CYREN

2016 CYBER THREAT Report

AUTOMATED THREAT INTELLIGENCE:

The Key to Preventing, Mitigating, and Identifying Cyber Breaches

Table of Contents

INTRODUCTION

Lior Kohavi
Chief Technical Officer, CYREN, Inc.

There is a false perception that sophisticated attacks are too difficult to prevent and the only alternative is detection. But detection is **NOT** the new prevention. Cybersecurity professionals must make it their mission to **STOP** attacks, not just become proficient at detecting them.

It's no secret that cybercriminals are willing to spend a lot of time and money to obtain the information they desire. And, the risk that these criminals will be caught and convicted is relatively low. Despite well-publicized botnet takedowns, like that of Darknode this past July, researchers estimate that less than 1% of cybercrimes receive a corresponding conviction. With such low risk and high returns, the difficult truth is that cybercrime will continue largely unabated, and target organizations—including businesses, consumers, and government agencies—must improve their protection capabilities.

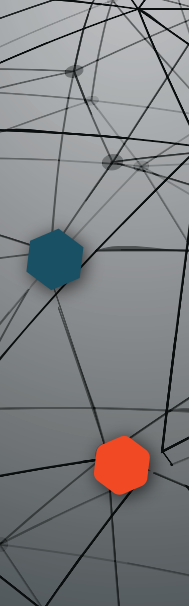
Some in the cybersecurity industry feel that today's sophisticated attacks are too difficult to prevent using traditional human analysis and on-premise appliances. If we follow this chain of reasoning, the only way to defend against cyberthreats is to detect breaches after the fact. Those of us at CYREN respectfully disagree. We believe that the solution to the ongoing "protection versus detection" dilemma lies in the complete automation of the detection framework, incorporating advanced analysis of potential threats to improve prevention. CYREN is disrupting the threat intelligence market with a new approach that combines a worldwide, cloud-based platform with mass-scale automated analysis of global data patterns, to deliver

unique zero-day threat prevention. By adopting this model, cybersecurity professionals can more effectively protect their information, their organization, and most importantly, their customers.

For businesses, mobile technology and high-utility cloud services (such as software as a service) combine to create a fluid network perimeter—one that can no longer be protected by simply throwing more people and resources at the problem. Security professionals must deploy better, smarter, and more nimble solutions. One such example is the use of massive cloud-based sandbox arrays that harness the power of big data, global intelligence, automation, and the elastic scale of cloud computing. Because these types of solutions rely on global cyber intelligence and automate threat analysis on a mass-scale (rather than traditional human analysis or reactive procedures), users are proactively protected against all types of threats, including targeted, zero-day, and advanced persistent threats (APTs).

In this year's annual report, CYREN presents a series of notable threats, breaches, and cybercrime statistics detected by CYREN over the course of the last twelve months. Using the power of automation and big data, CYREN rapidly identified and mitigated each of these threats, halting significant and powerful breaches with the potential to do irreparable damage to major global organizations.

The coming years will be critical as companies work to develop better solutions to protect businesses, governments, and consumers. CYREN is fully committed to leading the way by developing state-of-the-art automated solutions that leverage the 17 billion pieces of data we gather daily, and the cyber intelligence we disseminate through 500,000 global points of presence in 200 countries.



The Cloud Sandbox Array: A New Tool Against Cybercrime

Finding and Blocking Sophisticated Zero-day Attacks

A brand new tool to fight cybercrime helps CYREN stop a significant attack involving fake WhatsApp and Facebook emails.

As cybercriminals become stealthier in their efforts to breach systems, the need for advanced cybersecurity technology is clear. **Enter cloud-based multi-sandbox arrays.**

Background: The Nature of Threats

In today's world, threats to corporate and personal cybersecurity are either repackaged versions of previously seen threats or completely unknown. To identify threats and create corresponding antivirus (AV) solutions, suspected malware is analyzed and then a rule set or signature is created for the AV engine so that the threat is detected the next time it appears. Unfortunately, rule-sets typically only get published every 24 to 48 hours. As a result, a huge volume of threats remains undetected because the detection rule or signature has not yet been created or the customer system hasn't yet been updated.

Sometimes an object (such as a file or web script) passes through AV or URL filtering tests as seemingly 'safe' (with no known suspicious codes), yet cybersecurity professionals may still deem the object as suspicious for other reasons. For example, the email that delivered the object, or the object itself may contain website addresses that are brand new or are related to a recent malicious email outbreak.

Identifying and blocking known malware is an established process; what complicates the process is the scale of Internet traffic and the requirement to distribute timely signatures for newly discovered threats.

On top of these challenges, corporations now also have to worry about the insidious zero-day threat; malicious files and web objects that have never been seen or analyzed. These types of threats are designed to take advantage of previously unexploited vulnerabilities in popular browsers and applications. Ultimately, the challenge for cybersecurity professionals becomes how to identify and block the increasing number of undetected, unpublished, and invisible threats.

In analyzing zero-day attacks, CYREN analysis identifies clues that exist in the everyday threat environment. For example, by examining the details associated with the domain or email blast that delivered the malware, it's possible to identify attributes that are suspicious, such as URLs less than 24-hours old or files discovered via detection of a spam outbreak.

CYREN analysts have also found that traditional external analysis techniques are no longer sufficient to identify zero-day malware. In order to determine if a suspicious file is malicious, it is critical to observe the file's behavior as it executes. This type of observation forms the basis for a 'sandbox'—a virtual computing environment used to detonate a suspicious file, and instrumented to observe and capture the file's behavior. However, because a typical sandbox analysis requires significant computing

resources, large-scale rapid observations are difficult. In addition, realizing that malware could be identified in a sandbox environment, cybercriminals have started programming evasive code into the malware, which enables the virus to self-determine execution within a sandbox, and then take measures to disguise its true nature by putting itself to sleep for several weeks, for example.

The Solution: Cloud-based Multi-Sandbox Arrays

CYREN combats the single sandbox dilemma by utilizing the power of cloud-computing to create a multi-sandbox array. This patent-pending approach enables automated analysis of suspicious files through a series of sandboxes and other proprietary, advanced analysis techniques, making it much more difficult for zero-day malware to evade detection. And, because files are analyzed in the cloud, threats are identified in minutes, without the challenge of waiting for security appliance computing resources to free up.

The multi-array, cloud-based sandbox service delivers mass-scale, automated threat analysis based on different investigation mechanisms or different platform/environment simulations. Using a unique new form of threat analysis language built specifically for the CYREN array, the system initiates an analysis process, continuously calculating a "reputation score" for the item under analysis, with a low score of '0' meaning 'not a threat' and high score of '100' meaning 'confirmed malicious threat.' The automated process then directs potential threats through one or more sandboxes, ensuring optimal detection by finding an environment in which the malware will activate or "detonate." To manage the analysis path through the array that the threat will follow, CYREN's proprietary language normalizes the output from different sandboxes, using the results from each to determine whether the file or object under scrutiny is evading analysis by suppressing or hiding its behavior. If the system determines that the malware is attempting evasion, the path through the array is dynamically adjusted to apply different analysis techniques to ensure that the true behavior of the object is exposed and fully analyzed.

If a threat is confirmed, CYREN instantaneously updates its global cyber intelligence platform, providing proactive state-of-the-art protection for CYREN customers. This approach further ensures that if an organization is already infected with this malware through some other vector, outbound zero-day threat communications are disrupted.

PREDICTION

As malware becomes more sophisticated, it will learn and become 'aware' of specific sandboxes, preventing "detonation" of the malware and subsequent detection. Cloud-based multi-sandbox arrays will prevent this, since the malware can't recognize every possible environment.

