APRIL 2015

CYREN

CYBERTHREAT Report

THE GROWING RISK TO BUSINESS DATA

from malware and breaches

THE ENTERPRISE UNDER ATTACK

Lior Kohavi
Chief Technical Officer, CYREN, Inc.

The regular cadence of high-profile security breaches that we saw during 2014 continued into 2015, with health insurance giant Anthem providing the latest entry in a growing list of major corporate victims. We will not review the Anthem breach in this report as it has already been covered extensively in many other places, but CYREN does believe that this attack is important because it represents a shift in targeting by cyber criminals.

While we do not expect breaches involving credit card details to disappear, general identity theft offers a lucrative growth opportunity for the criminals. Throughout the first quarter of 2015, CYREN saw lower-profile occurrences of identity theft that also targeted healthcare organizations – on both the provider and insurer sides of the industry. The most popular tactic used to create the breach is a phishing email that steals credentials from the recipients by appearing to be from a legitimate source or website, once again emphasizing the value of a Web security solution that can react to such threats in real-time.

The driver for this is clear: in the course of their everyday business, healthcare organizations accumulate large volumes of personal data, including highly-prized social security numbers. And as we revealed in the CYREN 2015 Security Yearbook, this type of data is worth ten times as much on the black market as credit card details, as it can be monetized by criminals in multiple ways.

Because of this, we expect these attacks to grow in frequency until healthcare organizations are able to harden their security practices enough to reduce the high ROI that the cyber criminals achieve from such campaigns. It should be noted though, that other enterprises that hold similar data will also suffer the same sort of attacks.

In this quarterly report, we provide comprehensive statistics on the threat landscape and take a deeper look at some techniques that the criminals are using to gain access to enterprise networks including:

- Web malware
- Email attachment – macro malware
- Breaches to Slack and HipChat social collaboration services

We hope that by covering these threats in more detail, readers of this report can arm themselves with the knowledge and tools to better protect their organization and its' data from the cyber criminals.

In February it was revealed that Forbes.com was compromised as part of a 'watering hole' campaign that was active in the last days of November 2014. In a watering hole attack, a website that is regularly visited by users from a targeted organization is compromised to serve malware to enable infiltration of the target. While the attackers were reportedly targeting US defense companies, the exploits affected all visitors to Forbes.com.

The attack appears to be the work of an espionage group known as the "Sunshop Group". This group is also behind a 2013 watering hole campaign that used the US Department of Labor website to serve malware.

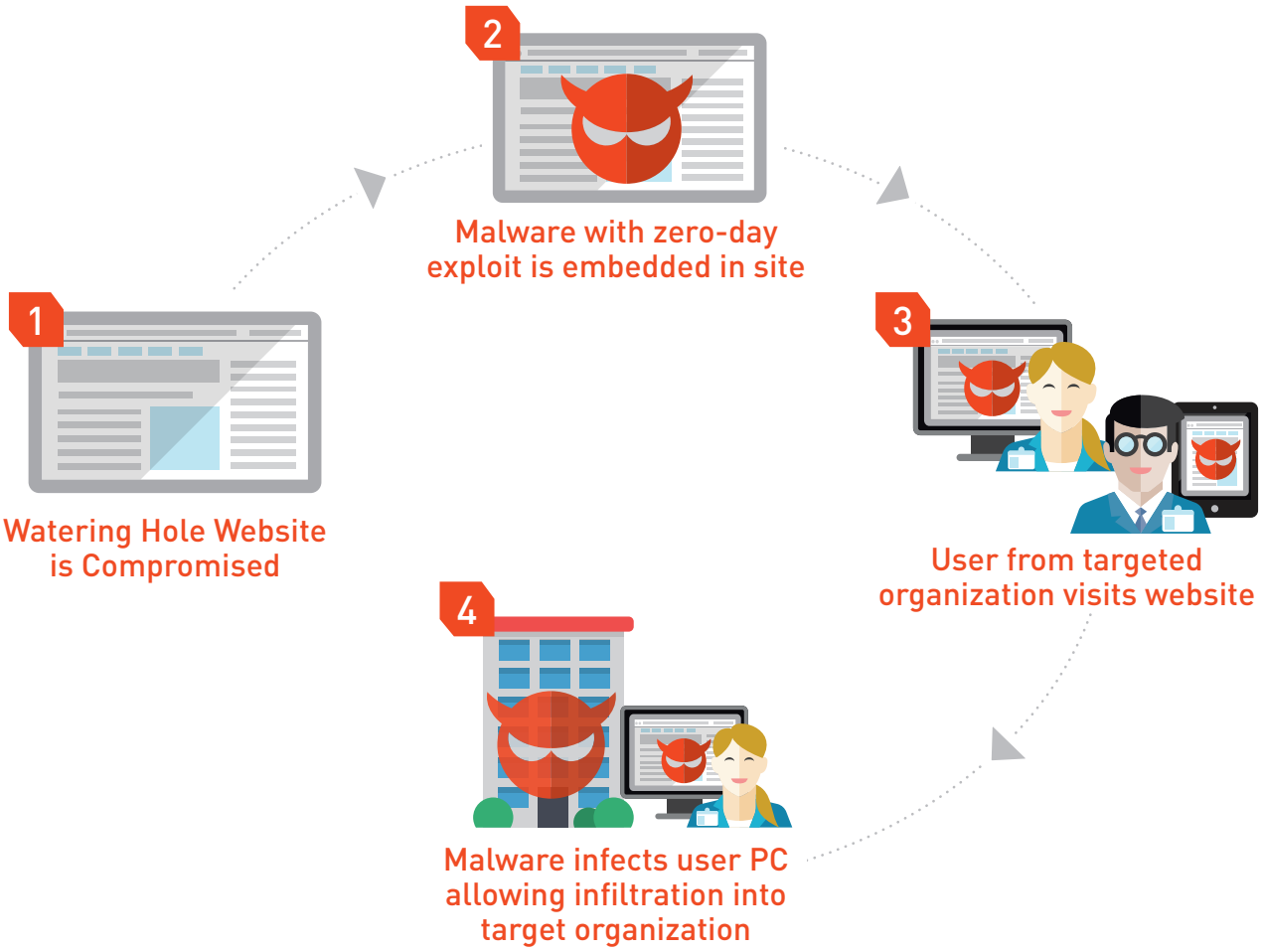
This attack highlights how businesses of all sizes can be exposed to the threats of Web malware where the site serving the malware is reputable – and therefore trusted by the user - and is unlikely to be blocked by most Web filtering solutions. To avoid these attacks, a combination of Web filtering and inline malware scanning of files returned by a browser query - such as that provided by CYREN WebSecurity (see sidebar below) – is the most effective solution.

