INTERACTIVE PENETRATION TESTING
AGENDA

- A Framework for Comparing Cyber Attacks
- Getting to know WannaCry Ransomware
- Penetration Testing – Kinds and Stories
- Conclusions and Recommendations
COMPARING CYBER-ATTACKS

Cyber Attack Kill Chain Model

RANSOMWARE

Why WannaCry?
- Damage? 230,000 computers in over 150 countries
- Attributed to North Korea / Lazarus Group?
- Famous 0 day? NSA.. (Eternal Blue/Double Pulsar)
- Shadow Brokers leak?
- Destructive nature?
- We are still vulnerable? TSMC infected on 8/6/2018

Primary Reason
- First “at scale” attack to join both Weapons Grade Malware (0 day threats) and Modular Scripting techniques...
WANNACRY DEMO

Sandbox analysis from App.Any.Run
**HOW DOES WANNACRY WORK?**

Kill Chain Mapping

<table>
<thead>
<tr>
<th>Stage</th>
<th>Core Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>3. Delivery</td>
<td>SMBv1, TCP Port 445</td>
</tr>
<tr>
<td>4. Exploitation</td>
<td>Eternal Blue 0 day</td>
</tr>
<tr>
<td>5. Installation</td>
<td>Cscript / VBScript</td>
</tr>
<tr>
<td>6. C2</td>
<td>Beacons via TOR</td>
</tr>
<tr>
<td>7. Actions/Objective</td>
<td>Destroy (encrypt) Data</td>
</tr>
</tbody>
</table>

![Diagram showing the stages of Wannacry's attack](image-url)
# TRUSTED SOFTWARE – AN INSIDER THREAT

<table>
<thead>
<tr>
<th>Type</th>
<th>Calculator.exe</th>
<th>Malware.exe</th>
<th>abc.exe</th>
<th>Cscript / Powershell</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reputation</td>
<td>Trusted Application</td>
<td>Virus</td>
<td>Zero Day Exploit</td>
<td>Dual Use</td>
</tr>
<tr>
<td>Known GOOD (WHITE)</td>
<td>Known Bad (BLACK)</td>
<td>Unknown (GRAY)</td>
<td>Known GOOD (WHITE)</td>
<td></td>
</tr>
<tr>
<td>Detection</td>
<td>App Whitelisting</td>
<td>Antivirus</td>
<td>App Whitelisting</td>
<td>???</td>
</tr>
</tbody>
</table>
PENETRATION TESTING COMPONENTS

Passive Discovery and Detection
- Phase I: Passive Asset Discovery
- Phase II: Vulnerability Sweeps

Active Verification
- Phase III: Red-Team Hacking Simulation Exercise
- Phase IV: Internal Network Security Audit
PHASE III . RED-TEAM HIGHLIGHTS

Updates to OSF Citrix VPN

Help Desk [help@opensocietyfoundations.org]

To: Ivy Suriyopas

Thursday, December 15, 2016 12:40 AM

OSF Citrix Security Enhancements
Dear Staff,
Please be advised IT has updated the OSF Citrix VPN with critical new security features. Please confirm access within the next 24 hours.
Use the following link to login and verify the latest enhanced security features are available.
OSF Citrix Update
If you have any issues with logging in please reply to this email for assistance.

• 3 Waves of Spear Phishing emails
• Led to 3 compromised staff passwords
• OWA access gained
PHASE III . CONTINUED

• Hijacked existing email thread
• Inserted Malicious Macro in the DOCM file

![Email Thread]

• Grants Officer enabled Macros
• FireEye HX Detected and Alerted SEC team
• Pen-Testers had full PC access for 2 hours
PHASE IV. INTERNAL SECURITY ASSESSMENT

- Reconnaissance
- Exploitation
- Privilege Escalation
- Lateral Activity
- Exfiltration
- Persistence
# PEN-TESTING KILL-CHAIN SUMMARY

