proofpoint

Proofpoint Threat Report

December 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

DarkSideLoader — You Don't Need To Jailbreak Your iPhone To Find Malware

In the past, iOS users who wanted to install software from so-called "rogue app stores" had to jailbreak their phones. In the process, they gained access to a variety of free, pirated, and often illicit software and, more importantly, opened themselves up to one of the few vectors for app-based malware on iOS.

In December, however, Proofpoint researchers "discovered a rogue app store that allows iOS device users to download apps from a catalog claiming 1 million apps onto their iPhones or iPads *without jailbreaking the devices*". The potential for bad actors to exploit the device access afforded through a rogue app store is quite large, setting the stage for users to unwittingly download remote access Trojans, load malicious configuration files, and otherwise provide beachheads for access to corporate and personal information via non-jailbroken devices.

Proofpoint researchers have dubbed this type of rogue app store "DarkSideLoader" because it allows side loading of apps (good, bad, and

otherwise) on devices where such action would not previously have been possible.

These rogue app stores are a prime source of so-called “riskware”, although risky apps are readily available in legitimate app stores as well. The bottom line is that users need to be mindful of the apps they install from any source since elevated permissions, communication with potentially malicious or compromised servers, and even access to network data are surprisingly common among apps that appear benign.

For details from Proofpoint experts on DarkSideLoader and the threat even seemingly harmless apps can pose to individuals and organizations, see:

- http://proofpoint.com/us/threat-insight/post/DarkSideLoader-Rogue-App-Stores-Targeting-Non-Jailbroken-iOS-Devices
- http://www.proofpoint.com/us/threat-insight/post/Risky-Mobile-Apps-Steal-Data

Malvertising Campaigns Find New Ways To Push Angler Exploit Kit

Domain shadowing typically uses stolen registration credentials to malicious subdomains from legitimate domains. Attackers can then use these subdomains, which look reasonable to most end users and often make it past reputation-based content filters, to filter and redirect users to the exploit kits of the attacker’s choice.

Proofpoint researchers noticed that particular malvertising attacks were making use of shadow domains to deliver Angler EK to users in ways that bypassed many of the defenses used by both ad networks and some types of security infrastructure. As the researchers pointed out, “These adaptations will enable malvertising to remain an effective malware distribution method for months to come.”

Check out the full analysis from Proofpoint researchers on the use of shadow domains in malvertising here: http://proofpoint.com/us/threat-insight/post/The-Shadow-Knows

Gootkit Expands Its Footprint

Gootkit is a JavaScript-based banking Trojan that has primarily focused on customers from several French banks. It has evolved throughout 2015 and has been observed infecting PCs directly via Angler EK and indirectly via the Bedep Trojan and appeared to begin targeting Italian banks as early as March 2015. By

the end of November, Proofpoint researchers had observed Gootkit attacks first in Canada and then in the UK.

In the UK, Gootkit was dropped at the end of a malvertising campaign via Angler, targeting customers of several financial institutions there. This follows a larger trend of formerly geographically isolated malware expanding its footprint as cybercriminals seek new targets for their attacks.

Read more about the latest on Gootkit from Proofpoint researchers here: http://proofpoint.com/us/gootkit-banking-trojan-jumps-channel

Threat News

Proofpoint Researchers Deliver Their 2016 Cybersecurity Predictions

Every year, Proofpoint's threat researchers deliver their biggest cybersecurity predictions for the coming year based on historical data and current trends. For 2016, the "human factor" will remain the biggest issue to watch as attackers continue to build on their successes in social engineering by going after the end users who are far more fallible than increasingly sophisticated cybersecurity tools.

While end users will be particular targets for cybercriminals in the coming year, Proofpoint researchers also expect a few more trends will stand out:

- Commodity, off-the-shelf malware is making it easier and cheaper for both sophisticated actors and less savvy cybercriminals to engage in successful targeted attacks.
- Cybercriminals will broaden their attacks, adapting, for example, banking Trojans to capture credentials outside of traditional online banking targets or going beyond end user PCs and attacking ATMs and other embedded systems.
- The "Next Big Thing" is on its way, as evidence mounts that attachment-based schemes are nearing the limits of their effectiveness.
- Social and mobile threats will continue to evolve and become increasingly dangerous for both individuals and organizations.

