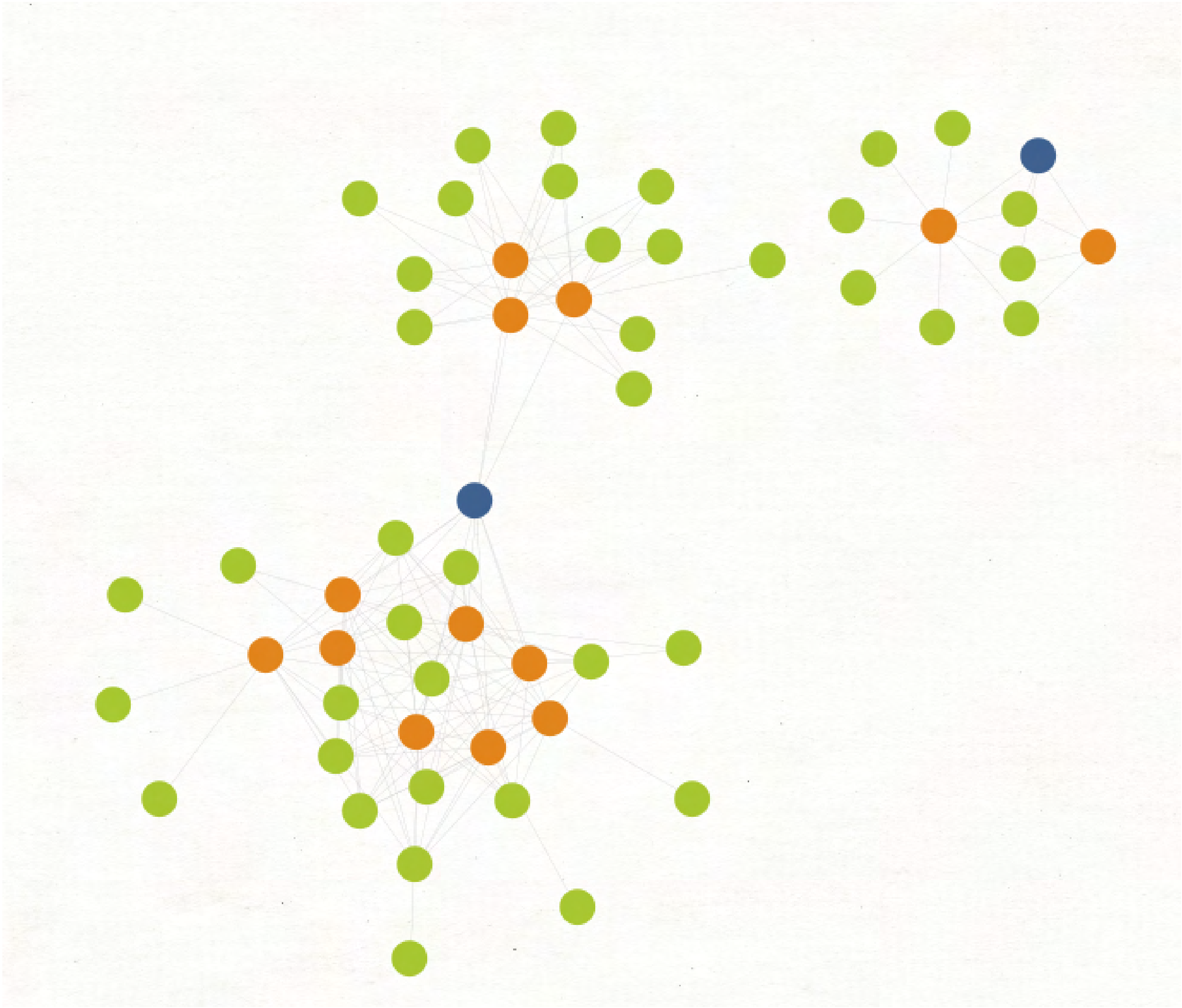
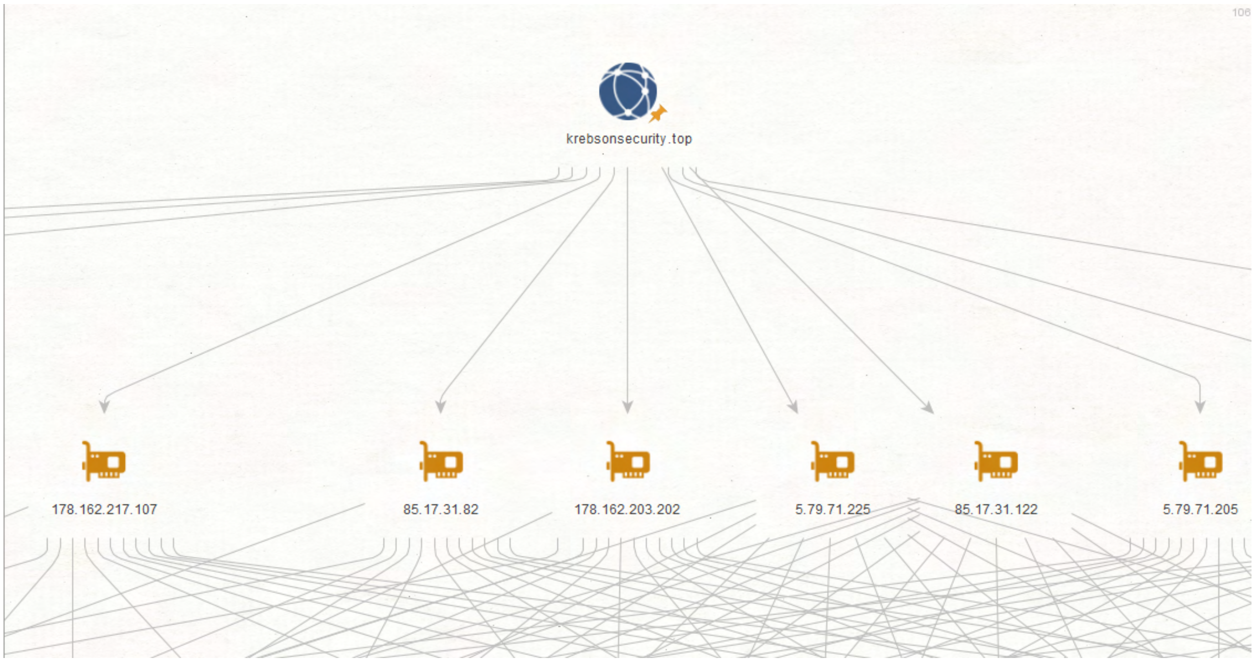
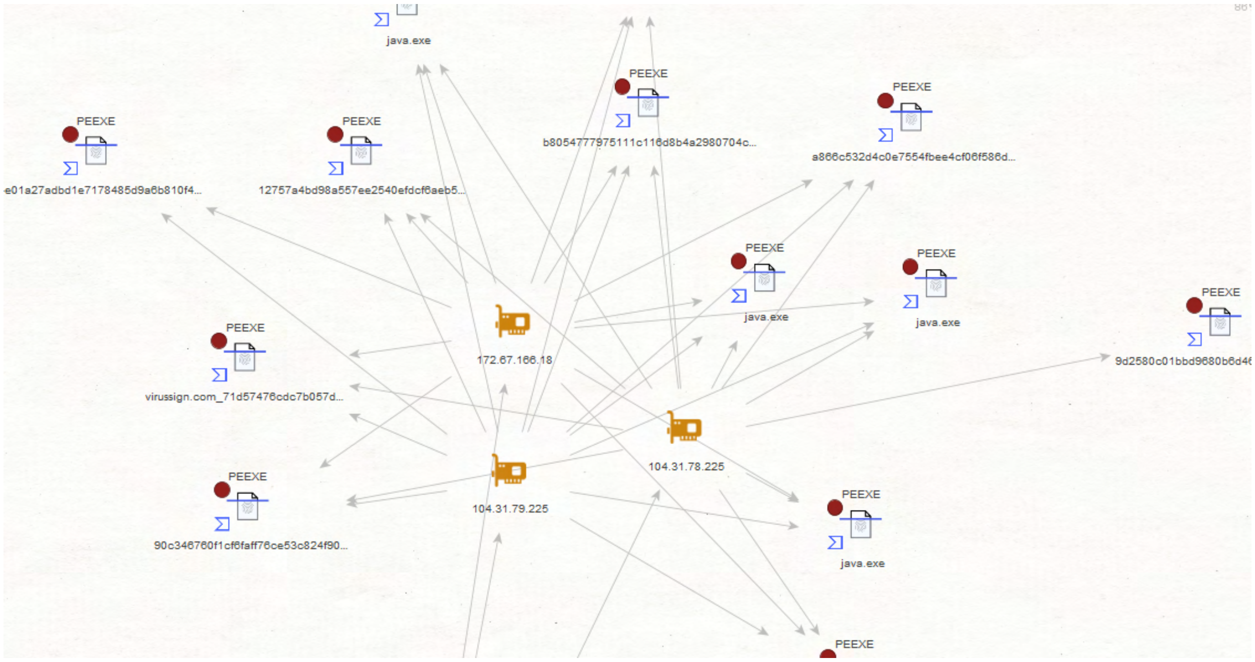
00. Cybercriminals Launch a Typosquatting Campaign Impersonate Legitimate Cybercrime Researcher Brian Krebs Drop Malware - An Analysis



