INTERNET CRIME COMPLAINT CENTER'S (IC3)
SCAM ALERTS
AUGUST 13, 2013

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.

SPAM CONTINUING TO CAPITALIZE ON THE FBI'S NAME

The IC3 continues to receive reports of spam e-mails that use FBI officials' names and titles in online fraud schemes. Although there are different types and variations of these schemes, the recipients are typically notified that they are a beneficiary of a large sum of money. The latest round of spam e-mails use the name of James Comey, newly confirmed FBI Director.

The IC3 has posted multiple PSAs since July 2004 that warn consumers to beware of e-mails that use the FBI's name. Some messages can contain malicious software or malware. To learn more, go to: https://www.ic3.gov/media/2011/110809.aspx.

DHS NOTES RISE IN BRUTE-FORCE ATTACKS AGAINST NATURAL GAS COMPANIES

SCMagazine featured the following article on July 1, 2013

A subgroup of the U.S. Department of Homeland Security is warning companies that the energy sector has increasingly been targeted by brute-force attacks.

Hackers using some 50 IP addresses have attempted to infiltrate the process control networks belonging to natural gas companies, according to a recent newsletter (PDF) from the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

The campaign leveraged brute-force attacks – where saboteurs routinely run through a list of passwords or characters to gain access – against mostly companies in the Midwest and Great Plains that operate gas compressor stations, from February 22 through March 8. None of the attacks were successful, however.

The newsletter also said that between October and May, ICS-CERT responded to more than 200 incidents targeting the critical infrastructure sector, and more than half the incidents, 53 percent, occurred against energy companies.

In most cases, attackers used watering-hole attacks, where hackers infect websites frequently visited by their targets, as well as SQL injection and spear phishing attacks (targeted email ruses designed to get victims to click malicious links or attachments).

Lila Kee, a member of the North American Energy Standards Board, which promotes security standards for the natural gas and electric industry, told SCMagazine.com on Monday that the energy sector has likely been targeted more than other critical infrastructure operators because of the widespread impact a successful attack could have on the country.

"If you look at what can cause the most devastation if there was a successful attack, the devastation could be much greater than in some of those other critical infrastructure [sectors]," Kee said.

While the reports earlier this year from gas compressor stations were a "success story" – showing how the government and private sector can partner to better mitigate risks – Kee also said that increased attacks suggest a need for security standards that are specific to industries within the critical infrastructure sector, which supports the country's vital operations, such as gas production, water, transportation and financial services.

"We want to be able to respond to attacks as quickly as possible, but we also want to make sure we put measures in place to prevent these attacks," Kee said, adding that standards that are "very specific to the wholesale electric industry" were necessary to thwart future campaigns.

ATTACKERS USE SKYPE, OTHER IM APPS TO SPREAD LIFTOH TROJAN
SC Magazine featured the following article on June 1, 2013

Users receiving shortened URLs in Skype instant messages, or similar IM platforms, should be wary of a new trojan, called Liftoh.

So far, it has primarily infected users in Latin America, said Rodrigo Calvo, a researcher at Symantec.

When targeted, victims receive a message in Spanish containing a shortened URL. The messages appear as if they are coming from someone on the user's Skype contact list who is linking to a photo. If clicked, the link redirects users to 4shared.com, which is hosting a URL, which initiates a weaponized zip file containing Liftoh. The trojan is capable of downloading additional malware.

The malicious URLs have been clicked on more than 170,000 times, according to Symantec.

NEWLY LAUNCHED UNDERGROUND MARKET SERVICE HARVESTS MOBILE PHONE NUMBERS ON DEMAND
Webroot.com featured the following article on July 4, 2013

In May of 2012, we highlighted the increasing public availability of managed SMS spam services that can send hundreds of thousands of SMS messages across multiple verticals. These services are assisted through the use of proprietary or **publicly obtainable phone number harvesting and verifying DIY applications.**

In this post, I'll profile one of the most recently advertised managed mobile phone number harvesting service which allows full customization of the harvesting criteria based on the specific requirements of the customer.

