proofpoint

Proofpoint Threat Report

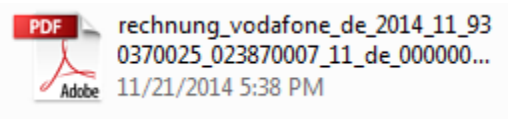
November 2014

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

Threat Models

Long-running Campaign Installs "Emotet" Malware in Germany

In recent weeks, Proofpoint researchers have been observing a fairly large e-mail campaign. It targets German users by utilizing phishing lures that lead to “Emotet” banking malware. This campaign is able to burn through several dozen compromised websites per day to stay ahead of reputation filters. The URLs used redirect to ZIP files with names designed to match the e-mail lures, such as “rechnung_vodafone_de.zip”, with executable files. The executable filenames also match the campaign lures, e.g., "rechnung_vodafone_de_2014_11_930370025_023870007_11_de_000000383 7_888830.exe," and use a PDF (or similar) file icon to trick users into thinking that the executable file is actually a safe document. The combination of the long filename that hides the extension and the accompanying file icon makes for a convincing ruse:



Antivirus detection of this malware is poor, with fewer than four percent of antivirus engines detecting the file at first submission.

Samples of e-mail templates observed in the most recent campaign follow:

Ihre Telekom Mobilfunk RechnungOnline Monat November 2014 (Nr. 4774055700252885)

245444-00104@t-mobile.de
November 21, 2014 at 12:29 AM
To: [redacted]
Ihre Telekom Mobilfunk RechnungOnline Monat November 2014 (Nr. 4774055700252885)

T

ERLEBEN, WAS VERBINDET.

Ihre Rechnung, November 2014

Guten Tag,

mit diesem Schreiben erhalten Sie eine Benachrichtigung über Ihre aktuelle Rechnung. Die zur Zahlung fällige Summe für November 2014 beläuft sich auf: **245,86 Euro**.

Im Anhang finden Sie die gewünschten Dokumente zu Ihrer Mobilfunk RechnungOnline für November 2014. Rechnung_2014_11_46289058_A_1229474_R_91_7237.pdf

Das ist eine automatische generierte Nachricht. Bitte antworten Sie nicht auf diese E-Mail.

Mit freundlichen Grüßen

Ralf Hoßbach
Leiter Kundenservice

24,95
€

© Kundenservice Rechnungonline Telekom 2014

Internet Voting Hack Alters PDF Ballots in Transmission

The practice of Internet voting has been kept to a bare minimum in the United States, in large part due to threats to its integrity.

On the heels of the recent midterm elections, researchers at Galois, a computer science research and development firm in Portland, Oregon, sent a reminder to decision makers and voters that the matter still isn't well in hand.

Take a look at the following paper, *Modifying an Off-the-Shelf Wireless Router for PDF Ballot Tampering* (http://galois.com/wp-content/uploads/2014/11/technical-hack-a-pdf.pdf). Published by researchers Daniel M. Zimmerman and Joseph R. Kiniry, it explains an attack against common home routers that would allow a hacker to intercept a PDF ballot and use another technique to modify a ballot before sending it along to an election authority.

PDF ballots have been used in Internet voting trials in Alaska, as well as in New Jersey, as a voting alternative for those displaced by Hurricane Sandy. The ballots are downloaded, filled out, and e-mailed; the e-mail is equivalent to putting a ballot into a ballot box. Then election authorities either print the ballots and count them by hand, or count them with an optical scanner.

The attack described by Galois is certainly not the only one that threatens Internet voting; malware on a voter's computer could redirect traffic or cause a denial-of-service condition at the election authority. But the attack described in the paper is undoubtedly much more quiet, enough so that the researchers say it would be undetectable, even with a forensic investigation.

"We describe a more subtle attack at the transport level, which changes the raw data traveling through the electronic mail system between the voter's computer and the election authority," Zimmerman and Kiniry write in their paper.

Once a hacker is able to sit in the traffic stream, he will be able to intercept a ballot in traffic and modify data within the PDF to change the submitted votes.

Threat News

How a Cyber Crime Gang Targets Traveling Executives Through Hotel Wi-Fi

A sophisticated malware campaign known as Darkhotel is using Wi-Fi networks at luxury hotels in Asia and across the globe to track and attack executives of major companies.

