2018 WEBROOT THREAT REPORT

MID-YEAR UPDATE

KEY REPORT STATS

SECURITY ISN'T PERFECT, AND THREAT ACTORS DON'T STAND STILL.

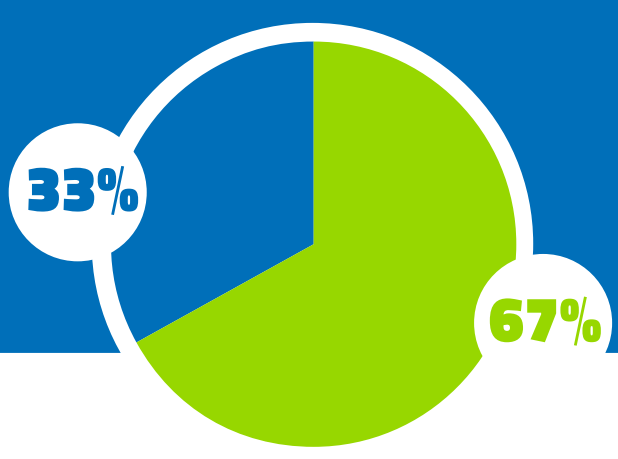
This mid-year update to our annual Threat Report shines a light on the trends and changes we saw during the first half of 2018.

PHISHING

60% The amount phishing attempts increased from Jan to June 2018

93% of breaches start with phishing attacks[1]

WEBSITES MOST IMPERSONATED BY PHISHING IN H1 2018



MAJOR THREATS, GREATEST HITS

Ransomware, cryptojacking, and botnets continue to dominate the threat landscape, but they've seen some interesting developments.

.1% combined of Spyware and Adware, Spam URLs, and Keyloggers and Monitoring

RANSOMWARE

- Increasingly more targeted
- Uses unsecured remote desktop protocol (RDP)
- Criminals may do recon for cryptomining first

CRYPTOMINING

- New #1 threat
- Very profitable, minimal criminal footprint
- Works on any device, even IoT
- Will account for ~3% of world's electricity consumption by 2020

BOTNETS

- Emotet, Trickbot, Zeus Panda are prevalent and persistent
- Concentrate on credential-gathering
- Now use UPnP to turn routers into C&C nodes

HARDWARE VULNERABILITIES

- Critical processor vulnerabilities: Meltdown and Spectre
- Fixed now, but gave bad actors open access to private data

What to do:

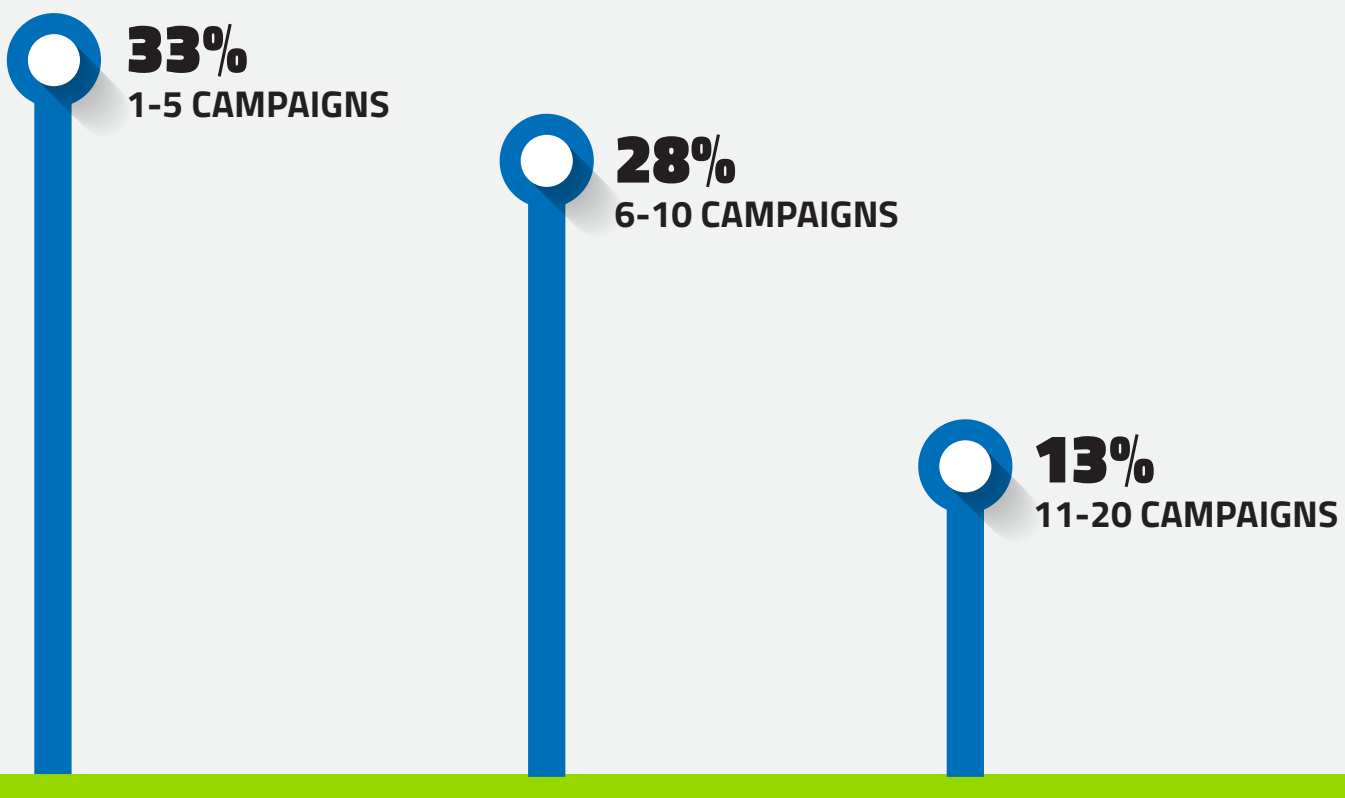
STOP THREATS WITH SECURITY AWARENESS TRAINING

22% of employees have clicked at least one phishing link in the last year.

End users need ongoing training to avoid risks.

Click-through rate based on number of email campaigns

The more training campaigns you run, the more the phishing email click-through rate drops.



For more details on the data, read the full mid-year update to the Webroot® Threat Report.

WEBROOT® Smarter Cybersecurity™

webroot.com/2018ThreatReportUpdate

[1] Verizon. "2018 Data Breach Investigations Report." (April 2018)