CYREN

INTERNET THREATS
TREND REPORT

OCTOBER 2014

THE STATE OF CORPORATE SECURITY

Lior Kohavi
Chief Technical Officer, CYREN, Inc.

The Companies—Home Depot, JP Morgan Chase, Target

The Information—56 million credit cards, 76 million 'households,' 7 million small businesses, and 110 million accounts

The Impact—According to recent reports, Home Depot estimates that investigation, credit monitoring, call center, and other costs could top $62 million. Target's stock fell by almost 14% in the months following news of the breach, with profits down 46% by the end of Q4 2013, and breach-related expenses totaling $146 million. The impact of the JP Morgan Chase data breach has yet to be determined, but early reports suggest the costs could top that of Target.

These are just a few of the big names that have hit the headlines recently. But, it's not just large organizations being hacked. Regional small- to medium-sized businesses (SMBs) are potentially even greater targets, as hackers view SMB security as less sophisticated and easy to breach. According to a 2013 Verizon report, which analyzed 47,000 security incidents, 40% of all confirmed breaches involved companies with fewer than 1,000 employees; more notably, the largest single segment of corporate breach victims among companies with less than 1,000 employees were companies with fewer than 100 employees.

When you consider that an estimated 60% of all companies experiencing a cybersecurity breach go out of business within six months of the attack, it is a wonder that all corporations aren't making cybersecurity a higher priority. Yet, the level of corporate complacency with regard to cybersecurity remains high. CYREN regularly hears from potential (and even a few current) clients, "We're too small to be noticed by cybercriminals." Or "We're not a government agency with classified data. Why would someone want to break into our systems?" Additional news reports suggest that IT security staff do not even meet with the executive staff on a regular basis. (One report cited only 1% of IT and IT security staff engaging in weekly staff meetings with executive staff).

Ultimately, no one needs a crystal ball or series of complex research studies to predict that cyberattacks are on the increase and will continue to remain so for the foreseeable future. Yet, many of these attacks could be stopped simply by investing in the solutions and staff needed to protect both the organization and the customers.

CYREN continues to remain at the forefront of cybersecurity innovation and protection. And, while we can stop more than 99% of cyberattacks from happening, we can only do so with organizations and corporations that recognize that a very real threat exists.

Q3 INTERNET THREATS TREND REPORT SUMMARY

In the third quarter of 2014, attention was focused on celebrity account hacking and corporate data breaches. By the end of the quarter, cybersecurity professionals had received yet another agonizing reminder that no system is perfect with the announcement of the Shellshock bug affecting the BASH shell. Cybercriminals also used global tragedies, such as Ebola and airline disasters, to further enhance their phishing, spam, and malware distribution efforts.

