INTERNET CRIME COMPLAINT CENTER'S (IC3) SCAM ALERTS NOVEMBER 25, 2011

This report, which is based upon information from law enforcement and complaints submitted to the IC3, details recent cyber crime trends and new twists to previously-existing cyber scams.

VICTIMS OF THE TECH SUPPORT SCAM ARE DEFRAUDED A SECOND TIME

The IC3 has produced Scam Alerts advising the public of an ongoing telephone scam in which callers purport to be an employee of a major software company. The callers have very strong accents, most referred to as "Indian." The callers report the users' computers are sending error messages and a virus has been detected. The victims are convinced to allow the caller remote access to their computer. As the victims' computers are searched, the caller points out infected files. The victims are advised that the virus can be removed for a fee and are asked to provide their credit card information. Whether the users pay for the removal of the virus or not, many reported difficulties with their computers afterwards.

The subjects of this scheme have devised yet another avenue to further defraud victims. Fraudsters are now calling those who had recently purchased software and offering them a refund within three to four months of the purchase. The callers are still described as having "a strong Indian accent." In some cases, the victims were asked if they were satisfied with the service they received. When the response was negative the caller offered a refund. Other victims were told the company was going out of business and therefore the victim was due a refund. Some were advised they needed to complete a form, at which time the caller asked for remote access to assist in the completion of the form. The caller said the fastest method for a refund was to use the card from the original purchase and wire the money. At this point, the caller helped the victims open an account via a wire transfer company to receive their refund. The victims later discovered funds were taken from their accounts and wired to India..

BANKING TROJAN NOW CIRCULATING OVERSEAS COULD SOON REACH U.S.
SCMagazine featured the following article on September 6, 2013:

http://www.scmagazine.com/banking-trojan-now-circulating-overseas-could-soon-reach-us/article/310632/?DCMP=EMC-SCUS_Newswire

The Hesperbot trojan has been distributed via sophisticated phishing emails.

Researchers at IT security company ESET have discovered a banking trojan that is targeting users who bank online in the Czech Republic, Turkey, Portugal and, most recently, the United Kingdom.

Stephen Cobb, ESET's security evangelist, told SCMagazine.com on Friday that the campaign to infect computer and mobile devices resembles a "full court press" for online banking information, and that the end goal is to get money out of accounts.

Although the trojan - known as Hesperbot - has remained a predominately international threat, Cobb said that he believes the "sophisticated" malware is only being tested at the moment – and that "it's a possibility this can be tested out in America."

The trojan is predominately infecting users through what Cobb said are deceptive phishing emails. The Czech Republic email, which claims to come from the Czech Postal Service, alerts recipients that they have a parcel and provides a link to track the package.

Cobb said that those who click on the link will unknowingly begin downloading malicious code to their computer all while being distracted by a realistic looking Czech Postal Service website that pops up in their browser.

Some of the malicious modules loaded into the computer to capture banking information include web-injects, keyloggers and form-grabbers, Cobb said, adding that users are also prompted via the faux website to enter their mobile number.

Consequently, those who enter their mobile number will receive an SMS text message containing an app that, when downloaded, infects the mobile and provides the "bad guys" with a means of circumventing two-factor authentication required by many European banks, Cobb said. Android, Symbian and BlackBerry devices have been targeted.

"We've not yet seen any attribution indicators at this point," said Cobb. "But we're not looking to attribute right away - we're looking to see what the code does to make sure we can defend against it." He added that researchers see Hesperbot as similar, yet more sophisticated, than similar trojans such as SpyEye and Zeus.

"The big picture to me is that this is proof that banking trojans have a lot of life left in them," Cobb said. "This is a whole new banking trojan. While it's got a lot of features of the others, it's not reusing code. It's built from the ground up."