Malware delivered from these websites generally takes two forms.

1. The user downloads a malicious file (or a file download is initiated automatically) that is disguised as something benign, such as a PDF document.
2. The exploit happens without the user's awareness, such as when a Flash-based animation is played.

In either case the source of the Web malware are predominantly exploit kits. These kits, in the form of obfuscated JavaScript on the final destination page, scan the user's versions of various browsers and add-ons for unpatched vulnerabilities, then deliver the appropriate payload to begin the process of compromising the victim's computer.

Watering hole Attack



CYREN WebSecurity

Applied Cyber Intelligence for Enterprises

CYREN security solutions are time-tested and field-proven. Over 200 technology providers and security vendors as diverse as Google, Microsoft, NETGEAR, Check Point, and Websense use cloud-driven security technologies and data from CYREN, the trusted provider to the security industry.

Every day, the CYREN cloud collects over 17 BILLION transactions from 600+ MILLION users across multiple security domains to assemble an unmatched view of cyber threats as they emerge.

CYREN deploys innovative detection technologies, including custom sandbox arrays and automated processes, on a global basis. As a result, intelligence gained from any transaction within the CYREN cyber security platform instantly updates protection for all users.

Our cyber security platform automatically investigates IPs, domains, hosts, and files associated with suspicious behavior and maintains risk scores, enabling instantaneous reclassification. This real-time, actionable cyber intelligence is available as intelligence data feeds, or as full-function security products for Business users.

CYREN WebSecurity—Our premier Applied Cyber Intelligence solution. CYREN WebSecurity is a cloud-based secure web gateway that applies our leading Cyber Intelligence to deliver uncompromising protection and enforcement of Web policy for enterprise users - in any deployment model, and without the cost and complexity of traditional appliance-based solutions.

CYREN WebSecurity not only delivers the best protection, it does so at the lowest Total Cost of Ownership (TCO), and in a model that enables and supports the evolution and competitiveness of today's enterprise IT organizations. CYREN WebSecurity provides comprehensive protection for business users – whether office-based, remote, or roaming and also protects users of Guest WiFi or Public WiFi services.

The most prevalent Web malware in Q1 2015, as analyzed by CYREN, includes such exploit kits in 5 of the top 10 positions. This includes malware detected as "JS/Blacole.DF.gen", which is better known as "Blackhole". The Blackhole exploit kit, which is reportedly available for rent, scans the visiting system to determine the versions of popular software such as Adobe Flash, Adobe Reader, Java, Windows, as well as various browsers. Once the kit detects a vulnerability - for example, an older version of Adobe Flash - on the visiting system, the relevant exploit is loaded, enabling the controller of the exploit kit to gain a foothold on the now-infected system. Having gained control of the visitor, the controller can then deliver further malicious content, which may include a wide range of badware such as fake AV, ransomware, or keylogging software to steal banking and Web credentials.

The other entries in the top 10 Web malware for Q1 illustrate that modern malware is primarily focused on making money. The two most prevalent entries are identified as JS/SEOHide.A and JS/Faceliker.a. Both SEOHide and FaceLiker are specifically focused on methods for generating revenue by hijacking the resources and activities of unsuspecting site owners and site visitors.

