proofpoint

Proofpoint Threat Report

February 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

Cybersecurity: Tackling the Threat from Within

Cybersecurity has long been synonymous with defense against intruders or typified by “defending the castle walls.”

As a general rule, anti-virus solutions, firewalls, e-mail filtering systems, and other digital defenses are looking for external threats.

But what if the intruders are the occupants of the castle?

In other words, what if your own employees seek to defraud your company by copying the customer database, embezzling cash, or stealing sales leads?

Figures from PricewaterhouseCoopers’ (PWC) Global Crime Report, a consultancy, suggest that more than half of all people seeking to defraud a company are within the fortress walls.

That figure has risen steadily over the past few years, according to the firm. And it seems to be the younger members of the staff who are the driving force in this trend.

A change in the nature of fraud was also observed in the same survey. Now, criminals are as likely to indulge in procurement fraud as they are to steal cash or data. (An example of procurement fraud is making false company purchases.)

Internal fraud can be difficult to discover because it tends to be more complex than external threats. By definition, perpetrators on the inside are well aware of the systems and have a practical understanding of how to exploit the weaknesses.

And the reasons behind an attempt to steal can be complex, as well.

Oftentimes, it can take a long time for firms to pinpoint when money or other assets are disappearing.

The amazing complexity of the computer networks is part of the reason that scammers get away with so much for so long. Computer systems are inherently difficult to monitor. And the problem is compounded by an overwhelming lack of insight into how many devices are connected to a large, corporate network.

In other words, much of the activity on a company's network could be going unwatched and hence open up an opportunity for anyone keen to pilfer cash in hidden accounts.

Mapping connections between individuals, devices, and applications makes recognizing anomalies and fraud all the more difficult.

Ultimately, deterrence works best when data capture is united with monitoring. Otherwise, a failure to spot fraud can have a bigger long-term impact on a company's reputation than on its profits.

And reputation is essential.

Dyre Straits: Evolution of the Dyre Banking Trojan Challenges Traditional Defenses

The Dyre banking Trojan, also dubbed "Dyreza" and "Dyranges", has been a steady and faithful threat in the cybercrime landscape since 2014 and for the better part of last year, the driving forces appeared to be content to make use of it with few or no changes. Delivery techniques remained static until late in the year. But since that time, a dramatic evolution of the malware and infrastructure has taken place. Now, as a case in point, these actors have modified their TTPs (http://stixproject.github.io/data-model/1.1.1/ttp/TTPType/) in an attempt to improve malware delivery and installation rates. Specifically, Proofpoint researchers observed constant modifications to spam templates, URL randomization, JavaScript obfuscation, and attempts at analysis and sandbox evasion.

Dyre is distributed through unsolicited, daily high-volume e-mail campaigns that deliver malicious URLs via zipped executable attachments. The vast majority of the e-mail is created using simple, plain-text templates.

By contrast, several recently observed campaigns contained sophisticated HTML-formatted e-mail.

Generally speaking, cybercriminals continue to use lures that have something to do with a delivered message, document, fax, invoice, banking, or IRS theme. Proofpoint records reveal that these lures have been used by Dyre perpetrators since Dyre was first detected in the summer of 2014. Most likely, the attackers determined (through testing) that they were effective. Below are a few examples of e-mail *Subjects*:

- Important – New Outlook Settings
    - Lure: Outlook
- Your tax return was incorrectly filled out
    - Lure: IRS
- Payment Advice – Advice Ref[GB583174] / CHAPS credits
    - Lure: UK-based retail bank
- Important information about your account
    - Lure: UK-based retail bank
- Important – Please complete attached form
    - Lure: UK-based retail bank
- <bank_name> - Important Update, read carefully!
    - Lure: UK-based retail bank
- Employee Documents – Internal Use
    - Lure: Document notification

The criminals behind Dyre continue to develop and progress their malicious URL generation scheme. At one time, a single URL was used from each malicious domain. According to Proofpoint researchers, "This made detection and creation of signatures relatively easy based on the URI path, because it was possible to create one-to-one signatures for full URLs."

