Cyber Security Resources For Local Government

June 8, 2017
<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peter Bloniarz</td>
<td>Executive Dir. and Senior Policy Advisor NYS Cyber Security Advisory Board</td>
</tr>
<tr>
<td>Jaime Daley</td>
<td>Senior Intelligence Analyst New York State Intelligence Center</td>
</tr>
<tr>
<td>Douglas Fassbender</td>
<td>Contracts Manager, NYS Division of Homeland Security &amp; Emergency Services</td>
</tr>
<tr>
<td>Kimberly LaCroix</td>
<td>Security Governance Risk &amp; Compliance NYS Enterprise Information Security Office</td>
</tr>
</tbody>
</table>
## NIST Cybersecurity Framework

<table>
<thead>
<tr>
<th>IDENTIFY</th>
<th>Identify business context, assets, risks, and threats. Governance and risk management strategy.</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROTECT</td>
<td>Develop and implement appropriate safeguards</td>
</tr>
<tr>
<td>DETECT</td>
<td>Detect cyber security incidents</td>
</tr>
<tr>
<td>RESPOND</td>
<td>Take action after a reported or detected cyber incident.</td>
</tr>
<tr>
<td>RECOVER</td>
<td>Restore business capabilities after an incident</td>
</tr>
</tbody>
</table>
Local Government Threat Brief

NYS Cyber Security Conference

June 8, 2017
Cyber Threat Landscape
Threat Actors Impacting Local Gov’t

- **Financially motivated** – For Profit
  - Ransomware
  - Data Breaches (PII)
  - Business Email Compromise (BEC)
Ransomware: 2014 - May 2017

- Trojan.Cryptowall Infection
- Tesla/Alphacrypt
- Locky
- Cerber
- CryptXXX
- Other Ransomware

TLP: WHITE
Data Breaches

MS-ISAC 2016 Sub-Entity Data Breakdown

- University / College EDU: 25%
- GOVT LOCAL: 28%
- Law Enforcement LOCAL: 4%
- GOVT STATE: 16%
- K-12 School EDU: 17%
- Health STATE: 7%
- Health LOCAL: 3%
1. **Purchase Order Fraud variant**
   - a.k.a. Bogus Invoice Scheme, Supplier Swindle
   - May include spoofed domains and copied purchase orders
   - Schools are frequent SLTT targets

2. **W-2 and PII Phishing variant**
   - Results in PII data breach
   - Targets finance or HR depts
   - Results in filing of fraudulent tax returns
   - Spoofed or compromised executive account

3. **Financial Fraud variant**
   - Results in a wire transfer; Millions lost
   - Targets finance or HR depts
   - Spoofed or compromised executive accounts

---

**Report Attempts to MS-ISAC, IC3 (IC3.gov), and the IRS**

**TLP: WHITE**
Threat Actors Impacting Local Gov’t

- Politically motivated
  - Responses to current events: Social / Political
  - Hacktivist Groups (*Anonymous*)
    - Grievance: use of force by LE
    - Impact: 25% attacks target local governments (website defacements, DDoS)
Total Defacements by Day

- WordPress patch released fixing vulnerability
- WordPress security team discloses vulnerability
- MS-ISAC Cybersecurity Advisory sent out
New York State Police’s Role in Cybersecurity
Fusion Center Mission

• New York State Intelligence Center (NYSIC)
• Staffed by 20+ local, state, federal law enforcement and homeland security agencies
• 24/7/365 criminal, terrorism and cyber intelligence support
CAU Mission

To gather, analyze and disseminate timely and relevant cyber threat information and intelligence (criminal or homeland security-related) to:

– State and local law enforcement
– Local/county/state government IT personnel
– Federal law enforcement and cybersecurity partners
– Private sector (CIKR)
Intelligence Analysis and Production

• Formal Intelligence Bulletins
  – Technical & Non-technical audiences
    ✓ Examples

• Daily, proactive open source / social media research for relevant cyber-intelligence → Notifications
June 8, 2017

New York State Intelligence Center

31 Tech Valley Drive, Second Floor, East Greenbush, NY 12061
Phone: 866-48-NYSIC (866-486-9742) Fax: (518) 786-9358

Type: Cyber Bulletin #17-02

Date: April 18, 2017

Attn: Information Technology Personnel (All Sectors)

Subject: Unicode Domain Spoofing Attack Impacting Multiple Browsers

Summary:
The New York State Intelligence Center (NYSIC) Cyber Analysis Unit (CAU) is aware of recent open source reports regarding domain spoofing attacks impacting several popular web browsers. This tactic allows malicious actors to mimic legitimate domains and obtain security certificates.