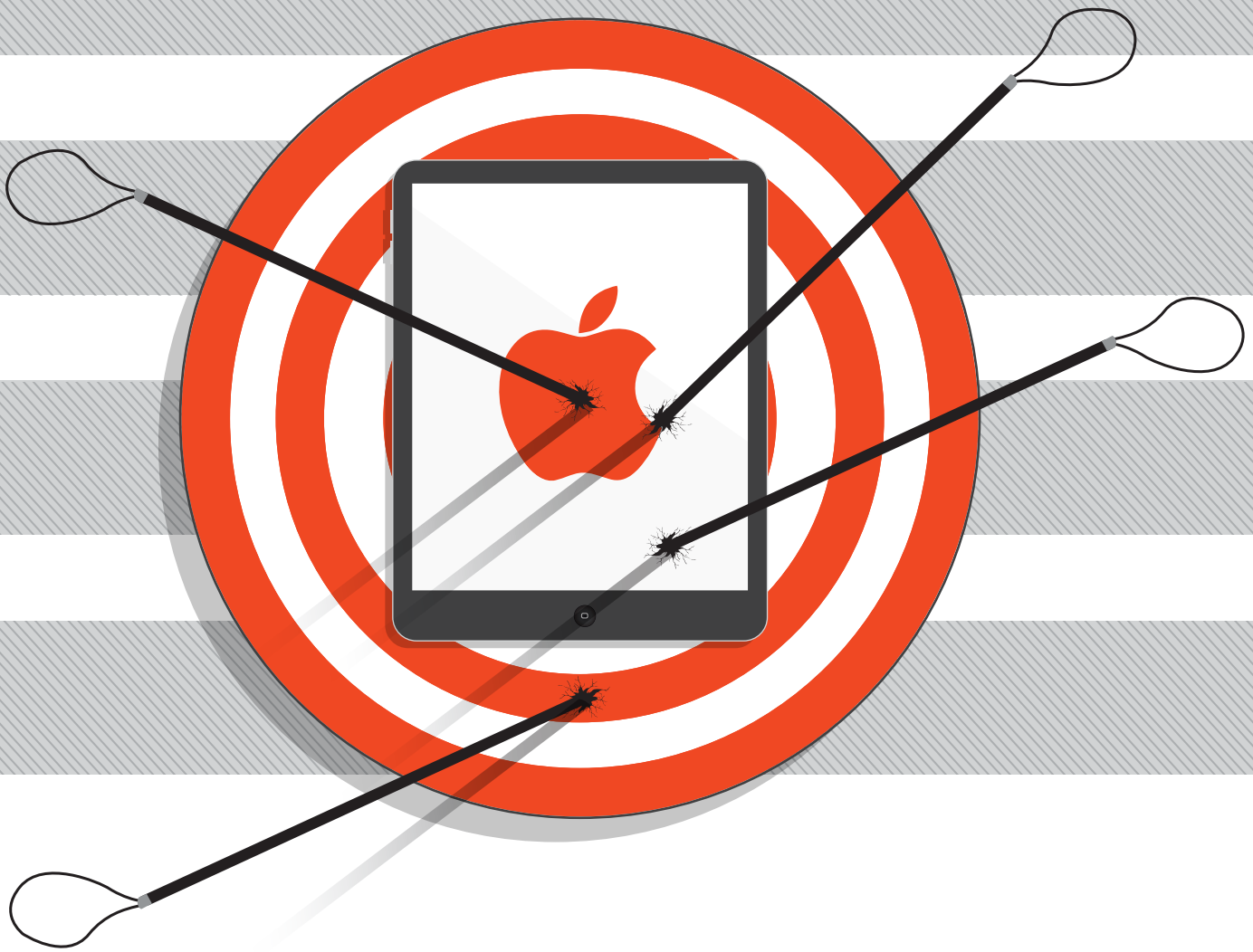
The High-profile Data Breach Quarter

From celebrity Apple iCloud accounts to Home Depot and the possibility of a Backoff-type virus attack on their point-of-sale systems (POS), virtually no one went unscathed as a result of this wide-spread and high-profile hacking. Consumers found that cybercriminals once again had access to their credit card numbers, celebrities learned that personal and private information had been shared worldwide via the Internet, and corporate CEOs began to count individual data breach losses in the hundreds of millions of dollars.

Bugs and Malware Left Unchecked

The announcement of the discovery of a major flaw in the BASH shell left computer programming and cybersecurity professionals reeling. Having gone unnoticed for over 20 years, the Shellshock bug leaves hundreds of millions of devices, including servers and computers, vulnerable to major attack. As consumers learned that once again their personal credit and banking information had been stolen from a major corporate retailer, news reports began to circulate that Home Depot had a long history of failing to update security systems and fully fund cybersecurity staff. Coincidentally (or not) a few weeks prior to the Home Depot announcement, the U.S. federal government released a warning about the Backoff malware indicating that it was the focus of several POS data breach investigations. It seems that while all top antivirus providers had updated their antivirus services to protect from Backoff, retailers had not been updating their systems.

Further Report Highlights: Diet spam featured heavily, accounting for 31% of all spam emails this quarter, and The Russian Federation, followed by Vietnam continue to hold the top spots for zombie countries.



APPLE USERS BECOMING #1 TARGET

In the wake of the Apple iCloud celebrity data breach, CYREN decided to take a deeper look at cybercrime targeted at the Apple device market.

The Great Celebrity Photo Hack

In early September, corporate water coolers were abuzz with news of photos being leaked on the Internet of celebrities in questionable [cough—ahem] states of dress. Celebrities have long been known to prefer Apple products over others and news quickly spread that cybercriminals gained access to the photos via Apple's iCloud service.

Appearing almost as quickly as the news of the photos, was the speculation on how criminals hacked into iCloud. Initially, theories included vulnerabilities in the Find My iPhone service, combined with "brute-force hacking" (systematic checking of all possible user names or passwords until the correct one is found). Within hours, however, Apple announced that their computer systems (which house user iCloud data) had not been hacked.

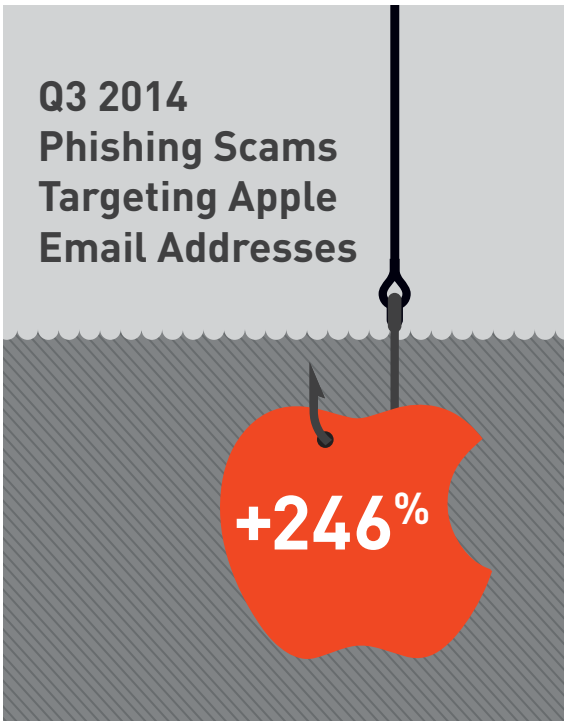
"...After more than 40 hours of investigation, we have discovered that certain celebrity accounts

were compromised by a very targeted attack on user names, passwords and security questions, a practice that has become all too common on the Internet. None of the cases we have investigated has resulted from any breach in any of Apple's systems including iCloud® or Find My iPhone."

This "very targeted attack on user names, passwords and security questions" implies a mix of phishing as well as the techniques used by Chris Chaney (see sidebar below); by doing research on celebrities, hackers were able to guess the answers to security questions and then use the reset password feature. Investigators suspect that the breach is the work of a ring of hackers (some of which are likely based in the United States), but their identities remain unknown. Security experts also speculate that other highly personal information, such as phone call logs, calendars, text messages, and even confidential documents such as contracts and movie scripts could also have been stolen, as this type of data is also commonly backed up in iCloud.

