Homeland Security

National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)

CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE NOTE

May 8, 2018; 0900 EDT

CYBERCRIME AND THE DARKNET: EFFECTS ON CYBERSECURITY PRACTICES

KEY FINDINGS

Darknet platforms and their growing popularity present unique challenges to cybersecurity. Blocking all Darknet traffic is difficult and often unduly burdensome for many system operators. Command-and-Control (C2) servers hosted on the Darknet are difficult to uncover and shutdown, making the Darknet an attractive haven. The proliferation of stolen credentials on Dark Web markets leave systems vulnerable, even if systems have secure networks.

SCOPE NOTE: The Department of Homeland Security (DHS)/National Protection and Programs Directorate (NPPD)/Office of Cyber and Infrastructure Analysis (OCIA) produced this note as part of a series exploring the use of Darknet technologies by cybercriminals and is intended to inform cybersecurity professionals about the Darknet's impact on established cybersecurity practices. Source citations in this product limited to those that are publicly accessible to ensure the widest possible dissemination.

This product was coordinated with DHS/NPPD/Office of Infrastructure Protection/National Infrastructure Coordination Center, DHS/NPPD/Office of Cybersecurity and Communications/National Cybersecurity and Communications Integration Center, DHS/Transportation Security Agency/Office of Intelligence and Analysis, Cyber Threat Intelligence Integration Center, Central Intelligence Agency, Federal Bureau of Intelligence, and Sandia National Laboratories.

Background

Tor, often called The Onion Router, is a Darknet platform that anonymizes users' Internet Protocol (IP) addresses.[i] Tor is primarily used in two ways: to access the Open Web (the portion of the Web accessible with traditional Web Browsers) or to access the hidden services of the Dark Web (which is only accessible via Darknet platforms).[ii] In 2017, Tor use grew more than 50 percent, rising steadily from 2 million daily users at the end of 2016 to 3 million daily users by December 2017.[1] Tor and other Darknet platforms present unique challenges for cybersecurity because of the ways they route, anonymize, and encrypt network traffic.

Over-reliance on IP Address Filtering May Insufficiently Address Darknet Threats

Blocking traffic originating from specific IP addresses is a traditional cybersecurity technique, but Darknet platforms make the process more complicated.[2] Cybersecurity systems can flag and prevent traffic coming from malicious IPs (such as known bot IPs), but Darknet platforms automatically mask all originating IP addresses. System administrators therefore have to block all Darknet traffic. This could be ineffective, burdensome, and may also block legitimate privacy-conscious individuals. Additionally, Tor nodes are located all over the world, and Tor

[i] For more information, please see OCIA's June 2017 Critical Infrastructure and Resilience Note, *The Darknet and Dark Web: A Primer* (FOUO). https://hsin.dhs.gov/ci/iir/OCIA/OCIA%20Products%20DocLib%20HSIN/OCIA%20-%20The%20Darknet%20and%20Dark%20Web%20-%20A%20Primer%20(FOUO).pdf

[ii] The Tor Project estimates that less than five percent of Tor traffic is for Dark Web hidden services. The other 95% of traffic is directed to the Open Web. Tor Project. (2017). "TorMetrics: Clients." http://metrics.torproject.org. Accessed 7 December 7, 2017.

traffic may therefore be routed through foreign countries.[3] Systems and websites that block foreign IP addresses might deny access to domestic users if their traffic is routed through foreign countries.[4]

OCIA assesses that IP filtering will likely become less practical if Tor use continues to grow. Blocking legitimate traffic might not be a significant concern at 3 million daily Tor users, but IP filtering would likely become impractical for many organizations if Tor continues to grow to 100 million or a billion users; too many legitimate users would be denied access.