For more details and predictions, see: https://www.proofpoint.com/us/threat-insight/post/Cybersecurity-Predictions-for-2016.

It's Tax Season – Time For Scam IRS Emails To Deliver Malware Payloads

Tax season is just around the corner in the U.S. and cybercriminals have already begun their annual tax-related campaigns using phony emails from the Internal Revenue Service (IRS) to give renewed impetus to attacks.

The latest tax phishing campaign, as described in SCMagazine and elsewhere, alerts recipients that they are the beneficiaries of a refund from the IRS.

Interestingly, the email includes a ZIP attachment containing a JS file. The JS file activates Windows PowerShell for the purpose of downloading the payload. This occurs as soon as the ZIP file is opened.

A close analysis of the payload revealed that there were multiple payload families involved: Kovter (primary) and CoreBoT (secondary).

See https://heimdalsecurity.com/blog/security-alert-fileless-kovter-teams-modular-corebot-malware-irs-spam-campaign/ for more details.

Web Attack Knocks BBC Websites Offline

In a demonstration of the power of a distributed denial of service attack (DDoS), a large web attack recently rendered all the BBC's websites temporarily inaccessible. A DDoS attack is an attempt to make an online service unobtainable by overwhelming it with traffic from a multitude of sources.

The sites were hit at about 7:00pm UTC on Thursday, December 31 and visitors were greeted with an error message. The outage lasted roughly four hours, at which time the BBC announced that its website was operating normally. Four hours, however, is a high-impact outage for a site that, according to Internet analytics firm comScore, ranks only behind Google and Facebook in visitor numbers in the UK.

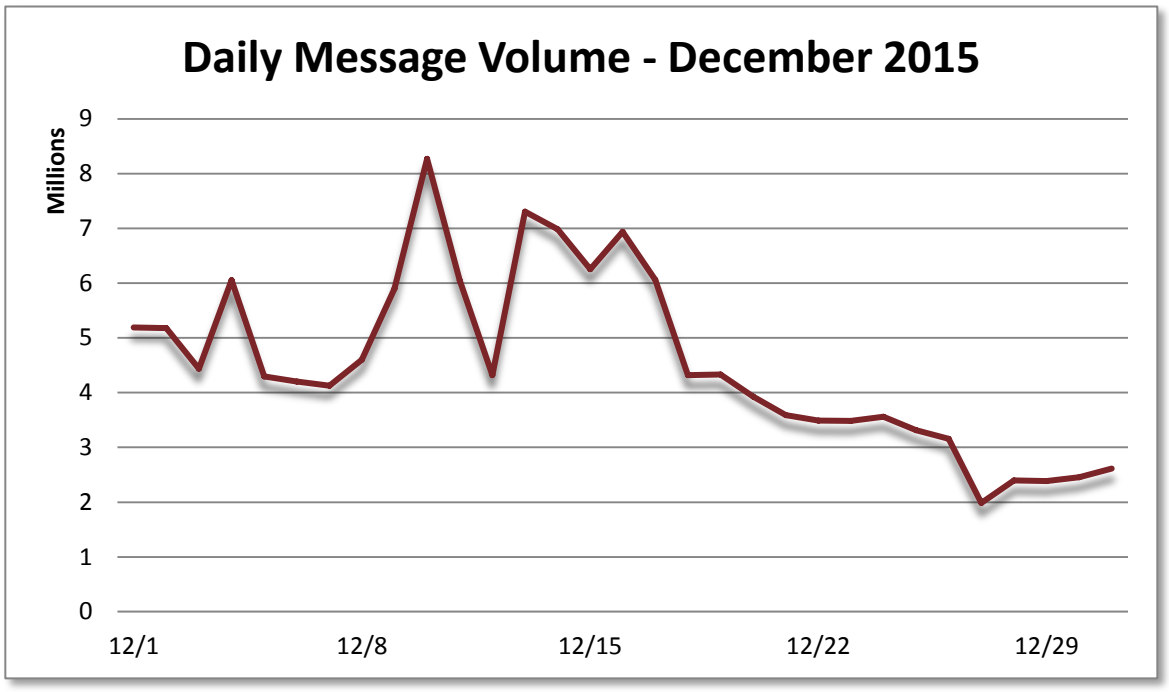
At the same time, the average size of a DDoS attack is increasing globally, with even "average" attacks approaching 1 gigabit per second of malicious traffic, making outages at organizations less equipped to mitigate the attacks than the BBC a very real possibility.

