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

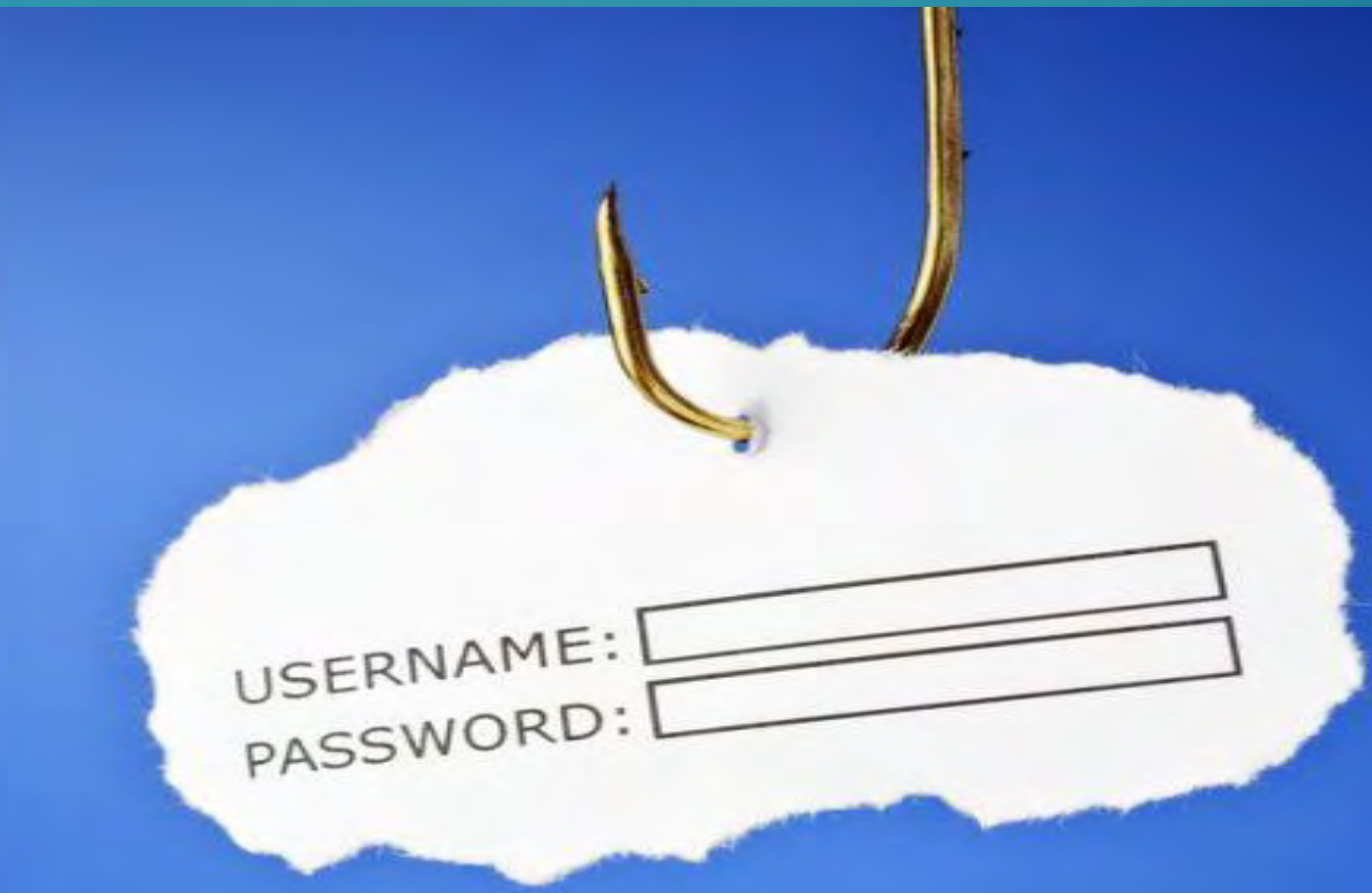
Types of Important Information

- 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!



