proofpoint

Proofpoint Threat Report

October 2014

The Proofpoint Threat Report explores threats, trends, and transformations that we see within our customer base and in the wider security marketplace.

Threat Models

Abandoned Subdomains Pose a Security Risk for Businesses

Many companies set up subdomains for use with external services, but then forget to disable them when they stop using those services, thus creating a loophole for attackers to exploit.

Because many service providers don't properly validate the ownership of subdomains pointed at their servers, perpetrators can set up new accounts and abuse forgotten subdomains by claiming them as their own.

Removing or updating DNS entries for subdomains that are no longer actively used would appear to be standard procedure, but according to researchers from Detectify, a Stockholm-based provider of website security scanning services, this type of an oversight is actually quite widespread among companies.

Seventeen service providers were identified by Detectify researchers as not handling subdomain ownership verification properly. In many cases, these are high-profile domains. At least 200 organizations are currently affected, according to the researchers.

The risk to website owners depends on what can be done on a third-party service once a domain is pointed to it. If the service allows users to set up Web pages or Web redirects, attackers can exploit the situation to launch credible phishing attacks by creating rogue copies of the main website.

According to Detectify, some of the subdomains exposed to this form of hijacking belonged to various types of organizations, including government agencies, health service providers, insurance companies, and banks.

The security firm created an online tool (https://redoctober.detectify.com/) that can help organizations check their subdomains for vulnerability to this attack. Note that the tool first requires users to prove they have control over the domains to be scanned.

Hackers Target ATMs in Russia, Eastern Europe

Not only are cybercriminals targeting the computer systems of big banks, but they're also firing at their ATM machines, especially in Eastern Europe and Russia.

Researchers for Kaspersky Lab, a security company, and INTERPOL, the world's largest international police organization, say they have discovered malicious software allowing criminals to empty cash machines. The company said that at the request of a financial institution it began a forensic examination into the hack of multiple ATMs in Eastern Europe and Russia. (The institution remained nameless.)

At the time of the investigation, around March of this year, the malware was active on more than 50 ATMs at banking institutions in Eastern Europe and Russia. According to Kaspersky, the malware has spread to the US, Israel, Malaysia, France, India, and China. As ATMs are not connected to the Internet, it may not be possible to register attacks unless the victimized banks report them.

Video footage obtained from security cameras at infected ATMs shows that the hacks occur at night, and only on Sundays and Mondays. Furthermore, the malware only accepts commands at specific times on Sunday and Monday nights.

The criminals insert a bootable computer disk loaded with malicious software into the system. The ATM is then rebooted, at which point the software is uploaded to the ATM's system. Once the ATM is rebooted a second time, the criminals enter a unique combination of digits (every time) on the ATM's keyboard. Another set of numbers is entered after a phone call is made by the hacker (on-site) to an operator to receive further instructions.

Four minutes later, the ATM starts dispensing cash.

Mr. Kaspersky said his company is now assisting Russian police, and INTERPOL has alerted the affected member countries. Investigations are ongoing.

Threat News

How One Criminal Hacker Group Stole Credentials for 800,000 Bank Accounts

A new report from Proofpoint shows the increasing sophistication of cybercrime infrastructure. Proofpoint reports that one Russian-speaking criminal organization employed third-party services, used technology and services to promote the efficacy of adjusting to business security challenges, and even created alternate revenue streams for itself in order to commit the theft.

To begin the process, the attackers purchased lists of stolen administrator logins for WordPress sites. They then uploaded malware to those sites.

Click here for the next disturbing steps in the process: http://www.darkreading.com/cloud/how-one-criminal-hacker-group-stole-credentials-for-800000-bank-accounts/d/d-id/1316484.

Microsoft Windows Zero-Day Vulnerability (CVE-2014-4114) Used by Russian Espionage Group "SandWorm"

A zero-day vulnerability impacting all supported versions of Microsoft Windows and Windows Server 2008 and 2012 has been discovered and revealed by iSIGHT Partners, in close collaboration with Microsoft. A patch was made available for this vulnerability on Tuesday, October 14.

Whether the SandWorm team is working on behalf of the Russian government or attempting to misdirect investigators by appearing to do so, its behavior does appear to be connected to some "professional government or nation-state mission," said Philip Lieberman, president of Lieberman Software. Nation-states "only use their highest value assets against high-value targets."

