with behavioral and reputation scoring to create up-to-the-moment cyber intelligence.

To stem the tide of cyberthreats targeting the enterprise, business leaders need to think about solutions that integrate and utilize cyber intelligence from industry experts. At CYREN, we have built the world's largest and most comprehensive cyber-intelligence database. To keep this current, every day we collect and analyze over 17 billion online transactions.

CYREN cyber intelligence powers the security solutions of over 200 global partners; we are the security provider to the security industry, and we specialize in creating solutions that identify and block previously unknown threats.

The people at CYREN work day and night to increase the size, scope, and value of our data, enrich the level of analysis, and enhance and expand our solutions to ensure that enterprises can be protected from ever-encroaching cyberthreats. The cybercriminal thrives on threat innovation; at CYREN, we are committed to identifying and stopping cybercrime by innovating cybersecurity solutions with an even greater opposing force. Some of our newest advances include:

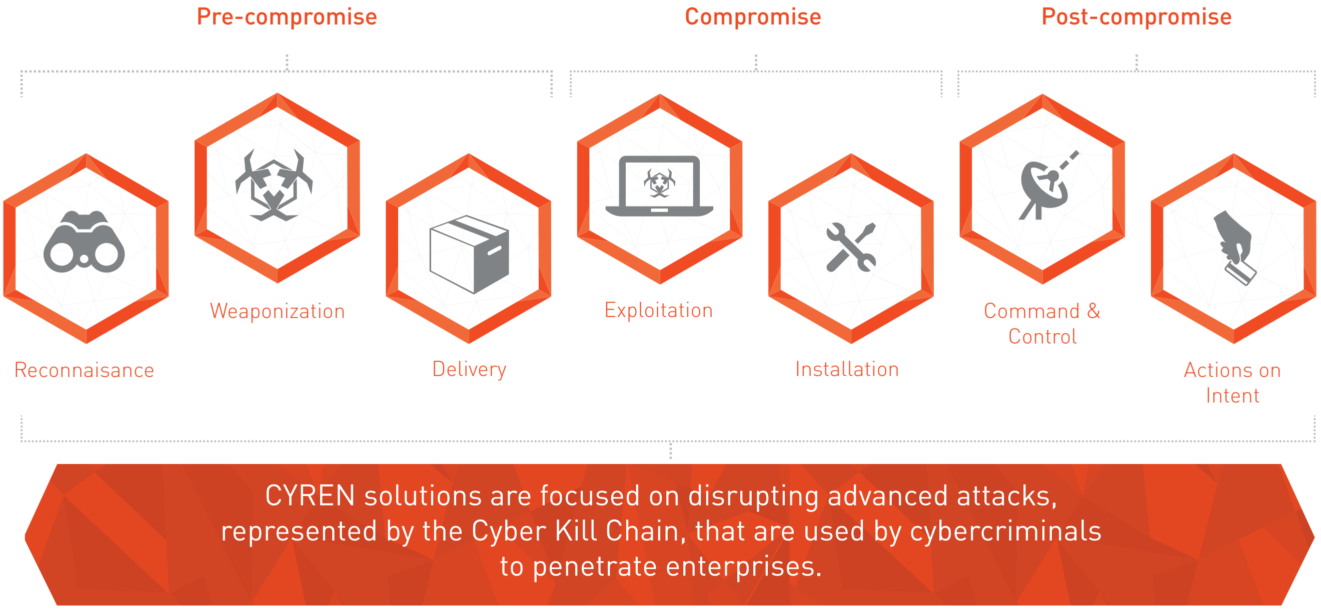
- Making the massive cyber-intelligence that already powers the security industry available direct to businesses or enterprises, through a cloud-based web security solution
- Pioneering a detection method that leverages our massive database to identify and stop advanced persistent threats as early as possible
- Using our deep and broad global threat data, to find new ways to understand the subtle differences between cybercriminal, legitimate user, and machine behavior patterns to create security solutions that protect the enterprise on all levels

In this Yearbook, along with the numbers, we present an in-depth analysis of individual threats captured by CYREN in 2014 to illustrate how the cybercriminals engage in the business of crime, how they target the business enterprise, and what CYREN is doing to halt the advance of cybercrime in its tracks.

INTRODUCTION

CYREN cyber intelligence powers the security solutions of over 200 of the largest IT and security technology providers in the world. As the security provider to the security industry, CYREN maintains the broadest and deepest real-time Internet threat database in the world. Every day, we collect and analyze 17 billion pieces of threat data to protect 600 million global users. Threat data is gathered and cyber intelligence disseminated through 500,000 global points of presence in 200 countries.

The Cyber Kill Chain



CYREN solutions are focused on disrupting advanced attacks, represented by the Cyber Kill Chain, that are used by cybercriminals to penetrate enterprises.

In developing this report, we put our massive dataset to work, analyzing a number of unique (and not so unique) cybercrime trends from 2014. From noteworthy corporate attacks to the Internet of Things, 2014 was a busy year. Phishing trends continued to be prominent in the early part of the year; the first mobile ransomware debuted mid-year; the third quarter saw massive attacks on businesses; and by the end of the year most of the world was checking their credit card and bank statements regularly to make sure that cybercriminals had not yet targeted their accounts as a result of the point-of-sale malware that found its way into the networks of Home Depot and other major retailers and enterprises. On top of it all, the world is getting ready for the Internet of Things, and the likelihood of 26 billion new Internet-connected devices by 2020.

Protecting the enterprise is the focus of this 2015 Yearbook. Attacks against business are growing in scope and scale, with cybercriminals targeting corporations of all sizes and profiles. We proudly feature in this report a number of new analytic techniques that will enable improved predictive capabilities to stop cybercriminals at the earliest stages of an attack.

We also examine both old and new trends in malware, including a highly dangerous version of the old Melissa virus that targets personally identifiable information, such as passwords and other sensitive corporate data. In the phishing section, we explore how social engineering is creating opportunity for cybercriminals to deploy advanced persistent threats against businesses. And in mobile malware we look at what the future holds for the increasing number of devices that we use to capture and hold sensitive information.

In closing, we take a brief look at the impact the industrial Internet of Things will have on today's business from a cybercrime perspective, demonstrating the importance of cybersecurity to prevent criminals from using building management systems and other large-scale industrial Internet-connected systems as a means to target businesses.

PROTECTING THE ENTERPRISE

How CYREN Uses Data, Analytics, and Unique Technology to Protect Global Businesses

Cybercrime is big business: it costs the global economy more than $400 billion[1] annually. As more and more companies move their business operations and sensitive data online, incidents and costs are only expected to increase. With low risk of getting caught or prosecuted, low operational costs, and incredibly high rates of return, cybercriminals are heavily incented to expand their criminal activities. Attacks will grow in scope and scale, becoming stealthier, targeted, and customized, with the "unknown" threats, such as APTs, zero-day attacks, dynamic Trojans, and stealth bots posing the greatest risk to the enterprise. In fact, in just the last year CYREN estimates that the average number of daily emails sent containing malware has increased by almost 50 percent; new malware samples have grown by 15 percent; and the number of phishing URLs tracked by CYREN have increased by 233 percent.

Threats are Stealthy

Threats are distributed via the cloud, from botnet zombies, from websites hosting third-party or syndicated advertising, and via socially engineered content in emails and social media. One cybercrime study reports that criminals injected search engine optimization (SEO) words and phrases into websites, to drive search traffic to malware-ridden sites.

Threats are Targeted

Cybercriminals no longer blanket the Internet with a single worm; they focus attacks on an industry sector (such as financial institutions), a single government entity, a type of device, or a single valuable corporate target. And now advanced persistent threats (APTs) and zero-day exploits mean that targeted attacks may be undetectable with traditional methods, even in closely monitored environments.

Threats are Customized

Malware is modified and reengineered to avoid detection and to target specific devices. Ransomware volume has exploded in the last two years, with one form of 2014 ransomware generating an estimated $30 million for cybercriminals. Sophisticated social engineering makes these attacks difficult for even high-tech business users to identify.

Threats Are Different: Cybercriminals, Crime, and Information

Gone are the days of teenagers sitting in their parents' basement trying to break into DOD systems. Today's cybercriminal is a professional; they run or participate in cybercrime syndicates, are university-educated, and can generate millions of dollars from a single attack. Cybercriminals are also organized, rarely working independently. They have developed a sophisticated business ecosystem with each criminal assuming a different role in the cybercrime lifecycle. They have a multitude of tools at their disposal to manage exploits, expand attacks, and advance their agenda. On top of it, information is saved and distributed in a way that makes it easy to target with stolen credentials—such as cloud storage locations (Sharepoint sites, Google Docs, or Amazon Cloud), or mobile devices, such as smart phones, e-readers, tablets, and even Internet of Things gadgets.

Developing Innovative Cybersecurity Solutions

The challenge for many businesses is not only understanding these new threats, but also properly mitigating their associated risk. Many companies make the mistake of underestimating their corporate risk, thinking that because they're not a Fortune 1,000 organization, they're not on a cybercriminal's target list. Every company maintains some form of information that is valuable, and if a criminal can get that information with little effort, then the return on investment is high.

The vast amount of threat data that CYREN sees and analyzes on a daily basis provides a unique opportunity to dig deeper into the anatomy of these threats and examine them for details about the criminal and the crime. By collecting and analyzing massive volumes of threat data, in the form of malware, malicious URLs, and spam, cyber intelligence can be quickly updated into solutions and data feeds that help mitigate corporate risk.

