Preventing Ransomware: Tools, Tips, Techniques and Technology

Tim Brown, Executive Director, CISSP, CISA
Not sure if you noticed...

We are under attack!
Public Sector Breaches

- 16% of reported breaches
- 52% involved hacking
- 33% involved social attacks/engineering
- 28% involved malware
- 21% due to error events
- 23% of breaches involved actors of nation-states

Source: 2019 Verizon Data Breach Investigations Report
Public Sector Breaches

- 71% were financially motivated
- 25% motivated to gain strategic advantage
- 29% involved use of stolen credentials
- 56% took months (or longer) to discover

Source: 2019 Verizon Data Breach Investigations Report
Public Sector Breaches

- 95.6% of malware delivered by e-mail
- 15.1% delivered via web
- 64.4% involved an office type document

Source: 2019 Verizon Data Breach Investigations Report
Public Sector Phishing

4.48% click rate

Source: 2019 Verizon Data Breach Investigations Report
In other news...

Supply chain attacks are up 78%

Cloud does not fix the problem...
70 million records stolen or leaked as a result of poor configuration of S3 buckets

1 in 36 mobile devices have high risk applications installed

Source: 2019 Symantec Internet security Threat Report
Ransomware
1. Inventory\Control of Hardware Assets
2. Inventory\Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs
Backups are critical.
  - Multiple iterations
  - Test backups
  - Keep backups isolated
    - Copy of backups off-site.
    - Air gap

Prevention

Isolate administrator accounts

Multifactor authentication
Prevention

Log management best practices
- Storing logs in a secure central location
- Take logs offsite
- Consider a log\threat monitoring service

Check systems for anomalies
- May lay dormant for several weeks prior to launching an attack
- When restoring from backup, keep in mind you may be restoring the instigating files\threats, which will simply relaunch
Prevention

Training/awareness program
Common types of attacks
Common symptoms...being able to recognize a breach.
Test programs, such as phishing

Keep up to date...
MS-ISAC
InfraGard
Vendor sources
**Prevention**

- **Vulnerability scanning**
  - MANY tools available
  - Can start small and build
  - Don’t just identify...Remediate!

**Patch**
- Patch
- Patch
- Patch
**Reaction**

- Incident response plan
  - What to do...
  - Who to contact...

- Reporting plan
  - See something-Say something
  - Ties into training and DR planning

- Segmentation/fire breaks?
NETWORK OF FLORIDA FUSION CENTERS
Areas of Responsibility

Florida Fusion Center (FFC) (Statewide)
Tallahassee, FL
FloridaFusionCenter@fdle.state.fl.us
(850) 410-7645

Tampa Bay Regional Intelligence Center (TBRC)
Tampa, FL
TBRC@fdle.state.fl.us
(813) 318-5600

Northwest Florida Fusion Center (NWFFC)
Pensacola, FL
nwfloridafusion@fdle.state.fl.us
(850) 595-2100

Central Florida Intelligence eXchange (CFIX)
Oroldo, FL
CFIX@ocfl.net
(407) 858-9950

North Florida Fusion eXchange (NFFX)
Tallahassee, FL
nffx@flcjn.net
(850) 410-8869

Southwest Florida Fusion Center (SFIX)
Ft. Myers, FL
SFIX@colliersheriff.org

Northeast Florida Fusion Center (NEFFC)
Jacksonville, FL
Contact@NortheastFloridaFusion.org
(904) 256-5950

Southeast Florida Fusion Center (SFFC)
Miami, FL
sffx@mdpd.com
(305) 470-3880

Palm Beach, FL
pbregionalfusion@pbso.org
(561) 688-3700
Attack launched by a nation-state for political reasons
$250-$300 million in damages
Hit by NotPetya, which cause an estimated $10 billion in damages worldwide
  Made to resemble Petya, ransomware attack irreversibly encrypted computers’ master boot records
Spread to all of their data centers, crippling shipping worldwide
One lone domain controller was offline in Ghana due to an unrelated power outage
Reaction | Practice your plans...
Some things to keep in mind

US Mayors conference met in June
Represents cities with population of at least 30,000

...Paying ransomware attackers encourages continued attacks on other government systems, as perpetrators financially benefit...

The United States Conference of Mayors has a vested interest in de-incentivizing these attacks to prevent further harm.

Now, therefore, be it resolved, that the United States Conference of Mayors stands united against paying ransoms in the event of an IT security breach.
Some things to keep in mind

Plan your requests
Too many tools?