Tue 3/6/2018 11:49 AM

[redacted] <[redacted]@students.post.edu>

Update

To [redacted]

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

Tue 3/6/2018 11:49 AM

[redacted] <[redacted]@students.post.edu>

Update

To [redacted]

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

Tue 3/6/2018 11:49 AM

[redacted] <[redacted]@students.post.edu>

Update

To [redacted]

This is your last warning your University of Washington mailbox will stop sending and receiving messages in th next 72 hours. Kindly increase your mailbox size by filling out the necessary mailbox requirement. CLICK HERE to complet

Tue 3/6/2018 11:49 AM

[redacted] <[redacted]@students.post.edu>

Update

To [redacted]

This is your last warning your University of Washington mailbox will stop sending and receiving messages in th next 72 hours. Kindly increase your mailbox size by filling out the necessary mailbox requirement. CLICK HERE to comple

hello

From: [redacted] <[redacted]@uw.edu> Add

To: Undisclosed recipients <>, ;

Date: Mon, 5 Mar 2018 11:12:20 +0000

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

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

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

Scanning for vulnerabilities

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

Source: Wikipedia

SHODAN 48.64.0/19,204.69.8.0/21,205.175.96.0/1 port:445 Explore Downloads Reports Enterprise Access Contact Us

My Ac

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS

4,566

TOP COUNTRIES

United States	4,566

TOP ORGANIZATIONS

University of Washington	4,566

TOP OPERATING SYSTEMS

Windows 7 Enterprise 7...	623
Darwin	523
Windows 10 Enterprise ...	460
Windows 10 Enterprise ...	188
Windows 10 Enterprise ...	152

TOP PRODUCTS

Samba	260

140.142.199.11
tritonia.fhl.washington.edu
Darwin
University of Washington
Added on 2018-03-01 00:55:52 GMT
United States, Seattle
Details

```
SMB Status
Authentication: enabled
SMB Version: 1
Capabilities: unicode,large-files,nt-smb,rpc-remote-api,nt-status,level2-oplocks,nt-find,infolevel-passthru,large-readx,large-
itex,unix,extended-security
```

128.95.13.59
D-128-95-13-59.dhcp4.washington.edu
University of Washington
Added on 2018-03-01 00:41:40 GMT
United States, Seattle
Details

```
SMB Status
Authentication: enabled
SMB Version: 2
Capabilities: raw-mode
```

69.91.128.95
D-69-91-128-95.dhcp4.washington.edu
Darwin
University of Washington
Added on 2018-03-01 00:35:02 GMT
United States, Seattle
Details

SMB Status

SHODAN 8.64.0/19,204.69.8.0/21,205.175.96.0/1 port:3389 Explore Downloads Reports Enterprise Access Contact Us

My Ac

Exploits Maps Images Share Search Download Results Create Report

TOTAL RESULTS

2,083

TOP COUNTRIES

United States	2,083

TOP ORGANIZATIONS

University of Washington	2,083

TOP OPERATING SYSTEMS

Windows 7 or 8	11
Windows XP	1

128.208.221.23

kestrel.rad.washington.edu
University of Washington
Added on 2018-03-01 01:08:43 GMT
United States, Seattle
Details

SSL Certificate
Issued By:
|- Common Name: **VIL-Ftp-Server**
Issued To:
|- Common Name: **VIL-Ftp-Server**

Supported SSL Versions
TLSv1, TLSv1.1, TLSv1.2

```
Remote Desktop Protocol
\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00
```

128.208.236.90

D-128-208-236-90.dhcp4.washington.edu
University of Washington
Added on 2018-03-01 01:05:09 GMT
United States, Seattle
Details

SSL Certificate
Issued By:
|- Common Name: **strand-PC**
Issued To:
|- Common Name: **strand-PC**

Supported SSL Versions
TLSv1, TLSv1.1, TLSv1.2

```
Remote Desktop Protocol
\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00
```

