proofpoint

Proofpoint Threat Report

July 2015

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

Threat Models

It's Not Personal, It's Business: Malware Return on Investment and the Return of Malicious Macros

The return of malicious macros as an exploit technique in email-borne threats, via ever-evolving campaigns, begs the question: how is it that such an *outdated* technique is now an integral part of far-reaching malware campaigns?

Fundamentally, organized cybercrime is a business and therefore, technology is chosen for its ability to generate revenue. When technology and user behavior change, and people adapt defensive measures to new threats, likewise do bad actors adjust attack techniques in order to orchestrate a successful campaign.

But sometimes, just sometimes, defenses falter, in that they lose sight of outdated threats; of course, the return of malicious macros positions one to carefully observe and understand the operatives behind these adaptations (campaign variations). Such a detailed examination is both business case study and technical analysis.

Proofpoint's new report, *The Cybercrime Economics of Malicious Macros* (https://www.proofpoint.com/us/id/PPWEB-Malicious-Macros) takes a good look at both the technical and business aspects of malicious macros; thus, by delving into the minds of the threat actors, it provides valuable behavioral insight.

At the end of the day, if technical innovation and business value go hand in glove, then the inevitable result is return on investment. In the case of malware, such a formula can lead to a groundbreaking trend.

Most importantly, Proofpoint's research paper enables better defense of organizations against the aforementioned threat, and future advanced threats.

See also: https://www.proofpoint.com/us/threat-insight/post/Its-Not-Personal-Its-Business.

Not-So-Innocents Abroad: Dridex Actor Shifts Focus to Europe

The malicious macro campaigns of late continue to grow with vitality and dynamism as threat actors adjust techniques, payloads, and targets. As new innovations come and go, some actors naturally persevere. One such actor is behind Dridex Botnet No. 120.

Proofpoint researchers have been following this actor for quite some time. Recently, the perpetrator was detected directing an *OLE/MIME* formatted attack toward recipients in Europe. Most interesting is the fact that "this technique causes the attachment to appear as a normal .doc file to the end user while resisting analysis by automated tools that do not include the ability to read the OLE content." A campaign such as this, targeting Polish users, occurred on 10 June of this year.

Ultimately, the labyrinth of delivery techniques underscores the commitment of threat actors to "adapt and evade" while all the time relying on successful manipulation of the end user.

For the particulars, read on: https://www.proofpoint.com/us/threat-insight/post/not-so-innocents-abroad-dridex-actor-shifts-focus-to-europe.

Threat News

Data Breach Investigation Report—the Missing Section: Phishing

Phishing is a powerhouse cyber threat. In fact, of the 2,122 breaches disclosed in the *Data Breach Investigation Report* this year, 463, or roughly 25%, were classified as "phishing."

This close study reveals interesting facts:

- Phishing is, for the most part, targeted.
  Of the 1,391 incidents involving phishing, 805 employed malware. Of the 805, 391 (57%) were delivered via emailed links, and 319 (46.5%), via attachment.
  - *Bear in mind that some emails had both flavors.*
- Roughly 25% (351) of the 1,391 incidents involved hacking (mainly via backdoors).
- The main objective is to acquire secret, or confidential, information. This attribute is markedly the most compromised.
- In the long, long line of events, it is the victims' *assets* that ultimately suffer.

Consequently, and most importantly, it should be a given that detection, or "discovery," is synonymous with anti-virus solutions.

Read on and view a host of telling pictorial enumerations: https://securityblog.verizonenterprise.com/?p=7111.

Finnish Teen Convicted of More Than 50,000 Computer Hacks

And the verdict is in: Julius Kivimaki is found guilty of 50,700 "instances of aggravated computer break-ins."

Mr. Kivimaki was accused of perpetrating high-profile computer crimes over a time period of two years before his arrest in September 2013. Court records illustrate that Harvard University and MIT were among his victims.

The stings were, quite simply, composed of hijacking email, blocking traffic to websites, and stealing credit card details.

