proofpoint

Proofpoint Threat Report

June 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

When Threat Intelligence Meets Business Intelligence

The perpetual cycle of adaptation and innovation by cybercriminals, as documented in Proofpoint's *The Human Factor 2015* (https://www.proofpoint.com/us/threat-insight/post/The-Human-Factor-2015), is manifested every day in insidious new techniques concocted by attackers in order to evade detection and ultimately, to infect new systems. The wrongdoers continuously evolve business schemes to better track the success (or lack thereof) of their techniques. The optimization of growth and profitability is of paramount importance to them.

Proofpoint researchers have observed a tracking technique used by certain malicious macro writers. Quite simply, when a user "enables content" for a particular developer's macro, a VBScript, a batch file, and one or two other files are created, depending on which version of Windows the client is running. These files execute in series and download a malware payload, as well as downloading a "statistics image". The "statistics-enabled macro" feature was introduced around February 2015. Take note of its operating condition here:

https://www.proofpoint.com/us/threat-insight/post/When-Threat-Intelligence-Meets-Business-Intelligence.

This tracking approach highlights the extent to which the perpetrators' technical strategies are chosen and driven by business metrics.

More recently, Proofpoint researchers observed a marked change in the statistics feature, namely, the macro loads two images, one when the payload is downloaded, and a second, different image once it can verify that the infection process is complete. An example (and analysis) can be found here: https://www.proofpoint.com/us/threat-insight/post/When-Threat-Intelligence-Meets-Business-Intelligence.

Image-tracking statistics confirm that the attackers have secured a tremendous increase in effectiveness at evading "standard" email defenses. Moreover, their rate of success is greater than 70%, in terms of installing the malware payload and infecting the target client. This is critical threat intelligence for security professionals, as well as important business intelligence for threat actors, who evaluate the success of their campaigns. Even the malicious macro developers benefit from this intelligence as they are eager to demonstrate return on investment and drive future business.

Lessons Learned From the Ramnit Botnet Takedown

The successful takedown of a well-known botnet can be attributed to big data. In February of this year, Europol, together with Microsoft, Symantec, and AnubisNetworks, led the takedown operation of the Ramnit botnet.

"It is not a matter of if you will be breached, but when" has become an adage, the truth of which is recognized by the security community as a whole. It is no longer enough to prevent a breach. Strategies to detect and remediate incidents, as they occur, must be integral parts of the overall process.

The harsh reality is that in most cases, organizations are oblivious of what is happening, namely, that a data breach was suffered or that they are being assaulted by hackers. Reputational harm and lost revenue are the usual byproducts of lack of planning—the lack of fundamental threat intelligence.

Read the particulars and pay heed to a few key takeaways: http://www.darkreading.com/endpoint/lessons-learned-from-the-ramnit-botnet-takedown/a/d-id/1320861.

Threat News

Japan Pension Service Hack Used Classic Attack Method

Japan's pension system has been hacked and more than a million cases of personal data (combinations of names, identification numbers, birth dates and addresses) have been leaked as staff computers were improperly accessed by an external email virus.

The hackers are believed to have used the classic "targeted email attack" maneuver.

Japan Pension Service (JPS) reported the attacks to the Metropolitan Police Department on May 19th. The origin of the blitz remains undisclosed but according to reputable Japanese mass media, the Backdoor.Emdivi Trojan horse turned out to be the culprit. Interestingly, the Trojan has been linked to previous compromises of critical infrastructure since the end of 2014. Given its sophistication, the cyberweapon has often escaped notice. Click here for more information: http://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=27975.

The police investigation is ongoing.

The data were leaked when agency employees opened an infected attachment to an email. The attachment masqueraded as a Ministry of Health document.

Here's the breakdown of the cases, numbering in all some 1.25 million:

- Approximately 52,000 involved the theft of pension IDs, names, birth dates and addresses.
- Another 1.17 million involved the leak of pension IDs, names and birth dates.
- In the remaining 31,000 cases, only pension IDs and names were stolen.

