APRIL 2018

CYREN

CYBERTHREAT Report

The Phishing Issue

From Targeted Attacks to High-Velocity Phishing

TABLE OF CONTENTS

INTRO: Phishing on the Rise in Business Seas 3

PHISH GUTS: The Anatomy of a Phishing Attack 4

PHISH SCHOOL: Understand Phishing Terminology 5

TROPHY PHISHING: How Business Email Compromise Reels in the Big Catch 6

PHISHING FOR FUNDS: Financial Phishing & Tax Refund Theft Soaring 9

THE PHISHING HURRICANE: Targeting Victims of Natural Disasters with Phishing 10

THE PHISH ARE BITING: What Companies Can Do to Improve Protection 11

ANTI-PHISHING ECONOMICS: What's the ROI on Phishing Security? 12

PHISH FOOD: An In-depth Interview with Cyren Phishing Expert Andrey Maevsky 13

THE PHISH MARKET: Why Trusted Brands Can't Always Be Trusted 17

GONE PHISHIN': Phishing Sites Don't Last a Zero Day 18

Cyren GlobalView Threat Data Update: Q4 2017 19

Phishing on the Rise in Business Seas

> “Phishing attacks are growing exponentially. So must the response.”

In the last year, the number of active phishing URLs being monitored by Cyren’s global security cloud has grown by 93%, to over 10 million. To be clear…this is net growth. Consensus estimates are that, on average, 1.5 million new phishing websites are created every month, and studies show that half of these URLs have served their useful life and are already inactive within 24 hours, as phishing campaigns are aggressively managed by the phishers. [You can read more on p. 18 about zero-day phishing sites.]

Interestingly, the increase in phishing is seen at both the volume level, as well as the targeted recipient level, with a significant upswing in both large-scale botnet-distributed campaigns and targeted “spearphishing” and “whaling” attacks.

The reality is that phishing was the most successful type of attack on businesses in 2017, with 29% of IT managers reporting a breach, according to the annual Cyren-Osterman Research survey conducted in September. (Number two was ransomware, with 18% of businesses reporting at least one infection in the prior 12 months.) The size of the organization doesn’t matter—these statistics are from mid-sized companies with 100-3000 employees.

Phishing is on the rise for several reasons—most fundamentally because it works. Phishing provides a robust ROI to the criminal gangs behind it, as barriers to entry have fallen and the “phishing-as-a-service” economy has evolved to lower costs and make it possible for even the non-technical aspiring criminal to get into the game. We also can’t lose sight of the fact that phishing’s primary distribution channel—email—is the easiest and only reliable way to reach business users directly.

Cyren is uniquely positioned to observe, analyze, and halt phishing attacks as they happen. In this updated phishing issue, we explore recent trends in phishing, provide insight into the mind of a phisher, and examine the lifecycle of a phishing site. To begin to stem the increasingly negative impact of phishing, companies must continue the shift to cloud-based security with the kind of real-time detection and blocking of suspected zero-hour phishing sites that Cyren’s security cloud provides.

Siggi Stefnisson
Vice President of Threat Research
Cyren

PHISH GUTS

The Anatomy of a Phishing Attack

While most folks know what phishing is, few realize the lengths to which a criminal will go to initiate a phishing attack. More than just distributing emails with fake corporate logos like LinkedIn or Facebook, cybercriminals design attacks carefully by using fake clickable advertising, spoofing well-known online brands, and creating legitimate-looking phishing websites to capture the sensitive data that the unsuspecting victim enters.

STEP 1 VICTIM IDENTIFICATION

Mass Phishing Attack
- Untargeted, large group of victims.

Targeted Phishing Attack
- Specific group, or high profile victim.

$2.3 BILLION

Amount lost to businesses in the last three years due to targeted spear phishing of CEOs, according to an FBI report.

STEP 2 SOURCE SETUP

Brand Names
- Phisher selects a brand name for mass email distribution, such as Apple, PayPal, or Dropbox
- Using a newly created domain or a hacked website, hacker builds webpages that resemble the one for the trusted brand name.

98%

98% of phishing website URLs target name brands such as Apple, PayPal, Dropbox, Google, and Microsoft

Sophisticated Content
- Phisher develops an email with legitimate-looking content such as legal or financial information.
- Spoofs the email address of someone at the target organization or of a known contact to the target.

STEP 3 DISTRIBUTE ATTACK

$3 BILLION

The FBI estimates a 1300% increase in business email compromise attacks (BECs) between 2015 and 2017, with total estimated losses of more than $3 billion.

Mass Distribution
- Phisher sends a mass distribution email containing brand logos/name and links to fake webpages.
- Places links to fake web pages in banner ads, on social media, or in text messages.

Targeted Distribution
- Phisher sends email to specific target victim or group.

STEP 4 HOOK VICTIMS

Click Fake Links
- Victims click on link in the email and enter sensitive credential information into fake web page.

Respond Directly To Email Request
- Victim responds directly to email with requested information, such as login credentials or financial information.

28%

Percentage of phishing attacks that targeted a specific victim

81%

Percentage of hacking-related breaches that leveraged either stolen and/or weak passwords*

*SOURCE: 2017 Verizon Data Breach Investigations Report

STEP 5 EXPAND OR MONETIZE

Develop Additional Attacks
- Phisher uses stolen credentials for the next phase of the attack (such as an APT).
- Collects additional email addresses from hacked accounts for future attacks.

Financial Gain
- Phisher sells the stolen credentials on the black market.
- Phisher steals money using credentials from bank, PayPal account, or fake wire transfer.

$60 MILLION

Amount stolen from SMBs in financial phishing scams by a cybercriminal recently arrested by Interpol

PHISH SCHOOL

Understand Phishing Terminology

THREAT TYPES

PHISHING

A homophone of the word 'fishing,' phishing is an attempt to entice a person into providing sensitive or confidential information which can be used or monetized by cybercriminals. In a phishing scam, criminals distribute electronic content to a series of victims, in which the content is specifically designed to trick the user into engaging in a particular activity, such as clicking a link or responding to the email. The victims, thinking the content is real, provide the phisher with personally sensitive information such as usernames, passwords, banking, financial, and/or credit card details. Methods of phishing distribution include email, online advertising, and SMS.

SPEAR PHISHING

A targeted phishing attack focused on a specific person or group of people and often involves research and spoofing of the sender name and e-mail address. Blocking these types of attacks usually requires "imposter protection" security capabilities.

CLONE PHISHING

A phishing attack in which the 'phisher' uses a genuine, previously delivered email to create an identical (or almost identical) email containing similar content, attachment, recipient, and sender email address. A fraudulent link or attachment replaces the original one. Because the email appears to come from a legitimate source, this spoofed email is used to gain trust with the victim.

WHALING

A form of spear phishing focused on senior corporate executives or high-profile individuals, such as those in government. Often the threat actor uses a business email compromise (BEC) scam to gain access to the executive's email. Email content may take the form of a legal request, customer complaint, or an executive-level issue. The content may request the recipient perform a task, such as providing employee records or sending a wire transfer, or contain malicious links that when clicked and viewed have a highly professional and legitimate look and feel.

