National Fraud Intelligence Bureau

Date Range: 02-08/09/2013
Date Disseminated: Sept 2013
Reference: CEFOSP09

Cyber Enabled Fraud: An Open Source Perspective

This report contains information for law enforcement, individuals, and / or organisations that may impact on an immediate basis and aims to be issued on a weekly basis. Longer term threats have can be found in the Cyber Enabled Fraud: Horizon Scanning document, which we aim to issue on a bi-weekly basis. We have included NFIB comments where appropriate; however we would appreciate hearing from you, particularly if you find this document useful and or wish to contribute.

The articles referred to can be viewed by clicking on the titles.

Purpose

The purpose of this report is to inform readers of the emerging and future cyber enabled fraud threat picture and technological developments potentially facing UK law enforcement and public/private sector bodies. The document should be used not only to raise awareness but also to inform disruption and prevention initiatives.

Much of the information contained within has been produced from a variety of open sources that are publicly available therefore this report is NOT PROTECTIVELY MARKED. NFIB accepts no responsibility for the accuracy of any of the open source reporting referred to in this report.

CORROBORATED THREATS

Dropsmacked and Boxed In: Understanding the New Threats in Online File Sharing

Usage of file synchronisation and sharing technology has quintupled from 2010 to 2012 and over 25% of IT workers now use an FSS technology to do their jobs, creating a number of new threats to information security. Hackers can create accounts for companies on the cloud service and from there upload and download data. Also, using malware called DropSmack, an attacker can sync files from home PCs onto computers on protected networks, and can even use that sync functionality to have Dropbox serve as the command and control for the malware itself.

NFIB Comment: The use of cloud storage by employees to store sensitive company data poses a major risk to UK businesses. The NFIB has received reporting regarding the hacking of cloud services and businesses should ensure that they have appropriate mechanisms in place to protect their information.

Fraud Schemes Targeting Small Merchants

A fraud indictment against five alleged cyber thieves behind global fraud schemes that compromised 160 million cardholders has shown that numerous smaller merchants were targeted for card data. The ability to target different types of entities and exploit information from those systems is allowing criminals to hit smaller targets, but over time gather a significant number of stolen [payments] cards to resell.

NFIB Comment: Small and Medium Enterprises (SMEs) are increasingly attractive targets for hackers as large companies take steps to protect their business from cyber attacks. This is corroborated in NFIB reporting where SME's are increasingly featuring in reporting.

New Online Banking Trojan 'Hesperbot' steals banking details and has a mobile malware element

A bank account-raiding Trojan called Hesperbot has infected computers in UK, Turkey, the Czech Republic and Portugal. The software is distributed via convincing-looking emails, which are dressed up as legit package tracking documents from postal companies or correspondence from an internet provider and other outfits which trick users into downloading and running a malicious Windows executable, named with a .pdf.exe file extension. Hesperbot can silently snoop on passwords by logging a user's keystrokes, take screenshots, record from a video camera if one is connected, intercept network traffic, and pipe all this snaffled data to the crooks' command server. The Trojan can also set up a hidden VNC service, allowing miscreants to remotely log in and take control of the computer. Victims are also persuaded to install the mobile malware component of Hesperbot on their Symbian, Blackberry or Android phone.

NFIB Comment: The relatively small number of victims reported to have fallen victim to this scam may reflect the difficulties that criminals face in using online banking details gained through these means. The possibility that a large dataset of online banking details derived from this will become available on the black market cannot be discounted.

Warning: A New DDoS-Fraud Link

DDoS attacks used as a distraction for a new, extremely effective account takeover scheme involving the takeover of a banking institution's payment switch which has hit several institutions in recent months and likely have led to millions of dollars worth of fraud.

NFIB Comment: The use of DDoS to disguise fraud attacks on the banking sector has previously been highlighted.

UNCORROBORATED THREATS

THESE ARE PROVIDED FOR INFORMATION AND PLANNING AS APPROPRIATE

Fake YouTube Site Strikes Visitors With Three-Staged Attack

Security researchers have discovered a malicious website posing as a legitimate YouTube page with a phony Flash Player update which shows malware laden porn videos, followed by a ransomware attack designed to extort money from victims, hijack a victim's system, and steal account credentials. Researchers at Malwarebytes noted that although all three of these tactics are widespread, their combination in this way is rare.

The Mysterious Mevade Malware

Fox-IT published evidence that the recent growth in the number of Tor users could be attributed to a botnet abusing the Tor network to hide its command and control server. The Mevade malware family downloaded a Tor component, possibly as a backup mechanism for its C&C communications. Feedback provided by the Smart Protection Network shows that the Mevade malware was, indeed, downloading a Tor module in the last weeks of August and early September. Tor can be used by bad actors to hide their C&C servers. One of the main actors is known as "Scorpion", another actor uses the nickname "Dekadent". Together, they are part of a well organized and probably well financed cybercrime gang. Mevade also has a backdoor component and communicates over SSH to remote hosts. Therefore, the risk for data theft is still very high.

NFIB Comment: The ability to hide Command and Control functions in the Tor network could increase a botnet's attack capabilities and duration.

Sham G20 Summit Email Carries "Split" Backdoor

A recent email purportedly from the event's planning team and refers to a "pre-summit meeting" is only the latest in these threats. The email arrives with a RAR attachment containing three files: one LNK file and two other binary files which are actually one file that was split into two so that they are not identified as a valid file. The LNK file contains custom commands that reconstruct the two separated binary files into one file and execute it. It communicates to its remote servers to execute malicious commands onto the infected system, and also downloads plugins, which will then execute various data-stealing behaviours such as screen capture and key logging.

Dirt Jumper DDoS Toolkit Gets Security Evasion Functionality

Attackers behind the DDoS attack toolkit called Dirt Jumper have added new functionality that can test a system in an attempt to slip malicious torrent packets past DDoS mitigation appliances. This could be just the first of many pieces of malware to attempt to incorporate these bypass techniques. Malware authors have made improvements to Dirt Jumper over the years and recently boosted the malware's internal engine and made improvements in how its command-and-control servers respond to analysts trying to probe them.

HANDLING INSTRUCTIONS

This report may be circulated in accordance with the protective security marking and caveats included within the report. The information contained in this report is supplied by the National Fraud Intelligence Bureau (NFIB) in confidence and may not be shared other than with the agreed readership/handling code without prior reference to the NFIB. Onward disclosure without prior authority may be unlawful, for example, under the Data Protection Act 1998.

This sheet must not be detached from the report to which they refer. This document is classified NOT PROTECTIVELY MARKED.

Protective Marking	NOT PROTECTIVELY MARKED
FOIA Exemption:	N
Suitable for Publication Scheme	N
Version:	1.0
Purpose	To provide a future looking assessment of open source information.
Owner	NFIB Deputy Director - Head of Intelligence & Interventions
Author	100411, Researcher, 99204a, Senior Analyst
Review By	Deputy Director John Unsworth
Date Created	11th September 2013

FEEDBACK
The NFIB welcomes feedback from our readers to evaluate the quality of our products through continuous improvement and to inform our priorities. Please would you complete the following NFIB feedback survey through: http://www.surveymonkey.com/s/AnalyticalProductsFeedback
This should take you no more than 2 minutes to complete. If you have other feedback or additional information that you would prefer to provide by email please send this to: NFIBfeedback@cityoflondon.pnn.police.uk