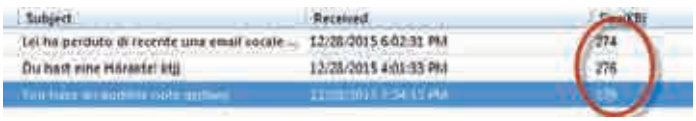
Real World Success: CYREN Cloud-based Multi-Sandbox Array Stop Major Attack

The benefits of this next-generation, advanced threat protection tool operating at cloud scale were proven in December 2015 when CYREN stopped a major attack involving password-stealing and bitcoin-mining malware. The attack arrived in mailboxes as emails purporting to be from WhatsApp or Facebook with an attachment labeled as an audible message. When opened, the file launched a malware variant alternately known as Bayrob, Nivdort, or Symmi, functioning as either a password-stealing Trojan or bitcoin-mining variant.

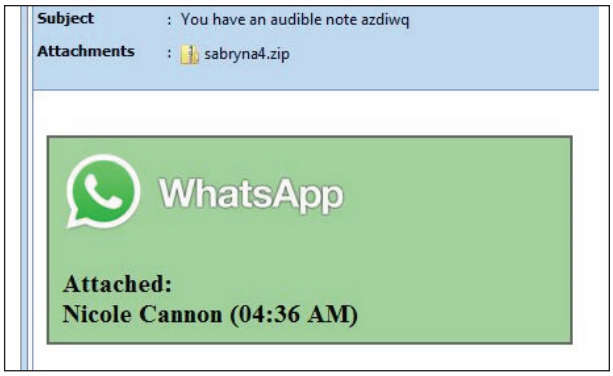
Bitcoin-mining can be highly profitable, but also extremely difficult given the high processing power requirements. Since a single computer is unable to process enough bitcoin mining data to make it worthwhile, cybercriminals are turning to the computing power of bots, distributing bitcoin-mining malware to leverage the collective processing power of thousands of machines.

In distributing the malware via the fake WhatsApp and Facebook emails, criminals attempt to obfuscate the malicious files by randomizing the filename. However, the structure and size of each email remains the same.

If opened on a Windows OS machine, the file creates a hidden folder, dropping two hidden executable files into it. It also creates a service that runs in the background, which contacts the command and control (C&C) server. The C&C then provides further malware for download, resulting in either password stealing or bitcoin mining. Stolen credentials or bitcoin mining instructions are provided from/to the same or alternate C&C servers.



While the structure of each malicious file is the same, the names of the files are different.

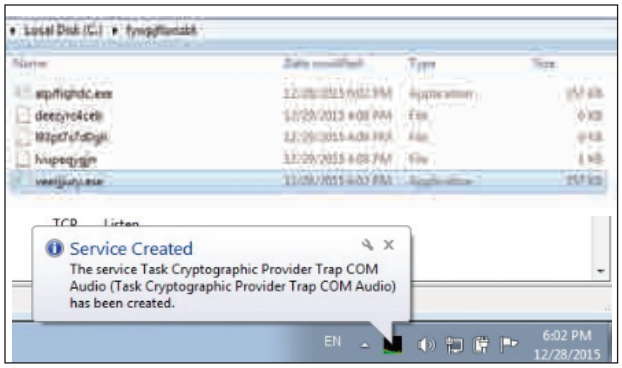


Malware arrives looking like Facebook or WhatsApp emails.

Nivdort hinders analysis in several ways, indicating its complexity. Typically, analysts (and even some automated analysis systems use computer memory dumps to obtain the malware's decrypted file string information, which can provide information such as the malware family name. In the case of Nivdort, however, the malware uses a memory dumping technique that ensures the strings are cleared from the computer's memory after execution, thus making the strings difficult to find and analyze.

In addition, the C&C address is not easily retrieved from the malware code. Instead the Nivdort malware family has its own complex domain generation algorithm (DGA) that generates domain names based on a plausible combination of words and phrases, such as finishdinner.net, winterforest.net, and possiblequestion.net.

:



Hidden folders are created, filled with executable files, and operations begin.

1) The domains that will be used to connect to the C&C are unknown to standard AV and URL filtering tools.

2) The address is unknown even to the malware; it simply tries every single domain provided by DGA until one of them responds (99% go nowhere). Even once they have been identified (using a standard sandbox system, for example), the number of domains is too vast to proactively take down or block.

3) In the case of the plausible domain names created by Nivdort, it is not possible to simply block what appear to be gibberish domain names, since some may be legitimate. Although the domain names are generated randomly, the partial phrase in the names makes the domains appear legitimate. As a result of this, standard security algorithms used to check the domain names for randomness will not categorize them as suspicious.

In analyzing a random sample of over 100 domains generated by Nivdort, CYREN researchers only found one that was actually registered.

Domains generated by the DGA include word combinations such as:

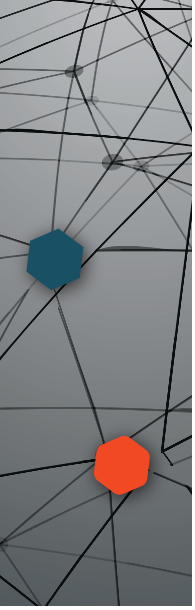
- simplequestion.net
- mountainmeasure.net
- winteranger.net
- subjectafraid.net
- possibleschool.net
- winterwheat.net

By directing intercepted malware to the cloud-based multi-sandbox array for analysis, CYREN was the first to identify it, with identification happening within minutes of initial analysis. The benefits and value of the multi-sandbox array were immediately evident when the system shifted the malware to a second sandbox, where it detonated, after the malware itself identified the first sandbox and did not exhibit any malicious behavior.

CYREN believes that the key to effective protection is to use highly automated, orchestrated frameworks that apply multiple analysis capabilities in an adaptive way. With this approach, CYREN can continuously add new analysis capabilities to the framework—ensuring that new evasion techniques developed by cybercriminals are met with equal and opposing force by CYREN, maintaining the balance of protection in favor of the end user.

PREDICTION

More and more threats will arrive via unexpected or legitimate-looking channels, but ultimately will still link back to classic threat vectors.



The Benefits of Big Data: Changing the Face of Cybersecurity

Using large data sources, cybersecurity professionals can not only stop obvious malware, but also find hints of lesser-known threats hidden in malicious sources.

CYREN sees 17 billion Internet transactions daily. In analyzing this data, we quickly find the low hanging rotten fruit—the obvious malware targeting companies and individuals. We also find less apparent and more sophisticated malware and outbreaks using AV heuristics and our patented Recurrent Pattern Detection. But realizing that dangerous content in the form of files, URLs, and IP addresses is still slipping through the cracks, CYREN is using its vast amount of security data to identify malicious domains and addresses in an entirely new way.

Often seemingly innocuous information for a URL or IP address—such as having been registered the day before—could indicate malicious intent. In examining daily Internet data, CYREN uses its reputation scoring analysis process to identify potentially malicious IP and URL addresses.

