Proofpoint Threat Report

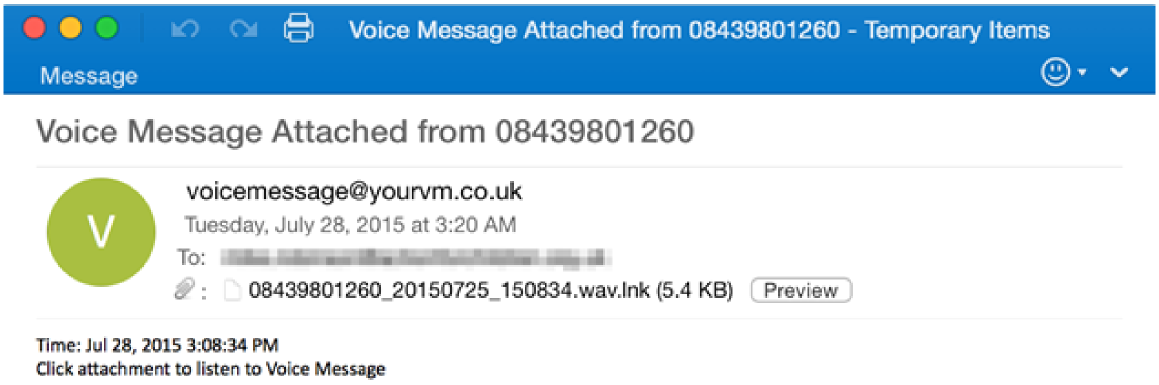
August 2015

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

Threat Models

The Missing .LNK: Dridex Actor Tries New File Format

Since late 2014, a variety of threat actors have been leveraging unsolicited email campaigns that distributed the Dridex banking Trojan using malicious macros embedded in document attachments. The attackers have continually innovated their "masking" techniques in an effort to stay ahead of defenses, and in August Proofpoint researchers detected another example of this innovation in a campaign comprised of millions of messages, of which the majority were targeted at organizations in the U.S. and U.K. The campaign contained a voice message lure in an attachment named "08439801260_20150725_150834.wav.lnk." See below:



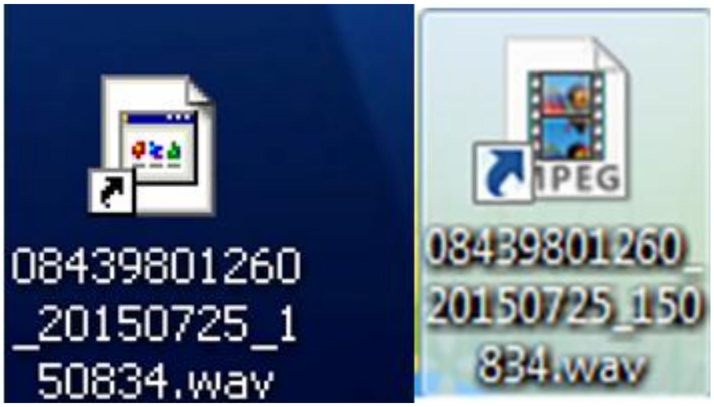
Voice Message Attached from 08439801260

voicemessage@yourvm.co.uk
Tuesday, July 28, 2015 at 3:20 AM
To: [redacted]
: 08439801260_20150725_150834.wav.lnk (5.4 KB)

Time: Jul 28, 2015 3:08:34 PM
Click attachment to listen to Voice Message

As we described in The Human Factor report for 2015, the voicemail email lure has been one of the most popular phishing templates, but this use of .lnk files was noteworthy because it had not been previously detected masking a Dridex payload.

In some versions of Microsoft Windows, “the wav.lnk file was represented with a Windows audio file (.wav) icon, while in others, a generic file icon was displayed.” See below:



Essentially, a double-click of the attachment calls “cmd.exe” (http://www.file.net/process/cmd.exe.html) to run a series of shell commands. In turn, the .lnk file is copied to a temporary directory and a .vbe file is extracted from the .lnk file. The .vbe file is then written to a disk and executed.

Ultimately, this dynamically generated script file downloads and executes Dridex Botnet No. 220 binary from the following URL: hxxp://laurance-primeurs[.]fr/345/wrw.exe.

