nuspire

The Greatest Threats of Q3 2020

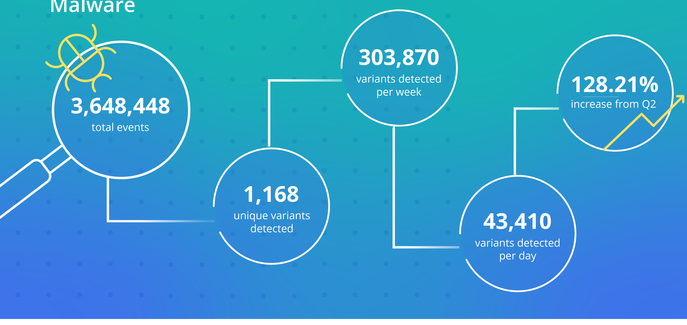
Nuspire's Q3 2020 Threat Landscape Report breaks down the latest attack methods-and how to combat them

Threat actors became even more ruthless in Q3 2020, shifting focus from home networks to overburdened public entities. New targets observed include the education sector and the Election Assistance Commission (EAC).

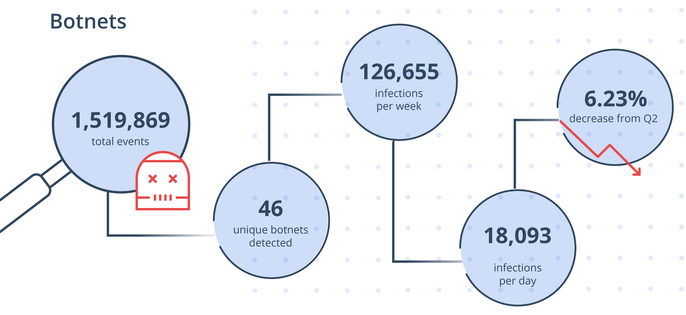
Read on to explore Nuspire's Q3 findings aggregated and correlated from our enterprise and mid-market client datasets and, our partner, Recorded Future.

Threats at a Glance

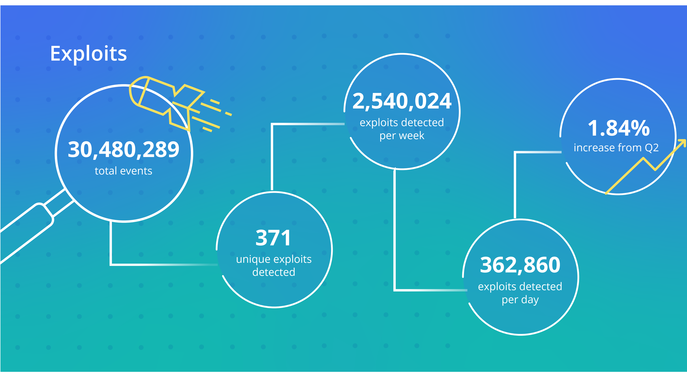
Malware



Botnets



Exploits



An Emotet Resurgence

Emotet remains one of the most prominent and prolific threats to enterprises in 2020. Major shifts in tactics, techniques and procedures (TTPs) include:

The replacement of TrickBot with QakBot as a final payload

A 1,000% increase in Emotet downloads, correlating with Emotet's packer change, which causes the Emotet loader to have a lower detection rate across antivirus software

Operators using new Microsoft Word document templates

Operators using password protected archives containing malicious macros to bypass detections

Read Nuspire's Q3 2020 Threat Report for further analysis and remediation recommendations to combat Emotet and Q3's other top threats.

nuspire

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