As demonstrated in our Map the Attack and the Botnet-Malware Connection articles, CYREN is using its massive dataset, combined with state-of-the art analytics to empower enterprises with a reference library of the potential vulnerabilities, as well as cybersecurity solutions that provide protection against even the stealthiest attacks.

[1] www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

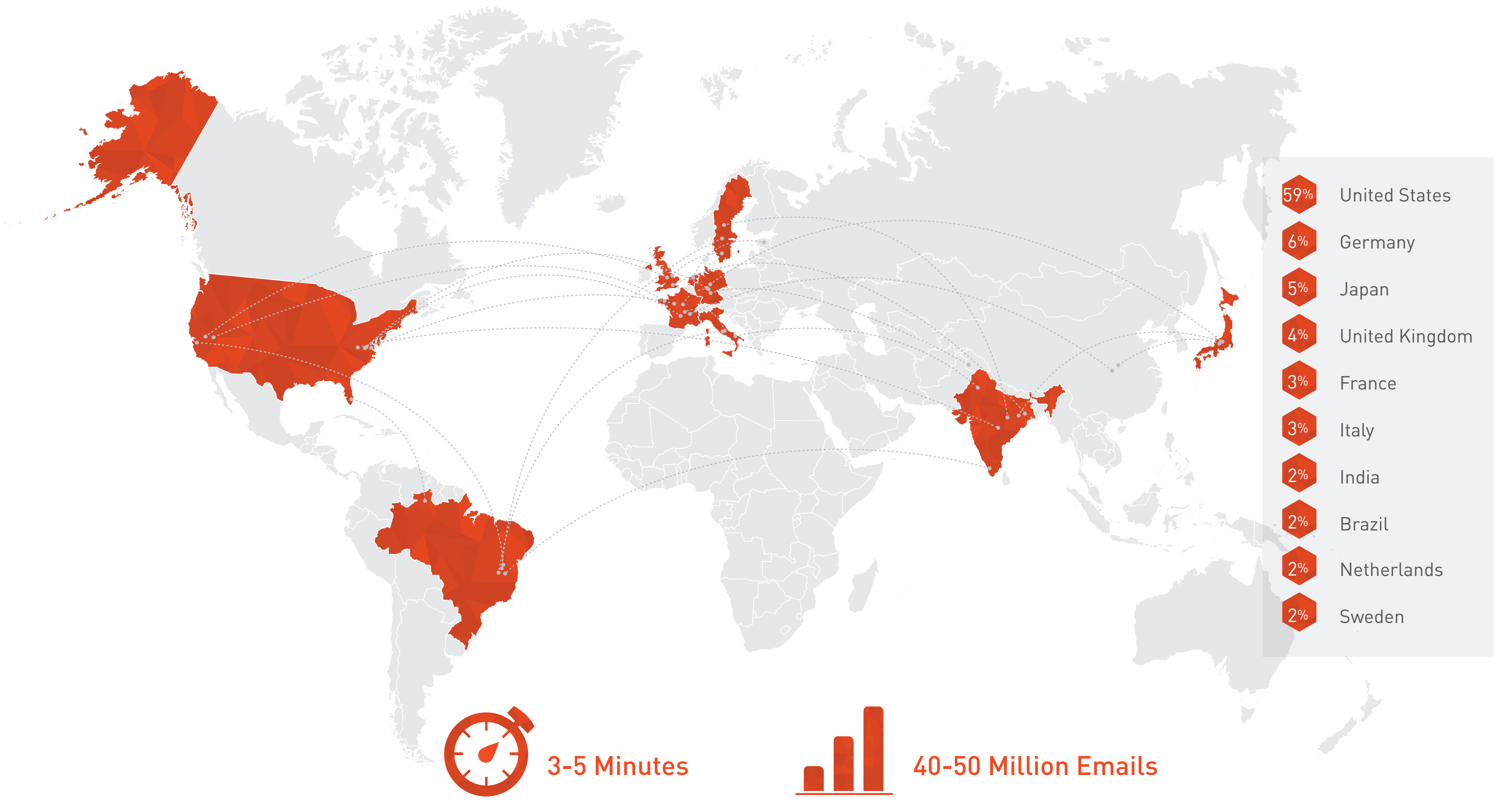
Map the Attack!

The attacks began in late 2013 and ran periodically throughout 2014.

Massive volumes of email threats—40 to 50 million emails distributed in short bursts lasting only three to five minutes each—were sweeping the globe. The attacks would continue for a week or two, then disappear for several months.

The attackers thought they were being smart. Each attack used a freshly registered domain and the attacker made sure that the email threat content was diverse. No pharmaceutical or casino spam for this cybercriminal, ensuring that filters didn't pick up on any traditional email threat content. The criminals also used zombies from around the globe to distribute the email threats.

In spite of this cybercriminal's best efforts, CYREN stopped the attack within seconds, protecting millions of users with our patented Recurrent Pattern Detection (RPD) technology.



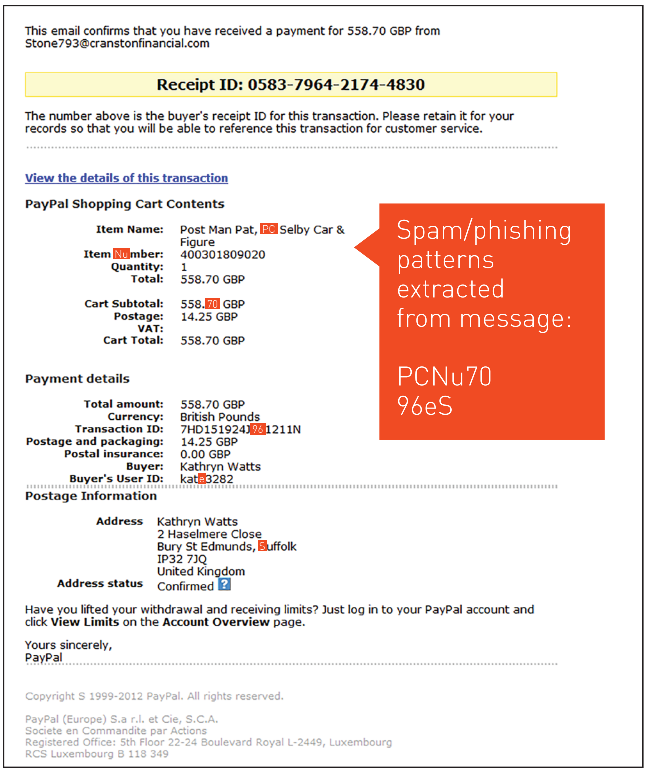
59%	United States
6%	Germany
5%	Japan
4%	United Kingdom
3%	France
3%	Italy
2%	India
2%	Brazil
2%	Netherlands
2%	Sweden

In analyzing the November email threat outbreak, CYREN determined that all the messages shared several unique, identifiable structure or distribution patterns or values such as:

- Pseudo-random combinations of characters from the subject and body of the email that are repeated throughout all the email messages
- The same website link appearing multiple times over the course of several emails
- Attacks being launched from blacklisted zombie machines
- Multiple emails being sent from senders at same the IP address
- The volume of the emails sent over a period of time

Using Recurrent Pattern Detection, CYREN was able to block this attack within minutes of initial email threat distribution.

Using RPD to identify the patterns in the threat data, CYREN solutions blocked the email threat without generating false positives. In addition, because RPD uses real-time analysis, CYREN was able to extract and analyze these new and volatile patterns within seconds of the outbreak, unlike traditional methods which only observe known senders, known content, and known patterns, and often take considerably longer to make an identification than the attack lasts. This information was stored in the vast RPD classification database to help further identify similar components in future attacks.



This email confirms that you have received a payment for 558.70 GBP from
Stone793@cranstonfinancial.com

Receipt ID: 0583-7964-2174-4830

The number above is the buyer's receipt ID for this transaction. Please retain it for your records so that you will be able to reference this transaction for customer service.

View the details of this transaction

PayPal Shopping Cart Contents

Item Name: Post Man Pat, PC Selby Car & Figure
Item Number: 400301809020
Quantity: 1
Total: 558.70 GBP

Cart Subtotal: 558.70 GBP
Postage: 14.25 GBP
VAT:
Cart Total: 558.70 GBP

Payment details

Total amount: 558.70 GBP
Currency: British Pounds
Transaction ID: 7HD151924J961211N
Postage and packaging: 14.25 GBP
Postal insurance: 0.00 GBP
Buyer: Kathryn Watts
Buyer's User ID: kate3282

Postage Information

Address Kathryn Watts
2 Haselmere Close
Bury St Edmunds, Suffolk
IP32 7JQ
United Kingdom
Address status Confirmed ?

Have you lifted your withdrawal and receiving limits? Just log in to your PayPal account and click **View Limits** on the **Account Overview** page.

