

A photograph of a modern glass skyscraper, viewed from a low angle looking up. The building's facade is composed of a grid of dark metal frames and large glass panels. The sky is a pale, overcast blue. A semi-transparent blue horizontal band is overlaid across the middle of the image, serving as a background for the title text.

Proofpoint Threat Report

December 2014

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

Threat Models

Cybercrime-as-a-Service: The New Criminal Business Model

Europol's European Cybercrime Centre (EC3) divulged that cybercrime is being increasingly commercialized, and by criminals who use legitimate services to hide their activities.

According to the 2014 Internet Organised Crime Threat Assessment (iOCTA) report (<https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta>), a service-based criminal industry is developing whereby an increasing number of those operating in the virtual underground are starting to make products and services for use by other criminals.

EC3 investigators noted that such a 'crime-as-a-service' business model can be viewed in the cyberworld, hence the report suggests that the barriers to entry into cybercrime are being lowered to the extent that even those without technical skills can participate.

The executive summary emphasizes how "mafia-style" gangs will look to venture into the market to buy up the relevant skills and tools.

The EC3 report continues that cybercriminals are also abusing legitimate services and tools, such as anonymization, encryption, and virtual currencies to carry out illicit activities.

To add to the maze of complexities, the 2014 iOCTA emphasizes that criminals mainly operate from outside EU jurisdictions and reveals that outdated legal tools and insufficient response capacities are to blame for the difficulty in bringing cybercriminals to justice.

This highly complex challenge for law enforcement is intensified by the difficulties faced by police in recruiting the right people and acquiring the right tools. Ultimately, more international collaboration is required if law enforcement is to be successful, given that modern cybercrime, especially organized crime, is by nature trans-national.

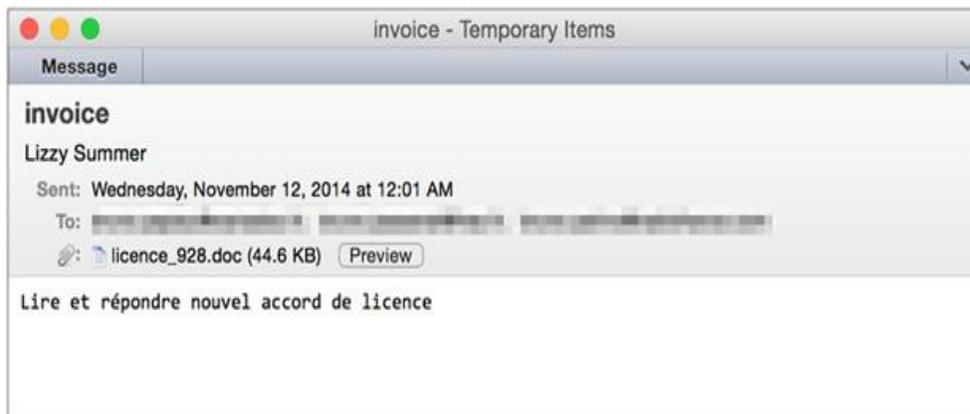
An international view of the threat posed by this ever-increasing form of crime must be taken.

Phishing: The International Language

Proofpoint researchers recently detected a targeted low-volume phishing campaign aimed at organizations in both France and Germany. The campaign provides us with an illustration of a phishing campaign that spans multiple languages and countries. It shows the role of language as another variable that malefactors can leverage to evade defense.

Twelve different Microsoft Word document attachments were detected in this campaign; they were cycled with multiple senders and headings (to evade reputation-based blocking) to create a classic longline phishing campaign. Automated analysis of the attachments revealed that the documents include a malicious macro, a VBA Trojan, that downloads and installs the Andromeda, or Gamarue, malware. Obfuscation of both the macro and the Andromeda payload enabled the perpetrators to achieve a high level of antivirus evasion: when Proofpoint analyzed them, the attachments were detected by less than ten percent of antivirus engines, and the Andromeda payload was detected by only five percent.

The campaign included e-mail templates in both French and German, with a variety of lures, subject lines, and message bodies. For instance, the following French e-mail asks the recipient to read and respond to the latest license agreement, while a German sample includes an invoice and requests payment by January 1:



These samples from a single campaign exemplify the variation of attachment names, lures, subject lines, and sender addresses that makes modern longline phishing campaigns so effective against reputation and signature-based defenses.

The moral of the story is clear: organizations must complement their existing anti-spam gateway with advanced detection capabilities.

Even the best traditional defenses are not enough.

Threat News

The Data Breach Payment Fight Heats Up

Who should be accountable following a data breach? The discord between retailers and banks over who should pay dearly is ramping up as the new year unfolds.

Currently, there is little legal framework to govern retail data breaches and thus merchants and banks have spent a good part of 2014 bickering about who is at fault in the wake of an attack.

