Lure. Deceive. Defeat.

Researching Deception for Accurate Post-Breach Detection

Omer Zohar

Head of Research, TopSpin Security

Agenda

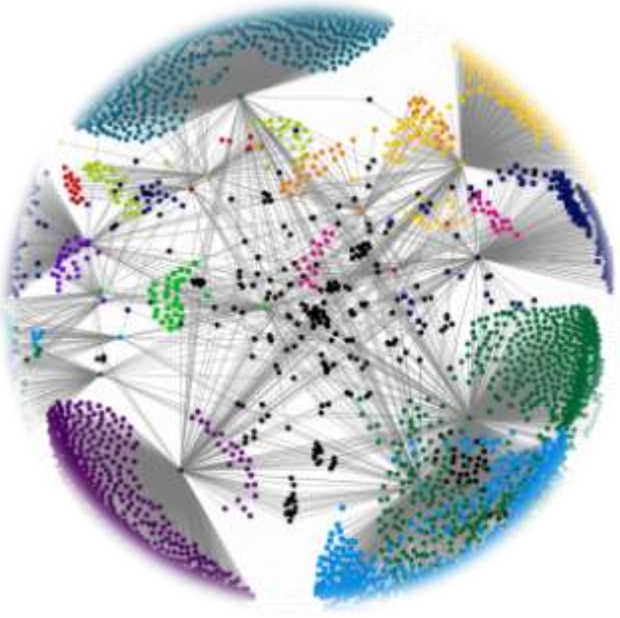
- Deception – an Introduction
- Putting Deception to the test
- How to Deceit
- Research Results
- Wrap up & Conclusions

Why are we talking about **post breach detection**?

Patchy perimeters

+

Chaotic internal networks



=

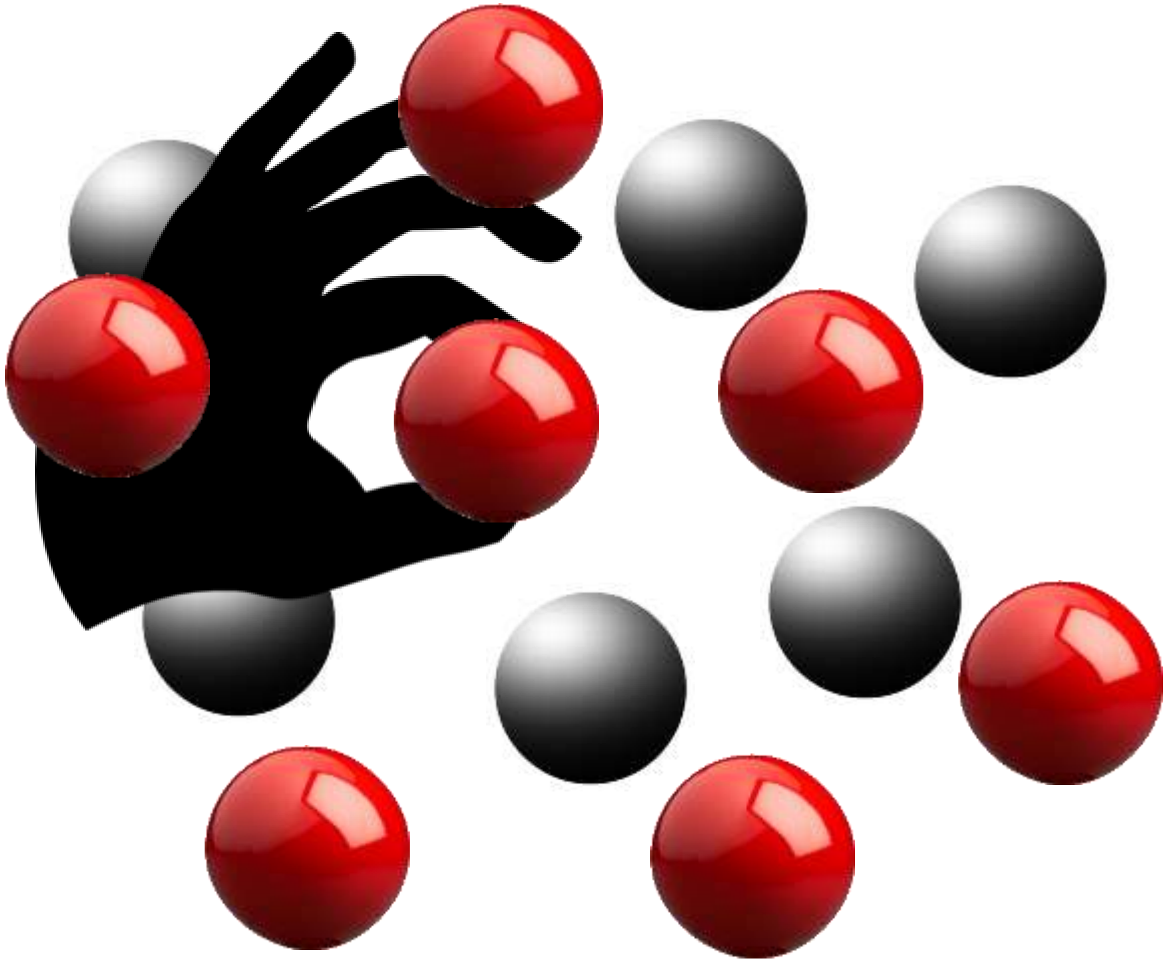
Fertile ground for attackers

Attackers have the advantage

99.999 % = Failure

1 = Success

Or do they?



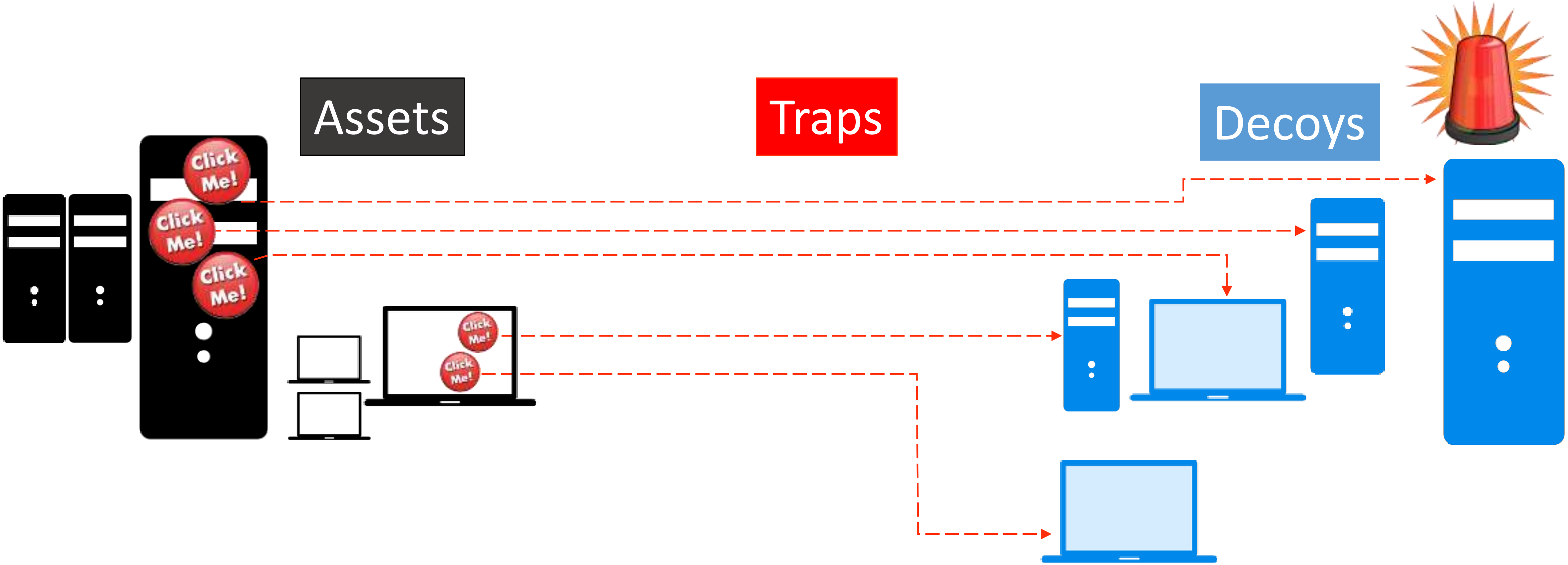
The defender's main advantage is the fundamental control of information

Which leads to the ability to apply Deception

How Deception Works – Traps and Decoys

Assets
Decoys

How Deception Works – Traps and Decoys



Now Wait a minute…

Does it really work

Seems like nobody checked

So we did…

Defining the research questions

Are decoys and traps effective in real-life scenarios?

Do attackers really take the bait?

What is the ideal deployment strategy?

Let the Games Begin

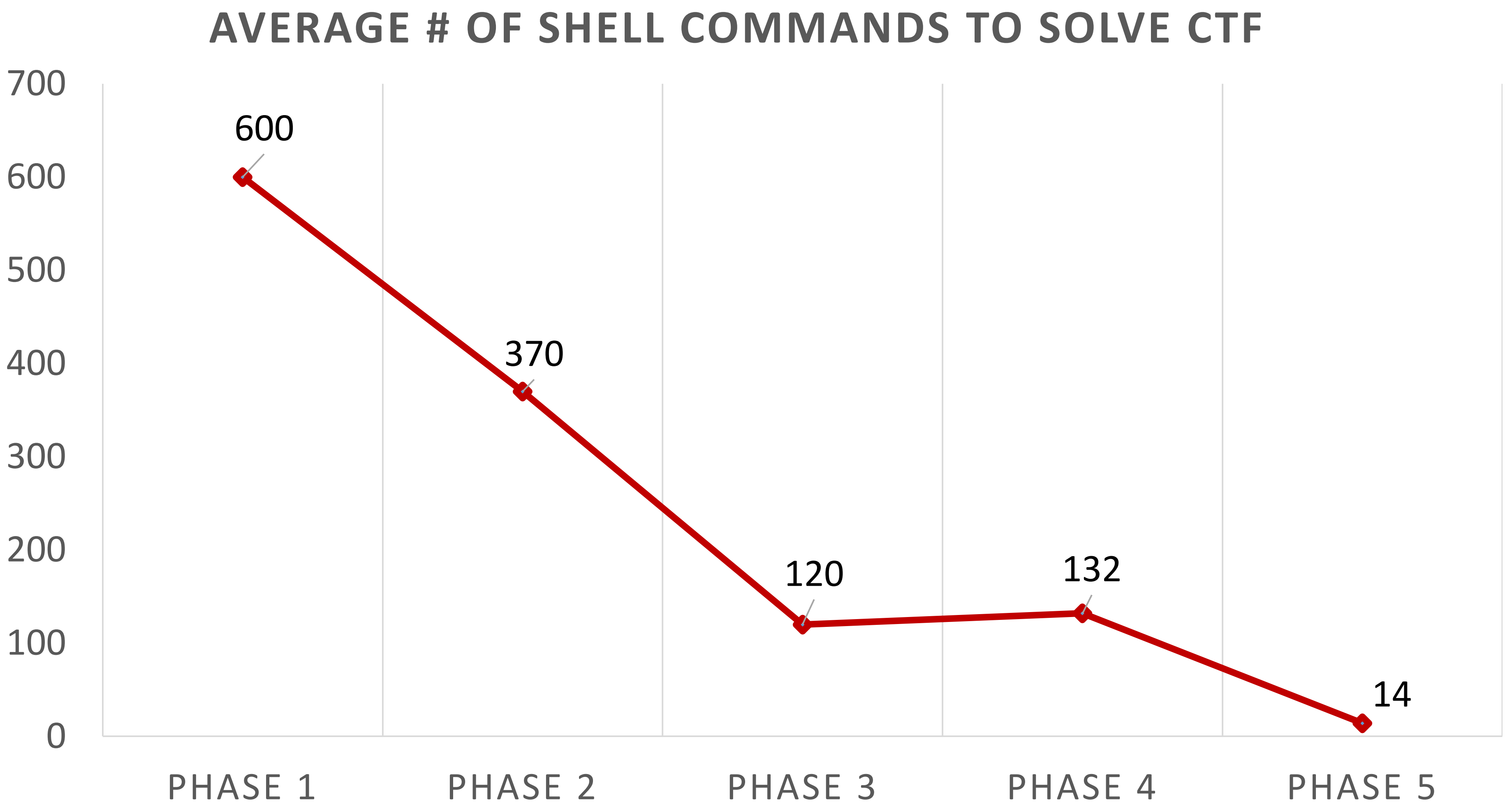
1. Build the Environment
2. Add data
3. Deception overlay
4. Build the challenge
5. Bring’em on!

CTF – Stats & Scores

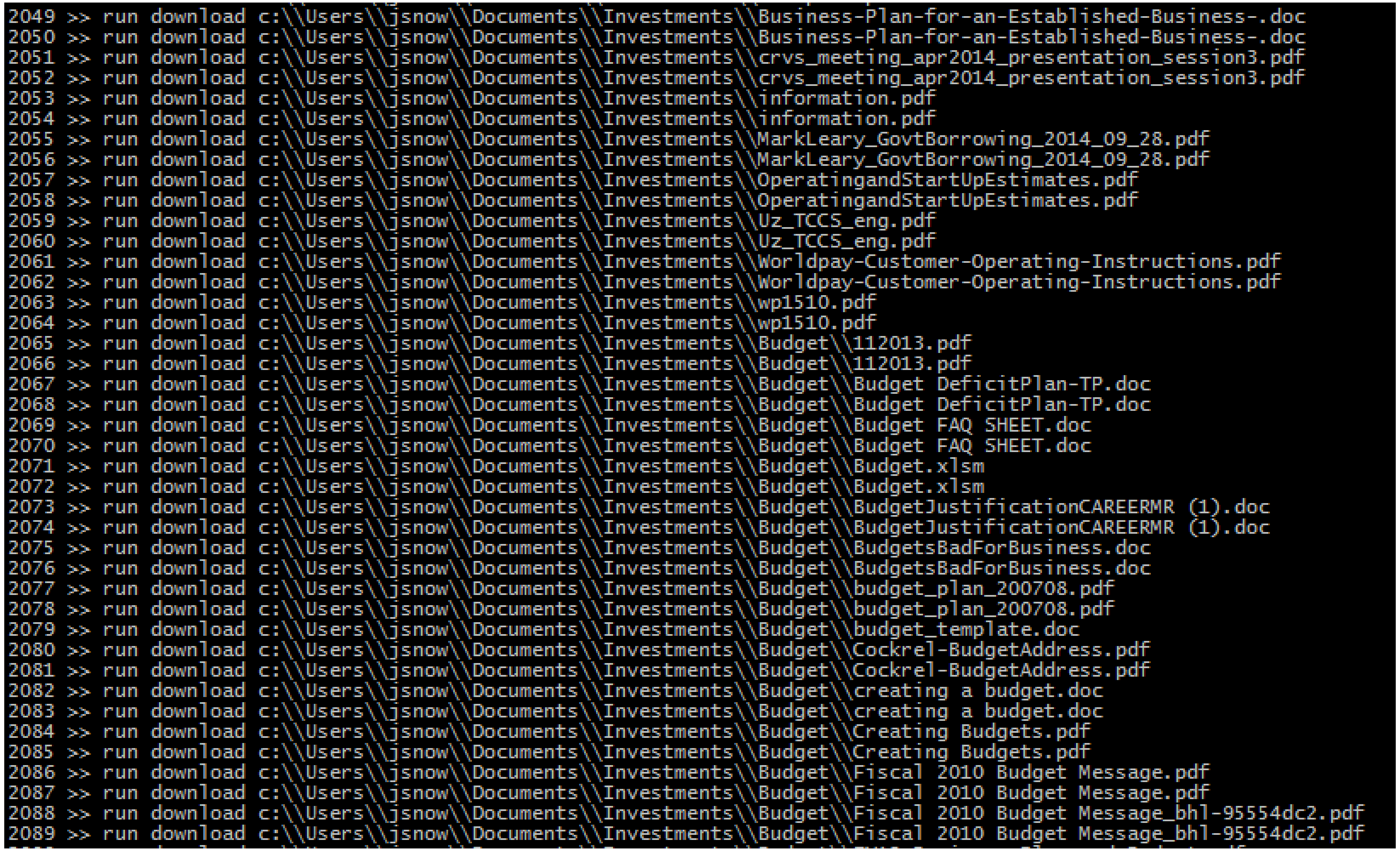
- Ran over a month
- Over 50 security professionals from all over the world
- 6-7 hours on average per player
- ~1.7M data lines collected

"I've seen a man who could change his face, the way that other men change their clothes."

