Resurgo
Cyber Threat Alert Summaries

Hi All,

On June 13th, 2017, DHS released a Joint Technical Alert on North Korea's DDoS Botnet Infrastructure". The alert provides indicators of compromise (IOC) and malware descriptions. Additionally, DHS and the FBI have identified IP addresses associated with a malware known as DeltaCharlie.

For a copy of the Technical Alert or the IOC's and detection signatures, contact me at ryan.ito@resurgo.net.

Additionally,

US-CERT has received information about the following IP addresses are suspected of using malicious X-Tunnel SSL certificates. IP address 94.142.140.191 was identified as using X-Tunnel SSL Certificate (SHA1)"7F0CDB0C3BF7325026A4F69C93C8463BBE4A2430". IP addresses 5.135.199.31 & 92.114.92.134 were identified as using X-Tunnel SSL certificate (SHA1) "A1833C32D5F61D6EF9D1BB0133585112069D770E".

The X-Tunnel malware functions of the tool include the ability to hook into system drivers, access the local LDAP server, access local passwords, use SSH, OpenSSL, search and replace local files, and of course be able to maintain a persistent connection to a pre-specified IP address, even if the host is behind a NATed firewall.

Notice
These flagged domains are not a definitive black list, but a recommendation and advisement provided by the DSS. It is up to the recipients of this information to decide how, when and where to use the information contained in these summaries.