# Are your cloud servers under attack?

# Brian Hileman

Sales Engineer @ 


Creator / Owner @ DLPtest.com
Past Sales Engineer @ OverWatchID
Past Professional Services @ InteliSecure

# PRESENTATION TOPICS

1. Monitor Exit and Entry Points
2. Maintain Visibility and Control
3. Investigation
4. Recommendations
5. Q & A

# LAYING THE GOUND WORK

Deployed AWS Lab

Laid the Bait

Installed DG Agent

1

# Monitor Exit and Entry Points

# MONITOR EXIT AND ENTRY POINTS

- RDP (Remote Desktop Protocol)
  - Within AWS the default security setting will not allow incoming RDP traffic. The suggested setting is to keep RDP locked down to specific IP Addresses.
  - For convenience many people open RDP to all external IP Address.
- How widespread is open RDP ?
  - There are over **3 million** identified IP addresses with RDP available on the Internet, 900,000 of which are located in the United States.
  - Source: https://www.darkreading.com/endpoint/the-risks-of-remote-desktop-access-are-far-from-remote/a/d-id/1331820

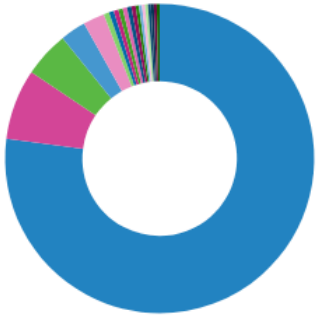
# HOW BAD COULD OPEN RDP BE?

