Validation of Current State Threats

*Who is targeting you, and how?*

The threat intelligence data below provides evidence that state sponsored actors, cyber criminals and hacktivists are actively pursuing specific information assets in the Government sector.

<table>
<thead>
<tr>
<th>Threat Category</th>
<th>Threat Actors</th>
<th>Specific Targets</th>
<th>Attack Vectors</th>
</tr>
</thead>
</table>
| Nation-State Sponsored Actors    | ► Deep Panda
   ► Putter Panda
   ► Sofacy Group
   ► Energetic Bear
   ► Tarh Andishan
   ► Syrian Electronic Army
   ► Bureau 121                     | ► Government agencies
   ► Critical infrastructure
   ► Energy Companies
   ► National Defense
   ► Parliament/legislative bodies
   ► Intellectual property          | ► Spearphishing emails
   ► Advanced malware
   ► Zero day exploits
   ► Unpatched vulnerabilities
   ► Malicious USB stick            |
| Cyber Crime                      | ► Central/Eastern European cyber gangs
   ► South East Asian cyber gangs
   ► Hackers for Hire               | ► Employee PII
   ► Voter records
   ► Credit card info stored by state agencies
   ► Drivers license records
   ► Education and health records   | ► Malicious documents (ex. .pdf)
   ► Spearphishing emails
   ► Unpatched vulnerabilities
   ► Commodity malware              |
| Hacktivists                      | ► Anonymous
   ► Lizard Squad
   ► LuizSec                         | ► Opposing political, ideological, or social entities                                               | ► Botnets
   ► DDoS
   ► Social Engineering campaigns   |
| Insider Threat                   | ► Disgruntled current or former employee
   ► Current employee not practicing good security                                                    | ► Sensitive information designed to embarrass current/former employer                              | ► Typically leverage trusted access they already have to networks
   ► May plant malware or other tool on network prior to leaving organization                           |
Anatomy of a Hack
How do threat actors target their victims?

Layer 1 – Common Attack Actions

External Actions: “before cyber-attack”
- Plan Activity
- Conduct Research & Analysis
- Develop Resources & Capabilities
- Conduct Reconnaissance
- Stage Operational Tools & Capabilities
- Initiate Operations

Internal Actions: “after cyber-attack”
- Deploy Capability
- Interact with target
- Exploit vulnerabilities
- Deliver Payload

Groundwork
Engagement
Presence
Effect/Consequence

Attack Stages

- Control
- Hide
- Expand
- Refine Targeting
- Establish Persistence

- Deny Access
- Consume Resources
- Alter/Manipulate Computer, Network, or System Behavior
- Extract Data
- Destroy HW/SW/Data
- Enable other Operations
CONTACT INFORMATION:

Joe Demarest | Executive Director | Cyber Security

Ernst & Young LLP
Office: 347-752-1589 |
joe.demarestjr@ey.com