Cyber Threats and Trends for 2022

S. Allen Eaves, Jr. CISSP, CISM, CRISC, SSCP, CFE
Managing Director, Gladiator and Centurion

SolarWinds to Log4j: How did the 2021 Predictions Go

- JBS Foods (world's largest meat processor) - Russian hacker group REvil.
  - JBS Foods paid an $11M ransom.
- Brenntag (chemicals and ingredients distribution) - DarkSide stole 150GB of files with demand of $7.5M, paid $4.4M ransom
- Acer (computer manufacturer) – REvile exploited Microsoft Exchange vulnerability to access files. $50M ransom demand
- French base global insurance company AXA attacked by Avaddon who stole 3TB shortly after they announced that they would stop reimbursing clients for ransomware payments.

All the prior events were in May 2021 following the Colonial Pipeline hack in April 2021

- Paid DarkSide $4.4 million dollars in bitcoin (with significant recovery)

SolarWinds to Log4j: How did the 2021 Predictions Go

- Ransomware evolving – more automation – 2/3 of attacks by low-level threat actors using ransomware tools
  - Increased extortion attacks

  -According to the UK National Cyber Security Centre, there were three times as many ransomware attacks in the first quarter of 2021 as there were in the whole of 2019
- Legitimate IT management tools used as malware

  -SolarWinds, Kaseya (REvile's attack of legit software update process - $70M ransom demand)
- Supply Chain Attacks
  - Quanta – Apple's major business partner (REvile) $50M ransom demand. Turned to target Apple and released product blueprints
  - SolarWinds Orion and Log4j
- Increased regulatory pressure and stronger penalties
  - Federal breach notification requirements expanded beyond PII?

Some Good News from 2021

- In November 2021, 5 individuals of the REvil group were arrested by Europol (European law enforcement agency)
  - According to Fortune, “the alleged hackers are suspected of involvement in about 5,000 ransomware infections”
  - The U.S. indited 2 men of the operation. According to NPR, “If convicted of all counts, each faces a maximum penalty of 115 and 145 years in prison”
- U.S. State Department has announced $10M reward for info leading to “any individual holding a key leadership position” in REvil