Mr. Kivimaki was notably ingenious: he was able to compromise more than 50,000 computer servers by taking advantage of an imperfection in Adobe's ColdFusion software to carry out his attacks. This exploitation ultimately led to the decay of tens of thousands of the computers because he was able to install backdoors, allowing him access to stored information.

Among other violations, he was formally charged with adding malware to approximately 1,400 of the servers, which enabled him to create a botnet. This botnet was ultimately used to carry out denial-of-service (DoS) attacks (http://searchsoftwarequality.techtarget.com/definition/denial-of-service) on other systems.

Such is a portrait of a cybercriminal.

Read further: http://www.bbc.com/news/technology-33442419.

Cyberespionage Group Pawn Storm Uses Exploit for Unpatched Java Flaw

A band of hackers, Pawn Storm, thought to operate out of Russia, has been targeting U.S. military, embassy, and defense contractor personnel for the past several years, and most recently, the White House and the North Atlantic Treaty Organization (NATO). Just this month, researchers spotted the sophisticated gang employing a *zero-day* vulnerability in Java. This flaw appears to be among those recently fixed by Oracle.

Recent targets received spear-phishing emails that contained links to Web pages hosting the exploit. The (malicious) links lead to supposed articles about geopolitical events.

The newly discovered exploit affects the latest version of the Java Runtime Environment: Java 8 Update 45. It was released in April of this year. Oddly enough, the exploit does not affect the older versions, namely Java 7 and Java 6, even though these versions no longer receive public security patches from Oracle.

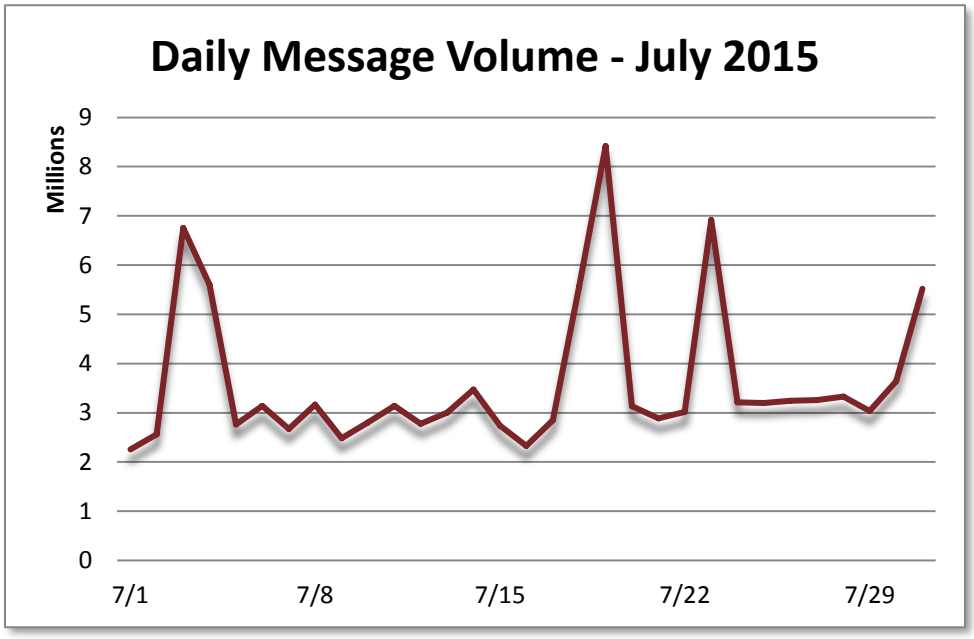
This is the first Java zero day made known in nearly two years.

See also https://en.wikipedia.org/wiki/Zero-day_%28computing%29 and continue reading: http://www.csoonline.com/article/2947461/data-protection/cyberespionage-group-pawn-storm-uses-exploit-for-unpatched-java-flaw.html.