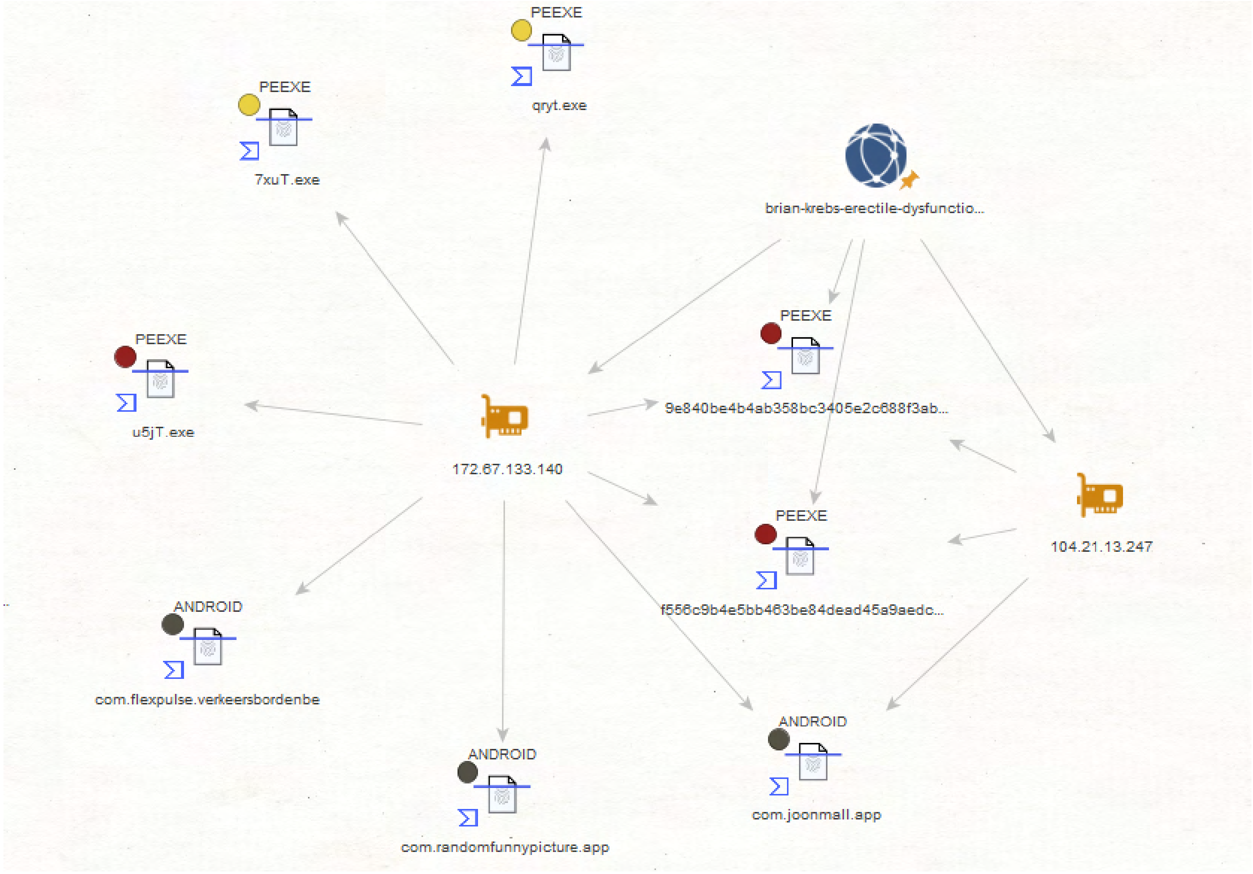
We’re recently became aware of a currently active RAT (Remote Access Tool) serving malicious software campaign that’s impersonating Brian Krebs in two of its C&C (Command and Control) servers and we’ve decided to take a closer look at the campaign including its domain IP and network infrastructure for the purpose of providing actionable intelligence on its infrastructure potentially assisting security researchers and OSINT analysts by providing them with the necessary information stay on the top of such type of threats.



