INFOGRAPHIC

Q1 2020 Threat Summary

MALWARE

2.4M+ DETECTED

1202 UNIQUE VARIANTS DETECTED

200K+ VARIANTS DETECTED PER WEEK

28K+ VARIANTS DETECTED PER DAY

22% DECREASE IN TOTAL ACTIVITY

BOTNET

1.2M+ DETECTED

46 UNIQUE BOTNETS DETECTED

107K+ INFECTIONS PER WEEK

15K+ INFECTIONS PER DAY

52% DECREASE IN TOTAL ACTIVITY

EXPLOITS

23M+ DETECTED

404 UNIQUE EXPLOITS DETECTED

2M+ DETECTIONS PER WEEK

278K+ DETECTIONS PER DAY

6.3% INCREASE IN TOTAL ACTIVITY

KEY TRENDS TO CONSIDER

Necurs botnet activity sharply decreased after Microsoft disrupted the botnet in March. By March 8-15 the Necurs botnet went completely silent, as zero traffic was observed.

Cybercriminals targeted known exploits in VPN, IoT and authentication technology—overall, vulnerability exploitation increased over the quarter by 6.3%.

A sharp increase in Executable and Linkable Format (ELF) variants targeting Internet of Things (IoT) devices with an attempt to further spread the Mirai Botnet this quarter. At its peak in Week 11, Nuspire observed 86% increase in activity.

Phishing attempts more than doubled (141%) over the last three months.

Get more real-world threat intelligence to help protect your organization from ever evolving cyber attacks. Nuspire is here to help.

DOWNLOAD THE FULL REPORT.