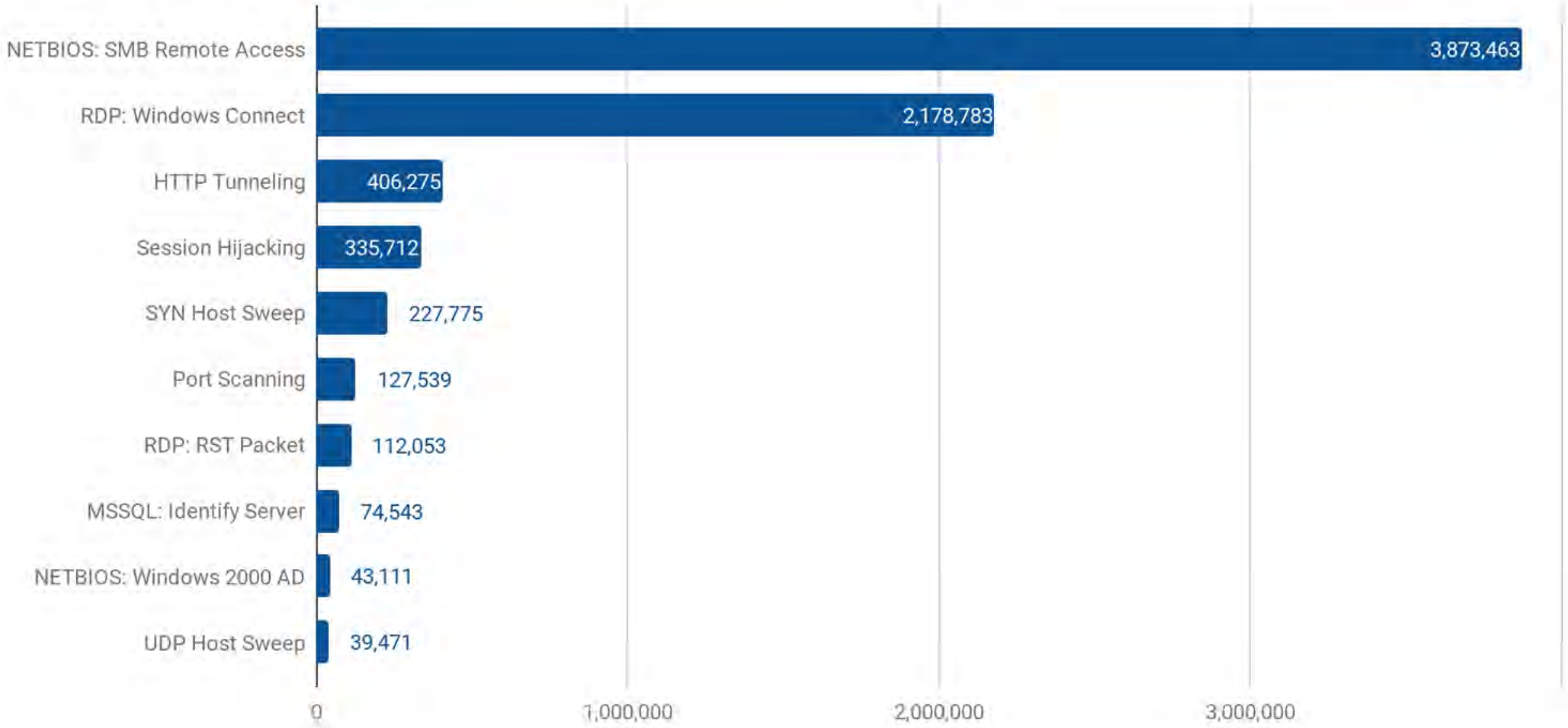
128.95.87.146

D-128-95-87-146.dhcp4.washington.edu
University of Washington
Added on 2018-03-01 00:57:23 GMT
United States, Seattle
Details

SSL Certificate
Issued By:
|- Common Name: **CC-MXL6061B6G.clients.uw.edu**

```
Remote Desktop Protocol
\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00
```

Top 10 Attacks: 24 Hours



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

Fri 12/1/2017 2:38 AM

Ana Cauce <Ana.Cauce@uw.edu>

Request

To Robert [redacted]

Hi Robert,

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

Thanks,

Ana Mari Cauce

Fri 3/2/2018 9:46 AM

[redacted]

Transfer Request

To [redacted]

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 [redacted]

Fri 3/2/2018 9:15 AM

Smith.Parry@[redacted].com

Ocean Physical Story

To [redacted]

Questions about the story.rtf
85 KB

Dear [redacted],

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.