Read additional key particulars here: http://www.japantimes.co.jp/news/2015/06/02/national/social-issues/japan-pension-service-hack-used-classic-attack-method/#.VXhyWkZSUXh.

X-Rays Behaving Badly: Devices Give Malware Foothold on Hospital Networks

TrapX, a security firm, warns that medical devices, including radiological systems, are merely a means to an end for malicious attackers.

According to a report from TrapX, *serious* breaches of hospital networks are assuredly more common than not, "as compromised medical devices often hide the telltale signs of malware infection and data theft."

The TrapX report claims that perpetrators are using unprotected medical devices, including radiological systems, to secure and maintain a firm position on healthcare networks and therefore avoiding detection by security software and IT staff.

The report combines details from TrapX customer engagements with healthcare firms and company-sponsored analysis of common medical devices.

TrapX discloses that medical devices, particularly PACS systems (picture archiving and communication [radiological imaging technology]) are nearly invisible to security systems and set the stage for malware infections to move furtively on hospital networks, and for threat actors to launch attacks on valuable IT assets.

Read the full report: https://securityledger.com/wp-content/uploads/2015/06/AOA_MEDJACK_LAYOUT_6-0_6-3-2015-1.pdf.

The report concludes that "the medical devices themselves create a far broader exposure to the healthcare institutions than the standard information technology assets."

The revelation is most perturbing: TrapX scientists believe that "a large majority of hospitals are currently infected with malware that has remained undetected for months, and in many cases, years."

Read more thought-provoking facts resulting from exhaustive researches of medical devices: https://securityledger.com/2015/06/x-rays-behaving-badly-devices-give-malware-foothold-on-hospital-networks/.

White House Calls for Encryption by Default on Federal Websites by Late 2016

The U.S. government has mandated the use of the HTTPS (HyperText Transport Protocol Secure) protocol across all publicly accessible federal websites and Web services by the end of next year.

The HTTPS-only directive is unprecedented.

Simply stated, deploying HTTPS will encrypt user authentication sessions in government websites. The protocol offers the most effective privacy protection available for public Web connections currently available with today's Internet technology.

Read the government missive: https://https.cio.gov/.

At present, a mere 28% of federal agencies run encrypted. The HTTPS websites include whitehouse.gov, cia.gov, nsa.gov, and omb.gov. Curiously enough, dhs.gov is as yet not HTTPS-enabled. See also https://pulse.cio.gov/https/domains/.

Moreover, HTTPS only guarantees the soundness of the connection between two systems. It does not guarantee the integrity of the systems themselves. HTTPS is not designed to protect a Web server from being hacked or compromised. It is also not designed to prevent the Web service from exposing user information during its normal operation.

Read on: http://www.darkreading.com/application-security/white-house-calls-for-encryption-by-default-on-federal-websites-by-late-2016/d/d-id/1320789?.

World's Biggest Data Breaches

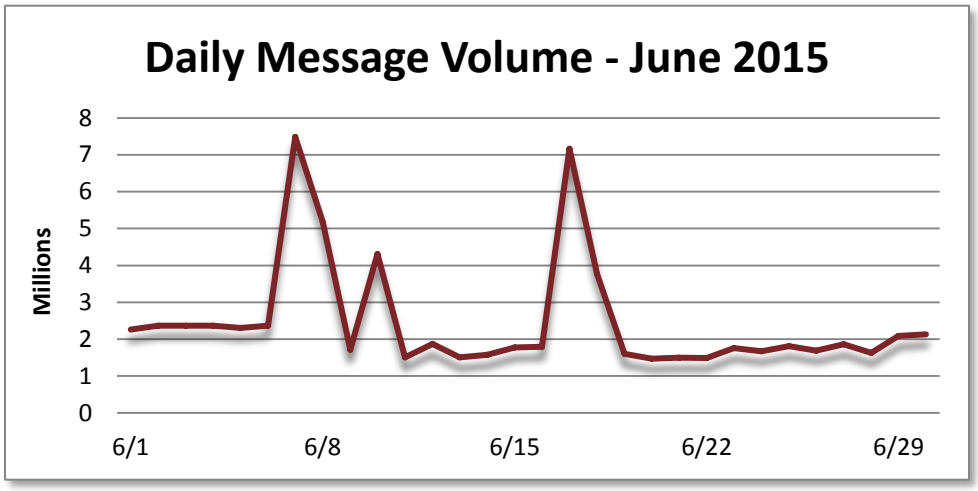
View information about an eclectic collection of data breaches: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/.

