URL Blacklist

These are all known threats related to threats related to
Banking Trojans
Oakbot ✅
Emotet ✅
Trickbot ✅

Emotet

OVERVIEW

Emotet (also known as Geodo) is a banking trojan written for the purpose of perpetrating fraud. It is usually distributed through large-scale spam campaigns with links to malicious word documents containing a PowerShell downloader script. Emotet is known to be bundled alongside Zeus Panda (Panda Banker), Trickbot, and IceID.

IOC's

http://93.156.165.186/
http://14.99.112.138/
http://219.92.13.25/
http://190.55.233.156/
http://108.48.41.69/
http://173.91.22.41/
http//173.91.11/41/
http://41.215.92.157/

REFERERENCE:
https://precisionsec.com/threat-intelligence-feeds/emotet/

Trickbot

OVERVIEW

A malware family first captured by FortiGuard Labs. This mode-based malware can extend its functionality by downloading new modules from it's servers and executing them on their C&C servers. This banking trojan can go as far as collecting it victims credentials, bank accounts, installed network apps, etc.

IOC's

<srv>107.175.87.142:443</srv>
<srv>114.8.133.71:449</srv>
<srv>119.252.165.75:449</srv>
<srv>121.100.19.18:449</srv>
<srv>131.161.253.190:449</srv>

REFERENCE

https://www.fortinet.com/blog/threat-research/new-variant-of-trickbot-being-spread-by-word-document

Qakbot

OVERVIEW
QakBot is financial malware known to target businesses to drain their online banking accounts. The malware features worm capabilities to self-replicate through shared drives and removable media. It uses powerful information-stealing features to spy on users' banking activity and eventually defraud them of large sums of money.

IOC's
hxxps://besthack[.]co/differ/50160153/50160153[.]zip
hxxps://besthack[.]co/differ/50160153/50160153[.]zip

92.67.244.225:443
96.3.93.39:443
173.31.254.105:443
192.158.217.32:993
47.21.79.34:443

Zeus Panda

https://securityintelligence.com/qakbot-banking-trojan-causes-massive-active-directory-lockouts/
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/qakbot-resurges-spreads-through-vbs-files

SIDE NOTES:
WannaCry
https://securityintelligence.com/unwrapping-the-mystery-did-a-big-slimy-internet-worm-make-hundreds-of-organizations-wannacry/