IP Filtering Biases Against Tor Leads to Tor-Hosted Alternative

In June 2013, Facebook unintentionally began blocking Tor users from accessing the social media site. To Facebook, attempted account access through shifting IPs is indicative of a hacked account or botnet. Facebook by default, denies site access by unrecognized IPs.[5,iii] Because Facebook recognized the potential for denying members with significant reasons for using anonymizing tools like Tor, the site opened a .onion site on the Tor Network.[6] It marked the first time a Certificate Authority (CA) certified a connection for Tor users.[7]

Hackers use the Darknet to Keep Their Command-and-Control Anonymous

Command-and-control servers (C2)[iv] are integral components of modern malware campaigns and are proliferating on both the Open Web and Darknet. Hiding these key components of malware infrastructure on the Darknet increases its resiliency. Limiting the frequency of communication between the C2 and infected devices reduces the likelihood that the malware will trigger intrusion detection alerts. The lowered risk of identification and takedown means that cybercriminals have less risk maintaining a simple hub[v] topology. Routing encrypted commands from control servers through Tor networks makes discovering a C2 difficult even if an intrusion is detected.[8] A growing trend is to set up multi-level control server systems that distribute commands through multiple servers; if one is taken down, the commands are automatically rerouted to keep the attack going.

If increased usage of Darknet platforms corresponds to a growth in volunteer nodes for those platforms, then bandwidth on those platforms increases and latency decreases.[vi] C2 servers hosted on the Darknet could benefit from anonymization without suffering the significant lags currently experienced. Web crawling and sinkholing, two common methods used to actively hunt malicious C2 servers and neutralize cyber threats, are similarly frustrated by how the Darknet handles IP addresses.

- Web crawlers, such as Malware Hunter, send traffic mimicking captured bots to IP addresses; when the crawler receives a reply, a C2 server may have been identified.[vii]
- Sinkholing attempts to redirect traffic from infected machines into a segregated controlled domain.[9]

As the malware transmits to that beacon, it does not have the ability to infect the larger system. Once quarantined, it can be studied and potentially traced.[10] A key attribute of the Darknet, however, is that the originating IP is unknown to the receiving device. Infected devices can only determine the IP address of the

[iii] Many sites also block Tor unintentionally using reputation-based IP filtering. Due to the uncommon amount of traffic emanating from Tor exit nodes and their susceptibility to abuse, the node IPs have a poor reputation and are blocked without regard to their actual use. Khattak, Sheharbano; et al. (2015). "Do You See What I See? Differential Treatment of Anonymous Users." *University of Berkeley.* p. 8. http://sec.cs.ucl.ac.uk/users/smurdoch/papers/ndss16doyousee.pdf. Accessed December 6, 2017.

[iv] In April 2017, Interpol announced that they had identified almost nine thousand command-and-control (C2) servers in the Asia-Pacific region alone. Interpol. (2017) "INTERPOL-led cybercrime operation across ASEAN unites public and private sectors." https://www.interpol.int/News-and-media/News/2017/N2017-051. Accessed November 3, 2017.

[v] A centralized overlay network (or 'hub') is the most direct and user-friendly model. The C2 server sits at the hub of the network with all coordinating bots receiving instructions directly; the C2 operator has a clear view of all activity and can push instructions to (or receive data from) each captured device directly. This topology is, however, more vulnerable compared to more intricate setups – if the C2 is taken down, the botnet collapses.

[vi] Tor users can volunteer their systems to be part of Tor infrastructure; encrypted messaging can pass through volunteer nodes on their way from sender to recipient. The more volunteer nodes on a system the less congestion and more messages can be routed at any given time.

[vii] In 2017, cybersecurity firms Recorded Future and Shodan announced the launch of Malware Hunter, a web crawler that seeks out C2 severs operating botnets on the Open Web. In a matter of months, it had identified over 3000 C2s. Shodan. (2017) "Malware Hunter: Finding the Command and Control Centers of Botnets across the Globe." https://malware-hunter.shodan.io/. Accessed November 4, 2017.

Darknet exit node, which changes often. It would be ineffective and incorrect to identify that exit node as a C2 node; furthermore, identifying a Darknet exit node for quarantine would block legitimate traffic from that node.

