proofpoint

Proofpoint Threat Report

May 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

Best Practices in Incident Response Automation

In early 2015, Proofpoint researchers looked at the key phases of the process of incident response. They particularly highlighted the importance of digital forensics and incident response (DFIR) as an integral part of the current detection and prevention toolbox. On the authority of Proofpoint researchers, "automation in incident response is a natural evolution of automation in security." It is one of the keys to effective DFIR.

Automation can mean anything from API calls for information gathering to automated network containment and account lockout.

Consider the following use cases and best practices for applying automation to an incident response process. Naturally, effectiveness and efficiency are the ultimate goals.

No-Argument Automation

Automation ought to start with understanding exactly what incident responders do to carry out their mission successfully. The explanation could be as simple as looking at the source and destination of an attack. Is the attack:

- Targeting a key department, such as finance?
- Aimed at a source code server?
- Victimizing the CFO/executive staff?
- Is the targeted system infected?
- Does the attack originate from a country unrelated to one's typical business associations?
- Is the attack related to a known command and control server?
- Is the attack the result of an IP range on an intelligence list?
- Is the attack using malware that is detected by a few or the majority of the antivirus tools?

Manually compiling and integrating security alert source data, and organizing data sets, can be a time-consuming and tedious undertaking for a single incident. And as we all know, to err is human. Thus, this process can be subjective, and prone to error.

The implementation of an automation system at the front end of the incident response process is a key marker for efficient and effective response.

Automation on Existing and Generated Data

Incident responders must analyze and then recommend preventive measures. But before they can make recommendations, their collected data sets are often analyzed and processed more thoroughly. See https://www.proofpoint.com/us/threat-insight/post/Best-Practices-in-Incident-Response-Automation.

An ideal resolution integrates a file of documents containing detailed information about an incident. This information would offer a situational awareness and, consequently, enable smart priority-setting.

For the two key best practices in this phase, click here: https://www.proofpoint.com/us/threat-insight/post/Best-Practices-in-Incident-Response-Automation.

And for supplementary protective actions and authoritative advice, read on: https://www.proofpoint.com/us/threat-insight/post/Best-Practices-in-Incident-Response-Automation.

GPU Malware Can Also Affect Windows PCs, Possibly Macs

A team of developers recently created a Linux rootkit that runs on graphics cards. They've also released a new proof-of-concept malware program that executes identically on Windows. A Mac OS X implementation is under development.

The developers' innovations and research intend to raise awareness that malware can infect GPUs (graphics processor unit).

According to the developers, the problem lies in existing security tools, which lack the means to scan the random access memory (RAM) used by GPUs.

The new Windows malware (for the purpose of demonstrating) is called "WIN_JELLY" and acts as a Remote Access Tool (RAT), or trojan.

RATs afford attackers far-reaching control over compromised computers and have been used in many targeted attacks in recent years.

Continue reading: http://www.itworld.com/article/2921095/gpu-malware-can-also-affect-windows-pcs-possibly-macs.html.

Threat News

Europe's Largest Airline Falls Prey to $5 Million Cyber Theft

Ryanair has been targeted in a $5 million international bank transfer scam.

The Irish airline recently investigated a fraudulent electronic funds transfer via a Chinese bank.

After working with the proper authorities and its banks, the airline understands that the funds have been frozen, and expects these funds to be repaid shortly.

Although the sum stolen was relatively small in corporate terms, the incident underscores the threat posed by cybercrime to banking and financial systems.

Guy Haselmann of Scotiabank describes cyber attacks as the "new Cold War." In his piece entitled *The Invisible Army*, he refers to President Obama's recent State of the Union address and the president's declaration of foreign cyber threats as a "national emergency."

Given Mr. Haselmann's vivid accounts and explicit language, the new Cold War may indeed be one of cyber warfare.

Ryanair has taken steps to prevent this type of transfer from happening again.

See the particulars: http://www.zerohedge.com/news/2015-04-29/europe%E2%80%99s-largest-airline-falls-prey-5-million-cyber-theft.

Anonymous Accused of Running a Botnet Using Thousands of Hacked Home Routers

Feeble security has paved the way for various groups of hackers, likely including Anonymous, to hijack hundreds of thousands of home and office Internet routers, as claimed by a new report by Incapsula, a cybersecurity firm.