If exploited, the flaw would let attackers remotely execute code on target systems.

Known targets include campaigns against: http://www.tripwire.com/state-of-security/incident-detection/microsoft-windows-zero-day-exploit-sandworm-used-in-cyber-espionage-cve-2014-4114/.

Financial Services Rank Cyberattacks Top Industry Worry

A recent report published by the Depository Trust & Clearing Corporation for the third quarter of 2014 found that 84% of financial firms ranked cyber risk as

one of their top five concerns, up from 59% in the first quarter of this year. Immediately following in the top five are:

- Impact of New Regulations (64%)
- Geopolitical Risk (62%)
- Sudden Dislocation in Financial Markets (43%)
- Disruption/Failure of a Key Market Participant (32%)

Note that some 76% of financial firms say that over the past year, they have added more resources for detection and mitigation of systemic risks.

Read the article in its entirety: http://www.darkreading.com/attacks-breaches/financial-services-ranks-cyberattacks-top-industry-worry/d/d-id/1316917?

Threat Insight Blog

Here we highlight interesting posts from Proofpoint's threat blog, *Threat Insight*. Subscribe to *Threat Insight* and join the conversation at http://www.proofpoint.com/threatinsight.

Calendar Spam Invites Trouble

Surges of old but familiar phishing and spam templates re-emerge every now and then. Techniques that we would expect to be too old to remain effective against modern filters are oftentimes resurrected. A recent spike of calendar spam typifies this situation.

This spam variant can still be effective because many filters do not consistently block calendar invites (*.ics). Also, routing from legitimate domains makes the messages more likely to evade sender-reputation filters.

Have a look at an example of calendar spam detected during the recent spike. http://www.proofpoint.com/threatinsight/posts/calendar-spam-invites-trouble.php

Dyreza Takes Stock

The banking malware called "Dyreza" or "Dyre" uses a man-in-the-middle attack that lets the hacker intercept unencrypted Web traffic while users mistakenly believe the connection they have with their online banking site is secure.

This malware has been implicated recently in multiple large-scale phishing campaigns and is expanding its reach to target users of cloud services, such as Salesforce. Dyreza uses a technique called "browser hooking" to view unencrypted Web traffic. The operation involves compromising a computer,

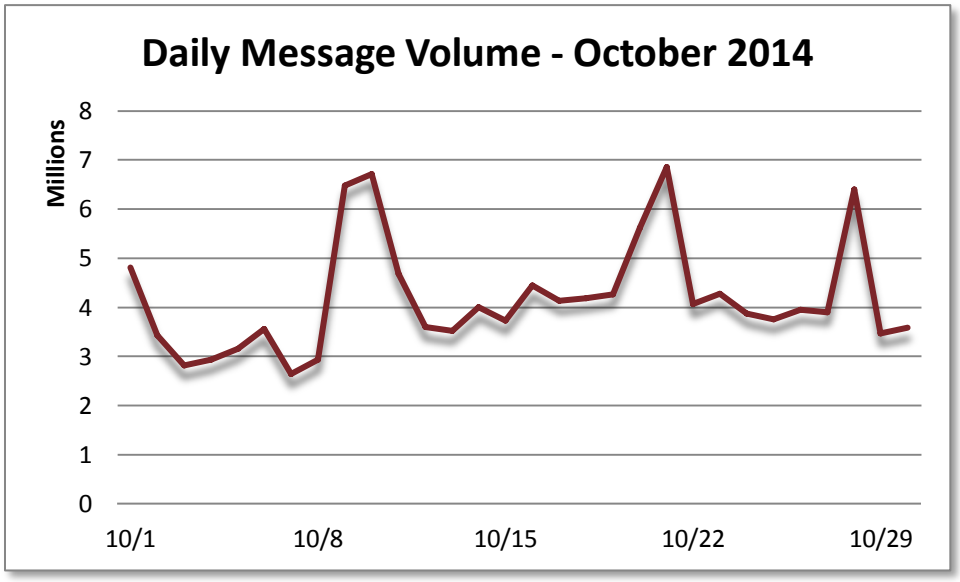
capturing unencrypted traffic, and then stepping in when a user tries to make a secure SSL (Secure Sockets Layer) connection with a website.