PRIMARY PHISHING ATTACK TACTICS & TECHNIQUES

PHISHING EMAIL WITH LINK TO FAKE WEBSITE

This is the most common form of phishing. Usually an email arrives in a victim's inbox that appears to be from a well-known brand, such as Amazon or eBay, requesting that the victim update his credentials.

ONLINE AD WITH LINK TO FAKE WEBSITE

It is increasingly common for a fake advertising banner or text advertisement to appear on a website that links back to a malicious URL. The unsuspecting victim clicks the link and enters credentials on the fake site. The sensitive information is then captured and saved by the cybercriminal.

SOCIALLY ENGINEERED EMAILS TO PERSUADE VICTIMS

Used increasingly by phishers, this type of technique involves socially engineering an email by spoofing the sender's name to make it look like it came from someone the victim knows, such as a colleague (often the CEO or another executive in the firm), a legal representative, a vendor, or a friend. For example, the head of accounting might receive a spoofed email from the CEO asking him to provide a password or specific corporate or financial information. The unsuspecting accountant does as requested, without realizing that he has provided sensitive data to cybercriminals.

TROPHY PHISHING

How Business Email Compromise Reels in the Big Catch

In the world of phishing, there are two types of "phishers:" those that use their nets to scour the ocean and capture as many victims as possible, and those that use a single rod and reel to catch the big haul trophy—the corporate executive, government official, celebrity, or other high-profile individual. This sophisticated and targeted form of phishing—called spear phishing or whaling when directed at high-level business executives—is on a dramatic upswing.

Spear phishing in the form of business email compromise (BEC) attacks have been increasing in number over the last few years, driven by their relative success rate compared to other financially motivated attacks. The FBI estimates a 1300% increase in BECs between 2015 and 2017, with total estimated losses of more than $3 billion. The 2017 Verizon Data Breach Investigations Report also calls out BEC as a major threat. In one reported incident, Leoni AG, the world's 4th largest manufacturer of wire and electrical cables, lost €40m.

Security researchers find that BEC attacks often take two forms: (1) A multi-phase attack, in which the attacker has gained access to the actual target's email account. Protection from this type of threat requires upfront URL protection so the phishing link doesn't arrive in the victim's inbox in the first place. (2) Email spoofing, which involves the attacker manipulating the names in the email fields or faking a corporate website domain to make it appear as if the email arrived from an internal or familiar external source. Protection from email spoofing requires email security that has an 'impostor detection' component, which is able to flag and block a spoofed email account or domain.

MULTI-PHASE SPEAR PHISHING

THE SCENARIO

In the latest BEC trend, cybercriminals are using social engineering to attack targets in multiple phases. Rather than engaging in a full assault at the onset with a fake request for corporate passwords or financial information, cybercriminals are now taking a little more time and slowly infiltrating an organization, first for reconnaissance and then to build the foundation for an attack that looks legitimate.

HOW IT WORKS

STEP ONE: Infiltration using scare tactics—Imagine you're a mid-level employee at a small- to medium-sized corporation and suddenly you find an email in your inbox telling you that your corporate Office 365 account is temporarily suspended because your password is expired and your email address needs to be reactivated. You click the link and it takes you to a web form on what looks like the Microsoft Office 365 site. You're asked to provide your corporate email address and current password, as well as other personal information such as company name and title, in order to reactivate the account.

Given employees' dependence on email, they are frequently highly motivated to avoid any possible interruption. And, frankly, for better or worse, today most employees are accustomed to receiving requests to update their passwords, making the fake 'deactivated email account' technique a fairly common and successful ploy. It's also not a direct pitch for financial records or credentials, which (for some) immediately raises a red flag. Criminals also know that robust cybersecurity services, as well as two-factor authentication, are not in use as often at small- to medium-sized businesses.

Block at the Beginning

The primary way to block a multi-phase spear phishing attack is at its start—with the original URL that arrived via email requesting, for example, an Office 365 email password. Security services should stop users from accessing phishing URLs with immediate "time-of-click" analysis and blocking, as well as with protection that identifies and blocks just-released "zero-day" and previously unknown phishing links based on the correlation of data across transactions.

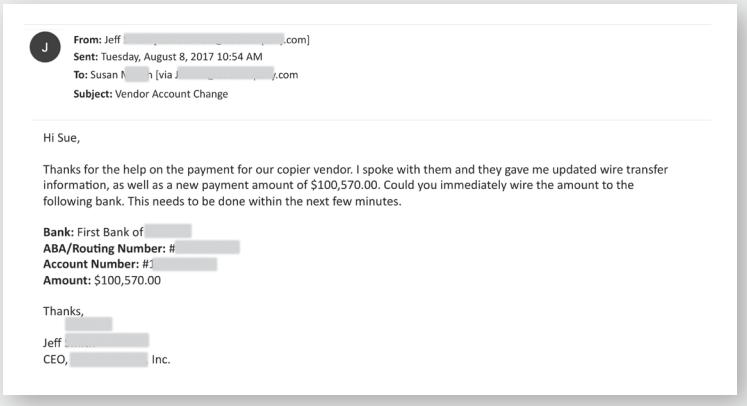
TROPHY PHISHING

continued from previous page

STEP TWO: Infiltration Survey & Exploration—Armed with your corporate login and password, the criminal can now survey the landscape, reading your email to learn more about the organization and get details about who you work with, who your customers are, the names of decision-makers, who manages HR data, who controls the finances, etc.

STEP THREE: Launch Attack—Having these details enables the criminal to launch an effective spear phishing attack. For example, using your email address, the criminal might send an email to your team member in accounts payables, who you've been working with to get one of your vendors paid. The email might look something like the example on the right.

Because the email arrives from a legitimate internal account, the targeted employee responds by initiating the wire transfer.



From: Jeff [redacted].com]
Sent: Tuesday, August 8, 2017 10:54 AM
To: Susan [redacted] [via [redacted].com
Subject: Vendor Account Change

Hi Sue,

Thanks for the help on the payment for our copier vendor. I spoke with them and they gave me updated wire transfer information, as well as a new payment amount of $100,570.00. Could you immediately wire the amount to the following bank. This needs to be done within the next few minutes.

Bank: First Bank of [redacted]
ABA/Routing Number: # [redacted]
Account Number: #1 [redacted]
Amount: $100,570.00

Thanks,
[redacted]
Jeff [redacted]
CEO, [redacted] Inc.

This email arrives from a real—but compromised internal account—making the scam more likely to succeed.

EMAIL SPOOFING

THE SCENARIO

Email spoofing is similar to the multi-phase example mentioned previously, in that an email arrives in an recipient's inbox appearing as if it came from an internal source, such as the CEO or another executive, or a well known external source, such as a vendor, accountant, or lawyer. However, in these instances, the email account itself has not been compromised. Instead the attacker "spoofs" the sender's email address or website domain to make it appear as if the email came from a known source.

