Proofpoint Threat Report

September 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

Targeted Attacks: PlugX Infects, Arid Viper Returns

In September, Proofpoint researchers detected and analyzed two highly targeted attacks, both of which demonstrated the continued status of email as the vector-of-choice of threat actors, even for sophisticated attacks. These attacks highlighted the continued evolution of techniques that threat actors use to infect their targets: changing email lures, new “masking” techniques, and convoluted infection chains.

Proofpoint analysis of a new advanced persistent threat (APT) that uses spear-phishing to deliver PlugX to targets in both the Russian military and telco sectors offers a compelling example of this evolution. The key findings from this analysis follow:

- As was demonstrated with Stuxnet, and now this latest APT, there is no strong dividing line between military and private sector when it comes to targeted attack tools and tactics. Although targeted at Russian state entities, this APT also struck Russian-speaking analysts at Western financial institutions. Businesses in the U.S. and Europe are at risk from “collateral

damage" in targeted attacks on state and military entities on the other side of the world and need to take measures to protect themselves.
- Cyberweapons used in one sector are readily repurposed to the other sector, and attacks such as these have become a constant occurrence given the covert nature of digital attacks and easy access to targeting information online.
- Traditional security tools and measures are frequently ineffective in combating these targeted attacks. As a result, private and public entities need to equip themselves with advanced tools that are devised to withstand increasingly sophisticated attacks and attackers.

Read the complete details of the analysis on *Threat Insight* at: https://www.proofpoint.com/us/threat-insight/post/PlugX-in-Russia

One of the major challenges of targeted attacks is that they can disappear from view for extended periods of time, leaving security professionals in the dark regarding their techniques and relevance. In September, Proofpoint researchers documented the return of Operation Arid Viper, an APT that was documented in February and has since seemed dormant. This update to Operation Arid Viper demonstrates that despite its relatively low profile since February, the Arid Viper/Desert Falcons threat remains a risk for organizations in Israel and elsewhere. The recent campaigns exhibit several important updates:

- Use of links instead of attachments
- New lures: still using pornographic video but most recent detections also included lures for auto accident footage
- New executable name: originally reported using "skype.exe" (and variations on "skype"), the recent samples used "chrome.exe"
- New command-and-control domains
- Added encryption for exfiltrated data

The complete analysis of the renewed Operation Arid Viper can be found on *Threat Insight* at: https://www.proofpoint.com/us/threat-insight/post/Operation-Arid-Viper-Slithers-Back-Into-View

Exploit Kits: Too Many Crooks in the Kitchen

As Proofpoint scientists have discussed time and time again, exploit kits are frequently used to deliver malware payloads onto victim systems. A mere click of a malicious link, a visit to a compromised site, or an encounter with malvertising are sample techniques commonly used by threat actors to direct victims to exploit kit (EK) servers.

Recently, Proofpoint researchers detected an infection attempt via malvertising in which the initial infection pulled in the Angler exploit kit. (See https://blogs.sophos.com/2015/07/21/a-closer-look-at-the-angler-exploit-kit/ and note that Angler currently accounts for approximately half of the total EK activity, according to Proofpoint statistics https://threatintel.proofpoint.com/).

See also the onset of the infection chain after the initial redirect and landing on the Angler EK here: https://www.proofpoint.com/us/threat-insight/post/Too-Many-Crooks-in-the-Kitchen.

The end result is an infection chain that is a tangle of malware, while "one payload after another attempts to pile onto the targeted client," as stated by Proofpoint experts.

Interestingly, in spite of the entrance of new, smaller players, such as the Hunter exploit kit (https://www.proofpoint.com/us/threat-insight/post/Hunter-Exploit-Kit-Targets-Brazilian-Banking-Customers), the exploit kit market continues to revolve around and unite with Angler.

Read the full post on *Threat Insight* for complete details of this incident and a look at the changing behavior of exploit kits: https://www.proofpoint.com/us/threat-insight/post/Too-Many-Crooks-in-the-Kitchen.

Malware: Dyreza Campaigners Set Sights on the Fulfillment and Warehousing Industry

The notorious Dyreza (aka Dyre) or "man-in the-browser" (MITB) banking malware is on the prowl again and is "significantly expanding its target set of entities from which to steal credentials," according to Proofpoint researchers.

Initially focused on intercepting end-user bank logins, Dyreza later expanded its horizons to include sites related to job hunting, file hosting, domain registration, website hosting, tax services, and online retail. To add to its assemblage of targets, Dyreza now has targeted many organizations directly involved in warehousing and fulfillment. (See https://www.proofpoint.com/us/threat-insight/post/Dyreza-Campaigners-Sights-On-Fulfillment-Warehousing-Industry).

In a typical campaign, the perpetrators provided an email disguised as a correspondence from a legitimate bank, with the following subject line: "You have received a secure e-mail," instructing the user to read and reply to the secure email by opening its attachment while connected to the Internet.