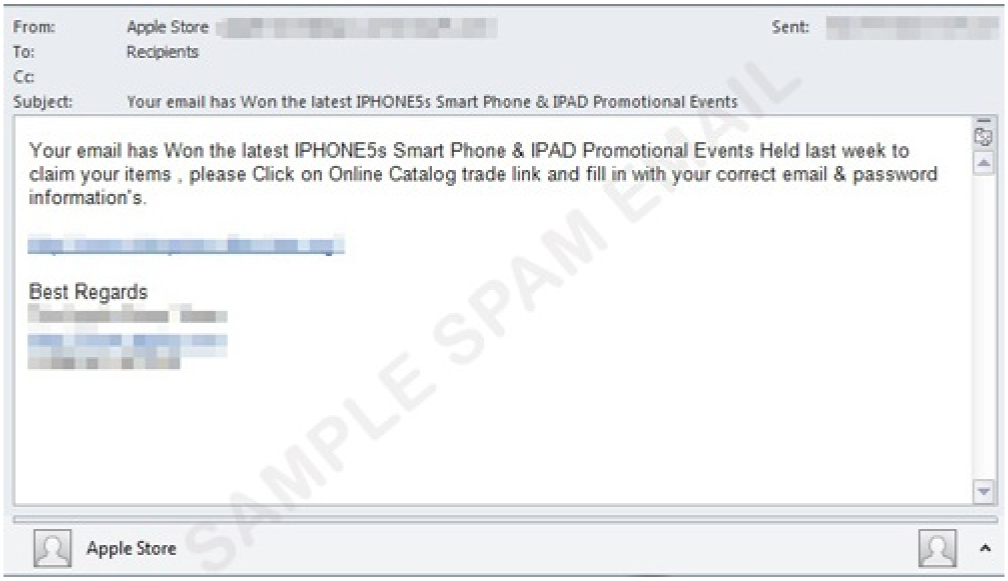
He added that clicking links in emails is risky and advised users to visit websites via the web address bar in their web browsers. Make sure your anti-virus is active and up to date, too, he added.

IPHONE 5S PHISHING MAIL ARRIVES IN TIME FOR LAUNCH

Towerwall Security posted the following on September 10, 2013:

While millions of mobile users are anticipating the launch of the new iPhone (5S and 5C), cybercriminals are already making their move to distribute spam that promise to give away the said devices for free, in the guise of a contest.

We saw samples of spammed messages that attempted to spoof an Apple Store email notification. The said message informs recipients that they won the latest iPhone 5S mobile phones and iPad.



From: Apple Store [redacted] Sent: [redacted]
To: Recipients
Cc:
Subject: Your email has Won the latest IPHONE5s Smart Phone & IPAD Promotional Events

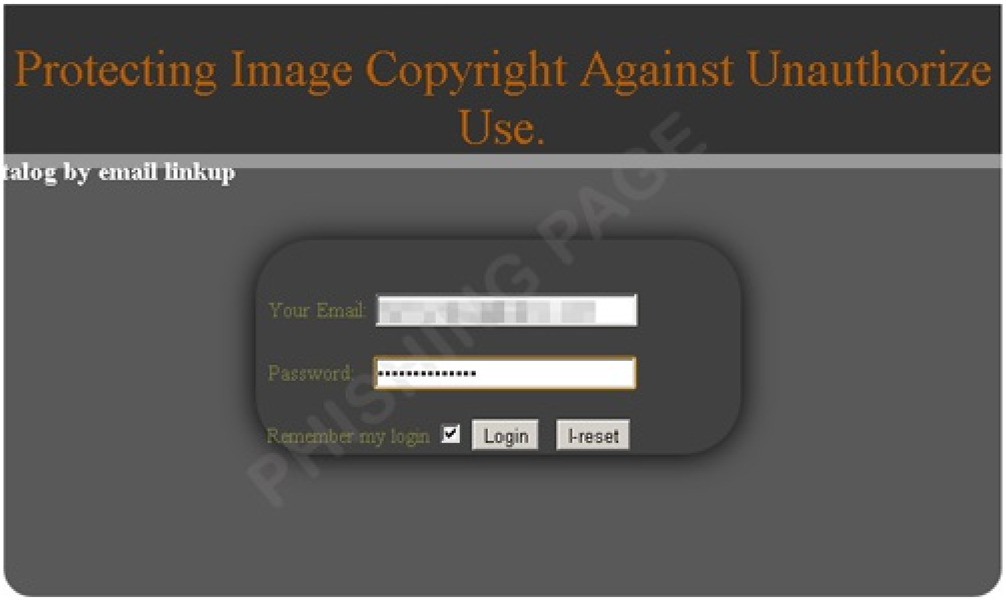
Your email has Won the latest IPHONE5s Smart Phone & IPAD Promotional Events Held last week to claim your items , please Click on Online Catalog trade link and fill in with your correct email & password information's.