The success of these attacks is based on the simplicity of the email that is sent. It will contain no malware, no attachment, and no links, all of which are the traditional threat signs. Impostor email attacks are typically low volume and targeted, rendering most defenses that rely on traditional end-point detection methods useless. The attacker ensures maximum success by hand-crafting each email to appeal to the target recipient.

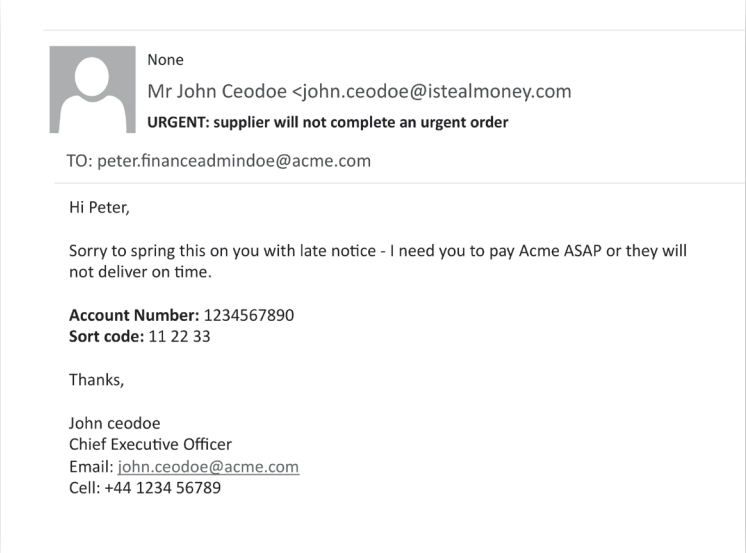
With no malware or attachments, endpoint detection will likely not identify and block the threat. That leaves the unsuspecting recipient in the finance team as your last line of defense.

continued from previous page

HOW IT WORKS

Your finance administrator has just received an email from the CEO telling him to send money to a vendor, so that they can deliver an urgently needed service or a product, and it needs doing NOW. How much time should he spend trying to decide whether the email is a threat or not? How much training is enough? And how much reliance can a business realistically place on non-technical users?

Some impostor emails are easier to recognize than others. For example, simply hovering over or clicking on the actual sender email address to ensure it matches the CEO's email address, rather than relying on the "from" field, will quickly demonstrate whether an email is legitimate or not. However, this assumes that the recipient takes the time to actual hover over the email address to verify authenticity, instead of instantly reacting to a "CEO request" to get something done asap.



None
Mr John Ceodoe <john.ceodoe@istealmoney.com
URGENT: supplier will not complete an urgent order

TO: peter.financeadmindoe@acme.com

Hi Peter,

Sorry to spring this on you with late notice - I need you to pay Acme ASAP or they will not deliver on time.

Account Number: 1234567890
Sort code: 11 22 33

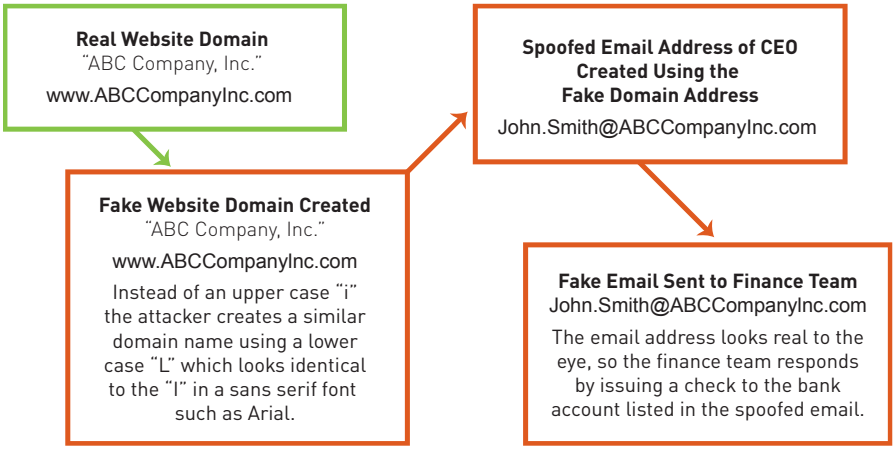
Thanks,

John ceodoe
Chief Executive Officer
Email: john.ceodoe@acme.com
Cell: +44 1234 56789

An example of what a spoofed email might look like.

IDN HOMOGRAPH ATTACK OR SCRIPT SPOOFING

More difficult to spot are attacks involving lookalike domains, also sometimes called an internationalized domain name (IDN) homograph attack or script spoofing. These attacks require a bit more effort from the attacker, who registers an email domain that reads like the target company's. It might be the same, except for a single character that has been replaced, dropped, or added. The CEO's name is then used to create a legitimate email address on this similar domain. The result is that all email fields appear valid, with the sender's name and email address seeming to match, but on closer inspection, they belong to a domain that just resembles the recipient's company's own.



Solve the email spoofing problem and keep users productive

Protecting from email spoofing requires an impostor detection capability that is fully integrated with existing email security. It should examine all of the email fields, including the subject and body text to look for the tell-tale signs of social engineering, as well as an examination of the email domain to determine whether there might be a close match with the company's own. It should also allow for input of a list of those users whose addresses an attacker might try and spoof. When the results of all of these tests are correlated, this impostor detection capability should determine the likelihood that an attack is underway and quarantine or tag emails as appropriate, based on this likelihood.

PHISHING FOR FUNDS

Financial Phishing & Tax Refund Theft Soaring

For the last few years, residents of countries around the globe have experienced a dramatic increase in the number of tax and financial phishing schemes.

It should come as no surprise that cybercriminals are taking advantage of the sense of urgency and seriousness with which most people take tax and banking matters. This, combined with an increase in cloud-based financial services, such as automated online tax submission and online banking, makes tax-based and financial phishing scams a profitable focus area for most cybercriminals.

But, urgency on the part of your average honest taxpayer isn't the only reason that cybercriminals are getting away with millions. The proliferation of crime-based "as-a-service" models is also to blame.

In both the legitimate and criminal business worlds, cloud-based "as-a-service" models are growing at a tremendous rate. The evolution of "phishing-as-a-service" (PhaaS) has significantly reduced the cost of entry for the wannabe hacker and it is facilitating more localized campaigns, such as the recent tax rebate phishing scam, detected by Cyren, that recently struck residents of Malaysia.

One of the prime takeaways of this trend is that the phishing service industry no longer enables just large-scale phishing attacks, but also an increasing "tail" of smaller, localized phishing attacks.

