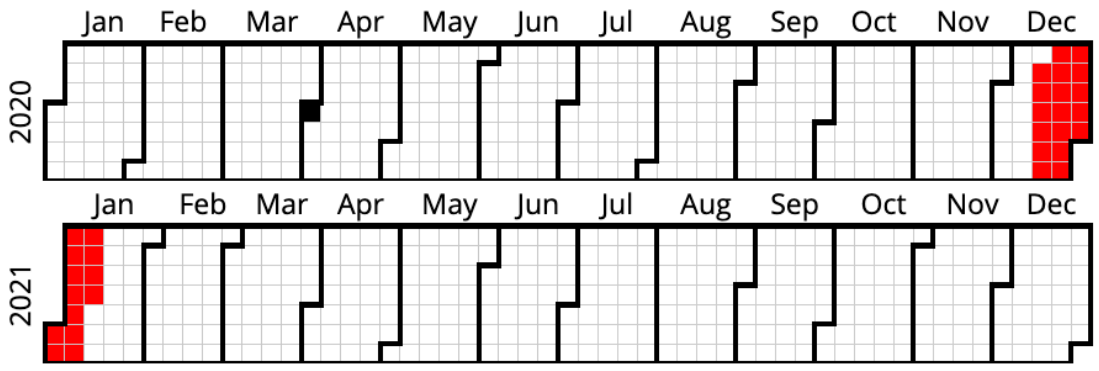
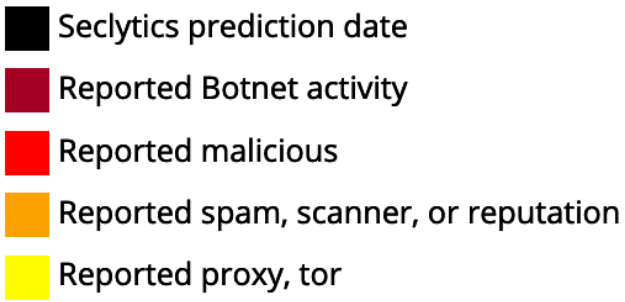
Sunburst Predictions

Seclytics Research Labs
augur@seclytics.com
1/13/2021

In a powerful demonstration of the value of predictive intelligence, SecLytics' Augur Predictive Threat Intelligence Platform accurately predicted command and control (C2) infrastructure of the Sunburst malware of the SolarWind's Orion software hack. Where traditional threat intelligence solutions could only warn once the supply chain hack had been publicly identified, Augur users got advance intelligence and blocking. Clients using Augur's Firewall and other endpoint integrations were also protected by automated blocking of exfiltration routes.

In Q1 2020, Augur detected the build-up of attack infrastructure attributed to two command and control infrastructure associated with the Sunburst malware. Augur predicted and blocked IPv4 5[.]252[.]177[.]25 and 5[.]252[.]177[.]21 eight months before the SolarWinds hack was made public. In addition, Augur predicted the C2 hostnames incomeupdate[.]com and accounts-updates[.]club.