**Opened RDP for 10 Days and had over 43,000 login attempts**

**TARGETED MACHINES**

| Computer Name | Total |
|---|---|
| workgroup\EC2AMAZ-JUMP | 43,946 |

**ATTEMPTED USER ACCOUNTS**



# WHO WAS TRYING TO LOG IN?

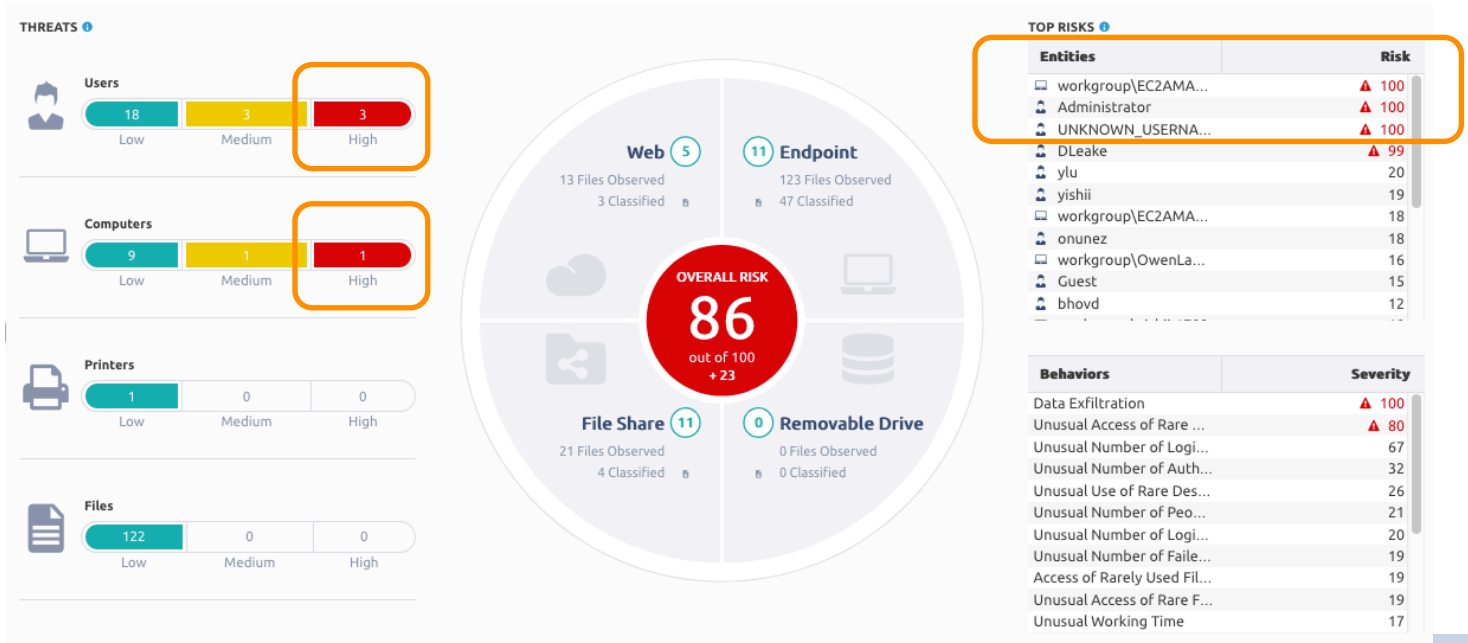
**FAILED SRC IP'S**

| IP Address | Total |
|---|---|
| 103.29.185.190 | 5,344 |
| 23.91.75.214 | 3,541 |
| 95.179.230.249 | 2,342 |
| 213.160.11.66 | 2,333 |
| 46.161.27.17 | 1,821 |
| 212.92.122.126 | 1,672 |
| 185.107.45.61 | 1,604 |
| 212.92.105.217 | 1,603 |
| 23.91.73.176 | 1,561 |
| 23.91.72.77 | 1,374 |
| 85.93.20.126 | 1,325 |
| 23.91.74.194 | 1,307 |
| 31.129.92.206 | 1,286 |
| 197.5.145.125 | 1,183 |
| 104.209.182.141 | 1,159 |
| 210.41.195.1 | 1,045 |

## Top 5 IP Address

1. PT Pascal – Indonesia
2. A Small Orange – USA
3. Choopa – Netherlands
4. Sparky GmbH – Germany
5. Petersburg Internet Network – Netherlands

# EXTRA INDICATORS USER AND ENTITY BEHAVIOR ANALYTICS (UEBA)



# WHAT HAPPENS IF A WEAK PASSWORD IS USED?

- On the AWS Server with RDP now opened externally, I created a local account called "admin" and set the password to "P@ssw0rd!”
- After the password was changed around noon, someone had compromised the account within **9 Hours!**
- Admin account was used 6 times from different IP Addresses over 4 days

# 2

# Maintain Visibility and Control

# MAINTAIN VISIBILITY AND CONTROL

### System Events

Based on what happens outside of user intervention.

Initiated at the OS level.

### User Events

Focus on what each individual is actively doing.

This includes command line, copy and paste, the use of applications.

### Data Events

File level including moving files from one location to another via email, uploading or downloading files, or USB usage.

# Review: Who and When

**ACTIVE USERS**

| User | Event Local Time |
|---|---|
| Administrator | 01/06/19 5:58:14 pm |
| admin | 01/05/19 12:06:56 am |
| admin | 01/04/19 8:35:46 pm |
| admin | 01/04/19 6:24:38 am |
| admin | 01/04/19 5:13:36 am |
| admin | 01/04/19 3:30:05 am |
| admin | 01/02/19 8:30:53 pm |
| admin | 01/02/19 11:47:56 am |
| Administrator | 01/02/19 11:32:05 am |

**AFTER HOURS LOG IN TIMES**

| User | Event Local Time |
|---|---|
| admin | 01/05/19 12:06:56 am |
| admin | 01/04/19 8:35:46 pm |
| admin | 01/04/19 6:24:38 am |
| admin | 01/04/19 5:13:36 am |
| admin | 01/04/19 3:30:05 am |
| admin | 01/02/19 8:30:53 pm |

# Review: Network Traffic

**DNS TOTAL**

| DNS Hostname | Application | Total |
|---|---|---|
| chat6.zoosk.com:5281 | chrome.exe | 189 |
| speed.mowinet.com.prod.hosts.ooklase... | chrome.exe | 141 |
| speedtest.ifiber.tv.prod.hosts.ooklaserv... | chrome.exe | 119 |
| speedtest5.wtechlink.com.prod.hosts.o... | chrome.exe | 33 |
| qcx.quantserve.com:8443 | chrome.exe | 21 |
| speedtest.eotnet.net | sysscan.exe | 11 |
| client.wns.windows.com | explorer.exe | 7 |
| www.speedtest.net | sysscan.exe | 2 |
| auth.svcs.verizon.com:22790 | chrome.exe | 1 |
| c.speedtest.net | sysscan.exe | 1 |
| dmd.metaservices.microsoft.com | svchost.exe | 1 |
| go.microsoft.com | svchost.exe | 1 |
| storecatalogrevocation.storequality.mic... | svchost.exe | 1 |
| www.microsoft.com | svchost.exe | 1 |