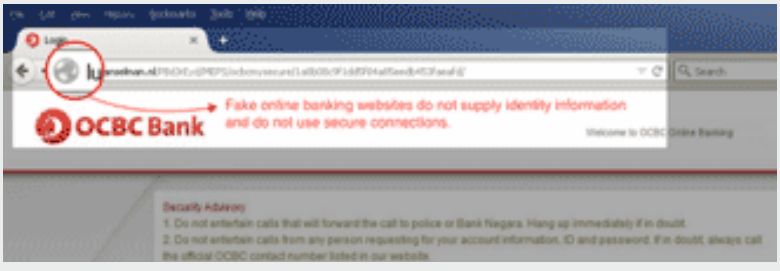
Tax/financial-focused phishing document sent to Malaysian citizens containing a shortened URL used to obfuscate a malicious hyperlink.

THINK BEFORE YOU CLICK! PREVENT FINANCIAL PHISHING

Implementing strong email gateway security can prevent both large-scale and localized phishing emails from reaching users in the first place. Email gateway security also blocks access to phishing links as a second layer of protection.

In addition, other ways to protect yourself and your company from financial and tax phishing fraud include:

- Type the address of your financial institution directly into your web browser.
- If you've accidently clicked a potential phishing link in an email, check the URL to see if it displays the financial organization's name, along with the "lock" icon to indicate you are using a secure connection.
- Enter fake credentials to see if you are rejected. Fraudulent online banking websites will typically just accept any login credentials and then redirect the user to more phishing pages to collect other types of sensitive information. Legitimate banking sites will automatically recognize the fake credentials and display a message that says the user name and password are incorrect or cannot be found.



A fake online banking login page will not supply a security login icon or a correct URL address.

Signed and verified online banking login page.

Targeting Victims of Natural Disasters with Phishing

> "In the aftermath of recent disasters, such as hurricanes and earthquakes, we're definitely seeing an uptick in a variety of scams aimed at stealing money and information"

Sigurdur Stefnisson, Vice President of Threat Research, Cyren

When the hurricane winds or earthquake aftershocks finally die down and people emerge from their places of safety, they're usually met with scenes of unfathomable disaster: houses completely destroyed, neighborhoods and places of business torn apart, and perhaps even injury and death.

While good-hearted people are ready to help with food, shelter, and aid, cybercriminals are creating a second disaster phase by taking advantage of victims and first responders with scams and phishing attempts. In the wake of the recent disasters of the last six months, Cyren's security labs observed a notable uptick in phishing attempts with subjects and content related to recent natural disasters.

How do criminals accomplish this?

Using Twitter and Facebook, cybercriminals post fake information about where victims can go for aid, where donors can give money, or where first responders can get assistance. These posts typically include a malicious URL that redirects to a fake website set up to collect donations. In addition, cybercriminals are also still using the tried-and-true method of email distribution containing fake links. When victims click the malicious social media or email links, they are taken to websites where they enter their credit card information, as well as personal data, such as name and address. Cyren analysts are also seeing searches on Google that lead to websites containing malware.

How can legitimate organizations distinguish themselves?

Legitimate organizations are finding they need to separate themselves from the unscrupulous pack of scammers. Disaster relief organizations should remind potential victims and donors to only trust established entities. These organizations can also regularly promote their actual website address and remind people to access their donation page by typing the address directly into the browser, instead of clicking on the potentially malicious and fake links they see on Twitter, Facebook, or through email.

How can both disaster victims and donors protect themselves?

Victims often find themselves out of their routines at the very best—or at worst, experiencing dramatic life and death scenarios. Donors may be viewing the disaster's impact live on television or on the Internet, or even be in communication with friends and family in the area. Both victims and donors have their defenses down and criminals leverage that opportunity. The best approach is to only trust well known and reputable entities. Unfortunately, new scams are being set up all the time. Always double check the legitimacy of the organization before you hand over personal financial information.

Businesses are targets too.

Cybercriminals are also targeting companies with phishing scams that leverage natural disasters. Cyren is seeing emails being sent directly to businesses with fake and malicious links related to disaster relief asking the recipient to click on the link, and provide personal information and credit card data.

What Companies Can Do to Improve Protection

With phishing increasing exponentially, companies need to think comprehensively about what they can be doing to protect and defend against phishing attacks.

PASSWORD MANAGEMENT

Password re-use makes phishing attractive for criminals. A breach into one system containing user names and passwords means that criminals will likely try to exploit the user names and passwords on other systems. Experts recommend a password manager that creates different and unique passwords for every site. Password managers also won't autofill information into a phishing site!!

TWO-FACTOR AUTHENTICATION

By requiring employees to use a combination of two different components in order to log into a website, such as something an employee knows (a PIN or password) and something he possesses (a phone or token), the user's identity is more likely to be verified as legitimate.

PHISHING INTELLIGENCE

Ensure your cyber security includes real-time phishing intelligence that draws from large data sources and analytics and provides real-time protection from emerging web threats on all devices, including smart phones and tablets; immediate phishing threat notification; and continuous protection for all users.

INTEGRATED WEB AND EMAIL SECURITY

Integrate your web and email security solutions to enable threat correlation across vectors and stop threats more quickly. Provide your employees with immediate protection from dangerous phishing attacks through powerful cloud-based Email Security Gateway and Web Security Gateway services. Email security filters an organization's inbound and outbound email to protect users from phishing threats, and should also offer time-of-click protection and impostor protection. Web security services protect company assets through multi-layered security which blocks phishing on any device, at any location.!

USER TRAINING

Educate and train employees on the dangers of phishing. Training options include everything from basic PowerPoints with phishing examples to simulated or "fake" phishing attacks to improve awareness for employees who fail the test and to ensure employees don't become complacent. Consider including the cost and implications of a successful phishing attack in your training so employees know how serious these types of attacks are.

What's the ROI on Phishing Security?

According to recent reports, in 2017 an estimated 70-80% of all businesses experienced a phishing attack. In the Cyren-Osterman Research security surveys of 2016 and 2017, IT managers rated it the top concern, along with ransomware. Yet many IT professionals continue to feel challenged in making a business case to upper management for adding more advanced email and web security to protect against this encroaching threat.

In a new report, security industry analyst Derek Brink of the Aberdeen Group has crunched the numbers and put a bottom line on the real risks and cost impact of phishing attacks, providing calculations for companies of different sizes and in different industry sectors. Using real world data sets from sources that include the Verizon Data Breach Investigations Report, NSS Labs, and Cyren Security Labs, the paper explains why phishing attacks are bypassing security and reaching users so often today, and lays out the new type of security required to better defend against them. He further quantifies the financial risks posed by phishing, and how to think about—and justify—IT security investments at your company from a business perspective.

THERE IS A LOT AT STAKE IN THE FIRST FEW MINUTES

According to Brink, the speed of your security is everything. Consider that the median elapsed time from phishing email receipt to the first user open is less than two minutes, and the median time from opening the email to the first user click on a phishing URL is less than four minutes. Taking this a step further, Brink calculates that 80% will have already clicked on the URL by the end of the first 60 minutes of a phishing attack. More profoundly, by the end of the first 24 hours, attackers have already hooked 99% of their eventual phishing victims—effectively, the phish is done.

The speed at which phishing campaigns operate is also evident in the extent to which phishing sites are actively managed. Brink cites statistics from Cyren's global security cloud which show that a full 20% of all phishing sites have served their purpose and are gone within the first hour, and 50% are inactive after the first 24 hours.

