Ransomware: Evolution & Cyber Threat Landscape

Presenter: Richard Cassidy | Alert Logic
PIONEERING TECHNOLOGY

1982

Accudata Founded

1985

Accudata recognizes the power of networking and joins forces with Novell to bring its network operating system (NOS) to businesses.

1989

Accudata pioneers the Ethernet switch through a partnership with Kalpana. In 1994, Cisco acquires Kalpana and, 20 years later, the partnership remains strong.

1994

Accudata sees the need for enhanced security across the expanding network and becomes one of the first to bring Check Point's FireWall-1 to businesses.

2008

Accudata recognized as Houston's largest computer network and systems integrator

2014

With a team that spans across Houston, Dallas, Austin, San Antonio, and Los Angeles, Accudata leads the way in the convergence of operations and information technology. Our focus - business outcomes.

2020

The Future of IoT

©Accudata Systems, Inc. 2016
Alert Logic – a Leader in Forrester’s 2016 NA MSSP WAVE™

Forrester Wave™: North American Managed Security Services Providers, Q3 ’16

The Forrester Wave™: Managed Security Services Providers, North America, Q3 2016

“Alert Logic has a head start in the cloud, and it shows.

Alert Logic is an excellent fit for clients looking to secure their current or planned cloud migrations, clients requiring a provider than can span seamlessly between hybrid architectures, and those that demand strong API capabilities for integrations.”

- Forrester WAVE™ Report

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.
## Before We Begin

### Housekeeping

- **Turn on your system’s sound** to hear the streaming presentation.
- **Questions?** Submit them to the presenter at anytime into the question box.
- The webinar will be **recorded & published**.
- **Technical Problems?** Click “Help”.

### Speaker

- **Richard Cassidy**
- Cyber Security Evangelist & Technical Product Marketing
Understanding Threats

The Analysis: Cyber Kill Chain® Approach

- Attacks are multi-stage using multiple threat vectors
- Takes organizations months to identify they have been compromised
  - 205 days on average before detection of compromise\(^1\)
- Over two-thirds of organizations find out from a 3\(^{rd}\) party they have been compromised\(^2\)

\(^1\) – IDC Worldwide Security and Vulnerability Management 2014–2018 Forecast
\(^2\) – M-Trends 2015: A View from the Front Lines
RANSOMWARE: THREAT ACTORS, CYBER ECONOMY & EVOLUTION
Three Classes of Threat Actor

Hacktivist

Cyber Criminal

Advanced Persistent Threat (APT)
Monetization

Underground Market

Crypto Currencies
Point & Click Ransomware Campaigns

Ransom32
- Crimeware-as-a-service
- Dashboard
- BitCoin payment stats
- Malware configuration
- Varied threat messages

Source: krebsonsecurity.com
**What is Ransomware?**

**CRYPTO RANSOMWARE**

- **Crypto** prevents access to files or data.
- Once installed on the host system, files are encrypted and rendered unusable until decryption key is provided.
- The latest trends in ransomware often involve high levels of encryption, making it difficult or even impossible to crack keys.
- Historically endpoint focused

**LOCKER RANSOMWARE**

- **Locker** denies access to the computer or device that has been infected.
- Locker variants will normally disable an interface or peripheral access to the device.
- Locker variants normally won’t affect the underlying operating system or files.
- Historically end point focused
History Of Ransomware Variants

Ransom demand variation over time.

- AIDS Trojan $189
- Gpcode $300
- Seftad $175
- Gpcode $175
- Anti-Virus XP $100
- Anti-Virus XP $50
- WinLock $10
- Reveton $150
- CryptoLocker $300
- FBI $300
- CoinVault $220
- Sypeng $200
- SimpLocker $200
- Find my iPhone $100
- CTB-Locker $700
- Cryptowall $500
- TeslaCrypt $500
- TorrentLocker $500

- File Encryption
- Scare-ware
- Lock out
- MBR Encryption
- SMS Lock Out
- Mobile
- Mac
INDUSTRY ANALYSIS
Proliferation of Ransomware

- 500% Increase in Ransomware infections over 2yrs
- 51 Million Endpoints Q3FY2015 alone
- Increase in Server Side Ransomware Variants Q4FY2015
- Increased ransom payments has led to stark increase in ransomware proliferation in 2015

Source: McAfee Labs, McAfee Labs Threats Report, November 2015
DISSECTING RANSOMWARE: THE CYBER KILL CHAIN
Understanding Ransomware

- Targeted Or Random E-Mail Campaigns
- Server Side Exploits (Malvertising, Compromised Sites, etc.)

