THREAT LANDSCAPE AT THE UW

JAMES POLAND, CYBER THREAT ANALYST (jwpoland@uw.edu)
AND
REBEKAH SKIVER THOMPSON, INCIDENT RESPONSE & THREAT INTELLIGENCE MANAGER (bskiver@uw.edu)

OFFICE OF THE CHIEF INFORMATION SECURITY OFFICER
UNIVERSITY OF WASHINGTON
OUTLINE

• Types of information that are of value
• Common targeting methods
• Case study
• Q&A
Note on terminology

- Adversary
- Threat actor/bad actor
- Black hat
- APT (Advanced Persistent Threat)/nation state
- Phisher/spammer
- Competitor
The Value of Information
The Value of Information

"If what you have is important, someone will want it."
Types of Important Information

- Personal: identification; financial; health-related; contacts
- Research/academic: subscription services; intellectual property
- Business: negotiations; financial account access; non-public records
Types of Important Information

- **Personal**: identification; financial; health-related; contacts
- Research/academic: subscription services; *intellectual property*
- Business: negotiations; financial account access; non-public records
Value of Personal Information

To the owner:

• Personal privacy
• Personal efficiency

To the adversary:

• $$ from sale, ransom
• Fraud
• Invasion of privacy
Value of Intellectual Property

To the academic:
- Results, publications
- Future grants/contracts
- Royalties, notariety
- Spinoffs

To the adversary:
- $$ from sale or ransom
- Knowledge without investment
- Market first
- Publish first
Types of Important Information

- Personal: identification; financial; health-related; contacts
- Research/academic: subscription services; intellectual property
- Business: negotiations; financial account access; non-public records
Types of Important Information

- Personal: identification; financial; health-related; contacts
- Research/academic: subscription services; intellectual property
- Business: negotiations; financial account access; non-public records
- Account access credentials
How are user credentials obtained?
How are user credentials obtained?

Phishing!
This is your last warning your University of Washington mailbox will stop sending and receiving messages in the next 72 hours. Kindly increase your mailbox size by filling out the necessary mailbox requirement. CLICK HERE to complete
This is your last warning. Your University of Washington mailbox will stop sending and receiving messages in the next 72 hours. Kindly increase your mailbox size by filling out the necessary mailbox requirement. CLICK HERE to complete.
This is your last warning your University of Washington mailbox will stop sending and receiving messages in the next 72 hours. Kindly increase your mailbox size by filling out the necessary mailbox requirement. CLICK HERE to complete.
This is your last warning that your University of Washington mailbox will stop sending and receiving messages in the next 72 hours. Kindly increase your mailbox size by filling out the necessary mailbox requirement. CLICK HERE to complete.
FYI details of the meeting can be found on this page.
Phishing by the numbers: 2017

494 unique phishing messages reported (targeting UW credentials)
• Approximately 35% fake UW Weblogin or O365 login pages

Victims
• 920 phishing victims (21% of all compromised accounts; down from 67% in 2016)
2018 (YTD)

- 1480 compromised accounts
- 193 phished (13% of all compromised accounts)
2018 (YTD)

- 1480 compromised accounts
- 193 phished (13% of all compromised accounts)

So if phishing is down, where are the compromised accounts coming from?
Suspect: Third Party Breaches and Password Re-use

haveibeenpwned.com:

60,894 u.washington.edu addresses

24,956 uw.edu addresses

Worldwide: 4,949,099,146 known accounts exposed in breaches
Credential Stuffing and Brute Force

• Use of known username/password combinations = “credential stuffing”
• Evidence of constant password guessing on the network

• See if your password has been exposed:
  https://haveibeenpwned.com/Passwords
<table>
<thead>
<tr>
<th>Password</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>123456</td>
<td>This password has been seen 20,760,336 times before</td>
</tr>
<tr>
<td>password</td>
<td>3,303,003</td>
</tr>
<tr>
<td>abc123</td>
<td>2,670,319</td>
</tr>
<tr>
<td>admin</td>
<td>41,812</td>
</tr>
<tr>
<td>seattle</td>
<td>21,071</td>
</tr>
<tr>
<td>seattleseahawks</td>
<td>69</td>
</tr>
<tr>
<td>rC#55a^k</td>
<td>0</td>
</tr>
</tbody>
</table>
https://haveibeenpwned.com/Passwords

