What You Can Expect Next - Cyber Threats and Trends in 2019

Presented by: S. Allen Eaves, Jr.
January 30, 2019
Agenda

• Threat Landscape Trajectory
• Machine Learning and AI
• Updates on the European Union’s GDPR and its effects
• So What?
• Q&A
Verizon 2018 Data Breach Investigations Report

- Breaches in the Financial industry - 79% external, 19%
Source Materials

- Trend Micro’s Mapping the Future: Dealing With Pervasive and Persistent Threats
- IBM – X-Force Labs
- Forrester blog discussing 2019 trends
- Gartner’s Top Strategic Predications for 2019 and Beyond
- Sophos Labs’ 2019 Threat Report
- McAfee Labs 2019 Threats Prediction Report
- Forbes’ list of 60 cybersecurity predictions
- Symantec’s Cyber Security Predictions: 2019 and Beyond
- RSA Security
- BitDefender
- Verizon’s 7 Trends Driving IT Transformation in 2019
- Kaspersky’s 2019 Predictions
- Beyond Trust… whose CTO stated: “There are three jobs in the world where you can be completely wrong all the time and still not worry about being fired. One is a parent. Another is a weatherperson. And the last one is a technology trends forecaster.”
Targets and Tactics continue to diversify

- Supply chain attacks and industry trust
- Increase in targeted attacks
- ‘Living off the land’
- Attacks against IoT
- Mobile attacks
- Cryptocurrency exchanges present easy targets
- Privileged account attacks to continue
- Ransomware attacks not going away
• In 2019, successful exploit-based attacks will involve vulnerabilities for which patches have been available for weeks or even months but have not been applied yet.
  – Tend Micro’s Mapping the Future: Dealing with Pervasive and Persistent Threats
  – Kaspersky’s predicts there will be no more big APTs
• Back to the basics on security (again)…. Verizon
Nation State Attacks

• Cyberespionage driven by trade war with China - US Justice Department
• Pre-2020 Election Influence (Russia) - Director of National Intelligence
• Sanctions driving an Increase in Iranian and North Korean cyber activity – US Cyber Command (hacking force in DoD)
  – $1.1 billion attempted theft from global banks
AI – Helpful or Overstated?

• 2019 ForcePoint Cybersecurity Predictions Report:
  – Disillusionment sets in as AI and machine learning are held accountable for their claims
  – **Prediction:** There is no real AI in cybersecurity, nor any likelihood for it to develop in 2019.

• Symantec’s Cyber Security Predictions:
  – Defenders will depend increasingly on AI to counter attacks and identify vulnerabilities
GDPR Impacts

• **IBM: WHOIS Behind Cyberattacks? Under GDPR, We May Not Know**
  – Identification of malicious domains connected to bad actors becomes an enormous challenge due to the elimination of WHOIS data

• **Brian Krebs:**
  – “I have worked the majority of my professional career to expose those who are doing the spamming and scamming. I can say without hesitation that an overwhelming percentage of that research has been possible thanks to data included in the public WHOIS registration records.”
So what?

• Be vigilant – implement systems for early breach detection
• Make people and non-security staff an effective line of defense
• Utilize the principle of least-privilege and only keep data on a need-to-know basis
• Patch promptly after testing
• Encrypt critical and sensitive data
• Use strong authentication including two-factor
Thank you!

S. Allen Eaves, Jr. – CISSP, CRISC, SSCP, CISM, CFE
Director of Information Security & Compliance Services
aeaves@jackhenry.com

Q & A