BEWARE THE "LONG TAIL"

Brink further warns that most businesses fail to fully account for phishing risk and probability. He crunches numbers in a statistical model to show that there's a 10% likelihood that losses from a successful phishing attack could cost a given business over $10M, on an annualized basis. He begins his assessment by calculating the median annual business impact of a successful phishing attack at $260,000 for a business with 1,000 users. He also calculates the probabilities of a range of losses, from low to high, including the likelihood of a catastrophic loss (defined as over $10 million) in a section where he explains the "long tail of risk." Brink argues the small but real risk of large losses in this "long tail" must be taken into account when defining what kind of security protection a business wants to have in place, instead of just focusing on average risk.

He then turns to the question of how to quantify the extent to which an investment in advanced email and web security services could reduce phishing risk, concluding that a modest investment in advanced email and web security offers a return on investment of 11.7 times , with an even greater potential pay-off in the millions of dollars as a result of reducing the "long tail" risk.

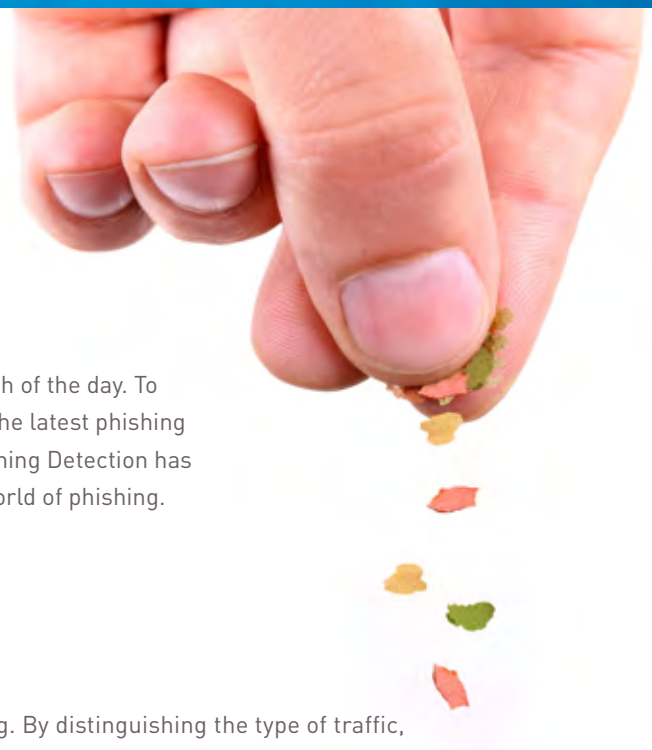
PHISHING ATTACKS ARE FAST. EVEN FASTER DETECTION MEANS BETTER PROTECTION

In the report, Brink also frames the problem with today's defenses by focusing on the timeline of phishing attacks, concluding that effective defense is really about speed. In the end, Brink tells us, protection needs to move faster than both attackers and users. He concludes his analysis by emphasizing the need for high-speed security solutions predicated on automated analysis and the correlation of massive amounts of data, in order to stop phishing emails before they reach users.

Complimentary copies of the report "Reducing the Risk of Phishing Attacks: It's About Time" from the Aberdeen Group are available at www.cyren.com.

PHISH FOOD

An In-depth Interview with Cyren Phishing Expert Andrey Maevsky



Cyren's team of anti-phishing experts is dedicated to protecting customers from becoming victims of 'phishers'.

Experience has taught us that phishers will go to great lengths to net the catch of the day. To capture information about the 'phishers' themselves, and better understand the latest phishing threats, Cyren's own Andrey Maevsky, Program Manager and Director of Phishing Detection has honed his knowledge and skills over the years by immersing himself in the world of phishing.

Aside from email, how are phishing attacks distributed?

Great question, because most people assume that email is the only way. Phishing via email is still the classic and old fashioned way to implement a phishing attack, and still very common, but there are other methods including social media, online advertising, and even text messages.

We are also seeing steady growth in social media phishing. It is an increasingly lucrative choice for the cybercriminal because there is so much personal data already available on the internet about the victim. We are also seeing links distributed by bots to social media websites, however, over the last year social media users have become a little more aware of the bot problem, so in general users are becoming more cautious of any type of social media posts and click-throughs. In terms of online advertising, we also seen a phishing attacks using actual "Ad Words," although this is extremely rare, since Google has many layers of protections in place.

We've also seen all types of phishing using fake advertising, including banner ads. In fact, sophisticated criminals can distinguish between the traffic that comes from a possible victim and traffic that might be coming from the corporate source looking to check up on the advertising. By distinguishing the type of traffic, the phishers can redirect the users accordingly; victims go to phishing sites; corporate website staff to "real" advertising sites.

The third way we are beginning to see phishing is through text messages, SMS, etc. It isn't very common yet, but we do expect to see an increase in this type of phishing threat in the coming years. We've even tracked an iPhone phishing attack using SMS. Unfortunately, while there is potential for an increase in this type of attack, telecom service providers are not yet including SMS or text messaging protection for their customers.

In the end, phishing is like every other industry—the bad guys want to use every possible channel to maximize their revenues, and they're working hard to optimize revenue by being creative. For our part, we're always trying to get into the heads of both the bad guys and the victims, because if you understand both sides, the better chance you have of protecting users.

continued from previous page

Do phishing pages also serve up malware?

Sometimes yes. Sometimes no. In the end it is about revenue. Malware on phishing sites could potentially mean more revenue for the cybercriminal, but it also means more cost and work in terms of purchasing and creating the malware or paying someone to deploy on the phishing site. The cybercriminal is also increasing the possibility that the fake site will be discovered through malware detection, so it means more risk for the cybercriminal since a working phishing site could get taken down based on the malware.

How does Cyren differentiate between ordinary spam and phishing emails?

There are really three different types of emails that are sent with the sole purpose of extorting money or information from the victim. The first is classic spam—that is, gambling/casino, pornography, pharmaceutical spam, etc. This type of email forms the basis for the spam economy. Since personal or financial credential theft is not the aim here we don't consider this a form of phishing.

Then there are the "419" email scams; the ones claiming to be from a wealthy prince who wants to 'give' the victim millions of dollars in cash. These types of scams are rarely purely digitally based; the victim isn't directed to a website to provide credit card information, instead, the victim begins one-on-one email interaction with the criminal who engages in human and social engineering. The victim will most likely lose credentials, as well as money, at some point in the scam, so Cyren considers this a form of phishing.

The third type of email is the classic 'phishing' email that people and security professionals commonly associate with the term; emails with fake logos and links that redirect the user to a website that captures personal or financial information.

With all three types of emails, we use a variety of prevention and protection techniques, including identifying the IP reputation of the sender, examining links, analyzing text, and cross referencing between emails by looking at things like the subject, domain, IP address and reputation, etc.