Exploiting the knowledge Gap

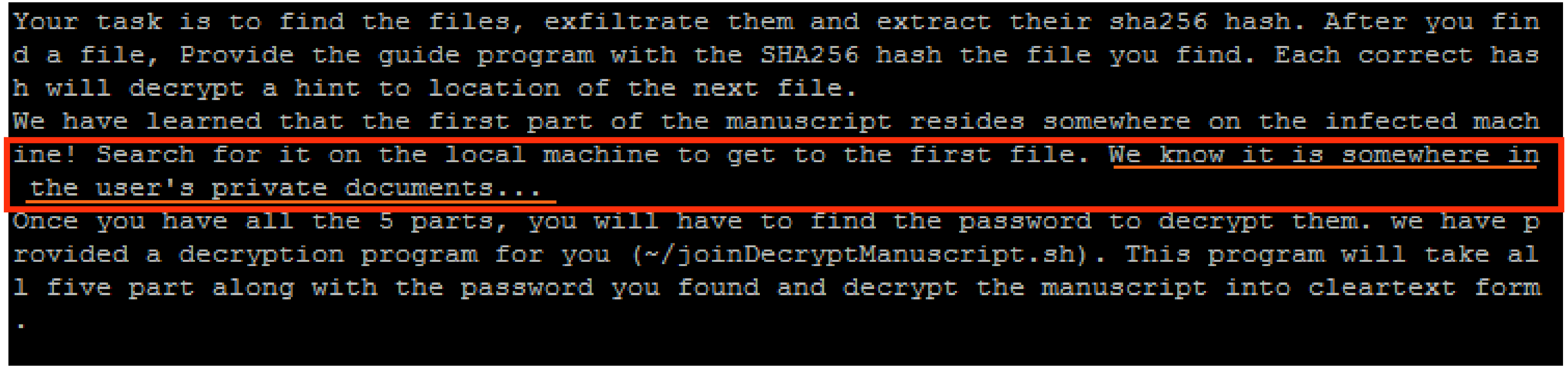


The “Spraying” Attack Pattern



```
2049 >> run download c:\\Users\\jsnow\\Documents\\Investments\\Business-Plan-for-an-Established-Business-.doc
2050 >> run download c:\\Users\\jsnow\\Documents\\Investments\\Business-Plan-for-an-Established-Business-.doc
2051 >> run download c:\\Users\\jsnow\\Documents\\Investments\\crvs_meeting_apr2014_presentation_session3.pdf
2052 >> run download c:\\Users\\jsnow\\Documents\\Investments\\crvs_meeting_apr2014_presentation_session3.pdf
2053 >> run download c:\\Users\\jsnow\\Documents\\Investments\\information.pdf
2054 >> run download c:\\Users\\jsnow\\Documents\\Investments\\information.pdf
2055 >> run download c:\\Users\\jsnow\\Documents\\Investments\\MarkLeary_GovtBorrowing_2014_09_28.pdf
2056 >> run download c:\\Users\\jsnow\\Documents\\Investments\\MarkLeary_GovtBorrowing_2014_09_28.pdf
2057 >> run download c:\\Users\\jsnow\\Documents\\Investments\\OperatingandStartUpEstimates.pdf
2058 >> run download c:\\Users\\jsnow\\Documents\\Investments\\OperatingandStartUpEstimates.pdf
2059 >> run download c:\\Users\\jsnow\\Documents\\Investments\\Uz_TCCS_eng.pdf
2060 >> run download c:\\Users\\jsnow\\Documents\\Investments\\Uz_TCCS_eng.pdf
2061 >> run download c:\\Users\\jsnow\\Documents\\Investments\\Worldpay-Customer-Operating-Instructions.pdf
2062 >> run download c:\\Users\\jsnow\\Documents\\Investments\\Worldpay-Customer-Operating-Instructions.pdf
2063 >> run download c:\\Users\\jsnow\\Documents\\Investments\\wp1510.pdf
2064 >> run download c:\\Users\\jsnow\\Documents\\Investments\\wp1510.pdf
2065 >> run download c:\\Users\\jsnow\\Documents\\Investments\\Budget\\112013.pdf
2066 >> run download c:\\Users\\jsnow\\Documents\\Investments\\Budget\\112013.pdf
2067 >> run download c:\\Users\\jsnow\\Documents\\Investments\\Budget\\Budget DeficitPlan-TP.doc
2068 >> run download c:\\Users\\jsnow\\Documents\\Investments\\Budget\\Budget DeficitPlan-TP.doc
2069 >> run download c:\\Users\\jsnow\\Documents\\Investments\\Budget\\Budget FAQ SHEET.doc
2070 >> run download c:\\Users\\jsnow\\Documents\\Investments\\Budget\\Budget FAQ SHEET.doc
2071 >> run download c:\\Users\\jsnow\\Documents\\Investments\\Budget\\Budget.xlsm
2072 >> run download c:\\Users\\jsnow\\Documents\\Investments\\Budget\\Budget.xlsm
2073 >> run download c:\\Users\\jsnow\\Documents\\Investments\\Budget\\BudgetJustificationCAREERMR (1).doc
2074 >> run download c:\\Users\\jsnow\\Documents\\Investments\\Budget\\BudgetJustificationCAREERMR (1).doc
2075 >> run download c:\\Users\\jsnow\\Documents\\Investments\\Budget\\BudgetsBadForBusiness.doc
2076 >> run download c:\\Users\\jsnow\\Documents\\Investments\\Budget\\BudgetsBadForBusiness.doc
2077 >> run download c:\\Users\\jsnow\\Documents\\Investments\\Budget\\budget_plan_200708.pdf
2078 >> run download c:\\Users\\jsnow\\Documents\\Investments\\Budget\\budget_plan_200708.pdf
2079 >> run download c:\\Users\\jsnow\\Documents\\Investments\\Budget\\budget_template.doc
2080 >> run download c:\\Users\\jsnow\\Documents\\Investments\\Budget\\Cockrel-BudgetAddress.pdf
2081 >> run download c:\\Users\\jsnow\\Documents\\Investments\\Budget\\Cockrel-BudgetAddress.pdf
2082 >> run download c:\\Users\\jsnow\\Documents\\Investments\\Budget\\creating a budget.doc
2083 >> run download c:\\Users\\jsnow\\Documents\\Investments\\Budget\\creating a budget.doc
2084 >> run download c:\\Users\\jsnow\\Documents\\Investments\\Budget\\Creating Budgets.pdf
2085 >> run download c:\\Users\\jsnow\\Documents\\Investments\\Budget\\Creating Budgets.pdf
2086 >> run download c:\\Users\\jsnow\\Documents\\Investments\\Budget\\Fiscal 2010 Budget Message.pdf
2087 >> run download c:\\Users\\jsnow\\Documents\\Investments\\Budget\\Fiscal 2010 Budget Message.pdf
2088 >> run download c:\\Users\\jsnow\\Documents\\Investments\\Budget\\Fiscal 2010 Budget Message_bhl-95554dc2.pdf
2089 >> run download c:\\Users\\jsnow\\Documents\\Investments\\Budget\\Fiscal 2010 Budget Message_bhl-95554dc2.pdf
```

Its so easy when you know where to look…



```
Your task is to find the files, exfiltrate them and extract their sha256 hash. After you fin
d a file, Provide the guide program with the SHA256 hash the file you find. Each correct has
h will decrypt a hint to location of the next file.
We have learned that the first part of the manuscript resides somewhere on the infected mach
ine! Search for it on the local machine to get to the first file. We know it is somewhere in
 the user's private documents...
Once you have all the 5 parts, you will have to find the password to decrypt them. we have p
rovided a decryption program for you (~/joinDecryptManuscript.sh). This program will take al
l five part along with the password you found and decrypt the manuscript into cleartext form
.
```

RTFM!

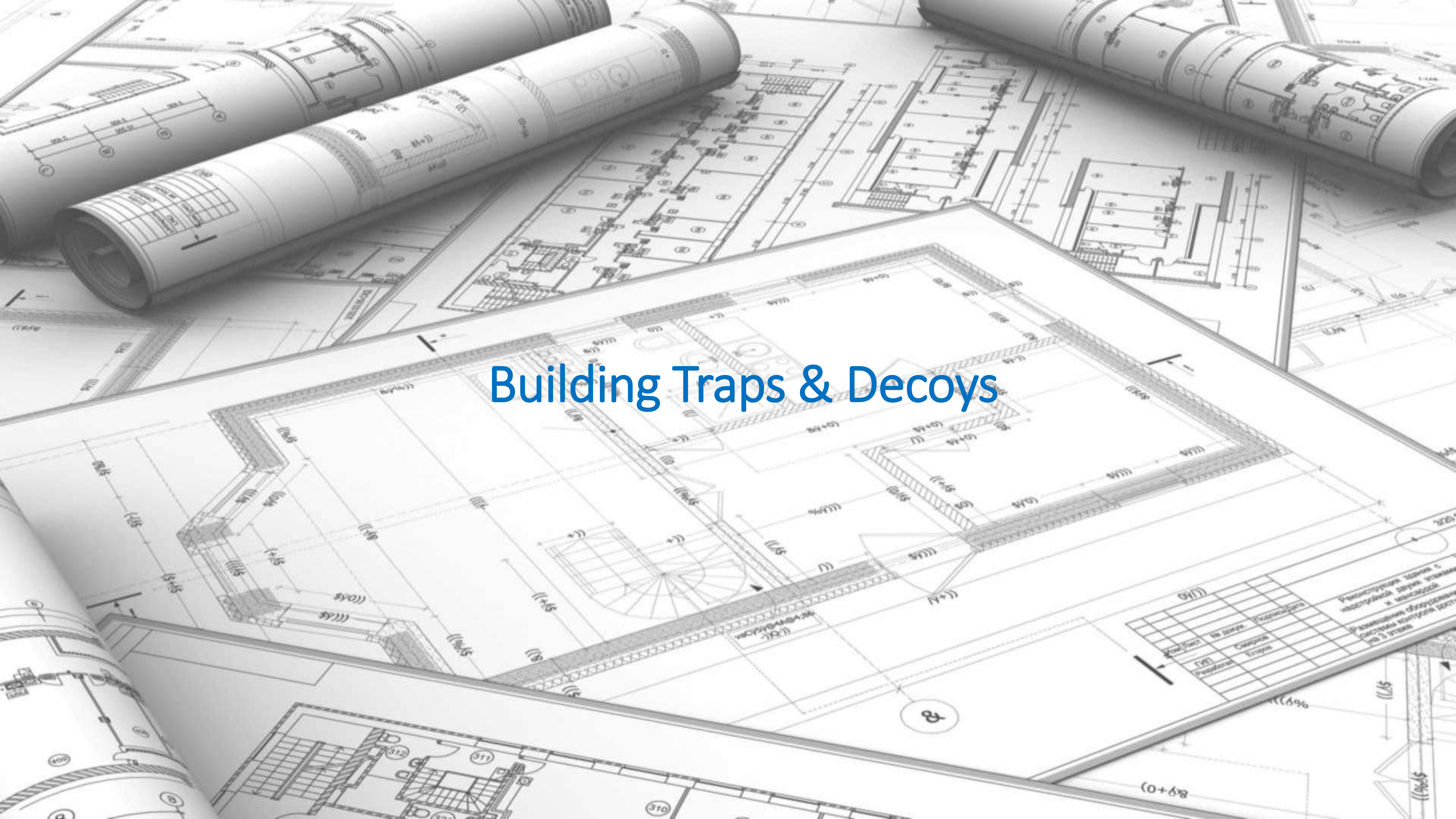
The Knowledge Gap = The difference between attacker’s perception and reality

The knowledge gap quickly decreases over time (but it always exists!)

A knowledgeable attacker = A sophisticated attack

Increase the Gap -> Increase Probability of Detection

Building Traps & Decoys



Decoys

Common Profiles

Servers
Workstations
Mobile devices
IOT (printers, router, cameras...)

Network entities designed to look like assets in the organization

Interactivity Level

Common Services

TCP
UDP
SMB
HTTP
ICMP
RDP
FTP
MYSQL
SMTP
SSH

Traps

Network

- Network Table Caches Poisoning (ARP, DNS, Netbios)
- Mounted Devices (Network Printers, Cameras)
- (half) Open Connection to decoys

File Based

- IT/Corporate Documents (txt, doc, xls pdf …)
- Canaries
- Emails (as file or inside PST)
- Logs
- Databases
- Recent files
- Host and lmHost files

Applications

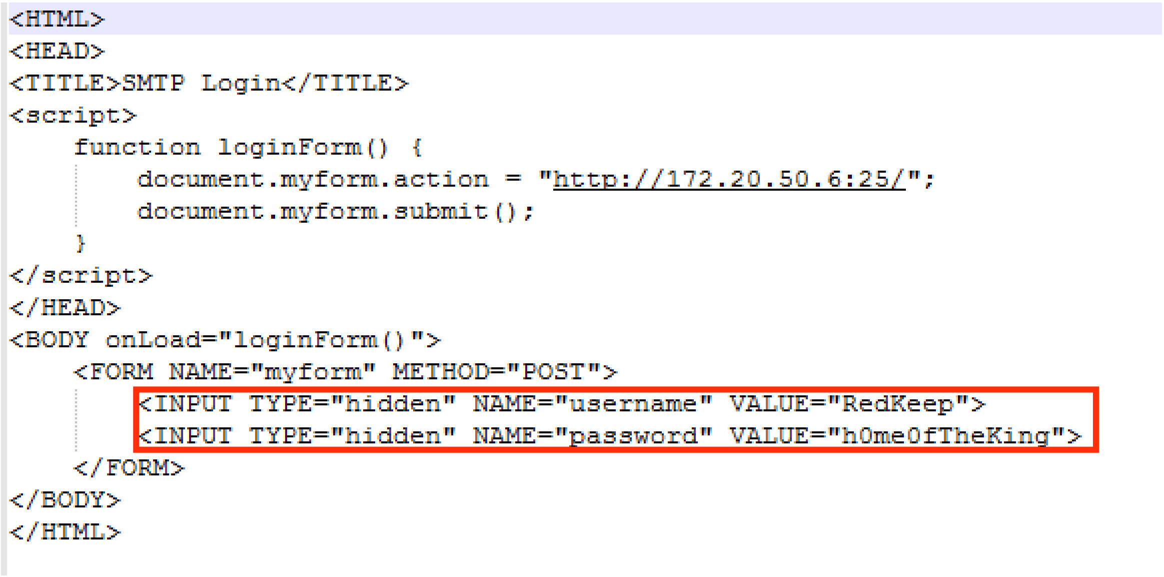
- Session Apps (SSH, FTP, RDP clients…)
- Browsers (History, Passwords, Bookmarks)
- App Uninstall information

Credentials

- Passwords and Hash injections
- Windows Credential Manager
- Password Managers

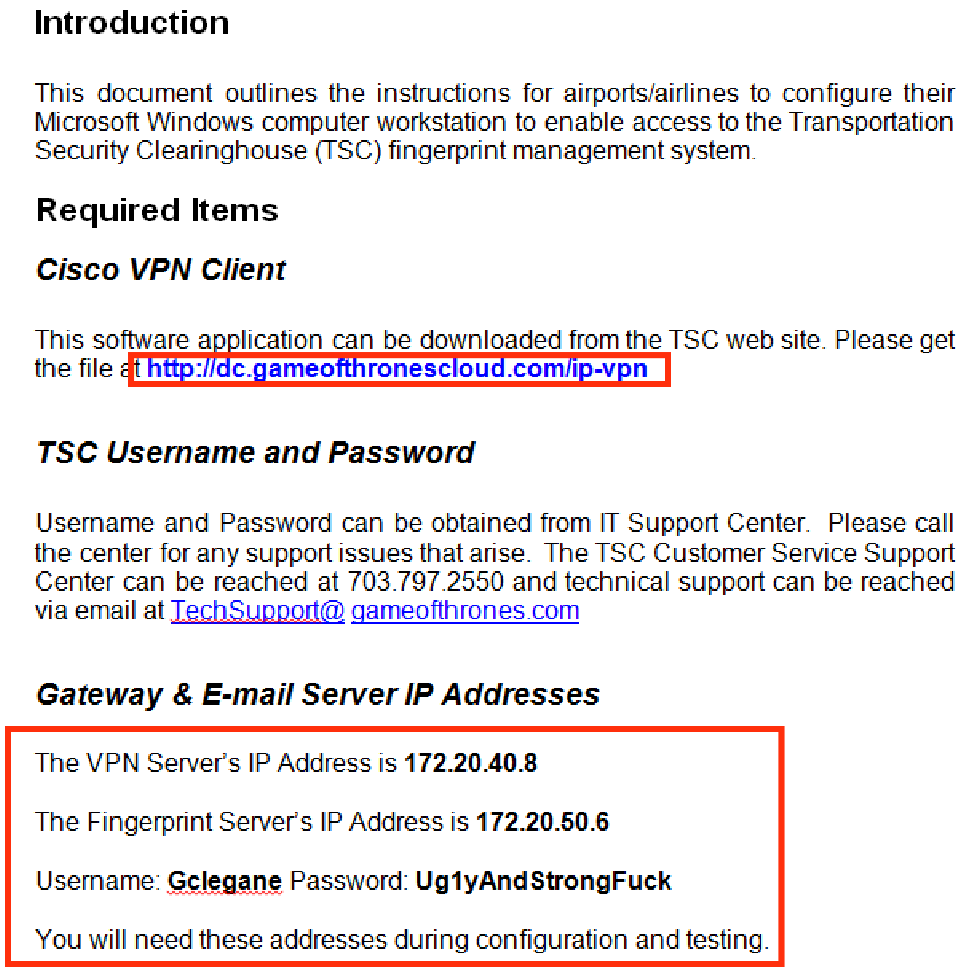
File Based traps

- Simplest trap, yet most versatile
- Understanding the organization is crucial



```
<HTML>
<HEAD>
<TITLE>SMTP Login</TITLE>
<script>
    function loginForm() {
        document.myform.action = "http://172.20.50.6:25/";
        document.myform.submit();
    }
</script>
</HEAD>
<BODY onLoad="loginForm()">
    <FORM NAME="myform" METHOD="POST">
        <INPUT TYPE="hidden" NAME="username" VALUE="RedKeep">
        <INPUT TYPE="hidden" NAME="password" VALUE="h0me0fTheKing">
    </FORM>
</BODY>
</HTML>
```

a configuration file



Introduction

This document outlines the instructions for airports/airlines to configure their Microsoft Windows computer workstation to enable access to the Transportation Security Clearinghouse (TSC) fingerprint management system.

Required Items

Cisco VPN Client

This software application can be downloaded from the TSC web site. Please get the file at **http://dc.gameofthronescloud.com/ip-vpn**

TSC Username and Password

Username and Password can be obtained from IT Support Center. Please call the center for any support issues that arise. The TSC Customer Service Support Center can be reached at 703.797.2550 and technical support can be reached via email at TechSupport@ gameofthrones.com

Gateway & E-mail Server IP Addresses

The VPN Server's IP Address is **172.20.40.8**

The Fingerprint Server's IP Address is **172.20.50.6**

Username: **Gclegane** Password: **Ug1yAndStrongFuck**

You will need these addresses during configuration and testing.

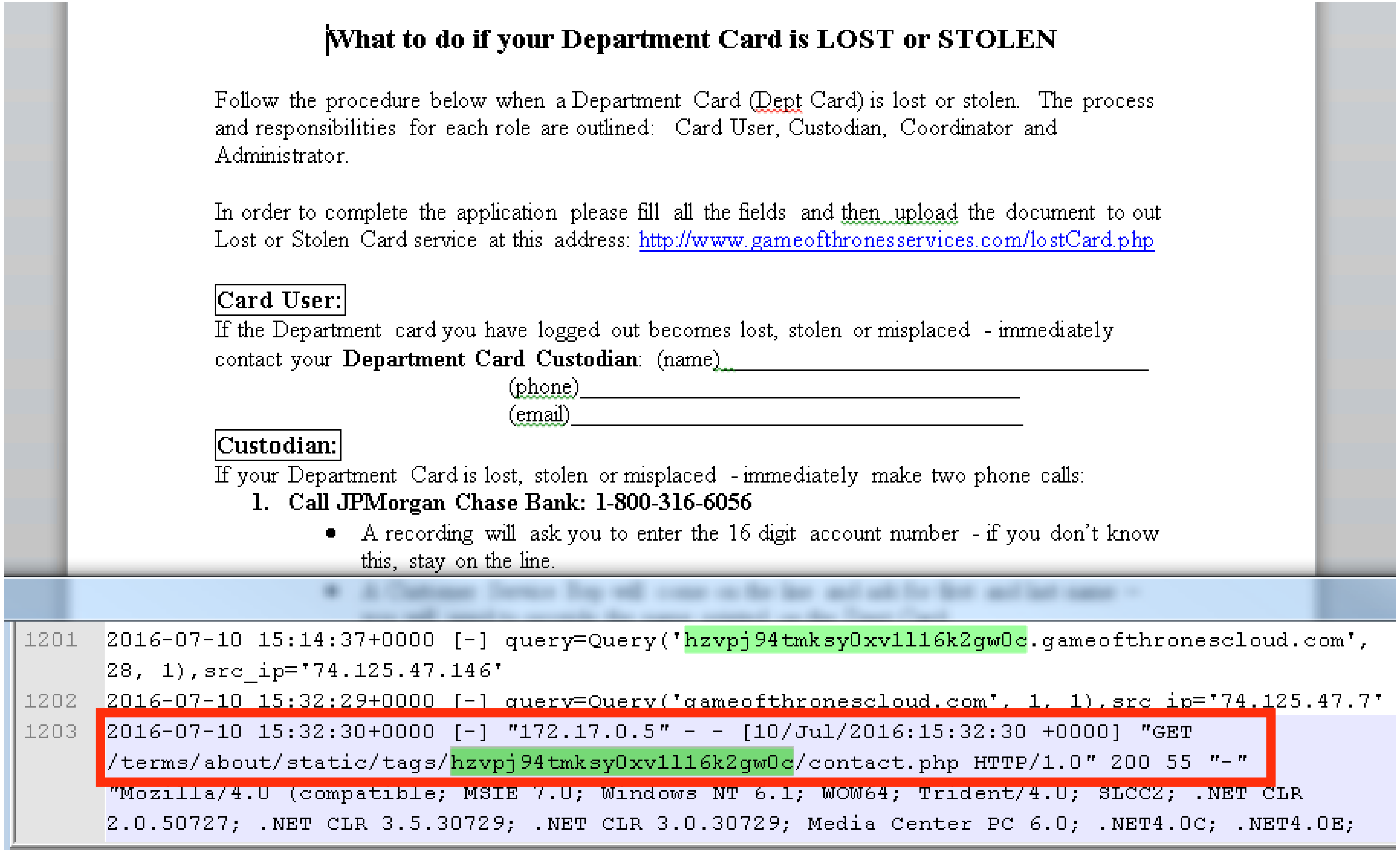
A guide on how to use the corporate a VPN

Who Opened my files?