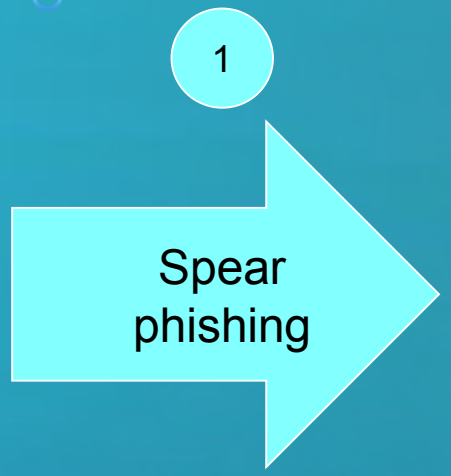
Please feel free to email with your answers to any questions about the story or our publication. Thanks in advance for your help

Kind regards,

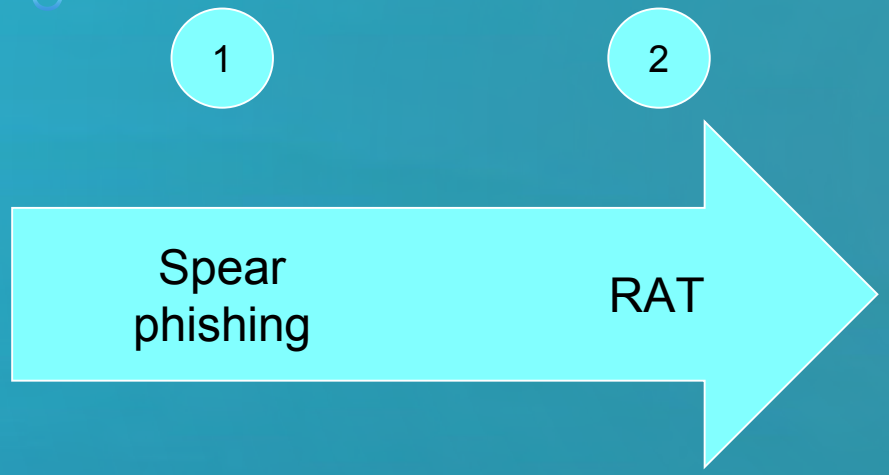
Smith.Parry
Senior Editor, C
917.710.0924
Smith.Parry gmail[.]com
twitter: SmithParry

CASE STUDY: Advanced Persistent Threat (APT)

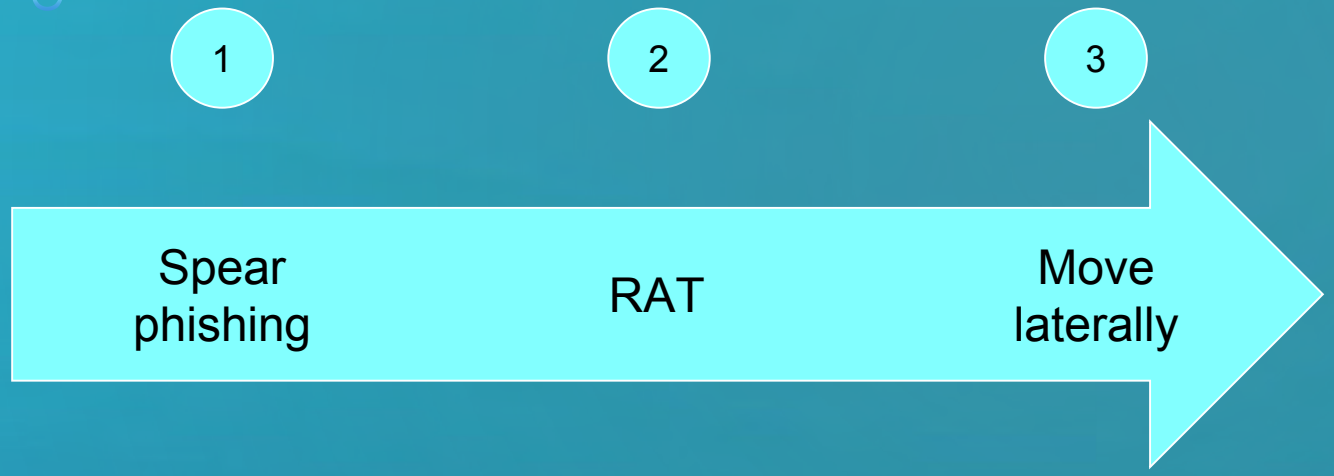
- Method of operation:
  - PHISH!!!
  - Target private network space
  - Dump credentials
  - Move laterally
  - Use advanced tools
  - Abuse web server