In January 2015, Dyre perpetrators updated their methods and are now generating hundreds of URLs per domain. (See *URL Randomization:* http://www.proofpoint.com/us/threat-insight/post/Dyre-Straits-Evolution-of-the-Dyre-Banking-Trojan-Challenges-Traditional-Defenses.)

An ill-fated click on the link in the e-mail body transports the user to an initial malicious site and then JavaScript content is pulled down from two more malicious domains. (See *Script Obfuscation and Sandbox Evasion:* http://www.proofpoint.com/us/threat-insight/post/Dyre-Straits-Evolution-of-the-Dyre-Banking-Trojan-Challenges-Traditional-Defenses .)

For a thorough presentation of *binary randomization* by Proofpoint experts, see also: http://www.proofpoint.com/us/threat-insight/post/Dyre-Straits-Evolution-of-the-Dyre-Banking-Trojan-Challenges-Traditional-Defenses.

Dyre's sudden burst of evolution to incorporate evasion techniques often associated with more sophisticated, targeted threats emphasizes a central challenge of today's threat landscape: "an increasingly broad spectrum of malware and attacks are leveraging the techniques that have made advanced threats so effective at bypassing traditional signature- and reputation-based defenses," as stated by Proofpoint experts.

Threat News

Cyber Attack Takes Down Dutch Government Sites

On Wednesday, February 11, Dutch government officials confirmed that the website assault at 09:00 GMT (04:00 ET) on Tuesday of that same week, crippled a string of its websites for more than seven hours, was attributed to cyber attackers. Backup plans proved ineffective because of the apparent size of the attack, exposing the vulnerability of critical infrastructure.

Coincidentally, on the same day as the Dutch attack, United States cybersecurity laws were intensified and the creation of an intelligence-gathering unit was instituted to coordinate analysis of cyber threats.

The Dutch debacle also followed warnings that sites belonging to French authorities had been targeted.

The outage affected most of the central government's major websites, which provide information to the public and the media, while phones and emergency communication channels remained operative.

The Dutch government confirmed that it had suffered a distributed denial of service attack (DDoS)—a bombardment of traffic to the sites intended to render them unavailable to users.

Investigators have not said who might have been responsible.

To learn more about the complexity of this attack, click here: http://www.bbc.com/news/technology-31440973.

Why Small Firms Struggle with Cyber Security

Simply put, "greed" is a term applied almost exclusively to those who want to earn more money or to keep what they have already earned. Cyber thieves are motivated by such greed, with an added dimension of stealing from and living at

the expense of others. In addition, cyber thieves have both the technical abilities and the drive to achieve great wealth.

In recent months, this skill set has served them well as they have stolen data from a spectrum of targets, including Home Depot, eBay, and Target.

The problem becomes far more acute for smaller organizations.

Smaller organizations have the same exposure to many of the same attacks as larger enterprises, yet their security expertise and resources are, as one would expect, comparatively smaller.

The sad reality is that these smaller firms suffer at the hands of the same bands of thieves, and are getting hit hard.

It has been suggested that approximately 30,000 websites per day are being compromised by cyber criminals.

And for smaller firms, the cost of becoming a victim of a hack or breach is vexing: $100,000 to $175,000 per instance.

Continue reading: http://www.bbc.com/news/technology-31039137.

Legal Liabilities in Recent Data Breach Extend Far Beyond Anthem

According to legal experts, the unprecedented breach of some 80 million personal records belonging to insurance giant Anthem could involve nearly sixty health insurance plans from Hawaii to Puerto Rico. The potential legal liabilities are astounding. In less than a month, more than 50 class-action lawsuits related to the breach have already been filed.

Under the Federal Health Insurance Portability and Accountability Act (HIPAA) privacy and security law, as well as state laws, responsibility for the breach could fall into the hands of the plans themselves. A rising series of private civil suits could also be on the horizon.

The premise is clear: Anthem, the other Blue plans, and the Chicago-based Blue Cross and Blue Shield Association, are bound by “business associate” agreements to promote a national, reciprocal claims payment network called BlueCard.

And the network is run by the association.

The breach was disclosed on Wednesday, February 4. The records of individuals in 14 Anthem plans were bared, in addition to the records of enrollees of 42 non-Anthem Blue plans. These records number in the millions.