**NETWORK DOWNLOADS**

| User | Application | DNS Hostname | Destination File Name | Destination Directory |
|---|---|---|---|---|
| admin | iexplore.exe | s9.picofile.com | بخریداری شده.rar | c:\users\admin\downloads |
| admin | iexplore.exe | dl.google.com | chromesetup.exe | c:\users\admin\downloads |
| Administrator | chrome.exe | mirror2.internetdownloadmanager.com | idman632build5.exe | c:\users\administrator\do... |

**NETWORK UPLOADS**

| User | Application ▲ | DNS Hostname | Source File Name | Source Directory |
|---|---|---|---|---|
| Administrator | chrome.exe | 1001-2.filemail.com | 720.mp4 | c:\users\administrator\downloads\video |
| Administrator | chrome.exe | 1002.filemail.com | 720.mp4 | c:\users\administrator\downloads\video |

# ADDITIONAL USER EVENTS

## Found: Some rules started to trigger, including some Advanced Threat Alarms

**DETECTION NAME**

| Detection Name | To... |
|---|---|
| ATP - DLL File Written to Disk | 91 |
| ATP - EXE File Written to Disk | 13 |
| DLP1007-D-User renames file | 8 |
| DLP1007-D-User renames file | 8 |
| [Info]-ATP3028 - Launch of Executable Recently Created | 6 |
| [Execution]-ATP5021 - DLL Load from Suspicious Temp Dir... | 1 |

**FORENSICS**

| Event Time | Computer Name | User Name | Operation Type | Detection Name | Application | Application Command Line |
|---|---|---|---|---|---|---|
| 01/04/19 7:10:10 am | workgroup\EC2AMA... | admin | Application Start | [Info]-ATP3028 - ... | software_reporter_tool... | "c:\users\admin\appdata\local\google\chrome\user data\swreporter\36.184.... |
| 01/04/19 7:10:10 am | workgroup\EC2AMA... | admin | Application Start | [Info]-ATP3028 - ... | software_reporter_tool... | "C:\Users\admin\AppData\Local\Google\Chrome\User Data\SwReporter\36.... |
| 01/04/19 7:10:10 am | workgroup\EC2AMA... | admin | Application Start | [Info]-ATP3028 - ... | software_reporter_tool... | "C:\Users\admin\AppData\Local\Google\Chrome\User Data\SwReporter\36.... |
| 01/04/19 7:00:43 am | workgroup\EC2AMA... | admin | Application Start | [Info]-ATP3028 - ... | chromesetup.exe | "C:\Users\admin\Downloads\ChromeSetup.exe" |
| 01/04/19 7:00:43 am | workgroup\EC2AMA... | admin | Application Start | [Info]-ATP3028 - ... | chromesetup.exe | "C:\Users\admin\Downloads\ChromeSetup.exe" |
| 01/04/19 6:32:22 am | workgroup\EC2AMA... | admin | Application Start | [Info]-ATP3028 - ... | dismhost.exe | C:\Users\admin\AppData\Local\Temp\D1CC1317-8225-4F65-9F58-F183D15F... |
| 01/04/19 5:14:26 am | workgroup\EC2AMA... | admin | Application Start | [Info]-ATP3028 - ... | ns.exe | "C:\Users\admin\Desktop\NS.exe" |
| 01/04/19 3:32:17 am | workgroup\EC2AMA... | admin | Application Start | [Info]-ATP3028 - ... | sysscan.exe | "C:\Users\admin\Desktop\sysscan.exe" |