2013 Spike in Tor "Users" Attributed to Darknet-Hosted Botnet

In late August 2013, the number of daily Tor users jumped from a steady 500,000 to over 6 million as botnet, Mevade, came online. Mevade used anonymized Tor addresses, ending in .onion, to communicate with infected devices over Tor. Three new encrypted circuits were created every time a bot connected to Tor, leading Tor Project to speculate that the increased demand on existing nodes could overwhelm the system.[11,12] An earlier and smaller botnet, SkyNet, similarly leveraged the Tor network but turned its bots into nodes, effectively boosting Tor load capacity and speeds.[13]

Stolen Credentials Available on the Dark Web Present Security Risks for Otherwise Secured Networks

The proliferation of stolen credentials on the Dark Web has created a significant resource pool for cybercriminals to bypass cybersecurity measures altogether, since cybercriminals who obtain legitimate and functioning user credentials, including user names and passwords can access otherwise well-designed, secure networks. Criminals with stolen credentials can therefore access networks and systems without having to identify vulnerabilities and develop exploits. Many data breaches do not become widely known for many months or years after their occurrence.[viii] Vendors of credentials on the Dark Web rely on incidents going un-reported to maintain profitability; once breaches are widely reported, continued functionality becomes dubious and prices drop.[14]

Hoards of College Credentials for Sale on the Dark Web

In March of 2017, the cybersecurity advocacy group, "Digital Citizens Alliance" identified 6.7 million higher education email addresses that were available on the Dark Web.[15] Many of the email addresses, undoubtedly, would not function or grant a cybercriminal exploitable access to vulnerable systems. Some, however, could have helped a cybercriminal access valuable intellectual property or personally identifiable information.[ix] University credentials can be especially valuable as cybercriminals can use them to compromise university computer systems and then launch attacks against third targets from those systems, betting that targets are less likely to identify activities from university IPs as malicious.[16]

The Office of Cyber and Infrastructure Analysis (OCIA) provides analysis to support public and private-sector stakeholders' operational activities and effectiveness and to inform key decisions affecting the security and resilience of the Nation's critical infrastructure. All OCIA products are visible to authorized users at HSIN-CI and Intelink. For more information, contact OCIA@hq.dhs.gov or visit http://www.dhs.gov/office-cyber-infrastructure-analysis.

Prepared By: Strategic Infrastructure Division

PDM17097

[viii] In 2017, it took an average 191 days for a company to identify a data breach and 66 days to contain it. *Ponemon Institute*. (2017). "2017 Cost of Data Breach Study." https://www-01.ibm.com/marketing/iwm/dre/signup. Accessed December 7, 2017. (Free with registration)

[ix] Universities with significant research and development grants may be particularly high-value targets. Digital Citizens Alliance. (2012). "Cyber Criminals, College Credentials, and the Dark Web." p. 2 http://www.digitalcitizensalliance.org/clientuploads/directory/Reports/DigitalCitizens_CollegeInfoTheft.pdf. Accessed November 18, 2017.