[redacted]

Best Regards
[redacted]

Figure 1. Fake Apple email

To get these prizes, they are asked to go to a specific website and disclose their email address and password. This will obviously result in your credentials ending up in the hands of cybercriminals.



Protecting Image Copyright Against Unauthorize Use.

talog by email linkup

Your Email: [redacted]

Password: ••••••••••••••

Remember my login ☑

Figure 2. Phishing page

The content of the message and the sender's email address are obviously fake. However, its combination of perfect timing plus popular social engineering hook may cause users to fall into the spammers trap. The most important thing to know is: "if it's too good to be true, it probably is".

Feedback provided by the Smart Protection Network indicates that this mail is particularly effective in targeting Southeast Asian users:

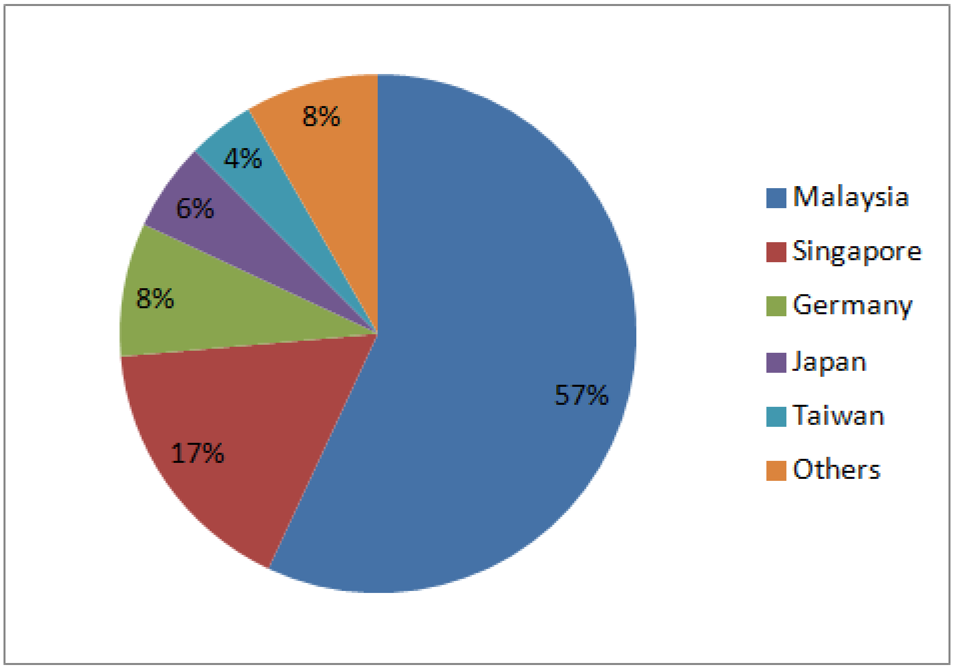


Figure 3. Most affected countries

Trend Micro blocks the said email message and blocks access to the phishing site.

STUDY: MEDICAL ID THEFT VICTIMS INCREASINGLY REPORT SPOOFED SITES AND PHISHING AS CAUSE OF FRAUD
SCmagazine.com posted the following on September 12, 2013:

As the number of individuals impacted by medical identity theft continues to climb, so does the number of victims fooled by spurious emails and websites designed to purloin their sensitive information, a study finds.

According to the "2013 Survey on Medical Identity Theft," the number of people who've fallen victim to this type of fraud has increased by 19 percent since last year, accounting for more than 1.8 million victims in 2013.

