Threat STOP

www.threatstop.com

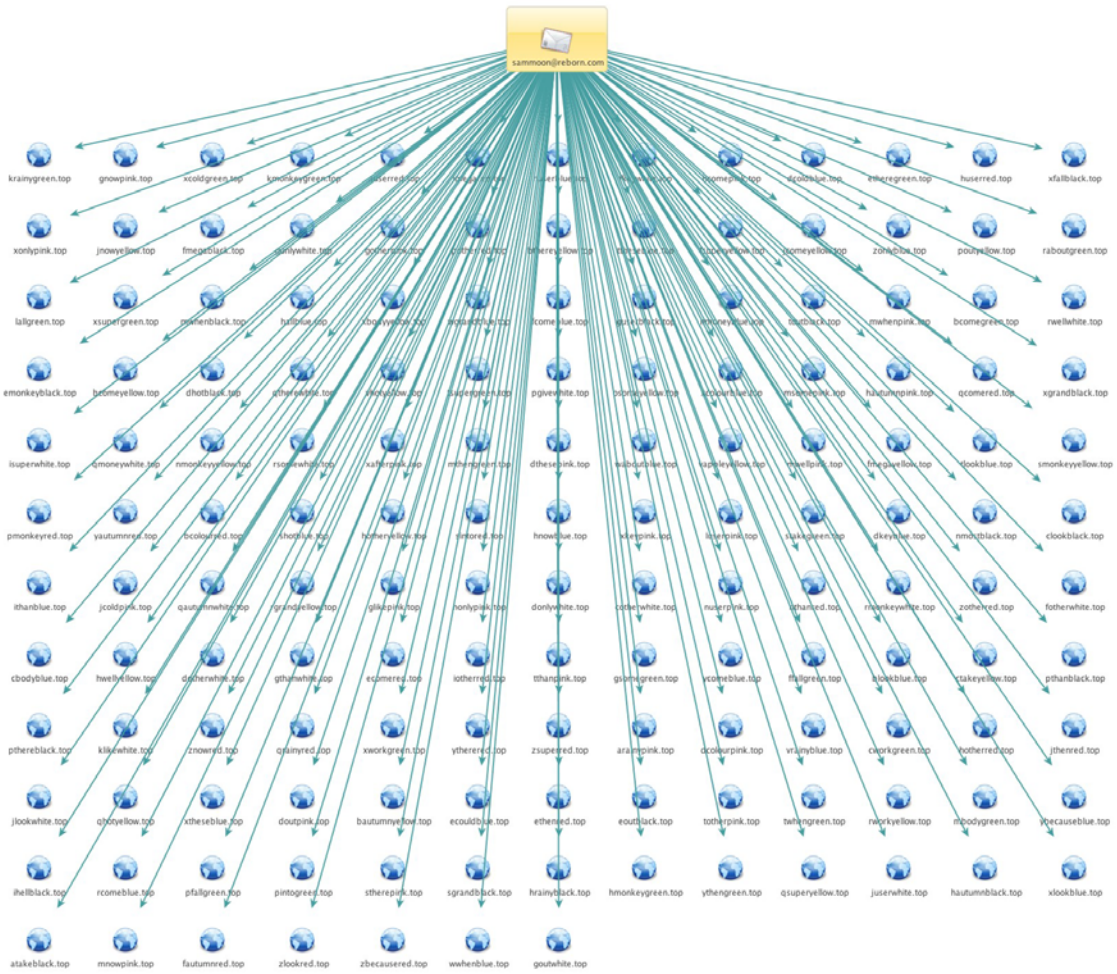
SECURITY ANALYSIS REPORT

Neutrino Exploit Kit DGA Infrastructure

Exploit kits are used by cyber criminals to take advantage of vulnerabilities on a machine in order to deliver various types of malware, including ransomware. This happens while the victim is browsing the Internet, many times through the use of compromised legitimate domains.

Recently, we have seen vast DGA infrastructures constantly popping up for the Neutrino EK. The randomly generated string is usually a subdomain to a set of domains following a certain pattern, and are registered by the same registrant. These domains are created by concatenating various parts such as letters, numbers, animal names, and colors, and forming a single string The common TLDs used for this infrastructure are .top and .xyz.

In one case, we came across an email address - sammoon@reborn.com - which had registered 150 domains following the pattern <letter><short word><color>.top.



