The Future of Ransomware & Other Cyber Attacks

Mark Dallmeier
Vice President Channels & Sales Operations
Avertium

Association of Local Government Auditors
September 10, 2019

Speaker Bio, Resources

• Turn Around & Transformation Consultant
• 400+ Audits & Assessments
• CEO, President, CSO, CMO
• Board Director, Advisor
• Serial Entrepreneur
• Industry Researcher, Analyst, Speaker

HP
Hitachi Global Services
Verizon Business
XO Communications
Avent
IT Partners
Sage Software
Stach & Liu, (BishopFox)
3Sigma Corporation
Qwest

Previous Research, Presentations
https://www.tvrms.com/resources

2018 & 2017 Cybersecurity Trends & Predictions:
“Cyber Attack Trends & Industry Predictions.”
“Future Impact of the Equifax Breach.”

2018 & 2017 Phoenix SAC Conference:
“Beyond Ransomware”
“The Future of Ransomware.”

2017 & 2016 TribalNet:
“The Mind of a Hacker.”
“Ransomware.”
Agenda

01 Threat History
   How we got here

02 Current State
   What we are dealing with

03 Predictions
   What we could be in for

04 Best Practices
   How to defend, protect, prepare

History of Cyber Threats, Attacks
Evolution of Ransomware, Business Email Compromise, Other Attacks
The Technological Weaponization of Criminal acts that are thousands of years old.

Julius Caesar, Chas Lindbergh Jr., John Paul Getty III, Frank Sinatra Jr., Patty Hearst
Current State & Evolution of Ransomware, other Attacks

Ransomware Evolution

- Misleading Applications
- Rogue/Fake Antivirus
- Locker Ransomware
- Crypto Ransomware

2008-2014
2010-2014
2013-

WannaCry
SamSam
GandCrab
Ryuk
2016 Explosion

CryptoHasYou, 777, 7ev3n, 7h9s, 8lock8, Alfa Ransomware, Alma Ransomware, Alpha Ransomware, AMBA, Apocalypse, ApocalypseVM, AutoLocky, Booyah, Brazilian, BrLock, CryLocker, CrypMIC, CrypToyFortress, CryptoGrim, CryptoShocker, CryptoTheft, CryptXXX 3.0, CryptXXX, DetoxCrypto, DirtyDecrypt, FairWare, Fakben, Fantom, Herbst, Hi Buddy!, Hitler, I PJeiphoos, Job Crypt LeChef, LeChef, Linux.Encoder, L MM Locker, Mobef, Nano: Operation Global III, PadC encryptor, Radamant, Rak Sanction, Satana, Scraper, Sport, Stampado, Strictor, TeslaCrypt 4.2, Threat Finder, Ungluk, Unlock92, VaultCrypt, ZeusLock 4.1A, zenRansom, UmbreCrypt, Zlader / Russian, Zyklon

Why Malware is Effective

$12B in BEC Damages
120% Growth

27% of Employees are Prone to Phishing

Diverse Exploit-Kits-Web-Docs-Links, New RaaS

THE SITUATION with crypto-ransomware changed with the emergence of CryptoLock in 2015. CryptoLock defined the business model and proved the opportunity. The growth in that business model has been explosive as this graphic clearly shows. Need we say more?
Growth from 2016-2017

Detections 2015 - 2017

- **2015**: $325M in projected damages
- **2016**: $1B in projected damages (2016 increase: 819%)
- **2017**: $5B in projected damages (2017 increase: 415%)

F-Secure The Changing State of Ransomware 2018

2018 Research

Detections FH 2017 – FH 2018

- **1H 2017**: 196,832
- **2H 2017**: 369,988
- **1H 2018**: 380,290

- **$8B in projected damages**

Families, Variants 2H 2017 – FH 2018

- **2H 2017**: 159
- **1H 2018**: 118

Trend Micro 2018
In recent months we’ve told you about ransomware distribution kits sold on the Dark Web to anyone who can afford it. These RaaS packages (ransomware as a service) allow people with little technical skill to attack with relative ease.

~ Sophos 2018
Ransomware Evolution

Cybercriminals continued to evolve their approach to maintaining and deploying ransomware; new ransomware families of 2018:

GandCrab, Ryuk, BlackHeart, SynAck, and Black Ruby.