# APPLICATION REVIEW

## Found: Applications were installed

**UNAUTHORIZED APPLICATIONS**

| Application | Company Name | SHA1 Hash |
|---|---|---|
| 71.0.3578.98_chrome_installer... | google inc. | FECE3D3DBE2F37C49B817A5... |
| chrmstp.exe | google inc. | B4D684BBA0F9E8F5A08300E0... |
| chrome.exe | google inc. | CBC93977B036EF2C6F9569F7... |
| chromesetup.exe | google inc. | 606B2BAB8A12C505D129CA0... |
| chromesetup.exe | google inc. | 943D7444ED9DD9A1A6AF4ED... |
| googlecrashhandler.exe | google inc. | 8EFEC0871A9BC4E2C31322B1... |
| googlecrashhandler64.exe | google inc. | 00A44BA18164ACEEACABE53... |
| googleupdate.exe | google inc. | E318FA476FA7D3BC0FA5A093... |
| googleupdatecomregistershell... | | 62BAE4B05F51B718F7D059E2... |
| googleupdatecore.exe | google inc. | D08A0C49CB44E9A3881DB85... |
| googleupdateondemand.exe | google inc. | 32440C5B976BFD530E601A46... |
| idm1.tmp | tonec inc. | 4AAFB0352F00E1422B70B7D... |
| idman.exe | tonec inc. | FAD852F8E87B73AA404E184F... |
| idman632build5.exe | tonec inc. | 264B0A0AC90F340F8C7AF058... |

Table Part 1

**UNAUTHORIZED APPLICATIONS**

| Application | Company Name | SHA1 Hash |
|---|---|---|
| idmbroker.exe | internet download manager, to... | BC623E2D7B89C880974E19A8... |
| idmintegrator64.exe | internet download manager, to... | 529EA955591A6483F817AF48... |
| iemonitor.exe | tonec inc. | 4FE43C0F03B1DB2B3E063D30... |
| kportscan3.exe | | 0FBC897BF6046718524D05B6... |
| mediumilstart.exe | internet download manager, to... | 9728FF8AA403F74F84C6D5F5... |
| ns.exe | | 629C9649CED38FD815124221... |
| setup.exe | google inc. | B4D684BBA0F9E8F5A08300E0... |
| software_reporter_tool.exe | google | EA090E725F10A3FC752A2FB6... |
| sysscan.exe | | EDE83D1146CC2BA58E3385A... |
| taskmgr.exe | | 338349D404DC8432C6497D3... |
| uninstall.exe | tonec inc. | 4AAFB0352F00E1422B70B7D... |
| uninstall.exe | alexander roshal | 3BE33842FF62D3E97F2AB0AB... |
| winrar-x64-561.exe | alexander roshal | 2F792BFA1859986ABDAF8A8... |
| winrar.exe | alexander roshal | EA8020EA78D0307E9147D8D... |