Overview:
The New York State Intelligence Center (NYSIC) Cyber Analysis Unit (CAU) is aware of recent open source reports regarding domain spoofing attacks based on the way several popular web browsers handle Unicode characters. The impacted browsers currently include Mozilla Firefox, Google Chrome, and Opera. Unicode was developed as a standard to encode and represent popular languages throughout the world.¹ Computer systems utilize Unicode as a means to convert various characters from multiple languages into a machine-readable format.²

Attackers can exploit similarities between languages by creating Unicode-based domain names, which resemble legitimate domain names after the conversion process. This attack method is also known as a homograph attack, which exploits the fact that characters across multiple languages may look alike.³

To illustrate an example of this exploit, NYSIC examined the domain “epic.com” utilizing Cyrillic characters⁴:

- The Roman alphabet character set - “epic”
- Cyrillic alphabet character set – “эпик”

As shown above, the two character sets appear to be identical. However, the Cyrillic character set can be converted from Unicode to ASCII using Punycode. ASCII is the most common format for text files used on the Internet.⁵ Punycode converts Unicode characters to a subset of ASCII consisting of letters, digits, and hyphens, utilized by DNS to represent domain names.
Notifications (June 2016-May 2017)

• Phishing/Spam (47)
• Threats to organizations (DDoS or potential data releases) (2)
• Website defacements (4)
• Website/network vulnerabilities (21)
• XXS (9)
Contact Information:

New York State Intelligence Center (NYSIC)
Cyber Analysis Unit
518-786-2191
cau@nysic.ny.gov
New York State Division of Homeland Security and Emergency Services (DHSES)

Agency and Cyber Funding Overview

June 8, 2017

Unclassified/For Official Use Only
DHSES Mission

Provide leadership, coordination and support for efforts to prevent, protect against, prepare for, respond to, and recover from terrorism and other man-made and natural disasters, threats, fires and emergencies.
Key DHSES Functions

- Maintaining situational awareness on emergencies across the state
- Coordinating state disaster response activities, including emergency response resource deployment
- Providing support and technical assistance to state and local response teams
- Promoting terrorism awareness and disaster preparedness education
- Managing disaster recovery programs and processing disaster recovery funding
- Supporting the development of statewide interoperable and emergency communications systems
- Conducting fire inspections and arson investigations
Key DHSES Functions

• Supporting the development of state and local disaster plans and strategies

• Providing training to first responders, elected officials and other stakeholders

• Helping to develop exercises to test disaster plans and capabilities

• Analyzing and sharing information on the current terrorist threat environment

• Conducting risk and vulnerability assessments of critical infrastructure

• Administering homeland security and emergency preparedness related grant programs
Homeland Security Grant Program Overview

- Federal grant program awarded to NYS from U.S. Department of Homeland Security (DHS) through Federal Emergency Management Agency (FEMA)
- 80% of the funding must be passed through to local government while 20% of funding can be used to support state projects
- DHSES provides awards to every county and NYC based on a risk funding model. Additionally, small amount of funding supports targeted grants.
- NYS Funding level for FY2016:
  - State Homeland Security Grant Program (SHSP): $76.9M
  - Urban Areas Security Initiative (UASI): $178.6M
SHSP and UASI Overview

• Projects must align to the New York State Homeland Security Strategy

• Grant Guidance: Limitations placed on the funding (e.g., no supplanting, 50% cap on personnel and some consultant costs)

• Funds Awarded to Counties – DHSES works through County designated points of contact (e.g., Emergency Managers, Sheriffs)

• UASI funds are for NYC region: NYC, Westchester, Nassau, Suffolk and PANYNJ
SHSP & UASI Overview

- Cyber Security is one of six national capability areas for improvement as identified in the National Preparedness Report.

