19 January 2016

Suspicious Domain Names and Internet Protocol (IP) Addresses Targeting Massachusetts Critical Infrastructure in November 2015

Product:

- Louisiana State Analytical & Fusion Exchange Cyber Fusion Unit, "Block List Summary, November 2015"
- ICS-CERT, "Fact Sheet–Recent Cyber Activity Targeting Critical Infrastructure Control Systems", 2015.
- MS-ISAC, "Malware IPs and Domains observed by MS-ISAC" November 2015.

(U//FOUO) Overview:

(U//FOUO) This document is intended to provide network security managers, information security officers and those responsible for cyber security in their respective organizations potentially malicious Internet Protocol addresses in Massachusetts and nationwide. These hosts have been associated with malicious code incidents. (Attached find an excel spreadsheet labelled "Massachusetts Malicious IPs and Domains November 2015" for the full list.)This is being provided for informational purposes only and not to be used in the course of a criminal investigation.

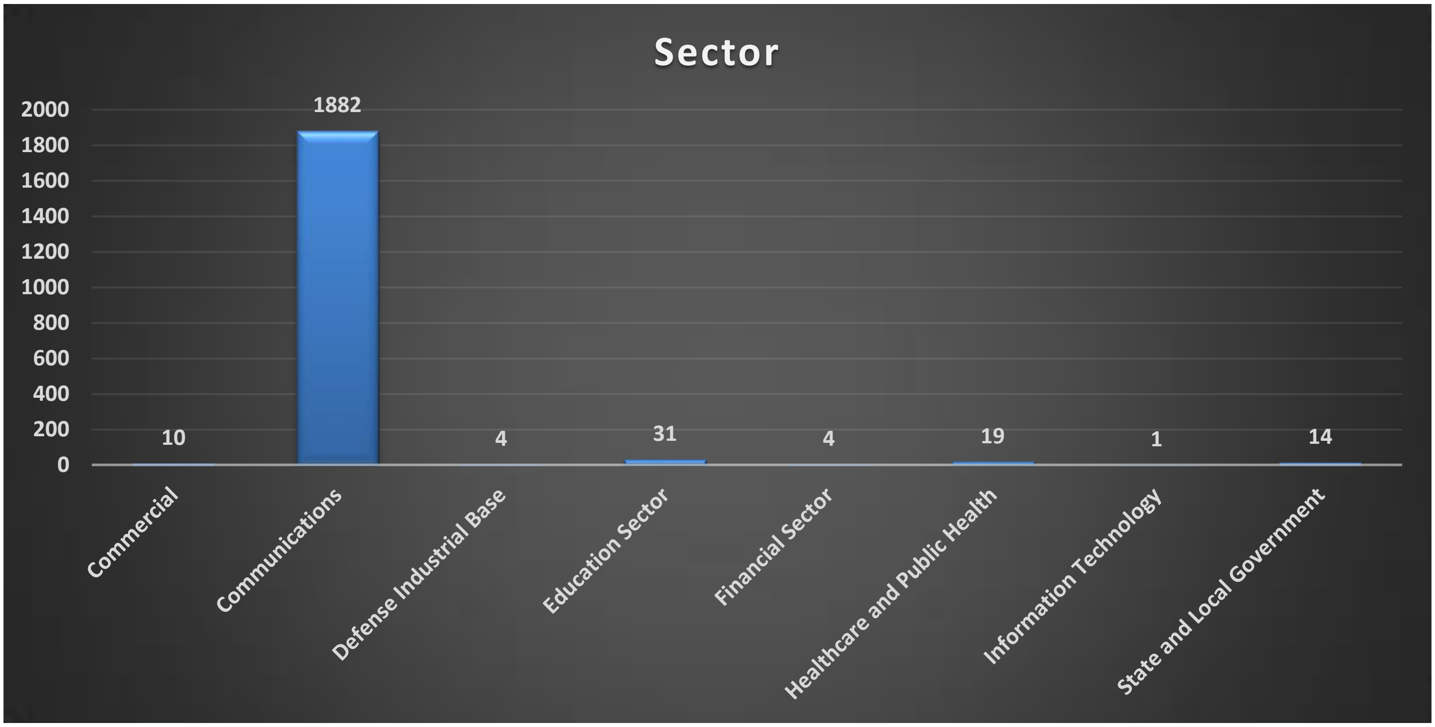
(U//FOUO) Between 01 November 2015 and 30 November 2016 DHS I&A was notified of 2582 instances in which suspicious activity on networks impacting the commercial, communications, defense industrial base, energy, financial, health and public health, higher education, information technology and state and local government sectors in Massachusetts. The nature of the suspicious activity appears to be the infection of local servers with malicious software (malware), in this case Aldibot, Andromeda, Blackenergy, Darkcomet, Dirtjumper, Dridex, Drive, Dyreza, Jedobot, Optima, Pandora, Poseidon, Smokeloader, Solar and Vertexnet.