With a classic phishing attack (not spam or 419), we can also analyze the URL that is typically included in the email to look for clues that the criminal is trying to make the URL look reliable by placing words or links to legitimate and trusted sites, like PayPal. In addition, we examine the structure of the website and its meta data, such as the domain's history, who it's registered to, etc. This is all done in an automated, "big data" way in our security cloud in order to correlate and analyze all the interrelationships in real time.

Are cybercriminals still using the technique of attaching an HTML file in phishing attacks?

Yes, but they've become less significant. With email attachments, people are more aware of the security issues and are being more careful about opening them, so criminals are using them less. From a threat perception perspective, victims tend to view attachments as a threat, but perceive links as safe and are thus more likely to click on them.

How do phishers actually use the website or domain for the phishing attack?

The answer really depends on whether the domain belongs to phishers or whether it is a compromised site. It also depends on how well the attack is planned and prepared. If the criminal owns the domain, there are no limitations in the number of different pages or the ability to generate randomness on the subdomain and/or path level to spread the attack load and improve the chances of not being detected. With compromised sites, the criminals don't have as much control. There is also less variance and less organization with the URLs. But of course there are exceptions.

Another trick we've seen increasingly in the last year are attacks that are initiated before the phishing site is actually up. There is a lot of human engineering here; the criminals send the phishing attack during the night when people are asleep and will not read the email. Upon arrival in the night, the email is scanned by the anti-spam filter, and the domain appears clean. However, in the morning when people wake up and check email, the linked page now contains phishing content.

continued from previous page

How many phishing pages could be hidden in a hacked website?

We've seen sites with as many as 5,000 pages hidden within. Setting up these sites is an automated process, just like sending emails. As long as you have some script that can generate pages, and you know how to link between the pages and the emails you are sending, then there is really no restriction on the number of pages a criminal can create.

The website cupsandcakes.cl hosted over 5,000 phishing pages.

Do anti-phishing solutions work on a specific URL page address, or do they block the whole website?

Unfortunately, that is one of the big dilemmas with anti-phishing service providers. Because legitimate websites are often compromised, you don't want to block user access to genuine parts of the website. On the other hand, you also want to keep users from being exposed to phishing URLs. There is always a compromise and balance that is involved in providing maximum protection while ensuring the lowest possible impact on legitimate usage. The answer is also a little bit different depending on the popularity and amount of traffic of the compromised website. If you see ten phishing pages on a popular, highly visited legitimate site, you're not going to block the whole site. You also look at the diversity and pace of the attack itself.

Some anti-phishing services do block everything that is flagged. This can be very frustrating for users. And companies that do this are often not sensitive to false positives. They're taking a broad approach, but this isn't something Cyren can live with. There is always a dilemma and struggle to find the right balance and protect as much as possible, and at the same time not harm legitimate users and websites.

How many victims are typically targeted in a phishing email outbreak?

It depends. If it is a targeted attack—for example, a cybercriminal has obtained login credentials to your Facebook or LinkedIn account—then the criminal may just target the names in your contact list. Other outbreaks can be huge and designed as a blast to everyone.

What happens to stolen credentials and what do they sell for on the black market?

In the case of phishing, stealing credentials is very often for the purpose of a black market sale. (Although it could be for self-usage as well.) In terms of the price, it depends on a variety of things. One of the criteria is the freshness of the database. I've seen several databases filled with email accounts and passwords that are more than one-year old, and they're worth nothing, even if there are some emails and passwords that may still be active. The type of users on the stolen list is also important. If it is a list of celebrity accounts, it is worth significantly more than a million random user accounts. The reputation and trustworthiness of the seller is also a factor. In fact, this is so important to some criminals that it is fairly common practice to hire a middle man to check both the data and the money transfer before they purchase a list from an unknown source.

continued from previous page

Is it the same people that are doing both the phishing and credential selling?

Sometimes yes, sometimes no. Some just provide a phishing service to another cybercriminal who is interested in selling the information. You could even coin a new term "Phishing as a Service" (PhaaS).

Do phishers target specific email services or domains?

You see attacks targeted for general audiences using blanket phishing spam to everyone, regardless of the email service, and you see focused attacks on specific email domains, such as Yahoo, Gmail, and iCloud. We don't see a significant difference in amount of attacks aimed at at one email service over another.

What's the most common phishing attempt you have ever seen?

The most common usually involve a spoof of Amazon, Ebay, Dropbox, PayPal, Gmail, banking in general (specific banks are targeted, but overall the industry is a huge target), and Apple. And, this list doesn't seem to be changing overall. Sometimes phishers focus on one brand more than another, and then a few months later switch to a different major brand. But, in general, the popular phishing brands are remaining the same.

To what extent are you seeing phishing-as-a-service (PhaaS) models changing the cost of entry, technical landscape, or time to market?

Phishing-as-a-service models are definitely becoming popular, but in general, I wouldn't say that these PhaaS models are changing the cost to criminals or lowering the bar to entrance into the phishing game. The world is becoming more educated about phishing, and criminals need to overcome more obstacles to get the victim to click on the link and then respond with the data. The phishing attempt must look legitimate to work.

In terms of time to market, a successful phishing-as-a-service model requires a relationship with the PhaaS provider. Once you've established that partnership with the PhaaS provider, you can reduce your time to market in a phishing attack, but only if you are familiar and have experience with that provider.

What do you expect to see in phishing in the coming months and years?

We haven't experienced any big game changers in the last year. Phishing trends in terms of technology and approach have remained fairly steady. Over the next couple of years I expect we will see a higher level of sophistication in terms of the technical aspects, such as more random generated URLs, IP addresses, etc. Also, we expect phishers to get better at the social and human engineering with phishing sites. For example, up until a year or so ago, it was fairly common to see a phishing site with old logos, an amateur design, etc. That is likely to change with as phishers develop more sophisticated-looking websites. in terms of social/human engineering, up until a year ago it was not very uncommon to see a phishing site with old logos and old designs/layout, etc. that is likely to change with more sophisticated looking websites. Criminals will begin to adapt more quickly.

Why Trusted Brands Can't Always be Trusted

Internet platforms, financial, and shopping brands are the most popular targets for phishing, according to the most recent phishing trends.

During Q1 2018, Cyren analysts examined approximately 2.7 million phishing URLs to learn which online brands were the most frequent targets for phishers to use in their fraudulent schemes. Among the top ten, Apple, Chase, and PayPal were the top three most frequently spoofed websites, accounting for more than half of the total phishing URLs. Banks, internet services, Google, and Microsoft rounded out the top ten.