Each of these domains can be the parent to multiple DGA subdomains. By doing a simple IP resolve for all subdomains of these domains, we found 24 IP's that are hosting Neutrino DGAs

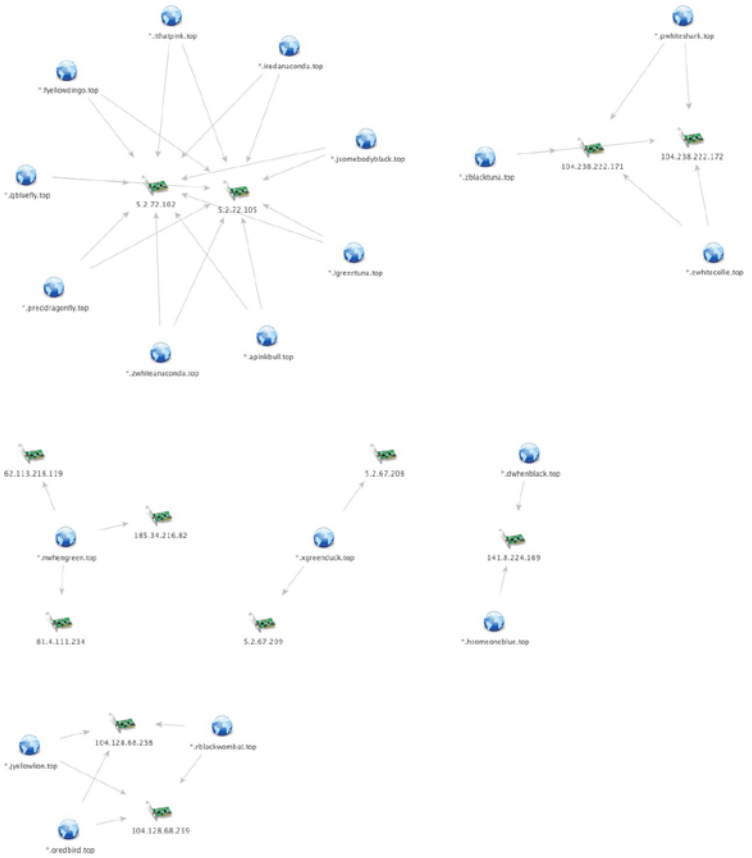
- 104.128.68[.]200
- 104.128.68[.]223
- 104.128.68[.]238
- 104.128.68[.]239
- 104.238.222[.]171
- 104.238.222[.]172
- 167.114.47[.]150
- 185.34.216[.]82
- 198.50.175[.]240
- 5.2.67[.]208
- 5.2.67[.]209
- 5.2.67[.]210
- 5.2.67[.]211
- 5.2.72[.]102
- 5.2.72[.]105
- 5.2.72[.]171
- 5.2.72[.]226
- 5.2.72[.]236
- 5.2.72[.]237
- 62.113.218[.]119
- 62.113.218[.]12
- 77.81.104[.]115
- 81.4.111[.]234
- 91.134.220[.]108

A follow up on the domain resolutions for these IP's gave us a list of a little over 1500 domains that are parents to DGA subdomains. In the section below, we will focus on a group of around 350 domain names found from this follow up, whose common denominator is the inclusion of a color as part of the domain name.

By doing a reverse Whois search on the pool of 350 domains, we found seven new email addresses used to register the patterned Neutrino domains mentioned on the front:

- fitchewb@gmail.com
- harry23@activist.com
- ivkolyvan@gmail.com
- jacky@supershaadi.com
- julia3@europe.com
- miamia@dallasmail.com
- nira@sms2sale.com

(continued on following page)



(continued)

While analyzing the domains registered by these email addresses, we noticed that some of the domains registered by these email addresses aren't being hosted on the list of 24 IP's seen above. This brought to the discovery of 6 new IPs also hosting many DGA domains:

- 141.8.224[.]169
- 78.46.167[.]135
- 78.46.167[.]133
- 178.33.217[.]64
- 151.80.7[.]122
- 176.31.223[.]165

This is not the first time we've seen vast Neutrino infrastructures like this. In mid-June we came across a group of three IPs that led us to a full DGA infrastructure:

- 209.222.30[.]216
- 45.63.96[.]182
- 37.130.229[.]105

These IP's hosted dozens of DGA subdomains to domains that follow a specific pattern, such as <letter><letter><animal(from a list of 50 pre-chosen animals)><letter>.top or <vowel><vowel>land.top.

During this analysis, we uncovered thousands of parent domains to Neutrino DGAs. ThreatSTOP DNS Firewall customers are protected from these domains, as well as all of their DGA subdomains. We are constantly finding new indicators in this ongoing analysis, and will continue protecting our customers from Neutrino EK.

www.threatstop.com