- Delivery of Infected Payload (Word, Excel, PDF, Malicious Link)
- Zero Day Browser Exploits (Via Infected or Malicious Websites)

- Command & Control Network Communication (Key Exchanges)
- Host File Encryption & Removal of Original Data

- Normally achieved in initial attack proliferation
- Crypto Worms – Seek additional internal hosts for infection

- Completion of Data Encryption/Locking Function
- Ransom Payment (BitCoin)
Ransomware: Anatomy of Attack – Client Side

- CERBER
  - Phishing Attack
    - E-Mail with infected attachment received & opened
    - Attachment infects local system, ransomware downloaded
    - Cerber searches for backups and shadow copies for deletion
    - Encrypts files and messages user for payment
  - Exploited WebSite
    - User visits malicious website (Typosquat, Compromise or Phishing e-mail)
    - Website exploits vulnerable web browser plugin
    - Ransomware downloaded to client machine
    - Cerber searches for backups and shadow copies for deletion
    - Encrypts files and messages user for payment
Case Study: Tewksbury Police Department

Attack
• Spam Email (fake notice of package delivery)
• Employee clicked on a link, downloaded malware
• Attacker gained access and encrypted data
• Ransom demand of $500

Impact
• Operation disruption
• Revert to manual processes
• No access to arrest records/warrants
• Unable to conduct ID verification

Five days with no IT function. Public and private security experts unable to decrypt. No technical mitigation.
Ransomware: Anatomy of Attack – Server Side

• SAMSAM

  • Unpatched JexBoss Vulnerability Targeted
    • Remote Shell Access gained to Web Application Server
  • SamSam Ransomware downloaded by attacker
  • Ransomware distributed via server to internal hosts
  • Shadow Backups searched and removed
  • Trojan Installed
  • Ransomware Encrypts files and messages user for payment
  • Average requests at $18,500 (45 BitCoins)
  • Money received by associates through BitCoin mixing to prevent trail being recorded
Case Study: SamSam Medical Targets

**Attack**

- Unpatched JexBoss Vulnerability discovered using Open Source scanning tools

OR

- Stolen (or Phished) login credentials used to gain access to vulnerable Web Application Server
- SamSam Ransomware Installed & Network Hosts Infected; Users messaged for Ransomware payment

**Impact**

- Operation disruption
- Loss of access to patient records
- Manual processes instigated, treatment delayed or cancelled
- Financial Impact (FBI recommendation in some cases is to pay ransom)

New variants targeting Education Sector
PROTECTION & MITIGATION
BEST PRACTICES
Ransomware: Detection & Mitigation

MONITOR & IDENTIFY
• Monitoring across all layers of the technology stack
• Effective Threat Intelligence, Research & Content
• Real-Time inspection across all data streams

DETECT & CONTAIN
• 24x7 Monitoring & Expert Analysis
• Detection of Ransomware IOC’s (Client & Server)
• Quarantine, Control & Blocking Capabilities

RESPOND & MITIGATE
• Complete Visibility of Ransomware Infection Campaign
• Incident Response & User Communication
• Security Controls & Best Practices Review
Ransomware: Protection Best Practices

- Backup strategy
- Patch management
- Endpoint security tools
- Log management strategy
- Data classification & inspection
- Cyber security awareness program
- Stay informed of the latest vulnerabilities
ALERT LOGIC APPROACH
Detecting Cyber Security Threats

Data Collection → Threat Data Analytics Platform → Threat Intel & Security Content → 24x7 Monitoring & Escalation → Continuous Detection of Threats & Exposures

Your Team → Threat & Exposure Remediation Tactics
## Preventing Malware Attack

**Customer Type**: Retail – E-Commerce  
**Threat Type**: CryptoWall (Ransomware)  
**AL Product(s)**: Cloud Defender

### MALWARE ACTIVITY
- Citrix Gateway Server becomes Infected with Malware
- Malware C2 Activity to malicious IP
- Analyst Investigates Events Data – TM & LM

### INCIDENT ESCALATED (Critical)
- Analyst performed detailed review of packet & log data to confirm Malware C2 Activity & identify potential lateral movement attempt
- Call to customer stakeholder to inform of threat and advise of remediation actions

### MALWARE CONTAINED
- Customer contains infected Citrix Server & removes from network
- Server recovered from backup
- Attack Source Blocked
- User access restored in under 25mins of initial incident escalation
Preventing Malware Attack

Customer Type: Manufacturing
Threat Type: Cerber (Ransomware)
AL Product(s): Cloud Defender

MALWARE ACTIVITY
- CD flags a possibly infected host with Cerber Trojan
- Cerber Trojan is a variation of a known Ransomware variant.
- Analyst begins immediate review of packet & log data

4 min

INCIDENT ESCALATED (Critical)
- Detailed data analysis discovers host calling out to a previously unknown C&C sever IP
- Traffic pattern through signature analysis also confirms analysis of Cerber Ransomware variant
- Analyst immediately calls customer stakeholder informing of critical incident and required remediation steps

11 min

MALWARE CONTAINED
- Customer disconnects infected host from its network.
- Malicious C2 IP Blocked
- Infected Host Re-Imaged
- Ransomware outbreak contained
- Full AV SCAN of entire organization performed to detect other potentially infected hosts
FURTHER RESOURCES
Websites to follow

http://www.securityfocus.com
http://www.exploit-db.com
http://seclists.org/fulldisclosure/
http://www.securitybloggersnetwork.com/
http://nvd.nist.gov/
http://cve.mitre.org/
https://www.alertlogic.com/weekly-threat-report/
Thank you.
Schedule a Complimentary Consultation to review your current capabilities to mitigate Ransomware Vulnerability Assessment Services

Backup Health Check

Email: Brian DiPaolo, Practice Director
BDiPaolo@AccudataSystems.com