INTERNET CRIME COMPLAINT CENTER'S (IC3)
SCAM ALERTS
MARCH 21, 2014

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.

419 SCAM EXPLOITING IC3'S NAME AND ONE OF CYBER'S MOST WANTED

The IC3 has received reports of unsolicited emails claiming recipients were entitled to compensation from the IC3 through confiscated assets of one of Cyber's most wanted criminals, Alexandr Sergeyevich Bobnev. The emails were purportedly sent from a law firm and requested the recipient contact them to receive, complete, and submit release forms necessary to claim $480,000,000 in compensation.

Recipients were provided a case identification number, file number, compensation amount, dates, and other "official" information. The company's name listed in the payout and the law firm's name were used in other fraudulent banking scams.

FRAUDULENT ON-LINE ADVERTISEMENTS OF HUMAN HAIR COINCIDE WITH ON-LINE RETAIL FRAUD

The demand for long hair, new hair styles, or hair to conceal a medical condition associated with hair loss is nothing new; however, it does appear the exploitation of human hair is on the rise. Human hair is sometimes preferred by consumers over synthetic hair due to the natural look, feel, styling versatility, and longevity. Based on analysis of recent targets, it appears there is a fairly consistent overlap in the sale of human hair on websites that also sell counterfeit wearing apparel commodities. A recent target domain was involved in the sale of counterfeit wedding dresses imported from China, as well as advertising human hair. This assessment identified 132 connected domain names referencing brand name shoes, bags, and dresses. An additional subject was also accused of selling fake hair, designer handbags, brand gym shoes, and boots. Additionally, a company in China, selling counterfeit brand name shoes, advertises Peruvian, Brazilian, Indian, and Malaysian virgin hair. Virgin hair refers to hair that is completely unprocessed and intact. To qualify as virgin hair, it must meet rigorous standards including; not been permed, dyed, colored, bleached, or chemically processed in any way. This also means it comes from a single donor, and all the cuticles are intact, running in the same direction. Usually, it also means that is has not been blow-dried, or exposed to harsh agents such as cigarette smoke and drugs. The hair is being advertised as human; however, consumers are receiving synthetic hair after paying a substantially higher price for this authentic commodity.

SC MAGAZINE POSTED THE FOLLOWING ON NOVEMBER 22, 2013:

http://www.scmagazine.com/firm-predicts-2014s-most-dangerous-malware-trends/article/322364/?DCMP=EMC-SCUS_Newswire&spMailingID=7442740&spUserID=NDg1NjI4MzU2MjIS1&spJobID=9965002 5&spReportId=OTk2NTAwMjUS1

FIRM PREDICTS 2014'S "MOST DANGEROUS" MALWARE TRENDS

As 2013 comes to a close, an anti-fraud company has begun warning enterprises about the most treacherous malware threats that are likely to strike in the coming year.

On Thursday, Trusteer, an IBM company, published its predictions on the five "most dangerous malware trends" practitioners and end-users should be aware of in 2014.

Threats that made the list were: source code leaks, which continue to hasten malware release cycles; saboteurs using "old school" techniques to bypass newer detection technologies; and the increased use of malware utilizing evasion tactics to stay off researchers' radars.

In addition, Trusteer predicted that fraudsters leveraging account takeovers via victims' devices, as opposed to from their own machines, should be top of mind. Notably, the firm also said that the use of mobile SMS-forwarding malware would become ubiquitous in 2014.

"The capability to forward mobile SMS messages will be a standard feature in virtually all major malware families with standalone SMS forwarding malware readily available," an infographic highlighting the findings said.

"Mobile SMS verification is rendered all but useless as an out-of-band authentication method. Furthermore, enterprises must be wary of the real potential for SMS communication compromise with the increasing popularity of BYOD," the firm advised.

On Friday, Amit Klein, CTO of the company, emailed SCMagazine.com and addressed some of the "old school" techniques he believes will be most dangerous in 2014.

"We increasingly see attacks by financial malware which prevents the victims from interacting with the genuine financial site, or reroutes such interaction away from the genuine site very early in the session," Klein said, naming man-in-the-browser (MitB) style HTML injection and pharming attacks – when the victim interacts with a "completely spoofed site," – as attack methods.

"…The upside for the attacker is that by preventing the interaction between the user and the site, the genuine site gets no wind of the attack (at least, of the phase of the attack involving the victim)," Klein continued.

In a blog post on the predictions, Klein further added that the trends showcase the resilient nature of cyber criminals faced with advanced security technologies.

"What's needed is a disruptive approach to security – an approach that addresses the root cause of infections and cyber crime," Klein said. "This approach will need to respond to new cyber crime techniques in real time, while also providing holistic protection."

SC MAGAZINE POSTED THE FOLLOWING ON NOVEMBER 19, 2013:

http://www.scmagazine.com/phony-anti-virus-programs-evade-detection-with-stolen-certificates/article/321734/?DCMP=EMC-SCUS_Newswire

PHONY ANTI-VIRUS PROGRAMS EVADE DETECTION WITH STOLEN CERTIFICATES

Malicious software disguised as phony anti-virus programs has been combated for half a decade, which is why attackers now are evading detection by using stolen digital certificates.

The researchers with anti-virus software company Bitdefender recently uncovered a batch of such samples, named Antivirus Security Pro, that have been tweaked to come with the digitally signed installer.

“More to the point, the installer file served via the internet is signed with a digital certificate issued for Ease Entertainment Services, LLC on November 22nd last year,” according to a post by Bogdan Botezatu, senior E-Threat analyst with Bitdefender. “The digital certificate is still valid (it has not been revoked yet). Most likely, it was stolen.”

The Bitdefender team alerted Ease Entertainment Services of the digital theft, so the certificate should be revoked soon, according to Botezatu, who explained that the criminals did not extend the validity of the time-stamp – it expires in November 2014 – because of how quickly compromised certificates are invalidated.

Antivirus Security Pro is a standard scam. Upon download, the bogus program scans systems and then falsely alerts users that their computers are infected with serious malware. Users are then required to pay for the full version in order to remove it.

“Modern operating systems treat digitally signed files differently when they attempt to perform system-wide modifications,” Botezatu wrote. “Prompts of unsigned applications trying to elevate their privileges attract much more user scrutiny than other prompts.”

For more information regarding online scams visit our Press Room page for the most current Public Service Announcements. https://www.ic3.gov/media/default.aspx