INTERNET CRIME COMPLAINT CENTER'S (IC3)
SCAM ALERTS
OCTOBER 23, 2012

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.

DATING EXTORTION SCAM

The IC3 has recently received reports regarding a scam that baits individuals into intimate online conversations and then extorting them for financial gain. The scam was initiated after the victims met someone online, such as on a dating site, and were asked to connect via a specific online social network. Shortly after, the conversations became sexual in nature. Later, victims received text messages, either containing their names, asking if it was them or containing a statement that indicated their names were posted on a particular website. The victims were provided a link to a page on the website that claimed they were a "cheater." Photos of the victims and their telephone numbers were also posted. There was an option to view and buy the posted conversations for $9. Victims were also given the option to have their names and conversations removed for $99. Some were even told that once the payment was made, the information would be removed within an hour and the website would not allow anyone to post anything pertaining to the victims' names again. However, reports do not indicate that the information was ever removed.

PAYDAY LOAN SCAMS

The IC3 has received thousands of complaints regarding pay day loan scams over the last three years and continues to see new variations of the scam. The scam involves victims who are relentlessly contacted, via the telephone, at their residences and places of employment. The subjects claim the victims are delinquent on a payday loan and must repay the loan to avoid legal consequences. The subjects use coercion techniques such as harassment, threats, and claims that they were representatives of government agencies and law firms. Only some of the victims have reported previously applying for a payday loan, others said they have never made such an application.

The subjects seem to have accurate information on the victims, including social security numbers, dates of birth, addresses, employer information, bank account numbers, names and telephone numbers of relatives and friends.

The subjects refuse to provide any details of the alleged payday loans and become abusive when questioned. Victims are threatened with legal actions, arrests and, in some cases, physical violence if they refuse to pay. Some have been told there was an outstanding warrant for their arrest. Many reported that subjects have also harassed their relatives, friends, and employers. In a couple of instances, the subjects came to the victims' places of employment and residences claiming to be process servers.

Over the last couple of months, the scam has evolved from just receiving telephone calls to also receiving official-looking emails purportedly from the United States Attorney. The emails reference the FBI, court proceedings, and serious allegations. Allegations include violation of federal banking regulations such as collateral check fraud, theft by deception, and fraudulently conducting electronic fund transfers. Recipients were instructed to contact the subject within 48 hours of receiving the email.

To educate consumers and reduce the number of victims of this scam, the IC3 has posted two Public Service Announcements (PSA) warning consumers. The first PSA was posted in December 2010 and the most recent was posted in February 2012. Both PSAs are available at https://www.ic3.gov/media/2012/120221.aspx and https://www.ic3.gov/media/2010/101201.aspx.

Dark Reading posted the following article on September 18, 2012:

NEW TDSS/TDL4 MALWARE INFECTS 46 OF FORTUNE 500

New Domain Generation Algorithm-Based Malware Claims At Least 250,000 Victims

A new iteration of TDSS/TDL4 malware has infected at least 250,000 victims, including 46 companies in the Fortune 500, researchers said Monday.

According to a new report on the TDSS/TDL4 malware published by security firm Damballa, the new attack is using domain generation algorithm (DGA)-based communication for command-and-control (C&C).

Used by Murofet, Sinowal and the recent Mac-based Flashback malware, DGA communications techniques are being used to successfully evade detection by blacklists, signature filters and static reputation systems, and to hide C&C infrastructure, Damballa reported.

TDSS/TDL4 is malware known to infect the master boot record (MBR) of computers, making it resistant to common practices in remediation. It has been described as the "indestructible" botnet, with the ability to act as a launch pad for other malware. At one point it was reported as having infected over 4.5 million victims.

A total of 85 hosting servers and 418 unique domains were identified as being related to the new TDSS/TDL4 threat, Damballa said. The top three hosting countries for the C&C servers are Russia (26 hosts), Romania (15 hosts) and the Netherlands (12 hosts).