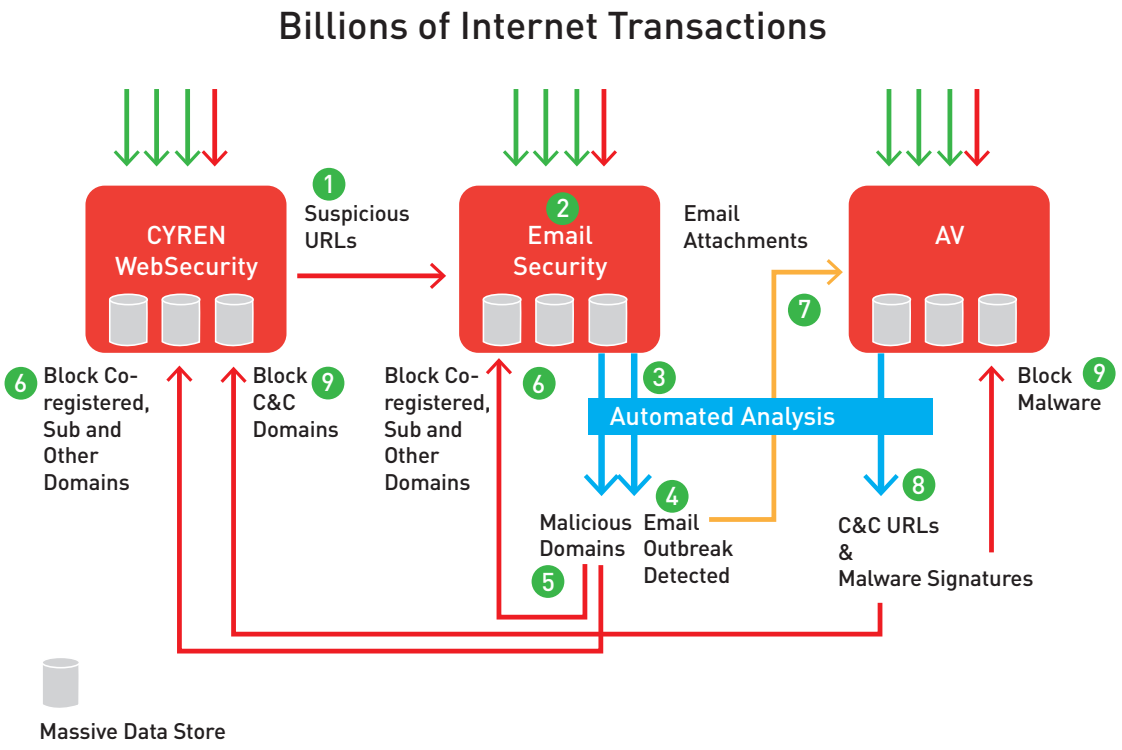
Using this approach, CYREN recently highlighted several suspicious URLs and IP addresses that were being accessed by employees at a company that uses CYREN WebSecurity, including legitimate sounding website names, such as invoice-myups.org.

Recognizing that the employees and the company were exposing themselves to potential malicious content, CYREN analysts began an immediate investigation by listing the domain names for automatic observation by CYREN threat analysis systems.

The domains were soon detected in an email-attached malware outbreak. The domain analysis had revealed that this domain and other domains used in similar attacks shared the same the registrant. CYREN immediately blocked emails and content originating from this domain, other domains with the same registrant, subdomains associated with the domain, and any other domain names used in the attack.

Analysis indicated that attack distribution occurred through emails containing malicious "Zeus-variant" macros embedded in attached Word documents. To halt malware download and distribution of other unidentified attachments, the CYREN system created new signatures to block these samples and variants. CYREN also identified and blocked the C&C servers.

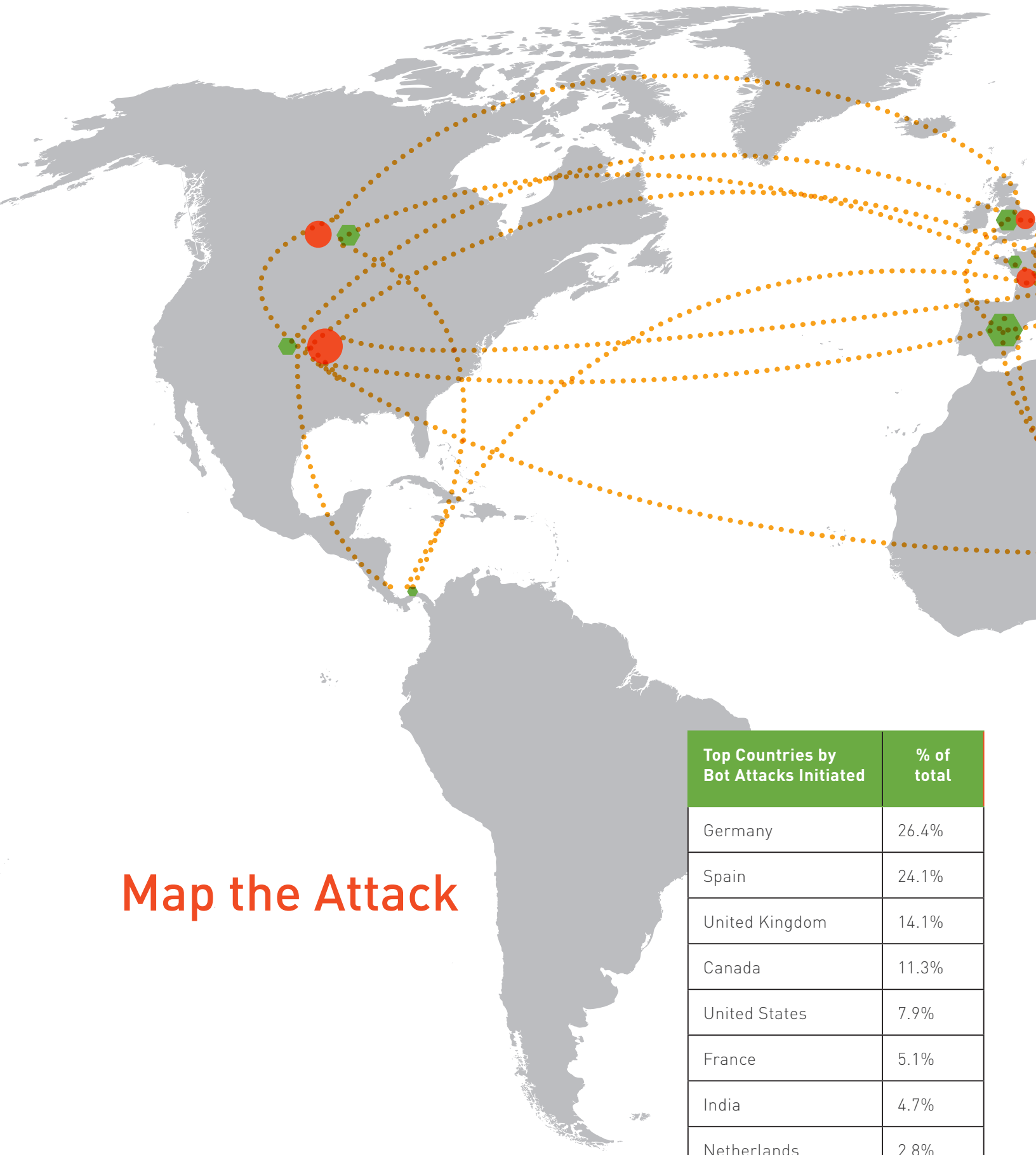
By using its vast data to identify suspicious URLs, CYREN has the ability to block malware emails, the malware itself, and C&C servers, providing protection to both email and Web users. In addition, CYREN identifies C&C domains as an indication that an APT has already breached security defenses and is now attempting to "phone home." This information can also be used by the affected organization to initiate a cleanup of infected devices.



Cybercriminals avoid detection by creating complex cross-referenced URLs, IP addresses, attachments, and files, which can all change in real time.