FaceLiker is a family of JavaScript-based clicker-Trojans which hijack mouse clicks on compromised websites to make

users like a particular Facebook page without their knowledge or consent. The malware hooks into web page mouse events, making a hidden Facebook like button follow mouse movements, essentially hijacking the clicks made by the unsuspecting user. Getting unsuspecting users to like a Facebook page is often a first step in spreading 'malvertising' scams on Facebook. For example, friends of the unsuspecting user see a highly-liked page with a title offering a free voucher to a well-known coffee chain. These friends then visit the links on the liked page and are tricked into filling in surveys or signing up for unwanted offers, generating 'pay for click' or affiliate marketing revenue for the cybercriminal.

SEOHide - Advanced blackhat search engine optimization

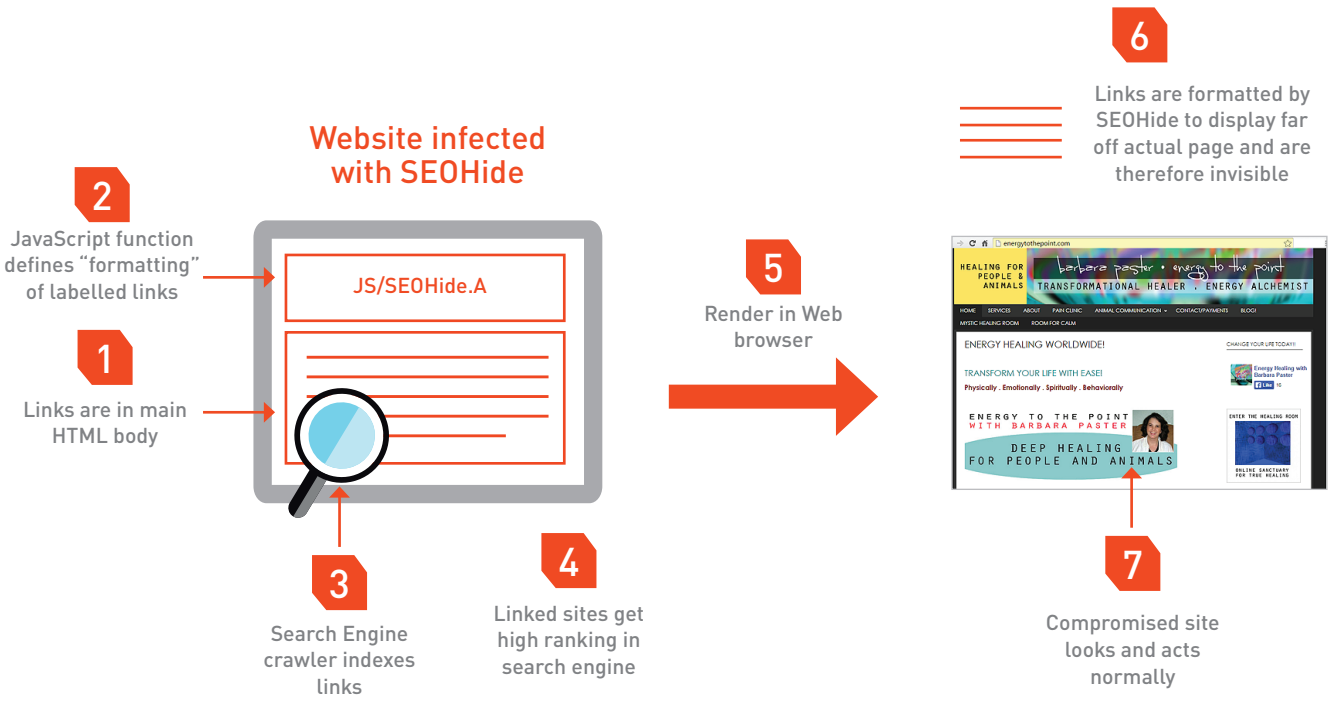
SEOHide is a family of JavaScript Trojans, which are commonly injected into compromised websites to boost the page ranking for specific websites by hiding hyperlinks to them within the infected sites. These type of Trojans are also known as 'blackhat search engine optimizers' as they use standard, although in this case malicious, SEO techniques to boost the placement of the targeted sites in search engine results. An example of such a compromised site is energytothepoint.com (pictured here) – where the compromised site continues to function as before while the links operate without the knowledge of the site owner.

Cybercriminals use this technique to give a short-term boost in search rankings to a site that they are targeting. This can be monetized in many ways – for example, they may be receiving commission on any business transacted through the site or, as is more usually the case, they are using the target site to deliver a malicious payload to unsuspecting visitors.

As an example of the techniques used, links could be "hidden" by making them the same color as the background or using minute font sizes. SEOHide uses techniques that are far more difficult to detect:

- The links are featured in the body of the page but are defined by a specific JavaScript function called "dnn", for example;

SEOHide - Advanced blackhat search engine optimization



- Easy access to payday loans

- The encoded JavaScript function "dnn" is actually a single line of CSS code :
  - o <style undefined>.dnn{position:absolute;top:-999px}</style>
- This code sets the position of all HTML objects having the class name "dnn". The value of "top" is "-999px", effectively hiding the object (in this case the hyperlinks or layers) way above the page display screen. This CSS code can therefore hide any type of element such as layers, paragraphs, images, anchors and more. If the attacker chooses to hide layer objects/elements, then the layers can sometimes contain several hyperlinks, thereby providing SEO for multiple pages.