Yours sincerely,
PayPal

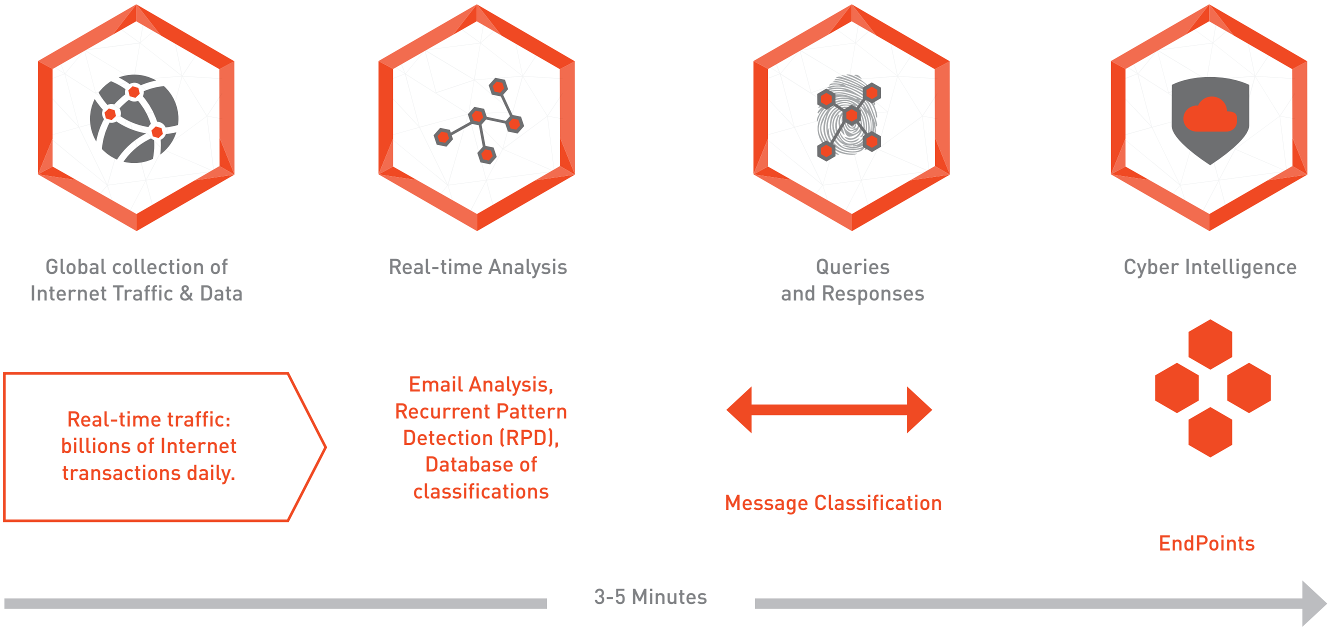
Copyright S 1999-2012 PayPal. All rights reserved.

PayPal (Europe) S.a r.l. et Cie, S.C.A.
Societe en Commandite par Actions
Registered Office: 5th Floor 22-24 Boulevard Royal L-2449, Luxembourg
RCS Luxembourg B 118 349

Spam/phishing patterns extracted from message:

PCNu70
96eS

CYREN Reccurrent Pattern Detection (RPD)


Global collection of Internet Traffic & Data
Real-time Analysis
Queries and Responses
Cyber Intelligence
Real-time traffic: billions of Internet transactions daily.
Email Analysis, Recurrent Pattern Detection (RPD), Database of classifications
Message Classification
EndPoints
3-5 Minutes

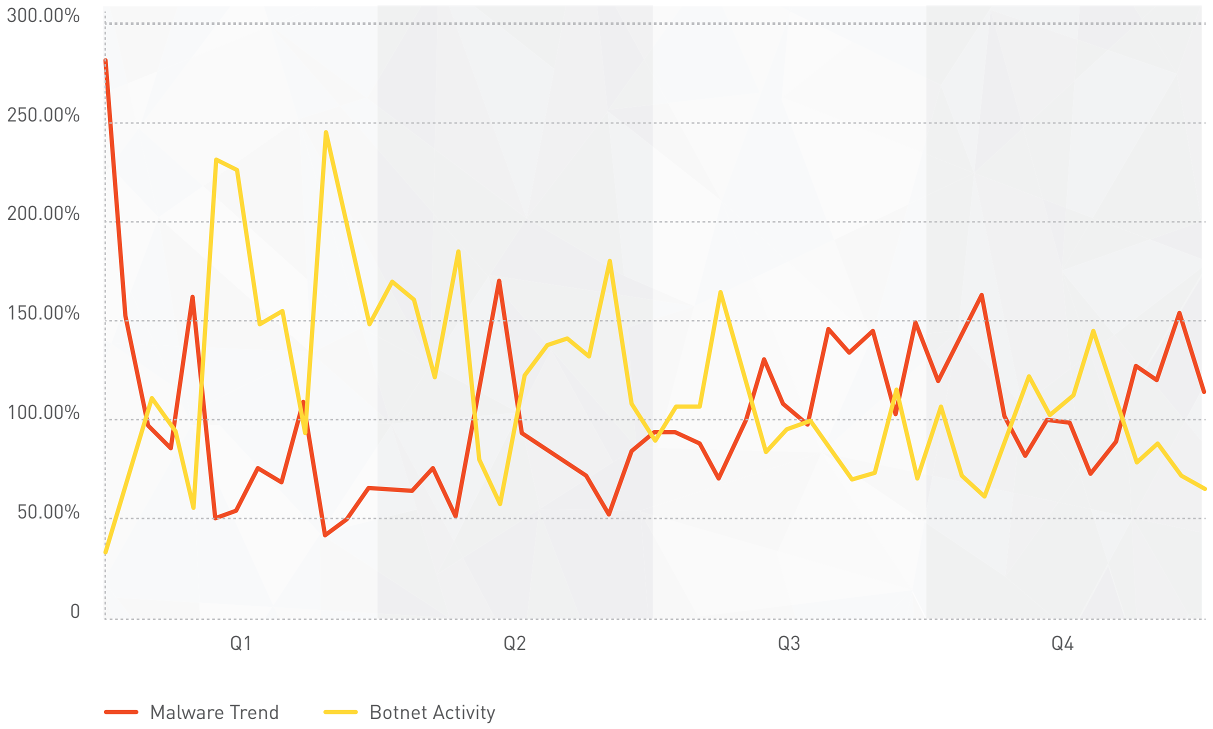
Predicting Malware in Advance

CYREN Analysts Examine Botnet Data for Links to Malware Distribution Trends

Picture this: CYREN issues an alert that a massive malware attack will begin in approximately one weeks' time. Enterprises now have five to seven days to take necessary precautions, including advising their employees of potential malware embedded emails. As a result of this advance notice, corporate cybersecurity experts are able to minimize any malicious emails that target the corporation and potentially stave off a wave of potential initial compromises associated with advanced persistent threat style attacks. Sound impossible? Perhaps not. We present a case study in how this may become reality.

CYREN analysts are working on better methods to predict significant malware attacks with confidence. Using a sample dataset, CYREN analysts have observed consistent fluctuations in botnet activity, so, theorizing that botnet owners were repurposing their network for expansion, the team went to work to determine if a broader trend could be observed. By analyzing massive volumes of threat data, the CYREN analysts believe they have identified a direct relationship; as spam botnet activity decreases, the amount of malware distributed increases, i.e. there appears to be a direct relationship between zombie activity and malware that could enable future malware attack prediction.

Botnet Activity vs. Malware Attacks in 2014



CYREN Analysts observe a direct relationship between zombies and malware, enabling future malware attack prediction.

The graph above illustrates the correlation between spam botnet activity and email-based malware distribution in samples examined to date. Each line (orange=malware and yellow=botnet) represents a different data set overlaid against the same dates. Over the course of 2014, peaks in malware clearly correspond to decreases in botnet activity. CYREN analysts suspect that this means that botnet owners are "repurposing" during these periods, with the primary objective being expansion of the botnet. The graph shows that malware increases when botnet activity is low, presumably as the cybercriminal uses malware distribution to groom and grow the botnet. The synchronized nature of the cycle suggests that botnet growth and distribution via malware emails is managed directly by individuals, not an automated component of the malware itself—illustrated by the fact that the botnet herders take regular breaks from sending spam, investing the time instead in sending malware to fuel future botnet growth.

The next phase of this research is to apply the analysis techniques we have developed to a broader dataset to establish if the theory remains true at the macro level of botnet activity.

Email continues to be a dominant medium of malware distribution, and it remains a highly profitable application of botnets. As cybercriminals grow more advanced, innovative, and stealthy, the need for truly predictive analytics becomes critical. In the future, a week's advance notice of an attack could potentially stop highly dangerous APT style attacks in the delivery phase, saving businesses both their reputation and millions in lost revenue. With our wealth of threat data, the analysts at CYREN are working to fuse many such seemingly unconnected threat types to derive unique insight into cybercriminal behavior and tendencies, and develop solutions to protect the enterprise before an attack even happens.

MALWARE

THE RETURN OF THE MACRO: AN IN-DEPTH ANALYSIS

Who doesn't remember the "Melissa" worm from 1999? Believing they were opening an email and attached document from a friend, victims unwittingly launched a macro, which automatically redistributed itself using copied email addresses from the victim's computer. At the time, this malware was so potent and unique that within hours it had spread around the globe. Once installed on a computer, the worm distributed the victim's confidential information and modified documents by inserting quotes from the TV series "The Simpsons".

