
SCTE®
CABLE-TEC EXPO®
FAST FORWARD 2021
ATLANTA, GA
OCTOBER 11-14
SCTE
a subsidiary of CableLabs®
UNLEASH THE POWER OF LIMITLESS CONNECTIVITY
2021 Fall Technical Forum
SCTE® • NCTA • CABLELABS®

SCTE
a subsidiary of CableLabs

Security & Privacy

Security Strategies in the Wake of Nation-State Attack Evolution

Nancy Davoust

VP II, Security Architecture
Comcast Cable

2021 Fall Technical Forum
SCTE • NCTA • CABLELABS

SCTE CABLE-TEC EXPO FAST FORWARD 2021

VIRTUAL EXPERIENCE
OCTOBER 11-14

Nation-State Attacks Increased 100% Since 2017

Most Advanced Persistent Threats come from Nation-State Attacks

"*Nation States, Cyberconflict and the Web of Profit*", HP Wolf Security, HP, https://threatresearch.ext.hp.com/web-of-profit-nation-state-report/, April 8, 2021

Professional Groups in Operation for 10+ years

Who

- North Korea
- Russia
- China
- Iran
- eCrime (non-nation sponsored organized cyber attackers)

What

- Infiltrate Targets & Stay Below the Radar
- Recognizance to Map Network Resources and Gather Credentials
- Exfiltration to Plant Malware, Steal Data or Perform Other Criminal Acts

Nation-State Attacker Goals

- Political Statements
- Political Influence
- Theft of Political or Military Data
- Disinformation Campaigns
- Disruption of Services with Economic Impacts
- Financial Gain

Nation-State Attacker Advances

Types of Attacks

- Election Interference
- Ransomware Exfiltration
- Corporate Espionage
- Economic Damage

Political Posture

- July 2021 – China passed a zero-day vulnerability law which states that anyone in China finding a zero-day vulnerability is required to provide the information to the CCP and is prohibited from sharing it otherwise

Protections Against Nation-State Attacks

1. Patch!
2. Strong Authentication for People, Applications and Devices
3. Full Lifecycle Management with Least Privileges for Application and Data Access
4. Data Encryption at Rest, in Transit and in Queue
5. Logging & Monitoring Levels Appropriate to Risk Level
6. System, Device and Application Hardening with Adjustable Policy Configurations
7. Ransomware Protection (data duplication and application rebuilds for resiliency)
8. Micro-segmentation to Reduce Blast Radius
9. Consistent and Constant Use of and Updates to Best Security Practices including Zero Trust Principles

Zero-Day Software Vulnerabilities

- Nation-state attackers are proficient in utilizing outdated software to attack
- Software update patch notes utilizes to create exploits
- WannaCry
  - Microsoft SMB protocol exploit

Defenses:

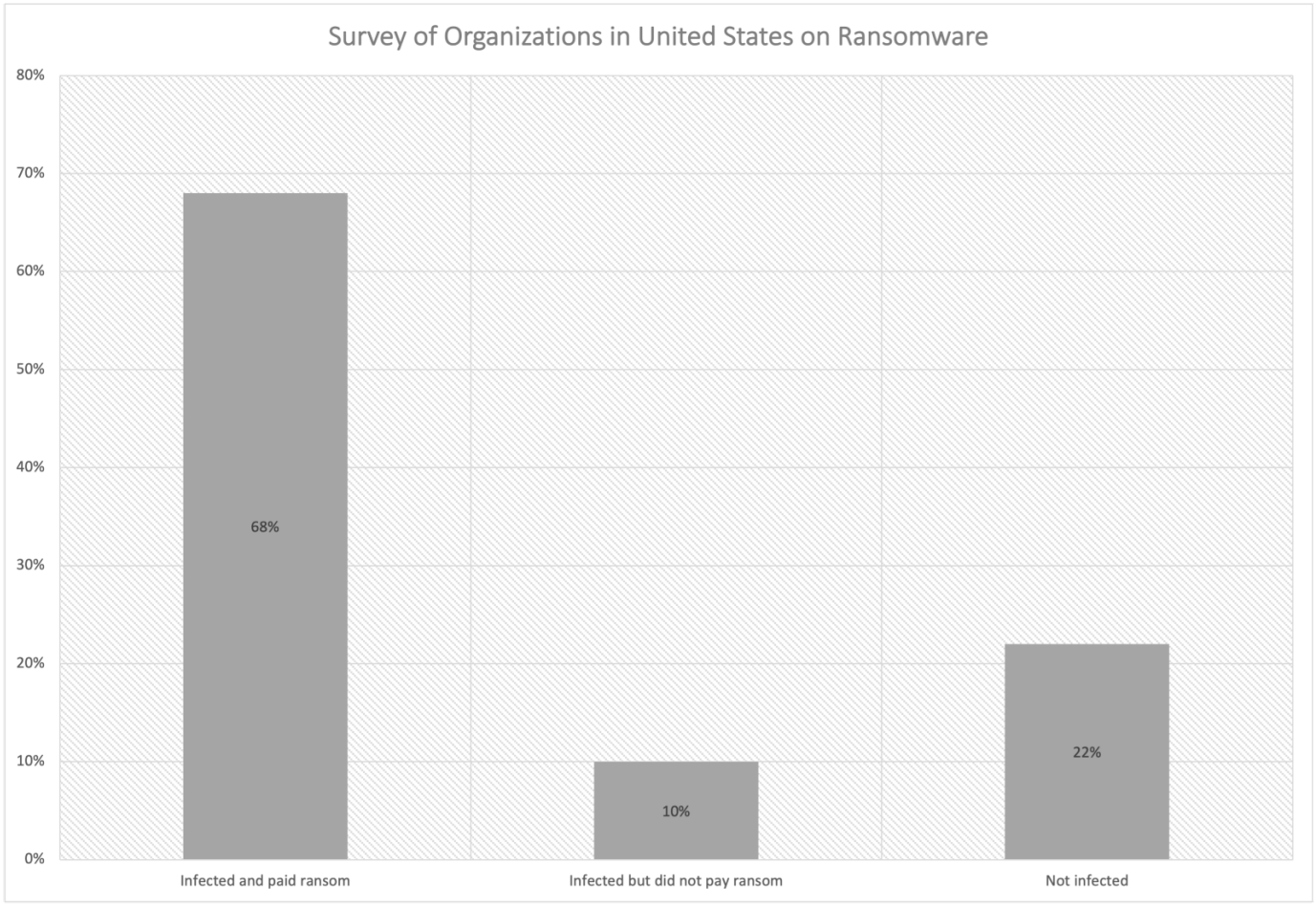
- Immediate patching process for security patches
- Monitoring of system