Search engine vendors eventually catch up to this 'boosting' of the target site and it is removed from search results but, by then, the criminals have achieved their goal and moved on.

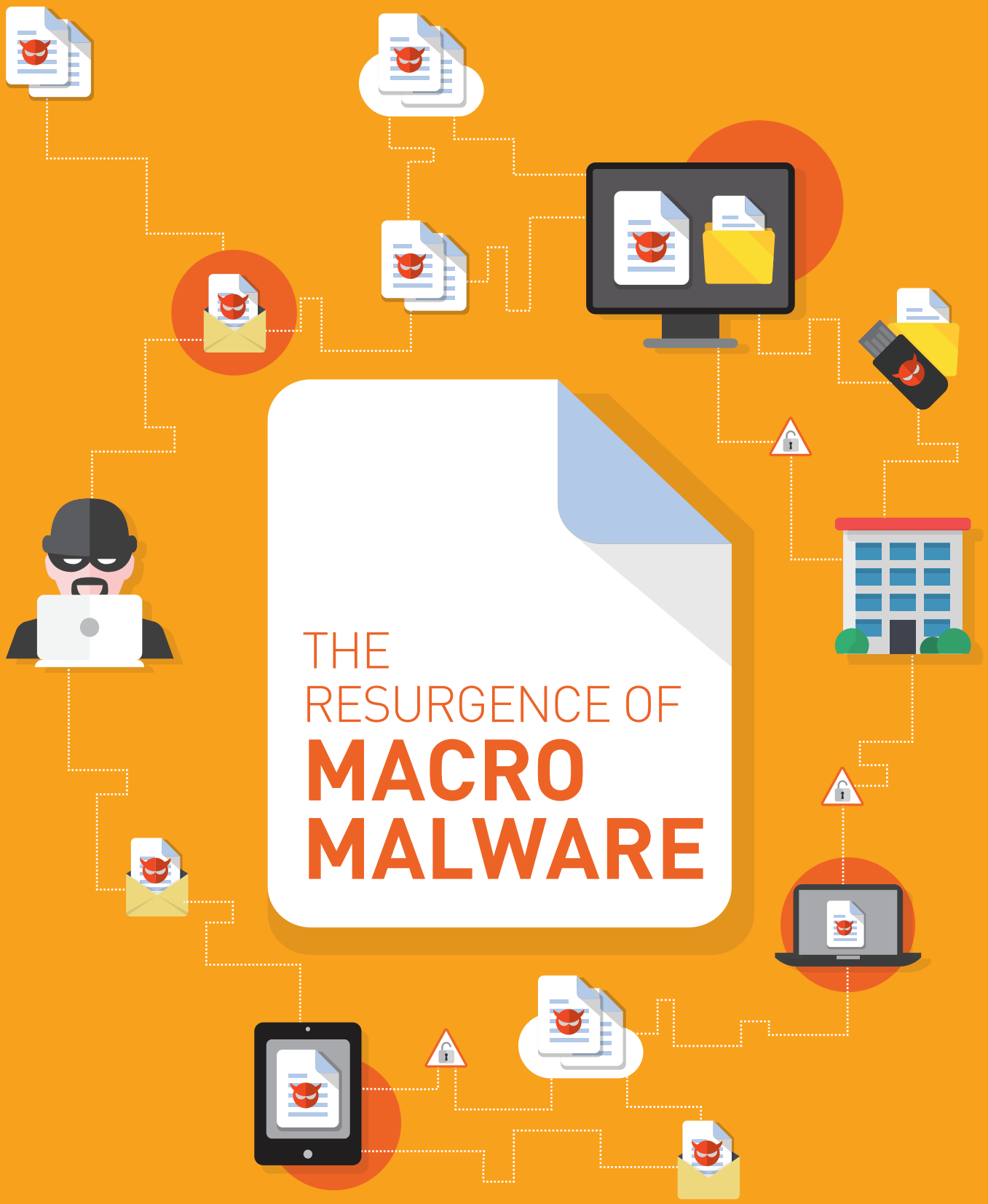
As part of the SEO strategy, the hyperlink tags would include several keywords, which are mostly related to the product that is being "sold". In this case one of the targets is payday loans and therefore the links and tags include related terms. In sites promoting pharmacy pages, pharmaceutical terms that are common to pharma email spams such as Cialis, Viagra and the like, are used.

THE CHALLENGE TO IT ADMINISTRATORS OF KEEPING SECURITY CURRENT

While exploit kits may use previously unseen, or "zero-day" vulnerabilities –unknown even to the software originator –most use vulnerabilities that are well known, relying on the fact that end users find it difficult to keep up with security updates and patches. To illustrate the extent of the threat, consider that the most recent Adobe Flash update (released on April 14th, 2015) addressed no less than 22 known vulnerabilities.

This shows that IT administrators will significantly improve resistance to threats by ensuring all end-user software is fully patched and updated. This still presents a significant challenge in an environment with many users and multiple versions of software.