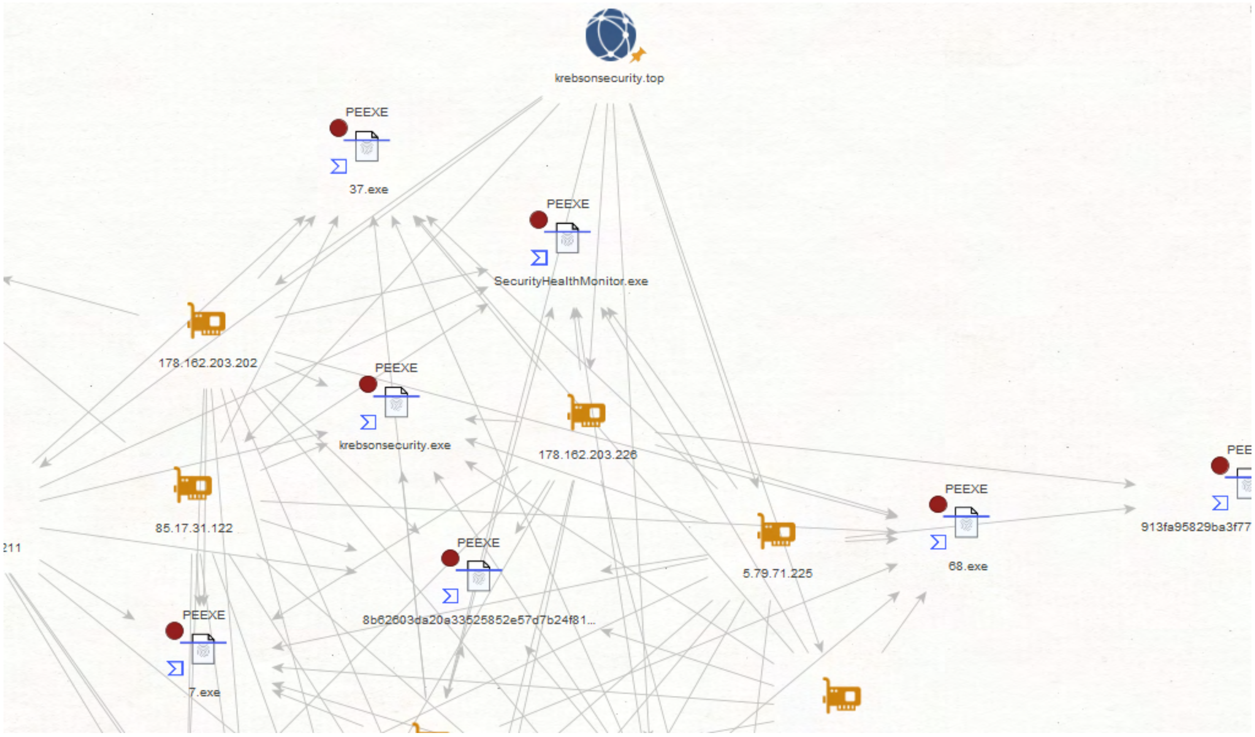
Sample screenshot of the botnet's C&C infrastructure that is using a typosquatted domain impersonating Brian Krebs