Table Part 2

# REVIEW : TIMELINE OF EVENTS

**TIMELINE**

| Operation Type | Detection Name | Application | Application Command Line |
|---|---|---|---|
| Application Start | [Info]-ATP3028 - Launch of Executable Recently Created | chromehistoryview.exe | "C:\Users\admin2\Downloads\chromehistoryview\ChromeHistoryView.exe" |
| Application Start | [Info]-ATP3028 - Launch of Executable Recently Created | idman632build5.exe | "C:\Users\Administrator\Downloads\idman632build5.exe" |
| Application Start | [Info]-ATP3028 - Launch of Executable Recently Created | chrmstp.exe | "C:\Program Files (x86)\Google\Chrome\Application\71.0.3578.98\Installer\chrmstp.exe" --type=crashpad-ha |
| Application Start | [Info]-ATP3028 - Launch of Executable Recently Created | chrmstp.exe | "C:\Program Files (x86)\Google\Chrome\Application\71.0.3578.98\Installer\chrmstp.exe" --configure-user-se |
| Application Start | [Info]-ATP3028 - Launch of Executable Recently Created | googleupdateondemand.e... | "C:\Program Files (x86)\Google\Update\1.3.33.23\GoogleUpdateOnDemand.exe" -Embedding |
| Application Start | [Info]-ATP3028 - Launch of Executable Recently Created | chromesetup.exe | "C:\Users\Administrator\AppData\Local\Microsoft\Windows\INetCache\IE\JWFHPCOH\ChromeSetup.exe" |
| Application Start | [Info]-ATP3028 - Launch of Executable Recently Created | kportscan3.exe | "C:\KPortScan 3.0\KPortScan3.exe" |
| Application Start | [Info]-ATP3028 - Launch of Executable Recently Created | winrar.exe | "C:\Program Files\WinRAR\WinRAR.exe" "C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\IE\ |
| Application Start | [Info]-ATP3028 - Launch of Executable Recently Created | winrar.exe | "C:\Program Files\WinRAR\WinRAR.exe" "C:\Users\admin\Downloads\خریداری شده.rar" |
| Application Start | [Info]-ATP3028 - Launch of Executable Recently Created | uninstall.exe | "C:\Program Files\WinRAR\uninstall.exe" /setup |
| Application Start | [Info]-ATP3028 - Launch of Executable Recently Created | winrar-x64-561.exe | "C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\IE\TZ38BZGO\winrar-x64-561.exe" |
| Application Start | [Info]-ATP3028 - Launch of Executable Recently Created | software_reporter_tool.exe | "c:\users\admin\appdata\local\google\chrome\user data\swreporter\36.184.200\software_reporter_tool.ex |
| Application Start | [Info]-ATP3028 - Launch of Executable Recently Created | software_reporter_tool.exe | "C:\Users\admin\AppData\Local\Google\Chrome\User Data\SwReporter\36.184.200\software_reporter_too |
| Application Start | [Info]-ATP3028 - Launch of Executable Recently Created | chromesetup.exe | "C:\Users\admin\Downloads\ChromeSetup.exe" |
| Application Start | [Info]-ATP3028 - Launch of Executable Recently Created | dismhost.exe | C:\Users\admin\AppData\Local\Temp\D1CC1317-8225-4F65-9F58-F183D15FFFB6\dismhost.exe {C1F8032E-9 |
| Application Start | [Info]-ATP3028 - Launch of Executable Recently Created | ns.exe | "C:\Users\admin\Desktop\NS.exe" |
| Application Start | [Info]-ATP3028 - Launch of Executable Recently Created | sysscan.exe | "C:\Users\admin\Desktop\sysscan.exe" |

# SUSPICIOUS APPLICATIONS

## Found 3 of the newly installed applications came back as suspicious from VirusTotal

**VIRUSTOTAL STATS**

| Application | VirusTotal Status | VirusTotal Match Percent ▾ |
|---|---|---|
| sysscan.exe | Suspicious | 61.97 |
| ns.exe | Suspicious | 52.17 |
| kportscan3.exe | Suspicious | 47.14 |
| brt.exe | Not Suspicious | 7.35 |

# RECAP

- We have an AWS open to the internet
- Someone used the Admin account to gain access into the AWS server
- Someone installed Chrome and did some internet browsing
- The login events also show someone started using the Administrator account
- Someone installed 3 suspicious applications which are used for network scanning

- One item I didn't share is that I am now locked out of my server since the person using the Admin account changed all the passwords

# 3

# Investigation

# STARTING THE INVESTIGATION

- Locked down RDP
- Regained access to the server using the DG agent to run a PowerShell script to create a new admin account
  - Reset all the passwords
- Pulled back the forensics
  - Windows Event Logs
  - MFT
  - Registry
  - Web History