- Open sourced by

thinkst
applied research

Canarytokens project



What to do if your Department Card is LOST or STOLEN

Follow the procedure below when a Department Card (Dept Card) is lost or stolen. The process and responsibilities for each role are outlined: Card User, Custodian, Coordinator and Administrator.

In order to complete the application please fill all the fields and then upload the document to out Lost or Stolen Card service at this address: http://www.gameofthronesservices.com/lostCard.php

Card User:

If the Department card you have logged out becomes lost, stolen or misplaced - immediately contact your **Department Card Custodian**: (name)_____________________________________

(phone)__________________________________

(email)___________________________________

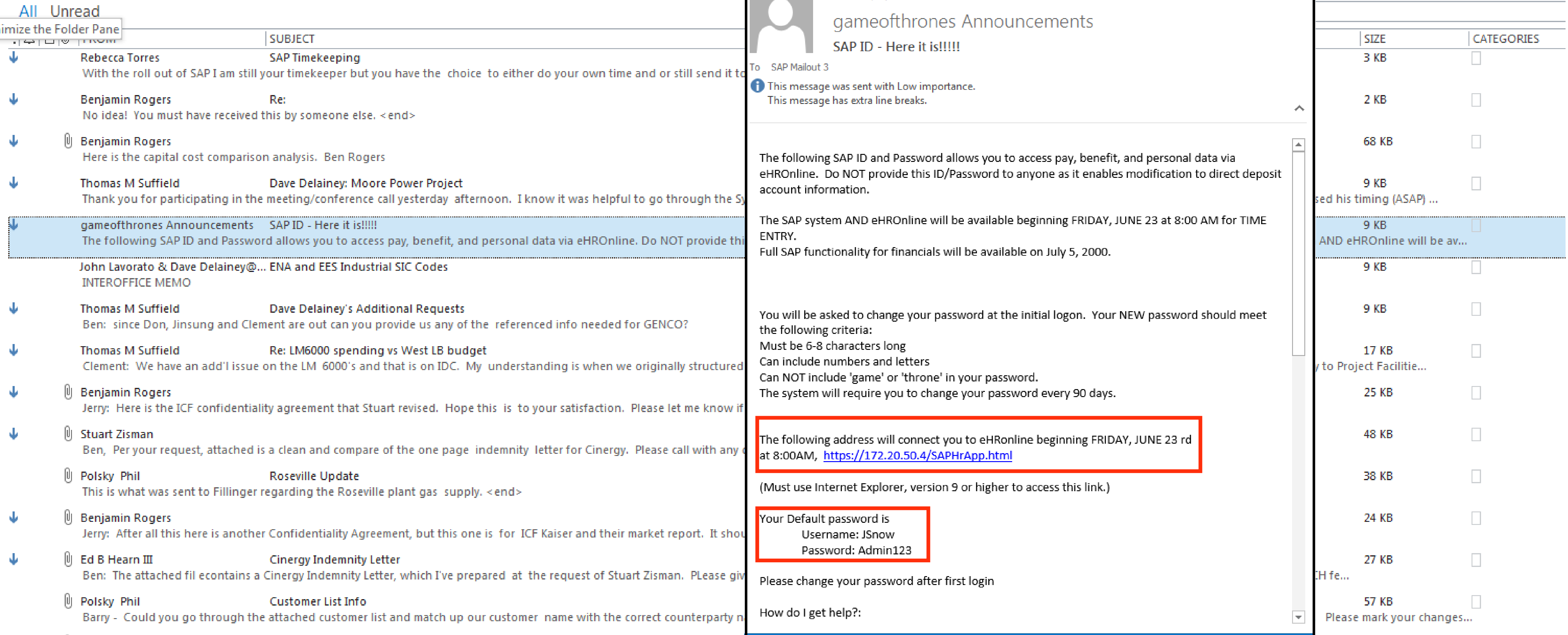
Custodian:

If your Department Card is lost, stolen or misplaced - immediately make two phone calls:

1. **Call JPMorgan Chase Bank: 1-800-316-6056**
   - A recording will ask you to enter the 16 digit account number - if you don't know this, stay on the line.

```
2016-07-10 15:14:37+0000 [-] query=Query('hzvpj94tmksy0xv1l16k2gw0c.gameofthronescloud.com',
28, 1),src_ip='74.125.47.146'
2016-07-10 15:32:29+0000 [-] query=Query('gameofthronescloud.com', 1, 1),src_ip='74.125.47.7'
2016-07-10 15:32:30+0000 [-] "172.17.0.5" - - [10/Jul/2016:15:32:30 +0000] "GET
/terms/about/static/tags/hzvpj94tmksy0xv1l16k2gw0c/contact.php HTTP/1.0" 200 55 "-"
"Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR
2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E;
```

Emails



FROM | SUBJECT | SIZE | CATEGORIES

Rebecca Torres — SAP Timekeeping — 3 KB
With the roll out of SAP I am still your timekeeper but you have the choice to either do your own time and or still send it to

Benjamin Rogers — Re: — 2 KB
No idea! You must have received this by someone else. <end>

Benjamin Rogers — 68 KB
Here is the capital cost comparison analysis. Ben Rogers

Thomas M Suffield — Dave Delainey: Moore Power Project — 9 KB
Thank you for participating in the meeting/conference call yesterday afternoon. I know it was helpful to go through the Sy ... sed his timing (ASAP) ...

gameofthrones Announcements — SAP ID - Here it is!!!!! — 9 KB
The following SAP ID and Password allows you to access pay, benefit, and personal data via eHROnline. Do NOT provide thi ... AND eHROnline will be av...

John Lavorato & Dave Delainey@... — ENA and EES Industrial SIC Codes — 9 KB
INTEROFFICE MEMO

Thomas M Suffield — Dave Delainey's Additional Requests — 9 KB
Ben: since Don, Jinsung and Clement are out can you provide us any of the referenced info needed for GENCO?

Thomas M Suffield — Re: LM6000 spending vs West LB budget — 17 KB
Clement: We have an add'l issue on the LM 6000's and that is on IDC. My understanding is when we originally structured ... y to Project Facilitie...

Benjamin Rogers — 25 KB
Jerry: Here is the ICF confidentiality agreement that Stuart revised. Hope this is to your satisfaction. Please let me know if

Stuart Zisman — 48 KB
Ben, Per your request, attached is a clean and compare of the one page indemnity letter for Cinergy. Please call with any

Polsky Phil — Roseville Update — 38 KB
This is what was sent to Fillinger regarding the Roseville plant gas supply. <end>

Benjamin Rogers — 24 KB
Jerry: After all this here is another Confidentiality Agreement, but this one is for ICF Kaiser and their market report. It shou

Ed B Hearn III — Cinergy Indemnity Letter — 27 KB
Ben: The attached fil econtains a Cinergy Indemnity Letter, which I've prepared at the request of Stuart Zisman. PLease giv ... CH fe...

Polsky Phil — Customer List Info — 57 KB
Barry - Could you go through the attached customer list and match up our customer name with the correct counterparty n ... Please mark your changes...

Jinsung Myung — Model for Cinergy — 995 KB
I changed Heat rates for Caledonia and Gleason, and Start Charge for Gleason. Heat rates has no impact on numbers. Only ... we can stay with previo...

Clement Lau — Info Memo, Pictures, Maps — 3 KB
I have saved the first info memo (generic version, w/o mentioned of Orion) under "EGC12-Generic-051100" and various site

SAP ID - Here it is!!!!! - Message (Plain Text)

04:40 23/06/2015 ג' יום

gameofthrones Announcements

SAP ID - Here it is!!!!!

To SAP Mailout 3

This message was sent with Low importance.
This message has extra line breaks.

The following SAP ID and Password allows you to access pay, benefit, and personal data via eHROnline. Do NOT provide this ID/Password to anyone as it enables modification to direct deposit account information.

The SAP system AND eHROnline will be available beginning FRIDAY, JUNE 23 at 8:00 AM for TIME ENTRY.
Full SAP functionality for financials will be available on July 5, 2000.

You will be asked to change your password at the initial logon. Your NEW password should meet the following criteria:
Must be 6-8 characters long
Can include numbers and letters
Can NOT include 'game' or 'throne' in your password.
The system will require you to change your password every 90 days.

The following address will connect you to eHRonline beginning FRIDAY, JUNE 23 rd at 8:00AM, https://172.20.50.4/SAPHrApp.html

(Must use Internet Explorer, version 9 or higher to access this link.)

Your Default password is
Username: JSnow
Password: Admin123

Please change your password after first login

How do I get help?:

Most triggered Trap!
Triggered by 27% of Contestants

Email

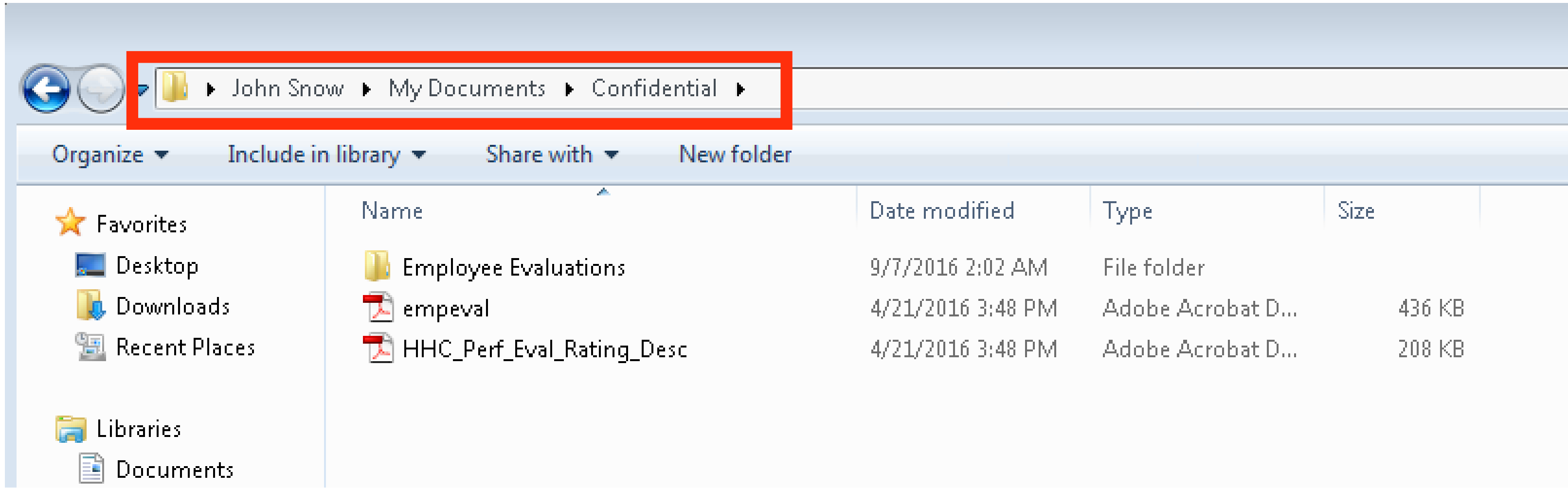
Email

WHEN YOU CONTROL THE MAIL YOU CONTROL
INFORMATION
5A
quickmeme.com

Wait…

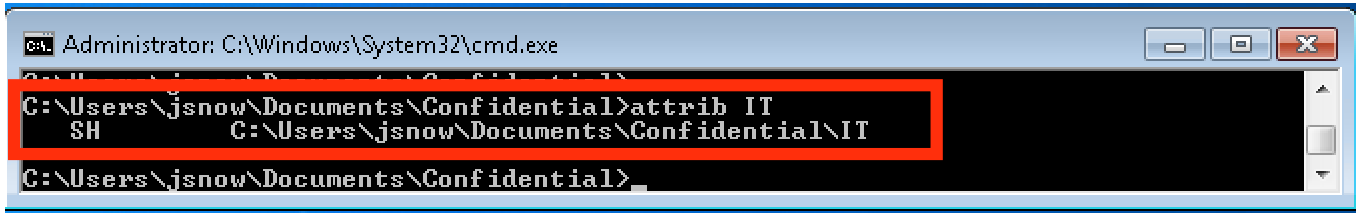
Can our users get in the way?

Permissions and System



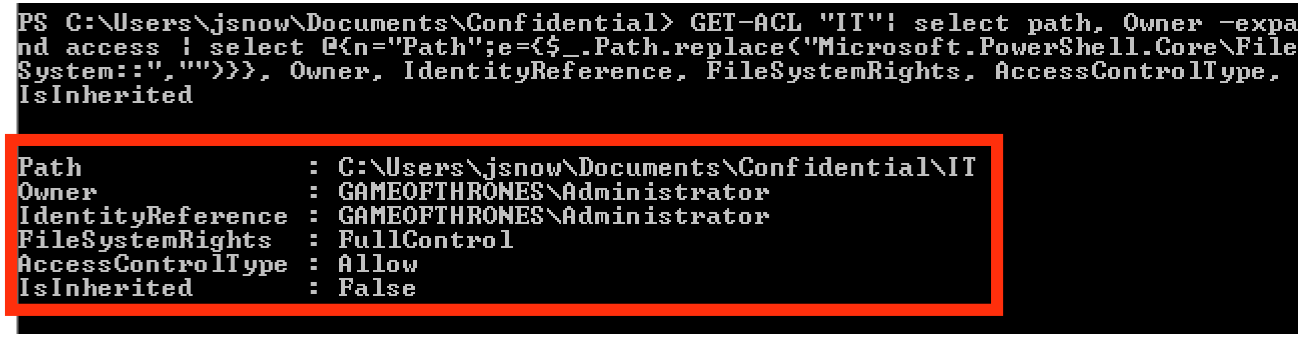
Name	Date modified	Type	Size
Employee Evaluations	9/7/2016 2:02 AM	File folder	
empeval	4/21/2016 3:48 PM	Adobe Acrobat D...	436 KB
HHC_Perf_Eval_Rating_Desc	4/21/2016 3:48 PM	Adobe Acrobat D...	208 KB

- Hidden + System directory
- Locked to Domain Admin User
- Files Inside are unique traps
- Access to folder monitored by a canary.



```
C:\Users\jsnow\Documents\Confidential>
C:\Users\jsnow\Documents\Confidential>attrib IT
   SH          C:\Users\jsnow\Documents\Confidential\IT

C:\Users\jsnow\Documents\Confidential>_
```



```
PS C:\Users\jsnow\Documents\Confidential> GET-ACL "IT"| select path, Owner -expa
nd access | select @{n="Path";e={$_.Path.replace("Microsoft.PowerShell.Core\File
System::","")}}, Owner, IdentityReference, FileSystemRights, AccessControlType,
IsInherited

Path                  : C:\Users\jsnow\Documents\Confidential\IT
Owner                 : GAMEOFTHRONES\Administrator
IdentityReference     : GAMEOFTHRONES\Administrator
FileSystemRights      : FullControl
AccessControlType     : Allow
IsInherited           : False
```

Traps

Network

- Network Table Caches Poisoning (ARP, DNS, Netbios)
- Mounted Devices (Network Printers, Cameras)
- (half) Open Connection to decoys

Applications

- Session Apps (SSH, FTP, RDP clients…)
- Browsers (History, Passwords, Bookmarks)
- App Uninstall information

File Based

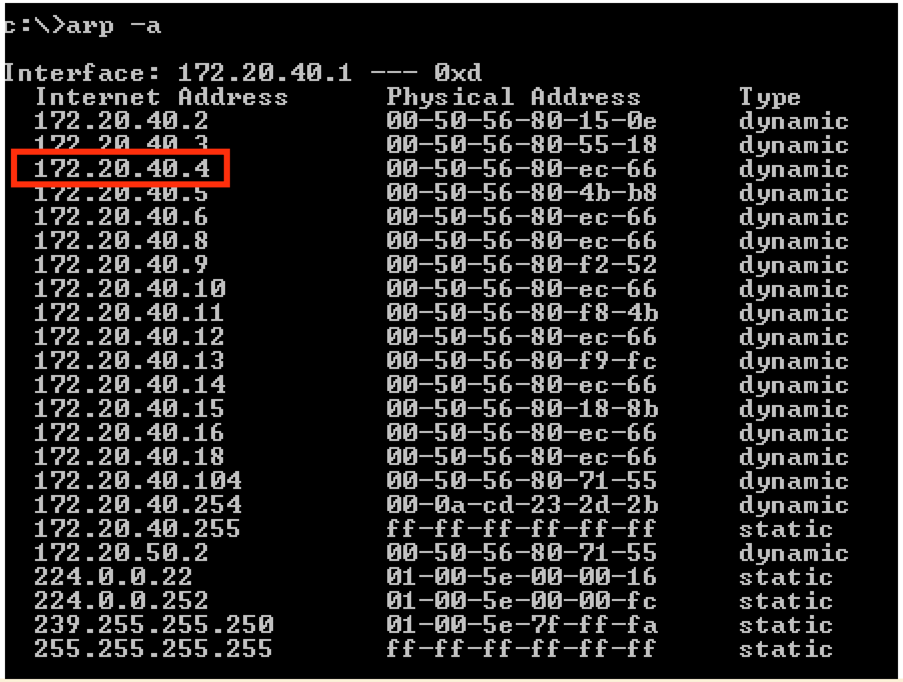
- IT/Corporate Documents (txt, doc, xls pdf …)
- Canaries
- Emails (as file or inside PST)
- Logs
- Databases
- Recent files
- Host and lmHost files