Read on: https://www.proofpoint.com/us/threat-insight/post/The-Missing-LNK.

Hunter Exploit Kit Targets Brazilian Banking Customers

What are exploit kits? Fundamentally, they are toolkits used to manipulate security holes in order to spread malware. They are “important components of the cybercrime infrastructure,” according to Kevin Epstein, Proofpoint’s VP of Threat Operations, and it is noteworthy that “they enable attackers to target one or more exploits at clients without requiring that they actively download a file or attachment.” See also: https://zeltser.com/what-are-exploit-kits/.

Proofpoint research scientists recently detected and analyzed a new exploit kit (EK) called “Hunter.”

Initially, this campaign targeted Brazilian banking customers by means of a phishing ruse. More specifically, the links redirected to a malicious site, which Proofpoint researchers determined hosted a previously undocumented exploit kit.

The Hunter EK can be fetched by means of iframes (inline frames) and IMG (image) tags.

Learn more about this new exploit kit and the phishing templates employed to spread it here: https://www.proofpoint.com/us/threat-insight/post/Hunter-Exploit-Kit-Targets-Brazilian-Banking-Customers.

Threat News

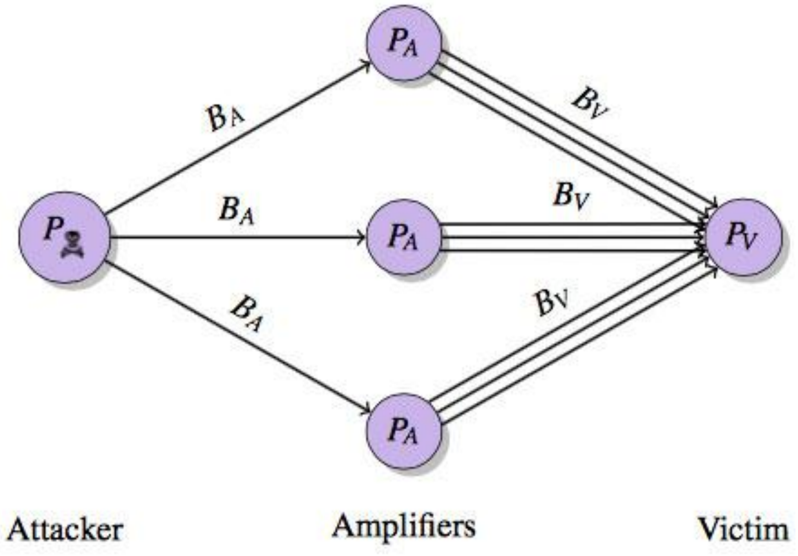
BitTorrent Clients Can Be Made to Participate in High-Volume DoS Attacks

A new variety of denial-of-service (DoS) attack has been discovered and the stunt can be manipulated and brought off by a single attacker. Basically, the fraudster exploits weaknesses in the BitTorrent protocol family.

“The weaknesses in the Micro Transport Protocol (µTP), Distributed Hash Table (DHT), Message Stream Encryption (MSE), and BitTorrent Sync (BTSync) protocols” let the perpetrator “insert the target’s IP address instead of his own in the malicious request,” as stated by Help Net Security.

To set a Distributed Reflective DoS (DrDoS) attack in motion, an attacker sends the formed request to other BitTorrent users. These users, in turn, act as reflectors and amplifiers. And the end result is the inevitable: the victim is inundated with responses.

See the pictorial representation of how a threat actor carries out the attack:



For additional details, see: http://www.net-security.org/secworld.php?id=18769.

IRS Says Cyberattacks More Extensive Than Previously Thought

The U.S. Internal Revenue Service (IRS) recently acknowledged that a hacking stint, revealed in May and involving one of its computer databases, was far more extensive than previously described.

The theft claimed the data of nearly three times as many taxpayers as first revealed.

The original estimate by the IRS included about 114,000 U.S. taxpayers. According to the IRS, the tax return information of these taxpayers had been accessed by cyber criminals in an illegal manner over the preceding four months, coupled with yet another 111,000 unsuccessful attempts.

A reexamination has pinpointed an additional 220,000 incidents of breached data, according to the tax collection agency. Another 170,000 suspected failed attempts by third parties were identified.