More details:

Sample screenshot representing the way the harvested data could be presented:

	A	B	C
1	7929	ОАО "Мегафон" Столичный филиал	Москва
2	7911	ОАО "Мобильные Телесистемы"	Санкт-Петербург
3	7911	ОАО "Мобильные Телесистемы"	Калининградская область
4	7902	ЗАО "Ярославль-GSM"	Ярославская область
5	7911	ОАО "Мобильные Телесистемы"	Санкт-Петербург
6	7925	ОАО "Мегафон" Столичный филиал	Москва
7	7952	ОАО "Санкт-Петербург Телеком"	Санкт-Петербург
8	7904	ОАО "Санкт-Петербург Телеком"	Санкт-Петербург
9	7910	ОАО "Мобильные Телесистемы"	Москва
10	7916	ОАО "Мобильные Телесистемы"	Москва
11	7917	ОАО "Мобильные Телесистемы"	Москва
12	7961	ОАО "Вымпел-Коммуникации"	Ярославская область
13	7915	ОАО "Мобильные Телесистемы"	Ярославская область
14	7927	ОАО "Мегафон" Поволжский филиал	Республика Татарстан
15	7987	ОАО "Мобильные Телесистемы"	Чувашская Республика
16	7953	ОАО "Санкт-Петербург Телеком" Петрозаводск	Республика Карелия
17	7910	ОАО "Мобильные Телесистемы"	Ярославская область
18	7902	ЗАО "Ярославль-GSM"	Ярославская область
19	7937	ОАО "Мегафон" Поволжский филиал	Республика Башкортостан
20	7911	ОАО "Мобильные Телесистемы"	Санкт-Петербург
21	7910	ОАО "Мобильные Телесистемы"	Ярославская область
22	7915	ОАО "Мобильные Телесистемы"	Ярославская область
23	7985	ОАО "Мобильные Телесистемы"	Москва
24	7950	ОАО "Санкт-Петербург Телеком"	Санкт-Петербург
25	7927	ОАО "Мегафон" Поволжский филиал	Республика Башкортостан

The default harvesting criteria consists of the following options: - user ID on the Web site from where the mobile phone number was originally harvested - name/nickname - city -

education background - work position - contact details (as provided) - ICQ and Skype

Custom harvesting capabilities: - harvesting based on regions, cities, type of companies or E-shops - age, sex, interests, work positions - 100% custom harvesting based on a potential customer's preferences

It's worth emphasizing on the fact that the service explicitly points out the time frame required for the harvesting to take place: - from a 1000 to 35,000 harvested phone numbers based on criteria - 1 to 12 hours - from 50,000 harvested numbers and more based on criteria – 72 to 86 hours

The accepted payment method is WebMoney. Next to the actual harvesting of mobile phone numbers on demand, the vendor is also 'vertically integrating' within the marketplace by also offering phone number verification services as well as actual SMS spamming/SMS based TDoS (telephony denial of service attack) services.

We expect to continue observing an increase in vendors offering cybercrime-as-a-service solutions with vertical market integration in mind, in an attempt by the cybercriminals operating them to occupy an even bigger market share within the TDoS and the SMS spam market segments.

STYX EXPLOIT PACK: DOMO ARIGATO, PC ROBOTO
Krebsonsecurity.com featured the following article on July 08, 2013

Not long ago, miscreants who wanted to buy an exploit kit — automated software that helps booby-trap hacked sites to deploy malicious code – had to be fairly well-connected, or at least have access to semi-private underground forums. These days, some exploit kit makers are brazenly advertising and offering their services out in the open, marketing their wares as browser vulnerability "stress-test platforms."

Styx Pack victims, by browser and OS version

Aptly named after the river in Greek mythology that separates mere mortals from the underworld, the **Styx** exploit pack is a high-end software package that is made for the underground but marketed and serviced at the public styx-crypt[dot]com. The purveyors of this malware-as-a-service also have made a 24 hour virtual help desk available to paying customers.

Styx customers might expect such niceties for the **$3,000 price tag that accompanies this kit**. A source with access to one Styx kit exploit panel that was apparently licensed by a team of bad guys shared a glimpse into their operations and the workings of this relatively slick crimeware offering.

The Styx panel I examined is set up for use by a dozen separate user accounts, each of which appears to be leveraging the pack to load malware components that target different moneymaking schemes. The account named "admin," for example, is spreading an executable file that tries to install the Reveton ransomware.