Credentials

- Passwords and Hash injections
- Windows Credential Manager
- Password Managers

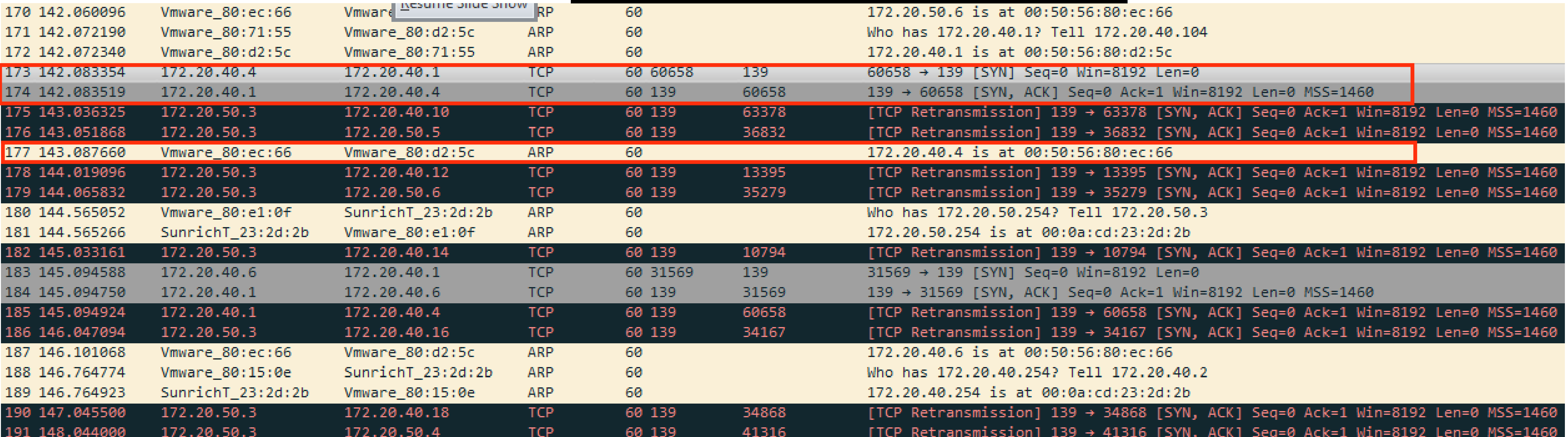
Arp Cache

- Static entries :-(
- Syn Spoofing :-)



```
c:\>arp -a

Interface: 172.20.40.1 --- 0xd
  Internet Address      Physical Address      Type
  172.20.40.2           00-50-56-80-15-0e     dynamic
  172.20.40.3           00-50-56-80-55-18     dynamic
  172.20.40.4           00-50-56-80-ec-66     dynamic
  172.20.40.5           00-50-56-80-4b-b8     dynamic
  172.20.40.6           00-50-56-80-ec-66     dynamic
  172.20.40.8           00-50-56-80-ec-66     dynamic
  172.20.40.9           00-50-56-80-f2-52     dynamic
  172.20.40.10          00-50-56-80-ec-66     dynamic
  172.20.40.11          00-50-56-80-f8-4b     dynamic
  172.20.40.12          00-50-56-80-ec-66     dynamic
  172.20.40.13          00-50-56-80-f9-fc     dynamic
  172.20.40.14          00-50-56-80-ec-66     dynamic
  172.20.40.15          00-50-56-80-18-8b     dynamic
  172.20.40.16          00-50-56-80-ec-66     dynamic
  172.20.40.18          00-50-56-80-ec-66     dynamic
  172.20.40.104         00-50-56-80-71-55     dynamic
  172.20.40.254         00-0a-cd-23-2d-2b     dynamic
  172.20.40.255         ff-ff-ff-ff-ff-ff     static
  172.20.50.2           00-50-56-80-71-55     dynamic
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```



```
170 142.060096   Vmware_80:ec:66    Vmware             RP    60                        172.20.50.6 is at 00:50:56:80:ec:66
171 142.072190   Vmware_80:71:55    Vmware_80:d2:5c    ARP   60                        Who has 172.20.40.1? Tell 172.20.40.104
172 142.072340   Vmware_80:d2:5c    Vmware_80:71:55    ARP   60                        172.20.40.1 is at 00:50:56:80:d2:5c
173 142.083354   172.20.40.4        172.20.40.1        TCP   60 60658      139         60658 → 139 [SYN] Seq=0 Win=8192 Len=0
174 142.083519   172.20.40.1        172.20.40.4        TCP   60 139        60658       139 → 60658 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
175 143.036325   172.20.50.3        172.20.40.10       TCP   60 139        63378       [TCP Retransmission] 139 → 63378 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
176 143.051868   172.20.50.3        172.20.50.5        TCP   60 139        36832       [TCP Retransmission] 139 → 36832 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
177 143.087660   Vmware_80:ec:66    Vmware_80:d2:5c    ARP   60                        172.20.40.4 is at 00:50:56:80:ec:66
178 144.019096   172.20.50.3        172.20.40.12       TCP   60 139        13395       [TCP Retransmission] 139 → 13395 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
179 144.065832   172.20.50.3        172.20.50.6        TCP   60 139        35279       [TCP Retransmission] 139 → 35279 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
180 144.565052   Vmware_80:e1:0f    SunrichT_23:2d:2b  ARP   60                        Who has 172.20.50.254? Tell 172.20.50.3
181 144.565266   SunrichT_23:2d:2b  Vmware_80:e1:0f    ARP   60                        172.20.50.254 is at 00:0a:cd:23:2d:2b
182 145.033161   172.20.50.3        172.20.40.14       TCP   60 139        10794       [TCP Retransmission] 139 → 10794 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
183 145.094588   172.20.40.6        172.20.40.1        TCP   60 31569      139         31569 → 139 [SYN] Seq=0 Win=8192 Len=0
184 145.094750   172.20.40.1        172.20.40.6        TCP   60 139        31569       139 → 31569 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
185 145.094924   172.20.40.1        172.20.40.4        TCP   60 139        60658       [TCP Retransmission] 139 → 60658 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
186 146.047094   172.20.50.3        172.20.40.16       TCP   60 139        34167       [TCP Retransmission] 139 → 34167 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
187 146.101068   Vmware_80:ec:66    Vmware_80:d2:5c    ARP   60                        172.20.40.6 is at 00:50:56:80:ec:66
188 146.764774   Vmware_80:15:0e    SunrichT_23:2d:2b  ARP   60                        Who has 172.20.40.254? Tell 172.20.40.2
189 146.764923   SunrichT_23:2d:2b  Vmware_80:15:0e    ARP   60                        172.20.40.254 is at 00:0a:cd:23:2d:2b
190 147.045500   172.20.50.3        172.20.40.18       TCP   60 139        34868       [TCP Retransmission] 139 → 34868 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
191 148.044000   172.20.50.3        172.20.50.4        TCP   60 139        41316       [TCP Retransmission] 139 → 41316 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
```

Traps

Network

- Network Table Caches Poisoning (ARP, DNS, Netbios)
- Mounted Devices (Network Printers, Cameras)
- (half) Open Connection to decoys

Applications

- Session Apps (SSH, FTP, RDP clients…)
- Browsers (History, Passwords, Bookmarks)
- App Uninstall information

File Based

- IT/Corporate Documents (txt, doc, xls pdf …)
- Canaries
- Emails (as file or inside PST)
- Logs
- Databases
- Recent files
- Host and lmHost files

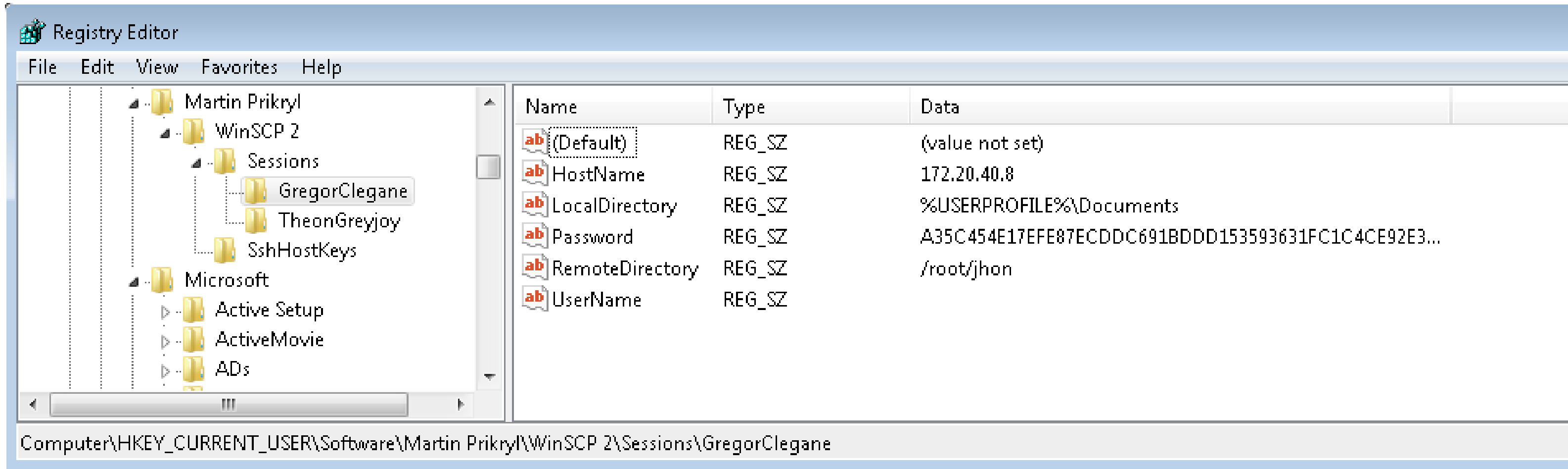
Credentials

- Passwords and Hash injections
- Windows Credential Manager
- Password Managers

Common Applications

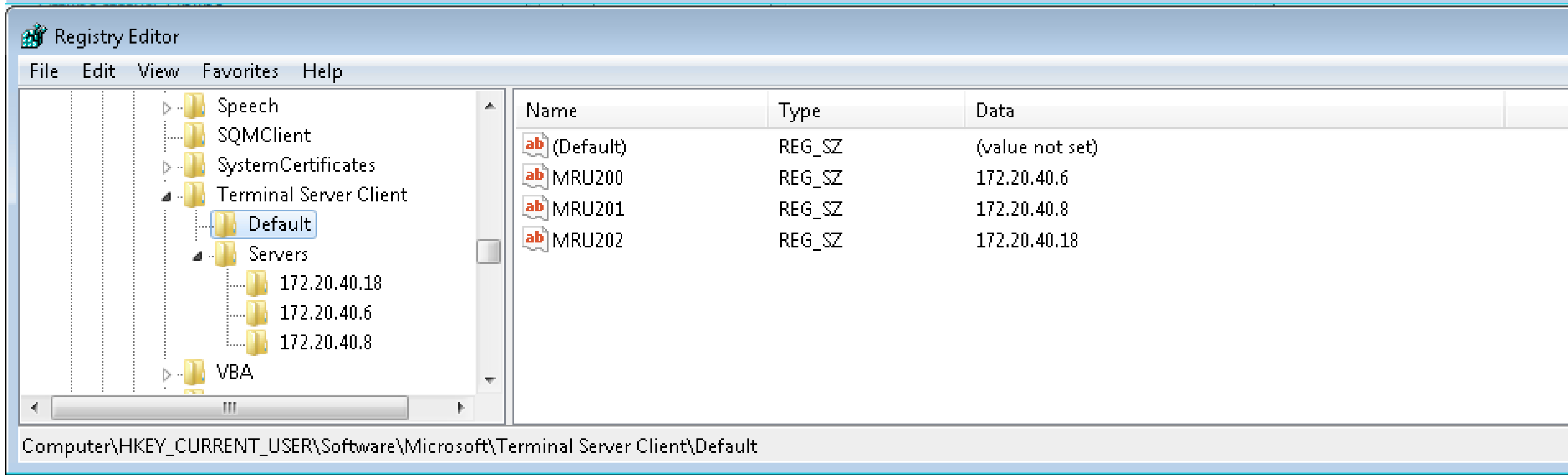
- Any Application that contains credentials, locations or useful info
- Can be file or registry
- Installed or not…

- How to create?



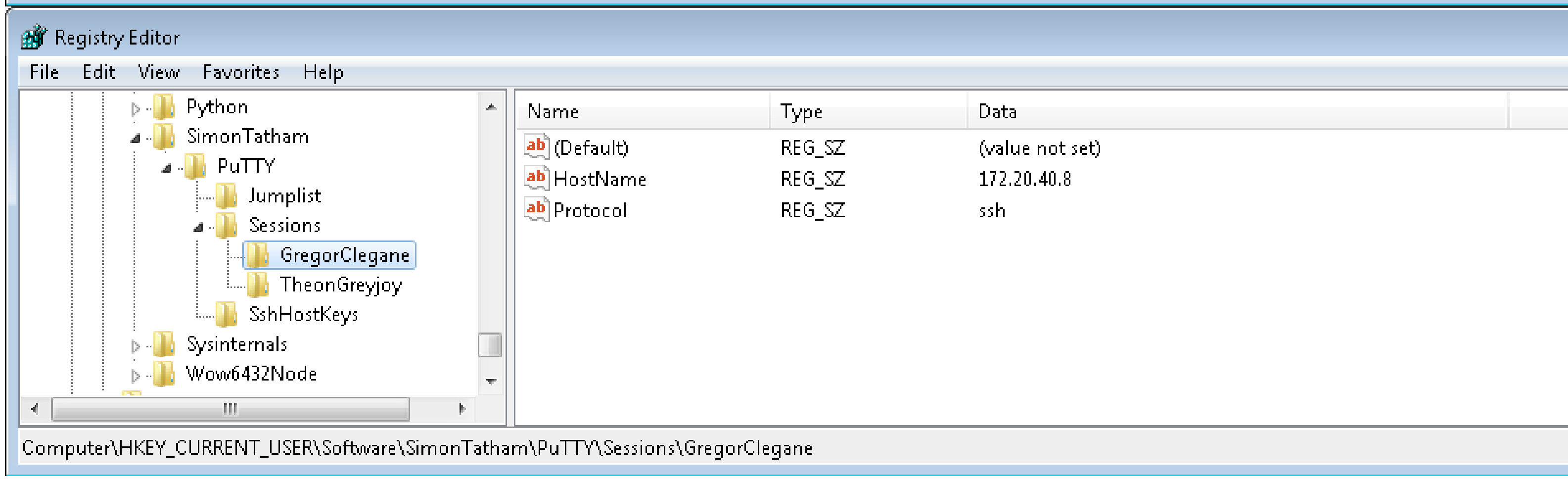
Name	Type	Data
(Default)	REG_SZ	(value not set)
HostName	REG_SZ	172.20.40.8
LocalDirectory	REG_SZ	%USERPROFILE%\Documents
Password	REG_SZ	A35C454E17EFE87ECDDC691BDDD153593631FC1C4CE92E3...
RemoteDirectory	REG_SZ	/root/jhon
UserName	REG_SZ	

Computer\HKEY_CURRENT_USER\Software\Martin Prikryl\WinSCP 2\Sessions\GregorClegane



Name	Type	Data
(Default)	REG_SZ	(value not set)
MRU200	REG_SZ	172.20.40.6
MRU201	REG_SZ	172.20.40.8
MRU202	REG_SZ	172.20.40.18

Computer\HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default

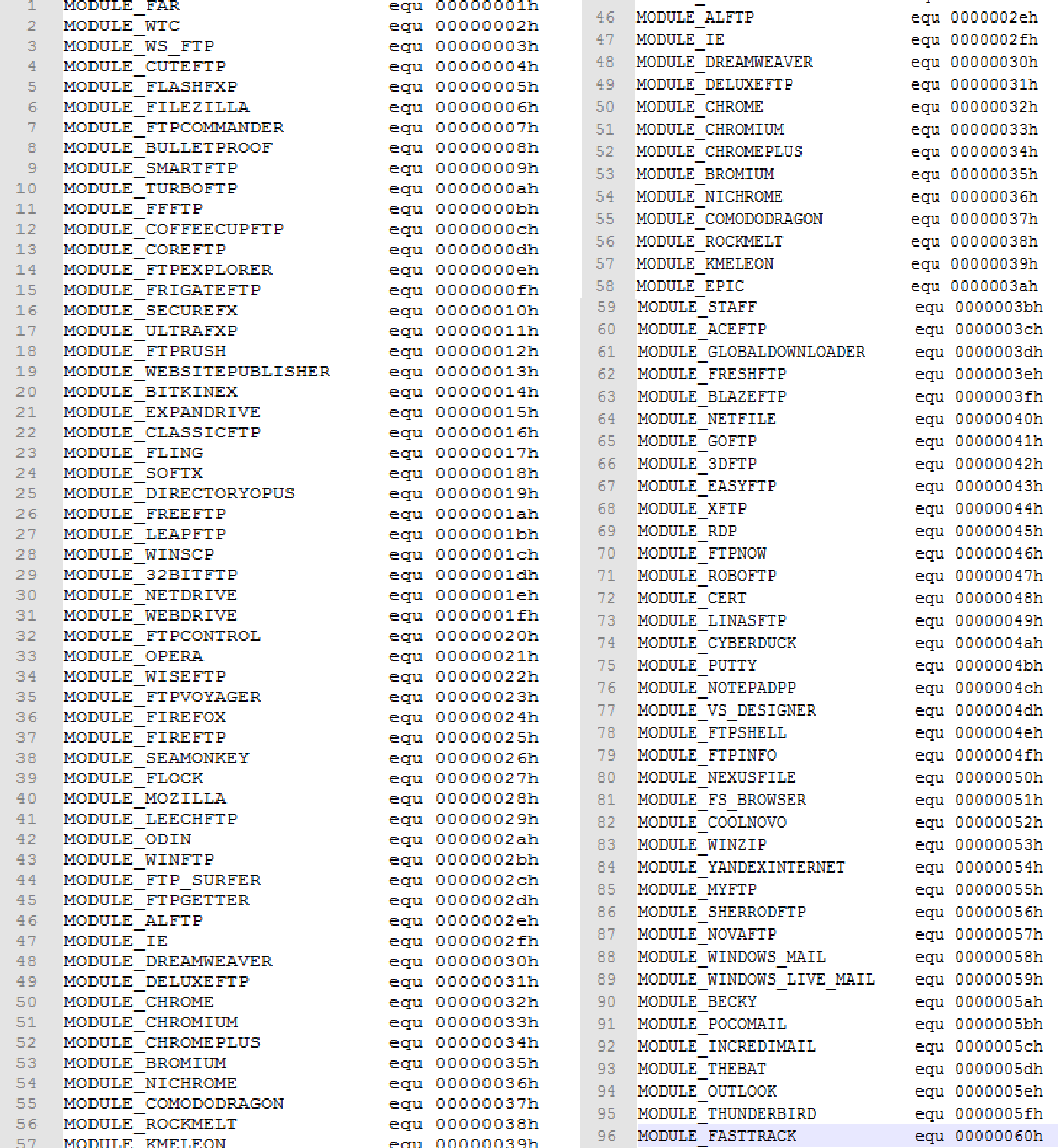


Name	Type	Data
(Default)	REG_SZ	(value not set)
HostName	REG_SZ	172.20.40.8
Protocol	REG_SZ	ssh

Computer\HKEY_CURRENT_USER\Software\SimonTatham\PuTTY\Sessions\GregorClegane

Common Applications

- Leaked malware source are your friend
- 200+ potential applications…