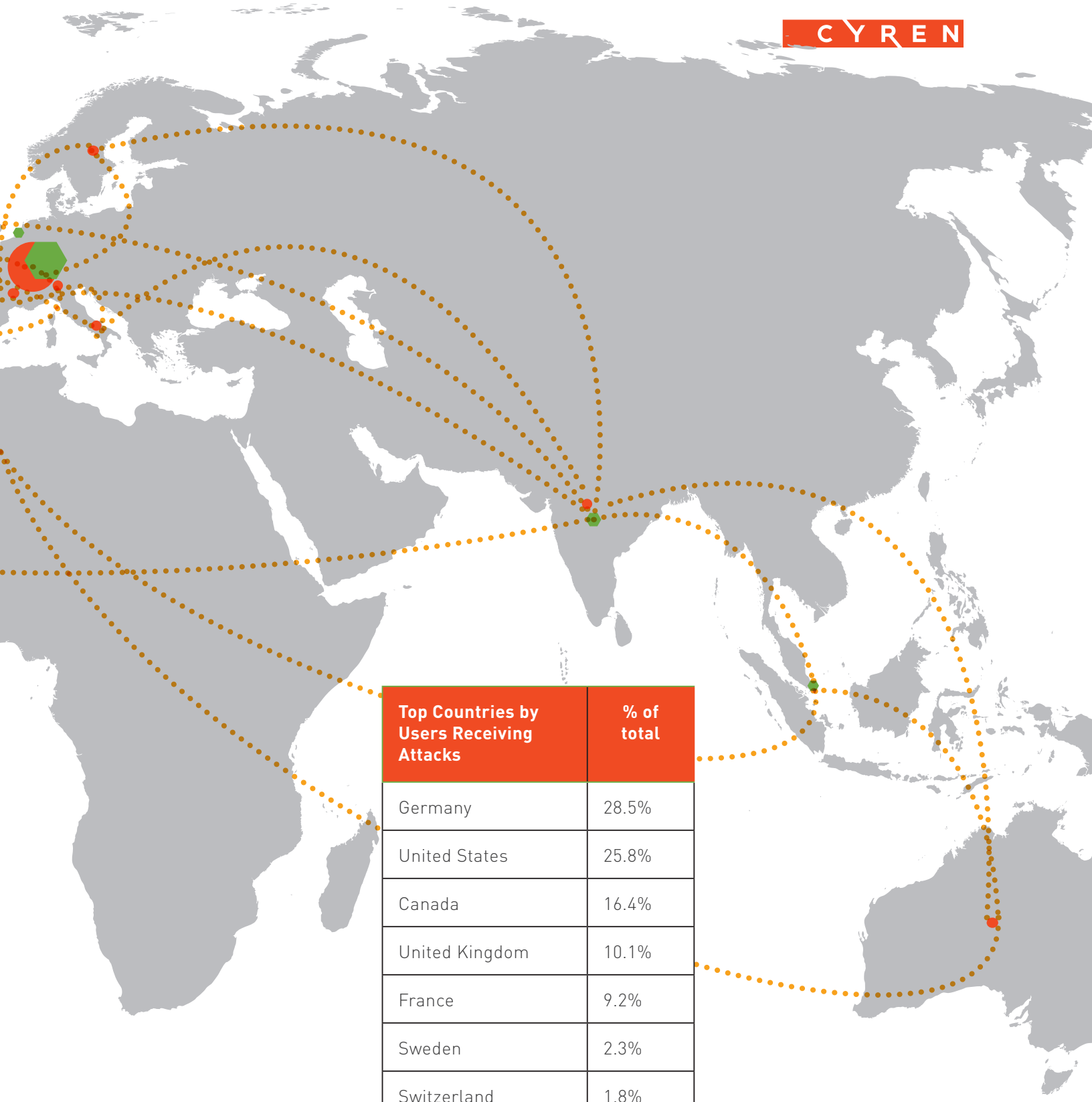
PREDICTION

Cybercriminals will target corporations using sophisticated social engineering involving personalized phone calls and knowledgeable (but fake) emails to convince employees to open malicious files, giving the attacker a foothold within the organization. Large data analysis will begin to help flag potentially dangerous URLs and IP addresses before employees fall victim to scams.

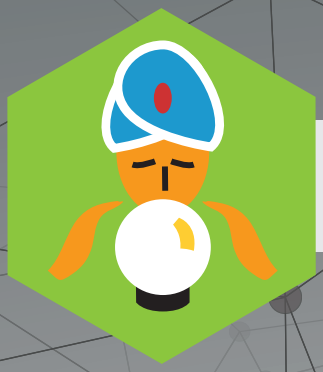


Map the Attack

Top Countries by Bot Attacks Initiated	% of total
Germany	26.4%
Spain	24.1%
United Kingdom	14.1%
Canada	11.3%
United States	7.9%
France	5.1%
India	4.7%
Netherlands	2.8%
Singapore	2.2%
Panama	1.5%



Top Countries by Users Receiving Attacks	% of total
Germany	28.5%
United States	25.8%
Canada	16.4%
United Kingdom	10.1%
France	9.2%
Sweden	2.3%
Switzerland	1.8%
Australia	1.7%
Italy	1.5%
Austria	1.5%
India	1.2%



2016 PREDICTIONS

As malware becomes more sophisticated, it will learn and become 'aware' of specific sandboxes, preventing "detonation" of the malware and subsequent detection. Cloud-based multi-sandbox arrays will prevent this, since the malware can't recognize every possible environment.

Cybercriminals will target corporations using sophisticated social engineering involving personalized phone calls and knowledgeable (but fake) emails to convince employees to open malicious files, giving the attacker a foothold within the organization. Large data analysis will begin to help flag potentially dangerous URLs and IP addresses before employees fall victim to scams.


More and more threats will arrive via unexpected or legitimate-looking channels, but ultimately will still link back to classic threat vectors.
Increasingly cybercriminals will continue to use sophisticated, yet subtle, incremental changes in their approach to cybercrime.
Ransomware threats will increasingly target mid-tier enterprises. The potential returns from locking a device holding corporate data are much greater than with a consumer device.

Malware Newsmakers of 2015

New and old malware are showing increasing sophistication.

With as many as one million new malware threats being released each day, it comes as no surprise that many of these viruses are advanced and targeted. CYREN examined the various malware threats that appeared during 2015 and discovered some interesting trends, some new creations, and a few fashion makeovers.

Gunpowder

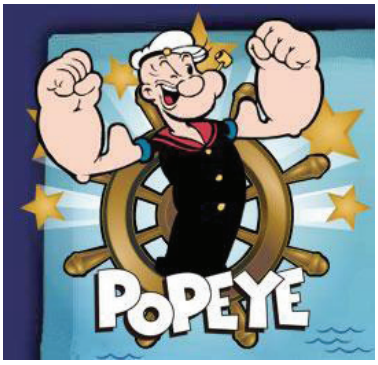
Appearing in June 2015, Gunpowder (also seen as Gunpoder) is Android malware distributed via SMS messages through the phone's contact list, under the message "a fun game ^_^." Defined as an "information stealer," its primary purpose is to steal sensitive data from the victim's phone. Researchers have found this malware in 13 countries and estimate that 49 unique samples of the virus exist. Notably, the malware is programmed to search the Android device to determine if the victim is located in China. If so, the malware does not activate.

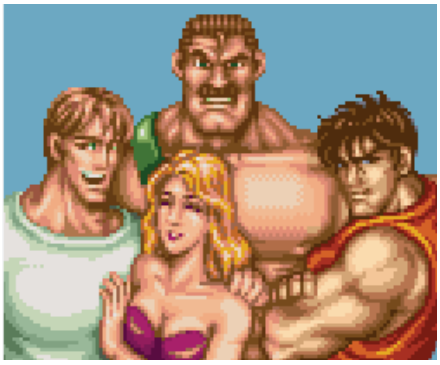
The malware arrives hidden in old Nintendo games for Android along with aggressive adware, involving multiple advertising libraries, to obfuscate it and confuse antivirus detection. Unfortunately because of the advertising components, this malware is still often mistakenly identified as adware.

