WELCOME

- Jim Kennedy
  - Binary Defense Stow, Ohio
  - Manager of Software Development and Customer Support

- Paul Sems
  - TrustedSec Strongsville, Ohio
  - Practice Lead, Remediation Services
JIM’S AGENDA

• Anatomy of a targeted attack and the failures that allowed it
  • Point of entry
  • Movement
  • Target acquisition
  • Final compromise
  • Payday 1.2 Million
POINT OF ENTRY

- Phish sent to elementary custodian
  - Email filter
  - Phishing training
  - Web filter
COMPROMISE

- Payload execution
  - Local admin
  - Applocker
  - Powershell
MOVEMENT

- Total compromise of every computer in the district
  - SMBv1
TARGET ACQUISITION

- Traffic patterns
- Name
- Board minutes
FINAL COMPROMISE

- Bank website redirection
  - Web filter
  - User URL verification
  - Bank 2FA
THREE MONTHS

- No idea
  - EDR/MDR
    - Crowdstrike
    - Carbon Black
    - Me
  - Remediation
    - Ship your logs
    - Log DNS
Avoiding cybersecurity mistakes that can cost organizations Millions.
Avoiding cybersecurity mistakes that have cost organizations Billions.
Who:
Threat Actors
1) Social-Engineering Attacks
2) Fast-Track Penetration Testing
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit

set> exit

Thank you for shopping with the Social-Engineer Toolkit.
HACK THE GIBSON...AND REMEMBER...HUGS ARE WORTH MORE THAN HANDSHAKES

root@kali:~/.set# umount /media/root/FLASH
2018 - Verizon Breach Report

Top Threat Actors

1) Organized Crime
2) State-Affiliated
3) System Admins
Why?
Threat Actor
Motivation
FBI Statistics

2018 Overall Statistics

**IC3 COMPLAINTS LAST 5 YEARS**

<table>
<thead>
<tr>
<th>Year</th>
<th>Complaints</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014</td>
<td></td>
</tr>
<tr>
<td>2015</td>
<td></td>
</tr>
<tr>
<td>2016</td>
<td></td>
</tr>
<tr>
<td>2017</td>
<td></td>
</tr>
<tr>
<td>2018</td>
<td></td>
</tr>
</tbody>
</table>

- **# Of Complaints Reported Since Inception (’00):** 4,415,870
- **Approximately 300,000 Complaints Received Per Year On Average**
- **$2.71 Billion Victim Losses in 2018**
- **Over 900 Complaints Received Per Day On Average**
Merck did what any of us would do when facing a disaster: It turned to its insurers. After all, through its property policies, the company was covered—after a $150 million deductible—to the tune of $1.75 billion for catastrophic risks including the destruction of computer data, coding, and software. So it was stunned when most of its 30 insurers and reinsurers denied coverage under those policies. Why? Because Merck’s property policies specifically excluded another class of risk: an act of war.
### 2018 Impact in Ohio

<table>
<thead>
<tr>
<th>Rank</th>
<th>State</th>
<th>Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>California</td>
<td>$450,482,128</td>
</tr>
<tr>
<td>2</td>
<td>New York</td>
<td>$201,090,065</td>
</tr>
<tr>
<td>3</td>
<td>Texas</td>
<td>$195,611,047</td>
</tr>
<tr>
<td>4</td>
<td>Florida</td>
<td>$178,141,470</td>
</tr>
<tr>
<td>5</td>
<td>North Carolina</td>
<td>$137,230,988</td>
</tr>
<tr>
<td>6</td>
<td>Ohio</td>
<td>$97,730,046</td>
</tr>
<tr>
<td>7</td>
<td>Illinois</td>
<td>$82,849,726</td>
</tr>
<tr>
<td>8</td>
<td>Michigan</td>
<td>$80,929,815</td>
</tr>
<tr>
<td>9</td>
<td>New Jersey</td>
<td>$79,711,752</td>
</tr>
<tr>
<td>10</td>
<td>Massachusetts</td>
<td>$68,242,216</td>
</tr>
</tbody>
</table>

*Total Losses by Victim per State*
How:
Threat Actor Methods
iPhone

https://googleprojectzero.blogspot.com/2019/08/implant-teardown.html
iPhone
iPhone

