DEALING WITH EMAIL SPAM & THREAT INTELLIGENCE

Deane Davis
EMAIL SPAM
Profitable for Criminals, Expensive for Companies
EMAIL SPAM – PHISHING

- Product & Services Advertising (fake and real)
- Social Engineering
- Malware
The .PL in the e-mail address stands for Poland.

From: "Sarah Norton" <ciaja_wyy@wp.pl>
Date: March 10, 2016 at 3:42:39 PM EST
To: @hsn.net
Subject: [EXTERNAL] Incident at HSN - Attn: 

Hello (727) 872-1000 

I was advised to contact you about the conflict that happened at HSN (2501 118th Ave N, SAINT PETERSBURG, FL, 33716-1920) on Tuesday. Kindly see the enclosed document for comprehensive details on the incident.

Would you kindly view the complaint and reply with your thoughts on this?

Good Luck!
Sarah Norton
Morning [Redacted],

How are you doing today? I want you to send me the list of W-2 copy of employees wage and tax statement for 2015, I need them in PDF file type, you can send it as an attachment. Kindly prepare the lists and email them to me ASAP.

Thanks

Exec's Full Name
PREPENDING MESSAGES

Please Note: This email has originated from an external sender. Treat any links and attachments with a heightened degree of awareness.

If you think this email is malicious or spam, please do not open any attachments or links and forward to...
THINGS YOU CAN DO

- Train Employees to spot phishing attempts
  - Beware of links in email. If you see a link in a suspicious email message, don't click on it. Rest your mouse (but don't click) on the link to see if the address matches the link that was typed in the message.
  - A common technique used by phishers is trying to impart a sense of urgency and trying to get you to supply the requested information quickly.

- Flag external e-mail in some fashion that will allow users to quickly identify e-mail as either internal or external

- Provide a means that allow users to submit suspected spam for evaluation by the Security staff

- Block all Office Documents with Macros at your spam gateway

- Ensure you have updated DNS SPF records for your domains

- Block all external messages with a FROM address using your domain name if possible

- Look at implementing Domain-based Message Authentication, Reporting & Conformance (DMARC)
  - https://dmarc.org/
THREAT INTELLIGENCE

Tons of Great Sources, Challenging to Make Actionable
Threat Intelligence

The art of intelligence is:
- Managing uncertainty.
- Converting intelligence information into fact.
- Making the unknown into actionable.

The objective is always:
1. More information;
2. Higher fidelity “better” information; and,
3. More timely information

Cyber Threat Intelligence isn’t any different
Threat Intelligence

- Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard. -Gartner
https://www.gartner.com/doc/2487216/definition-threat-intelligence

- Threat intelligence in it's most basic form, is Indicators of Compromise (IoCs), such as an IP address associated with command and control infrastructure, malicious phishing domain names, or URL paths to download malware. - Centripetal
http://www.centripetalnetworks.com/how-it-works.php#
More Information Desired

- Pixels are information. Cyber Indicators are information.

- Information requires processing and analysis to become actionable.

- Binary implementations (block/allow) won’t work in uncertain (intel) environments.

- The more information the better so long as it can be focused, prioritized, and handled by its fidelity.

- Automated application, processing, and risk triage are the key enablers for a Cyber Intelligence workflow.
Components Needed for Successful Threat Intelligence Consumption

- **Dynamic Threat Intelligence**: Dynamically receive updates from partner sources.
- **Pro-Active Network Defense**: A solution able to take action (e.g. block and alert events) in real-time.
- **Real-Time Results**: Visualize active inbound and outbound cyber threats, with context, in real-time.
Dynamic Threat Intelligence Sources

**Open Source**
- AlienVault
- US-CERT
- FeedOo Tracker
- Team CYMRU
- Malware Domain List
- DShield.org
- SPAMHAUS
- I Want You for C.I. Army

**Commercial**
- CrowdStrike
- Cyveillance
- iDefense
- iDefense
- Verisign
- ThreatTrack
- Symantec
- ISIGHT Partners
- The Media Trust
- Emerging Threats
- Dell SecureWorks
# Proactive Network Defenses & Real-time Results

<table>
<thead>
<tr>
<th>Feature</th>
<th>TI Device</th>
<th>Firewall</th>
<th>Proxy</th>
<th>IDS/IPS/FE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Traffic Acceptable Use / Corporate Policy</td>
<td></td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non-Web Acceptable Use / Corporate Policy</td>
<td></td>
<td></td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Stateful Traffic Filtering</td>
<td></td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Segmentation</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Layer 3 Routing / NAT</td>
<td></td>
<td></td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Malware Signature Inspection</td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Malware Detonation</td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>High Speed, Dynamic, Scaled Enforcement</td>
<td></td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Real Time per packet Monitoring &amp; Logging</td>
<td></td>
<td></td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Internal Host Correlation (All Traffic)</td>
<td></td>
<td></td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Compliance Assurance (OFAC, ITAR, etc.)</td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Risk Orchestration: Allow, Alert, Log, Branch, Divert, Block Host, Block Threat</td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
</tr>
</tbody>
</table>
DHS’s Automated Indicator Sharing (AIS)

The goal of the AIS initiative is to achieve near real-time sharing of cyber threat indicators by enabling DHS’s National Cybersecurity and Communications Integration Center (NCCIC) to

1. Receive indicators from the private sector;
2. Remove unnecessary personally identifiable information and other sensitive information; and,
3. Disseminate the indicators to, as appropriate, other Government departments and agencies and the private sector.

NOTE: The AIS feed is different than the CISCP.

- Although they are actually similar now, the plan is for AIS to be indicators and the CISCP to provide context and analytics.
Information Sharing Specifications for Cybersecurity

AIS Leverages TAXII, STIX, MAEC and CYBOX.

The inter-relationship of these initiatives is as follows. STIX uses languages such as (but not limited to) CybOX and MAEC to represent cyber security event information, and TAXII serves as the transport mechanism for STIX information.

- **TAXII (Trusted Automated eXchange of Indicator Information)**
  - TAXII’s objective is to establish a framework for standardized, trusted, and automated exchanges of cyber threat information.
  - Models supported are: source-subscriber data feed, peer-to-peer, and hub-and-spoke

- **STIX (Structured Threat Information eXpresssion)**
  - STIX is an initiative seeking to define standardized and structured representations of cyber threat information.

- **CybOX (Cyber Observable eXpression)**
  - CybOX is a structured language that describes entities within an organization’s cyber operational environment.

- **MAEC (Malware Attribute Enumeration and Characterization)**
  - MAEC is a structured language for describing malware attributes.

[https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity](https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity)
Leveraging DHS’s AIS Feed

1. You will need a solution to consume the information such as:
   - Collaborative Research into Threats (CRiTS) – Open Source
   - Centripetal Network’s Rulegate – Commercial
   - Soltra Edge – Free/Commercial

2. Complete the agreements with DHS
   - Sign the U.S. Department of Homeland Security Automated Indicator Sharing Terms of Use
     - Note: In February DHS and DOJ will be publishing some recommended definitions and clarifications based on the recent Cybersecurity Information Sharing Act (CISA) specifically around liability protection.
   - Complete and Sign the AIS Interconnection Agreement

3. Configure your system to ingest AIS feeds
   - Generate your Cert and provide it to DHS
   - Configure your solution and apply fidelity weighting if possible
Questions

THANK YOU