Dubbed “Darkhotel espionage campaign” by Kaspersky Lab, it has been in operation over the last four years and continues to use hotel and business center Wi-Fi networks today in order to provide the attackers with precise, global-scale access to high-value targets.

According to Costin Raiu, Director of Global Research and Analysis at Kaspersky Lab, the hackers operate methodically. They never target the same person twice.

Kaspersky Lab became aware of the apparent hacks after it observed an increased number of customer infections via its security network. They were all traced to hotels in Asia.

The threat from Darkhotel is ongoing. Overall, the infection count numbers in the thousands and that is only set to grow.

For a detailed explanation of the process, and an operative avoidance tactic, click here: http://abcnews.go.com/Technology/cyber-crime-gang-targets-travelling-executives-hotel-wi/story?id=26806725.

Identity Fraud Rises; 61% of Breaches Caused by Stolen Credentials

According to Javelin Strategy & Research's *2014 Identity Fraud Report: Card Data Breaches and Inadequate Consumer Password Habits Fuel Disturbing Fraud Trends*, in 2013, 13.1 million consumers sustained injuries from identity fraud. That is the second-highest number on record.

One of the trends includes an increase in existing card account fraud and losses. Existing card accounts refer to both account numbers and/or actual cards for existing credit and card-linked debit accounts. Losses due to existing account fraud grew forty-five percent to $16 billion, accounting for eighty-eight percent of all US fraud losses.

In-depth studies follow: http://www.duosecurity.com/blog/identity-fraud-rises-61-percent-of-breaches-caused-by-stolen-credentials.

Malicious Phishing Attacks Are Far More Effective Than Most Businesses Realize, Claims Expert

In spite of the constant threats posed by hackers, organizations have failed to give high priority to cybersecurity. Thus they leave themselves vulnerable to the increasingly sophisticated methods used by cyber criminals.

According to security expert Neira Jones, organizations “haven't fixed the basics” when it comes to protecting their data from cyber criminals. A major reason behind this is a “lack of cybersecurity awareness programs.”

Jones goes on to analyze the matter: http://www.computing.co.uk/ctg/news/2382628/malicious-phishing-attacks-are-far-more-effective-than-most-businesses-realise-claims-expert.

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.

'Tis the Season to Be Phishy

Cyber Monday presents yet another occasion for scammers and malware authors to capitalize on popular interest to spread their malicious software and fleece credulous consumers.

While e-mail phishing and spam are well-known vectors for these campaigns, social media has given operators a new set of tools to reach their potential victims. However, because many of the defenses that organizations have deployed to stop unsolicited e-mail are not effective against social media spam and phish, they are able to reach end users when e-mail-based campaigns would have been blocked.

To see and learn about the mechanics of a typical scam, click here: http://www.proofpoint.com/threatinsight/posts/tis-the-season-to-be-phishy.php.

Streaming Media Site Hit by Malvertising

According to Proofpoint researchers, a widely known live video streaming platform was made a victim of a malvertising campaign. The site has been actively serving malware to visitors as a result of an ongoing mass injection campaign against OpenX, an open source ad server. It serves as an instructive example in the operation of an injected JavaScript.

Exploits served by infected sites will silently infect visitors with malware, without them having to "click on" or "agree to" anything: visiting the website can and does result in infection.

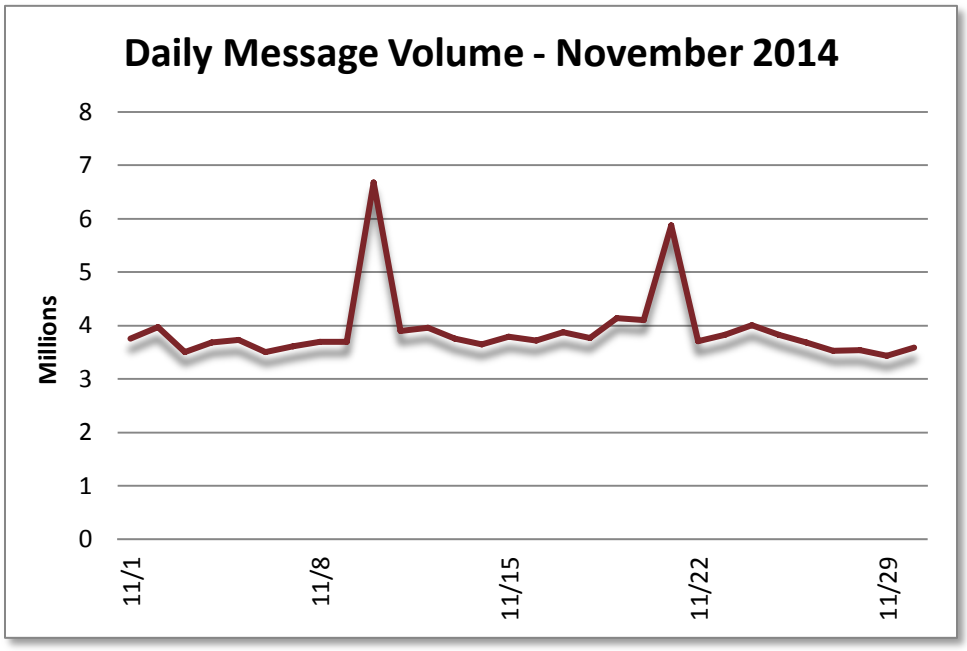
Note that Proofpoint researchers notified the owners of the infected site of their findings and worked with them to help them resolve the issue.

