IMPACTS ON CONFIDENCE
IMPACTS ON CONFIDENCE
NEGATIVE

-----

POSITIVE
F.U.D.

PLAN OF ACTION
F.U.D.
F.U.D.

Everything you need to know about EternalBlue – the NSA exploit linked to Petya

Meltdown and Spectre: ‘worst ever’ CPU bugs affect virtually all computers

The Guardian

Healthcare

Indiana hospital shuts down systems after ransomware attack

WannaCry ransomware used in widespread attacks all over the world

Yahoo says 2013 hack hit all 3 billion user accounts, triple initial estimates
VULNERABILITY

THREAT / EXPLOIT

BREACH
2.5 Million More Americans Added To The Equifax Security Leak, What To Do Now

Everything you need to know about EternalBlue - the NSA exploit linked to Petya

Meltdown and Spectre: 'worst ever' CPU bugs affect virtually all computers

The Guardian

F.U.D.

cyberscoop

Indiana hospital shuts down systems after ransomware attack

KrebsonSecurity

WannaCry ransomware used in widespread attacks all over the world

Yahoo says 2013 hack hit all 3 billion user accounts, triple initial estimates
PLAN OF ACTION
Reverse engineering for malware analysis

cheat sheet

by @0tt0b
<table>
<thead>
<tr>
<th>Function Unique Identifier</th>
<th>Function</th>
<th>Category Unique Identifier</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Identify</td>
<td>ID.AM</td>
<td>Asset Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.BE</td>
<td>Business Environment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.GV</td>
<td>Governance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.RA</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.RM</td>
<td>Risk Management Strategy</td>
</tr>
<tr>
<td>PR</td>
<td>Protect</td>
<td>PR.AC</td>
<td>Access Control</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.AT</td>
<td>Awareness and Training</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.DS</td>
<td>Data Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.IP</td>
<td>Information Protection Processes and Procedures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.MA</td>
<td>Maintenance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.FT</td>
<td>Protective Technology</td>
</tr>
<tr>
<td>DE</td>
<td>Detect</td>
<td>DE.AE</td>
<td>Anomalies and Events</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE.CM</td>
<td>Security Continuous Monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE.DP</td>
<td>Detection Processes</td>
</tr>
<tr>
<td>RS</td>
<td>Respond</td>
<td>RS.RP</td>
<td>Response Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.CO</td>
<td>Communications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.AN</td>
<td>Analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.MI</td>
<td>Mitigation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.IM</td>
<td>Improvements</td>
</tr>
<tr>
<td>RC</td>
<td>Recover</td>
<td>RC.RP</td>
<td>Recovery Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.CO</td>
<td>Communications</td>
</tr>
</tbody>
</table>

Source: NIST Framework For Improving Critical Infrastructure Cybersecurity, v. 1.0 (Feb. 12, 2014) at p. 19.
First 5 CIS Controls
Eliminate the vast majority of your organization’s vulnerabilities

1: Inventory of Authorized and Unauthorized Devices
2: Inventory of Authorized and Unauthorized Software
3: Secure Configurations for Hardware and Software
4: Continuous Vulnerability Assessment and Remediation
5: Controlled Use of Administrative Privileges

All 20 CIS Controls
Secure your entire organization against today’s most pervasive threats

6: Maintenance, Monitoring, and Analysis of Audit Logs
7: Email and Web Browser Protections
8: Malware Defenses
9: Limitation and Control of Network Ports
10: Data Recovery Capability
11: Secure Configurations for Network Devices
12: Boundary Defense
13: Data Protection
14: Controlled Access Based on the Need to Know
15: Wireless Access Control
16: Account Monitoring and Control
17: Security Skills Assessment and Appropriate Training to Fill Gaps
18: Application Software Security
19: Incident Response and Management
20: Penetration Tests and Red Team Exercises

Source: Center for Internet Security (www.cisecurity.org/controls)
STRATEGIES to MITIGATE
TARGETED CYBER INTRUSIONS
ASD TOP 4 PREVENTS OVER 85% OF INTRUSIONS

Mitigation 1: Application Whitelisting
Mitigation 2: Patch Applications
Mitigation 3: Patch Operating Systems
Mitigation 4: Minimise Administrative Privileges
Basic Security Hygiene
Basic Security Hygiene

- Patch, Patch, and Make Sure You Did!
- Principle of Least Privilege
- Control Administrative Privileges
- Strong, Well-Protected Passwords
- Multi-Factor Authentication
- Security Awareness Training
PLAN OF ACTION

F.U.D.
Questions?