Fortunately, a range of tools are provided by software originators and third parties for just this purpose. For example, those using Microsoft Windows environments can use Windows Server Update Services (WSUS) to control the distribution of Windows updates and also for 3rd party applications. Where users are expected to apply updates themselves, proper education is essential to ensure that they understand the importance of allowing the patch processes to take place.



THE RESURGENCE OF MACRO MALWARE

Persistent use of a particular malware distribution technique is a sure sign that it is working for the cybercriminal. This is definitely true of the continuing surge in the use of macro malware. A brief recap:

- Microsoft's popular Office applications include macro functionality based on VBA (Visual Basic for Applications);
- In March 1999 the Melissa macro virus was put in the wild and infected an estimated 20% of computers worldwide, by targeting a vulnerability in VBA macro processing;
- To mitigate this vulnerability without abandoning the macro capability altogether, Microsoft patched Office to force users to actively decide whether to run any macro or not by showing a warning pane and requiring them to click on "enable" or "allow" before processing the macro.

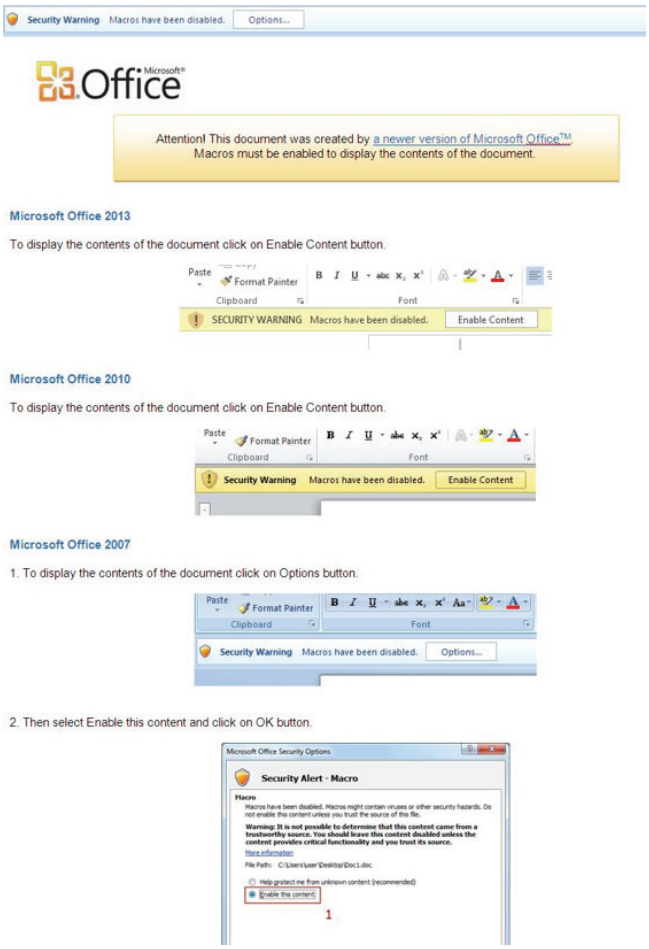
As a result of this change, macro viruses fell out of favor and cybercriminals moved on to other malware types and means of infection. Then, in November 2014, CYREN observed an outbreak of over 3.02 billion emails containing new macro-malware. Subsequent outbreaks in December consisted of as many as 1.2 billion emails a day.

The novelty for the malware distributors was in the social engineering that was used to propagate the threat. The trick is to persuade users to click on the "enable" button in Word or Excel, thereby activating the malware. The tricks rely on the premise that users may not be familiar with why macros are 'blocked' as standard, and also that they may be conditioned to click 'enable' when they see this sort of message as it will also appear when opening innocuous attachments that have been sent by a trusted contact. Examples of the methods used are:

- Showing only a blurred image when the victim opens the file. Readable text says: "The document is blurred due to security reasons. Click the 'Enable' button above to view the document".
- Showing an unreadable string of text with instructions suggesting that the coding is incorrect and that by pressing the "Enable Content" button, the document will be rendered readable. When the victim clicks on the button, the macro code automatically executes and drops or downloads other executable files.
- A new method, first seen in March 2015 - Informing the user that the document was created by a newer version of Microsoft Office – requiring the user to enable macros in order to display the contents. As shown in the related image, instructions for enabling macros are provided for multiple versions of Word.

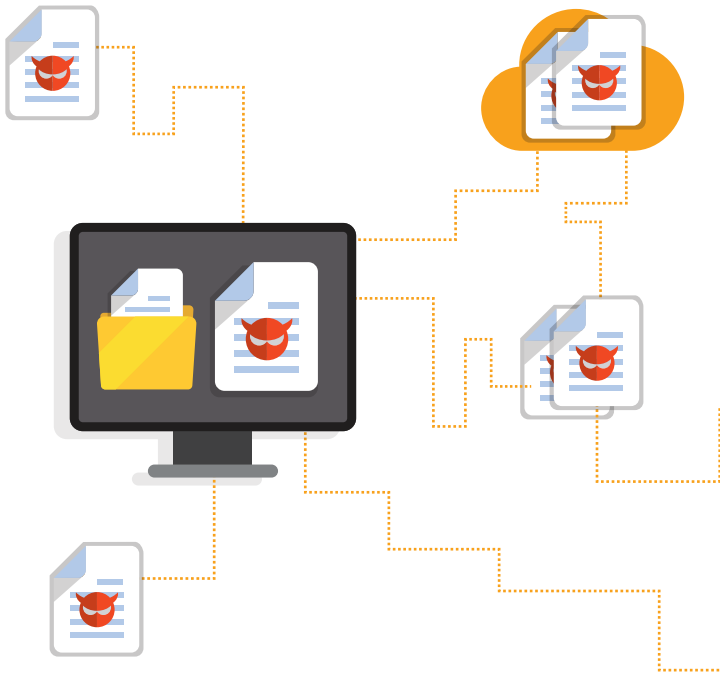
While the underlying macro programming language – "Visual Basic" – might imply that the malware is not sophisticated, it is as complex as any other modern malware. Most variants of recent macro malware that CYREN has captured and analyzed are encrypted