By today's standards, this macro seems tame. Although the malware did millions of dollars in damage to personal and corporate systems (including Microsoft and Intel) neither the creator, nor the distributor gained much monetarily from its propagation. And, thanks to both time and software updates, by the mid-2000s macro viruses like Melissa, were essentially extinct. In fact, between 2010 and 2013, CYREN did not observe any significant classic "macro virus" volume, primarily due to Microsoft blocking the ability to open macros without user permission in its software.

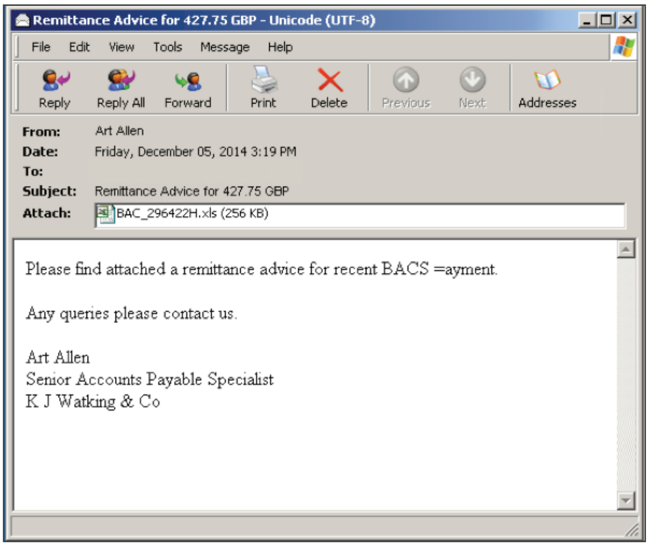
Fast forward to 2014. In the first and second quarters of 2014, CYREN began to observe macro-malware belonging to the Trojan families of Zbot and Dridex. Then in early November, CYREN observed an outbreak of over 3.02 BILLION emails containing advanced 2nd generation macro-malware. Subsequent outbreaks in December consisted of as many as 1.2 billion emails in one day. Unlike earlier versions, this macro malware did not exhibit the same infection routines seen among early macro viruses.

Macro Malware 2014

The malware lifecycle evolves based on changes in the motivation and goals of malware authors and cybercriminals. Fifteen years ago, the criminals that created Melissa were interested in mischief and fame. Today, criminals are driven by the profit motive, with enterprises that store personally identifiable information and other types of sensitive information being easy targets.

What It Looks Like

Macro malware typically arrives via email with an attachment that contains a macro-based phishing attack or a malicious binary executable file distributed in the form of a macro-embedded MS Office document (usually Word or Excel) with the malicious code written using the Visual Basic for Applications (VBA) scripting language.



From: Art Allen
Date: Friday, December 05, 2014 3:19 PM
To:
Subject: Remittance Advice for 427.75 GBP
Attach: BAC_296422H.xls (256 KB)

Please find attached a remittance advice for recent BACS =ayment.

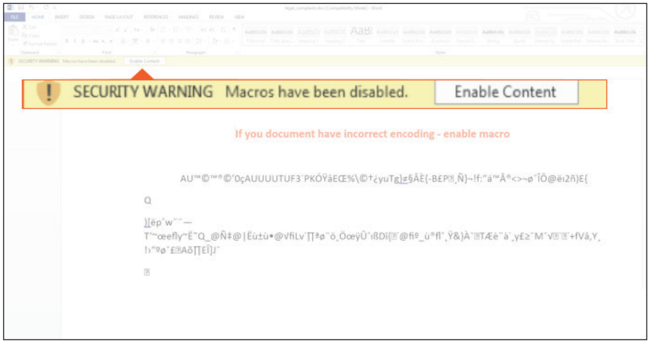
Any queries please contact us.

Art Allen
Senior Accounts Payable Specialist
K J Watking & Co

What makes the current versions of macro malware particularly dangerous is that the code is often heavily obfuscated making detection difficult. Further, the macro-embedded documents are not designed to infect other documents; instead the document itself serves as a vessel for executable malware that, when running on the victim's PC, steals login credentials and other types of personal transactions, such as credit card data.

In this example detected through CYREN's AntiMalware and Virus Outbreak Detection solutions, the victim receives a socially engineered email claiming to be from the Banker's Automated Clearing Services (BACS), an entity that provides electronic financial transaction processing.

Because the problems with the macro-enabled features in MSOffice documents, Microsoft has disabled the tool. However, users can still manually allow the opening of a macro. It is this feature that cybercriminals are using to exploit victims by tricking them into believing that they need to enable the macro in order to read the document or spreadsheet contents.



If you document have incorrect encoding - enable macro

AU™©™®©'0çAUUUUTUF3`PKÓŸåEŒ%\©†¿yuTg}≠§ÂÈ{-B£P,Ñ}¬!f:"á™Å®<>¬ø˜ÎÔ@ëı2ñ)E{

Q

}[ëp'w˜˜—
T'~œefly~Ë˜Q_@Ñ‡@|Ëù±ù•@√fiLv`∏ªø˜ö¸ÖœÿÛ`ıßDi{@fiº_ù®fl`,Ÿ&}À˜TÆè˜à`,y£≥˜M˜√+fVå,Y,
!›"ºø`£AõΠEÎ]J˜

One such socially engineered document shows only a blurred image when the victim opens the file. Readable text says: "The document is blurred due to security reasons. Click the 'Enable Button' above to view the document".

Similarly, in the example shown above the victim sees an unreadable string of text and instructions suggesting that the coding is incorrect and by pressing the "Enable Content" button, the document will be readable. When the victim clicks on the button, the macro code automatically executes and drops or downloads other executable files.

Once running, the malware monitors Internet Explorer, Chrome, and Firefox browser activities, with the capability of grabbing screenshots and logging keystrokes.

Macro malware is a good example of malware authors and distributors adapting to increased security measures and repurposing older tricks (that users may have forgotten) to spread malware.

NOTORIOUS MACRO MALWARE

Based on samples CYREN received in 2014, most of the executable threats delivered via macro-based malware belong to notorious banking Trojan families like Zbot and Dridex.

While not new, these Zbot and Dridex variants have been repackaged to evade detection from file-based scanners. During the 2nd half of 2014, CYREN received many Zbot, Gamarue and Fareit variants repackaged in .Net or VB-based packers.

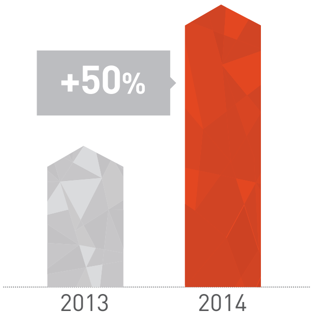
Malware like Dridex continues to use short-lived websites to facilitate attacks and manage botnets, evading security solutions by being unknown and transitory. In addition, these families of malware incorporate auto-update mechanisms, quickly spreading unique instances of its components and payloads to evade file-based detections in a matter of hours or even, a few minutes.

CYREN has also observed several attacks using Angler, Fiesta, SweetOrange, Nuclear and other exploit kits, which continuously and quickly incorporate zero-day exploits to deliver malware related to advertising fraud or"malvertising" campaigns.

2014 Malware Year in Review

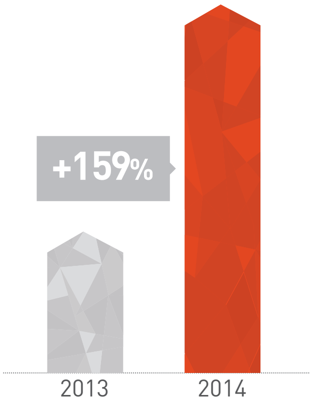
Emails Containting Malware

In the last year, the average number of daily emails sent containing malware increased by almost 50 percent, from an average of 1.69 billion in 2013 to 2.5 billion in 2014. CYREN captured 83 million new malware samples in 2014, up by 15 percent from the previous year, with the monthly average of 7 million, rising from 6.1 million in 2013.



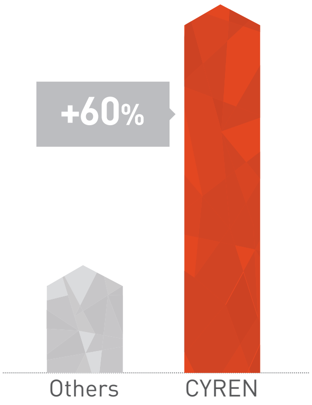
Malware URLs

In December, CYREN observed its largest email attached malware outbreak for the year, with 10.7 billion emails sent on the 18th of the month, followed by another 10.7 billion malware-embedded emails on the 23rd. Malware URLs tracked by CYREN in the GlobalView Cloud increased by 159% to 1.06 million in 2014.



Zero-hour Malware Detection

CYREN detects ~100% of all zero-hour malware, 60% more than other leading anti-virus solutions. During 2014, in comparing our rates to the top 46 AV engines on the market we found that these other AV solutions only detected 40% of the same zero-hour malware.



PHISHING

BUSINESS ENTERPRISES THREATENED BY SOPHISTICATED PHISHING

Nowhere have cybercriminals been more successful with social engineering than in the world of phishing. Consumers receive bank and credit card emails that look so real it's no surprise that they often click on the links and enter their personally sensitive and identifiable information. Employees receive phishing emails claiming to be from their corporate HR department requesting an update to their usernames and passwords, and many employees (including plenty of cyber-savvy ones) comply.