CYREN Analytics Observes Increase in Targeting of Apple Users

If there is one thing the celebrity phishing-photo scandal taught us, it's that Apple users are a significant target for scams and hacking. While the iOS and OSX operating systems still remain



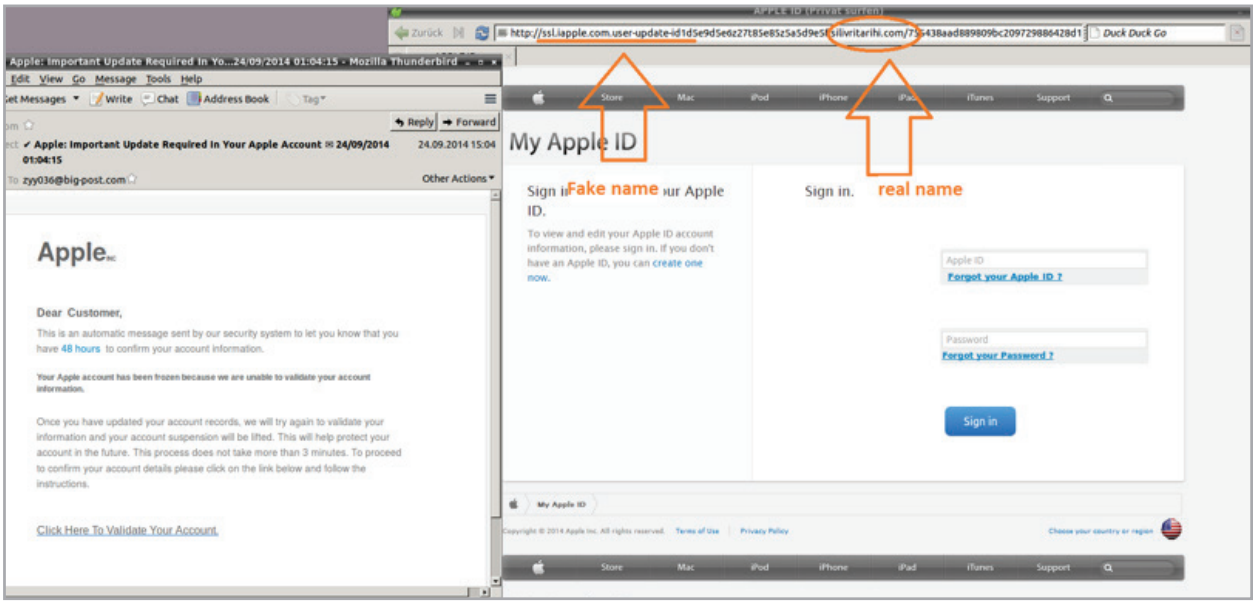
Did the Celebrity Photo Hackers Take a Page from the Chris Chaney Book?

In December 2012, "Hollywood Hacker" Chris Chaney was sentenced to 10 years in prison and ordered to pay $66,179 in restitution for hacking into computers owned by individuals associated with the entertainment industry and for distributing the illegally obtained content. He obtained passwords by clicking on the "forgot your password" function and correctly guessing the security questions based on his research into celebrities' personal lives. Once inside celebrity email accounts, he changed the settings to forward copies of the emails to his personal inbox. Celebrities didn't even know their account settings had been changed, even after they regained control of their accounts.

relatively safe, more and more individuals globally are buying Apple devices and using Apple services, which could account (in part) for the increased targeting of Apple users. There are currently more than 800 million Apple IDs in use. Over 300 million individuals hold iCloud accounts, giving them access to 5 GB of online storage, as well as email, calendar, and photo stream. And, phishing attacks are at least three times more likely to be successful on a smart phone than on a desktop or laptop, mainly because telltale giveaways, such as fake links, logos, and email addresses, aren't as easily visible on a small mobile phone screen.

With the news of the Apple-based hack into celebrity accounts, CYREN decided to take a deeper dive into our own analytics to see if we had observed an increase in Apple phishing. Overall, phishing scams targeting Apple users were up 246% from the 1st quarter of 2014 – with CYREN tracking over 7,000 new Apple phishing sites in the week of the celebrity hack. This seems to coincide with anecdotal evidence we were hearing from Apple iCloud users, citing their own personal observation of more phishing and spam emails slipping into their email boxes undetected.

In one Apple phishing example captured by CYREN, this criminal attempted to mislead the victim by faking the URL. You need to look closely and understand URL addressing to see that the real domain is silivritarihi.com and not a legitimate apple address.



Phishing example identified by CYREN

On top of increased phishing, CYREN began to wonder if Apple made the situation more confusing for users by initiating a new email alert campaign shortly after news of the celebrity attacks. It informed Apple iCloud users that their Apple ID was recently used to sign into an iCloud account via a web browser.

While the email is entirely legitimate, it presents several problems for iCloud users in that it looks very similar to phishing emails and it gives scammers a perfect opportunity to copy and paste correct content into fake emails to attempt to make their phishing emails look legitimate.


Your Apple ID was used to sign in to iCloud via a web browser.
September 08, 2014 10:13 AM
From Apple

Dear

Your Apple ID (@mac.com) was used to sign in to iCloud via a web browser.

Date and Time: September 8, 2014, 7:02 AM PDT

If you recently signed in to iCloud.com, you can disregard this email.

If you have not signed in to iCloud.com recently and believe someone may have accessed your account, you should reset your password at My Apple ID.

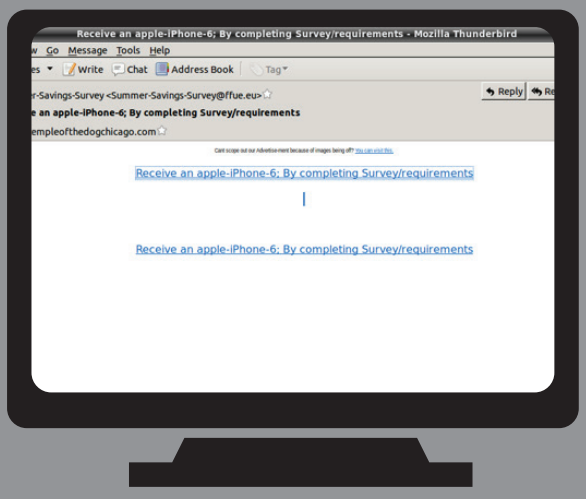
Apple Support

My Apple ID | Support | Privacy Policy
Copyright © 2014 Apple Inc. 1 Infinite Loop, Cupertino, CA 95014, United States. All rights reserved.

