FinCEN
FINANCIAL CRIMES ENFORCEMENT NETWORK

Executive Alert

INTELLIGENCE DIVISION

Date: December 2, 2014

Tor Darknet IP Addresses: Increasing Link to Cybercrime Against Financial Institutions

Our BSA analysis of 6048 IP addresses associated with the Tor darknet found that in the majority of the SAR filings, the underlying suspicious activity, most frequently account takeovers, might have been prevented if the filing institution had been aware that their network was being accessed via Tor IP addresses. Darknets are Internet based networks used to access content in a manner designed to obscure the identity of the user and his or her associated Internet activity.

This FinCEN Executive Alert to financial institutions is for informational purposes only, and does not request financial institutions to take any specific action. The information contained in this Executive Alert is intended to be shared with your institution's executives in BSA/AML compliance and Cyber Security.

Tor, Darknets, and Cybercrime

Darknets also known as cypherspace, the Deep web, or anonymous networks are Internet based networks that individuals use to access content in a manner designed to obscure the identity of the user and his or her associated Internet activity. Tor is the largest darknet with between 500,000 and a million users worldwide. Tor nodes are dedicated servers with an IP address that relay encrypted communications between users of the Tor darknet. They are readily identifiable through open source research.

- Tor has been associated with a variety of cybercrimes, including child pornography and darknet marketplaces for illicit goods and services.
- Some online businesses routinely detect IP addresses associated with Tor nodes and block these customers from accessing their services because they have determined that Tor activity often is connected to cybercrime.

Hidden Tor Connections Permeate SAR Filings

We conducted a BSA data search against a list of 6048 known Tor nodes covering the period from 8/2/2001 to 7/14/2014; this search yielded 975 hits across 318 unique documents. The transactions associated with these SARs totaled $23,888,549. Analysis of these documents found that few filers were aware of the connection to

Tor, that the bulk of these filings were related to cybercrime, and that Tor related filings were rapidly rising.

An analysis of these SARs revealed that:

- *Filers Unaware of the IP Association with Tor.* A keyword search of the narratives for "Tor" revealed that only 10 SARs referenced the Tor darknet. In two SARs, the filer filed because of a customer's use of Tor. Even in these, however, it is unclear if knowledge of this was immediate, or after the suspicious activity in question occurred.

- *Identity Theft and Account Takeover Often Cited.* Our analysis of the type of suspicious activity indicates that a majority of the SARs were filed for account takeover or identity theft. In addition, analysis of the SARs filed with the designation "Other" revealed that most were filed for "Account Takeover," and at least five additional SARs were filed incorrectly and should have been "Account Takeover".

Diversity of Filers						
FILER	Money Services Businesses	Depository Institutions - Banks	Broker Dealers	MSB - Prepaid Card Providers	Depository Institutions- Credit Unions	MSB - Virtual Currency Exchangers
SARS	138	133	27	15	3	2
%	43%	42%	8%	5%	1%	1%

Filers Awareness of IP Association		
FILER	Knew IPs were Tor-related	Did NOT know IPs were Tor-related
# of SARS	10	308
% of Filers	3%	97%

Types of Suspicious Activity in Tor-related SARs		
SUSPICIOUS ACTIVITY	# of SARs	Percentage
Other[1]	164	52%
Identity Theft	140	44%
Money Laundering	110	35%
Unusual use of money transfer(s)	78	25%
Account Takeover	77	24%
Unauthorized electronic intrusion / Computer Intrusion	13	4%
Provided questionable or false documentation	12	4%
Suspicious concerning the source of funds	11	3%
Two or more individuals working together	9	3%
Forgeries	8	3%
Transaction with no apparent economic, business, or lawful purpose	8	3%
Suspicious use of multiple accounts	6	2%

[1] A review of Suspicious Activity referred to as "Other" determined that the majority of these activities were associated with Account Takeover and/or Identity Theft.

Elder financial exploitation	4	1%
Embezzlement/theft/disappearance of funds	3	1%
Counterfeit Instrument	2	1%
Suspicious use of noncash monetary instruments	2	1%
Multiple individuals with same or similar identities	2	1%
Market manipulation	1	< 1%
Suspicious documents or ID presented	1	< 1%
Structuring	1	< 1%
Refused or avoided request for documentation	1	< 1%
Transaction out of pattern for customer	1	< 1%

- *SARs Referencing Tor Nodes Increasing Over Time*. Our analysis of the filing dates of SARs referencing known Tor nodes also reveals significant increases in filings over the period. From October 2007 to March 2013, filings increased by 50 percent. During the most recent period, March 1, 2013 to July 11, 2014, filings rose 100 percent.

Awareness May Be Key to Countering Tor related Cybercrime

Financial Institutions may benefit immediately from a heighted awareness of Tor nodes and incorporating this knowledge into their transaction monitoring efforts to prevent unauthorized intrusions and other cybercrime.

- Our narrative analysis of SARs related to account takeovers found that the unauthorized logins to customer accounts may have been prevented if the filing institution had been aware that the IP from which the login originated was associated with a known TOR node.

Please contact the FinCEN Resource Center at FRC@fincen.gov if you have any questions pertaining to this report. Please reference 250331/IFM in the subject line of the e-mail.