Examples of Macro Malware Techniques in Microsoft Word



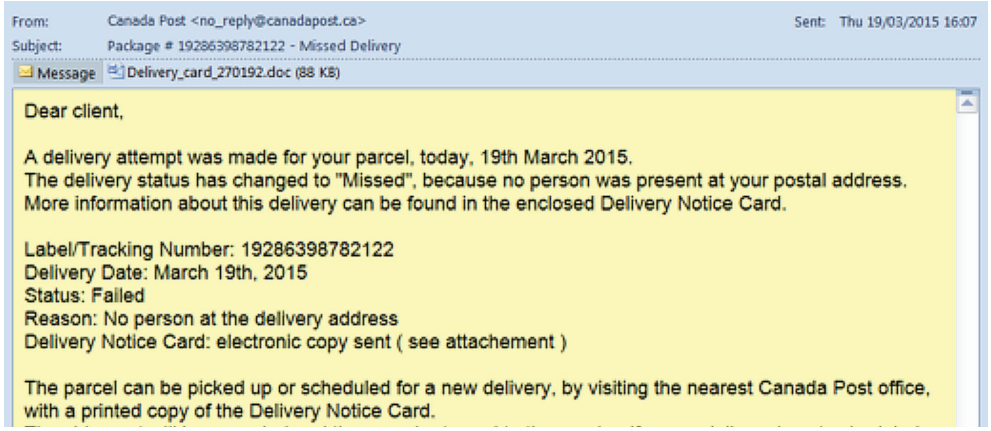
and download other malware from dedicated servers. These malware downloads include notorious banking Trojan families like Zbot and Dridex. In Q1 CYREN also detected a brand-new variants of macro malware with additional functionality beyond simply downloading and installing other malware. These variants gather system information and send this to a remote server. The information gathered includes: currently logged on user names, a list of network users, user account details, a list of shared folders, host IP configuration, tasks and services, and a list of installed applications. This sort of data is useful for planning individualized phishing or other types of attack on a target organization.

In the most recent macro-malware variants, Trojan code is downloaded from Pastebin.com. Pastebin.com is a website where anyone can store text for a certain period of time. The website is primarily used by legitimate programmers to store pieces of source code or configuration information, but users can store any type of text there. The idea behind the site is to make it easy for people to share large amounts of text online. The implications of this new approach to malware delivery for business users are serious; with the code hidden in a legitimate site it is extremely difficult for standard Web filtering products to identify the traffic (the request to pastebin.com for the malware code) as being a threat.



The initial delivery method of choice for the current crop of macro malware is via email attachment. One of the big advantages for malware distributors is that document attachments are rarely blocked by email security applications (as opposed to executable files). Here too, the current variants are successful in evading most antimalware engines.

The "Canada Post" example shown here includes a .doc attachment that was detected by only 4 antimalware engines (out of 56 checked) upon receipt. This illustrates that organizations cannot solely rely on traditional antivirus for malware detection.

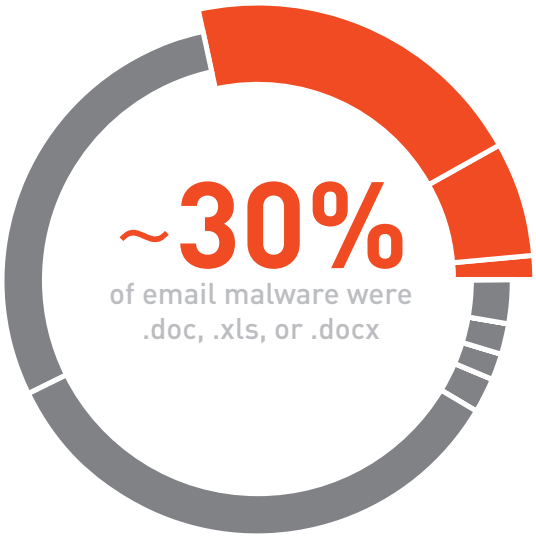


Canada Post Example

This .doc example was detected by only 4 of 56 Antimalware engines.