Anthem has posted to its website the names of all 42 Blue plans whose members have been impacted by the breach.

These include any members who used the BlueCard network of the Chicago-based Blue Cross Blue Shield Association and sought care in any of the 14 states where Anthem-owned Blue plans do business.

In an e-mailed statement, the Blue Cross Blue Shield Association indicated that the FBI, federal and state regulatory authorities, and Anthem's own internal teams are investigating the data breach in all respects.

For additional details, click here: http://www.modernhealthcare.com/article/20150223/NEWS/302239977/legal-liabilities-in-recent-data-breach-extend-far-beyond-anthem.

EU Data Protection Three Years On: Playing Catch-Up With a Changing World

January 2012 gave rise to new EU rules designed to establish a secure and unified sphere of activity involving the collection, use, and retention of data.

Consumer research was undertaken two years earlier amid growing concerns around online data privacy, the evolving digital landscape, and globalization. These concerns gave impetus to a change in regulation.

Individuals would now experience greater control over their personal data, while businesses would be made more accountable for that data, with stricter requirements for protection and penalties around data breaches. The new rules would commit the 28 European member states to a set of consistent, legally enforced regulations and rigid definitions. And organizations outside the EU that collect, store, or process European data would have to abide by these rules.

But three years have come and gone, and such a period of time is an eternity in the rapidly evolving digital universe. It is likely to be another year before the proposals are instituted.

Consumer attitudes have changed considerably since 2012. Moreover, new tools and technologies have revolutionized the way data can be used and is being used in business.

The rules manifestly seek to build a strong framework around the use of personal data in research and they heed the need to anonymize such data.

Continue reading: http://www.itproportal.com/2015/02/22/eu-data-protection-three-years-playing-catch-up-changing-world/.

Threat Insight Blog

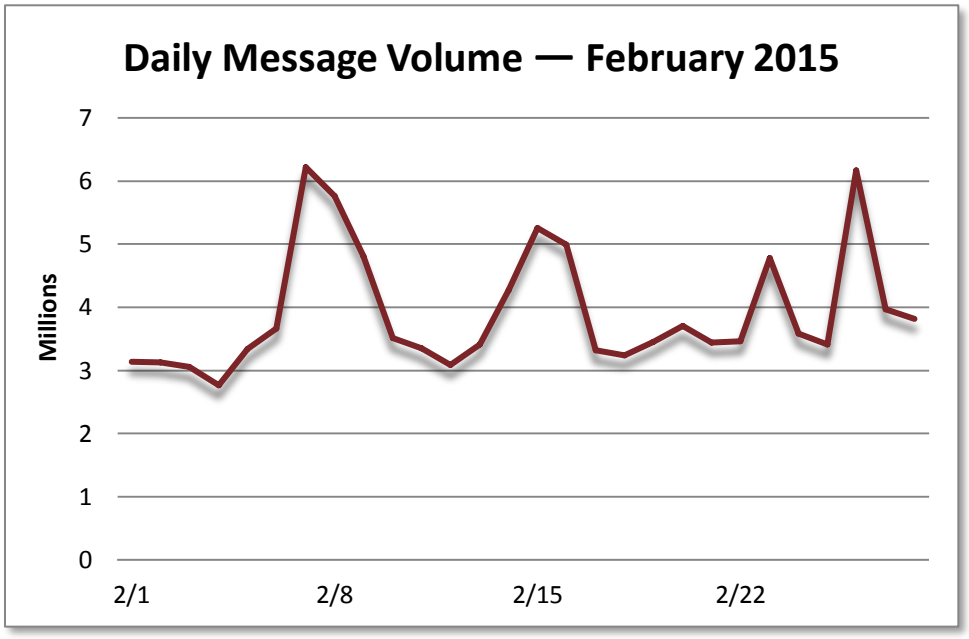
Here we highlight interesting posts from Proofpoint's threat blog, *Threat Insight*. Subscribe to *Threat Insight* and join the conversation at http://www.proofpoint.com/threatinsight.