This selection of online brands by phishers provides a useful indicator of phishing motivation:

- **Financial sites are clearly targets because stolen credentials provide criminals with direct access to money and/or bitcoins, in addition to login credentials that could be resold on the black market.**
- **Online services, such as Apple, Google, and Microsoft serve as an 'Attack Platform' for cybercriminals; stolen credentials from a list of Gmail or Apple subscribers can be resold or possibly used to hack other websites, since many people use the same credentials (user names & passwords) for login on multiple sites. Additionally, email or social media logins can be used to target contacts of the victim.**
- **Shopping or commerce websites, such as Amazon and Alibaba offer criminals both credential information and the possibility of online shopping sprees or financial data if the victim stores credit card or banking information with the online services.**

Brand	% phishing URLs
Apple	17.1%
Chase	13.1%
PayPal	12.2%
Wells Fargo	2.6%
DocuSign	1.9%
Dropbox	1.9%
Microsoft	1.8%
Google	1.6%
General Email Phishing	1.5%
Alibaba	1.5%
IRS.gov	1.3%
poste.it	1.0%
LinkedIn	0.9%
Bank of America	0.9%
Facebook	0.8%
Amazon	0.7%
RBC	0.6%
Adobe	0.6%
DHL	0.4%
American Express	0.3%
Other	37.3%

GONE PHISHIN'

Phishing Sites Don't Last a Zero Day

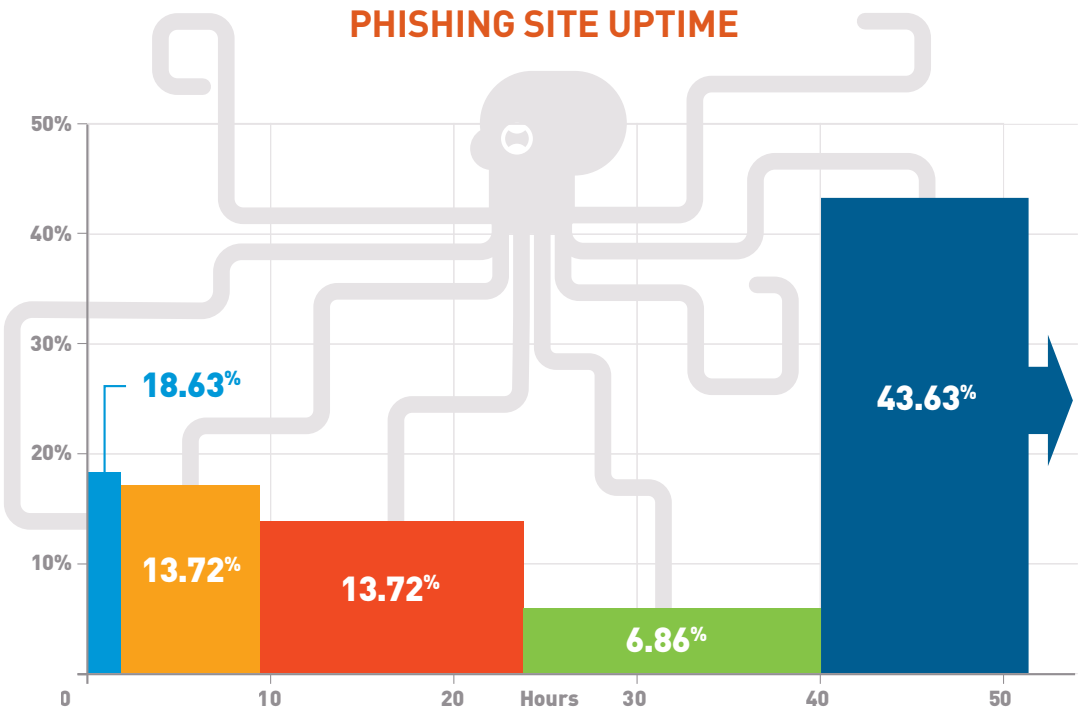
In an effort to better understand the complete phishing picture, Cyren experts examined phishing sites tracked and flagged by Cyren's phishing intelligence data and analyzed how long these phishing sites remained online and active.

Because Cyren systems observe billions of internet transactions on a daily basis, our analysts often have a unique opportunity to do a deep dive into specific data sets, like quarterly phishing numbers. Using data from Cyren's phishing intelligence, we analyzed how quickly website owners and their web hosting services responded to notifications that their sites had been hacked. Unfortunately, most hosting services pay very little attention to site hacking; site owners usually only become aware of a hack upon seeing a browser warning, or strange traffic numbers and destination sites in site analytics.

NOTABLY, THE HIGHLIGHTS OF CYREN'S FINDINGS INCLUDED:

- Nearly 20% of sites are gone within three hours.
- Half are gone within a day.
- Of the remaining 50%, over 40% stuck around for over two days.

While sites are still live, phishers resend email campaigns. Since greater than 50% of the sites examined remained useful for two days or more, clearly phishers are getting good mileage out of a hacked site. This also suggests that late protection still has some value for security providers, as the site may still be active; however, solutions offering full protection need to be prioritized and encouraged in order to block phishing sites during zero hour attacks.

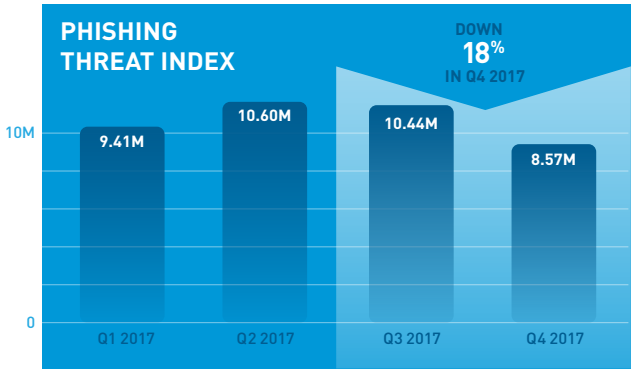


Cyren GlobalView™ Threat Trends—Q4 2017

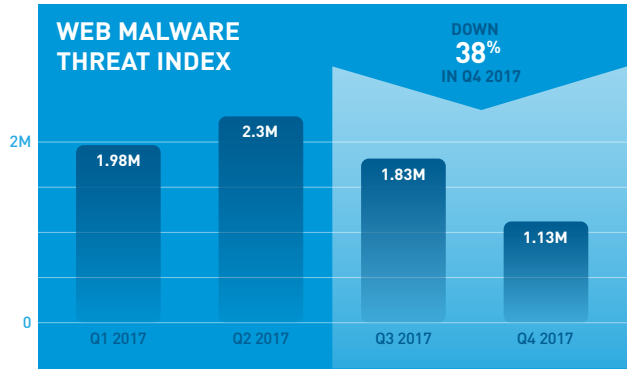
The Cyren GlobalView Threat Trend Indices are published quarterly and are indicators of global tendencies for the principal types of internet threats. The indices are compiled from operational data from the Cyren GlobalView Threat Intelligence Cloud, which processes over 25 billion web and email transactions daily.

Threat activities during the 4th quarter of 2017 continued along a similar path as previous periods, with a few notable exceptions. Spam email experienced some dramatic peaks and valleys, with a daily high of over a billion (1.05B) and a low of 224 million, a 4x range. Similarly email malware attachments in Q4 saw a peak day of 118 million and a low of 45K—an amazingly dramatic 2600x swing, showing the volatility of email malware activity and how large botnet-driven campaigns can reach insane numbers.

