proofpoint

Proofpoint Threat Report

March 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

From Hacking Systems to Hacking People

"Visual hacking" or "shoulder surfing" are expressions that can be used to describe the technique of looking over a person's shoulder to catch a password and the like. They are simply direct observation techniques, unjustified attacks on people's privacy.

This visual hacking can occur anywhere and anytime but hacking within office walls can be a lot more deliberate, targeted, and successful, given that users tend to be aware of strangers in a public place but let their guard down at the office.

These low-tech attack methods call for an information security environment that values data privacy, and a self-policing culture.

A vast digital universe is used by a company's work force, but the task of protecting the immense amount of data created, replicated, and consumed falls principally on IT security teams.

Complex defenses against hackers targeting company networks and systems via high-tech attacks have been developed by data security experts, but as defenses become even more sophisticated, hackers will undoubtedly identify new access points. Will there be a profound shift from hacking systems to hacking people? This remains to be seen.

But to err is human and this may very well be one of the greatest weaknesses in the data security pipeline. New research reveals just how easy visual hacking can be. *Visual hacking* is defined as a low-tech method used to capture sensitive, confidential, and private information for unauthorized use. The study, a *3M Visual Hacking Experiment* (http://solutions.3m.com/wps/portal/3M/en_US/3MScreens_NA/Protectors/Industries/VisualHackingExperiment/?WT.mc_id=www.3Mscreens.com/visualhacking), positioned a white-hat hacker into the offices of eight companies throughout the US, under the guise of a temporary or part-time worker, who attempted to hack sensitive or confidential information using merely visual means.

Employee contact lists, customer information, corporate financials, employee access and login information, and employee credentials were among the information captured.

The findings shed light on the potential consequences of hacking people: in 88 percent of attempts, the white-hat hacker could visually hack sensitive information from a worker's computer screen or from hard-copy documents.

This dramatic disclosure indicates that corporate data is at serious risk of a much larger data breach. Even more disturbingly, these hacks generally took place quickly (63 percent occurred within half an hour) and passed unnoticed (in 70 percent of instances, the visual hacker wasn't stopped by anyone).

Employees are more mobile than ever, and data is being accessed not only in the office but also from public places, making visual hacking virtually untraceable.

There are other examples of people-hacking. Employees can be targeted via other relatively low-tech means, like social engineering and spear phishing. Insider threats are also an area of increasing concern.

Defense against these threats will require new ideas and a vigorous commitment to security and data privacy from the work force at large.

Critical to the well-being of a company is a shift in corporate culture toward an environment that values security and data privacy. Protecting company data must become the responsibility of every employee.

And finally, a healthy company will encourage candor, and perhaps even praise employees, when they bring forth unpleasant information.

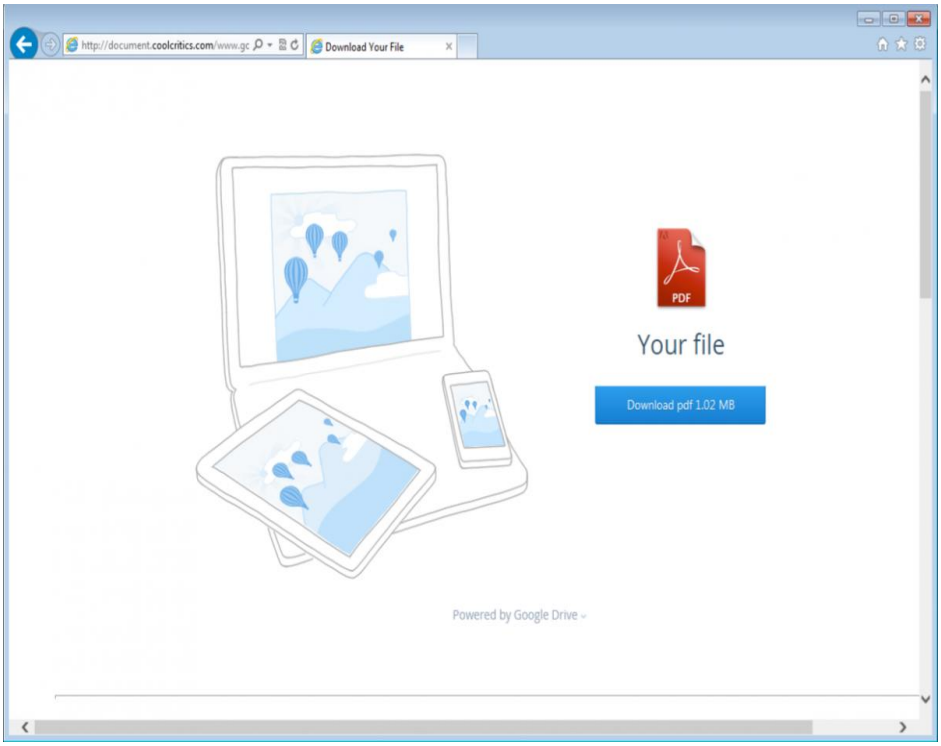
What Attachments?: Credential Phishing with Cloud-Based Documents

Credential phishing, the infamous technique used by malware campaigners, remains popular and is becoming even more attractive as Outlook Web Access credentials join other webmail accounts as frequent objects of abuse. As the trend toward cloud-based document usage becomes more widespread, perpetrators will further leverage this new behavior to attempt to lure users to their messages.

