Malicious URL attacks have returned with a vengeance. Ransomware reigns supreme. And fraudsters are aggressively working to impersonate trusted brands in email, social media and the web. Those are just a few of the standout trends we saw in the third quarter.

Here are highlights from the Proofpoint Q3 2017 Threat Report.

**EMAIL**

Malicious email soared 85% from the prior quarter as one of the world’s most prolific attackers launched massive ransomware campaigns. Here’s a breakdown of attacks by type.

- **Malicious URLs** shot up 600% vs. the prior quarter.
- **Ransomware** accounted for 64% of all malware traffic.
- **Email Fraud** increased 29% vs. the prior quarter.
- **Banking Trojans** accounted for 24% of all malicious email traffic.

“**The Trick**” accounted for 70% of that total.

**DOMAIN SPOOFING**

Attackers are aggressively registering lookalike domains that can be used for typo squatting and domain spoofing.

- Suspicious domain registrations outnumbered defensive registrations 20 to 1.
- Defensive registration of brand-owned domains fell 20% vs. the year-ago period.

**SOCIAL MEDIA**

Fraudulent support accounts used for “angler phishing” doubled from the year-ago quarter.

- 10% more phishing links on branded social channels vs. the prior quarter.
- 5% more fake customer-support accounts over the previous quarter.

To learn more about third-quarter threat trends and recommendations for protecting your organisation, get the full Proofpoint Q3 2017 Threat Report.