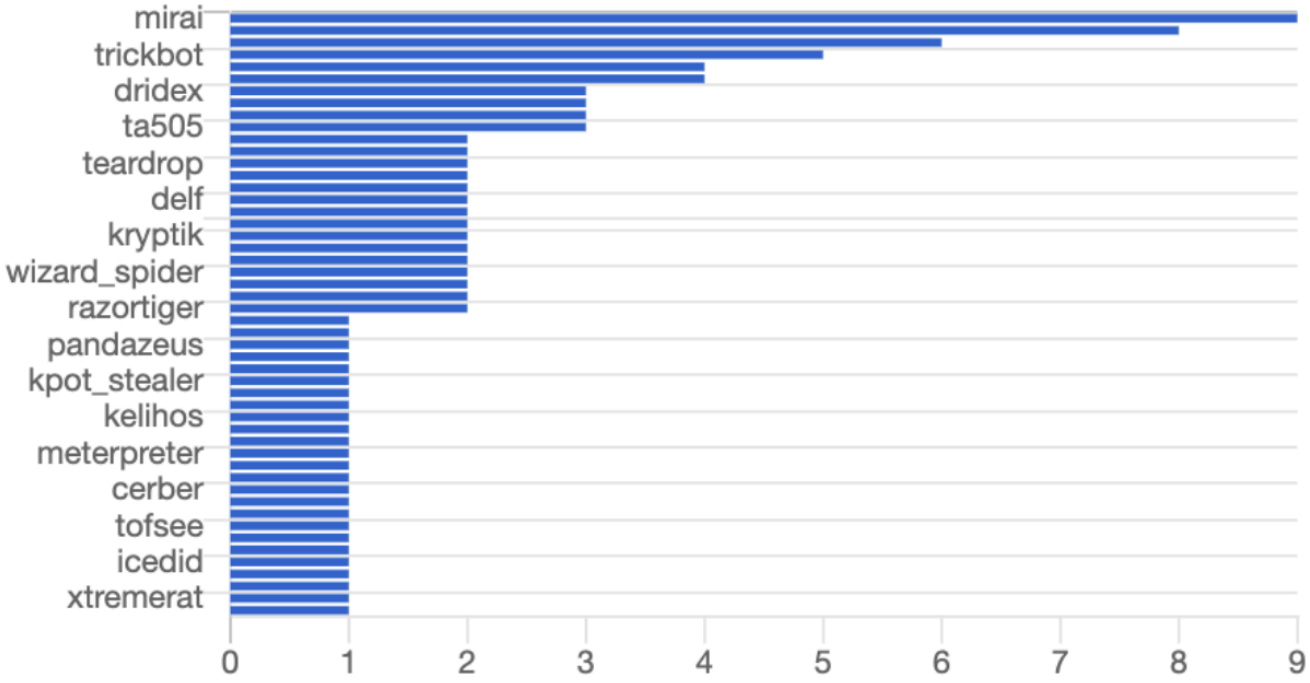


Seclytics, Inc
4660 La Jolla Village Drive #100
San Diego, CA 92122

+1 (650) 264-9702
info@seclytics.com
www.seclytics.com

Augur Threat Actor Profile profile-126597 has been attributed to APT groups: TA505, TA544, and APT33. The threat actor profile comprises more than 12 BGP prefixes that have been confirmed to be malicious by several threat intelligence sources since April 2020.

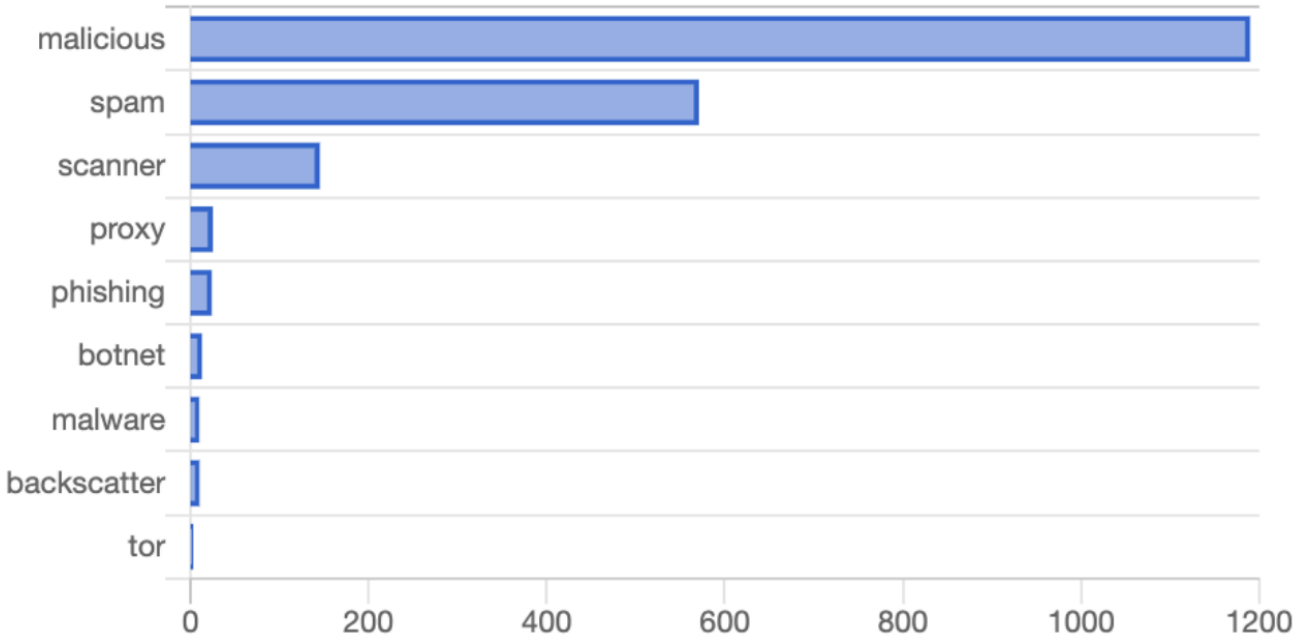
The threat actor profile has been involved in Mirai, Trickbot, and Dridex related malware campaigns as shown below.



Seclytics, Inc
4660 La Jolla Village Drive #100
San Diego, CA 92122

+1 (650) 264-9702
info@seclytics.com
www.seclytics.com

In addition, the threat actor profile has been involved mainly in malware and spam related campaigns as shown below.



For more information about Augur's predictive intelligence email us at augur@seclytics.com.

Seclytics, Inc
4660 La Jolla Village Drive #100
San Diego, CA 92122

+1 (650) 264-9702
info@seclytics.com
www.seclytics.com