Proofpoint researchers recently analyzed a prime example of this kind of attack. The example also highlights a clever innovation on the part of perpetrators.

Among the most common e-mail-borne threats currently detected by Proofpoint are Google Apps credential phish. Hence, organizations that have adopted Google Apps for regular internal use are particularly susceptible to these types of clicks.

In this example, rather than taking a potential victim straight to a faux login page, a click of the link brings up a realistic Google docs shared document landing page.



The page is a perfect replica of an authentic Google page, with the exception of its mode of delivery: it is delivered via HTTP rather than HTTPS. When the recipient fails to notice this warning sign, he downloads the file. The Google login page then appears. Once again, it is almost identical to the authentic login page. A casual observer would not be able to tell the difference.

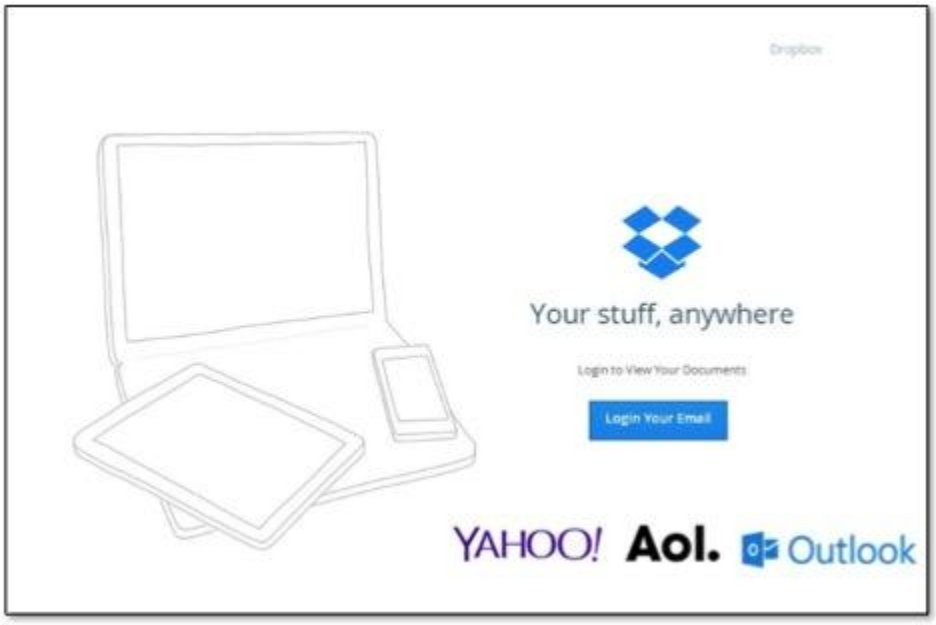
Note that the corrupt document also supports logins for other webmail services, such as Yahoo, Hotmail, AOL, as well as an "other" option to facilitate entering any corporate credentials, and thus enabling the attackers to grab additional logins.

As a rule, such a ruse would have been dropped after the credentials had been submitted. But in this case, the attackers follow through with the login by displaying an actual document.

Ultimately, this technique reduces the risk of a user realizing immediately that something is amiss and thus gives the attackers more time to make use of the stolen credentials.

Yet another advantage of credential phishing from compromised Google accounts is that with relative ease, credible, targeted phish are delivered to addresses scraped from a victim's list of contacts, and are used to populate the list of recipients for the next step of the campaign.

A similar method of attack employs a faux Dropbox document to capture credentials from the cloud-based document-sharing service. The login page gives the appearance of legitimacy:



Hacking by means of cloud-based document services and application accounts adds yet another layer of opportunity to create targeted and potentially effective and lucrative campaigns via valuable hacked e-mail accounts.

Inevitably, credential phishing with cloud-based documents will continue to grow in popularity as attackers leverage its advantages and attempt to stay ahead of defenses.

Threat News

Rocket Kitten Phishing With Woollen Goldfish and GHOLE

A cyberthreat group called *Rocket Kitten* is spear phishing in Israel and throughout Europe using "GHOLE" (malware) and "(Operation) Woolen-GoldFish" attacks hosted on Microsoft products.

So far Rocket Kitten has launched two campaigns.

GHOLE is believed to have been active since 2011.