GandCrab emerged in Q1 2018 and was noted for improved encryption and decryption routines and persistence within infected systems. Indicating the developers could adjust quickly to GandCrab’s success or failure in the wild. $2B in Damages!

BlackHeart packages a malicious payload alongside a legitimate but outdated version of AnyDesk, hiding what the ransomware was doing in the background.

SynAck was the first to utilize a doppelgänging technique, introduced in 2017, that can make detection and analysis by researchers difficult.

Black Ruby functions as ransomware and also installs a Monero cryptocurrency miner. Cryptocurrency mining is considered highly profitable ventures by cybercriminals.

2017 – 2018 Predictions

• Phishing
• Spear-Phishing
• Targeted Attacks – Whaling
• Coordinated Attacks
• Automated Attacks

• Targeted, Automated Multi-Stage Attacks Integrated w/ Physical Attacks
• Orchestrated Multi-Threaded Attacks Utilizing Malware, Ransomware and Weaponized Tool Kits
• Bundled into Criminal Storefronts Powered by As a Service Platforms/Services
Threats & Attacks

- **Phishing**: Harvesting Credentials, Malware Delivery = *Fraud, Theft*
- **Ransomware**: Coinhive, Dorkbot, SynAck, Black Ruby, Ryuk = *Theft, Damage*
- **Business Email Compromise**: Fraud, Scams, Malware Delivery = *Theft*
- **Business Process Compromise**: Fake Business Processes = *Theft, Espionage*
- **System Process Compromise**: Monero Cryptomining = *Theft*

- **Embedded Code**: Specter, Meltdown
- **AI-Malware-Exploit Kits**: GandCrab, Coinhive, Dorkbot
- **Botnet-DDoS-PDoS**: Mirai, WireX, Reaper, Hajime, BrickerBot
- **Telnet Brute Force, SSH, APT, Malwareless Attacks**: Stuxnet, RDP
- **Harvesting, Snooping, Skimming**: Traffic Spirit, MageCart, etc.

---

2018: Laying the Groundwork

City of Allentown computer systems hit by virus that will require nearly $1M fix

Ransomware Attack Costs Idaho County $100,000

Credit Union Cybersecurity in 2018: Biggest Threats and 3 Practical Solutions

Local Government Cybersecurity in 2018: Blocking Ransomware and Other Threats

Credit Union

Local Government
According to a report by Malwarebytes, there has been a 363% year-over-year increase in the first half of 2019.

Current State: Targeting Sectors

Coordinated Ransomware Attack Cripples Local Government Organizations in Texas

August 19, 2019

The Texas Department of Information Resources (DIR) recently reported that the systems of 23 organizations in the state, mainly smaller local governments, were affected by ransomware attacks that ramped last Saturday, August 17. The attacks, according to DIR, appeared to be coordinated, with the evidence gathered so far indicating that the attacks were initiated by a single threat actor.

In a statement, the DIR said, “Currently, DIR, the Texas Military Department, and the Texas A&M University System’s Cyberresponse and Security Operations Center teams are deploying resources to the most critically affected

Healthcare Value Chain Targeting
The FBI revealed that over 100 enterprises have suffered from Ryuk attacks since 2018, mostly logistics, technology companies and small municipalities.

Trend Micro 2019
Tactics

Fileless Events: 18% Higher Than All of 2018

Ransomware Related Detections Outpacing all of

Damages $11B +

Rash of ransomware continues with 13 new victims—most of them schools
Elsewhere, dentists get in on the fun and Baltimore raids parks money to pay for repairs.

Source: Compraciti, Inc.

Ransomware Attacks Are Testing Resolve of Cities Across America

The New York Times
Ransomware & Crimeware Predictions

“While GandCrab may no longer be a threat, other forms of ransomware will rise up and take its place, especially given how many organisations have chosen to pay six-figure sums after falling victims to an attack. That’s despite law enforcement and security companies telling them not to give in to the demand.”
-ZDNet Article: Cybercrime: Ransomware attacks have more than doubled this year August 28, 2019.

WHAT...??