# DIVING INTO THE WEB HISTORY

| URL | Title | Visited On |
|---|---|---|
| https://accounts.google.com/ServiceLogin?service=mail&pass | Gmail | 1/4/19 7:01 |
| https://mail.google.com/mail/ | Inbox (73) - salsadance1956@gmail.com - Gmail | 1/4/19 7:01 |
| http://gmail.com/ | Gmail | 1/4/19 7:01 |
| https://gmail.com/ | Gmail | 1/4/19 7:01 |
| https://www.google.com/gmail/ | Gmail | 1/4/19 7:01 |
| https://accounts.google.com/signin/v2/identifier?service=mai | Gmail | 1/4/19 7:01 |
| https://accounts.google.com/signin/v2/sl/pwd?service=mail& | Gmail | 1/4/19 7:02 |
| https://accounts.google.com/signin/v2/challenge/selection?se | Gmail | 1/4/19 7:02 |
| https://accounts.google.com/signin/v2/challenge/kpe?service | Gmail | 1/4/19 7:02 |
| https://accounts.google.co.za/accounts/SetSID?ssdc=1&sidt= | Gmail | 1/4/19 7:03 |
| https://accounts.youtube.com/accounts/SetSID?ssdc=1&sidt= | Gmail | 1/4/19 7:03 |
| https://mail.google.com/accounts/SetOSID?authuser=0&cont | Gmail | 1/4/19 7:03 |
| https://mail.google.com/mail/#inbox | Inbox (73) - salsadance1956@gmail.com - Gmail | 1/4/19 7:03 |
| https://mail.google.com/mail/#inbox/FMfcgxwBTsXZmrmZfZV | Norma is shy. Why don't you take the first step? 💌 - salsadan | 1/4/19 7:03 |
| https://www.lovoo.com/ | LOVOO - Online dating app for flirting, chatting, and getting to | 1/4/19 7:03 |
| https://www.lovoo.com/profile/5c257d5b9eeb81eac935868e | Norma, age 64, from Los Tamarindos, is looking for dates in Lo | 1/4/19 7:03 |
| http://email.mg.lovoo.com/c/eJx1UcluhDAM_Ro4opCQAAcOr | LOVOO - Online dating app for flirting, chatting, and getting to | 1/4/19 7:03 |
| https://app.adjust.com/jhymfi_e4d04u?deep_link=lovoo%3A% | LOVOO - Online dating app for flirting, chatting, and getting to | 1/4/19 7:03 |
| https://lovoo.com/profile/5c257d5b9eeb81eac935868e | LOVOO - Online dating app for flirting, chatting, and getting to | 1/4/19 7:03 |
| https://n62g.adj.st/profile/5c257d5b9eeb81eac935868e?adju | LOVOO - Online dating app for flirting, chatting, and getting to | 1/4/19 7:03 |
| https://www.google.com/url?q=http://email.mg.lovoo.com/c | LOVOO - Online dating app for flirting, chatting, and getting to | 1/4/19 7:03 |
| https://mail.google.com/mail/#inbox/FMfcgxwBTsgVMTjrnqV | Your Top Matches, David - salsadance1956@gmail.com - Gmai | 1/4/19 7:03 |
| http://seniorblackpeoplemeet.com/v3/convertprofile?SID=33 | SeniorBlackPeopleMeet.com - The Senior Black Dating Network | 1/4/19 7:04 |
| http://www.seniorblackpeoplemeet.com/v3/convertprofile?S | SeniorBlackPeopleMeet.com - The Senior Black Dating Network | 1/4/19 7:04 |
| https://www.google.com/url?q=http://SeniorBlackPeopleMee | SeniorBlackPeopleMeet.com - The Senior Black Dating Network | 1/4/19 7:04 |
| https://www.seniorblackpeoplemeet.com/v3/convertprofile?S | SeniorBlackPeopleMeet.com - The Senior Black Dating Network | 1/4/19 7:04 |