4

Verizon Data Breach Investigations Report - 2021

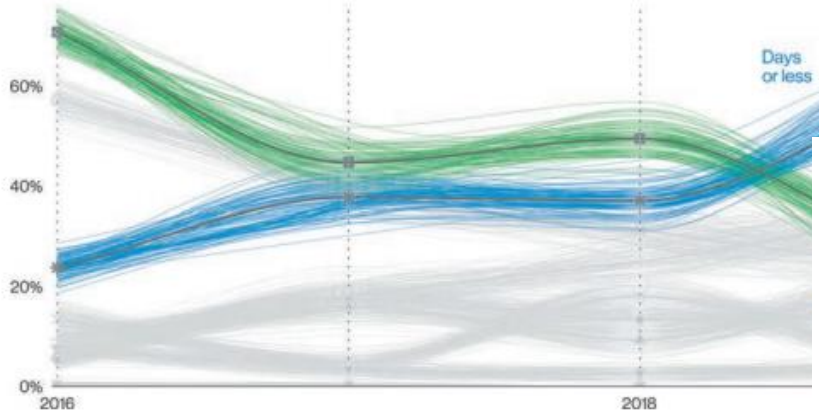

Figure 39. Discovery over time in breaches

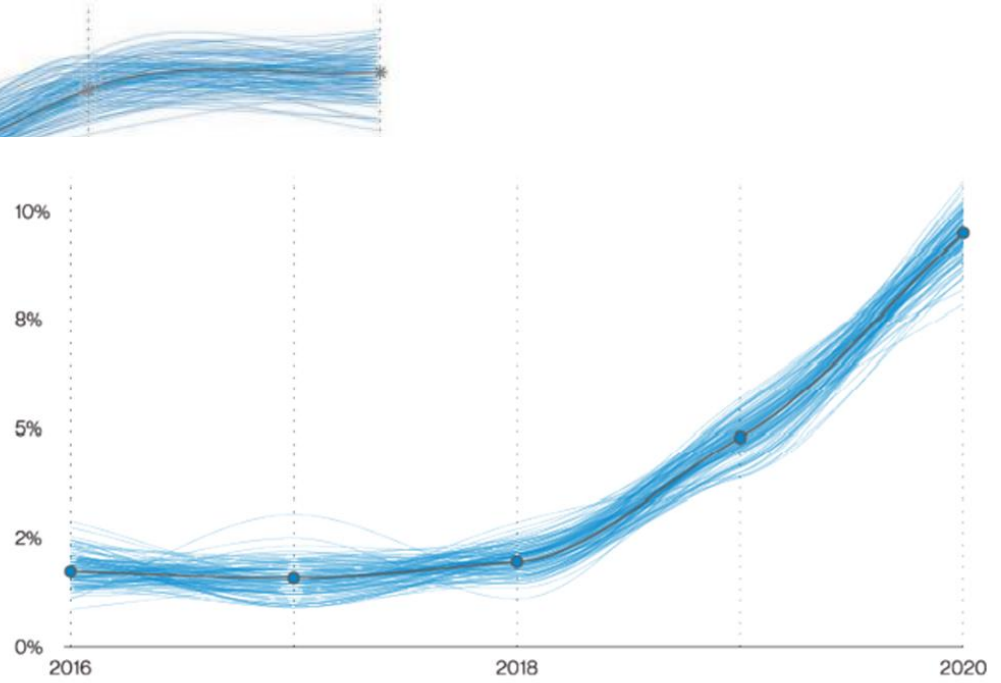

Figure 83. Ransomware in breaches over time

According to Sophos, the average total cost of recovery from a ransomware attack has more than doubled in a year, increasing from $761,106 in 2020 to $1.85M in 2021.

Of the cases reported the average ransom paid was $170,404.

In 2021 out of all ransomware victims, **32% paid the ransom**

46% of all global cyberattacks were directed towards the United States keeping it as the most highly targeted

6

- Forbes' *The Five Biggest Cyber Security Trends In 2022* and *Cybersecurity in 2022 – A Fresh Look at Some Alarming Stats*
- NetSpi's *New Year, New Trends: 2022 Cybersecurity Predictions*
- Security Magazine's *Expect 2022 to be the year of cybersecurity'*
- 2022 Cybersecurity Trends: A Q&A with Fortinet CISOs
- Splunk's *Data Security Predictions 2022*
- *Verizon's 2021 Data Breach Investigations Report*
- *Sophos 2022 Threat Report*
- *Crowdstrike 2021 Global Threat Report*
- Cybersecurity Trends: IBM's Predictions for 2022
- 2022 Cybersecurity Predictions from the RSA Conference Advisory Board
- 2021 Cyber Attacks Hit Infrastructure and Critical Facilities Across the US
- *Cybersecurity Predictions for 2022 from F5 Labs (and Friends)*
- Purdue University's *Cyber Predictions for 2022*
- DarkReading's *5 AI and Cybersecurity Predictions for 2022*
- BeyondTrust's *Cybersecurity Predictions for 2022 and Beyond*

2022 Predictions

- Cybersecurity insurers will require more cybersecurity protections and ask more technical questions
- More focus on risk in cybersecurity budgeting compared to just meeting compliance needs or to check-the-box
- Cybersecurity will be a key factor in partnership decisions
  - Gartner predicts that, by 2025, 60% of organizations will use cybersecurity risk as a "primary determinant" when choosing business partners
- List of “terrorist organizations” that can’t be paid ransom will increase - pushback from private business to proposed ransomware disclosure proposals

2022 Predictions

- Beyond Double Extortion – Ransomware gets even more disruptive
  - Extortion will not stop at victim's organization and will go after business partners
- Ransomware syndicates may shift focus from nations such as the US and the UK to stay out of active law enforcement's crosshairs
- Blockchain used to hide and obfuscate malicious traffic making it difficult for defenders to spot malicious activity (similar to the benefit and challenge brought by encryption)
- Look for additional pressures from multiple concurrent/hybrid attacks. Ransomware and DDoS

Take a Zero Trust approach reduce exposure

Leverage current Threat Intel into live analytics

Review traditional protections - Decrypt for Security Inspection

Fast track critical security fixes. Test and patch promptly

Solidify detection and response plans. Not just prevention

Use Risk Assessments to most effectively improve security

Cyber Threats and Trends for 2022

S. Allen Eaves, Jr. CISSP, CISM, CRISC, SSCP, CFE
Managing Director, Gladiator and Centurion