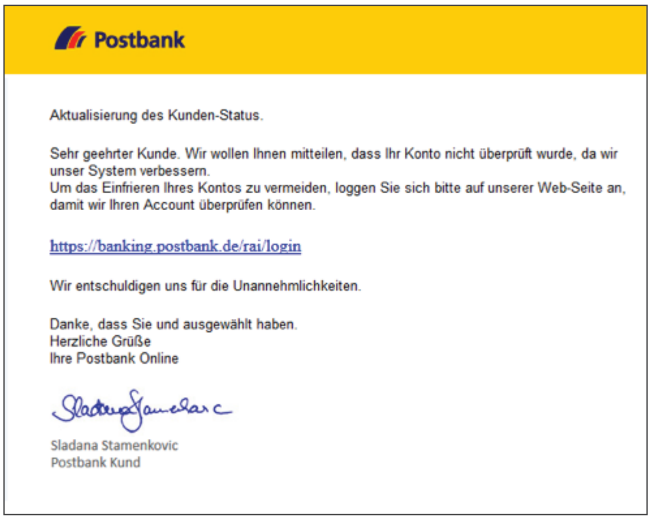
Phishing has become an insidious and highly dangerous cybercrime activity, in part because of its strong connection to Advanced Persistent Threat (APT) style attacks. In fact, spear-phishing is the number one preferred method by APT attackers to infiltrate enterprise networks. With a simple spear-phishing email to an employee, cybercriminals can quickly gain entry to corporate systems. From there, they can build on that access and develop the threat to the point that one day the enterprise experiences a data breach of the same scope and scale as the recent one with Sony Entertainment. That is, a breach where the criminal has complete and total access to all information and data owned and or managed by the enterprise.

Phishing Attack Analysis – Postbank.de

CYREN has been tracking a number of large-scale phishing attacks, including this one targeting customers of Postbank.de. The level of sophistication with this example is consistent with the type of phishing attacks typically focused on the business enterprise.

In the case of the Postbank.de attack, the attack was massive in volume, with an estimated 6.5 billion emails sent during the 1st day of the attack.

Individuals receiving the fake emails saw legitimate looking logos, with links to what appeared to be the real Postbank.de website. What made this particular attack unique was that cybercriminals had gone to great lengths to hijack up to tens of thousands of different websites, many of them WordPress-based, in turn using these sites to host the data entry collection point.



Postbank

Aktualisierung des Kunden-Status.

Sehr geehrter Kunde. Wir wollen Ihnen mitteilen, dass Ihr Konto nicht überprüft wurde, da wir unser System verbessern.
Um das Einfrieren Ihres Kontos zu vermeiden, loggen Sie sich bitte auf unserer Web-Seite an, damit wir Ihren Account überprüfen können.

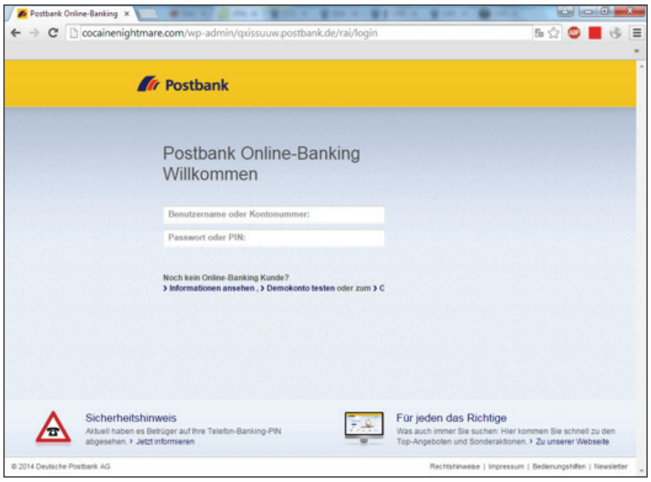
https://banking.postbank.de/rai/login

Wir entschuldigen uns für die Unannehmlichkeiten.

Danke, dass Sie und ausgewählt haben.
Herzliche Grüße
Ihre Postbank Online

Sladana Stamenkovic
Postbank Kund

- gardnersgarbage.com/wp-admin/altsvfdfnojw.postbank.de/rai/login
- cocainenightmare.com/wp-admin/jxhirh.postbank.de/rai/login
- amazingindiatravel.com/wp-admin/dithrjizubapfdp.postbank.de/rai/login



Postbank Online-Banking

cocainenightmare.com/wp-admin/qxissuuw.postbank.de/rai/login

Postbank

Postbank Online-Banking
Willkommen

Benutzername oder Kontonummer:

Passwort oder PIN:

Noch kein Online-Banking Kunde?
› Informationen ansehen , › Demokonto testen oder zum › C

Sicherheitshinweis
Aktuell haben es Betrüger auf Ihre Telefon-Banking-PIN abgesehen. › Jetzt informieren

Für jeden das Richtige
Was auch immer Sie suchen: Hier kommen Sie schnell zu den Top-Angeboten und Sonderaktionen. › Zu unserer Webseite

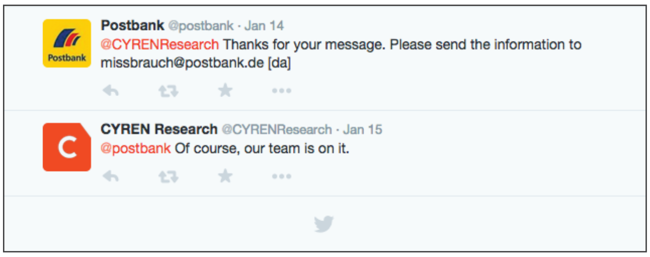
© 2014 Deutsche Postbank AG

Rechtshinweise | Impressum | Bedienungshilfen | Newsletter

In fact, CYREN detected more than 19,000 different URLs in just one 12-hour period, with a total of 78,000 unique URLs distributed over a few days.

How CYREN Stopped the Postbank.de Attack

When an attack of this magnitude is detected by CYREN, immediate steps are taken to ensure that the impact is minimized on the end-user. Because we analyze billions of Internet transactions on a daily basis, we have a unique view of phishing threats as they emerge. In turn, detected phishing URLs are blocked for customers using CYREN WebSecurity, Embedded URL filtering, and Phishing Feed.



Postbank @postbank · Jan 14
@CYRENResearch Thanks for your message. Please send the information to missbrauch@postbank.de [da]

CYREN Research @CYRENResearch · Jan 15
@postbank Of course, our team is on it.

In addition, CYREN team members take extra steps to make sure that the source target for the attack is notified that their enterprise and customers are under threat.

2014 Phishing Year in Review

233%

The number of phishing URLs tracked by CYREN increased dramatically in 2014, up by 233% from 2013.

In 2014 CYREN tracked over

2,500,000

Phishing URLs, compared to only 765,000 in 2013.

Common Brand Names Used in Phishing Attacks in 2014

Most phishing attacks used brand names commonly known (and likely used) by the target victims, such as PayPal, Apple, Chase Bank, Postbank.de, and Facebook. However, there were some notable new names among phishing targets this year, including AirBnB and online gaming sites, such as the NCSOFT Games GuildWars, Blade and Soul (Blade and Soul phishing specifically targeted the Japanese market), and BLIZZARD's BattleNet system.

Other Well-known Brand Names	Dropbox Amazon Ebay Yahoo
Top Bank Brand Names Used in Phishing	Chase NatWest Wells Fargo ANZ Halifax RBC
Post Bank Names Used in Phishing	Postbank.de Postepay Italy
Other Brand Names with Significant Volumes	Navy Federal Credit Union USAA Military Home SFR (French Telecom Company) Tax Refund Services, including HMRC and Canada Revenue Service
Latin American Brand Names	Cielo Payments Banco Bradesco Bancolombia Itau
Asian Brand Names	Alibaba Made-in-China Taobao
Largest Single Outbreaks	Postbank.de (~93,000 URLs in three to four days) GuildWars (Online Gaming site, with ~250,0000 URLS over the course of several months, and still continuing) OKQ8 (Swedish)
Social Networks	Facebook was the unquestionable leader, with almost no phishing related to Twitter or other major social networks. Unique Names BLIZZARD Battle.net AirBNB

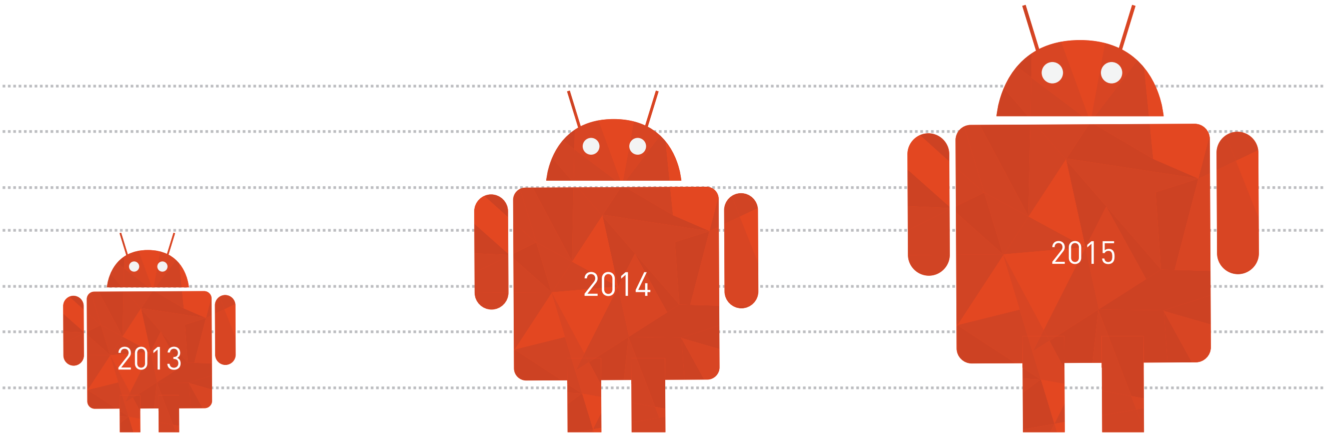
2014 Top Brand Names Used in Phishing

1. PayPal
2. Apple
3. Google

MOBILE MALWARE

MALWARE ON THE MOVE: CYREN PREDICTS CONTINUED INCREASE IN MOBILE MALWARE

Whether you're using your smart phone to login to corporate webmail or to check your bank balance, mobile business app use is here to stay. And, with increasing mobile device use comes malware designed to steal personal and corporate data, and infiltrate corporate systems. Mobile malware is now extremely attractive to cybercriminals. During 2014, CYREN noted a 61% increase in the amount of mobile malware targeting Android devices.