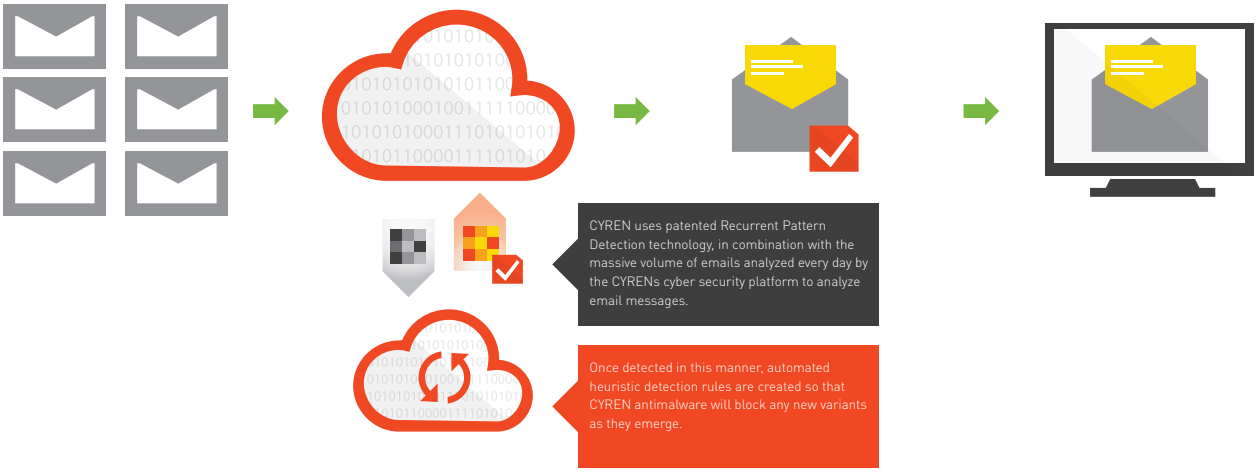
CYREN detection of zero-hour macro malware does not rely on traditional signature, or even heuristic malware detection methods. CYREN instead uses a patented Recurrent Pattern Detection technology, in combination with the massive volume of emails analyzed every day by the CYREN cyber security platform. Because of this, the same attachment that is received by CYREN multiple times from multiple compromised or "zombie" sources is identified as malware and then blocked by CYREN– all within moments of an outbreak starting. Once detected, automated heuristic detection rules are created so that CYREN antimalware will block new variants as they emerge. In the absence of a CYREN-based solution, businesses should educate users about the threat of macro-malware.

Percent of Attached Malware that is .DOC or .XLS Over the Past 6 Months



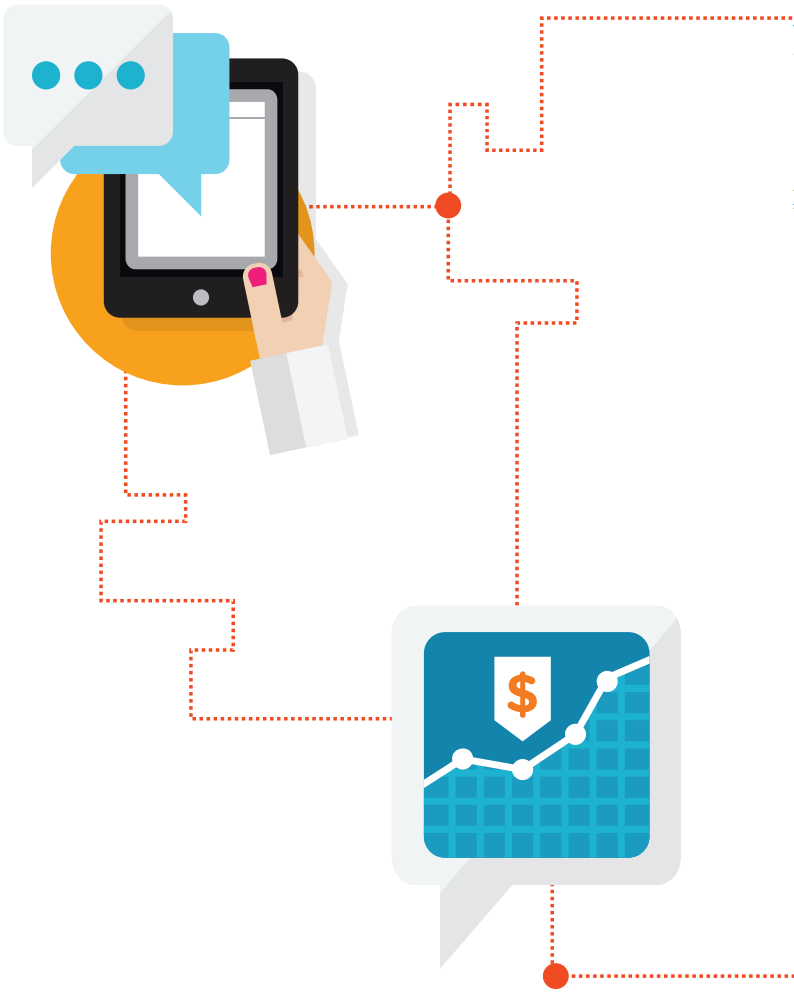
Nearly 30% of all email attached malware sent in the last 6 months has been macro malware, with .doc, .xls, or .docx extensions. In the preceding 6 month period there was virtually no such malware.

