Ransomware, cryptojacking, and botnets continue to dominate the threat landscape, but they've seen some interesting developments. The amount phishing attempts increased from Jan to June 2018. 60% of breaches start with phishing attacks.

**Key Report Stats**
- **Phishing**: 60% of breaches start with phishing attacks.
- **Malware**: 35%
- **Cryptojacking**: 12%
- **Botnets**: 8%
- **Proxy Avoidance & Anonymizers**: 5%

**Major Threats, Greatest Hits**

**Ransomware**
- 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

**Cryptojacking**
- Emotet, Trickbot, Zeus Panda are prevalent and persistent
- Concentrate on credential-gathering
- Now use UPnP to turn routers into C&C nodes
- Critical processor vulnerabilities: Meltdown and Spectre
- Fixed now, but gave bad actors open access to private data

**Botnets**
- 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.
- 13% of employees have clicked at least one phishing link in the last year.
- End users need ongoing training to avoid threats.

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.com/2018ThreatReportUpdate