The infographic specifically discloses selected losses of more than 30,000 records.

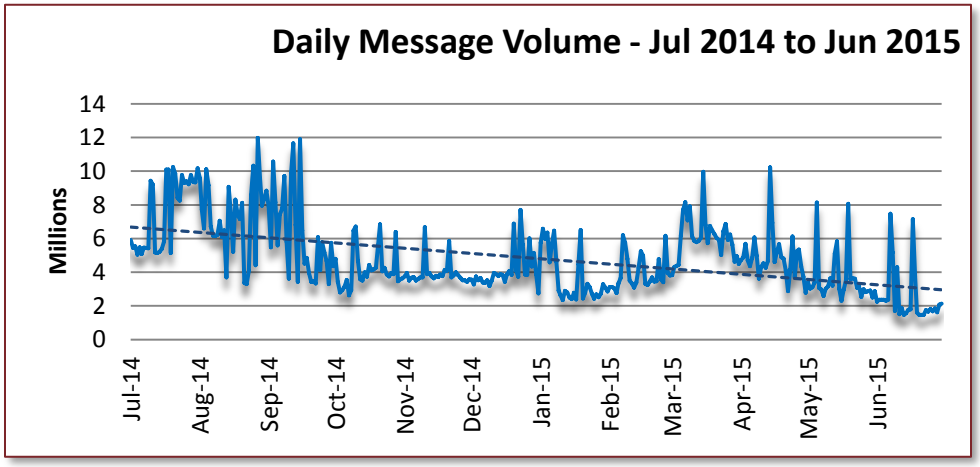
Threat Trends

Spam Volume Trends

Proofpoint tracks spam volumes via a system of honeypots. The volumes historically track with that of our customer base. June's daily spam volume was turbulent. It began above 2 million for a good part of the first week and then skyrocketed to well over 7 million. A rather abrupt decline to below 2 million highlighted the start of the second week. An instantaneous leap to above 4 million followed in addition to another dramatic decline to below 2 million. Ever-so-slight fluctuations just below 2 million led to the next striking rise to over 7 million at the start of the third week. That rise brought yet another fall. For the most part, the rest of the month stabilized at below 2 million. The very end of the month barely capped 2 million.



By comparison, June-over-May reflected a slight decrease in the volume of spam (30.33%). The year-over-year spam tally decreased by 64.33%.



Spam Sources by Region and Country

The EU was at the top of the heap once again, while the U.S. grabbed second for the sixth month in a row. China comfortably won possession of third, while Russia retained fourth, and Argentina re-emerged to capture fifth.

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

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

The table below details the percentage of total spam volume for the May 2015 and June 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 29.15%, the EU generated the majority of the world's spam. The remaining four countries in the top five slots were collectively responsible for 21.83%—well below the output of the EU.

May 2015			June 2015		
1	EU	23.59%	**1**	EU	29.15%
2	US	11.98%	**2**	US	12.11%
3	China	9.11%	**3**	China	4.80%
4	Russia	4.27%	**4**	Russia	2.52%
5	Indonesia	2.09%	**5**	Argentina	2.40%

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

May 2015			June 2015		
1	Germany	2.27%	**1**	Germany	4.71%
2	Spain	2.04%	**2**	Spain	3.48%
3	Italy	1.92%	**3**	Romania	3.10%
4	Netherlands	1.87%	**4**	Italy	2.67%
5	France	1.42%	**5**	Bulgaria	1.65%

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