Vulnerabilities By Year

Distribution of all vulnerabilities by CVSS Scores

<table>
<thead>
<tr>
<th>CVSS Score</th>
<th>Number Of Vulnerabilities</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-1</td>
<td>28</td>
<td>1.70</td>
</tr>
<tr>
<td>1-2</td>
<td>113</td>
<td>6.80</td>
</tr>
<tr>
<td>2-3</td>
<td>21</td>
<td>1.30</td>
</tr>
<tr>
<td>3-4</td>
<td>311</td>
<td>18.80</td>
</tr>
<tr>
<td>4-5</td>
<td>174</td>
<td>10.50</td>
</tr>
<tr>
<td>5-6</td>
<td>571</td>
<td>34.50</td>
</tr>
<tr>
<td>6-7</td>
<td>146</td>
<td>8.80</td>
</tr>
<tr>
<td>7-8</td>
<td>5</td>
<td>0.30</td>
</tr>
<tr>
<td>8-9</td>
<td>285</td>
<td>17.20</td>
</tr>
<tr>
<td>Total</td>
<td>1654</td>
<td></td>
</tr>
</tbody>
</table>

Weighted Average CVSS Score: **6.7**
Windows 10

Vulnerabilities By Year

- 2015: 57
- 2016: 172
- 2017: 268
- 2018: 257
- 2019: 357

Vulnerability Distribution By CVSS Scores

- CVSS Score Ranges:
  - 0-1
  - 1-2
  - 2-3
  - 3-4
  - 4-5
  - 5-6
  - 6-7
  - 7-8
  - 8-9
  - 9-10

- 2015: 57
- 2016: 172
- 2017: 268
- 2018: 257
- 2019: 357

https://www.cvedetails.com
Android

Vulnerabilities By Year

Distribution of all vulnerabilities by CVSS Scores

<table>
<thead>
<tr>
<th>CVSS Score</th>
<th>Number Of Vulnerabilities</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-1</td>
<td>15</td>
<td>0.60</td>
</tr>
<tr>
<td>1-2</td>
<td>98</td>
<td>4.00</td>
</tr>
<tr>
<td>2-3</td>
<td>12</td>
<td>0.50</td>
</tr>
<tr>
<td>3-4</td>
<td>595</td>
<td>24.50</td>
</tr>
<tr>
<td>4-5</td>
<td>211</td>
<td>8.70</td>
</tr>
<tr>
<td>5-6</td>
<td>212</td>
<td>8.70</td>
</tr>
<tr>
<td>6-7</td>
<td>505</td>
<td>20.80</td>
</tr>
<tr>
<td>7-8</td>
<td>28</td>
<td>1.20</td>
</tr>
<tr>
<td>8-9</td>
<td>752</td>
<td>31.00</td>
</tr>
<tr>
<td>Total</td>
<td>2428</td>
<td></td>
</tr>
</tbody>
</table>

Weighted Average CVSS Score: 7.4
Take Action
Prevention
Prevention

1. Good Password Hygiene: 
   No Double Dipping with Passwords!
2. The number of the day is 2: 
   Use MFA when possible!
3. Backup: Keep ‘em Separated: 
   Protect your backups!
4. An Apple A Day keeps the Hackers away: 
   Do your updates... now!
5. Where’s Waldo? 
   Expect fraudulent e-mail!
Take Action
Tools!
Hacking Demo

• KALI Linux

• Windows 10 – Updated

• User “Clicked” a link...
Password Audit

• SpecOpsSoftware
  • https://specopssoft.com/product/specops-password-auditor/

• KnowBe4
  • https://www.knowbe4.com/free-it-security-tools
Changes to LDAP – March 2020

Install tools:
Install-Module PSWinReportingV2 -Force
Install-Module Testimo -Force

Enable Logging:
Set-WinADDiagnostics -Diagnostics 'LDAP Interface Events' -Level Basic -SkipRoDC
Changes to LDAP – March 2020

Review Logs:
$Events = Find-Events -Report LdapBindingsDetails, LdapBindingsSummary - DatesRange Last7days -DetectDC

Test LDAPS Connection:
test-netconnection yourdomain.com -port 636
Security Baseline

Free for K-12!
• CIS CAT-PRO
• BuildKits!
• CSAT

• [https://www.cisecurity.org/cis-securesuite/pricing-and-categories/](https://www.cisecurity.org/cis-securesuite/pricing-and-categories/)

• [https://csat.cisecurity.org/](https://csat.cisecurity.org/)
Microsoft Scorecard

• Demo
Questions?

TrustedSec.com

The information security industry is constantly evolving—keep up by following TrustedSec’s active social media, blogs, podcasts, and webinars.

Follow Us
@TRUSTEDSEC