Upon opening the attachment, the user encounters a fake "secure" Microsoft Office document. In outward appearance, the document is encrypted but in fact, it is not. The user is urged to enable the content to view the document. When the "Enable Content" button is pressed in Microsoft Word, macros embedded in the document are then enabled and a secondary payload is activated. Critical to note is the attackers' request for Internet connectivity in the lure email. "This specific macro, known as Xbagging or Bartallex, downloads the payload from the Internet rather than unpacking it from within an email attachment, a technique used to avoid detection by security programs" said the Proofpoint team.

Read more about this continued evolution of Dyre/Dyreza behavior on *Threat Insight*: https://www.proofpoint.com/us/threat-insight/post/Dyreza-Campaigners-Sights-On-Fulfillment-Warehousing-Industry.

Threat News

More Than 80% of Health-Care IT Leaders Say Their Systems Have Been Compromised

According to the 2015 KPMG (Klynveld, Peat, Marwick, Goerdeler) Health-Care Cybersecurity Survey, the vast majority of health-care organizations have experienced cyberattacks in the last two years.

KPMG's report has revealed that four-fifths of executives at health-care providers and payers report that their information technology has been compromised by cyberattacks. Only half of those IT executives are confident they are adequately prepared to prevent future attacks.

The magnitude of the threat of attack against health-care information has grown exponentially but the incorporation of cybersecurity in the technology and network architecture to secure that information has not always followed.

Ultimately, sensitive patient data is at risk.

The results exhibited that executives believe the greatest vulnerability in data security is *external attackers* (65%), followed by *sharing data with third parties* (48%), *employee breaches* (35%), *wireless computing* (35%), and *inadequate firewalls* (27%). Unsurprisingly, the No. 1 information security concern is *malware infecting systems* (67%).

The survey polled 223 CIOs, CTOs, chief security officers, and chief compliance officers at health-care providers and health plans.

See the survey: http://advisory.kpmg.us/content/dam/kpmg-advisory/PDFs/ManagementConsulting/2015/KPMG-2015-Cyber-Healthcare-Survey.pdf.

For the entire article: http://www.computerworld.com/article/2975988/healthcare-it/more-than-80-of-healthcare-it-leaders-say-their-systems-have-been-compromised.html.

Under DDoS Attack? Look for Something Worse

Distributed Denial of Service (DDoS) attacks are more dangerous than one might think. The damage scope from such attacks goes way beyond the temporary downtime of a corporate web site. Companies report complete disruption to their operations, and in some cases, there has been a loss of sensitive data.

According to a new survey, DDoS attacks can have major financial and data loss implications, in addition to the obvious, massive inconvenience. Kaspersky Lab found that almost one in three DDoS attacks coincides with a network intrusion. The study was comprised of over 5,000 companies.

Evgeny Vigovsky, head of Kaspersky DDoS Protection said, “Those other attacks may or may not originate from the same party, but they can go undetected if IT staff is totally focused on defending against the DDoS.”

Note that the number-one target of DDoS is corporate web sites, followed by customer portals/logins (38%) and then communications services (37%).

Nearly a quarter of attacks result in loss of data, possibly attributed to accompanying attacks. And finally, the incidence of DDoS attacks wanes in comparison with malware, phishing, and network intrusions, according to the survey.

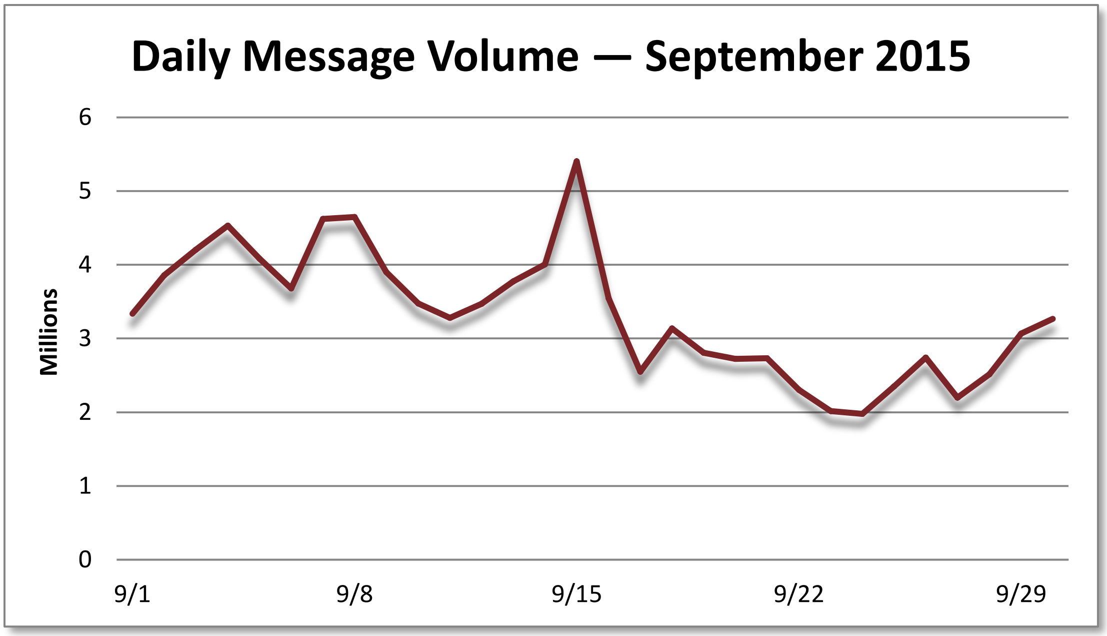
Read the details of the study: http://www.networkworld.com/article/2984648/security/under-ddos-attack-look-for-something-worse.html.