Malware Attack Detection by CYREN




LESSONS
LEARNED
FROM THE
SLACK &
HIPCHAT
BREACHES
$
Login
Administrator
Password
* * * * 6 8 4 2

SLACK AND HIPCHAT BREACHES



In late March Slack confirmed they had suffered a security breach where "there was unauthorized access to a Slack database storing user profile information". Slack is a recently launched team collaboration tool that offers organizations a way to simplify communications, file-sharing, project management and more. Organizations sign up their employees who then collaborate in open, searchable groups.

During the breach, which continued for about four days, the hackers had access to a central database which includes user names, email addresses, and one-way encrypted ("hashed") passwords. In addition, this database contains information that users may have optionally added to their profiles such as a contact number and Skype ID. In a blog post following the breach, Slack said that the company noticed "suspicious activity" on a small number of accounts: "As part of our investigation we detected suspicious activity affecting a very small number of Slack accounts. We have notified the individual users and team owners who we believe were impacted and are sharing details with their security teams." This statement seems to imply that the hackers gained access to the actual chat and share areas of some organizations which have signed up to Slack. This would give them access to all shared documents, code and discussions – many of which may contain confidential company information.

The Slack breach comes one month after a similar breach at another productivity startup – HipChat, which also offers intra-business chat and collaboration. They issued a similar announcement, telling of, "suspicious activity on the HipChat service that resulted in unauthorized access to names, usernames, email addresses, and encrypted passwords for a very small percentage (<2%) of our users."

There are two main lessons that organizations must learn from these breaches:

- Online (cloud) business tools are now targets for cybercriminals: the popularity of these tools has not escaped their attention. They offer a treasure trove of business credentials (emails and passwords as well as Skype usernames), as well as internal business data that can potentially be used for espionage. The advantages that group discussions, searchability and access across multiple platforms bring to businesses, also open up potential risks. In addition, employees often treat the collaboration tools as if they are internal systems and may be less cautious with the information that they share.
- User passwords must be managed carefully: The breaches of Slack and HipChat enabled hackers to obtain encrypted passwords. While both services assured users that the passwords were safe, the possibility to decrypt them exists. A secondary benefit to the criminals of obtaining these passwords is that – whether they use a single signon (SSO) approach or not - the logon-id and password used for the chat platform, may well be identical to that used for other internal business systems. Because of this, when using these platforms, administrators should force users to choose passwords that are sufficiently complex and different from those used within the organization.

CYREN

CYBERTHREAT Report

Applied Cyber Intelligence

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 direct to Web traffic for customers through the CYREN WebSecurity product.

17B pieces of threat data

600M Global Users

500,000 Global points of presence

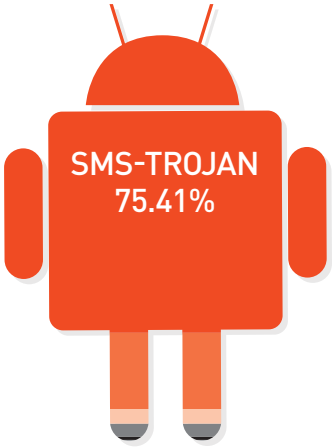
200 Countries

Macro Malware on the Rise

Nearly 30% of all email attached malware sent in the last 6 months has been macro malware, with .doc, .xls, or .docx extensions. In the preceding 6 month period there was virtually no such malware.

Malware URLs tracked by CYREN

1.02 Million

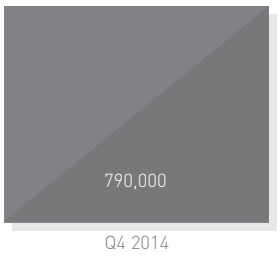


Android Malware by Type

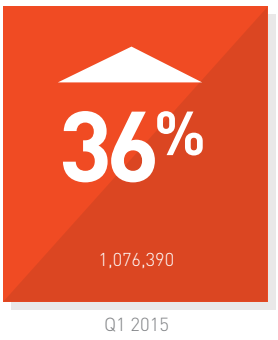
SMS-Trojan	75.41%
Spyware	2.97%
Adware/PUA	17.49%
Backdoor	3.36%
Other	0.76%

Android Malware Levels

New android malware detected in Q1 was 1,076,390 compared to 790,000 in Q4 2014.



Q4 2014

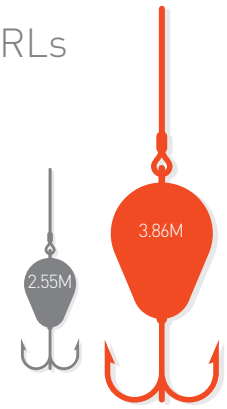


Q1 2015

Phishing URLs

51%

CYREN has seen a 51% increase in phishing URLs since January 1st.



Spam levels

Average daily amount of spam emails sent 48.8 billion per day in Q1 2015 compared to 53.6 billion per day sent in Q4 2014

Spam topics

Dating	40%
Pharmacy Products	17%
Job Offer	13%
Phishing	3%
Stock	2%
Replica	1%
Other	24%

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