Example of legitimate Apple email.

Apple iPhone6 Adware Scams

Cybercriminals were given a further opportunity for revenue generation courtesy of Apple's iPhone 6 launch. As in the past, the excitement about the new iPhone provided fertile ground for new phishing and adware scams. In the example below, users are enticed to click on suspect links by the offer of a brand new, free iPhone 6.



THE BASH-SHELLSHOCK BUG

Shellshock exploded on the scene this quarter, making headlines in major newspapers and security blogs. Discovered by a French security expert in mid-September and disclosed publicly in late September, it has been deemed by many as the "world's most dangerous Internet security bug."

Shellshock is the name given to a security hole in the Unix/Linux "Bash" Shell, version 1.0.3. The bug, having gone completely unnoticed for 21 years, leaves hundreds of millions of Internet-connected devices (including servers and computers) vulnerable to hackers. In fact, it is believed hackers began exploiting it almost immediately upon the announcement of its discovery, using worms to scan for vulnerable systems and infect them. Many security experts also believe that hackers, and even government entities, could have been taking advantage of the Shellshock vulnerability for years.

Bash—which stands for Bourne-Again SHell—is a command processor that typically runs in a text window enabling system administrators and others to issue commands to an operating system without a graphical user interface (GUI). Despite its rather unfortunate name, Bash is a legitimate and popular tool, offering functional improvements over other types of "shell" tools.

By knowing how to access the Shellshock vulnerability and sending a malformed request to a web server, an attacker can cause the Bash shell to execute any command allowed based on the system permissions. In other words, Bash makes hacking into a vulnerable website rather easy. Hacked servers can then be used as DDOS or spam zombies or could hide phishing, malware or spam pages. While the original vulnerability was quickly patched, there have been new reports of other vulnerabilities, so additional patches are expected.

Security researchers have shown that the vulnerability does not just endanger web servers. DHCP (used to allocate IP addresses when users

connect to a network) and Secure Shell (SSH) can be exploited to perform the attack, as long as Bash is the shell. These vectors would endanger Linux/Unix users who, for example, used Wi-Fi with a compromised DHCP server.

CYREN detected Shellshock attacks using the "CGI-based web server attack" technique through a specially crafted HTTP cookie header request field as seen below. Attackers have also used other HTTP request header fields such as 'User-Agent,' 'Accept,' 'Referer' and 'Host' to inject the malicious Bash commands.

CYREN detects the sample as Unix/Flooder.AN. Upon execution, the attacker may perform the following actions (and more) to the infected system remotely:

- Run command instructions in command shell
- Get local IP address
- Scan networks and use hardcoded user/password combinations to login
- Perform UDP/TCP/JUNK/HOLD/STOP flooding

Mac & Bash: Vulnerable? Sort of.

Bash (Bourne-Again Shell) is a command prompt available on computers running Unix-based operating systems, including Macs. While Mac users are theoretically at risk, users would need advanced technical knowledge to enable certain features on their OSX systems in order for a cybercriminal to successfully launch a remote Internet attack targeted at that Apple computer. Since the average Apple computer user rarely (if ever) uses or accesses these technical components, a remote attack isn't likely to happen on grandma's Apple laptop. Fortunately, Apple didn't assume that most users were safe and immediately rolled out its 'OS X bash Update 1.0' for OSX Mavericks, Mountain Lion and Lion users.

```
.rodata:080ACFDE aHold           db 'HOLD',0             ; DATA XREF: sub_804AA67+125↑o
.rodata:080ACFE3 aHoldFloodingSD db 'HOLD Flooding %s:%d for %d seconds.',0
.rodata:080ACFE3                                         ; DATA XREF: sub_804AA67+193↑o
.rodata:080ACFE3                                         ; sub_804AA67+204↑o
.rodata:080AD007 aJunk           db 'JUNK',0             ; DATA XREF: sub_804AA67+21B↑o
.rodata:080AD00C aJunkFloodingSD db 'JUNK Flooding %s:%d for %d seconds.',0
.rodata:080AD00C                                         ; DATA XREF: sub_804AA67+289↑o
.rodata:080AD00C                                         ; sub_804AA67+2DB↑o
.rodata:080AD030 aUdp            db 'UDP',0              ; DATA XREF: sub_804AA67+300↑o
.rodata:080AD034 aUdpFloodingSFo db 'UDP Flooding %s for %d seconds.',0
.rodata:080AD034                                         ; DATA XREF: sub_804AA67+3E9↑o
.rodata:080AD054 aUdpFloodingSDF db 'UDP Flooding %s:%d for %d seconds.',0
.rodata:080AD054                                         ; DATA XREF: sub_804AA67+43A↑o
.rodata:080AD077 aTcp            db 'TCP',0              ; DATA XREF: sub_804AA67+469↑o
.rodata:080AD07B aTcpFloodingSFo db 'TCP Flooding %s for %d seconds.',0
.rodata:080AD07B                                         ; DATA XREF: sub_804AA67+579↑o
.rodata:080AD07B                                         ; sub_804AA67+5C7↑o
.rodata:080AD09B aKillattk       db 'KILLATTK',0         ; DATA XREF: sub_804AA67+5FA↑o
.rodata:080AD0A4 aKilledD_       db 'Killed %d.',0       ; DATA XREF: sub_804AA67+669↑o
.rodata:080AD0AF aNoneKilled_    db 'None Killed.',0     ; DATA XREF: sub_804AA67+672↑o
.rodata:080AD0BC aLolnogtfo      db 'LOLNOGTFO',0        ; DATA XREF: sub_804AA67+687↑o
.rodata:080AD0C6 aRecvS          db 'recv: %s',0Ah,0     ; DATA XREF: sub_804B113+119↑o
```

Code Snippet of Backdoor Functions

Tragedy drives the headlines. A simple click through the leading news websites tells a sad story: More Ebola Victims. Expanding War in the Middle East. Death, Floods, Famine. The list goes on. The use of "sensationalism" to promote a headline or sell an item is nothing new. And, in the 3rd quarter, hackers put this technique to good use.