2017 – 2018 Predictions

- Phishing
- Spear-Phishing
- Targeted Attacks – Whaling
- Coordinated Attacks
- Automated Attacks

- Targeted, Automated Multi-Stage Attacks Integrated w/ Physical Attacks
- Orchestrated Multi-Threaded Attacks Utilizing Malware, Ransomware and Weaponized Tool Kits
- Bundled into Criminal Storefronts Powered by As a Service Platforms/Services
Ransomware Attack Hits 400 Dental Offices Across the US

The attack struck on Monday morning and targeted The Digital Dental Record, a provider of IT software to dental offices. Reportedly, 400 dental practices have been affected nationwide.

“Relatively new on the ransomware scene, Sodinokibi (A.K.A. REvil) has already made impressive profits for its administrators and affiliates, some victims paying as much as $240,000, while a network infection netted $150,000 on average.”

~ BleepingComputer August 30, 2019

The Rising Tide of Crimeware-as-a-Service

Malware, botnets, phishing and backdoors are all offered on the cheap as subscription. These days even crime is in the cloud.

2020 & Beyond

Beyond: Cyber Hostage
Human, Physical, IT

- Highly Orchestrated Attacks
- Targeting Business, Individuals, Government, IT
- Utilizes IoT Exploits to Gain Full Situational Control
- Physical Buildings, Transportation Devices w/ People Involved
- Acceptance of Various Payment Types

Beyond: Criminal Enterprise 2.0

- Bundled Services
- Based on Bitcoin, Cyber Currencies
- 24x7 Support
- Industry, Geography, Market Segment Focused
- Potential Business Opportunities
- Self Funded Via Fiat Currency Value Inflation

Beyond: Business & Brandjacking

- Duplicated Business Process
- Supply and Value Chain Command and Control
- Targeted at Products, Lines of Business or Brands Initially (beta testing)
- Can lead to new Federal or Industry Seal of Approval – Certification, Regulation
How to Defend, Protect, Prepare

- **Patching** (Planned, Automated)
- **Passwords** (Methods, Vault)
- **Backups** (Full-Off Network)
- **People** (SETA, Internet Usage, Disengaged Employees)

  - Limit, Lock Down Admin System Access Control/Write
  - **Encryption** (At Rest, In Transit)
  - **Limit, block network access** (RDP, etc), email ext delivery
  - **Updated BCDR Plans** (Ransomware, Social Engineering)
  - **Business Process Audits**

Summary:
Disengaged and disgruntled employees are the weakest link.
BEC, Phishing and Attacks that exploit legacy unpatched or non-hardened systems will be pervasive.
Audit and Assess these areas.

- Security Ops, Monitoring
- End Point, IoT Protection
- IoT Inventory, Assessment & Penetration Testing
People, Passwords, Patching, Program

**People**
- Security Education, Training & Awareness Programs (SETA)
- Cyber Declarations & Address Disengaged, Disgruntled Employees
- Phishing Simulations

**Passwords**
- Password Phrases with Special Characters
- Infrequent Changes
- Password Vaults and Manager Programs

**Patching**
- Prioritize Systems and Assets that are Vulnerable (crown jewels)
- Understand Frequency of Updates, Patching
- Prioritize Patching Timeframes, Windows

**Program**
- Identify Gaps in Maturity Level of Program, Policies, Technologies
- Update BCDR Plans to Address BEC, Phishing, Ransomware
- Cyber Hygiene Program (Vulnerability Management)

---

**What is Optimal:**

- **Cyber Declaration from C Suite** – Training is not Enough
- **Integrate Physical - Cyber – Employee Engagement Programs, into Risk Audits, Assessments, Processes**
  - Expanded SOC; Include Physical & Macro-Micro Geographical – Social Intelligence
- **Table-Tops & Simulated Physical and Cyber Attacks – Whaling.**
- **Simulated Ransomware, BPC, BEC Attacks**
  - Integrate Response Methods into BCDR Plans
  - Next Gen Authentication, Access Control Tech-Methods
  - Master Change Management (its inevitable)
Questions

- Trends, Attacks
- How to Defend, Prevent, Prepare
- Governance, Programs, Approach

*Offer: 1-2 hour fireside chat with a Practice Manager

Thank You!

Mark Dallmeier
Vice President Channels & Sales Operations

Direct: 602-410-7793
email: Mark.Dallmeier@avertium.com