“...investing in yet more point product will do little to improve security status and nothing to increase the return on investment of existing solutions”

-Sean Keef
Skybox Security
Some things to keep in mind

Plan your requests

Set priorities

Make budget requests in writing
Some things to keep in mind

Have purchasing requests part of your emergency plan...
NWRDC Philosophy

We fulfill our mission by supporting our customers in accomplishing their goals and missions

We are a service organization that provides solutions to meet our customers’ business needs

Each customer has unique needs, and therefore, requires unique solutions
NWRDC CUSTOMERS BY REGION

**Northwest**
- Holmes County School District, Bonifay
- Calhoun County School District, Blountstown
- Liberty County School District, Bristol
- Panhandle Educational Cooperative, Chipley
- Washington County School District, Chipley
- Wakulla County School District, Crawfordville
- Walton County School District, DeFuniak Springs
- Franklin County School District, Eastpoint
- ELC of the Emerald Coast, Ft. Walton Beach
- Chipola College, Marianna
- Jackson County School District, Marianna
- Santa Rosa County School District, Milton
- Jefferson County School District, Monticello
- Bay County School District, Panama City
- Gulf Coast State College, Panama City
- Escambia County School District, Pensacola
- University of West Florida, Pensacola
- Gulf County School District, Port St. Joe
- Gadsden County School District, Quincy

**Tallahassee:**
- Agency for State Technology
- Auto Data Direct
- Department of Business and Professional Regulation
- Department of Education
- Department of Financial Services
- Department of Health
- Department of Highway Safety and Motor Vehicles
- Department of Revenue
- Department of State
- Florida Agricultural and Mechanical University (FAMU)
- FAMU Developmental Research School
- Florida Board of Governors
- Florida Center for Interactive Media
- Florida Commission on Human Relations
- Florida Department of Education
- Florida Lottery
- Florida Prepaid College Board
- Florida State University (FSU)
- Florida State University System
- Florida State University
- FSU Facilities
- FSU Foundation
- FSU Health Services
- FSU Police Department
- Florida Virtual Campus
- Leon County Government
- Leon County Schools
- Statewide Guardian ad Litem
- Tallahassee Memorial Health Care

**East Central**
- College of Central Florida, Ocala
- Orlando:
  - Florida Virtual Schools
  - Orange County Clerk of Courts
  - Orange County Comptroller
  - Orange County Government
  - University of Central Florida

**Southeast**
- Palm Beach State College, Lake Worth
- Palm Beach County Health Care District, Palm Springs
- West Palm Beach:
  - Palm Beach County Clerk and Comptroller
  - Palm Beach County School District
  - Palm Beach County Government

**South**
- A.D. downtime University School, Boca Raton
- City of Boca Raton
- Florida Atlantic University, Boca Raton
- City of Delray Beach
- Monroe County School District, Key West
- Dade County School District, Miami
- Florida International University, Miami

**Northeast**
- Nassau County School District, Fernandina Beach
- Santa Fe College, Gainesville
- University of Florida, Gainesville
- City of Jacksonville
- Florida State College at Jacksonville
- University of North Florida, Jacksonville
- Columbia County Schools, Lake City
- Florida Gateway College, Lake City
- Sumter County School District, Live Oak
- Madison County School District, Madison
- Taylor County School District, Perry
- Florida School for the Deaf and the Blind, St. Augustine
- St. Johns County School District, St. Augustine

January, 2019
NWRDC Partnerships

CenturyLink  Forescout
SecureWorks  Cyxtera
TelaForce  Symantec
Microsoft CSP  AWS*
**Why Secureworks™ Incident Response**

**IR Accreditations and Affiliations**

NSA/NSCAP CIRA, NCSC/CPNI CIR, FIRST, DHS, CREST, FBI, NH-ISAC, FS-ISAC, NCFTA, USSS, NIST, and ENISA

---

**EXPERIENCE & EXPERTISE**

- 100+ Global Responders Specializing in:
  - Complex Cyber Incident Response
  - Cyber Threat Hunting
  - Digital Forensic Analysis
  - Malware Analysis
  - Cloud Incident Response
  - IR Planning and Testing

- 1000+ IR Engagements Annually

- 10+ Years of Onsite IR Services

---

**THREAT INTELLIGENCE & PROPRIETARY TOOLS**

- 18+ Years of cyber attack and cyber threat data, synthesized with incident response casework

- 70+ CTU™ researchers to produce, analyze and validate threat intelligence

- Red Cloak™ behavioral analytics power our proprietary toolset to detect sophisticated adversaries and lower your costs to respond

---

**SPEED OF RESPONSE**

- 4 Hour Callback and Triage
- 24 Hour Remote IR Start\(^1\)
- 36 / 48* Hour Onsite / In-Transit\(^2\)

---

\(^1\)Emergency IR started within 24 hours of agreement on scope

\(^2\)Onsite to the affected location within 36 hours

Applies to the USA, Japan, Australia, EU member states, and the Schengen Area

\(^2\)In-transit to the affected location within 48 hours

Applies to all other countries
How Secureworks Incident Response Can Help

**Scenario**

- We need a global IR team on standby to assist and advise us with complex cyber events 24x7x365

**IR Service Component**

- Incident Management Retainer
- Emergency Incident Response
- Targeted Threat Hunting Assessment
- Incident Response Workshops and Exercises
- Incident Response Plan Review / Development
- Incident Response Readiness Assessment
Forescout provides agentless VISIBILITY of all connected devices across entire Enterprise

Forescout integrates with vulnerability scanning and agent-based patching solutions to ensure every device connecting to the network has a clean VA scan and is patched if needed
By natively integrating into the Active Directory environment, Forescout sees the authenticated users group memberships and privilege levels.