Please note that henceforth, blog stories and excerpts will be located exclusively at the URL immediately above. So as to better expound on our expertise of threat models and attacks, we are merging this section of the *Threat Report* with *Threat Models*.

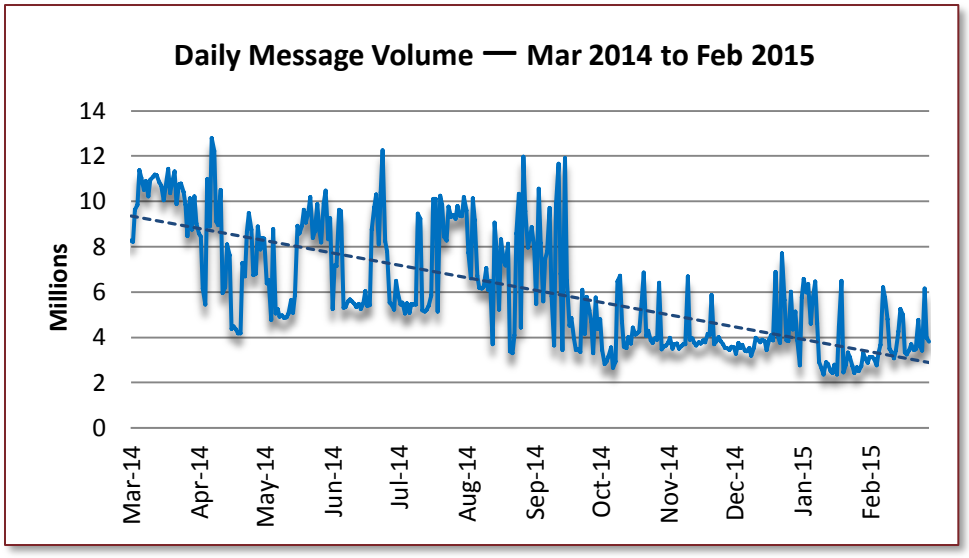
Threat Trends

Spam Volume Trends

Proofpoint tracks spam volumes via a system of honeypots. The volumes historically track with that of our customer base. February's daily spam volume was a tale of highs and lows beginning at roughly 3 million and rising to above 6 million by the end of the first week. Week two underwent a gradual plummet to 3 million and immediately thereafter, a gradual ascent to 5 million capped the week. The descent to just above 3 million came afterward and a brief plateau of 3.5 million defined the end of week three. Yet another spike to nearly 5 million characterized the start of the final week of February. A gradual downturn to 3.5 million, a dramatic spike to above 6 million, and one final dive to 4 million capped the month.



By comparison, January-over-February demonstrated a meager increase in the volume of spam (6.10%). The year-over-year spam tally decreased by 53.77%.



Spam Sources by Region and Country

The EU recaptured the top position in January in a commanding way, while the USA retained its position in second place. Vietnam also defended its stronghold by recapturing third and Argentina obstinately hung on to fourth. Russia rose to the occasion and snatched fifth from China.

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

		Sep '14	Oct '14	Nov '14	Dec '14	Jan '15	Feb '15
Rank	1st	EU	China	China	EU	EU	EU
	2nd	Vietnam	EU	EU	China	USA	USA
	3rd	China	Russia	USA	USA	Vietnam	Vietnam
	4th	Argentina	Vietnam	Russia	Russia	Argentina	Argentina
	5th	Korea	USA	Argentina	Vietnam	China	Russia

The table below details the percentage of total spam volume for the January 2015 and February 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 35.30%, the EU generated the vast majority of the world's spam. The remaining four countries in the top five slots were collectively responsible for 15.62%—well below the output of the EU.

January 2015			February 2015		
1	EU	40.36%	**1**	EU	35.30%
2	USA	5.68%	**2**	USA	6.67%
3	Vietnam	4.53%	**3**	Vietnam	3.64%
4	Argentina	3.84%	**4**	Argentina	2.85%
5	China	2.14%	**5**	Russia	2.46%

The following table displays the top five spam-sending member states of the European Union (EU) for February 2015.

February 2015		
1	Germany	4.45%
2	Spain	4.10%
3	Italy	3.48%
4	Romania	2.21%
5	Bulgaria	1.97%

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