Upon opening the game for the first time, the user is asked to agree to terms that include accepting 'pushed' advertising and collecting information from the device.

The malware author uses an open software Nintendo emulator for Android called Nesoid (Nintendo NES emulator for Android phones) to run the games, and to program additional features, including inserting an offer in which the victim is asked for a payment to use the cheat feature in the game.

Upon installation, the malware obtains information about the user's device, International





After pressing Ok or Cancel, the victim is able to access and play the game.

Mobile Equipment Identity (IMEI), International Mobile Subscriber Identity (IMSI), browser history, and browser bookmarks, among other things.

Unfortunately, because the malware does include actual games and the malicious code is obfuscated by advertising libraries, many victims and antivirus detection organizations have no idea that malware is actually collecting sensitive data.

Hidden Secrets: Stegaloader/Gatak—Steganography Malware

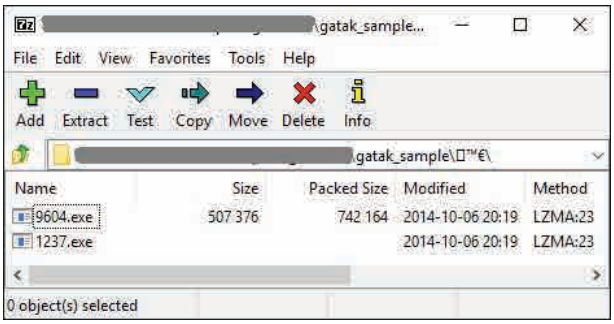
Steganography is the age-old practice of concealing a file, message, image, or video within another file, message, image, or video. In the world of digital cybercrime, steganography often means including steganographic coding inside the actual transport layer, such as a document or image file.

The Stegaloader/Gatak malware (detected by CYREN as W32/Gatak in 2015), leverages steganography techniques used in the Duqu and Zeus/Zbot malware from a few years earlier. Designed as an information stealer, in the case of Stegaloader/Gatak, it completely hides malicious code within a .png image file.

The Stegaloader/Gatak downloaded image file.

```
public final void a() {
    long v6 = 3;
    long v4 = 1;
    this.a(new i(), "sdk", f.a(10).c());
    this.a(new h("profile"), "profile", f.a());
    this.a(new io.presage.services.c.e(), "config", f.a(0).d());
    this.a(new c("apps"), "apps", f.a(2).c());
    if(Build.VERSION.SDK_INT >= 5) {
        if(io.presage.utils.f.a().a("com.android.browser")) {
            this.a(new io.presage.services.c.f(Uri.parse("content://com.android.browser/history"),
                    "history"), "history-browser", f.a(v4).c());
        }

        if(io.presage.utils.f.a().a("com.android.chrome")) {
            this.a(new io.presage.services.c.f(Uri.parse("content://com.android.chrome.browser/history"),
                    "history"), "history-chrome", f.a(v4).c());
        }

        if(io.presage.utils.f.a().a("com.sec.android.app.sbrowser")) {
            this.a(new io.presage.services.c.f(Uri.parse("content://com.sec.android.app.sbrowser.browser/history"),
                    "history"), "history-samsung", f.a(v4).c());
        }

        this.a(new d(Browser.BOOKMARKS_URI, "bookmarks"), "bookmarks-browser", f.a(v6).d());
        if(io.presage.utils.f.a().a("com.sec.android.app.sbrowser")) {
            this.a(new d(Uri.parse("content://com.sec.android.app.sbrowser.browser/history"), "bookmarks"),
                    "bookmarks-samsung", f.a(v6).d());
        }

        this.a(new j(Uri.parse("content://com.android.browser/searches"), "search"), "search", f
                .a(v6).d());
    }
```

As seen here, the malware collects the victim's browser history.



The malware typically arrives as a bundled file in software cracking tools.

Upon file execution, the cracking tool displays the following window used to generate software keys for a specific software program. It also runs the Gatak malware (9604.exe) alongside the cracktool without the user knowledge.

After running an additional series of complex operations, the malware retrieves the image and then the hidden encrypted data via a steganography technique, using a combination of these APIs to get the pixel data of the image: GdipGetImageHeight, GdipGetImageWidth, and GdipBitmapGetPixel.

This malware downloader may also install other modules or malware for stealing sensitive information. CYREN found that some of malware variants install the Vundo malware creating adware, ransomware, and scareware on the victim's system.

CYREN researchers believe that cybersecurity professionals will increasingly see more of this type of malware, since it's extremely difficult to decrypt the hidden code in the image file, and therefore difficult to analyze and protect against the malware.

Alina

After the 2014 "Backoff" point-of-sale (POS) malware debacle that infected at least 1,000 major retailers, including Home Depot, Target, and UPS, businesses were hoping that new forms of point-of-sale malware would disappear, at least for a while. Unfortunately, this was not to be the case, as 2015 introduced us to new and more creative forms of POS malware, including variations of "Alina," originally discovered in 2012. (Security professionals believe that the source code for Alina was sold on the black market, spurring the creation of other POS malware, including Sparks, JackPos, and the infamous Backoff.)

Like most POS malware, Alina targets credit card swipe systems by infecting them with a virus that gathers all the credit card data and sends it to a server, where the data is compiled. The data is then sold on the black market by cybercriminals, resulting in card fraud and identity theft. The current version of "Alina" is much like the original, but now also includes new features such as screen capture and keylogging.

Alina uses a memory scraping technique to gather and steal the credit card data. Although most POS systems running Windows OS encrypt credit card data once it processes a payment, the data is briefly available unencrypted in the system's memory, enabling malware, like Alina, to capture it by generating search algorithms using regular expressions based on well-documented payment card format standards.

In April, several new variants of Alina surfaced in the US, Canada, and South America, including FighterPoS. Reports suggest that in the span of just one month, tens of thousands of pieces of credit card data were stolen. The value to the cybercriminal of this new version of Alina should not be underestimated, as security researchers have seen the software being sold underground for as much as $5,000 USD.

In June 2015, security professionals discovered another version of Alina, called MalumPoS. Although it uses the same memory scraping techniques, this malware specifically targets POS software developed by MICROS (owned by Oracle), widely used by hotels, restaurants, and retailers in the US.

While typically POS machines are infected through direct intrusion, such as manual installation via a USB drive or brute-force hacking, in the second half of 2015, CYREN observed other versions of Alina distributed via spam emails with Word and Excel document file attachments.

PREDICTION

Ransomware threats will increasingly target mid-tier enterprises. The potential returns from locking a device holding corporate data are much greater than with a consumer device.

2015 Malware Comparison

CYREN observed many new and sophisticated trends in malware during the past year. Notably, new variants of several older malware types (observed in previous years) made a significant comeback in 2015.

Highlights: 2015 Malware Trends

During 2015, CYREN researchers observed the following malware trends:

- **Regular use of macro malware (Word and Excel) for distribution**

  Seldom used before 2015, but now seen frequently.

- **Email malware still a popular infection vector**

  Volume averages several billion emails per day, with a peak of 15 billion one day in November.

- **Focus on financial-specific, such as point of sale (POS) systems**

  Cybercriminals found that deploying point-of-sale (POS) malware for information stealing delivered strong returns.

- **A regional diversity of C&C destinations**

  Because criminals are global it is particularly easy to leverage or hijack infrastructure in any country.