Phony email that opens an execute (.exe) file.

The Malaysia/Ukraine Airline Tragedy

The tragic shooting down of Malaysia Airlines Flight 17 in July helped fuel 3rd quarter malware trends. In this fake email pretending to be from CNN, victims click on the link only to be taken to an executable file, where a Trojan is downloaded with the purpose of controlling the victim's PC for DDOS attacks, spamming, phishing, or other criminal acts.

Loss of Beloved Actor and IS Executions

This past quarter, the world of the cybercriminal and Facebook collided once again when fake news feeds appeared on Facebook, purporting to have exclusive news about the death of Robin Williams. When users clicked on the link, they were told that in order to view the video, they first needed to "like" the link, thus giving more credibility to the video and helping it to spread further on the social network. Of course, no such video existed, and instead, users were redirected (based on the device they were using) to a variety of different apps in the Google Play store. Similar posts appeared on news feeds promising videos of IS (The Islamic State – previously ISIS) executions.

Since the apps were generally from reputable companies, CYREN suspects that the fake

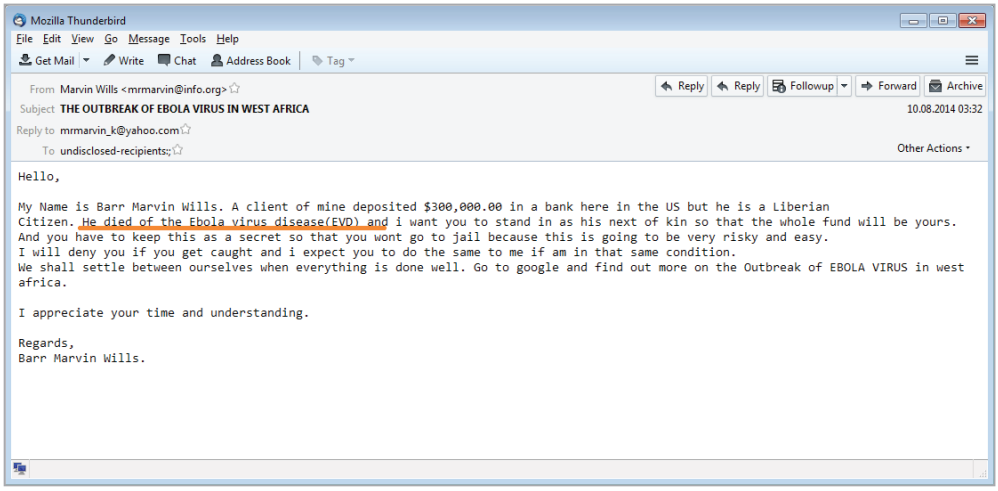
This fake Facebook video re-directs users to

news video, with its adware redirects, provided some affiliate revenue for the news feed creator. Fortunately, having gotten much better at detecting malicious and fake content, within a few hours Facebook had erased all the posts.

Classic 419 Scam Targets Ebola Headlines

In the latest "419" rendition, scammers have capitalized on the West African Ebola outbreak to distribute an email claiming the recipient is the beneficiary of a large amount of money left in a bank account by a client who became a victim of Ebola. To add credibility to the email, the sender suggests the recipient "go to google and find out more on the Outbreak of EBOLA VIRUS in West Africa."

The scammer—Barr Marvin Wills—uses a semi-realistic dollar figure ($300,000) to entice the victim. Other versions also appearing on the Internet claim miracle cures for Ebola by simply contacting the doctor or "priest" listed in the email and presumably paying them money for their cure.



Example of 419 scam email using the Ebola outbreak.

Malware Trends

Compared with the second quarter, the number of unique malware samples collected by CYREN's GlobalView™ Security Lab increased by 35% during Q3, with a total of nearly 22 million malicious scripts, files and docs.

Microsoft Botnet Takedown Targets Houdini; Dunihi Virus Lives On.

At the end of the second quarter, Microsoft made headlines by filing a civil lawsuit against "two foreign nationals, Mohamed Benabdellah and Naser Al Mutairi, and a U.S. company, Vitalwerks Internet Solutions, LLC (doing business as No-IP.com), for their roles in creating, controlling, and assisting in infecting millions of computers with malicious software—harming Microsoft, its customers and the public at large." The two primary malware types—Bladabindi (NJrat) and Jenxcus (NJw0rm)—were distributed by Mohamed Benabdellah (aka Houdini) and Naser Al Mutairi using No-IP domains 93 percent of the time.

At the beginning of the third quarter, Microsoft announced that they had reached a settlement with Vitalwerks (No-IP.com); having reviewed the evidence, Microsoft determined that Vitalwerks had not knowingly supported or been involved with the subdomains used to support and distribute the malware associated with Mohamed Benabdellah and Naser Al Mutairi.