More than 300,000 new medical identity theft cases cropped up during the one-year period, the study found. The survey was conducted by the Ponemon Institute and sponsored by the Medical Identity Fraud Alliance (MIFA) and data breach prevention firm ID Experts.

The study, in its fourth year, surveyed nearly 800 adults in the U.S. who self-reported that they, or their close family members, were victims of medical identity theft.

Along with the rise in medical identity fraud, experts also saw a significant uptick in dubious websites being erected by saboteurs and spam emails being sent - all with the intent of tricking individuals into giving up their medical information.

Between 2012 and 2013, the percentage of medical identity theft victims reporting spoofed websites and phishing emails as the likely cause of their troubles doubled. This year, eight percent of respondents cited the cyber schemes as the cause of their issues, while only four percent of victims reported the same in 2012.

In the report, medical identity theft was defined as a person using an individual's name or personal identity "to fraudulently receive medical service, prescription drugs and goods, including attempts to commit fraudulent billing."

Larry Ponemon, chairman and founder of the Ponemon Institute, told SCMagazine.com earlier this week that in this study, and in other Ponemon studies, the frequency of spear phishing targeting medical identity theft victims has gone up.

Furthermore, spear phishing, attempts to infiltrate an individual's network or steal their data by crafting a targeted ruse they are likely to open via email, is likely under-reported among medical identity theft victims, Ponemon added.

"A lot of people aren't even aware that they have fallen for a phishing scam because they were so sophisticated," he said. "The ability to record it is difficult because people aren't even aware that it's happened to them."

In the study, the groups also found that seven percent of medical identity theft victims believed a data breach suffered by their health care provider, insurer or related organizations, was the cause of fraud. Last year, six percent of respondents cited those reasons as the cause.

NEW VARIANT OF ANDROID RANSOMWARE "FAKE DEFENDER" SURFACES

SCmagazine.com posted the following on September 13, 2013:

Researchers believe a spam campaign is spreading a new variant of mobile ransomware.

Malware called "Fake Defender," was first discovered in June, but security firm Symantec has now detected that the malware's authors are using a different ruse to target Android users, primarily in Russia.

The malicious application, detected as fakedefender.B., is designed to look like the official application for an adult video website, a Wednesday blog post by Symantec researcher Roberto Sponchioni said. But once users install the app, messages warn them to run an antivirus scan that is supposedly Avast AV.

Once the spurious AV scan is finished, the user's phone is locked for their "protection," and the app asks for a ransom payment of $100 via a prepaid MoneyPak card.

DARKLEECH SAYS HELLO

Fireye.com posted the following on September 14, 2013:

There's never a dull day at FireEye - even on the weekends. At approximately 7:29 AM PDT today, we were notified by several security researchers that a fireeye[.]com/careers HR link was inadvertently serving up a drive-by download exploit. Our internal security, IT operations team, and third-party partners quickly researched and discovered that the malicious code was not hosted directly on any FireEye web infrastructure, but rather, it was hosted on a third-party advertiser (aka "malvertisement") that was linked via one of our third-party web services. The team then responded and immediately removed links to the malicious code in conjunction with our partners in order to protect our website users. More information on this third-party compromise (of video.js) can be found at hxxps://twitter.com/heff.

Technical Details

The full redirect looked like this:

```
hxxp://www[.]fireeye[.]com/careers/
(redirect to) -> hxxp://xxx[.]xxxxxxxx[.]com/career/
CareerHome.action?clientId=8aa00506326e915601326f65b82e1fcb
(calls) -> hxxp://vjs[.]zencdn[.]net/c/video.js (VULNERABLE JAVASCRIPT)
(calls) -> hxxp://cdn[.]adsbarscipt[.]com/links/jump/ (MALVERTISEMENT)
(calls) -> hxxp://209[.]239[.]127[.]185/591918d6c2e8ce3f53ed8b93fb0735cd
/face-book.php (EXPLOIT URL)
(drops) -> MD5: 01771c3500a5b1543f4fb43945337c7d
(Update_flash_player.exe)
```