For the enterprise, this is particularly dangerous as employees use mobile devices to access corporate websites, webmail, and share sensitive information with other employees. CYREN believes that not only is mobile malware here to stay; but also that mobile devices will become a primary target for cybercriminals in 2015, using a variety of methods, including malvertising, ransomware, banking malware, Near Field Communication (NFC) threats, and pre-installed malware on newly purchased devices.

Mobile Malvertising

One of the key ways cybercriminals target the enterprise is through "malvertising". By inserting malware-ridden advertisements into legitimate webpages and advertising networks, cybercriminals can use fake ads as a quick and easy way to spread threats. In fact, in the past year fake advertisements were found on several legitimate sites, including Facebook, The New York Times, Spotify, and The Onion. To gain access to the legitimate sites, cybercriminals typically first place real non-malicious ads to develop trust and then eventually insert malware into the code behind the ad, duping both the website owner and the reader.

Because cybercriminals go to great lengths to make these ads seem real and attractive, malvertisements have become a highly successful threat vector; users click on the fake ad and their devices are infected. For example, an individual with an Android device scans their Facebook page and sees an ad purportedly from CNN about breaking news on a plane crash. The individual clicks on the link, only to be redirected to a fake website. In the meantime, the user has downloaded a Trojan onto their device which captures all their contact information, screen names, and passwords, including those used to login to their employer's website. With this type of information now accessible to the cybercriminal, it is much easier to infect the devices (including tablets, laptops, and desktops) belonging to other employees and ultimately develop a gateway for advanced persistent threats.

Mobile Ransomware

Ransomware will continue its destructive march through mobile devices in 2015. Early in the year, we wrote about some of the first ransomware for Android, in particular Simplocker (see call-out box) that targeted the individual with demands of payment in exchange for file decryption. In 2015, CYREN predicts that mobile devices including phones and tablets will be even more aggressively targeted with ransomware.

Near Field Communications Malware

2015 will see increased use of NFC in payment systems. CYREN believes that criminals are working to find ways to take advantage of this new technology. Near Field Communications works by enabling smart devices such as Androids or iPhones, to establish radio communications with other devices (a payment kiosk in a grocery store check-out line, for example) by bringing them into close proximity (typically less than 10 centimeters). Once in proximity the chips in each device exchange encrypted payment information. Most device manufacturers, including Apple, Google, Samsung, Motorola, LG, has incorporated NFC technology into their devices. The potential danger with NFC comes not necessarily from the device itself, but from potential for legitimate NFC software to be hacked and/or malware to be installed in the form of a separate application on the phone that intercepts data from the NFC device and captures personally sensitive information. In addition, if cybercriminals can find a way to inject a point-of-sale NFC device with a form of malware that specifically targets the NFC component, (in much the same way criminals targeted Home Depot, or use skimmer technology on ATMs), then credit card data could be captured.

Banking Malware

Mobile banking Trojans are here to stay. CYREN believes that banking malware will continue with similar infection methods to those used in 2014. The reason for this is simple—they work. For example, malware on an infected PC asks the victim to enter a phone number and mobile device type. The malware will then send the user an SMS message containing a malicious download link to the mobile device. After the victim has installed the malware on the device the attacker is able to intercept and steal sensitive information.

Pre-installed Mobile Malware

In 2014, a large number of Android phones shipped directly from a factory in China arrived with pre-installed spyware. Disguised as the GooglePlay store app, the spyware runs in the background and cannot be detected by the user, periodically sending the user’s personal data to a server located in China. The application also allows cybercriminals to secretly install other malicious applications. The type of information collected on these Android phones (model “N9500” by the Chinese manufacturer Star) includes user names and passwords, online banking data, and email and text messages among other things. Because this malware is installed in the device’s firmware, it cannot be uninstalled or deleted. CYREN expects that pre-installed malware on cheaply made phones will likely continue in 2015.

61%

CYREN noted a 61% increase in the amount of mobile malware targeting Android devices.

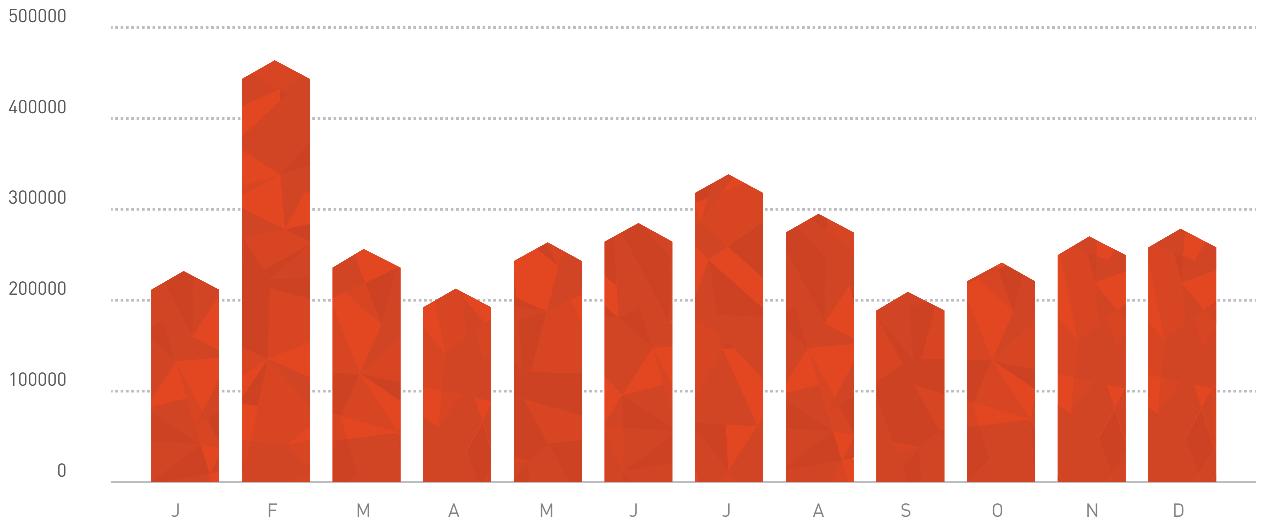
ANDROID MOBILE MALWARE: FIRST TRUE RANSOMWARE APPEARS

The first generation ransomware, known as Kohler, locked user’s screen and then displayed a message claiming that the user had been viewing child pornography. Unless the victim was willing to pay the fee to unlock the device, the police would be notified. This ransomware did no harm to the device beyond locking the home screen. To remove the malware the user simply had to factory restore the device after a backup had been done or remove the locking service with a debugging method. The second-generation ransomware, Simplocker was distributed via drive-by download from porn sites by pretending to be an antivirus application, porn application, or a system update. This malware not only locked the device screen but also encrypted specific file types, such as videos, images, documents and other personal files, requiring payment to unlock them. To propagate, Simplocker sends SMS messages to every contact on the user’s device, with a link to the malware. The ransomware uses the TOR network to connect to a command and control server; information about the infected device is then uploaded to the server.

2014 Mobile Malware in Review

Mobile malware continues to expand at an alarming rate. Android malware, in particular grew by 61% in 2014, with an average of 9,170 new samples per day and 278,940 samples per month. The largest number of samples appeared in February 2014 (463,971) and the smallest number in September (239,237).

Android Malware by Month

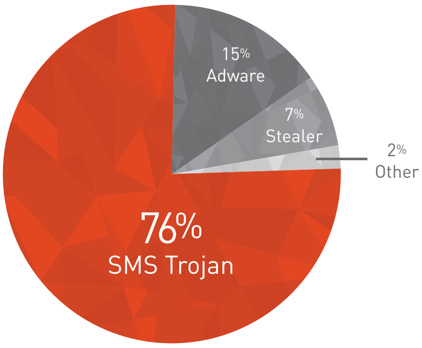


Top 5 Mobile Malware Applications for 2014

The top five mobile malware applications detected by CYREN in 2014 were:

1. AndroidOS/Airpush
2. Android OS/Leadbolt
3. AndroidOS/Revmob
4. AndroidOS/Opfake
5. AndroidOS/FakeInst

Mobile Malware by Type



In examining the Android malware clusters over a one-month period, 76% were SMS Trojan, 15% Adware, 7% Infostealer, and the remaining 2% either Exploits or some other form of malicious application.