The takedown of the Bladabindi-Jenxcus botnets were a huge boost for the good guys. However, considering that Microsoft had detected more than 7.4 million cases of Bladabindi-Jenxcus viruses in just the past 12 months, it is no surprise that these viruses are still discovered, lurking on personal and corporate computers. In fact, a CYREN analyst detected "Dunihi" (a virus in the Bladabindi family) during the third quarter, and with a little digging was able to view the author's code name "Houdini" (Mohamed Benabdellah) and his Skype address (Houdini-fx) at the start of the malware code.

```
?DdfHsdREsedfgWEsdgdrfRvdcCXGbYYDA
'<[ recoder : houdini (c) skype : houdini-fx ]>

'=-=-=-=-= config =-=-=-=-=-=-=-=-=-=-=-=-=-=-=

host = "8.no-ip.biz"
port = 100
installdir = "%temp%"
lnkfile = true
lnkfolder = true
```

Sample Code from "Dunihi"virus detected by a CYREN analyst.

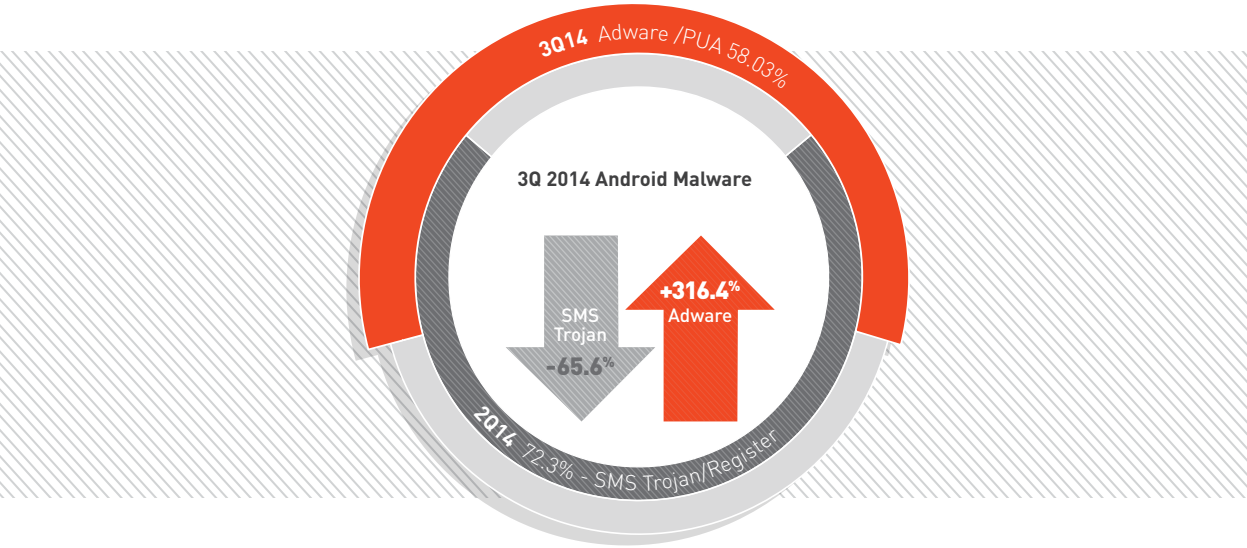
Backoff Point-of-Sale (POS) Data Breaches

Recent high-profile retail data breaches have resulted in millions of dollars in lost revenue, falling stock prices, and frustrated customers. In August, the United States Computer Emergency Readiness Team (US-CERT), in collaboration with the National Cybersecurity and Communications Integration Center (NCCIC), United States Secret Service (USSS), Financial Sector Information Sharing and Analysis Center (FS-ISAC), and Trustwave Spiderlabs, released an advisory "to provide relevant and actionable technical indicators for network defense against the PoS malware dubbed 'Backoff' which has been discovered exploiting businesses' administrator accounts remotely and exfiltrating consumer payment data."

CYREN had detected "Backoff" in the wild for some time, and although there is no confirmation that Backoff was the POS malware used to breach Home Depot, this particular variant has been known for at least a year. All current top antivirus software (including CYREN) provides protection from Backoff, but only if the virus software is up-to-date, which it appears was not the case with Home Depot and other well-known retailers that experienced a data breach in the last year.

Android Malware Trends

During the third quarter of 2014, adware or some form of potentially unwanted application (PUA) accounted for slightly more that 58 percent of all Android malware distributed. SMS/Trojan malware came in a distant second, accounting for approximately 25 percent of all Android malware. This contrasts significantly with second quarter of 2014, when SMS Trojan was the most common Android malware detected by CYREN at 72.3 percent, and adware coming in with only 14 percent.

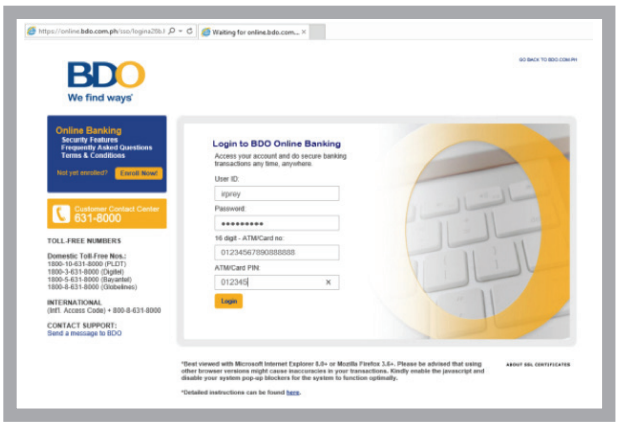


In addition to the suspected large increase in Apple phishing discussed earlier, CYREN detected a notable phishing incident involving DNS poisoning.