According to a report by Trend Micro, the malicious activities of Rocket Kitten have been centered on different public and private Israeli and European organizations. They were mostly interested in the defense industry, the IT sector, government entities, and academic organizations, as was evidenced by malware samples from files with macros specific to the GHOLE malware campaign.

According to Bharat Mistry, a cybersecurity specialist with Trend Micro, a notable aspect of the attacks was the apparent absence of sophisticated skills required to carry them out. "Hackers no longer have to use handwritten scripts, but can use commercial, off-the-shelf tools." Ultimately, this made it more difficult to track the perpetrators. "It's harder to track because they wouldn't have had an online history. They won't have been associated with groups in the past. It's always difficult unless you see a pattern in the code."

Read on: http://www.scmagazineuk.com/rocket-kitten-phishing-with-woollen-goldfish-ghole/article/404693/.

Researchers Find Same RSA Encryption Key Used 28,000 Times

Imagine if the key to a house was shared with 28,000 other homes.

In essence, researchers with Royal Holloway of the University of London recently ascertained just that while scanning the Internet to see how many servers and devices are still vulnerable to the Web security hole known as *FREAK*.

The FREAK flaw was uncovered on March 3 and has the power to permit an attacker to weaken a connection that uses the SSL/TLS (Secure Sockets Layer/Transport Layer Security) cryptographic protocols. The flaw makes it much easier to break the encryption and view the traffic.

This was the latest in a string of flaws found over the last year in widely used open-source software.

As many as a quarter of the hosts on the Internet were vulnerable to FREAK. And researchers with Royal Holloway decided to investigate just what percentage still hadn't been fixed.

The project (which involved forcing a host to accept a 512-bit RSA key to secure a connection) yielded a surprising result: 9.7 percent of nearly 23 million hosts, or approximately 2.2 million, are still accepting 512-bit keys. (Encryption keys of that length have been considered insecure for more than a decade.)

Considering the grave nature of FREAK and that a few weeks have passed since the issue was made public, the number was shocking.

But perhaps most astonishingly, the researchers also found that many hosts (servers or other Internet-connected devices) share the same 512-bit public key.

Continue reading: http://www.pcworld.com/article/2897772/researchers-find-same-rsa-encryption-key-used-28000-times.html.

Microsoft Wants to Kill Passwords in Favor of Biometric Authentication in Windows 10

Microsoft is out to abolish passwords by providing an option to log into devices that use its upcoming Windows 10 OS. Called "Windows Hello", the biometric authentication technology will allow the use of fingerprints, faces, or irises to prevent unauthorized access to laptops, tablets, phones, and other devices.

Inconvenient and insecure, passwords nevertheless remain the primary method of protecting personal information.

Microsoft claims that biometric authentication is more secure than passwords. Biometric information is authenticated on the device itself and isn't stored on a remote server.

As reported by Microsoft, the biometric information is not used for network authentication, and users can opt out of biometric authentication if desired.

Microsoft's biometric authentication will initially support Intel's technology for authentication using face scans.

Continue reading: http://www.computerworld.com/article/2898654/microsoft-wants-to-kill-passwords-with-biometric-authentication-in-windows-10.html.

Dridex Banking Trojan Spreading Via Macros in XML Files

Dridex, the strain of banking malware that leverages macros in Microsoft Office to infect systems, operates by initially arriving on a user's computer as a malicious spam e-mail with a Microsoft Word or Excel document attached to the message. When the document is opened by a user, a macro embedded in the document surreptitiously triggers a download of the Dridex banking malware, and thus enables it to steal banking credentials with subsequent attempts to generate fraudulent financial transactions.

The hackers are still at it, now using XML files as a lure.

Researchers at Trustwave recently announced that several hundred messages had been "corralled" last month for attempts at exploiting users' trust in Office documents. It is obvious that these attempts were made to convince users to enable macros and thus download the banking malware onto their machines.

Passed off as remittance advice or payment notifications, the fraudulent XML files are strategically positioned to dupe users and thus sway them into executing the malicious code.

Read on: https://threatpost.com/dridex-banking-trojan-spreading-via-macros-in-xml-files/111503.

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 share 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.