123456  This password has been seen 20,760,336 times before
password   3,303,003
abc123      2,670,319
admin       41,812
seattle    21,071
seattleseahawks  69
rC#55a^k  0

Choose unique, complex passwords and change default passwords
Vulnerability (computing)

In computer security, a vulnerability is a weakness which allows an attacker to reduce a system's information assurance. Security incidents are the intersection of three elements:

• A system susceptibility
• Attacker access to the susceptibility
• Attacker capability to exploit the susceptibility

Top 10 Attacks: 24 Hours

1. NETBIOS: SMB Remote Access - 3,873,463
2. RDP: Windows Connect - 2,178,783
3. HTTP Tunneling - 406,275
4. Session Hijacking - 335,712
5. SYN Host Sweep - 227,775
6. Port Scanning - 127,539
7. RDP: RST Packet - 112,053
8. MSSQL: Identify Server - 74,543
10. UDP Host Sweep - 39,471
Free tools!

Vulnerability discovery
- Shodan
- OpenVAS
- Retina CS Community
- Microsoft Baseline Security Analyzer
- Rapid7 Nexpose Community Edition

Vulnerability exploitation
- Metasploit
- Kali Linux
- sqlmap
- THC Hydra
Targeted attacks

Use network scanning, open source information

- Spear phishing
- OS vulnerabilities

Goal: Obtain credentials/resources, place targeted malware, gain control of host (steal information/lateral movement on network)

Impact: Financial loss, loss of intellectual property, risk to national security
Spear phishing examples
Hi Robert,

How is your day going, are you in the office?

Thanks,

Ana Mari Cauce

---

Hi Elizabeth,

I want you to make a payment to a vendor for services. Confirm if you can get this done today so I can forward you the beneficiary details.

Regards,

Russell
Dear [Name],

I am writing a cover story for CEN, the magazine of the American Chemical Society, about ocean physical and am hoping you will have time for an interview. With the story, we’re hoping to really dig into the science of how the life cycle of ocean physical, as well as the rationale and mechanism for the various treatments in development (and other promising areas that might be explored).

On a separate note, we’re planning to cover this side of the problem in a separate piece, so if that’s an area you’d like to talk about, I’m all ears.

Please feel free to email with your answers to any questions about the story or our publication. Thanks in advance for your help.

Kind regards,

Smith.Parry
Senior Editor, C
917.710.0924
Smith.Parry@gmail.com
Twitter: SmithParry
CASE STUDY: Advanced Persistent Threat (APT)

- Method of operation:
  - PHISH!!!
  - Target private network space
  - Dump credentials
  - Move laterally
  - Use advanced tools
  - Abuse web server
1
Spear phishing

- Subject: Ocean Physical Story
- "CEN" => Chemical & Engineering News
- Lookalike domain
- "Smith.Parry", "Twitter: Smith.Parry", "Senior Editor"

Advanced Persistent Threat (APT) Case Study
• Persistent outbound communication via 80/tcp, 443/tcp
• Communication obfuscated
• Terminal session as Local Administrator

Advanced Persistent Threat (APT) Case Study
Advanced Persistent Threat (APT) Case Study

- Port scan
  - 10.0.0.0/8
  - 172.16.0.0/12
- Enumerate users
  - local, domain - sadm_, eadm_
- Spear phishing
- RAT
- Move laterally
- Mimikatz
  - Dump credentials
  - Pass-the-hash
Advanced Persistent Threat (APT) Case Study

1. Spear phishing
2. RAT
3. Move laterally

- Vulnerable web site => install web shell
  - Internal network port scan via nmap
  - Tunnel to targets via ssh
  - EternalBlue, install RAT
• Fortunately, never observed
Questions?

Jim Poland - jwpoland@uw.edu
Becky Skiver Thompson - bskiver@uw.edu