Note that many of these liability issues could be resolved through data breach legislation. While the US Congress held multiple hearings throughout 2014 to consider a possible bill to establish minimum data security standards, no serious proposal came close to passage.

The argument of retailers follows, as well as the counterargument of banks, among other interesting facts: <http://thehill.com/policy/cybersecurity/228161-the-fight-over-paying-for-data-breaches-heats-up>.

Spear Phishing: A Bigger Concern in 2015 (Why Bank Employees Are Increasingly Targeted)

While spear phishing was linked to numerous high-profile cyberattacks in 2014, hackers are now increasingly channeling their energies into phishing campaigns against bank employees rather than bank customers. Essentially, they are going after the bank itself.

Hackers are successfully targeting banking institution employees with convincing e-mail ruses. Designed to fool the employees into clicking on malicious links or providing details about account holders and their accounts, once clicked, credentials or other sensitive information becomes compromised.

And so begins the perpetration of fraud.

Find out why employees are such easy targets, as well as other interesting information: <http://www.bankinfosecurity.com/spear-phishing-bigger-concern-in-2015-a-7742>.

Emerging Global Cyberlaw Trends in 2014

From a global cybercrime perspective, the challenges of cybercrime and hacking loomed large and heavy. 2014 reminded the world that cybercriminal activities are growing in number and severity.

The message is clear: without sophisticated safeguarding, absolutely no computer system or network has the efficacy to thwart cybercriminal activity.

Vivid accounts of incidents, frightening statistics, and the status of cyberlaw can be read here: http://www.business-standard.com/article/technology/emerging-global-cyberlaw-trends-in-2014-115010500301_1.html.

Botnets in 2014: Zeus Surge, Lax Policies Place Web Users at Risk

The security landscape is likely to change in 2015 as botnets evolve and new, crippling security breaches are easily predictable.

The use of botnets is becoming an increasingly popular tool, and as noted in the Spamhaus project's *Botnet Summary for 2014*, botnet activity appears to be on the rise.

The perpetrators behind botnets can precipitate the acquisition of sensitive financial, banking, and personal data, which then may be sold on the black market.

As financial and personal data increases in value, botnet use rises. Are companies doing enough to stem the flow? Read the facts, statistics, and heed some sound advice here: <http://www.zdnet.com/article/botnets-in-review-2014-zeus-surge-lax-policies-place-web-users-at-risk/>.

Threat Insight Blog

Here we highlight interesting posts from Proofpoint's threat blog, *Threat Insight*. Subscribe to *Threat Insight* and join the conversation at <http://www.proofpoint.com/threatinsight>.

Dyreza as a Service

In October's Threat Report, we summarized the basic facts about the banking malware called "Dyreza" or "Dyre". This follow-on post elaborates on *Dyreza as a Service*.

To ensure persistence on a compromised computer, Dyre attempts to install itself as a service named *Google Update Service (googleupdate)*. The service is loaded or started automatically for all startups, regardless of type of service. The main executable runs from the Windows folder and uses a randomly named file with an .exe extension.

This product appears to be in a constant state of innovation, as is evidenced by the complexity, and oftentimes perplexity, of the processes.

Continue reading: <http://www.proofpoint.com/threatinsight/posts/dyreza-as-a-service.php>.

Cybersecurity Predictions for 2015

The dire need for sophisticated information security moved into the spotlight in 2014, driven by a steady parade of disclosures, which exposed more than one

billion user records, thorough compromises of critical infrastructure, and increasingly serious losses due to business disruption.

Cybercriminals are in a constant state of refinement. Their strategies and technical acumen are continuously evolving.

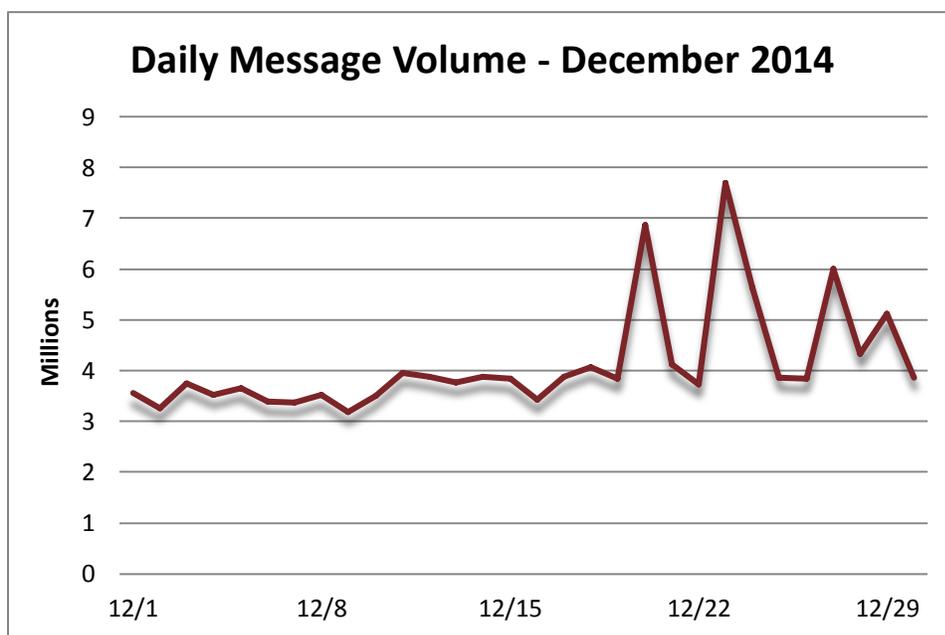
Greater scrutiny will be inevitable in 2015 in order to deter the actions of cybercriminals who will be plotting new and advanced threats with significant repercussions.