**Within the first hour of using Chrome they went to 120 different URLs, so wasting no time**

# WELL MAYBE WASTING A LITTLE BIT OF TIME

## Watched 2 YouTube Videos


Ellen Reveals She Called the Academy to Help Re-Hire Ke...
TheEllenShow

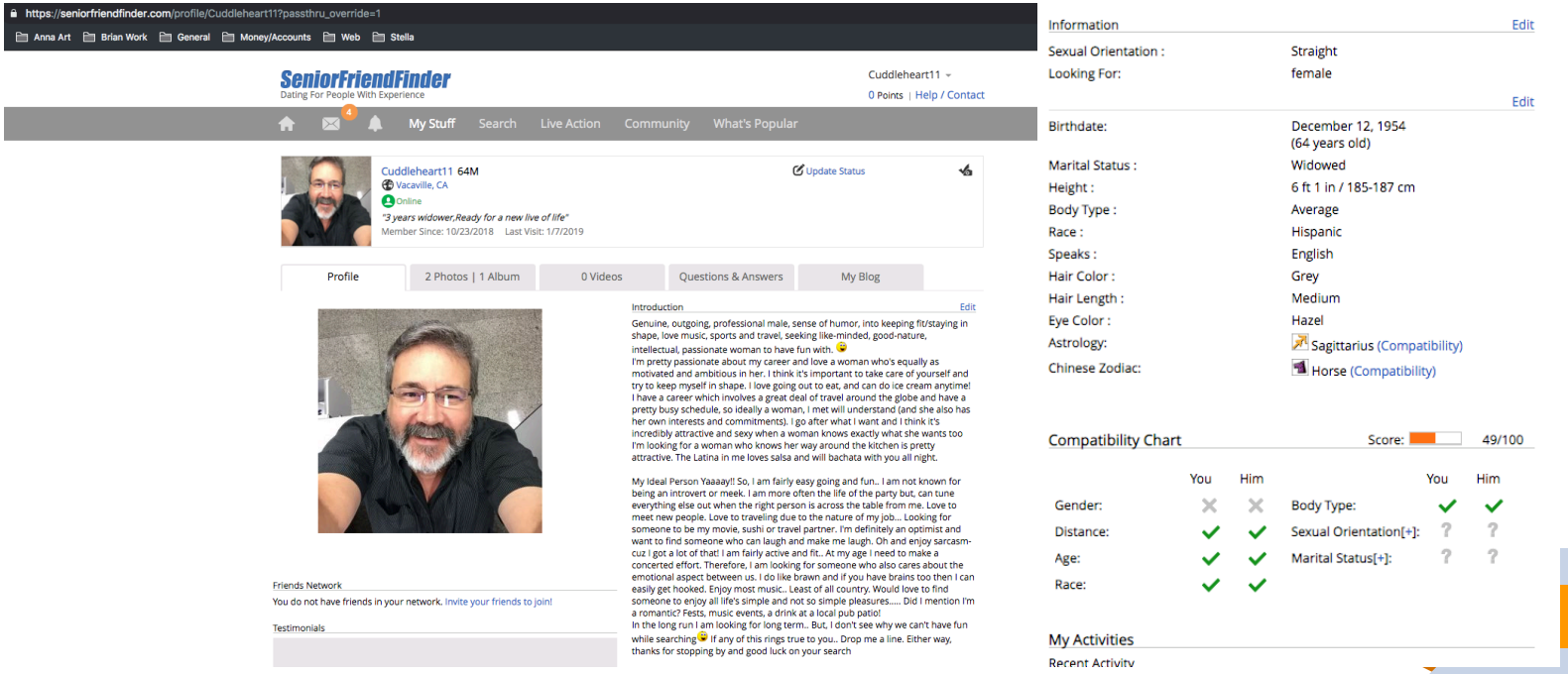

10 FAMILY FEUD US ANSWERS That Left STEVE HARVEY ...
YouTube · Bonus Round

# WEB HISTORY DEEP DIVE

- Signs into zoosk.com using Twitter SSO reveals two accounts:
  david101 and pickyman1954@gmail.com
- Signs into Gmail and elitesingles.com using salsadance1956@gmail.com
- Uses Google SSO to sign into LOVOO, C-Date, SeniorBlackPeopleMeet.com, Badoo, BlackPeopleMeet.com
- Signs into Yahoo mail using mary.jo15@yahoo.com
  - Web history also showed a password recovery for this account
- Chats with 148 people on Meetmindful.com