```
MODULE_FAR                  equ 00000001h
MODULE_WTC                  equ 00000002h
MODULE_WS_FTP               equ 00000003h
MODULE_CUTEFTP              equ 00000004h
MODULE_FLASHFXP             equ 00000005h
MODULE_FILEZILLA            equ 00000006h
MODULE_FTPCOMMANDER         equ 00000007h
MODULE_BULLETPROOF          equ 00000008h
MODULE_SMARTFTP             equ 00000009h
MODULE_TURBOFTP             equ 0000000ah
MODULE_FFFTP                equ 0000000bh
MODULE_COFFEECUPFTP         equ 0000000ch
MODULE_COREFTP              equ 0000000dh
MODULE_FTPEXPLORER          equ 0000000eh
MODULE_FRIGATEFTP           equ 0000000fh
MODULE_SECUREFX             equ 00000010h
MODULE_ULTRAFXP             equ 00000011h
MODULE_FTPRUSH              equ 00000012h
MODULE_WEBSITEPUBLISHER     equ 00000013h
MODULE_BITKINEX             equ 00000014h
MODULE_EXPANDRIVE           equ 00000015h
MODULE_CLASSICFTP           equ 00000016h
MODULE_FLING                equ 00000017h
MODULE_SOFTX                equ 00000018h
MODULE_DIRECTORYOPUS        equ 00000019h
MODULE_FREEFTP              equ 0000001ah
MODULE_LEAPFTP              equ 0000001bh
MODULE_WINSCP               equ 0000001ch
MODULE_32BITFTP             equ 0000001dh
MODULE_NETDRIVE             equ 0000001eh
MODULE_WEBDRIVE             equ 0000001fh
MODULE_FTPCONTROL           equ 00000020h
MODULE_OPERA                equ 00000021h
MODULE_WISEFTP              equ 00000022h
MODULE_FTPVOYAGER           equ 00000023h
MODULE_FIREFOX              equ 00000024h
MODULE_FIREFTP              equ 00000025h
MODULE_SEAMONKEY            equ 00000026h
MODULE_FLOCK                equ 00000027h
MODULE_MOZILLA              equ 00000028h
MODULE_LEECHFTP             equ 00000029h
MODULE_ODIN                 equ 0000002ah
MODULE_WINFTP               equ 0000002bh
MODULE_FTP_SURFER           equ 0000002ch
MODULE_FTPGETTER            equ 0000002dh
MODULE_ALFTP                equ 0000002eh
MODULE_IE                   equ 0000002fh
MODULE_DREAMWEAVER          equ 00000030h
MODULE_DELUXEFTP            equ 00000031h
MODULE_CHROME               equ 00000032h
MODULE_CHROMIUM             equ 00000033h
MODULE_CHROMEPLUS           equ 00000034h
MODULE_BROMIUM              equ 00000035h
MODULE_NICHROME             equ 00000036h
MODULE_COMODODRAGON         equ 00000037h
MODULE_ROCKMELT             equ 00000038h
MODULE_KMELEON              equ 00000039h
```

```
MODULE_ALFTP                equ 0000002eh
MODULE_IE                   equ 0000002fh
MODULE_DREAMWEAVER          equ 00000030h
MODULE_DELUXEFTP            equ 00000031h
MODULE_CHROME               equ 00000032h
MODULE_CHROMIUM             equ 00000033h
MODULE_CHROMEPLUS           equ 00000034h
MODULE_BROMIUM              equ 00000035h
MODULE_NICHROME             equ 00000036h
MODULE_COMODODRAGON         equ 00000037h
MODULE_ROCKMELT             equ 00000038h
MODULE_KMELEON              equ 00000039h
```

```
MODULE_EPIC                 equ 0000003ah
MODULE_STAFF                equ 0000003bh
MODULE_ACEFTP               equ 0000003ch
MODULE_GLOBALDOWNLOADER     equ 0000003dh
MODULE_FRESHFTP             equ 0000003eh
MODULE_BLAZEFTP             equ 0000003fh
MODULE_NETFILE              equ 00000040h
MODULE_GOFTP                equ 00000041h
MODULE_3DFTP                equ 00000042h
MODULE_EASYFTP              equ 00000043h
MODULE_XFTP                 equ 00000044h
MODULE_RDP                  equ 00000045h
MODULE_FTPNOW               equ 00000046h
MODULE_ROBOFTP              equ 00000047h
MODULE_CERT                 equ 00000048h
MODULE_LINASFTP             equ 00000049h
MODULE_CYBERDUCK            equ 0000004ah
MODULE_PUTTY                equ 0000004bh
MODULE_NOTEPADPP            equ 0000004ch
MODULE_VS_DESIGNER          equ 0000004dh
MODULE_FTPSHELL             equ 0000004eh
MODULE_FTPINFO              equ 0000004fh
MODULE_NEXUSFILE            equ 00000050h
MODULE_FS_BROWSER           equ 00000051h
MODULE_COOLNOVO             equ 00000052h
MODULE_WINZIP               equ 00000053h
MODULE_YANDEXINTERNET       equ 00000054h
MODULE_MYFTP                equ 00000055h
MODULE_SHERRODFTP           equ 00000056h
MODULE_NOVAFTP              equ 00000057h
MODULE_WINDOWS_MAIL         equ 00000058h
MODULE_WINDOWS_LIVE_MAIL    equ 00000059h
MODULE_BECKY                equ 0000005ah
MODULE_POCOMAIL             equ 0000005bh
MODULE_INCREDIMAIL          equ 0000005ch
MODULE_THEBAT               equ 0000005dh
MODULE_OUTLOOK              equ 0000005eh
MODULE_THUNDERBIRD          equ 0000005fh
MODULE_FASTTRACK            equ 00000060h
```

Traps

Network

- Network Table Caches Poisoning (ARP, DNS, Netbios)
- Mounted Devices (Network Printers, Cameras)
- (half) Open Connection to decoys

File Based

- IT/Corporate Documents (txt, doc, xls pdf …)
- Canaries
- Emails (as file or inside PST)
- Logs
- Databases
- Recent files
- Host and lmHost files

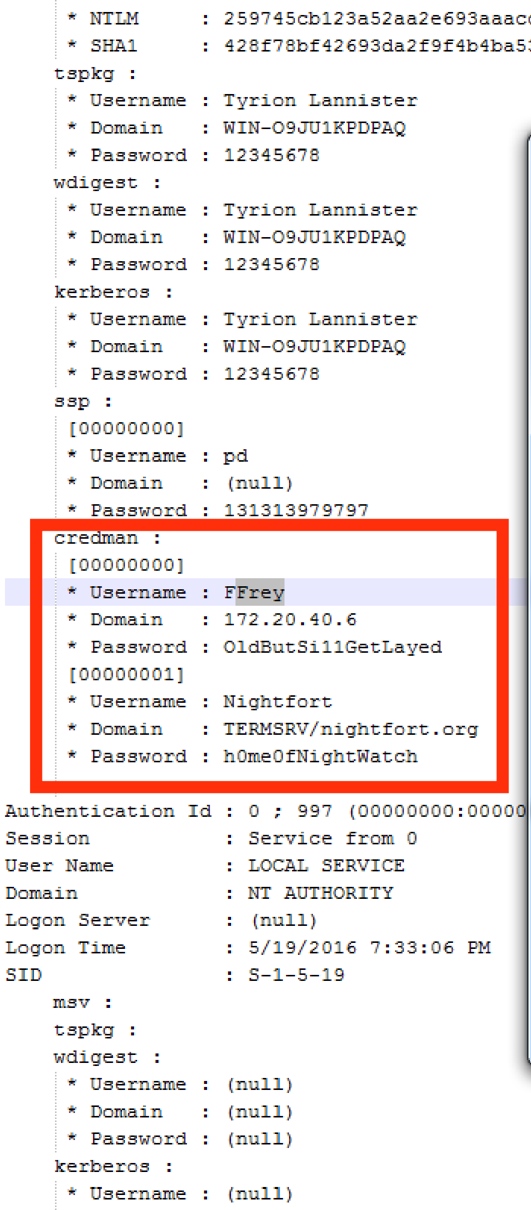
Applications

- Session Apps (SSH, FTP, RDP clients…)
- Browsers (History, Passwords, Bookmarks)
- App Uninstall information

Credentials

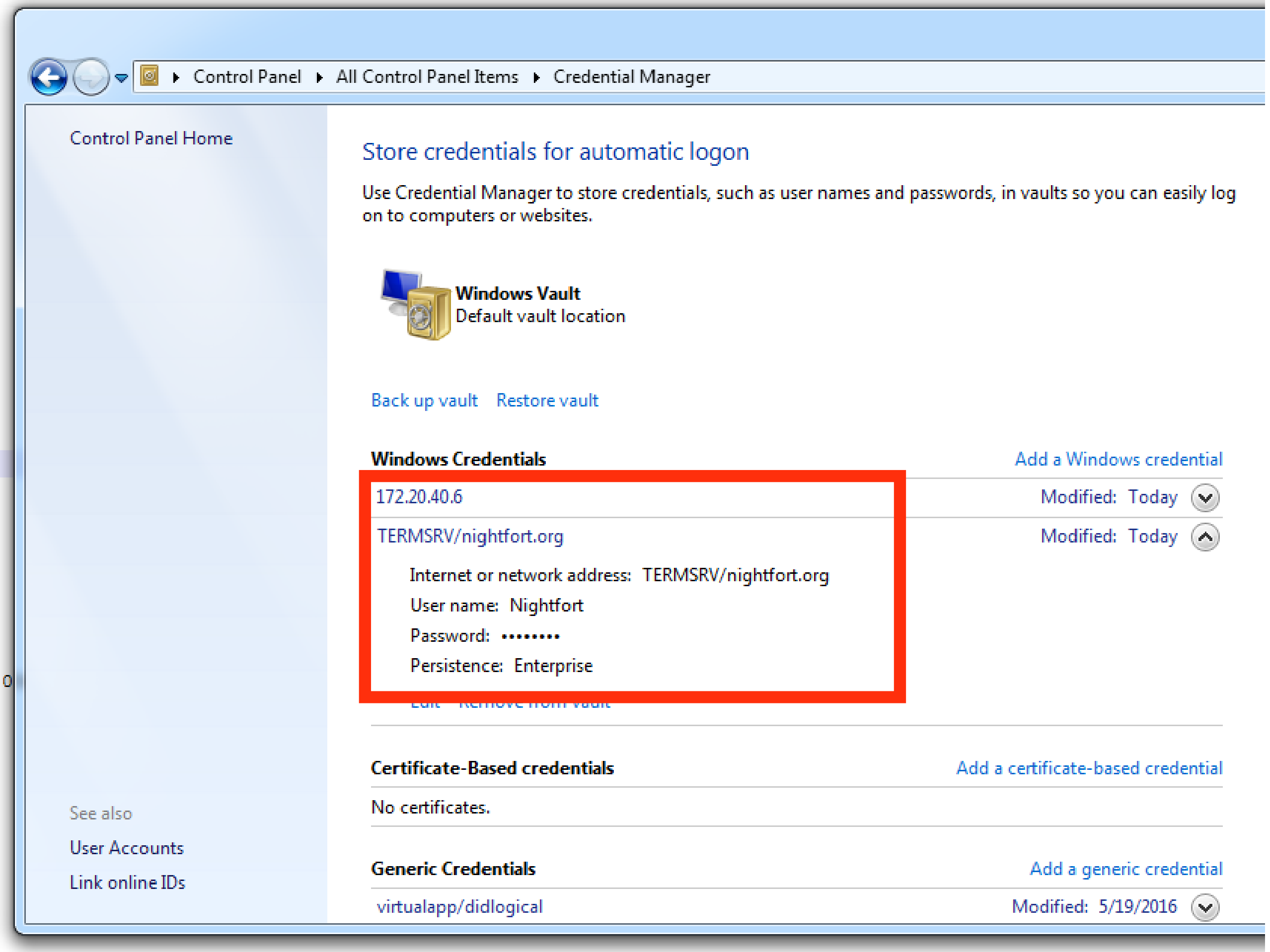
- Passwords and Hash injections
- Windows Credential Manager
- Password Managers

Windows Credential Manager



```
     * NTLM     : 259745cb123a52aa2e693aaacca2db52
     * SHA1     : 428f78bf42693da2f9f4b4ba537c5f101e275607
    tspkg :
     * Username : Tyrion Lannister
     * Domain   : WIN-O9JU1KPDPAQ
     * Password : 12345678
    wdigest :
     * Username : Tyrion Lannister
     * Domain   : WIN-O9JU1KPDPAQ
     * Password : 12345678
    kerberos :
     * Username : Tyrion Lannister
     * Domain   : WIN-O9JU1KPDPAQ
     * Password : 12345678
    ssp :
     [00000000]
     * Username : pd
     * Domain   : (null)
     * Password : 131313979797
    credman :
     [00000000]
     * Username : FFrey
     * Domain   : 172.20.40.6
     * Password : OldButSi11GetLayed
     [00000001]
     * Username : Nightfort
     * Domain   : TERMSRV/nightfort.org
     * Password : h0me0fNightWatch

Authentication Id : 0 ; 997 (00000000:00000
Session           : Service from 0
User Name         : LOCAL SERVICE
Domain            : NT AUTHORITY
Logon Server      : (null)
Logon Time        : 5/19/2016 7:33:06 PM
SID               : S-1-5-19
    msv :
    tspkg :
    wdigest :
     * Username : (null)
     * Domain   : (null)
     * Password : (null)
    kerberos :
     * Username : (null)
```



Control Panel ▸ All Control Panel Items ▸ Credential Manager
Control Panel Home
See also
User Accounts
Link online IDs

Store credentials for automatic logon

Use Credential Manager to store credentials, such as user names and passwords, in vaults so you can easily log on to computers or websites.

Windows Vault
Default vault location

Back up vault   Restore vault

Windows Credentials   Add a Windows credential

172.20.40.6   Modified: Today

TERMSRV/nightfort.org   Modified: Today

Internet or network address: TERMSRV/nightfort.org
User name: Nightfort
Password: ••••••••
Persistence: Enterprise

Edit   Remove from vault

Certificate-Based credentials   Add a certificate-based credential

No certificates.

Generic Credentials   Add a generic credential

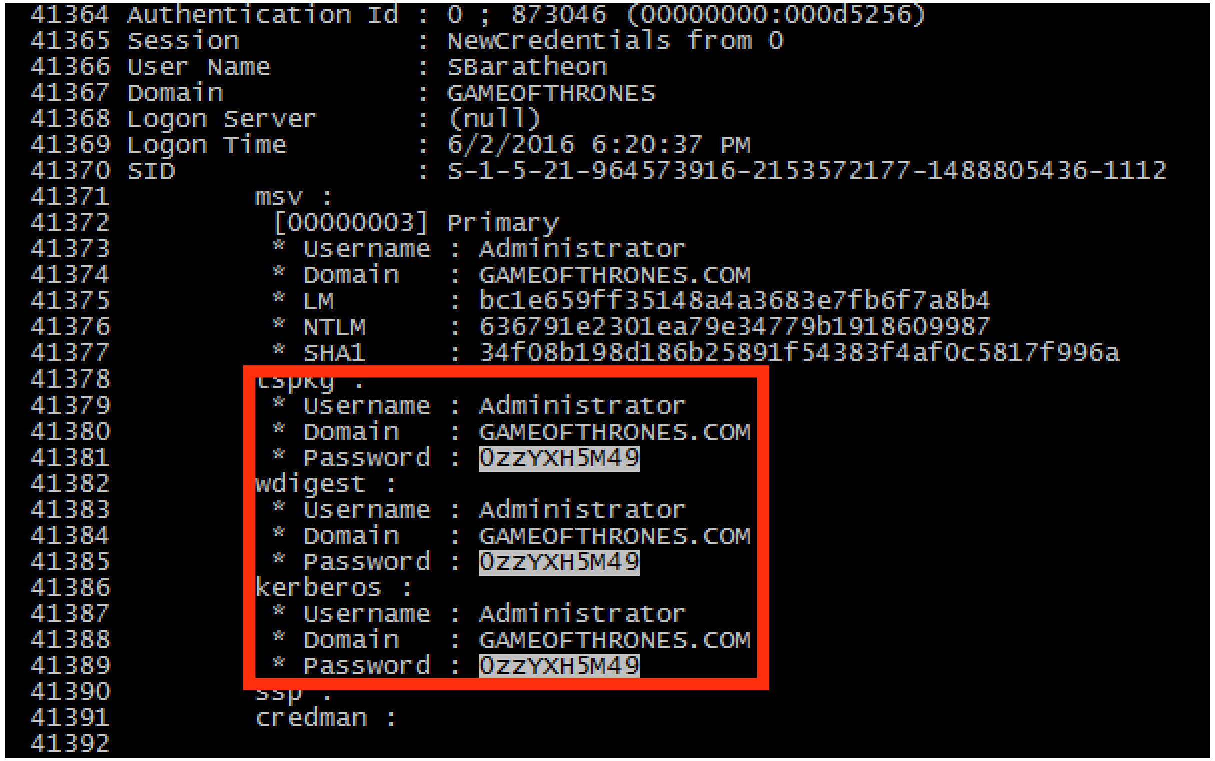
virtualapp/didlogical   Modified: 5/19/2016

Credential Injections

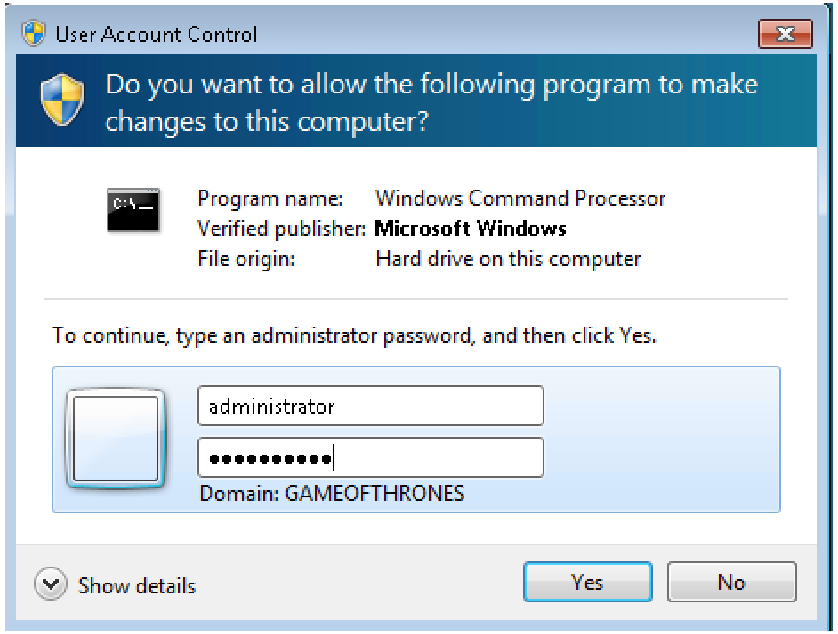
DCEPT

puts honeytoken credentials into memory by calling the CreateProcessWithLogonW Windows API

to launch a suspended subprocess with the LOGON_NETCREDENTIALS_ONLY flag.