	Malware Name	Infection Vector	Target	Purpose	C&C Connect?	C&C country	Notes
	Nivdort	Email attachment	Business, consumer	Information Stealer, Bitcoin Miner	Yes	Various	First observed in late 2012
	Evilgrab	Watering Hole Attacks	Specific regions and companies (initially Asia-Pacific)	Information Stealer, grabs audio/video/ screens	Yes	Netherlands	Also known as Farfli, first seen in 2012
	PlugX	Malicious Word and Excel	Business, consumer	Information Stealer, Backdoor	Yes	USA	Also known as Gulpix
	Potao	Email Attachment, Malicious Links	Business, consumer	Information Stealer, Downloader	Yes	Russia	Active since 2011
	Stegoloader	Bundled in Software Keygen Tools	Business, consumer	Downloader for information stealing and ransomware	Yes	France	Downloads instructions coded into image files (uses stegonogrpahy)
	Gunpowder	Hidden in Apps/Games, SMS to Contact List	Android	Information Stealer, Worm	Yes	Various	Also known as Gunpoder
	Pony Loader	Link to Malicious Dropbox , Malicious Word and Excel	Business, consumer	Downloader for banking Trojans, information stealing and ransomware	Yes	Various	Source code was leaked on the internet in 2012 and in 2014
	Punkey	USB drive, file download	POS	Gather credit card data, downloader, Keylogger	Yes	Cyprus, Russia, Finland	Collected data is encrypted using AES and then sent to the C&C server
	PoSeidon	USB drive, hacking	POS	Gather credit card data	Yes	Russia	Unlike other Alina variants, PoSeidon is actively developed and is frequently updated
	Alina	USB drive; Brute-force hacking, Malicious Word and Excel	POS	Gather credit card data	Yes	Brazil, Russia	Sparks, JackPos, PoSeidon, Backoff are newer variants of Alina
	Dridex	Malicious Word and Excel	Business, consumer	banking trojans	Yes	Thailand	Is possibly related to Zeus based on its code-base
	Hancitor	Malicious Word and Excel	Business, consumer	downloader for Banking Trojans and Ransomware	Yes	Russia, Europe	Uses the Tor network to send data.

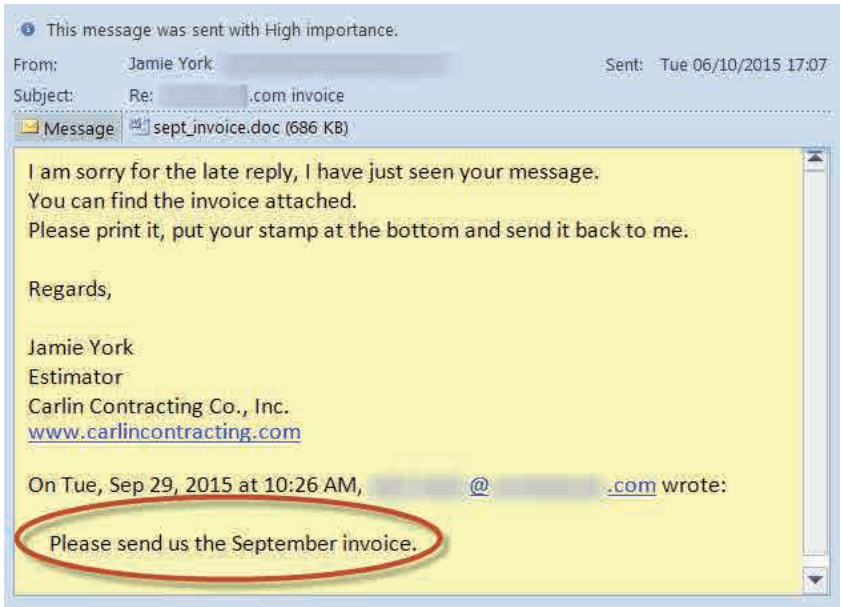
The Criminal Power of the Unknown: Incremental Changes Increase Malware Penetration Rates

CYREN automated intelligence systems are built to identify not only the big changes that threaten digital information, but also the subtle ones.

We know that cybercriminals are educated, competent, and money-driven. Therefore, it should come as no surprise that these folks are putting their innovative talents to work to create subtle, yet powerful changes to malware and spam distribution methods to improve the overall success of threats and breach attempts.

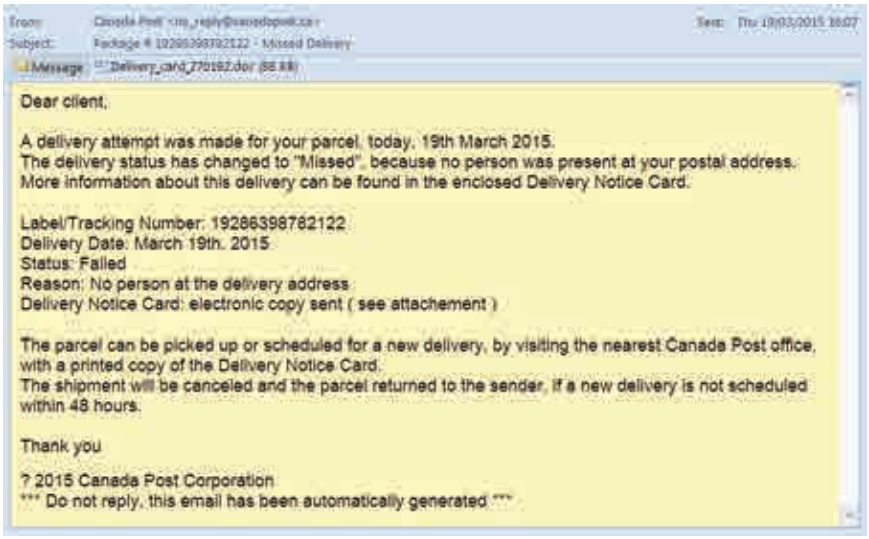
The email below is a good example of the changes cybercriminals make to entice recipients to open malicious files.

The email includes a .doc malware attachment. Nothing strange here. However, this email possesses several key features that make it seem legitimate: (1) Carlin Contracting is a real company, and carlincontracting.com is a legitimate web address; (2) the sender is an actual vice president at Carlin Contracting; and (3) the email itself appears to be a reply from Mr. York submitting an invoice requested by the recipient. The key and subtle trick used in this form of social engineering is the recipient sees their own address in the lower part of the mail, which leads them to believe that they may have actually sent the original email and simply do not remember doing so.



Everything Old is New Again: Macro Malware

In late 2014, CYREN observed the resurgence of macro malware. The trend continued in 2015 with new adaptive tricks, such as pairing macro malware with fake emails from delivery services, in this case Canadian Post



Dear client,

A delivery attempt was made for your parcel, today, 19th March 2015.
The delivery status has changed to "Missed", because no person was present at your postal address.
More information about this delivery can be found in the enclosed Delivery Notice Card.

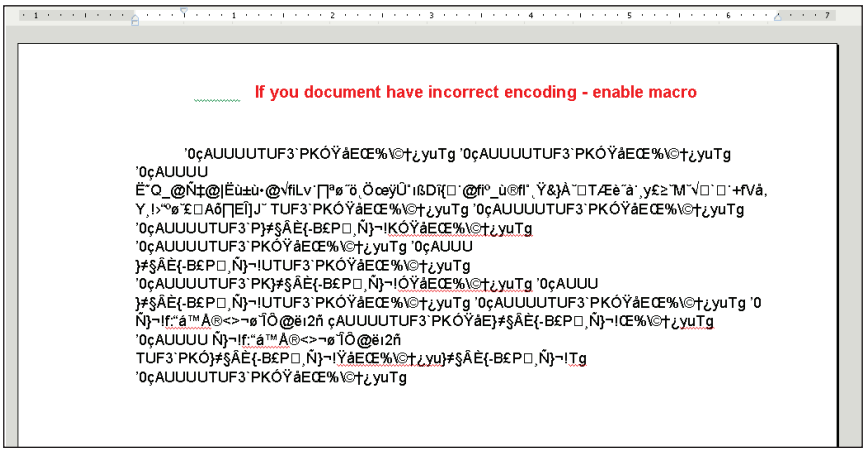
Label/Tracking Number: 19286398782122
Delivery Date: March 19th, 2015
Status: Failed
Reason: No person at the delivery address
Delivery Notice Card: electronic copy sent (see attachement)

The parcel can be picked up or scheduled for a new delivery, by visiting the nearest Canada Post office, with a printed copy of the Delivery Notice Card.
The shipment will be canceled and the parcel returned to the sender, if a new delivery is not scheduled within 48 hours.