Forescout can automatically send the repository of discovered devices and endpoints to the CMDB to ensure there is an up-to-date record of assets and Configuration Items to be incorporated into Disaster Recovery plans.
Symantec Email Security Solution Story

PROTECT AGAINST EMERGING THREATS
SYMANTEC MESSAGING SECURITY – ADD ON
- Machine Learning & Sandboxing
- Click-Time Protection
- Advanced Email Security Analytics
- SOC Integration
- Threat Remediation

ISOLATE DANGEROUS THREATS
SYMANTEC MESSAGING SECURITY- ADD ON
- Malicious URL Isolation
- Attachment Isolation
- Credential Theft Protection

STOP PHISHING ATTACKS
SYMANTEC MESSAGING SECURITY
- Link Protection
- Impersonation Controls
- Phishing Variant Detection
- Behavioral Analysis

PROACTIVELY PREVENT ATTACKS
SYMANTEC AWARENESS PLATFORM
- Customizable Security Assessments
- Detailed Reporting & Visibility
- Integrated User Education

BLOCK COMMON THREATS –
SYMANTEC MESSAGING SECURITY
- Heuristics
- Reputation Analysis
- Connection-level Detection
- AV Engine

PREVENT DATA LEAKAGE AND FRAUD PROTECTION
SYMANTEC MESSAGING SECURITY – ADD ON
- Advanced Detection Technologies
- Multi-Channel Data Protection
- Policy-Driven Controls
- Push & Pull Encryption
- Sender Policy Framework (SPF)
- DomainKey Identified Mail (DKIM)
- Domain Messaging Authentication Reporting & Conformance

- One Story
- One Integrated Solution
- One Company - Symantec
Why Symantec?

- **Comprehensive Defense** that includes Isolation & Fraud Protection
- **Integrated Cyber Defense** for Office 365
- **Deepest Visibility & Remediation** for Advanced Threats
- **Strongest** Data Protection Controls
- **Industry-Leading** Email Security Solution
NWRDC Backup as a Service

Service based on EMC’s Data Protection Suite
- Avamar, Networker, Data Protection Advisor, DD Boost, Encryption (at rest and transit), WORM (Retention Lock)
- All licensing included
- No upload/download or hidden fees
- Provide service on premise or cloud
NWRDC Backup as a Service

Pricing based on per GB capacity actually used

Based on usage AFTER deduplication
  Deduplication helps lower customer cost
  Backup 1 TB, but consume 200 GB means you pay for 200 GB

Can create air gapped backup sets
Backup as a Service

DATA DOMAIN REPLICATION PROCESS

Primary Storage

Backup Appliance

DD Replication

Air Gap

Isolated Recovery System

Recovery Hosts

Validation Hosts

Mgmt Host

1. Mgmt host issues open port command. DD Port brought online (default offline creating air gap)

2. Initiate DD Replication from A to B

3. Bring the DD port off line to recreate the air gap

4. Perform Desired Number of Fast Copy Operations per desired policy

5. Run Validation Routines; If Fail, send alert
Backup as a Service

DATA DOMAIN RESTORE PROCESS

1. Perform validation to ensure non-corrupted copy / restore point is identified
2. Leverage software DR procedures to ensure business critical system works as expected
3. Bring DD Port Online
4. Configure Backup Software environment to access Data Domain IRS target
5. Perform Data Set Recovery
6. Re-Create Air Gap by bringing DD replication port back offline

Data Domain solution can provide fast recovery of business critical data and volumes including host volumes, metadata such as active directory / forests / and other configuration data

© Copyright 2016 EMC Corporation. All rights reserved.
Northwest Regional Data Center (NWRDC), as a part of FSU, authorized according to Florida Statutes 1011.47 and 1004.649 as an auxiliary enterprise, is a government entity.

Please refer to Florida Statutes, Section 287.057 (3) (e)12 to validate that any government entity entering into an agreement with NWRDC is exempt from requirements for competitive solicitation.
Questions

Tim Brown
Executive Director, NWRDC
Tim_Brown@nwrdc.fsu.edu
850-645-3521