In May, it was stated by the agency that some 15,000 fraudulent returns were processed in the 2015 tax filing season. It remains to be seen exactly how many fresh instances stem from the additional breaches.

Read more about it here: http://www.reuters.com/article/2015/08/17/us-usa-tax-cybersecurity-idUSKCN0QM1VV20150817.

Two-Thirds of Organizations Are Potential Targets for Nation-State Cyberattacks

Two hundred fifteen attendees at the Black Hat USA 2015 security conference in Las Vegas, Nevada, were surveyed in August. This recent survey highlighted cyber corruption and graft. Among its findings, the Black Hat respondents revealed the following statistics:

- Nearly two-thirds (64%) of organizations are potential targets for nation-state cyberattacks. (Nation-state cyber espionage and targeted attacks can be defined as politically motivated.)
- Eighty-six percent of respondents have noticed an increase in targeted attacks clearly directed at their networks over the past year.
- Forty-one percent of respondents affirmed that they have seen a striking increase in the number of successful cyberattacks this past year.

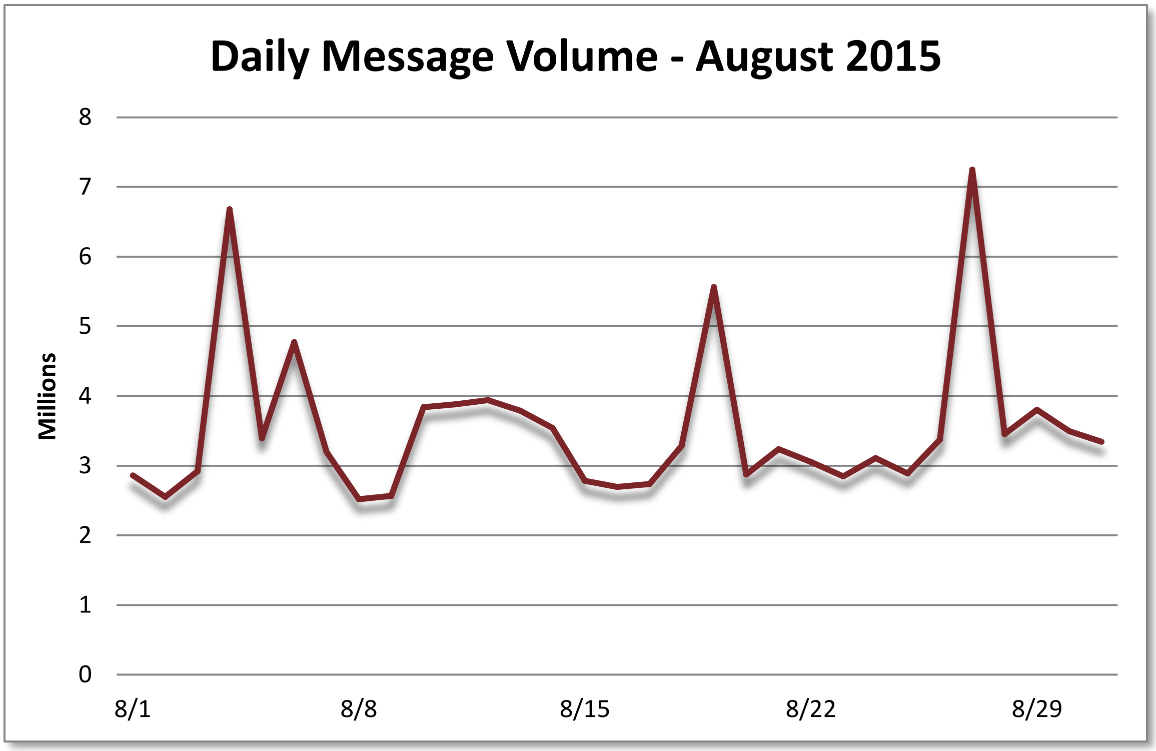
In the face of this apparent increase in attacks, *less than half* of the respondents *(47%)* reported that trust in the ability of their organizations "to detect and respond to a cyberattack rose in the last 12 months."