Thank you

? 2015 Canada Post Corporation
*** Do not reply, this email has been automatically generated. ***

Upon opening the malware, recipients see this:



If you document have incorrect encoding - enable macro

'0çAUUUUTUF3`PKÓŸåEŒ%\©†¿yuTg '0çAUUUUTUF3`PKÓŸåEŒ%\©†¿yuTg
'0çAUUUU
Ë¨Q_@Ñ‡@|Ëü±ù·@√fiLv`∏ª ø¯ö,Öœ ÿÜ`ıßDï{□`@fi°_ú®fl`¸Ÿ&}À¯□TÆê¨à`¸y£≥™M¨√□`□`·+fVå,
Y,!›°ø˝£□Aô∏EÎ]J" TUF3`PKÓŸåEŒ%\©†¿yuTg '0çAUUUUTUF3`PKÓŸåEŒ%\©†¿yuTg
'0çAUUUUTUF3`P}≠§ÂÈ{-B£P□,Ñ}¬!KÓŸåEŒ%\©†¿yuTg
'0çAUUUUTUF3`PKÓŸåEŒ%\©†¿yuTg '0çAUUU
}≠§ÂÈ{-B£P□,Ñ}¬!UTUF3`PKÓŸåEŒ%\©†¿yuTg
'0çAUUUUTUF3`PK}≠§ÂÈ{-B£P□,Ñ}¬!ÓŸåEŒ%\©†¿yuTg '0çAUUU
}≠§ÂÈ{-B£P□,Ñ}¬!UTUF3`PKÓŸåEŒ%\©†¿yuTg '0çAUUUUTUF3`PKÓŸåEŒ%\©†¿yuTg '0
Ñ}¬!f:"á™Å®<>¬ø¯ÎÔ@ëı2ñ çAUUUUTUF3`PKÓŸåE}≠§ÂÈ{-B£P□,Ñ}¬!Œ%\©†¿yuTg
'0çAUUUU Ñ}¬!f:"á™Å®<>¬ø¯ÎÔ@ëı2ñ
TUF3`PKÓ}≠§ÂÈ{-B£P□,Ñ}¬!ŸåEŒ%\©†¿yu}≠§ÂÈ{-B£P□,Ñ}¬!Tg
'0çAUUUUTUF3`PKÓŸåEŒ%\©†¿yuTg

The above example uses the classic macro malware trick of trying to persuade the user into clicking the "enable" button. Users thinks that by doing so, they will decode the text; in fact, they are activating the malware. Other "enable" tricks rely on user unfamiliarity with blocked macros and the conditioned response to click "enable" when they see a message asking them to do so.

Faked Email Headers Confuse Traditional Spam Filters

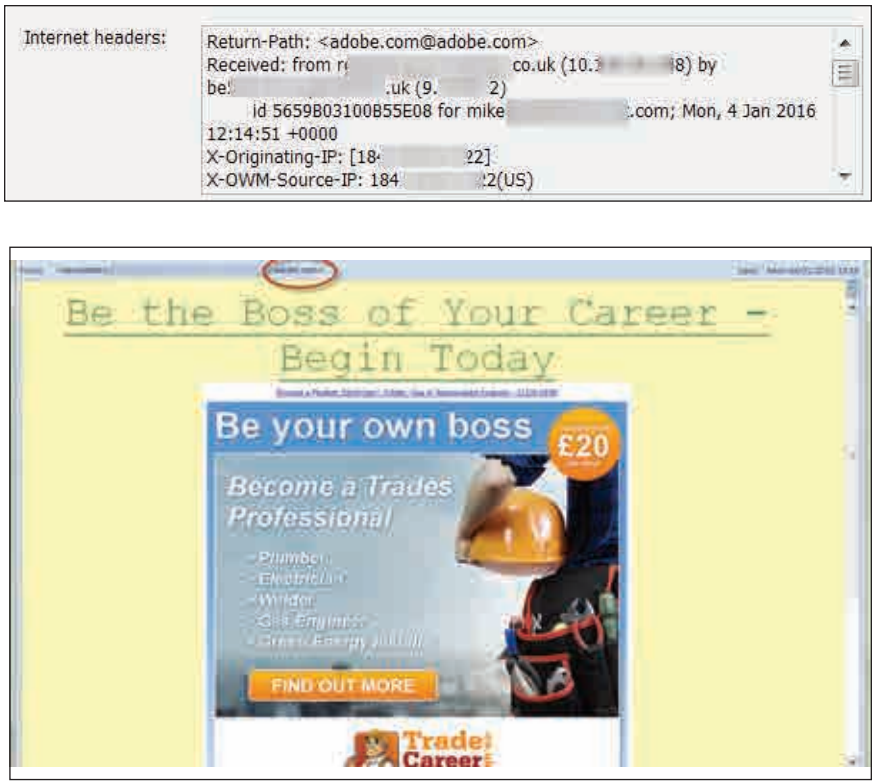
In this attack scenario, cybercriminals harvest legitimate email headers from compromised email accounts. (The headers can be viewed if you go to the detailed properties of any email, but most users do not take the added step of reviewing 'properties'.) These real headers are then added to spam emails that actually sell work-at-home scams or life insurance. Because the addresses and headers

TWO IS BETTER THAN ONE: DUAL EMAIL ATTACHMENT SCAMS

What better way to convince unsuspecting recipients that an email is legitimate than to actually send legitimate files! Cybercriminals are now turning to dual email attachment scams, in which one file is actually a working non-malicious .pdf decoy, and the other is a malicious .zip or .jar file.

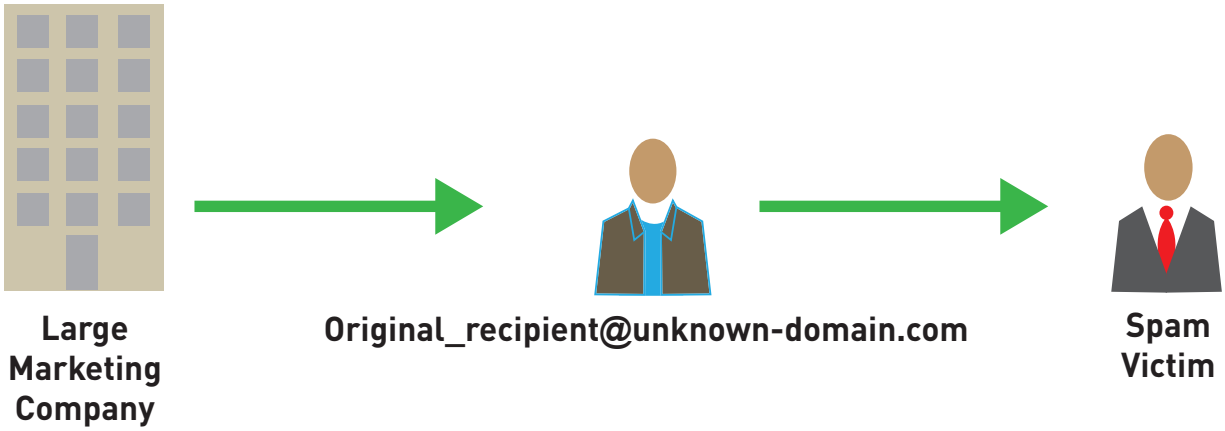
used are from well-known companies including GAP, Old Navy, Adobe, and WhatsApp, some spam filters allow the fraudulent emails to slip through.