```
Authentication Id : 0 ; 873046 (00000000:000d5256)
Session           : NewCredentials from 0
User Name         : SBaratheon
Domain            : GAMEOFTHRONES
Logon Server      : (null)
Logon Time        : 6/2/2016 6:20:37 PM
SID               : S-1-5-21-964573916-2153572177-1488805436-1112
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : GAMEOFTHRONES.COM
         * LM       : bc1e659ff35148a4a3683e7fb6f7a8b4
         * NTLM     : 636791e2301ea79e34779b1918609987
         * SHA1     : 34f08b198d186b25891f54383f4af0c5817f996a
        tspkg :
         * Username : Administrator
         * Domain   : GAMEOFTHRONES.COM
         * Password : 0zzYXH5M49
        wdigest :
         * Username : Administrator
         * Domain   : GAMEOFTHRONES.COM
         * Password : 0zzYXH5M49
        kerberos :
         * Username : Administrator
         * Domain   : GAMEOFTHRONES.COM
         * Password : 0zzYXH5M49
        ssp :
        credman :
```



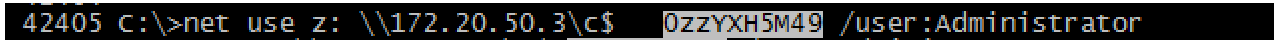
User Account Control

Do you want to allow the following program to make changes to this computer?

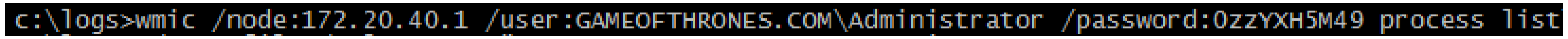
Program name: Windows Command Processor
Verified publisher: **Microsoft Windows**
File origin: Hard drive on this computer

To continue, type an administrator password, and then click Yes.

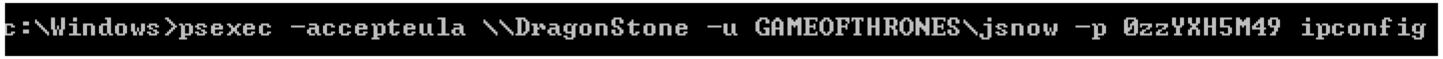
administrator
••••••••••
Domain: GAMEOFTHRONES



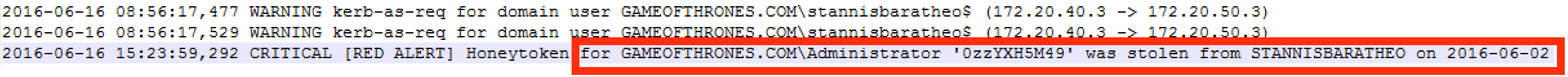
```
C:\>net use z: \\172.20.50.3\c$   0zzYXH5M49 /user:Administrator
```



```
c:\logs>wmic /node:172.20.40.1 /user:GAMEOFTHRONES.COM\Administrator /password:0zzYXH5M49 process list
```



```
:\Windows>psexec -accepteula \\DragonStone -u GAMEOFTHRONES\jsnow -p 0zzYXH5M49 ipconfig
```



```
2016-06-16 08:56:17,477 WARNING kerb-as-req for domain user GAMEOFTHRONES.COM\stannisbaratheo$ (172.20.40.3 -> 172.20.50.3)
2016-06-16 08:56:17,529 WARNING kerb-as-req for domain user GAMEOFTHRONES.COM\stannisbaratheo$ (172.20.40.3 -> 172.20.50.3)
2016-06-16 15:23:59,292 CRITICAL [RED ALERT] Honeytoken for GAMEOFTHRONES.COM\Administrator '0zzYXH5M49' was stolen from STANNISBARATHEO on 2016-06-02
```

Guidelines to making of a good trap

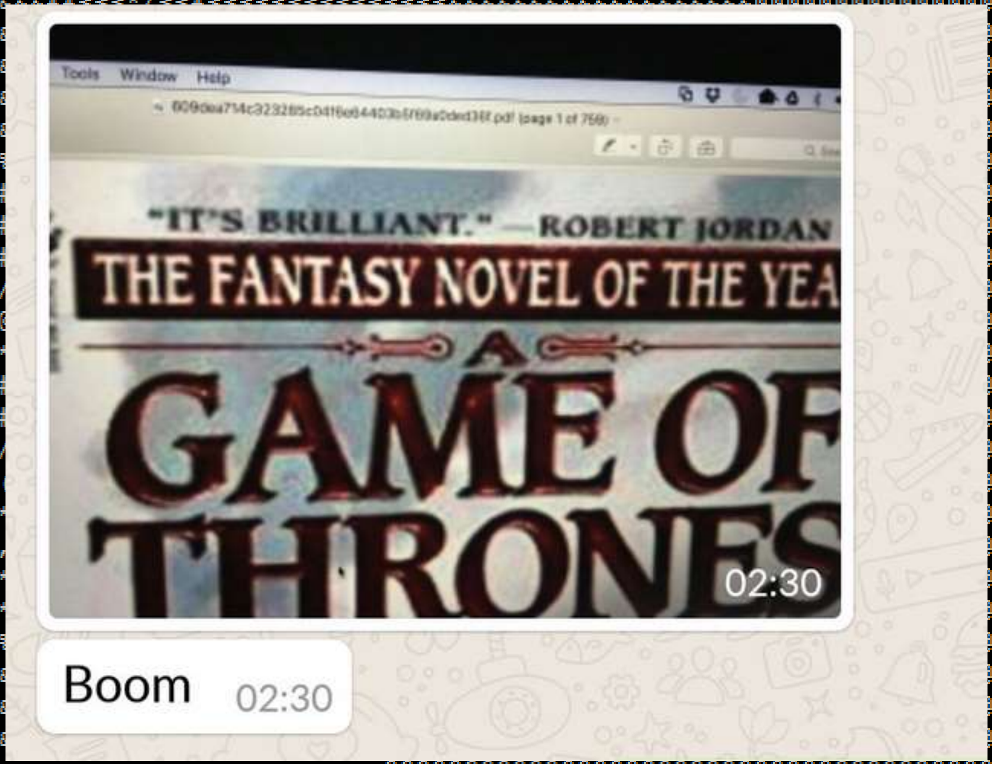
Blend in

Non-Intrusive

Low attack surface

CTF – Stats & Scores

- Ran over a month
- Over 50 security professionals from all over the world
- 6-7 hours on average per player
- ~1.7M data lines collected
- **One clear winner emerged (and has the drone to prove it!)**


Tools
Window
Help
"IT'S BRILLIANT." —ROBERT JORDAN
THE FANTASY NOVEL OF THE YEA
A
GAME OF
THRONES
02:30

Boom 02:30

"I've seen a man who could change his face, the way that other men change their clothes."

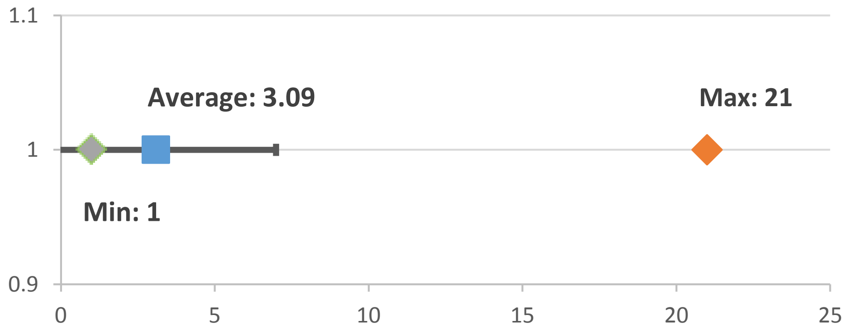
Results

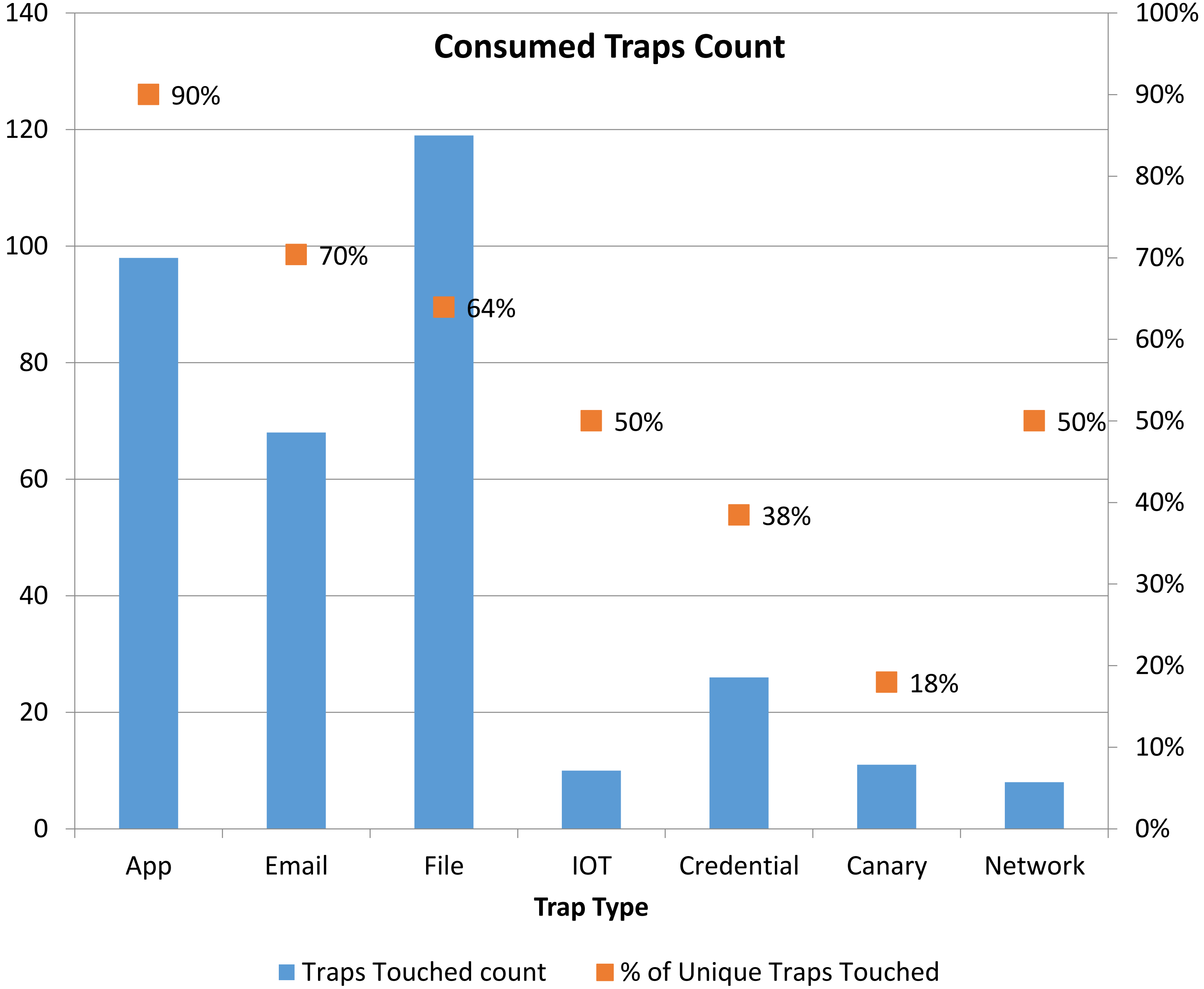
Who Took My Bait?

- 177 different traps laid
- Consumed 340 times
- Avg trap consumed 3.1 times
- Max trap consumed 21 times

62% of traps laid consumed

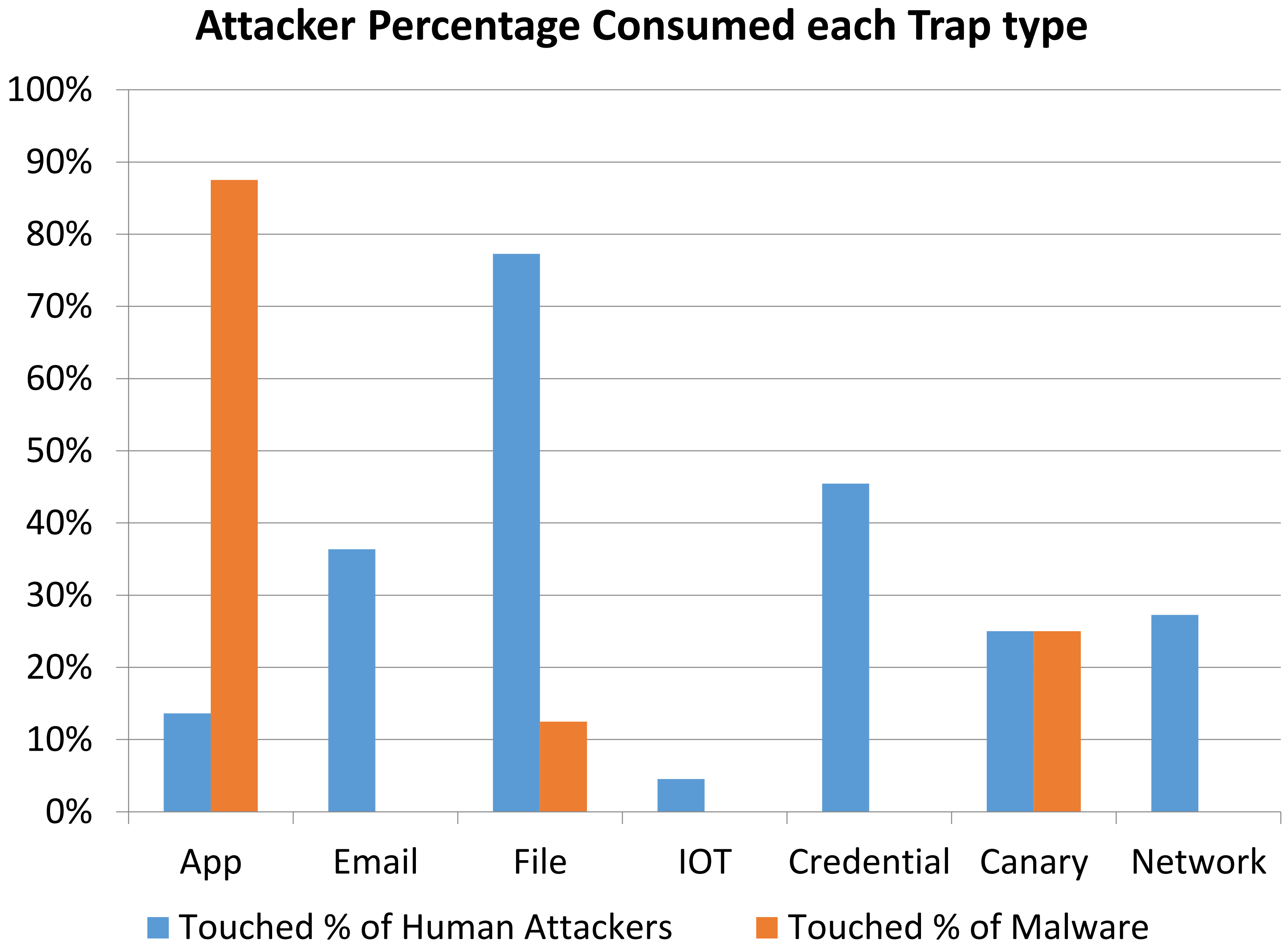
Consumed Traps Distribution





Who Took My Bait?

- Malware Vs Human Attacks differ in patterns
- Each Human Attacker triggered ~10.5 traps
- No one trap type covers all attackers.



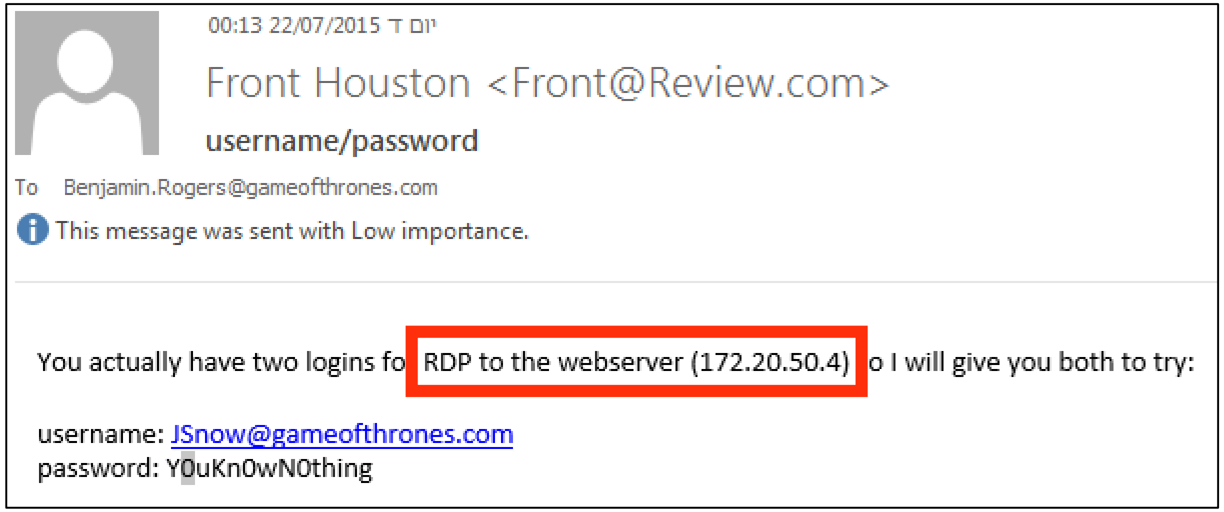
From Trap to Detection

The attackers' knowledge gap widened with every trap taken

Attackers may not use traps the way we intend them to *(but they still get caught!)*

One Man’s Gap

	Decoy IP	Service
✓	172.20.40.4	RDP/3389
	172.20.40.6	FTP/21
	172.20.40.6	RDP/3389
	172.20.40.6	SMB/445
	172.20.40.6	HTTP/80
	172.20.50.4	RDP/3389
	172.20.50.4	SMB/445
	172.20.50.4	HTTP/80
	172.20.50.6	FTP/21
	172.20.50.6	SMB/445



00:13 22/07/2015 יום ד

Front Houston <Front@Review.com>

username/password

To Benjamin.Rogers@gameofthrones.com

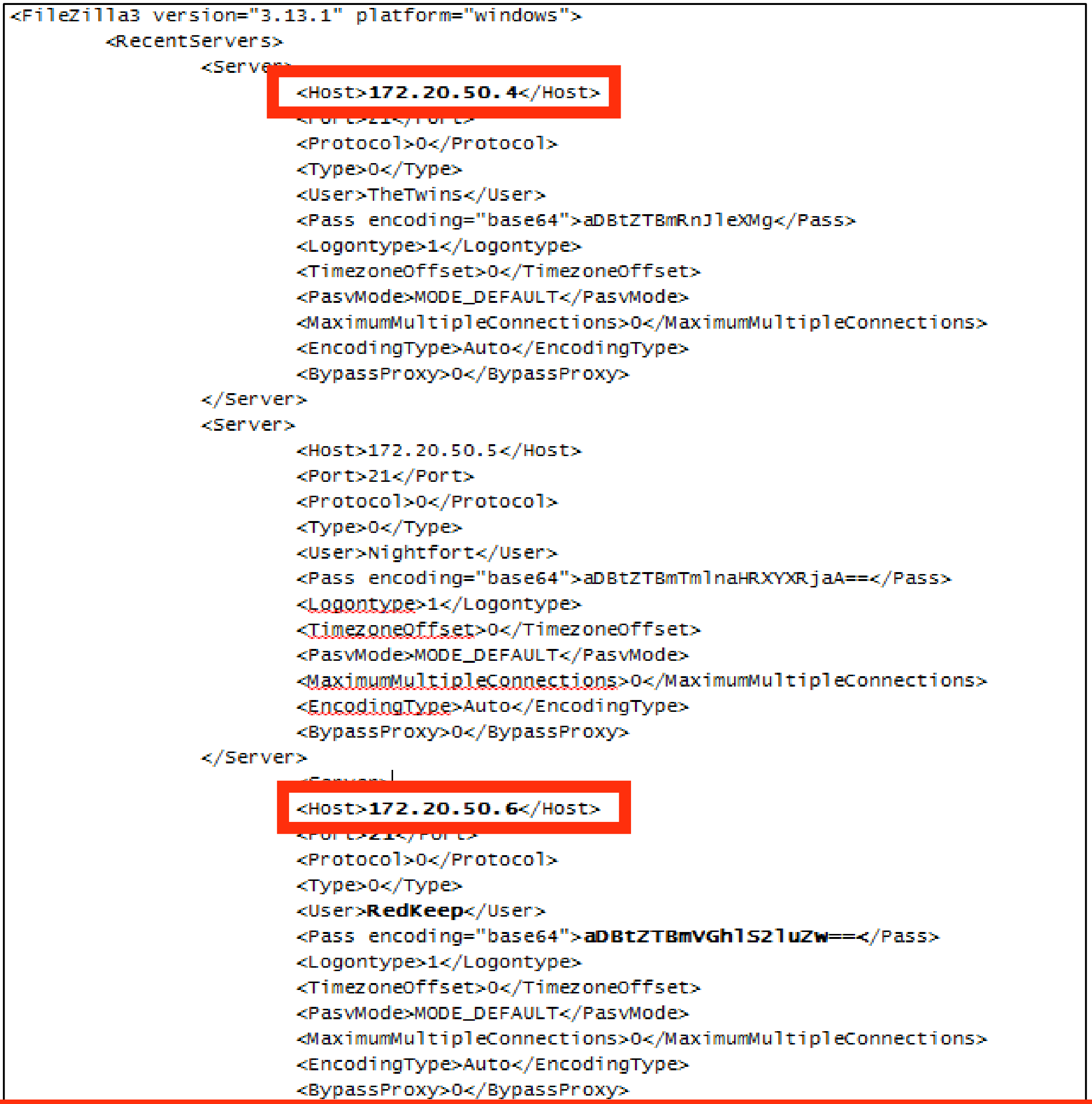
This message was sent with Low importance.

You actually have two logins fo RDP to the webserver (172.20.50.4) o I will give you both to try:

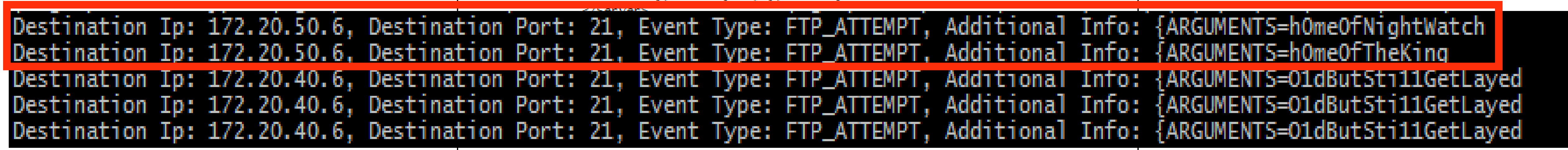
username: JSnow@gameofthrones.com
password: Y0uKn0wN0thing

One Man’s Gap

	Decoy IP	Service
✓	172.20.40.4	RDP/3389
✓	172.20.40.6	FTP/21
	172.20.40.6	RDP/3389
	172.20.40.6	SMB/445
	172.20.40.6	HTTP/80
	172.20.50.4	RDP/3389
	172.20.50.4	SMB/445
	172.20.50.4	HTTP/80
✓	172.20.50.6	FTP/21
	172.20.50.6	SMB/445