Consider the insights and advice of Proofpoint's expert researchers and scientists as you read the predictions of which threats will come to the forefront in 2015: <http://www.proofpoint.com/threatinsight/posts/cybersecurity-predictions-for-2015.php>.

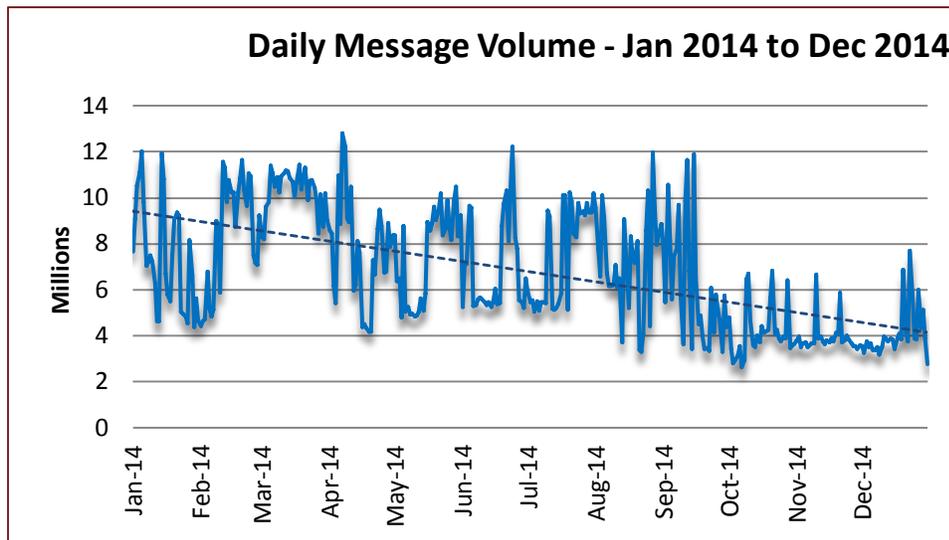
Threat Trends

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 fluctuated between 3 and 4 million until the approximate midpoint of week three, when it reached 4 million. Thereafter, four successive spikes of varying magnitudes (7, 7.5, 6, and 5 million) ensued. The bottoms of the first two spikes remained at roughly 4 million; the third spike fell to 4.25 million, and the final spike to 4 million closed the month in a dramatic way.



By comparison, November-over-December demonstrated a meager increase in the volume of spam (4.98%). The year-over-year spam tally decreased 40.88%.



Spam Sources by Country and Region

The EU recaptured the top position in December with great vigor reminiscent of past months, while China markedly dropped to second by a margin of over 14%. The USA retained the intermediary position while Russia retained fourth. Vietnam slid back into the scene to capture fifth.

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

		Jul '14	Aug '14	Sep '14	Oct '14	Nov '14	Dec '14
Rank	1 st	EU	EU	EU	China	China	EU
	2 nd	USA	USA	Vietnam	EU	EU	China
	3 rd	China	Argentina	China	Russia	USA	USA
	4 th	Argentina	Russia	Argentina	Vietnam	Russia	Russia
	5 th	Russia	China	Korea	USA	Argentina	Vietnam

The table below details the percentage of total spam volume for the November and December 2014 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 24.49%, the EU generated the majority of the world’s spam. The remaining four countries in the top five slots were collectively responsible for 25.36%—slightly above the output of the EU.

November 2014			December 2014		
1	China	20.60%	1	EU	24.49%
2	EU	20.06%	2	China	10.34%
3	USA	7.81%	3	USA	6.71%
4	Russia	4.66%	4	Russia	4.36%
5	Argentina	1.77%	5	Vietnam	3.95%



For additional insights visit us at
www.proofpoint.com/threatinsight

proofpoint™

Proofpoint, Inc.
 892 Ross Drive, Sunnyvale, CA 94089
 Tel: +1 408 517 4710
www.proofpoint.com