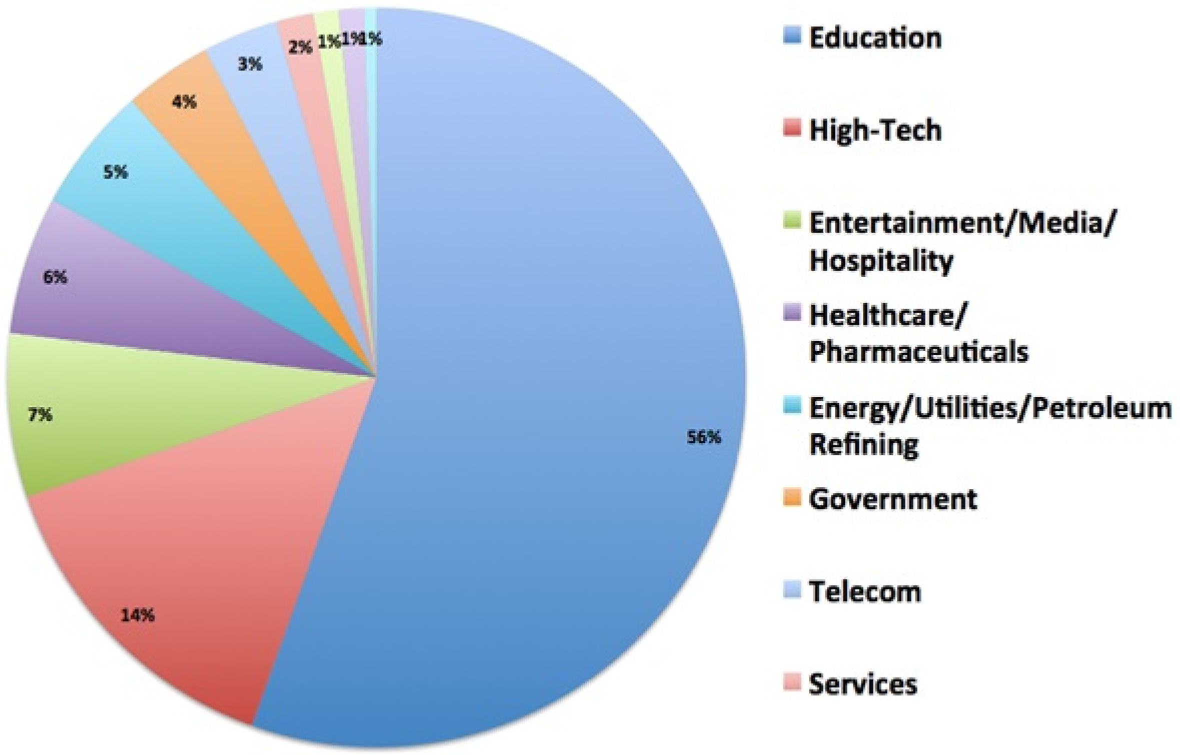
So what was this, anyway?

It turns out, this attack was not targeted and it was not a watering hole attack. Instead, this campaign appears to be a recent wave of the Darkleech malware campaign, where third-party Horde/IMP Plesk Webmail servers were vulnerable to attack and used to serve up Java exploits that ultimately drop yet another ransomware named Reveton (similar to Urausy) - yet other AV engines report it as a Zeus Bot (Zbot) variant.

Do FireEye products detect this attack?

Yes, the initial infection vector, payload, and corresponding Reveton callbacks were fully detected across all FireEye products prior to this incident being reported to us. In fact, this particular Reveton sample has been reported by approximately 49 of our worldwide customers, so far. Further intelligence about this threat is listed below:

- DTI Statistics for MD5: 01771c3500a5b1543f4fb43945337c7d
- MD5 first seen by our customers: 2013-09-14 07:12:40 UTC
- Number of unique worldwide FireEye Web MPS detections: 188+
- Number of unique FireEye Web MPS customers reported/alerted on this sample: 49+
- Number of industries affected: 12+



Lastly, FireEye acknowledges and thanks security researchers Inaki Rodriguez and Stephanus J Alex Taidri for bringing this issue to our attention.