java.exe
PEEXE
b8054777975111c116d8b4a2980704c...
PEEXE
a866c532d4c0e7554fbee4cf06f586d...
PEEXE
e01a27adbd1e7178485d9a6b810f4...
PEEXE
12757a4bd98a557ee2540efdcf6aeb5...
PEEXE
java.exe
PEEXE
java.exe
PEEXE
9d2580c01bbd9680b6d4
PEEXE
virussign.com_71d57476cdc7b057d...
172.67.166.18
104.31.78.225
PEEXE
90c346760f1cf6faff76ce53c824f90...
104.31.79.225
PEEXE
java.exe
PEEXE

Sample screenshot of the botnet's C&C infrastructure that is using a typosquatted domain impersonating Brian Krebs


PEEXE
qryt.exe
PEEXE
7xuT.exe
brian-krebs-erectile-dysfunctio...
PEEXE
u5jT.exe
PEEXE
9e840be4b4ab358bc3405e2c688f3ab...
172.67.133.140
104.21.13.247
PEEXE
f556c9b4e5bb463be84dead45a9aedc...
ANDROID
com.flexpulse.verkeersbordenbe
ANDROID
com.joonmall.app
ANDROID
com.randomfunnypicture.app

Sample screenshot of the botnet's C&C infrastructure that is using a typosquatted domain impersonating Brian Krebs



Sample screenshot of the botnet's C&C infrastructure that is using a typosquatted domain impersonating Brian Krebs

Sample botnet C&C server domains known to have been involved in the campaign:

hxxp://brian.krebsonsecurity[.]top
hxxp://brian-krebs-erectile-dysfunction[.]com

Sample malicious MD5s known to have been involved in the campaign:
9e840be4b4ab358bc3405e2c688f3ab1a9d286bd4fb9edb4468dc688962b4893
f556c9b4e5bb463be84dead45a9aedcf8bec41c1c2b503ea52719357943750e7

We'll continue monitoring the campaign using WhoisXML API's domain and IP reputation monitoring system and will post updates as soon as new developments take place.