- DHSES has identified the development of effective cyber security programs and policies as a priority.
  - One of 28 Critical Capabilities in NYS, Goal 10 – Enhance Cyber Security Capabilities

- Cyber security projects are an allowable program area – funds can be used for planning, equipment, training and exercises.
SHSP & UASI – Cyber Security Allowable Projects

- **Planning:** Maintain and update policies, standards and continuity of operations. Includes hiring of full- or part-time staff or contract/consultants to plan for and implement cybersecurity projects as well as provide cyber monitoring services.

- **Training:** Conduct, support and attend cyber security trainings. Includes overtime/backfill for approved training, consultant costs associated with the design and delivery of training, travel and supplies associated with training as well as paying for attendance at appropriate conferences and trainings.

- **Exercises:** Incorporate cyber security into exercises to build and test capabilities. Includes overtime/backfill for approved exercises, consultant costs associated with the design and delivery of exercises, travel and supplies associated with exercises.
SHSP & UASI – Cyber Security Allowable Projects

• Equipment Purchases: Equipment purchases to support cybersecurity are allowable under the following authorized equipment categories:

  • Biometric User Authentication Device;
  • Remote Authentication System;
  • Encryption/Forensic/Malware Protection Software;
  • Data Transmission Encryption;
  • Personal/Network Firewall System;
  • Intrusion Detection/Prevention System;
  • Vulnerability Scanning Tools;
  • Security Event/Incident Management Patch/Configuration Management Systems
### Summary of Funded Cyber Security Projects

<table>
<thead>
<tr>
<th>Grant Program</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHSP</td>
<td>$1.5</td>
<td>$1.1</td>
<td>$1.1</td>
<td>$1.3</td>
<td>$5.1</td>
</tr>
<tr>
<td>UASI</td>
<td>$5.7</td>
<td>$0.7</td>
<td>$12.9</td>
<td>$5.4</td>
<td>$24.8</td>
</tr>
<tr>
<td>Grand Total</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$29.9</td>
</tr>
</tbody>
</table>
Grant Funded Cyber Security Projects

• **PANYNJ Cyber Security Services – Risk Management:** Assessment of the current system including identifying vulnerabilities and provide system enhancements. Assistance with developing policies and procedures as well as providing forensic tools to support cyber investigations. (UASI funding FY 2016: $3M)

• **NYPD Data Analytics and Cybersecurity – Software:** Analytic software and services which protects the Department’s sensitive networks and data from cyber-attacks. The software offers state of the art cyber defense tools to discover links between attacks, uncover new attack vectors, and investigate and respond to potential malware infections. (UASI funding FY 2014: $3M; FY 2015: $3.5M)
Grant Funded Cyber Security Projects

• Fire Department of New York (FDNY) – Risk Management: Hire three staff analysts to develop cyber-security and risk mitigation plans and initiatives in support of the National Institute of Standards and Technology and develop initiatives to identify, protect, detect, respond and recover from cyber-threats. In addition, the FDNY has begun purchasing next generation firewalls and security platforms to protect against cyber threats to core networks and applications. (UASI funding FY 2015: $1.1M)

• Niagara County Emergency Management Cybersecurity Planning – Risk Management: Utilize a consultant to conduct a cybersecurity assessment of the internet and other communication technologies of the 911 center as well as the county data network that the 911 center is part of. (SHSP funding FY 2016:$15K)
Questions?

Contact:
Doug Fassbender
Contracts Manager, Grants Program Administration
NYS Division of Homeland Security & Emergency Services
doug.fassbender@dhses.ny.gov
(518) 242-5106
http://www.dhses.ny.gov/grants/
Nationwide Cyber Security Review (NCSR)

Kimberly LaCroix
Enterprise Information Security Office
NYS Office of Information Technology Services
Nationwide Cyber Security Review (NCSR)

- U.S. Department of Homeland Security sponsored and all State, Local, Tribal, and Territorial governments may participate

- Free, annual, cyber security self-assessment, aligned to the NIST Cybersecurity Framework and designed to evaluate cybersecurity maturity and risk management