SPAM

Spam: a Partnership in Cybercrime

Cybercriminals specialize in a variety of different areas, ranging from coding the malware to managing the botnets. As we reported in our second quarter trend report, spam in particular has one of the most advanced networks, from the harvester who steals valid email addresses, to the botmaster who controls the Internet-connected programs that distribute the spam, to the spammer who develops emails that attempt to evade anti-spam filters and entice the reader into clicking on malicious links. These roles are all intrinsic to each other, with the profitability of a spam campaign contingent upon a dependable email list, content that evades filters, and an effective botnet distribution system.

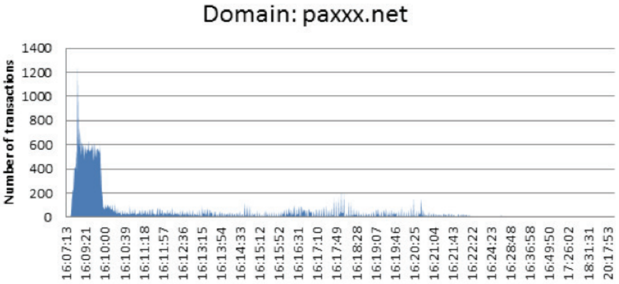
While overall the volume of global spam is declining, email nevertheless remains a primary attack vector for cybercriminals, because email spam (whether they contain pharmaceutical links or phishing links) still delivers lucrative money making opportunities for cybercriminals.

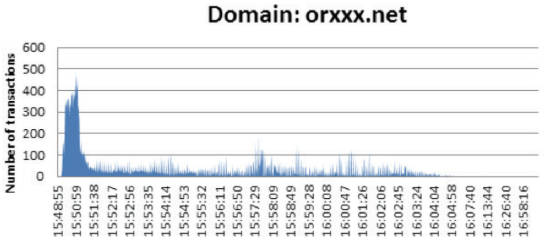
In analyzing spam attacks over the last year, CYREN observed a number of unique approaches, including rapid spam attacks, described in the following sections.

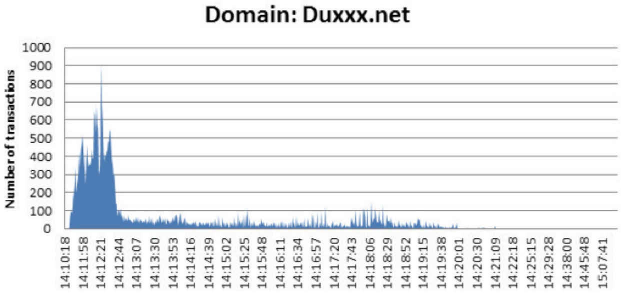
Rapid Spam Attacks

In late 2013 and early 2014, CYREN began tracking one of the largest and stealthiest spam attacks seen all year, with spammers distributing massive volumes of spam—40 to 50 million emails sent in short bursts lasting only three to five minutes each, over the period of several months.

As illustrated in the following three sample graphs from actual IP source addresses, the spam attacks would peak rapidly over a period of just minutes, and then rapid decline in volume until they had disappeared entirely from the Internet.







Through deep analysis of this attack, CYREN analysts determined that this particular spammer and his team had adapted their behavior based on past experiences with anti-spam filters. For example, to avoid detection the attackers used freshly registered domains as links. Further, in order to avoid anti-spam filters, internal email links matched both the sender domain and the Sender Policy Framework (SPF) record. (The Sender Policy Framework is a simple email validation system designed to detect email spoofing by providing a mechanism to allow receiving mail exchangers to check that incoming mail from a domain is being sent from a host authorized by that domain's administrators. Email spam and phishing often use forged sender addresses, so publishing and checking the SPF records is considered a good anti-spam technique.)

This spammer also sent emails containing diverse topics, which varied from the promotion of small businesses to a variety of different services, and avoided topics, such as pharmaceutical or gambling, that might trigger anti-spam filters. Finally, zombies from around the globe were used to distribute the spam.

Rapid Spam Propagation Methods

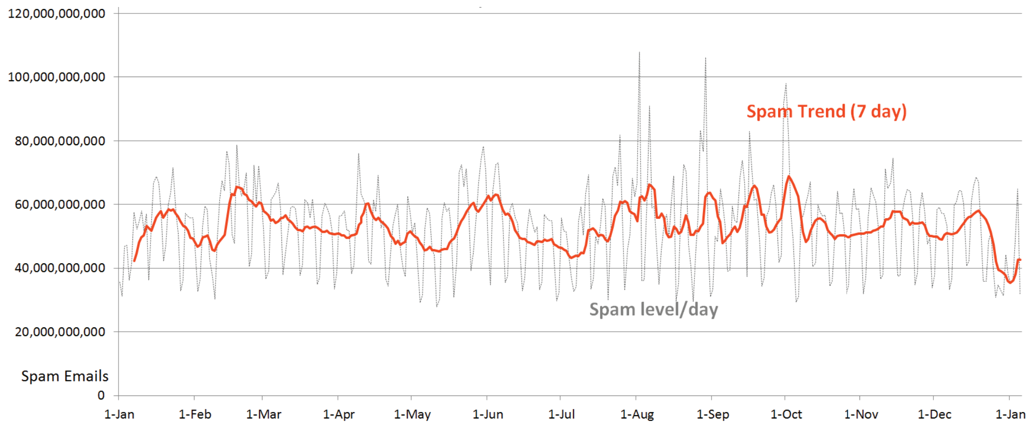
CYREN analysts believe that initially this spamming team used the "Snow Shoe" technique to spread the attack. With "Snow Shoe", the spammer employs a large range of static IP addresses to send out the attack at a very low volume. So, while the total volume of spam remains high, the volume of spam per IP address remains low. Later on, the cybercriminals began using compromised IP addresses (IP addresses from inside an infected network) to expand their attack.

CYREN's Recurrent Pattern Detection Blocks Rapid Spam

Using RPD to analyze the data, CYREN extracted and analyzed the new and volatile patterns related to this rapid spam outbreak within seconds. Unlike traditional methods which only observe known senders, known content, and known patterns, CYREN was able to block spam from this attack within seconds of seeing it within the system, and then store it in the vast RPD classification database to help further identify similar components in future attacks.

2014 Spam Year in Review

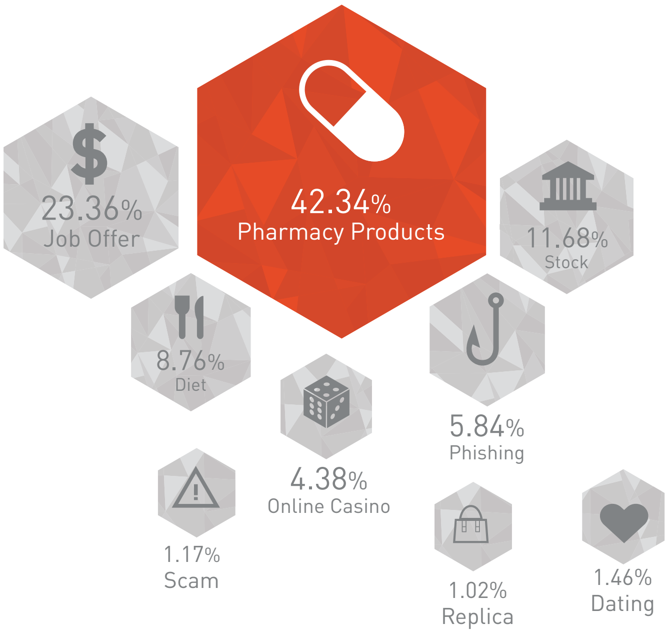
2014 Spam Levels



The amount of average spam per day declined by approximately 30% from 78.2 billion in 2013 to 54.6 billion in 2014. The months of August and May each hold the title of highest and lowest amount of single day spam, with 107.9 billion spam emails sent on the 2nd of August and 27.8 billion on the 11th of May.

2014 Spam Topics

Pharmaceutical spam led the spam topics in 2014 with 42.34% of the total, followed by job offers at 23.36%, stock at 11.68%, and diet at 8.76%. Online casinos, dating, and various other scams rounded out the remaining total.