```
<FileZilla3 version="3.13.1" platform="windows">
        <RecentServers>
                <Server>
                        <Host>172.20.50.4</Host>
                        <Port>21</Port>
                        <Protocol>0</Protocol>
                        <Type>0</Type>
                        <User>TheTwins</User>
                        <Pass encoding="base64">aDBtZTBmRnJleXMg</Pass>
                        <Logontype>1</Logontype>
                        <TimezoneOffset>0</TimezoneOffset>
                        <PasvMode>MODE_DEFAULT</PasvMode>
                        <MaximumMultipleConnections>0</MaximumMultipleConnections>
                        <EncodingType>Auto</EncodingType>
                        <BypassProxy>0</BypassProxy>
                </Server>
                <Server>
                        <Host>172.20.50.5</Host>
                        <Port>21</Port>
                        <Protocol>0</Protocol>
                        <Type>0</Type>
                        <User>Nightfort</User>
                        <Pass encoding="base64">aDBtZTBmTmlnaHRXYXRjaA==</Pass>
                        <Logontype>1</Logontype>
                        <TimezoneOffset>0</TimezoneOffset>
                        <PasvMode>MODE_DEFAULT</PasvMode>
                        <MaximumMultipleConnections>0</MaximumMultipleConnections>
                        <EncodingType>Auto</EncodingType>
                        <BypassProxy>0</BypassProxy>
                </Server>
                <Server>
                        <Host>172.20.50.6</Host>
                        <Port>21</Port>
                        <Protocol>0</Protocol>
                        <Type>0</Type>
                        <User>RedKeep</User>
                        <Pass encoding="base64">aDBtZTBmVGhlS2luZw==</Pass>
                        <Logontype>1</Logontype>
                        <TimezoneOffset>0</TimezoneOffset>
                        <PasvMode>MODE_DEFAULT</PasvMode>
                        <MaximumMultipleConnections>0</MaximumMultipleConnections>
                        <EncodingType>Auto</EncodingType>
                        <BypassProxy>0</BypassProxy>
                </Server>
```

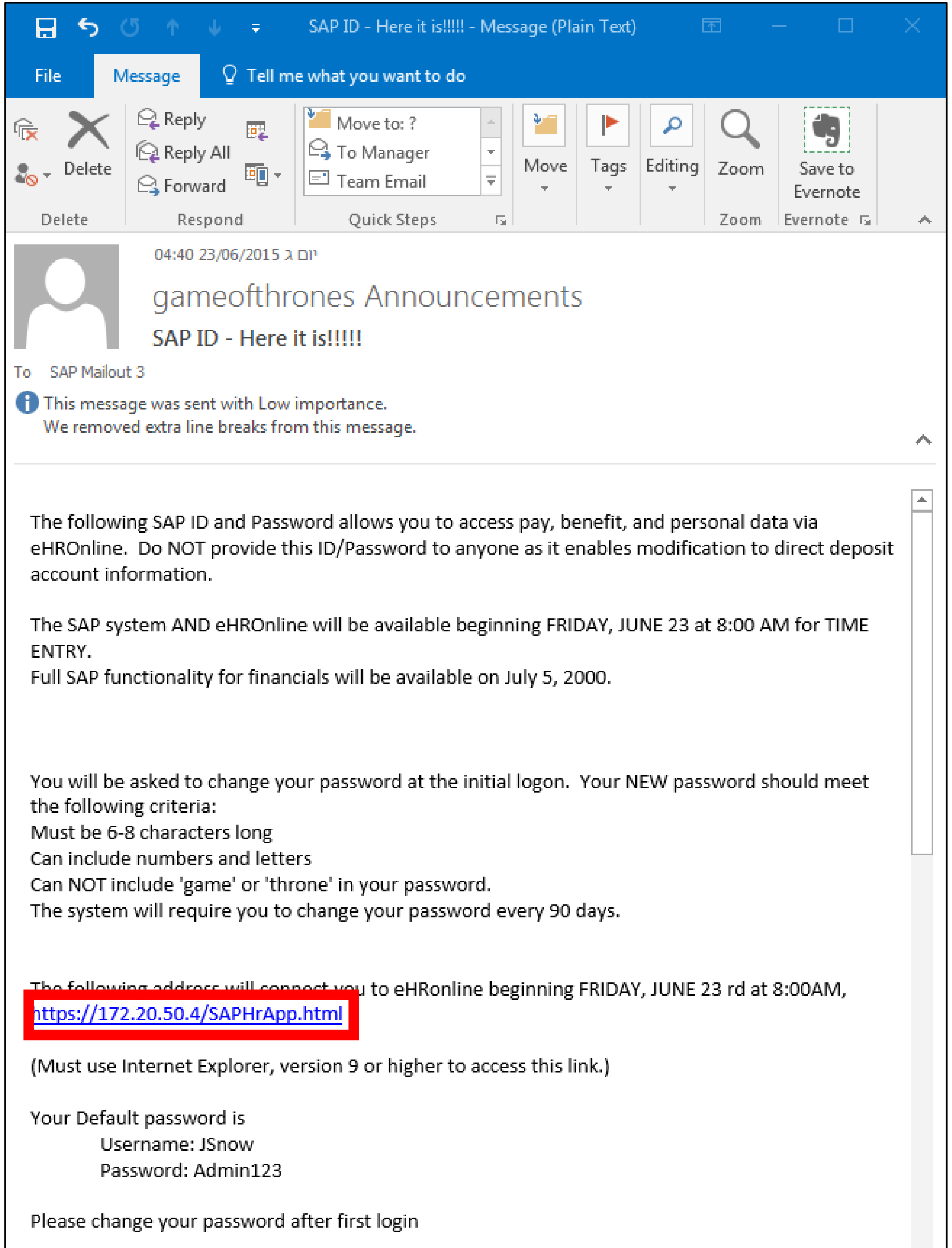


```
Destination Ip: 172.20.50.6, Destination Port: 21, Event Type: FTP_ATTEMPT, Additional Info: {ARGUMENTS=h0meOfNightWatch
Destination Ip: 172.20.50.6, Destination Port: 21, Event Type: FTP_ATTEMPT, Additional Info: {ARGUMENTS=h0meOfTheKing
Destination Ip: 172.20.40.6, Destination Port: 21, Event Type: FTP_ATTEMPT, Additional Info: {ARGUMENTS=01dButSti11GetLayed
Destination Ip: 172.20.40.6, Destination Port: 21, Event Type: FTP_ATTEMPT, Additional Info: {ARGUMENTS=01dButSti11GetLayed
Destination Ip: 172.20.40.6, Destination Port: 21, Event Type: FTP_ATTEMPT, Additional Info: {ARGUMENTS=01dButSti11GetLayed
```