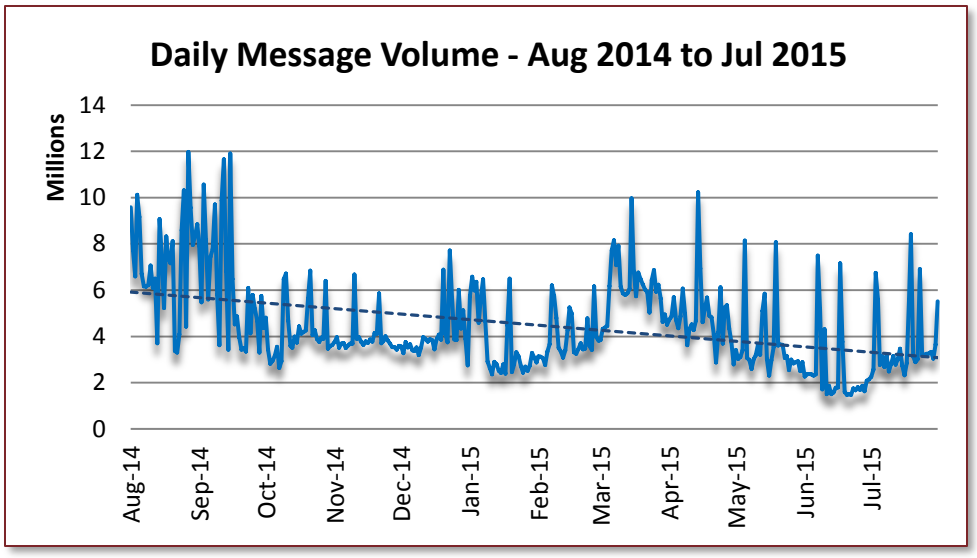
Threat Trends

Spam Volume Trends

Proofpoint tracks spam volumes via a system of honeypots. The volumes historically track with that of our customer base. July's daily spam volume was disorderedly. It began above 2 million at the very beginning of the first week and then with a surge, hit nearly 7 million. A rather abrupt decline to below 3 million followed and distinguished the midpoint of the first week. From that time forward, there was choppy movement around approximately 3 million. This trend lasted until the start of the third week. It was then that the most intense spike manifested itself to well over 8 million. Soon enough, another plunge to 3 million would occur. At the start of the fourth week, there was momentary stability. This calm would precipitate itself into another grand spike to 7 million. The spike would be short-lived and fall to the well-established position of 3 million. One final burst to nearly 6 million brought the month to a close.



By comparison, July-over-June reflected quite the increase in the volume of spam (46.92%). The year-over-year spam tally decreased by 51.53%.



Spam Sources by Region and Country

The EU won the gold yet again, and the U.S. nabbed second comfortably. China retained third and looked in fine form. Russia reigned supreme over fourth place, and Vietnam seized fifth to re-emerge in the Top 5 for the first time since February of this year. (Vietnam placed third at that time.)

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

		Feb '15	Mar '15	Apr '15	May '15	Jun '15	Jul '15
Rank	1st	EU	EU	EU	EU	EU	EU
	2nd	US	US	US	US	US	US
	3rd	Vietnam	Russia	China	China	China	China
	4th	Argentina	India	India	Russia	Russia	Russia
	5th	Russia	China	–	Indonesia	Argentina	Vietnam

The table below details the percentage of total spam volume for the June 2015 and July 2015 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 25.70%, the EU generated the majority of the world's spam. The remaining four countries in the top five slots were collectively responsible for 26.43%—slightly above the output of the EU.

June 2015			July 2015		
1	EU	29.15%	**1**	EU	25.70%
2	US	12.11%	**2**	US	11.34%
3	China	4.80%	**3**	China	7.82%
4	Russia	2.52%	**4**	Russia	4.73%
5	Argentina	2.40%	**5**	Vietnam	2.54%

The following table displays the top five spam-sending member states of the European Union (EU) for June 2015 and July 2015, in addition to the percentage of total spam volume for each country.

June 2015			July 2015		
1	Germany	4.71%	**1**	Germany	2.77%
2	Spain	3.48%	**2**	Spain	2.16%
3	Romania	3.10%	**3**	Romania	2.03%
4	Italy	2.67%	**4**	Italy	1.96%
5	Bulgaria	1.65%	**5**	Bulgaria	1.44%

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

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