Dyreza has undergone a few changes recently and Proofpoint security researchers have been right there to analyze them. The new features are highlighted here: http://www.proofpoint.com/threatinsight/posts/dyreza-takes-stock.php

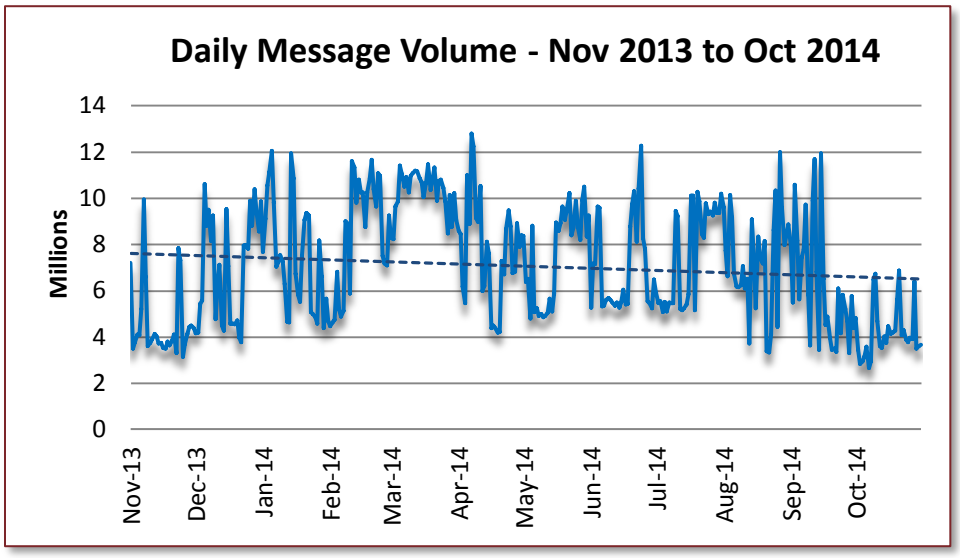
Threat Trends

Spam Volume Trends

Proofpoint tracks spam volumes via a system of honeypots. The volumes historically track with that of our customer base. October's daily spam volume was erratic, with moderate highs and lows through the very end of the month. Beginning with roughly 5 million and a gradual dip to 3 million, the start of the second week saw a dramatic shift to well over 6 million and then dipped to under 4 million by midweek. A gradual increase to the highest point of the month, 7 million, occurred at the close of the third week. The fourth week leveled off at 4 million. A sudden spike to just above 6 million nearly capped the month, before ending in another decline to a bit over 3 million.



By comparison, September-over-October demonstrated the most dramatic decrease in the volume of spam (32.38%) since November of last year (38.17%). The year-over-year spam tally decreased 43.10% in volume.



Spam Sources by Country

In an unprecedented move, China captured the top position in October. The EU slipped to second by a small margin for the first time since March of 2013. At that time, the EU placed third. Russia reentered the mix for the first time since August of 2014 to steal third, while Vietnam and the USA captured fourth and fifth, respectively.

The following table shows the top five spam-sending continents and countries for the last six months.

		May '14	Jun '14	Jul '14	Aug '14	Sep '14	Oct '14
Rank	1st	EU	EU	EU	EU	EU	China
	2nd	US	Vietnam	US	US	Vietnam	EU
	3rd	Argentina	US	China	Argentina	China	Russia
	4th	Russia	China	Argentina	Russia	Argentina	Vietnam
	5th	China	Russia	Russia	China	Korea	USA

The table below details the percentage of total spam volume for the September and October 2014 rankings noted above. The calculation for the EU is based on the inclusion of all member states, thereby producing a better representation of its volume. At 18.82%, China generated the majority of the world's spam. The remaining four countries in the top five slots were collectively responsible for 33.61%—nearly double the output of China.

September 2014			October 2014		
1	EU	24.99%	**1**	China	18.82%
2	Vietnam	13.36%	**2**	EU	15.61%
3	China	4.51%	**3**	Russia	9.25%
4	Argentina	3.68%	**4**	Vietnam	5.10%
5	Korea	3.66%	**5**	US	3.65%

For additional insights visit us at
www.proofpoint.com/threatinsight

proofpoint

Proofpoint, Inc.
892 Ross Drive, Sunnyvale, CA 94089
Tel: +1 408 517 4710
www.proofpoint.com