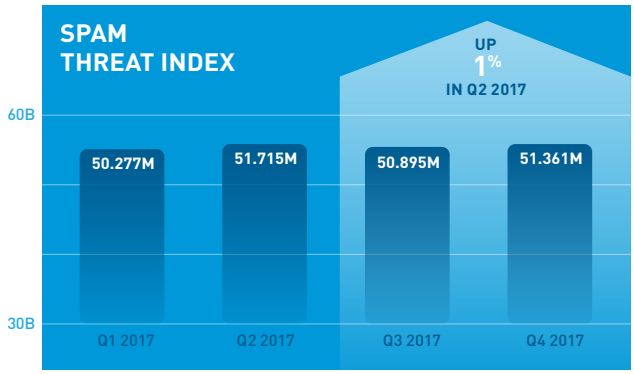
Detailed 2017 fourth quarter numbers are presented below.



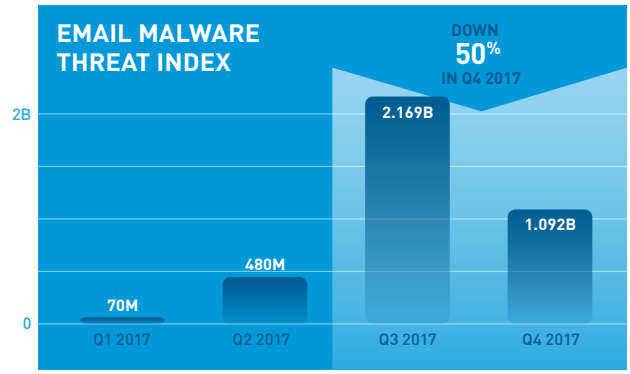
Active Phishing URLS



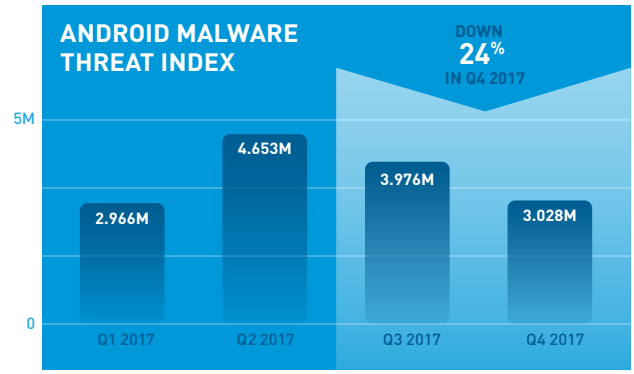
Active Web Malware URLs (millions)



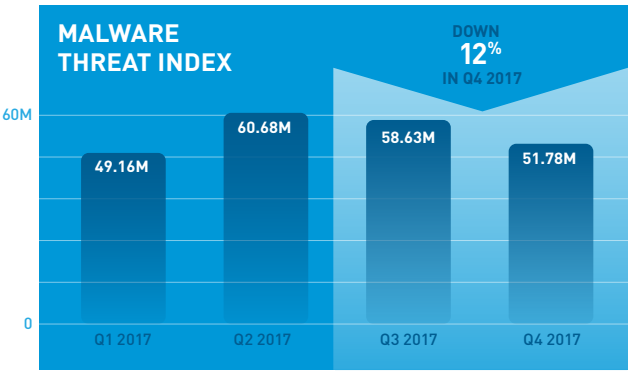
Spam Detected



Email Malware Detected

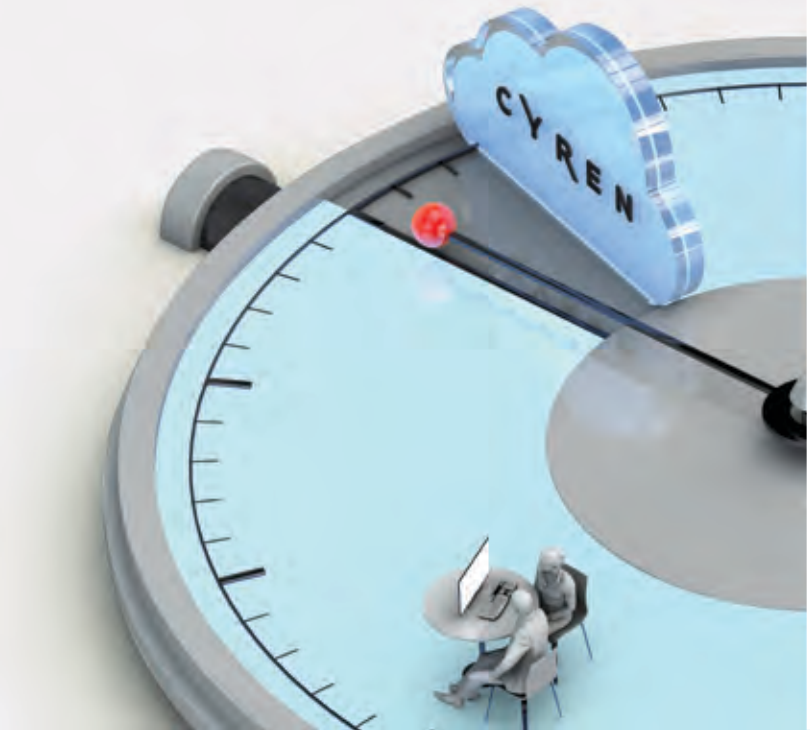


Android Malware Samples



Malware Samples

Cyren–The Fastest Time to Protection



The Appliance Window of Exposure

CYREN

More than 1.3 billion users around the world rely on Cyren's 100% cloud internet security solutions to protect them against cyber attacks and data loss every day. Powered by the world's largest security cloud, Cyren delivers fast time to protection from cyber threats with award-winning security as a service for web, email, sandboxing, and DNS for enterprises, and embedded threat intelligence solutions for security vendors and service providers. Customers like Google, Microsoft and Check Point are just a few of the businesses that depend on Cyren every day to power their security. Learn more at www.Cyren.com.

Headquarters

US Virginia
1430 Spring Hill Road
Suite 330
McLean, Virginia 22102
Tel: 703-760-3320
Fax: 703-760-3321

Sales & Marketing

US Austin
10801-1 North Mopac Expressway
Suite 250
Austin, Texas 78759

UK Bracknell
Maxis 1
43 Western Road
Bracknell
Berkshire
RG12 1RT

US Silicon Valley
1230 Midas Way
Suite 110
Sunnyvale, CA 94085
Tel: 650-864-2000
Fax: 650-864-2002

R&D Labs

Germany
Hardenbergplatz 2
10623 Berlin
Tel: +49 (30) 52 00 56 - 0
Fax: +49 (30) 52 00 56 - 299

Iceland
Dalshraun 3
IS-220, Hafnarfjordur
Tel: +354-540-740

Israel
1 Sapir Rd. 5th Floor, Beit Ampa
P.O. Box 4014
Herzliya, 46140
Tel: +972-9-8636 888
Fax: +972-9-8948 214

Cyren.com

@CyrenInc

linkedin.com/company/cyren