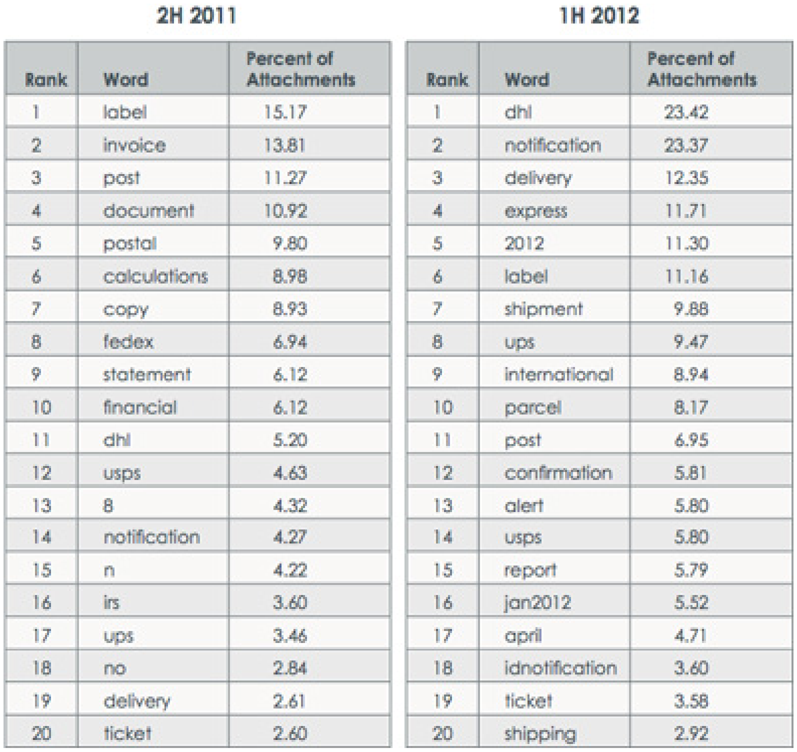
"By adding elusive DGA C&C capabilities to malware that already evades detection and circumvents best practices in remediation by infecting master boot records, TDL4 is becoming increasingly problematic," said Manos Antonakakis, director of academic sciences for Damballa.

"With its known ability to act as a launch pad for other malware and TDSS' history of sub-leasing access to their victims, these hidden infections in corporate networks go undetected for long periods of time," Antonakakis said.

Net-Security.org posted the following article on September 25, 2012:

TOP WORDS CYBER CRIMINALS USE IN FAKE EMAILS

The top words cybercriminals use create a sense of urgency, to trick unsuspecting recipients into downloading malicious files. The top word category used to evade traditional IT security defenses in email-based attacks relates to express shipping, according to FireEye.



2H 2011

Rank	Word	Percent of Attachments
1	label	15.17
2	invoice	13.81
3	post	11.27
4	document	10.92
5	postal	9.80
6	calculations	8.98
7	copy	8.93
8	fedex	6.94
9	statement	6.12
10	financial	6.12
11	dhl	5.20
12	usps	4.63
13	8	4.32
14	notification	4.27
15	n	4.22
16	irs	3.60
17	ups	3.46
18	no	2.84
19	delivery	2.61
20	ticket	2.60

1H 2012

Rank	Word	Percent of Attachments
1	dhl	23.42
2	notification	23.37
3	delivery	12.35
4	express	11.71
5	2012	11.30
6	label	11.16
7	shipment	9.88
8	ups	9.47
9	international	8.94
10	parcel	8.17
11	post	6.95
12	confirmation	5.81
13	alert	5.80
14	usps	5.80
15	report	5.79
16	jan2012	5.52
17	april	4.71
18	idnotification	3.60
19	ticket	3.58
20	shipping	2.92

Urgent terms such as "notification" and "alert" are included in about 10 percent of attacks. An example of a malicious attachment is "UPS-Delivery-Confirmation-Alert_April-2012.zip."

"Cybercriminals continue to evolve and refine their attack tactics to evade detection and use techniques that work. Spear phishing emails are on the rise because they work," said Ashar Aziz, founder and CEO, FireEye. "Signature-based detection is ineffective against these constantly changing advanced attacks, so IT security departments need to add a layer of advanced threat protection to their security defenses."

Cybercriminals also tend to use finance-related words, such as the names of financial institutions and an associated transaction such as "Lloyds TSB - Login Form.html," and tax-related words, such as "Tax_Refund.zip." Travel and billing words including "American Airlines Ticket" and "invoice" are also popular spear phishing email attachment key words.

Spear phishing emails are particularly effective as cybercriminals often use information from social networking sites to personalize emails and make them look mostly authentic. When unsuspecting users respond, they may inadvertently download malicious files or click on malicious links in the email, allowing criminal access to corporate networks and the potential exfiltration of intellectual property, customer information, and other valuable corporate assets.

FireEye highlights that cybercriminals primarily use zip files in order to hide malicious code, but also ranks additional file types, including PDFs and executable files.

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