Read on for more staggering statistics: http://www.scmagazineuk.com/two-thirds-of-organisations-are-potential-targets-for-nation-state-cyber-attacks/article/433005/.

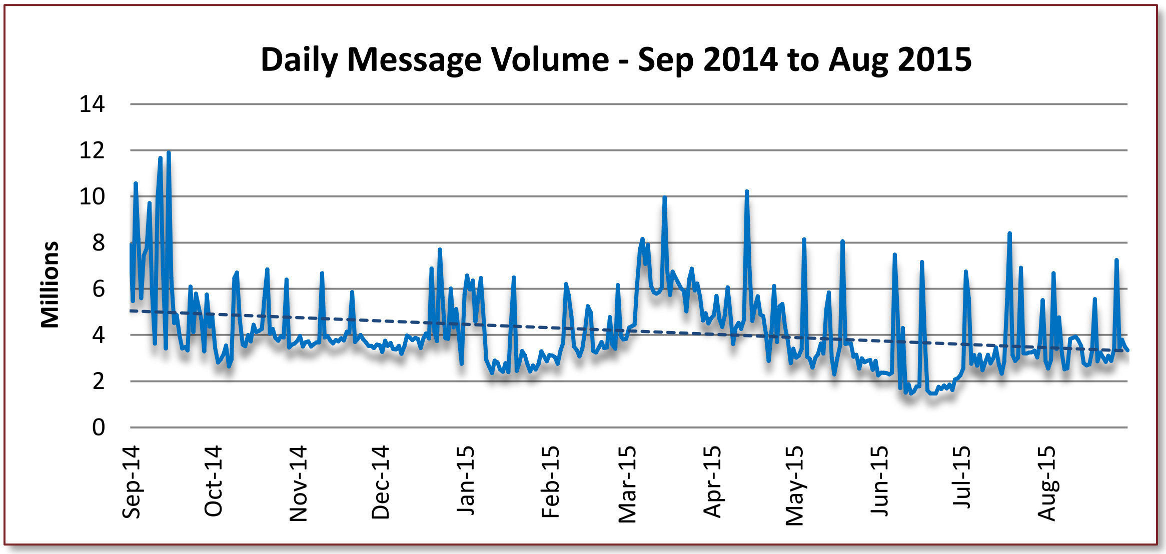
Threat Trends

Spam Volume Trends

Proofpoint tracks spam volumes via a system of honeypots. The volumes historically track with that of our customer base. August's daily spam volume was a varied collection of highs and lows. It began with a short dip below 3 million and then zigzagged instantaneously to roughly 6.75, 3.5, and 4.75 million. A gradual decline to 2.5 million capped the first week. With a slight tilt to nearly 4 million, a short plateau ensued. A gradual decline to 2.75 million completed the second week. A mini-plateau followed and then a grand spike to 5.5 million set a tumultuous ride in motion: a dive to 3 million and short bursts of activity thereabouts led up to the final and most impressive of the spikes (in the fourth week). At 7.25 million, a compelling dive to 3.5 million accentuated the fourth week. Ripples between 3 and 4 million capped the month.



By comparison, August-over-July reflected a slight decrease in the volume of spam (2.34%). The year-over-year spam tally decreased by 51.10%.



Spam Sources by Region and Country

The EU ruled yet again, and the U.S. held second place for the eighth straight month. China again came third and Vietnam captured fourth as Russia sank to fifth.

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

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

The table below details the percentage of total spam volume for the July 2015 and August 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 22.81%, the EU generated the majority of the world's spam. The remaining four countries in the top five slots were collectively responsible for 25.18%—insignificantly above the output of the EU.

July 2015			August 2015		
1	EU	25.70%	1	EU	22.81%
2	US	11.34%	2	US	10.93%
3	China	7.82%	3	China	6.60%
4	Russia	4.73%	4	Vietnam	4.07%
5	Vietnam	2.54%	5	Russia	3.58%

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

July 2015			August 2015		
1	Germany	2.77%	1	Germany	2.13%
2	Spain	2.16%	2	Romania	1.46%
3	Romania	2.03%	3	Spain	1.37%
4	Italy	1.96%	4	Czechoslovakia	1.18%
5	Bulgaria	1.44%	5	Italy	1.18%

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