Threat Intelligence
Q1 2020 Analytics
Overview
This publication provides an overview of our findings and key takeaways from the threat landscape analysis across all reports produced for AXA XL in Q1 2020. Through the AXA XL partnership with Accenture, we are able to offer a range of services to support our clients’ end-to-end cybersecurity needs. Our bespoke Threat Intelligence reports are produced specifically for AXA XL clients, to identify any cybersecurity vulnerabilities and threats, and help them to improve their security posture and overall risk. This summary gives a view of our findings and concludes with some actionable next steps to consider.

Current Threat Landscape

Weaponisation of COVID-19
The COVID-19 pandemic is being leveraged by threat groups for financial, political and espionage purposes. Techniques include phishing, social engineering, malware deployment, vulnerability exploitation and business email compromise.

Key targets: global; government, healthcare, pharmaceuticals, utilities, media

Ransomware attacks
We are seeing continued prevalence of extortion malware being deployed creating additional threats of data disclosure. Ryuk and Maze ransomware are popular for targeting global organisations. Organisations are often initially compromised by popular and successful Emotet or Trickbot trojans.

Key targets: global; local government, healthcare, oil and gas

State actor activity
An alleged Iranian espionage operation called the Fox Kitten campaign has been active since Q4 2019. It aims to steal information from target organisations to develop access routes and breach other companies by leveraging supply chain relationships from the initial infected corporation. The campaign leverages unpatched VPN and RDP services on hosts, which are increasingly being used to support remote working.

Key targets: United States, Europe, Israel, Saudi Arabia, Australia; oil and gas, aviation, telecommunications.

Key vulnerabilities tech findings

Use of outdated infrastructure and insecure protocols
Despite awareness of the risks involved in using outdated infrastructure and insecure protocols, 66% of assessed clients were exposed to web server vulnerabilities and several cases of usage of Telnet, HTTP (unencrypted web traffic) and FTP were observed. Of the web exposure threats identified, 72% related to vulnerable common web technologies.

Sensitive information leakage
10% companies were found to have sensitive manuals, product diagrams, or protocols exposed on public online repositories. These exposed documents may be a gateway to the exposure of valuable knowledge about the company or intellectual property.

Insecure remote access
There has been a surge in remote working activity and subsequent reliance on related infrastructure as a result of COVID-19. When surveyed, 30% of companies analysed had remote access vulnerabilities, which could lead to account takeover attacks. While enabling multi-factor authentication (MFA) can block 99.9% of all account takeover attacks, not many organisations have deployed it for remote workers.
Key vulnerabilities
industry findings

Financial services & retailer industry exposures
Banks and retailers continue to suffer from exposed bank account, credit or store card details that are being published or sold online. One in four banks assessed had leaked customer data, 88% of which was identified on the deepweb or dark net, with the rest on clearen sites such as Pastebin.

Manufacturing industry exposure
There has been a significant quarter-on-quarter rise in web vulnerabilities identified for those Manufacturing clients assessed. Manufacturers were also more exposed to Internet-facing infrastructure and web application weaknesses than other industries. They appear behind the curve on aspects of security despite higher business interruption exposures related to attacks on Operational Technology and Internet of Things footprints, which are increasingly becoming more connected.

Lessons learned from Cyber Claims*

Phishing is still the most common attack vector and was found in approximately 57% of cyber investigations last quarter. The second most prevalent attack vector is credentials access through vulnerable VPN or Remote Desktop Protocol (RDP) access, observed in approximately 15% of cyber investigations. Additionally, 43% of investigations involved successful attacks on cloud-based infrastructure and applications.

33% of the cyber investigations last quarter were related to Business Email Compromise (33%).

17% of the investigations included Ransomware attacks, while a further 17% included commodity malware. These incidents far outweighed other cyber attacks investigated due to the significant business disruption they caused, predominantly in the Manufacturing and Health sector.

RDP vulnerabilities were found to account for 50% of successful Ransomware attacks.

* Based on US figures only

Nature of matter
- 33% Business email compromise
- 17% Malware
- 17% Ransomware
- 11% Application compromise
- 6% OT/ICS
- 6% Unauthorised access to information
- 5% POS / Cred dump
- 5% Fraud

Attack vector
- 57% Phishing
- 15% Credentials access
- 14% Unidentified
- 7% Network access
- 7% External exploit
Be aware of phishing emails and provide training to all employees focusing on:

- Greater awareness of phishing, their “lures”, methods for success and potential business impact.
- Due to increased misinformation and targeting, use only trusted sources for up-to-date, fact-based COVID-19 information.
- Verifying the authenticity of the sources of emails, electronic communications (email and voice) before making decisions related to financial transactions, e.g., making payments, donations and/or transferring funds.
- Avoiding links and attachments from unsolicited emails and not revealing personal financial information.

Increase your focus on cybersecurity tasks related to remote working:

- Patch and update VPNs, network infrastructure, and remote-working devices.
- Conduct security log reviews, attack detection activity, and incident response and recovery preparation to anticipate the impacts of potential cyber attacks.
- Use MFA and strong passwords to reduce the success rate of remote account takeovers.
- Test business continuity plans and VPN limitations to ensure they are optimised to support changes in demand.

Reduce the likelihood of exposure to Ransomware attacks:

- Decommission insecure technologies (FTP, Telnet, HTTP) and replace with more secure alternatives (SFTP, SSH, HTTPS).
- Ensure regular online and offline backups of key business systems are undertaken and actively tested.
- Actively test incident response and business continuity plans with ransomware scenarios.
- Ensure antivirus and active threat detection software is updated and running across your enterprise.

Proactively monitor data breach and disclosure of sensitive data:

- Monitor all data breaches in the public domain and on dark web forums, to identify and remediate exposure of sensitive information.
- Actively monitor corporate brand activity and sensitive data disclosure related to the company on social media, Clear net (public Internet) and Dark net.
- Subscribe to cyber threat monitoring services to gain greater awareness of threats and proactively identify and remediate them.

As part of the AXA XL partnership with Accenture there are a number of pre-breach services available which may help with these key takeaways (fees apply for selected services).

For more information, please click here.