(U//FOUO) Sectors Impacted

(U//FOUO) Eight critical infrastructure sectors were impacted in November based on the incidents reported. These sectors include commercial, communications, defense industrial base, energy, financial, health and public health, higher education and information technology. The communications sector experienced the greatest impact, possibly due to the fact that

Department of Homeland Security
Office of Intelligence & Analysis
New England Region

Internet provider servers and systems are at a greater risk of malware infection due to poor Internet security practices of customers over which the sector's administrators have little or no control.

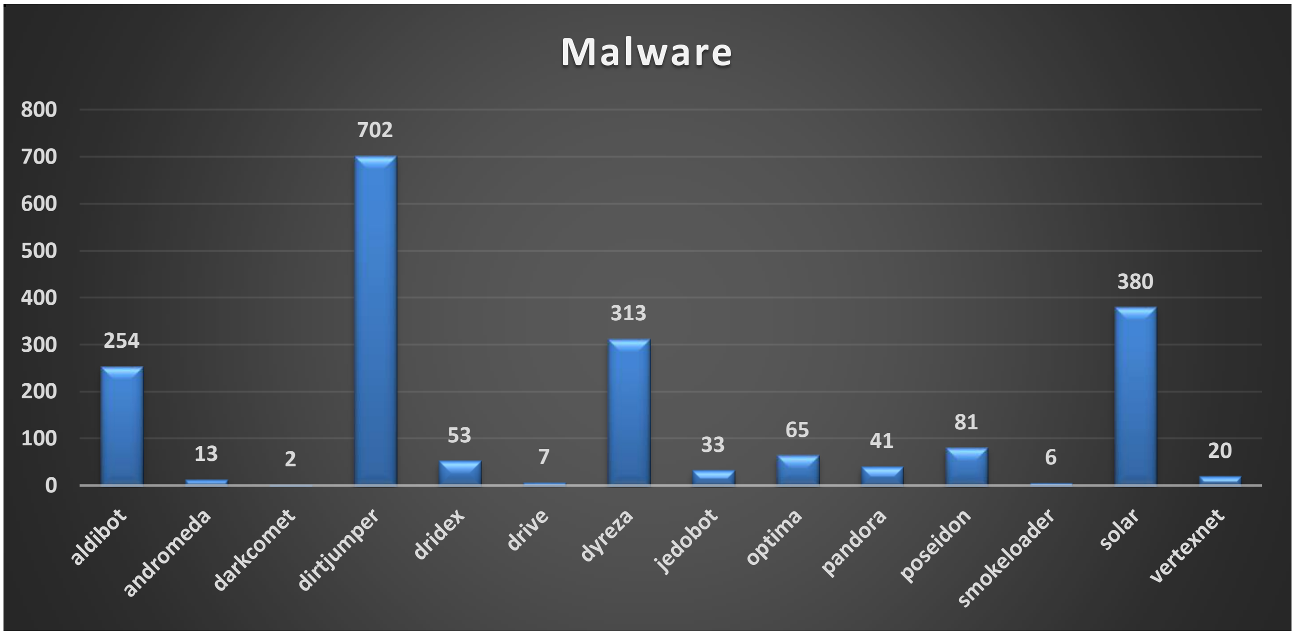


(U//FOUO) Botnet Detected

(U//FOUO) There were a total of fourteen types of bots detected impacting Massachusetts' critical infrastructure in November 2015. The most prevalent bot was the Dirtjumper toolkit. The Dirt Jumper family of DDoS (distributed denial-of-service) botnet kits was originally authored by an individual located in Russia who uses the handle 'sokol.' Various versions of Dirt Jumper were sold privately and leaked to the public. As time has passed, variants of Dirt Jumper have become publicly available.