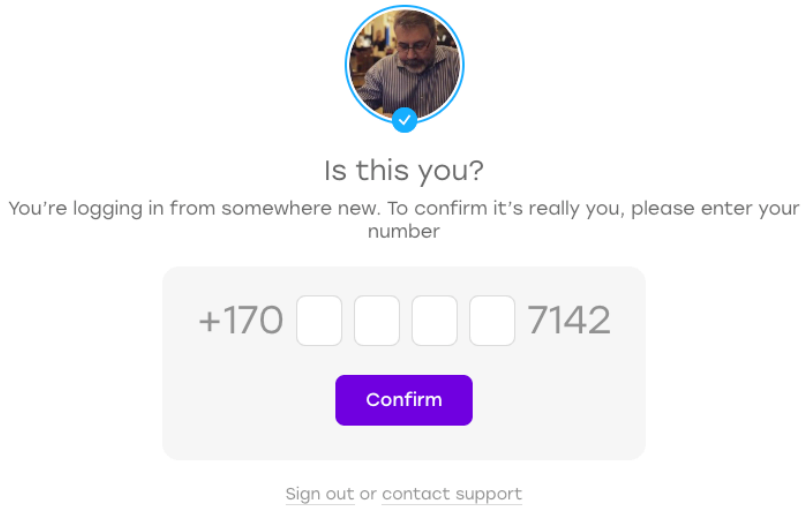
# AND MORE WEB HISTORY

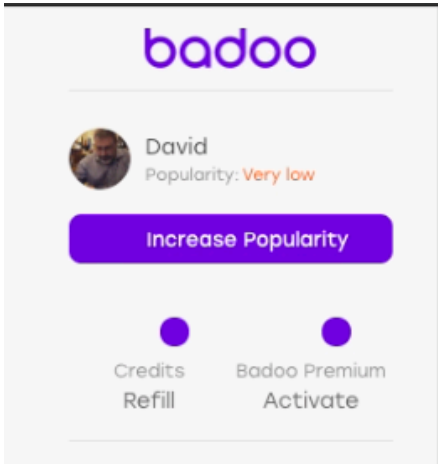
## Signs into a seniorfriendfinder.com account that is open



# AND EVEN MORE WEB HISTORY

## Signs into Badoo.com which again shows the profile info



# GOOGLE

## Started with a Google search for “pickyman1954@gmail.com” and got a hit!

SCAM SURVIVORS

Re: pickyman1954@gmail.com

Postby firefly » Thu Dec 27, 2018 6:27 pm

Additional email addresses reported online for being used in romance scams with stolen pictures from the same gallery:

- Waynell3194@gmail.com

- dan.burdell@gmail.com, danburdell@gmail.com - he was active on eHarmony.

There is a plethora of fake profile on various dating sites using the same stolen pictures or stolen pictures of the same person.

Stolen picture used:

On sugardaddyforme.com as:

Sugarrichhy
Someone to share real and new love with
52-year-old SugarDaddy
Austin, Texas, United States
Seeking SugarBaby 18 - 80
Personal Details
Marital Status: Divorced
Race: Caucasian
Income: More than $1,000,000
Body Type: Athletic
About Me:

On the same Wamba as:

Davidnathan
51 year, Taurus. Nigeria, Benin City

# DRAWING A CONCLUSION

- Seems like strange activity for a server, but this points to “catfishing”
  - The attacker is scamming a ton of woman via these online dating sites
  - Email addresses and images found in web history all point to dating scams
  - With the Mary Jo Yahoo account, they got her personal info including her phone number and then leveraged it to get into her Yahoo email account
- But why use an AWS Server
  - Clean IP Address
  - Not from a VPN which some dating sites may block

# Catfishing?

# Understanding Catfishing

- The term itself comes from *Catfish*, a 2010 movie that featured a man meeting a woman online before growing concerned about her true identity
- Definition is a fake or stolen online identity created or used for the purposes of beginning a deceptive relationship
- According to the FBI's Internet Crime Complaint Center (IC3) romance scams result in the highest amount of financial losses to victims when compared to other online crimes
  - In 2016, almost 15,000 complaints categorized as romance scams were reported to IC3 (nearly 2,500 more than the previous year), and the losses associated with those complaints exceeded $230 million

# 4

# Recommendations

# STRONG PASSWORDS

- Enforce strong passwords
  - There are many applications that still use local accounts so make sure they have the same requirements
- Password Dictionary
  - If haveibeenpwned.com currently has a database of 551,509,767 passwords then so do the bots that are running brute force attacks
  - Run your users passwords against a database to make sure these passwords are not being used

# GOLDEN IMAGE

- Most cloud providers make it easy to create and maintain images
  - The Amazon Machine Image service allows creation of reusable templates every time you spin up an EC2 instance
- Deploying a standard golden image allows for custom security controls and company applications to be installed, including security products
  - Knowing what comes installed by default allows for differential reporting

# OTHER RECOMMENDATIONS

- Keep RDP and SSH locked down
- Make sure that you are collecting events either with a third party tool or with cloud monitoring tools
- Once an incident occurs make sure there is a response plan and third party tools can help speed up gathering evidence

# CLOSING REMARKS

- All that sensitive data that I loaded on the server was not touched
  - Not all bad actors are trying to steal data
  - In my case I got a scammer that just wanted a clean work space
- Next time I might try to make the lab look more like a valuable target
  - I also took back control of my server pretty quickly, so it would have been interesting to leave them alone longer to see what they would have tried next

# THANKS!

**Any Question?**

You can find me at

https://www.linkedin.com/in/brianhileman/