See the malware that was delivered by the site, among other interesting facts: http://www.proofpoint.com/threatinsight/posts/streaming-media-site-hit-by-malvertising.php.

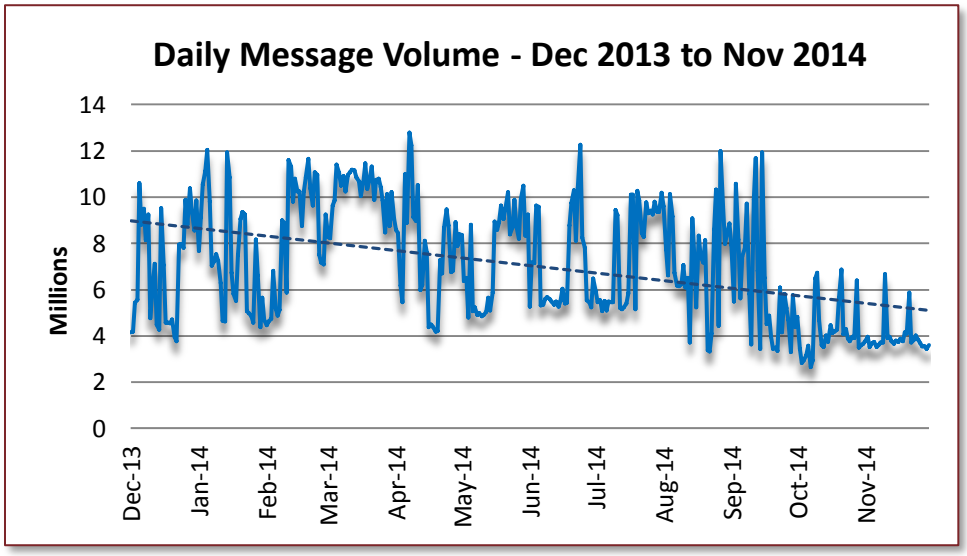
Threat Trends

Spam Volume Trends

Proofpoint tracks spam volumes via a system of honeypots. The volumes historically track with that of our customer base. The first week of November's daily spam volume fluctuated slightly, just below 4 million, until a dramatic spike to nearly 7 million at the beginning of the second week. Soon thereafter, it became steady again at just below 4 million and lasted until a lesser spike to 6 million just before the start of the fourth week. It almost immediately reverted back to the previous level, where it remained through the end of the month.



By comparison, October-over-November demonstrated a modest decrease in the volume of spam (6.21%). The year-over-year spam tally decreased 13.7%.



Spam Sources by Country

China recaptured the top position in November with pomp and splendor and the EU markedly retained second position to nearly match China. The USA captured the intermediary ranking, while Russia dropped to fourth, and Argentina made its way into fifth.

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

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

The table below details the percentage of total spam volume for the October and November 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 20.60%, China generated the majority of the world's spam for the second consecutive month. The remaining four countries in the top five slots were collectively responsible for 34.30%—well above the output of China.

October 2014			November 2014		
1	China	18.82%	**1**	China	20.60%
2	EU	15.61%	**2**	EU	20.06%
3	Russia	9.25%	**3**	USA	7.81%
4	Vietnam	5.10%	**4**	Russia	4.66%
5	USA	3.65%	**5**	Argentina	1.77%

threat insight

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