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

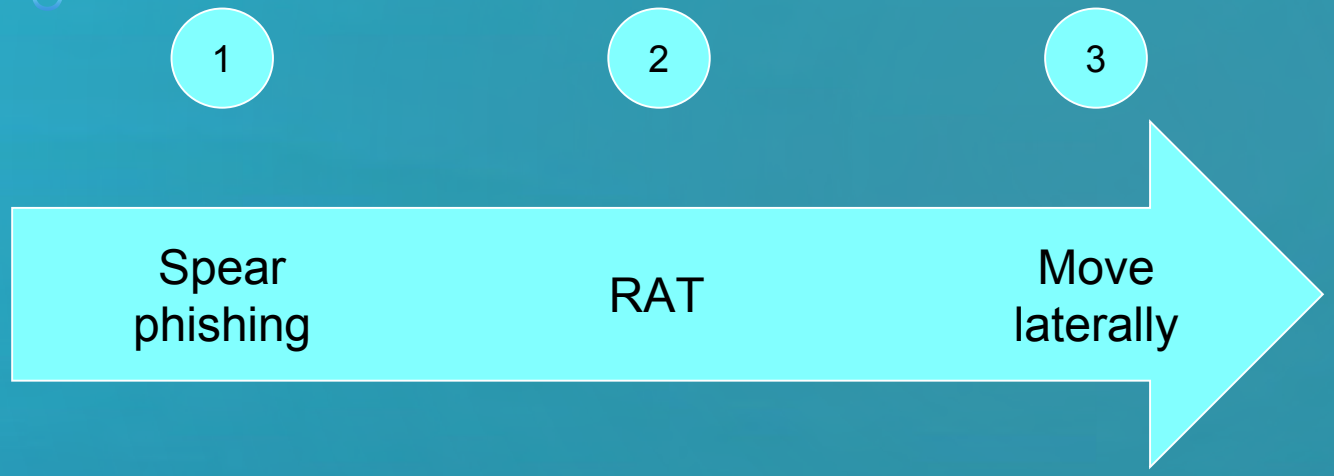


- Persistent outbound communication via 80/tcp, 443/tcp
- Communication obfuscated
- Terminal session as Local Administrator

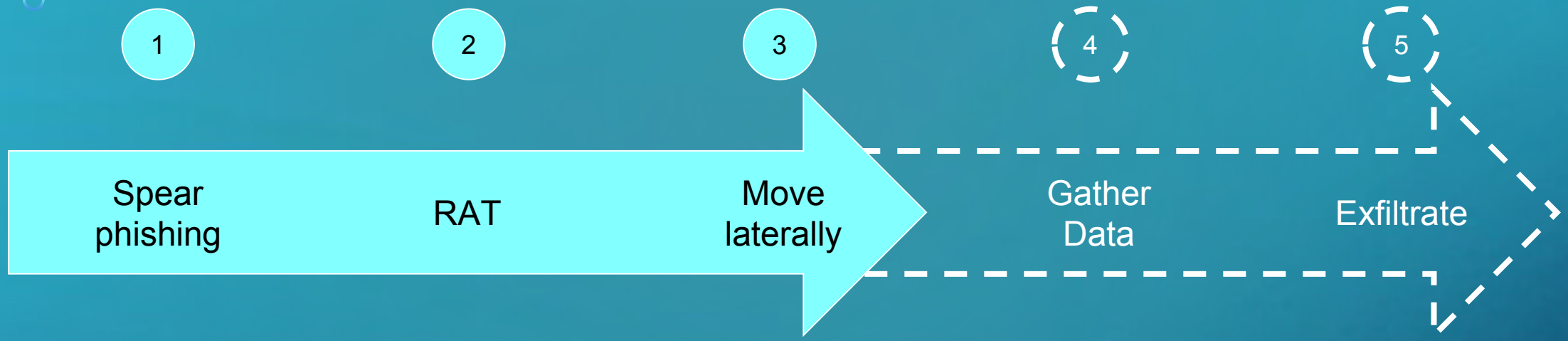


- Port scan
  - 10.0.0.0/8
  - 172.16.0.0/12
- Enumerate users
  - local, domain - sadm_, eadm_
- Mimikatz
  - Dump credentials
  - Pass-the-hash

Advanced Persistent Threat (APT) Case Study



- 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