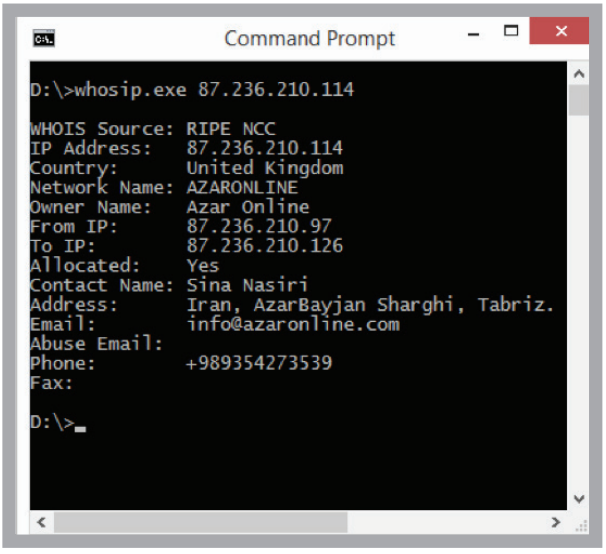
DNS Spoofing at Root of Recent Phishing Scam

CYREN analysts identified a phishing scam this quarter involving something other than typical phishing email or banking malware. Although intended victims would type the banking website address correctly, the page that appeared was in fact malicious.

In this case, a cybercriminal exploited a flaw in the DNS server managed by the Internet Service Provider, and then caused the name server to return an IP address of a phishing server instead of the IP address of the actual banking site. The only warning the victims may have received was a website security certificate pop-up indicating that the site's security certificate was not issued by a trusted authority.



Fake Login Page with Dummy Credentials Entered



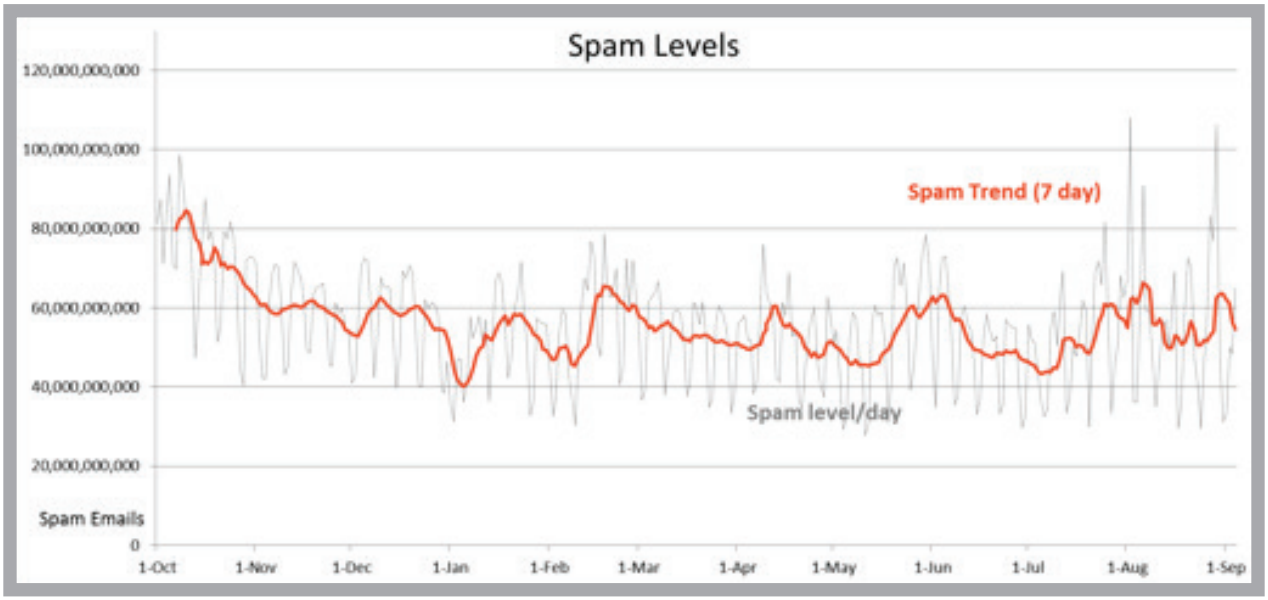
WHOIS Info Details for the phishing site

Monthly Spam Levels Remain Steady

During the third quarter, overall average spam levels remained the same, from a daily average of 55 billion in Q2 to 56 billion in Q3. Spam averaged 68% of all global email. There were notable spikes of diet related spam at the beginning and end of August with daily levels shooting up to near 110 billion emails per day.

Q3 2014 Spam Levels

In Q314 Diet Products Spam increasd by 288% to overtake Pharmacy Products as the top spam category.

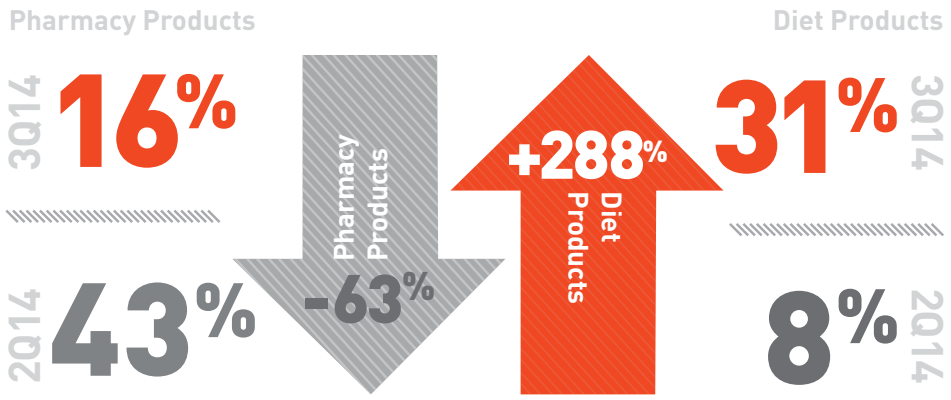


A New Top Spam Topic This Quarter

Pharmaceutical and diet spam exchanged places this quarter; with diet spam accounting for 31 percent of all known third-quarter spam, up an astounding 288 percent from the previous quarter. In contrast, second-quarter leader, pharmaceutical spam, dropped 63 percent, falling to third place and accounting for only 16 percent of this quarter's total spam. Spam related to job offers also increased dramatically from 22 percent in the second quarter to 30 percent currently. Stock and online casino spam rounded out the top five accounting for 11 percent and 8 percent of total spam in the third quarter.