Read more at http://www.bbc.com/news/technology-35204915.

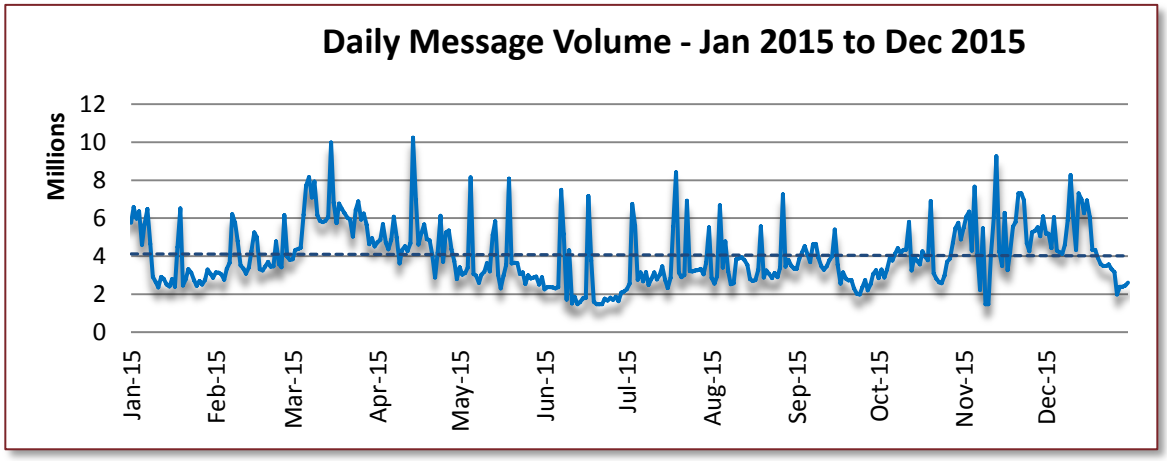
Threat Trends

Spam Volume Trends

Proofpoint tracks spam volumes via a system of honeypots. The volumes historically track with that of our customer base. December's daily spam volume was very high right up to the beginning of the Christmas holiday. Spam volume reached well above 8 million messages during the second week of December. By the third week, volumes trailed off dramatically and stayed below 4 million messages per day for the remainder of the month with the end of the year hovering between 2 and 3 million.



By comparison, monthly volumes were down in December from November by 11.6%, largely as a result of holiday-related slowdowns. However, volumes were up by 10.8% over December 2014.



Spam Sources by Region and Country

As in the past several months, the EU has been the single largest source of spam geopolitically worldwide, but China overtook the US in overall volumes in December. Russia kept the #4 spot while Vietnam reemerged as #5.

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

		Jul '15	Aug '15	Sep '15	Oct '15	Nov '15	Dec '15
Rank	1st	EU	EU	U.S.	EU	EU	EU
	2nd	U.S.	U.S.	China	China	U.S.	China
	3rd	China	China	EU	U.S.	China	U.S.
	4th	Russia	Vietnam	Russia	Russia	Russia	Russia
	5th	Vietnam	Russia	Vietnam	Indonesia	Panama	Vietnam

The table below details the percentage of total spam volume for the November 2015 and December 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 18.57%, the EU generated the majority of the world's spam. The remaining four countries in the top five slots were collectively responsible for 34.7%, a substantial increase from November, even as EU volumes declined slightly.

November 2015			December 2015		
1	EU	19.09%	**1**	EU	18.57%
2	U.S.	11.22%	**2**	China	13.99%
3	China	9.72%	**3**	U.S.	13.21%
4	Russia	5.47%	**4**	Russia	4.73%
5	Panama	2.25%	**5**	Vietnam	2.78%

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

November 2015			December 2015		
1	Germany	2.35%	**1**	Germany	4.79%
2	Italy	2.07%	**2**	UK	1.20%
3	U.K.	1.54%	**3**	Spain	1.10%
4	Romania	1.11%	**4**	France	0.93%
5	Spain	1.04%	**5**	Bulgaria	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