```
                        <TimezoneOffset>0</TimezoneOffset>
                        <PasvMode>MODE_DEFAULT</PasvMode>
                        <MaximumMultipleConnections>0</MaximumMultipleConnections>
```

One Man’s Gap

	Decoy IP	Service
✓	172.20.40.4	RDP/3389
✓	172.20.40.6	FTP/21
	172.20.40.6	RDP/3389
	172.20.40.6	SMB/445
	172.20.40.6	HTTP/80
✓	172.20.50.4	RDP/3389
	172.20.50.4	SMB/445
✓	172.20.50.4	HTTP/80
✓	172.20.50.6	FTP/21
	172.20.50.6	SMB/445



יום ג' 23/06/2015 04:40

gameofthrones Announcements

SAP ID - Here it is!!!!!

To SAP Mailout 3

This message was sent with Low importance.
We removed extra line breaks from this message.

The following SAP ID and Password allows you to access pay, benefit, and personal data via eHROnline. Do NOT provide this ID/Password to anyone as it enables modification to direct deposit account information.

The SAP system AND eHROnline will be available beginning FRIDAY, JUNE 23 at 8:00 AM for TIME ENTRY.
Full SAP functionality for financials will be available on July 5, 2000.

You will be asked to change your password at the initial logon. Your NEW password should meet the following criteria:
Must be 6-8 characters long
Can include numbers and letters
Can NOT include 'game' or 'throne' in your password.
The system will require you to change your password every 90 days.

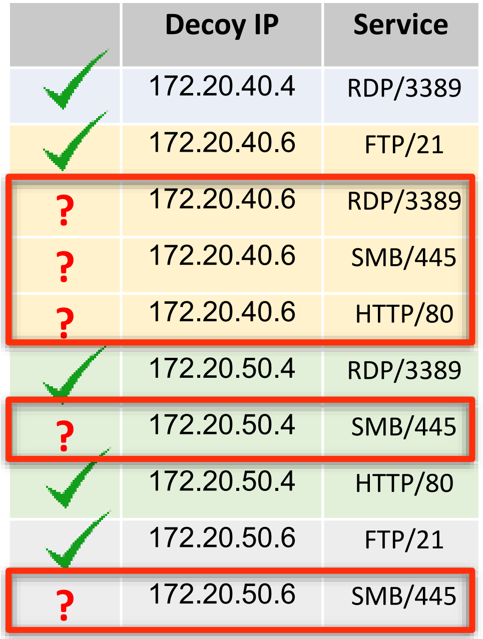
The following address will connect you to eHRonline beginning FRIDAY, JUNE 23 rd at 8:00AM,
https://172.20.50.4/SAPHrApp.html

(Must use Internet Explorer, version 9 or higher to access this link.)

Your Default password is
Username: JSnow
Password: Admin123

Please change your password after first login

One Man’s Gap

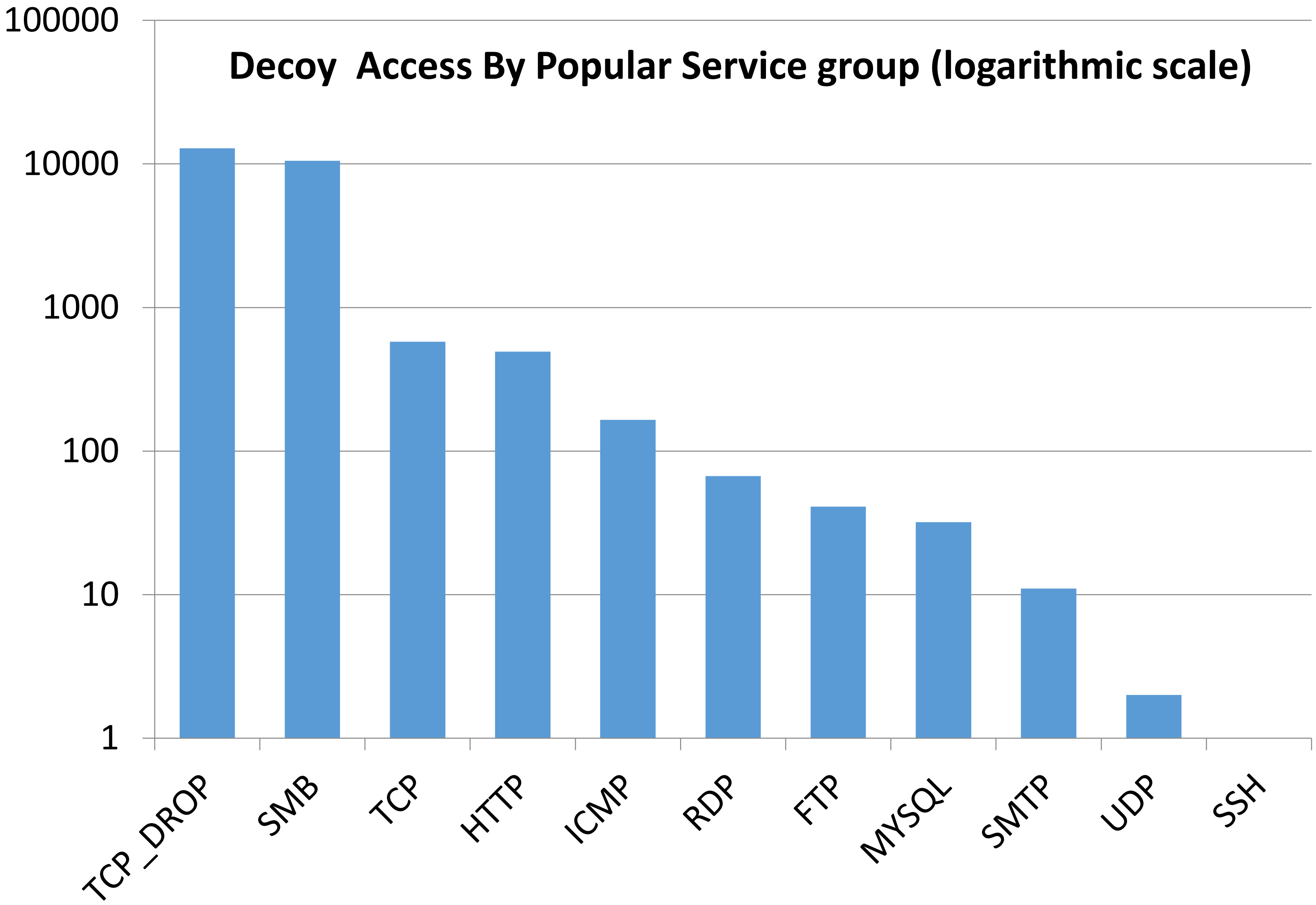


	Decoy IP	Service
✓	172.20.40.4	RDP/3389
✓	172.20.40.6	FTP/21
?	172.20.40.6	RDP/3389
?	172.20.40.6	SMB/445
?	172.20.40.6	HTTP/80
✓	172.20.50.4	RDP/3389
?	172.20.50.4	SMB/445
✓	172.20.50.4	HTTP/80
✓	172.20.50.6	FTP/21
?	172.20.50.6	SMB/445

- Attacker “expands his horizons”
- Information gap gets wider as attacker gets tangled in the decoy
- Total time wasted > 4H

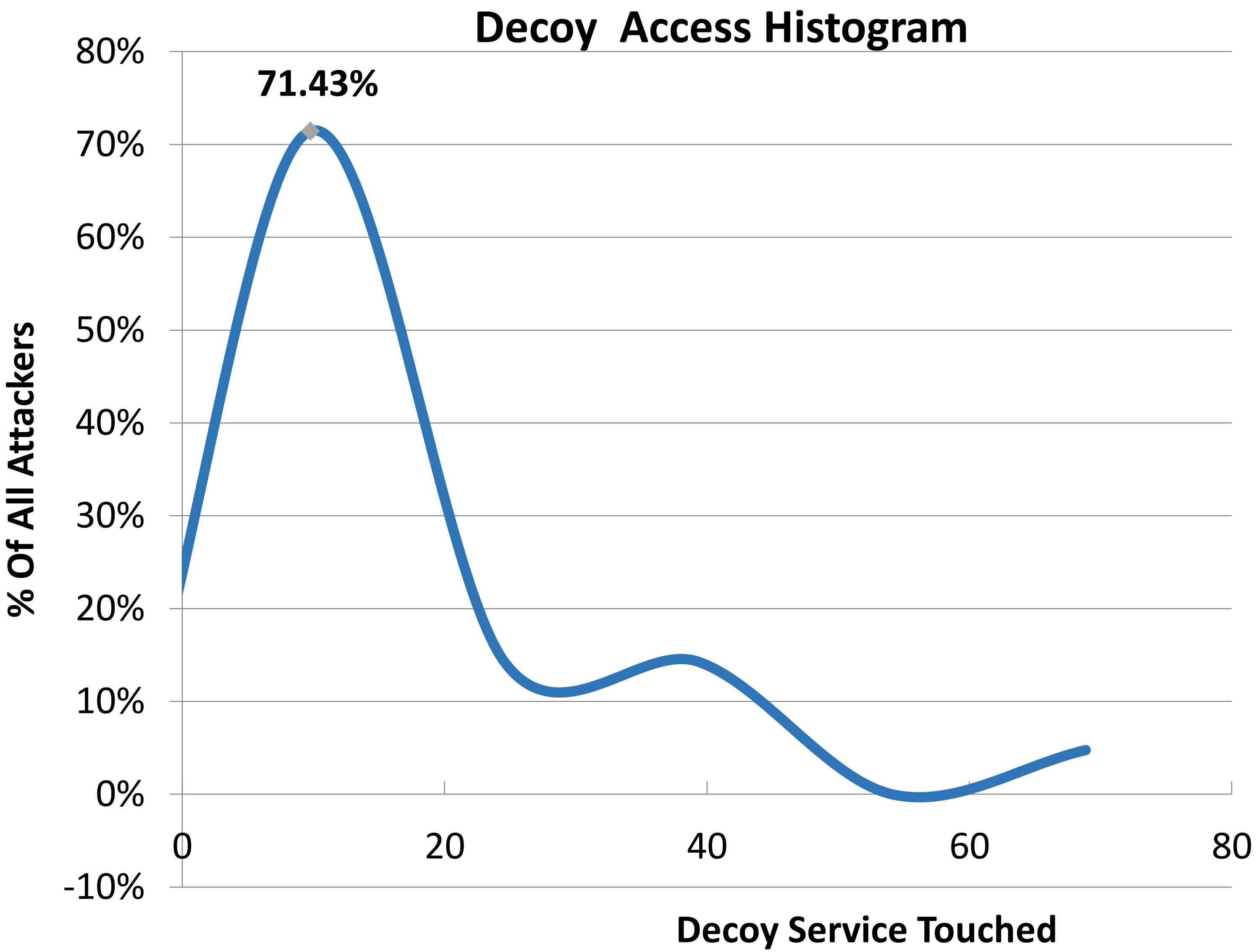
Decoy Access

- **Contestant interacted with 9.7 different decoy services**



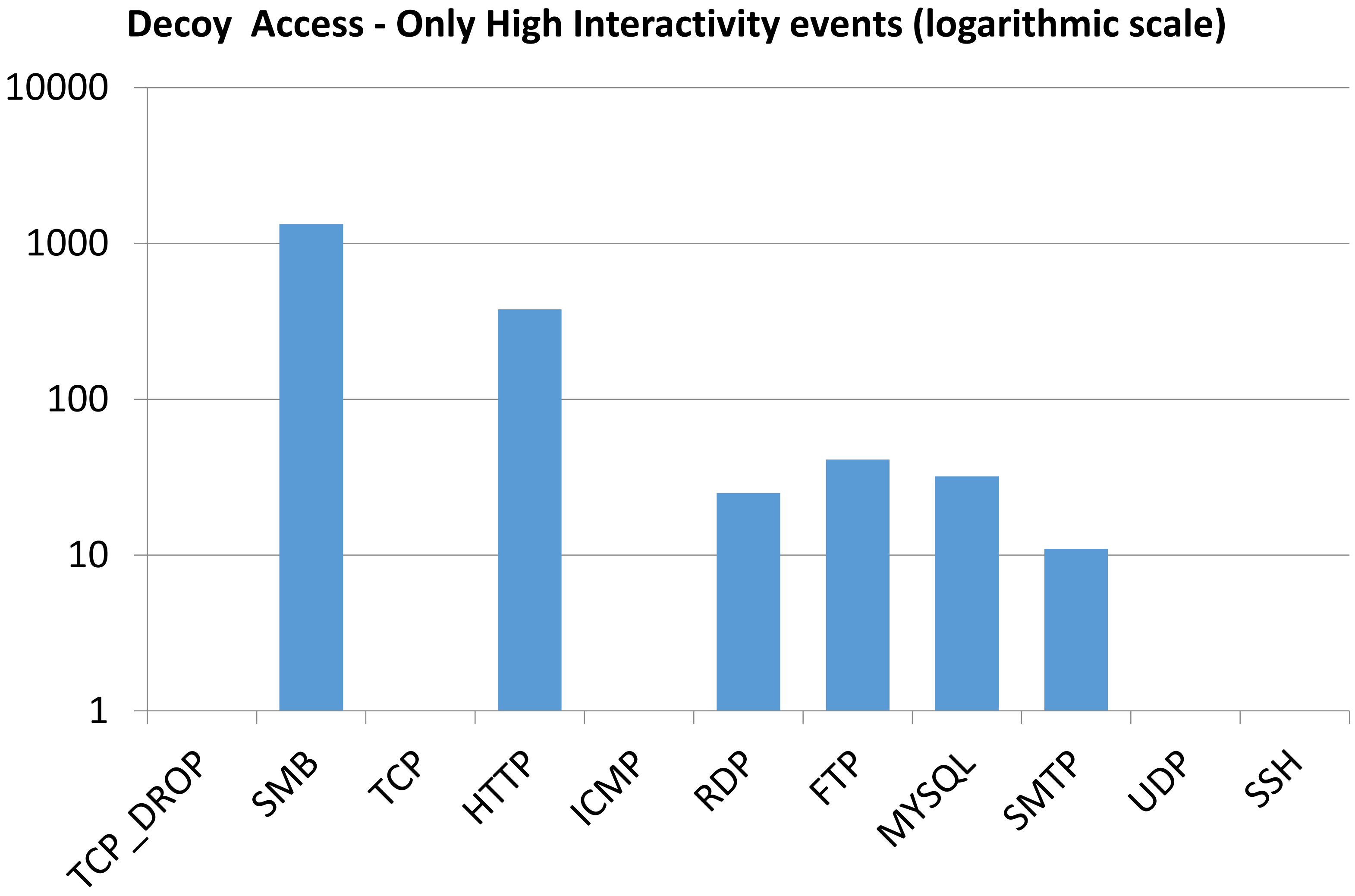
Decoy Access

- Less that 20% of attackers initiated most decoy events
- Scanning easily detected using decoys.



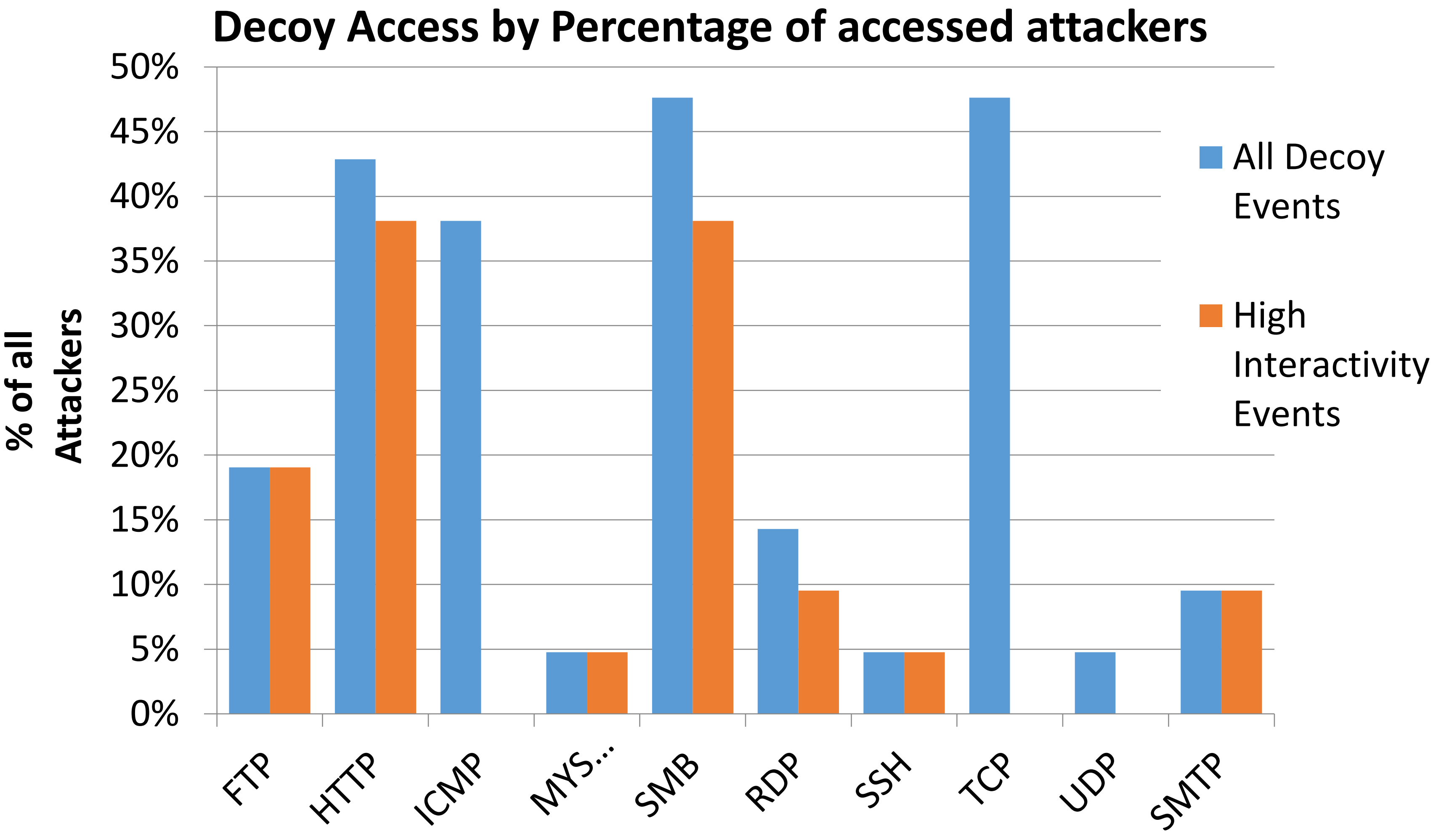
High Interaction Decoy Services

- 4 High interactivity Decoy access per attacker

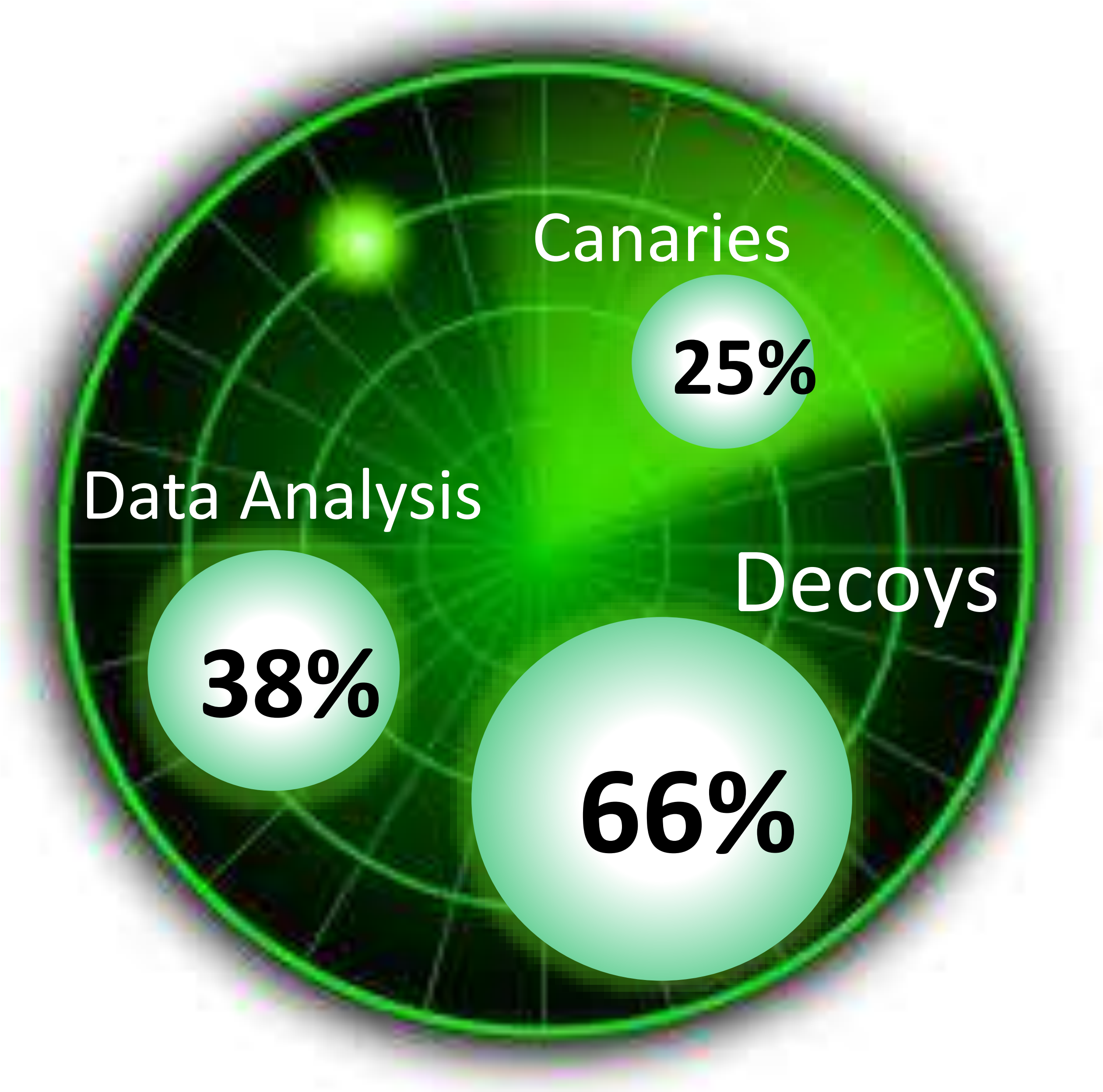


High Interaction Decoy Services

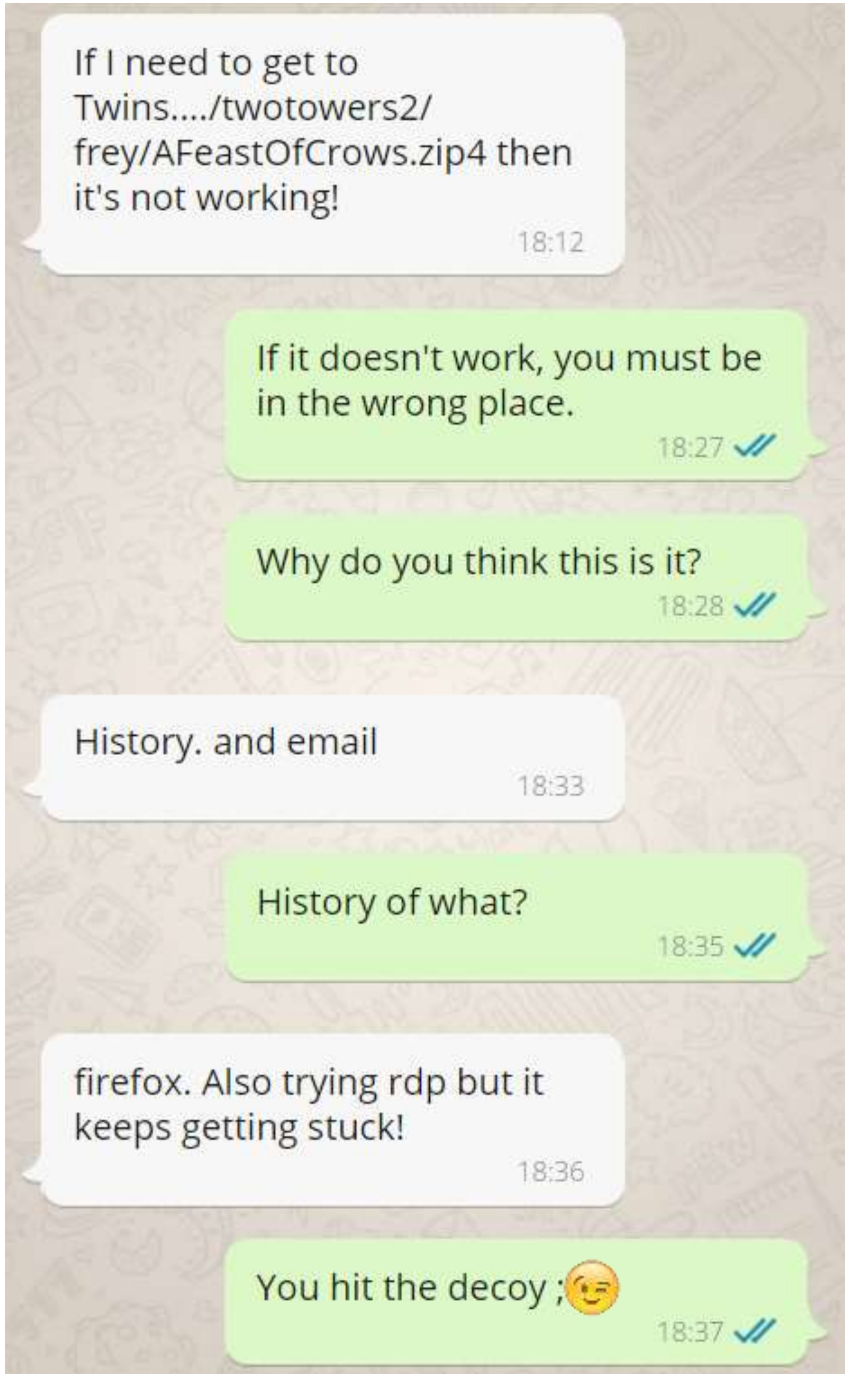
- Most scanners continued to interact with decoy
- Attacker had hard time differentiating between decoy and real machines.
- Service Diversity is essential for efficient detection



100% Detection



Just A small tidbit…



If I need to get to Twins..../twotowers2/frey/AFeastOfCrows.zip4 then it's not working!
18:12

If it doesn't work, you must be in the wrong place.
18:27 ✓✓

Why do you think this is it?
18:28 ✓✓

History. and email
18:33

History of what?
18:35 ✓✓

firefox. Also trying rdp but it keeps getting stuck!
18:36

You hit the decoy ;😉
18:37 ✓✓

Wrap up

Deception increases attacker knowledge gaps

The bigger it is, the easier it to detect

Diversity - Key to get coverage on all types of attacks

Traps and decoys tailored for the organization

End Goal is Detection – Not the decoys!

Relying on multiple detection mechanisms will increase detection effectiveness

Newman got it half right

Master of my Domain

Thank You!

omer@topspinsec.com
www.topspinsec.com