Because most antispam and security companies only scan the header component to try and trace the email trail, this criminal harvesting method creates the appearance of a legitimately redirected newsletter.



A legitimate email header from an Adobe Systems email is used in a spam attack.

Thus the poorly managed spam filters recognize the email flow as:



CYREN detected and blocked in near-real time all of these threats and their variants. It should be noted that they are illustrative of the ability of cyber criminals to continuously vary their tactics to bypass filtering technologies and fool unsuspecting users.

PREDICTION

Increasingly cybercriminals will continue to use sophisticated, yet subtle, incremental changes in their approach to cybercrime.

2015 Statistics: Android, Phishing, Malware, Spam

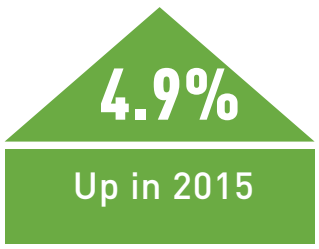
Malware Increases, but Phishing Explodes

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 and applies this cyber intelligence directly to its automated intelligence network and cybersecurity solutions. The following data is drawn from the CYREN GlobalView™ threat intelligence network covering traffic in over 200 countries and from over 600 million web and email users.

ANDROID

3.25 million

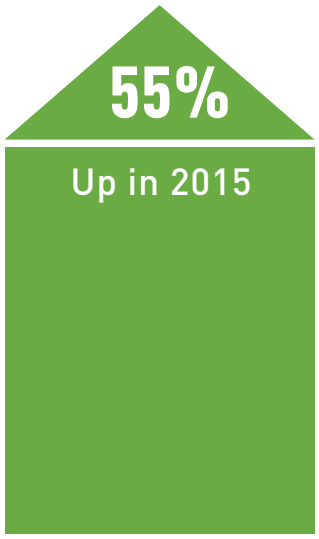
Sum of New Malware for 2015



PHISHING

3.96 million

Total Active Phishing URLS Tracked by CYREN in 2015



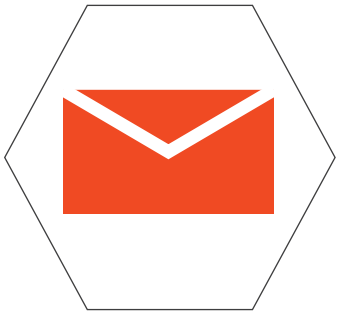
MALWARE

1.09 million
Total Active Malware URLs Tracked by CYREN in 2015

3%
Up in 2015

95.54 million
Sum of New Malware for 2015

14%
Up in 2015

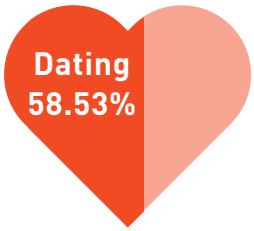


SPAM

51.75 billion
Average Daily Spam for 2015 Messages/Day

Down in 2015
5.52%

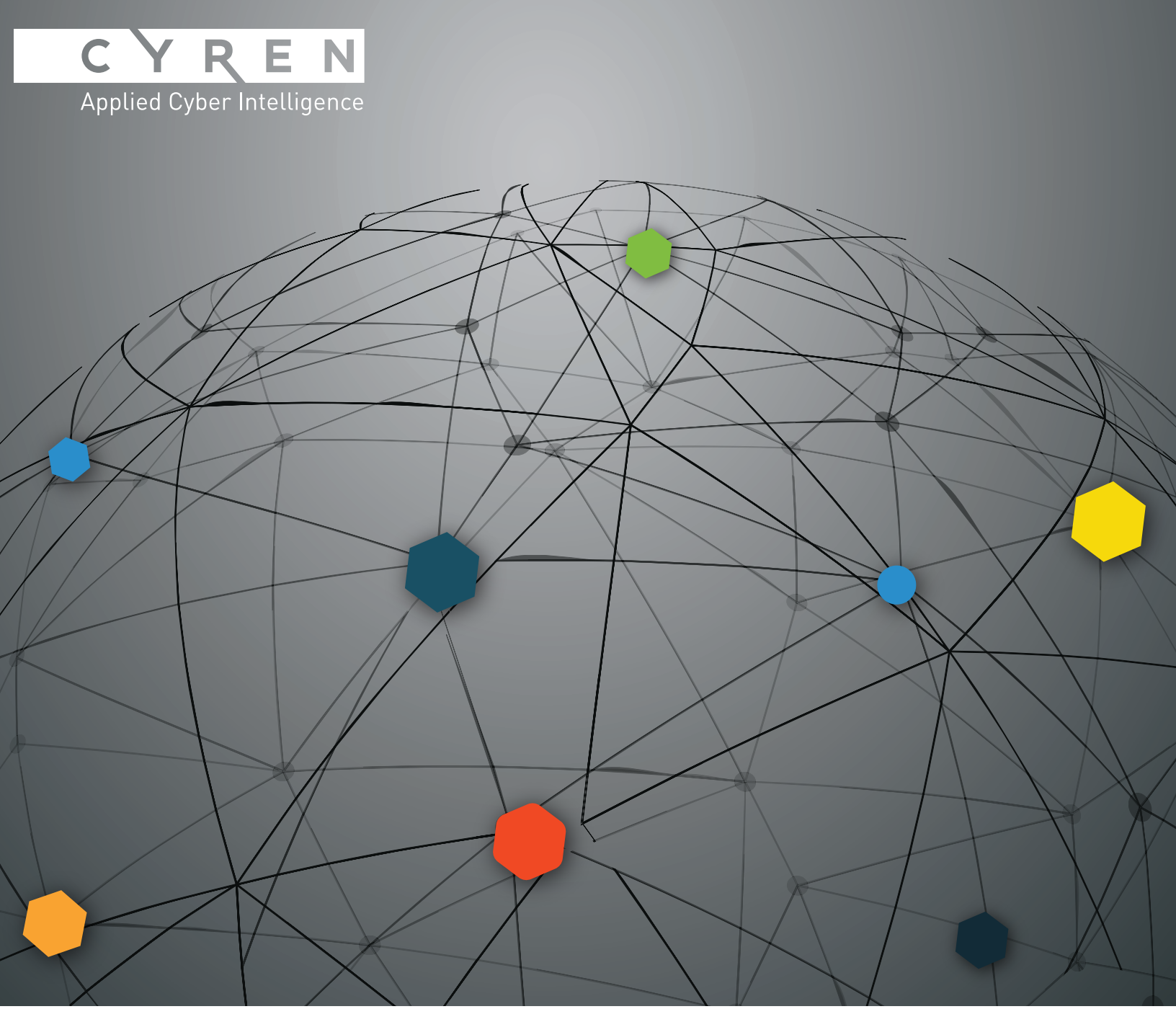
2015 Spam Topics



Job Offer	10.17%
Pharmacy Products	15.35%
Replica	5.56%
Other	3.28%
Casino	2.60%
Stock	2.54%
Scam/419	1.73%
Software	0.16%
Diet	0.08%
Degree	0.02%

CYREN

Applied Cyber Intelligence



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:+972-9-8948214

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