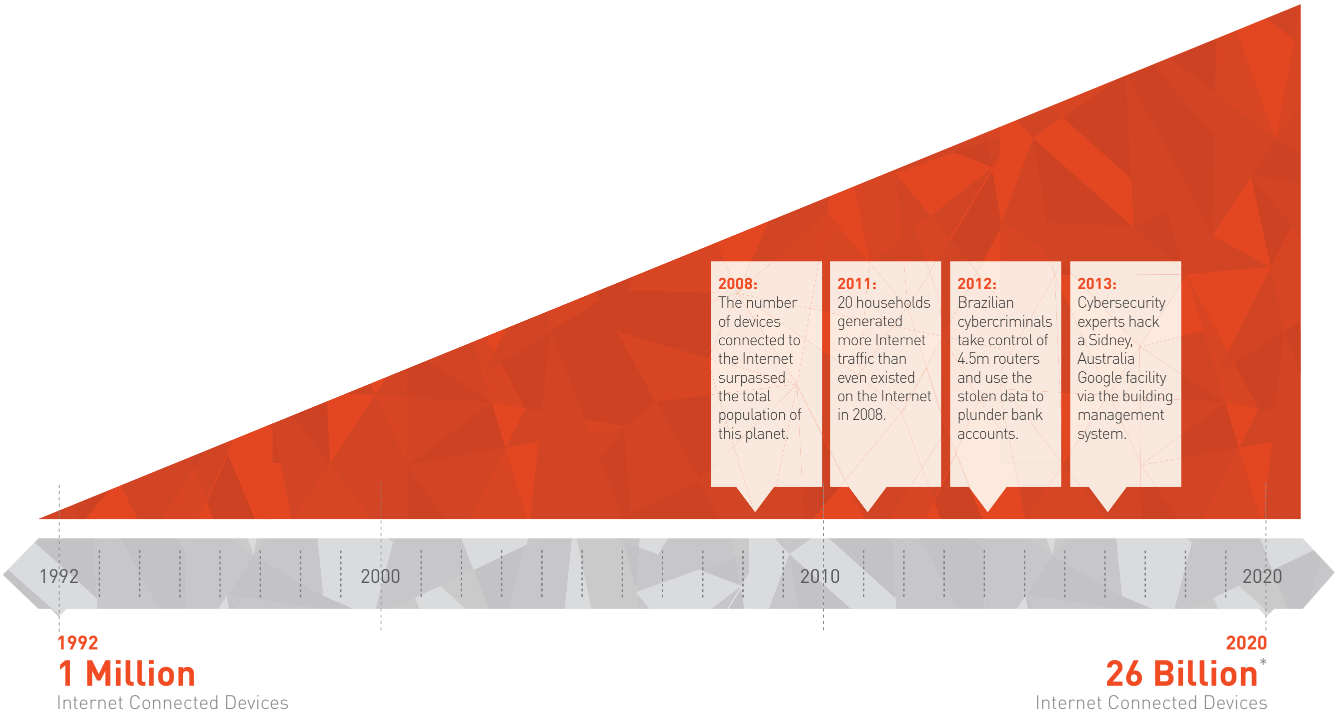


INTERNET OF THINGS

AN ASSESSMENT OF INDUSTRIAL IOT THREATS IN 2015 AND BEYOND

The Internet of Things (IoT) is hot. From light bulbs to refrigerators to smart TVs, companies are under tremendous pressure to get new IoT devices to market and consumers are instantly snapping them up. In fact, the number of devices that are or will shortly be connected to the Internet is rising rapidly.

ROI for the cybercriminal



2008: The number of devices connected to the Internet surpassed the total population of this planet.

2011: 20 households generated more Internet traffic than even existed on the Internet in 2008.

2012: Brazilian cybercriminals take control of 4.5m routers and use the stolen data to plunder bank accounts.

2013: Cybersecurity experts hack a Sidney, Australia Google facility via the building management system.

1992
1 Million
Internet Connected Devices

2020
26 Billion*
Internet Connected Devices

*Gartner

According to Gartner, by 2020 there will be more than 26 billion IoT devices in operation. Enterprises, in particular, are looking for new ways to drive efficiency and achieve significant cost savings by connecting large-scale industrial items, such as building management and security systems to "smart" Internet-connected platforms. This variation of the IoT is known as the Industrial Internet of Things, or IIoT.

In the coming year, the enterprise—from its people, to its devices, to its physical infrastructure—will become more connected than ever before. In examining the risks associated with the Internet of Things, CYREN decided to evaluate what IIoT really means to the enterprise from a cybersecurity perspective.

Industrial-scale Cybercrime

In 2013, cybersecurity experts hacked into the Sydney, Australia Google offices via the Tridium (Honeywell) building-management system. In this hack, the experts were able to view floor and roofing plans, alarm systems, equipment schedules, and piping plans. In addition to gaining access to building schematics, the security experts found that they were able to override the system controls for the building automation system, as well as gain access to any other system that ran on this same Internet-connected network. While they didn't intentionally breach other systems, the opportunity was clearly there.

As more and more corporations move to sustainable, smart, energy efficient buildings, industrial control systems (ICS) are just one of the many avenues that CYREN believes cybercriminals will begin to employ in the coming months. Corporate systems, such as building access swipe card systems or video surveillance systems, if not properly secured will present an ideal threat vector for the ambitious cybercriminal looking to make a few million (or billion) dollars over the course of a day or two.

Understanding the risk associated with IoT, in particular "Industrial IoT", will be key to protecting the enterprise in the coming years. Let's face it, the break-room smart fridge probably will not have the capacity to support an advance persistent threat, but the building-wide system that's connected via the network to the same IT infrastructure that houses the corporation's database of employee social security numbers will definitely have the capacity to host and launch a significant APT against that corporation.

CYREN is Protecting the Industrial Internet of Things

Using its database of 17 Billion transactions, CYREN is working today to deliver Internet of Things protection for the enterprise. For example, by developing a profile aligned to a building management system, we can define what a normal conversation in an ICS system might look like. Deviant data or "conversations" occurring in an ICS system would immediately be flagged and blocked.

Today, IoT security is best achieved through a combination of embedded (software development kit (SDK)) and security-as-a-service (SecaaS) capabilities, dependent on the type of IoT device in use and the ultimate value of that IoT device to a cybercriminal.

"Give Me Money. That's What I Want."

Ultimately, regardless of the type of IoT device—be it building management system, video surveillance system, or refrigerator—there is no question that money is the intrinsic driver for cyber-criminals. Gone are the days of the virus writer that simply wanted to gain a reputation. And, gone are the days of malware developed solely for the purpose of destroying hard drives and data; the value of sophisticated, undetected malware is much too high to simply use it for destruction. While privacy breaches, hacktivism, and terrorism remain potential end goals for attacks, for the vast majority of cybercriminals, it's money they want. And, if they can make a buck (or a few millions) by using an industrial IoT device to breach a corporate network, then you can bet that it will happen.

How Does an IoT Hack Happen?

While there is a fairly wide range of possible IoT breach vectors for a creative cybercriminal, the three most likely ways to engage in a malicious attack on an IoT device are through:

Poor Password Protection—Connected devices will come with a password that many users don't know how to reset; or if they do know how, they may reset it with an easily hackable one, such as "Password".

Firmware Exploit—Firmware can be exploited to change the behavior of a device and alter how the computing resources are utilized.

Other Bugs and Vulnerabilities—Cybercriminals regularly look for security holes or vulnerabilities in programming code. Once found, access into the system is fairly simple.

The Future of Internet of Things

In 2020 Gartner Estimates:

26B

Over 26 BILLION Internet-connected devices

Over a quarter billion connected vehicles on the road with automated driving capabilities

$50B

Booming low cost surveillance and spying generating a $50 billion global market

CYREN

Founded in 1991, CYREN (NASDAQ and TASE: CYRN) is a long-time innovator in cybersecurity. With full-function Security as a Service (SecaaS) solutions and security technology components for embedded deployments, CYREN provides web, email, endpoint and mobile security solutions that the world's largest IT companies trust for protection against today's advanced threats. CYREN collects threat data and delivers cyber intelligence through a unique global network of over 500,000 points of presence that processes 17 billion daily transactions and protects 600 million users. For more information, visit www.cyren.com.

CYREN Security Solutions

CYREN WebSecurity

CYREN WebSecurity delivers enterprise web security in an 'as a Service' model; protecting today's enterprise network with today's security technology. With CYREN WebSecurity, businesses gain massive improvements in protection, cost effectiveness, and control by switching to cloud-based protection. The enterprise can simplify its network infrastructure by allowing remote users to connect directly to the Internet through the CYREN global security platform, removing the need to bring traffic back to the security appliances. CYREN WebSecurity is powered by the Cyber Intelligence Platform that protects more than 600 million users, through 500,000 global points of presence.

CYREN AntiMalware

CYREN's anti malware solutions—Embedded AntiVirus and Mobile Security for Android—provide the best and broadest protection against new and zero-hour threats. With Embedded AntiVirus, businesses enjoy industry-leading performance with ultra-low processing, memory, storage, and band-width consumption. CYREN Mobile Security for Android delivers a comprehensive security Web and antivirus foundation for providers of mobile applications or services.

CYREN EmailSecurity

CYREN email security technologies provide industry-leading protection. Our email-security-as-a-service, virus outbreak detection, inbound and outbound antispam, IP reputation, phishing URL feed, and zombie IP feed solutions are simple to administer and scale to whatever size your business needs; protecting your employee and customer inboxes from threats across all devices. CYREN EmailSecurity solutions are available in both embedded and security-as-a-service models.

CYREN

U.S. HEADQUARTERS
7925 Jones Branch Drive, Suite 5200
McLean, VA 22102
Tel: 703-760-3320, Fax: 703-760-3321
www.CYREN.com

USA
1731 Embarcadero Road, Suite 230
Palo Alto, CA 94303
Sales: 650-864-2114
General: 650-864-2000
Fax: 650-864-2002

ISRAEL
1 Sapir St., 5th Floor, Beit Ampa
P.O. Box 4014
Herzliya, 46140
Tel: +972-9-8636 888
Fax: +972-9-8636 863

GERMANY
Hardenbergplatz 2
10623 Berlin
Tel: +49 (0)30/52 00 56 – 0
Fax: +49 (0)30/52 00 56 – 299

ICELAND
Thverholti 18
IS-105, Reykjavik
Tel: +354-540-7400
Fax: +354-540-7401