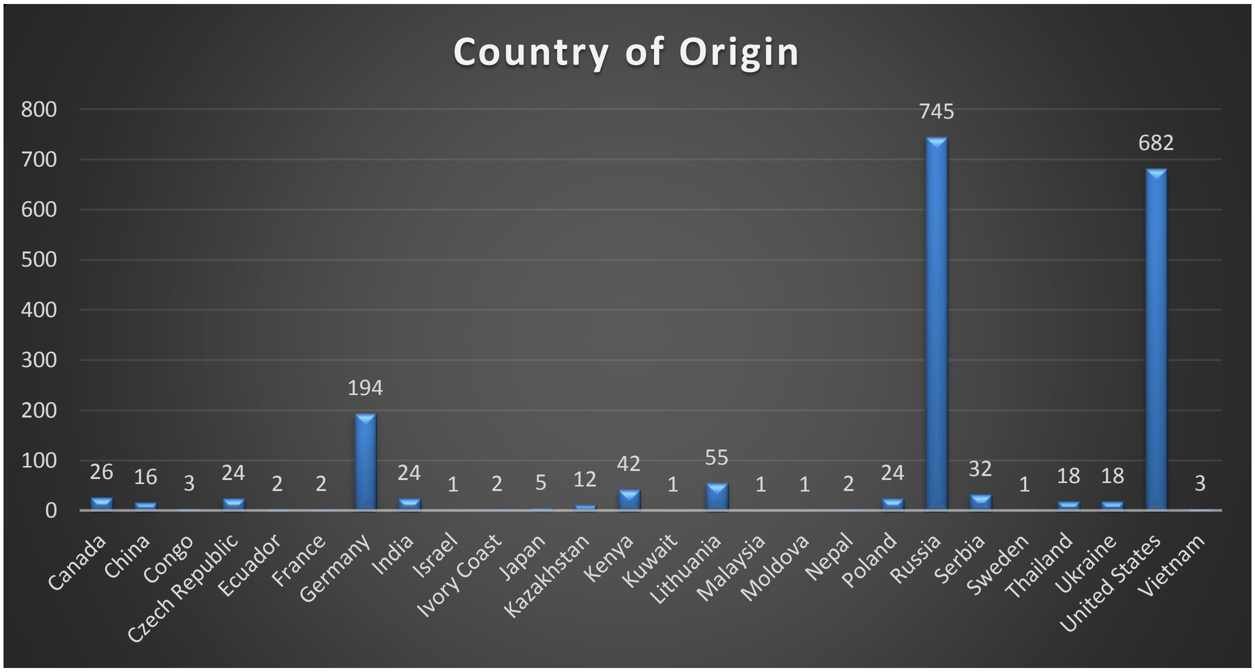
Department of Homeland Security
Office of Intelligence & Analysis
New England Region

(U//FOUO) The second most frequently seen malware was Solar. Solar, also known as Solarbot or Napolar, is an information stealing malware used by cybercriminals to collect data on credentials, and other valuable pieces of information. Cybercriminals first started to advertise Solar in May 2013, with a dramatic spike in usage starting in the summer of 2013 and a prominent spike of activity in South America. Solarbot is able to launch several types of DDoS attacks, can act as a reverse SOCKS5 proxy, steal POP3 and FTP login credentials from many email and FTP clients, and steal information entered by victims into Web forms in Internet Explorer, Mozilla Firefox, or Google Chrome. The malware's functionality can be extended through plug-ins. The bot's developers offer a plug-in SDK (software development kit) and also provide some example plug-ins to steal Bitcoin wallets or collect computer information.



(U//FOUO) IP Countries of Origin

(U//FOUO) Please note the actors engaged in this malicious activity may not be geographically located in the countries listed below but may possibly be passing through Internet Service Providers (ISPs) with IPs in these locations or engaged in IP spoofing:



(U//FOUO) Conclusion

(U//FOUO) 73 identified IPs were involved in 2582 incidents impacting nine Massachusetts critical infrastructure sectors in November 2015. The incidents noted in this report are not wholly inclusive of all malicious activity impacting Massachusetts critical infrastructure, but only those provided to the reporting parties. DHS I&A, the CFC and BRIC continue to be interested in information relating to:

- Attribution information for malicious activity on CI/KR networks
- The nature of the systems or data set threat actors are targeting
- Method of compromise or infection
- Whether information was exfiltrated, damaged, or altered by the incident
- The identification of any malware or IP addresses used in the incident

Department of Homeland Security
Office of Intelligence & Analysis
New England Region