Q3 2014 Spam Topics

In Q314 Diet Products Spam increasd by 288% to overtake Pharmacy Products as the top spam category.



Spam Zombie Countries

The Russian Federation once again led the zombie countries this quarter with 11.5 percent. Vietnam continued its upwardly mobile trend as a zombie producing country this quarter with 11.4 percent followed by China with 9.9 percent. Other long-time board leaders India, Iran, and Argentina stayed in the top 10. Belarus fell off the top 10 list this quarter, with Brazil resuming a spot on the leader board.

1.	Russian Federation	11.5%	**6.**	Taiwan	4.7%	**11.**	Germany	1.8%
2.	Vietnam	11.4%	**7.**	Argentina	3.1%	**12.**	Saudi Arabia	1.8%
3.	China	9.9%	**8.**	Ukraine	3.0%	**13.**	Korea	1.6%
4.	India	9.4%	**9.**	United States	3.0%	**14.**	Italy	1.4%
5.	Iran	5.6%	**10.**	Brazil	2.4%	**15.**	Thailand	1.3%

AND FINALLY...

Junk food lovers, now is your time. The secret is out and it is what you've been waiting to hear for years. Not only are water and milk bad for you, but an apple a day is worse than 30 cigarettes and eating low calorie salads will make you gain weight. At least, that's the news from diet spammers.


CNN National Health Alert

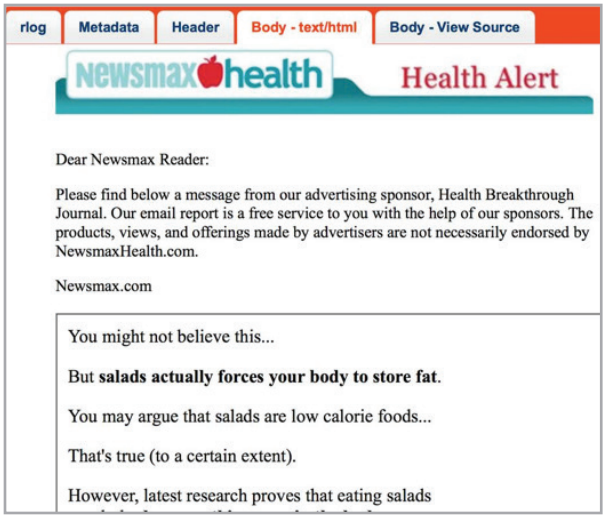
Water May End Your Life Early

Drinking even just one glass a day could lead to serious illness and potential fatality . See why this is so bad

YOU WONT BELIEVE THIS

Watch The Segment #1406324304 Now

Please this to make these end Thanks
~~2903+North~Pacific~Ave._7z Chicago_IL_60634-2033


rlog | Metadata | Header | Body - text/html | Body - View Source

Newsmax health — Health Alert

Dear Newsmax Reader:

Please find below a message from our advertising sponsor, Health Breakthrough Journal. Our email report is a free service to you with the help of our sponsors. The products, views, and offerings made by advertisers are not necessarily endorsed by NewsmaxHealth.com.

Newsmax.com

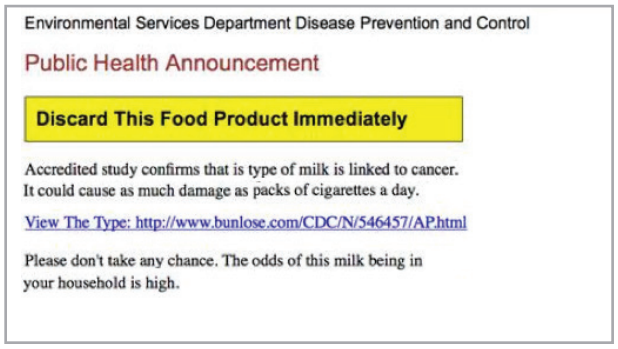
You might not believe this...

But **salads actually forces your body to store fat**.

You may argue that salads are low calorie foods...

That's true (to a certain extent).

However, latest research proves that eating salads


Environmental Services Department Disease Prevention and Control

Public Health Announcement

Discard This Food Product Immediately

Accredited study confirms that is type of milk is linked to cancer. It could cause as much damage as packs of cigarettes a day.

View The Type: http://www.bunlose.com/CDC/N/546457/AP.html

Please don't take any chance. The odds of this milk being in your household is high.


An Apple A Day Worse Than 30 Cigarettes (Latest Research)

Latest research shows certain "health foods" such as apples, salads and cherries actually cause heart attacks, diabetes and high blood pressure.

I was skeptical until I saw the real reason why.

It's a discovery by someone who spent more than 75 years treating patients...

And was branded as a medical genius of our times.

He actually uncovered the root cause of diseases, and here's how you can reverse most of the common (and scary) illnesses naturally in just a few days.

It'll blow your mind.

Reverse Common Illnesses Naturally Today

CYREN

ABOUT CYREN

CYREN is the global leader in information security solutions for protecting web, email, and mobile transactions. Our GlobalView Security Lab continuously innovates our cloud-based threat detection and proactive data analytics to provide comprehensive security solutions for businesses of all sizes. Our award-winning, patented technologies and global security platform increase the value and profitability of our partners' solutions as CYREN email, web, and antivirus capabilities protect over 550 million end users in 190 countries.

www.CYREN.com