1300 - Malicious CDNs: Identifying Zbot Domains en Masse via SSL Certificates and Bipartite Graphs

Sunday at 13:00 in Track 3
45 minutes | Art of Defense
Thomas Mathew*OpenDNS (Cisco)*

Dhia Mahjoub*Head of Security Research, Cisco Umbrella (OpenDNS)*

Prior research detailing the relationship between malware, bulletproof hosting, and SSL gave researchers methods to investigate SSL data only if given a set of seed domains. We present a novel statistical technique that allow us to discover botnet and bulletproof hosting IP space by examining SSL distribution patterns from open source data while working with limited or no seed information. This work can be accomplished using open source datasets and data tools.

SSL data obtained from scanning the entire IPv4 namespace can be represented as a series of 4 million node bipartite graphs where a common name is connected to either an IP/CIDR/ASN via an edge. We use the concept of relative entropy to create a pairwise distance metric between any two common names and any two ASNs. The metric allows us to generalize the concept of regular and anomalous SSL distribution patterns.

Relative entropy is useful in identifying domains that have anomalous network structures. The domains we found in this case were related to the Zbot proxy network. The Zbot proxy network contains a structure similar to popular CDNs like Akamai, Google, etc but instead rely on compromised devices to relay their data. Through layering these SSL signals with passive DNS data we create a pipeline that can extract Zbot domains with high accuracy.
Thomas Mathew
Thomas Mathew is a Security Researcher at OpenDNS (now part of Cisco) where he works on implementing pattern recognition algorithms to classify malware and botnets. His main interest lies in using various time series techniques on network sensor data to identify malicious threats. Previously, Thomas was a researcher at UC Santa Cruz, the US Naval Postgraduate School, and as a Product and Test Engineer at handsfree streaming video camera company Looxcie, Inc. He presented at ISOI APT, BruCon, FloCon and Kaspersky SAS.
Dhia Mahjoub
Dr. Dhia Mahjoub is the Head of Security Research at Cisco Umbrella (OpenDNS). He leads the core research team focused on large scale threat detection and threat intelligence and advises on R&D strategy. Dhia has a background in networks and security, has co-authored

patents with OpenDNS and holds a PhD in graph algorithms applied on Wireless Sensor Networks problems. He regularly works with prospects and customers and speaks at conferences worldwide including Black Hat, Defcon, Virus Bulletin, BotConf, ShmooCon, FloCon, Kaspersky SAS, Infosecurity Europe, RSA, Usenix Enigma, ACSC, NCSC, and Les Assises de la sécurité.

#defcon25/by_track/track3/sunday #defcon25/By_Day/_Sunday