Other user accounts appear to be targeting victims in specific countries. For example, the user accounts "IT" and "IT2" are pushing variants of the ZeuS banking trojan, and according to this Styx panel's statistics page, Italy was by far the largest source of traffic to the malicious domains used by these two accounts. Additional apparently country-focused accounts included "NL," AUSS," and "Adultamer" ("amer" is a derisive Russian slur used to describe Americans).

ZeuS Trojan variants targeted at Italian victims were detected by fewer than 5 out 17 antivirus tools. An exploit kit — also called an "exploit pack" (Styx is marketed as "Styx Pack") is a software toolkit that gets injected into hacked or malicious sites, allowing the attacker to foist a kitchen sink full of browser exploits on visitors. Those visiting such sites with outdated browser plugins may have malware silently installed.

Unlike other kits, Styx doesn't give a detailed breakdown of the exploits used in the panel. Rather, the panel I looked at referred to its bundled exploits by simple two-digit numbers. This particular Styx installation used just four browser exploits, all but one of which targets recent vulnerabilities in Java. The kit referred to each exploit merely by the numbers 11, 12, 13 and 32.

According to the considerable legwork done by Kafeine, a security blogger who digs deeply into exploit kit activity, Styx Kit exploit #11 is likely to be CVE-2013-1493, a critical flaw in a Java browser plugin that Java maker **Oracle** fixed with an emergency patch in March 2013. Exploit 12 is almost certainly CVE-2013-2423, another critical Java bug that Oracle patched in April 2013. In an instant message chat, Kafeine says exploit #13 is probably CVE-2013-0422, a critical Java vulnerability that was patched in January 2013. The final exploit used by the kit I examined, number 32, maps to CVE-2011-3402, the same Microsoft Windows font flaw exploited by the Duqu Trojan.

The Styx stats page reports that the hacked and malicious sites used by this kit have been able to infect roughly one out of every 10 users who visited the sites. This particular Styx

installation was set up on June 24, 2013, and since that time it has infected approximately 13,300 Windows PCs — all via just those four vulnerabilities (but mostly the Java bugs).

One very interesting pattern I observed in poking at this exploit pack — and 0thers recently — is the decreasing prevalence or complete absence of reported infections from **Google Chrome** users, and to a lesser extent users of recent versions of **Mozilla Firefox**. As we can see from the graphic at the top of this blog post, users browsing with Microsoft's **Internet Explorer** made up the lion's share of victims.

This Styx installation reports installing malware on systems of just a handful of Firefox users, and against **not a single Chrome user**. In fact, the author of this kit freely states in a Q&A from an underground forum sales thread that his kit doesn't even work against Chrome. For a complete breakdown of victims by browser and operating system, see this graphic.

Kafeine said he, too, has noticed a pronounced shift in the browser breakdowns from different exploit kits. "Not many exploit kits [perform] very well against Chrome," Kafeine said, noting that both Chrome and Firefox both now include integrated PDF readers, and that exploits against Adobe's PDF reader have traditionally been a key contributor to exploit kit infection statistics.

Kafeine said one malware gang whose work he has followed — an organized crime crew that uses the Gameover ZeuS variant — doesn't even attempt to infect Chrome users who wander into its malware traps. Instead, those users are hit with a social engineering attack that tries to trick them into installing the malware by disguising it as a Chrome browser update.

"Those users are automatically redirected to a fake Chrome update page," Kafeine said.

UK ROYAL BIRTH BEING USED TO DISSEMINATE MALWARE AND FRAUD
The following is a Cyber Internet Security (CIS) Cyber Alert released on July 25, 2013

The birth of Prince George of Cambridge to Prince William, Duke of Cambridge and Catherine, Duchess of Cambridge, on 22 July 2013, creates an opportunity for new and recycled Internet scams. Major events such as this tend to attract malicious individuals who use the event for their gain.

Internet watch groups and cyber security experts have already identified multiple fake domains/websites and spam taking advantage of the birth of the new prince. Based on previous royal family events, more spam and fraud will likely follow in the coming days. Internet users need to apply a critical eye and conduct due diligence before clicking links, visiting websites, or making purchases.