The hackers' *modus operandi* is to target routers configured with factory-default usernames and passwords. This is an "inexplicably negligent" mistake made by Internet service providers and users alike, Incapsula said.

The hijacked routers, mostly found in the U.S., Thailand, and Brazil, were infected with different kinds of corrupting malware. The routers were ultimately used to build a botnet that began attacks against innumerable targets in late December 2014.

(A botnet is a network of computers infected by a program that communicates with its creator to send unsolicited e-mails, attack websites etc.)

Continue reading about this ubiquitous, furtive behavior, and the lack of security through gross negligence: http://www.dailydot.com/politics/botnet-incapsula-research-report-default/.

In a similar vein, a few months ago, Proofpoint detected a four-week spam campaign sent to a small number of organizations. It primarily targeted Brazilian Internet users. The e-mails were created to look like they were sent via Brazil's largest Internet service provider, alerting recipients about an unpaid bill. The missives were, in fact, a stratagem to secure a click of a link, designed to trigger a hack of that same ISP's router equipment.

Needless to say, the primary motivation was to harvest online banking credentials and other sensitive data from victims.

Read Proofpoint's noteworthy research, as well as informed comments by one of its senior leaders, Kevin Epstein, here: http://krebsonsecurity.com/2015/02/spam-uses-default-passwords-to-hack-routers/.

https://www.proofpoint.com/us/threat-insight/post/Phish-Pharm.

Cost of a Data Breach Climbs to an Average of $3.8M

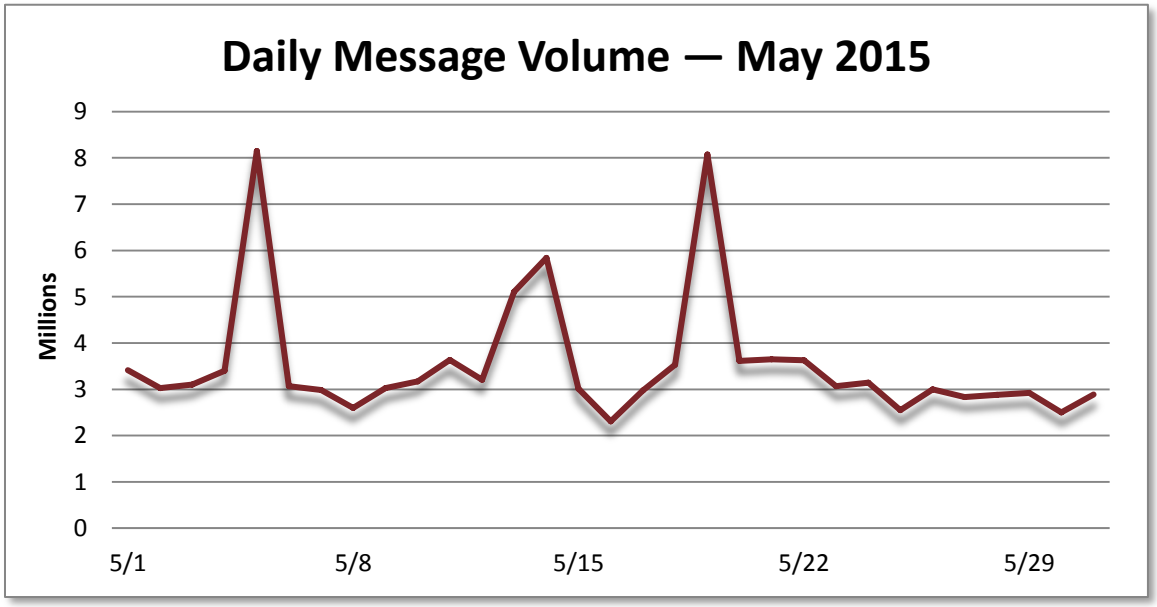
Criminal, damaging cyberattacks are becoming more frequent and widespread. A Ponemon Institute study finds that associated costs are rising partly because of that fact. The total average cost of a data breach for companies worldwide has increased to $3.8 million, a leap from $3.5 million a year ago. It is noteworthy that a higher frequency of malicious or criminal cyber activity has prevailed.

Ponemon's annual *Cost of a Data Breach* study follows a year of high-profile, powerful attacks. The victims include JPMorgan Chase, Sony, and Target, to name a few. The report concludes that malicious or criminal breaches are becoming more frequent and more costly, among other disquieting news. For the in-depth study, read on: http://ww2.cfo.com/data-security/2015/06/data-breach-costs-climb-average-3-8m/.