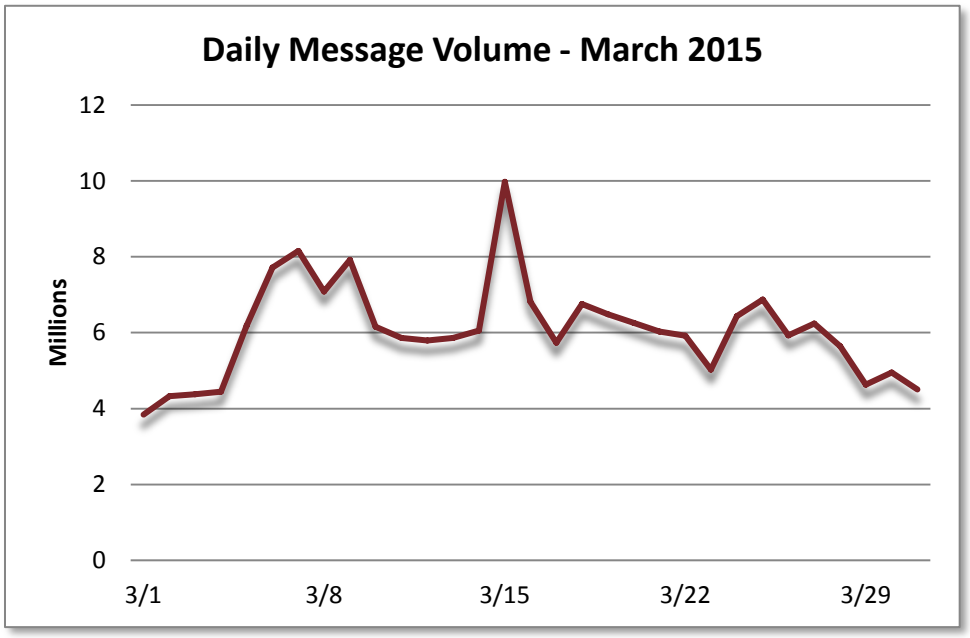
March's daily spam volume depicted more of the same drama of highs and lows observed of late. Beginning slightly below 4 million and climbing to above 8 million, the first week closed with a dip to just above 7 million.

Week two began with an almost immediate ascent back to 8 million, followed by a plunge to 6 million ensued. And then it plateaued.

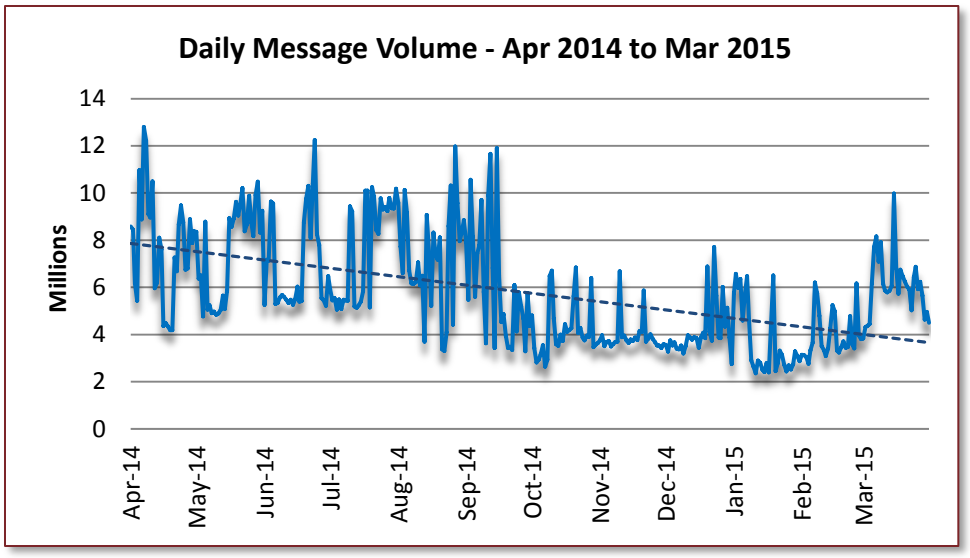
A sudden burst of activity to 10 million underscored the start of the third week. Thereafter, a sharp drop back to 6 million occurred.

Volumes fluctuated mildly throughout the remainder of the month.

The month closed at 4.5 million.



By comparison, February-over-March demonstrated the most significant increase in the volume of spam since December 2013 (54.37%). The year-over-year spam tally decreased by 41.04%.



Spam Sources by Region and Country

The EU fought its way to the top of the heap in March while the USA retained its second-place stronghold. Rising to the occasion to capture third was Russia, and reentering the scene, for the first time in a year, was India. India nabbed fourth while China found its way back into fifth.

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

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

The table below details the percentage of total spam volume for the February 2015 and March 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 30.89%, the EU generated the majority of the world's spam. The remaining four countries in the top five slots were collectively responsible for 23.02%—below the output of the EU.

February 2015			March 2015		
1	EU	35.30%	**1**	EU	30.89%
2	USA	6.67%	**2**	USA	9.75%
3	Vietnam	3.64%	**3**	Russia	5.24%
4	Argentina	2.85%	**4**	India	4.97%
5	Russia	2.46%	**5**	China	3.06%

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

February 2015			March 2015		
1	Germany	4.45%	**1**	France	3.56%
2	Spain	4.10%	**2**	Italy	3.28%
3	Italy	3.48%	**3**	Germany	3.19%
4	Romania	2.21%	**4**	Spain	2.54%
5	Bulgaria	1.97%	**5**	UK	1.62%

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