- Annual survey runs from **October 1 – December 30** – access to your organization’s survey results are available year round

- Anonymized results shared in a summary report to U.S. Congress in alternate (odd-numbered years)
Establish their organization’s baseline of cybersecurity maturity and risk awareness

See how their organization compares with similar organizations (peer to peer reports)

Participants in 2015 and 2016 now have a year-over-year comparison for their organization

Results inform executive management about the State and organizations’ cybersecurity programs and are used to establish priorities and drive improvement
Additional Resources For Local Government

June 8, 2017
### Prepare (Identify, Protect, Detect)

<table>
<thead>
<tr>
<th>Category</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Sharing</td>
<td>NYSIC; MS-ISAC and NYS ITS (esp. for vulnerabilities)</td>
</tr>
<tr>
<td>Assessment of Cyber Posture</td>
<td>US DHS/MS-ISAC</td>
</tr>
<tr>
<td></td>
<td>Nationwide Cyber Security Assessment</td>
</tr>
<tr>
<td>Training and Education</td>
<td>Federal agencies (see ITS “Training and Resources”)</td>
</tr>
<tr>
<td>Sample Standards, Policies</td>
<td>ITS</td>
</tr>
<tr>
<td>Cyber Exercises</td>
<td>US Dept. of Homeland Security</td>
</tr>
<tr>
<td>Community of Practice</td>
<td>Multi-State Info Sharing and Analysis Center</td>
</tr>
<tr>
<td>Cyber Risk Assessment</td>
<td>US DHS (Cyber Resilience Review, others)</td>
</tr>
<tr>
<td></td>
<td>OGS contracts (session at 3:30)</td>
</tr>
<tr>
<td>Vulnerability Scanning</td>
<td>US DHS “Cyber Hygiene Program,” NYS ITS</td>
</tr>
</tbody>
</table>
What To Do if You Get Hit with Ransomware

1. Follow technical steps (e.g. US DHS Fact Sheet on WannaCry)
2. Utilize your internal response plan for ransomware infection
3. Contact your local FBI Office Cyber Taskforce
4. Contact Multi-State ISAC
5. Contact the NYS Intelligence Center
6. Call 911 if it’s an immediate threat to public health or safety
## Respond and Recover

<table>
<thead>
<tr>
<th>Technical Advice</th>
<th>Federal guidelines (e.g. Ransomware, WannaCry, Business Email Compromise)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criminal Investigation (Exercises)</td>
<td>NY State Police, FBI Cyber Task Force</td>
</tr>
<tr>
<td>(Professional Assistance)</td>
<td>US Dept. of Homeland Security</td>
</tr>
<tr>
<td>One-on-one Guidance and Support</td>
<td>OGS contracts (in advance)</td>
</tr>
<tr>
<td></td>
<td>Report to NYSIC, MS-ISAC for limited assistance</td>
</tr>
</tbody>
</table>
Cyber Incident Response Team

• Help create a stronger, safer and more secure New York for all by providing cybersecurity support to state entities, public authorities, local governments, critical infrastructure, and schools

Governor Andrew Cuomo, 2017 State of the State
Response and Recovery

• Serve as a multi-agency strike force, assisting with response to cyber intrusions across the state

• Provide a single number to call to report cyber incidents, streamlining response efforts
Preparedness

• Create a go-to resource in how to better protect information technology assets from cyber-attacks, malware and ransomware.
  – Information and intelligence sharing
  – Vulnerability and risk assessments
  – Network scans
  – Training/education
  – Review cybersecurity policies
  – Coordinate exercises
How the CIRT Will Operate

• Support peer-to-peer networking and support
• Facilitate solutions to common needs
• Provide advice and guidance
• Serve as central coordinator of available resources
  – NYS: DHSES, NYSIC, ITS, DMNA, DOH, DFS, etc.
  – Federal: DHS, NIST, FTC, SBA, etc.
  – Multi-State ISAC
  – Private Sector (through OGS contracts)
Contact Information

Peter Bloniarz
Executive Director and Senior Policy Advisor
New York State Cyber Security Advisory Board

peter.bloniarz@exec.ny.gov
(518) 474-3522