nuspire

How are Cyberattackers Evolving Beyond Pandemic-Inspired Threats?

Nuspire's Q2 2020 Threat Landscape Report breaks down the latest attack methods—and how to combat them.

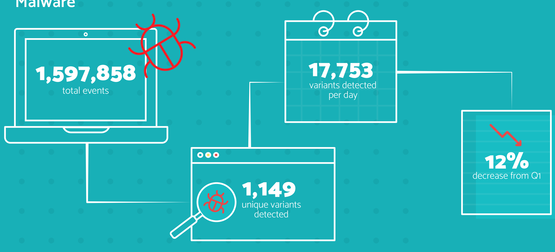
Attackers are starting to shift away from COVID-19 themed-attacks in favor of upcoming media events associated with the U.S. presidential election and Black Lives Matter.

Ransomware operators began forming cartels to share resources and tactics to further their empires.

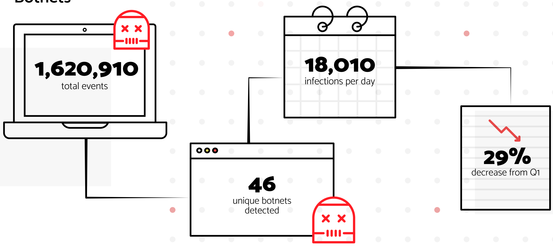
New Netgear router vulnerabilities were publicly disclosed, and a new Trojan zoomed into the top five list. The Trojan, MSOffice/Sneaky.Ltr, contains malicious macros hidden in Microsoft Office file attachments.

Threats at a Glance

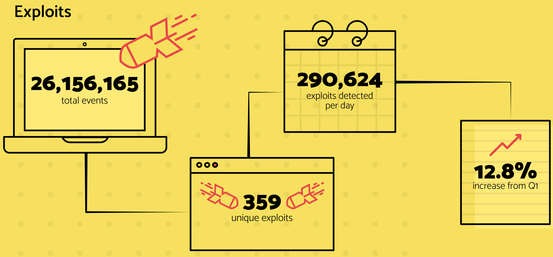
Malware



Botnets



Exploits



Malware Highlights

Most active: Emotet

6.21% decrease in activity

Wormable malware that spreads on connected network devices

New variant: MSOffice/Sneaky.Ltr

A weekly high of **17,000** events

Most vulnerable attack vector: off-network or off-VPN home environments

How to combat Consider next-generation antivirus (NGAV) endpoint protection to detect malicious software not only through signatures but also heuristics and behavior.

Botnet Highlights

Most active: ZeroAccess

Weekly high: **265,000** events

Activity attributed to leaked source code

Evolving: Cidox

12% increase in Q2 with spikes of 201% (week 4) and 241% (week 8)

Likely rootkit campaign targeting Microsoft Windows users

How to combat Use threat intelligence to determine if devices are reaching out to malicious hosts with C2 communications.

Exploit Highlights

Dominant: DoublePulsar

72% of all exploit attempts

Opens a backdoor to further infections

Remote code execution: Bash Remote Code

1,310% activity increase during Q2

Targets unpatched systems

How to combat Patch systems immediately after notification of a vulnerability.

Download the entire Q2 2020 report, which also provides a timeline of key events during the quarter.

nuspire

Nuspire, a leading managed security services provider (MSSP), takes an optimistic, people-first approach to cybersecurity. **Learn more** about our award-winning threat detection and response capabilities.