END NOTES

[1] Tor Project. (2017). “TorMetrics: Clients.” http://metrics.torproject.org. Accessed December 7, 2017.
[2] Techopedia. (2017). “Packet Filtering.” https://www.techopedia.com/definition/4038/packet-filtering. Accessed December 13, 2017.
[3] Tor Project. (2017). “TorMetrics: Users.” http://metrics.torproject.org. Accessed December 7, 2017.
[4] Fossen, Jason. (2011). “Windows Firewall Script to Block IP Addresses and Country Network Ranges.” https://cyber-defense.sans.org/blog/2011/10/25/windows-firewall-script-block-addresses-network-ranges. Accessed March 27, 2018.
[5] Fox-Brewster, Tom. (2014). “Facebook Opens Up to Anonymous Tor Users with .Onion Address.” https://www.theguardian.com/technology/2014/oct/31/facebook-anonymous-tor-users-onion. Accessed December 16, 2017.
[6] Fox-Brewster, Tom. (2014). “Facebook Opens Up to Anonymous Tor Users with .Onion Address.” https://www.theguardian.com/technology/2014/oct/31/facebook-anonymous-tor-users-onion. Accessed December 16, 2017.
[7] Franzen, Carl. (2014). “Facebook Just Created a New Tor Link for Users Who Wish to Remain Anonymous.” https://www.theverge.com/2014/10/31/7137323/facebook-adds-direct-support-for-tor-anonymous-users. Accessed December 7, 2017.
[8] Constantin, Lucian. (2012). “Tor Network used to Command SkyNet Botnet.” *Computer World*. http://www.computerworld.com/article/2493980/malware-vulnerabilities/tor-network-used-to-command-skynet-botnet.html. Accessed November 24, 2017.
[9] Sancho, David and Link, Rainer. “Sinkholing Botnets.” *Trend Micro.* https://www.trendmicro.co.kr/cloud-content/us/pdfs/security-intelligence/white-papers/wp__sinkholing-botnets.pdf. Accessed November 1, 2017.
[10] Ibid.
[11] Hopper, Nicholas. (2013). “Challenges in Protecting Tor Hidden Services from Botnet Abuse.” *University of Minnesota*, p. 2. https://www-users.cs.umn.edu/~hoppernj/fc14-botnet.pdf. Accessed December 10, 2017.
[12] Goodin, Dan. (2013). “Sudden Spike of Tor Users Likely Caused by One ‘Massive’ Botnet.” https://arstechnica.com/information-technology/2013/09/sudden-spike-of-tor-users-likely-caused-by-one-massive-botnet/. Accessed December 12, 2017.
[13] Constantin, Lucian. (2012). “Tor Network used to Command SkyNet Botnet.” *Computer World*. http://www.computerworld.com/article/2493980/malware-vulnerabilities/tor-network-used-to-command-skynet-botnet.html. Accessed March 24, 2017.
[14] Leger, Donna. (2014). “How Stolen Credit Cards are Fenced on the Dark Web,” *USA Today*. http://www.usatoday.com/story/news/nation/2014/09/03/stolen-credit-cards-fenced-on-the-dark-web/15020053/. Accessed November11, 2017.
[15] Digital Citizens Alliance. (2012). “Cyber Criminals, College Credentials, and the Dark Web.” p. 21 http://www.digitalcitizensalliance.org/clientuploads/directory/Reports/DigitalCitizens_CollegeInfoTheft.pdf. Accessed November 18, 2017.
[16] Ibid.

OMB Control No.: 1670-0027
Expiration Date: 10/31/2017

UNCLASSIFIED

Homeland Security

National Protection and Programs Directorate

NPPD Customer Feedback Survey

1. **Product Title:** OCIA - Cybercrime and the Darknet - Effects on Cybersecurity Practices

2. Please rate your satisfaction with each of the following:

	Very Satisfied (5)	Somewhat Satisfied (4)	Neither Satisfied Nor Dissatisfied (3)	Somewhat Dissatisfied (2)	Very Dissatisfied (1)
Timeliness of product	○	○	○	○	○
Relevance of product	○	○	○	○	○

3. How did you use this product in support of your mission?

□ Yes □ No Integrated into one of my own organization's information or analytic products

If so, which products?

□ Yes □ No Used contents to improve my own organization's security or resiliency efforts or plans

If so, which efforts?

□ Yes □ No Shared contents with government, private sector, or other partners

If so, which partners?

□ Yes □ No Other uses (please specify)

4. Do you have questions that this product didn't answer?

Yes ○ No ○ (Please specify)

5. How could this product be improved?

6. Would you like to see more on this topic?

Yes ○ No ○ (Please specify)

7. Are there other topics or questions you would like to see addressed by OCIA?

To help us understand more about your organization so we can better tailor future products, please provide (OPTIONAL):

Name:		*Sector:*	Select One
Organization:		*Partner Type:*	Select One
Contact Number:		*State:*	Select One

SUBMIT FORM

Privacy Act Statement

Paperwork Reduction Act Compliance Statement

UNCLASSIFIED

REV: 14 July 2016