Threat Trends

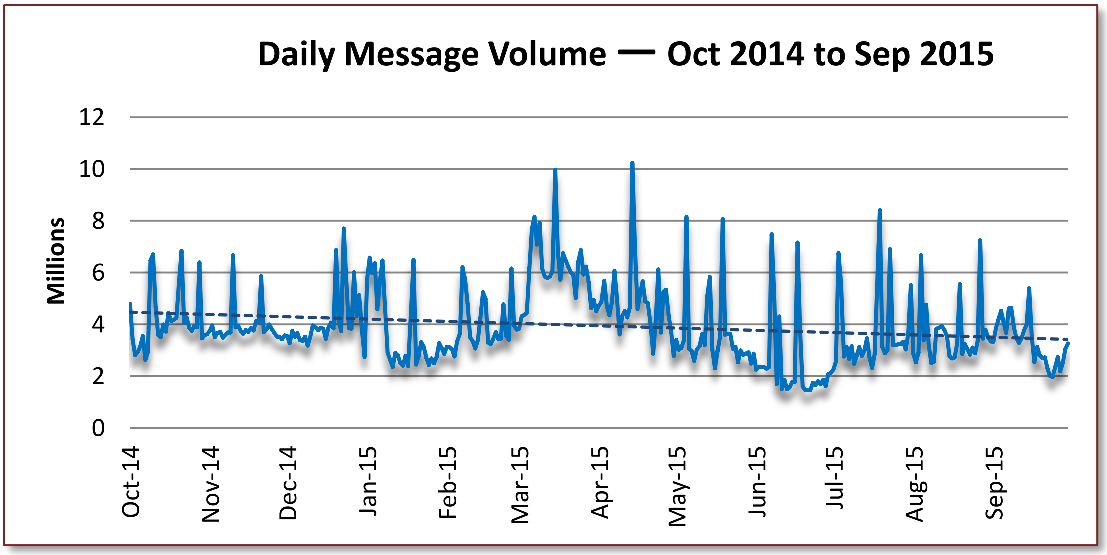
Spam Volume Trends

Proofpoint tracks spam volumes via a system of honeypots. The volumes historically track with that of our customer base. September’s daily spam volume was a hodgepodge of highs and lows. It began with a leap to 4.5 million from 3.3 million and maintained up to the start of the third week, at which point volume spiked at nearly 5.5 million. A swift decline to 2.5 million accentuated the third week. From that point forward, ripples between 2 and 3.25 million characterized the remainder of the month.

The month ended where it began, at roughly 3 million.



By comparison, September-over-August reflected a moderate decrease in the volume of spam (6.07%). The year-over-year spam tally decreased by 45.88%.



Spam Sources by Region and Country

The U.S. dethroned the EU to capture first place and China slid into second to beat out the EU by a hair. The EU settled for third as Russia maneuvered into fourth and Vietnam sank to fifth.

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

		Apr ’15	May ’15	Jun ’15	Jul ’15	Aug ’15	Sep ’15
Rank	1st	EU	EU	EU	EU	EU	U.S.
	2nd	U.S.	U.S.	U.S.	U.S.	U.S.	China
	3rd	China	China	China	China	China	EU
	4th	India	Russia	Russia	Russia	Vietnam	Russia
	5th	–	Indonesia	Argentina	Vietnam	Russia	Vietnam

The table below details the percentage of total spam volume for the August 2015 and September 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 14.62%, the U.S. generated the majority of the world’s spam. The remaining four entities in the top five slots were collectively responsible for 22.32%—well above the output of the U.S.

August 2015			September 2015		
1	EU	22.81%	1	U.S.	14.62%
2	U.S.	10.93%	2	China	7.94%
3	China	6.60%	3	EU	7.56%
4	Vietnam	4.07%	4	Russia	3.45%
5	Russia	3.58%	5	Vietnam	3.37%

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

August 2015			September 2015		
1	Germany	2.13%	1	Germany	1.67%
2	Romania	1.46%	2	U.K.	1.14%
3	Spain	1.37%	3	Romania	1.10%
4	Czech Republic	1.18%	4	France	1.08%
5	Italy	1.18%	5	Italy	0.89%

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