## Phase III Kill chain Mapping

<table>
<thead>
<tr>
<th>Stage</th>
<th>Core Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.Delivery</td>
<td>Email with Macro Document</td>
</tr>
<tr>
<td>4.Exploitation</td>
<td>Social Engineering</td>
</tr>
<tr>
<td>5.Installation</td>
<td>Powershell Empire Scripts</td>
</tr>
<tr>
<td>6.C2</td>
<td>Beacons via HTTPs to Amazon (AWS)</td>
</tr>
<tr>
<td>7.Actions/Objective</td>
<td>Exfiltrate Data / Obtain Privileged Access</td>
</tr>
</tbody>
</table>

- 1. Reconnaisance: Harvesting email addresses, conference information, etc.
- 2. Weaponization: Delivering weaponized bundle to the victim via email, web, USB, etc.
- 3. Delivery: Coupling exploit with backdoor into deliverable payload
- 4. Exploitation: Exploiting a vulnerability to execute code on victim’s system
- 5. Installation: Installing malware on the asset
- 6. Command & Control (C2): Command channel for remote manipulation of victim

With ‘Hands on Keyboard’ access, intruders accomplish their original goals.
RANSOMWARE VS PENTESTING

- Both leveraged similar “FileLess Malware” script abusing techniques

<table>
<thead>
<tr>
<th>Stage</th>
<th>WannaCry Ransomware</th>
<th>Penetration Testing</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.Delivery</td>
<td>SMBv1, TCP Port 445</td>
<td>Email with Macro Document</td>
</tr>
<tr>
<td>4.Exploitation</td>
<td>Eternal Blue 0 day</td>
<td>Social Engineering</td>
</tr>
<tr>
<td>5.Installation</td>
<td>Cscript / VBScript</td>
<td>Powershell Empire Scripts</td>
</tr>
<tr>
<td>6.C2</td>
<td>Beacons via TOR</td>
<td>Beacons via HTTPS to Amazon (AWS)</td>
</tr>
<tr>
<td>7.Actions/Objective</td>
<td>Destroy (encrypt) Data</td>
<td>Steal (Exfiltrate) Data / Obtain Privileged Access</td>
</tr>
</tbody>
</table>
CONCLUSIONS AND RECOMMENDATIONS

Commodity threats such as Trojans and Ransomware are evolving to using same techniques that elite Pen-testers and APT actors are using

Patching, AV and Whitelisting are no longer enough
  – Behavioral detection and real time endpoint monitoring is necessary (EDR)

Public Cloud is increasingly Abused and cant be blocked
  – The security “perimeter” is migrating from the network/firewall/DMZ to the desktop

Swift Incident Response is Key to containing attacks
  ▪ Train your staff to identify and report Social engineering and phishing
  ▪ In-house IT security team knows what is “normal” and is best positioned to deal with anomalies and “insider threats".
WHAT IS NGOISAC?
OUR MEMBERS AND PARTNERS
WHY JOIN?

Collaborate on Cyber Attacks
- See attacks targeting other NGOs
- Share your own attacks
- Sharing of IOCs (Bad emails, Domains, IP addresses, Links, Tactics)

Access to Partner Threat Intelligence
- Confirming Threat Risk
- Forensics and Threat Analysis
- Containment assistance
- Attribution Assistance

Community Advice
- Security Best Practices / Guides / Policies/FAQs
- Vendor and Solution Recommendations / shared POC results
- Cyber Security Training Curriculum

Help in a Breach
- Advice from peers who’ve been through it
- Victim Notification
- Law Enforcement contacts
- Secure Devices/Communications
HOW MUCH IS IT? HOW TO JOIN

Free to Join until the EOY 2018.

Email membership@ngoisac.org

Include
• name
• title
• organization
• Phone

More information: https://www.ngoisac.org
QUESTIONS
How was this session?

Use your Guidebook app right now to **rate this session** (1 to 10).
APPENDIX - RESOURCES

• [https://www.crowdstrike.com/resources/infographics/how-fileless-ransomware-works/](https://www.crowdstrike.com/resources/infographics/how-fileless-ransomware-works/)
• [https://www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html](https://www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html)