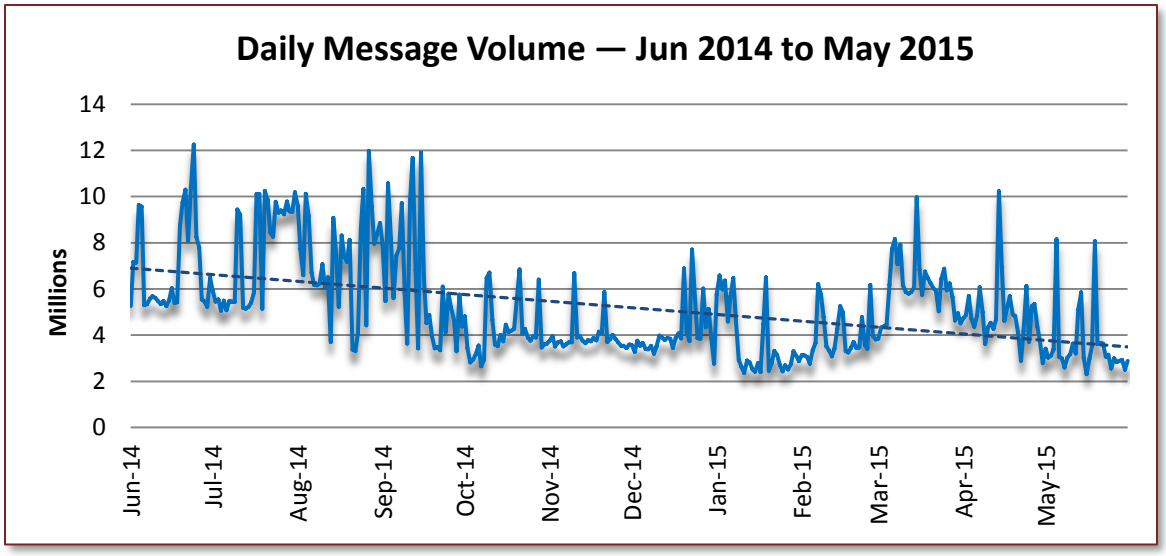
Threat Trends

Spam Volume Trends

Proofpoint tracks spam volumes via a system of honeypots. The volumes historically track with that of our customer base. May's daily spam volume swung like a pendulum. It clearly began above 3 million and almost immediately catapulted to approximately 8 million by mid-week. Thereafter, the volume fell to roughly 3 million. Week two had all the earmarks of week one and then some. A low of 2.5 million and a high of nearly 6 million underscored the week. The third week showcased yet another sudden burst of activity to 8 million. Thereafter, volumes leveled off and the month closed at roughly 3 million—.



By comparison, May-over-April reflected a modest decrease in the volume of spam (27.16%). The year-over-year spam tally decreased by 52.66%.



Spam Sources by Region and Country

The EU reigned for the sixth consecutive month while the U.S. secured second for the fifth month in a row. China seized third again, while Russia slipped into fourth, and Indonesia made its grand début.

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

		Dec '14	Jan '14	Feb '15	Mar '15	Apr '15	May '15
Rank	1st	EU	EU	EU	EU	EU	EU
	2nd	China	US	US	US	US	US
	3rd	US	Vietnam	Vietnam	Russia	China	China
	4th	Russia	Argentina	Argentina	India	India	Russia
	5th	Vietnam	China	Russia	China	TBD	Indonesia

The table below details the percentage of total spam volume for the April 2015 and May 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 23.59%, the EU generated the majority of the world's spam. The remaining four countries in the top five slots were collectively responsible for 27.45%—above the output of the EU.

April 2015			May 2015		
1	EU	14.45%	**1**	EU	23.59%
2	US	10.45%	**2**	US	11.98%
3	China	6.73%	**3**	China	9.11%
4	India	1.16%	**4**	Russia	4.27%
5	TBD	TBD	**5**	Indonesia	2.09%

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

April 2015			May 2015		
1	Italy	1.09%	**1**	Germany	2.27%
2	Netherlands	0.84%	**2**	Spain	2.04%
3	UK	0.49%	**3**	Italy	1.92%
4	Germany	0.44%	**4**	Netherlands	1.87%
5	Czechoslovakia	0.43%	**5**	France	1.42%

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