Ransomware

- Type of malware that encrypts user data
- Prompts for payment before decrypting
- Never guarantees that data will be decrypted
- Secondary charge to not leak data

Defenses:

- Separated disaster recovery environment
- Replica of production environment



Why We Care

IOT Device Security Vulnerabilities

Common Vulnerabilities are Exploited by Nation States

- Default Passwords & Strong Authentication

- Open Ports and Web Interfaces
- Susceptible Network Connections

- Inadequate Secure Software Updates (Mechanism and Frequency)
- Insecure Configuration (Mechanism and Storage)

- Lack of Integrity Monitoring

- Unprotected Secrets and Data

- Vulnerable Ecosystem

- Weak Supply Chain Security

Lessons Learned & Create Right Ecosystems

Improvements Needed

- Standards & Designs – Technical Implementations for How IoT Devices Should Comply
- Testing and Compliance Measures - Ensure Implementations Meet Laws and Standards
- Ongoing Operational Support – Secure Configuration and Patching

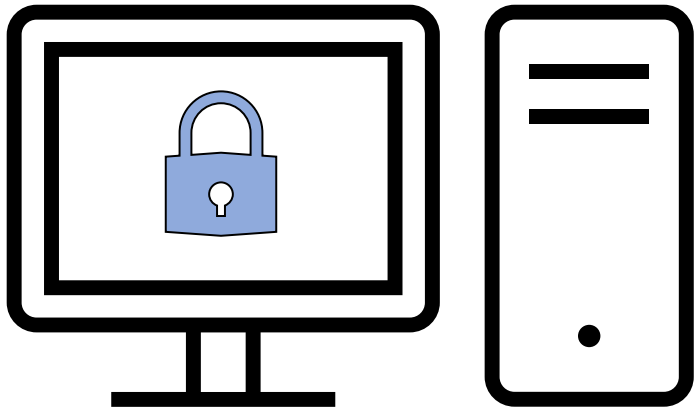
NIST Security Controls Framework

- Identity, Protect, Detect, Respond, Recover
- Measure Security Maturity

Keep Up on the Latest Vulnerabilities & Attacks!

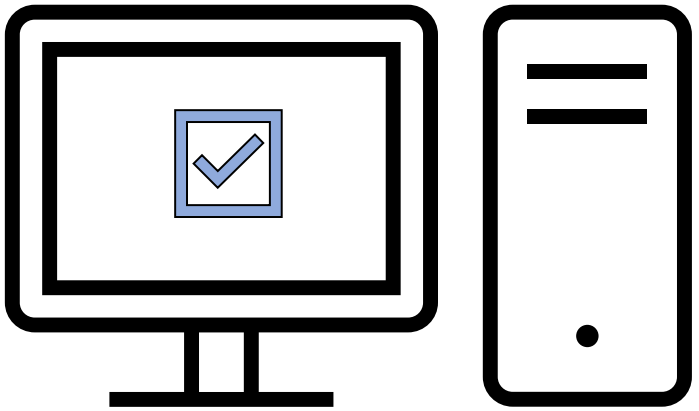
Create strong identity, authentication, and access policies

Authentication vs. Authorization



Authentication

Confirms users are who they say they are



Authorization

Confirms users have right to access specific resources

Identity, Authentication and Access

For People

Provide the right people with the right access at the right time

For Applications

Provide strong user and application authentication, and real-time authorization

For Devices

Provide device identity, device health, and strong authentication

Identity, Authentication and Access Necessities

For People

1. Managed Identity
2. Strong Authentication
3. Contextual Awareness
4. Secure and Managed Accounts
5. Least Privilege
6. Birthrights
7. Training
8. Monitoring

For Applications

1. SSO with Strong Authentication
2. Authorization
3. Session Management
4. Secure & Managed Accounts
5. Least Privilege
6. Supply Chain Security
7. Monitoring
8. MicroSegmentation

For Devices

1. Secure Identity
2. Strong Authentication
3. Device Lifecycle Management
4. Device Health
5. Secure Access
6. Secure & Managed Accounts
7. Least Privilege
8. Supply Chain Security

Passwordless for People

OpenID Connect & WebAuthN for Applications with Session Management

Just In Time Access for Devices & Resources with Session Management

In Conclusion

Create	Create better policies & standards
Awareness	Stay up to date on vulnerabilities & attacks
Plan	Plan on how to best use your resources to protect your customers and business
Prepare	Prepare for attacks with great visibility, response and recover options

SCTE® CABLE-TEC EXPO® FAST FORWARD 2021

ATLANTA, GA
OCTOBER 11-14

SCTE
a subsidiary of CableLabs®

Thank You!

Nancy Davoust & Emma Rochon

VP II, Security Architecture, Identity and Access
Security Architect 2
Comcast Cable
nancy_davoust@cable.comcast.com
emma_rochon@comcast.com