THREAT HUNTING:
FROM PLATITUDES TO PRACTICAL APPLICATION

Neil " Grifter " Wyler – Senior Threat Hunting & Incident Response Specialist

RSA

NEW PRESENTATION, WHO DIS?

HUNTING

What is it?

- Proactively searching through data in order to detect threats which have evaded traditional security measures.

Is it effective?

- It’s often more effective than working incidents out of a queue. While traditional security programs are still important, hunting takes you to the next level.

HUNTING

Why hunt?

- Again, because it’s proactive.
  - Aren’t you tired of being purely reactive?
- It’s much harder to hide when someone is actively looking for you.
- It’s much harder to hide when someone knows their environment.
- By the way, you’ll know your environment better than you ever have before.
- It increases value to your organization.

WHERE DO WE BEGIN?

Log All the Things

- Collect logs from key areas
  - OS Event Logs
  - Application Logs
  - Know who is authenticating where, and at what level
- Don't forget your network
  - Web Server logs
  - Proxy logs
  - Full … Packet … Capture

This can be an incredible amount of data

- Big Data is a part of your life now
  - Start small and grow your collection as you grow your program

RSA

WHERE DO WE BEGIN?

Situational Awareness

- Understand what normal looks like on your hosts and network.
  - Create a baseline that you can diff against
- Become intimately aware of what the norms are so that when an anomaly occurs, it sticks out like a sore thumb.

Leave preconceived notions at the door

- Don't always start with an IOC. Start with a question.
  - If data was leaving my environment, where's the most likely place it would leave?

HUNTING MINDSET

Have a plan but be ready to adapt

- Know what you're looking for and go try to find it.
  - But don't be discouraged if/when you don't
- Remain flexible
  - Sometimes what you started searching for will take you down a completely different path.
- Prepare for pivots, there will be many
- Find tools that help you make sense of the data you've collected
- Document everything you're doing and what you've learned
  - Share it!

SO, WHAT NOW?

EXECUTING A HUNT

The Plan

- Provide Hunters /w Network Architecture / Diagrams
- Identify Potential Targets
  - Tie IP Addresses to Assets
  - Business Criticality
- Focus on Directionality
  - Inbound
  - Outbound
  - Lateral Movement
- Determine Hunting Timeframe
  - 24 hours on Average

EXECUTING A HUNT

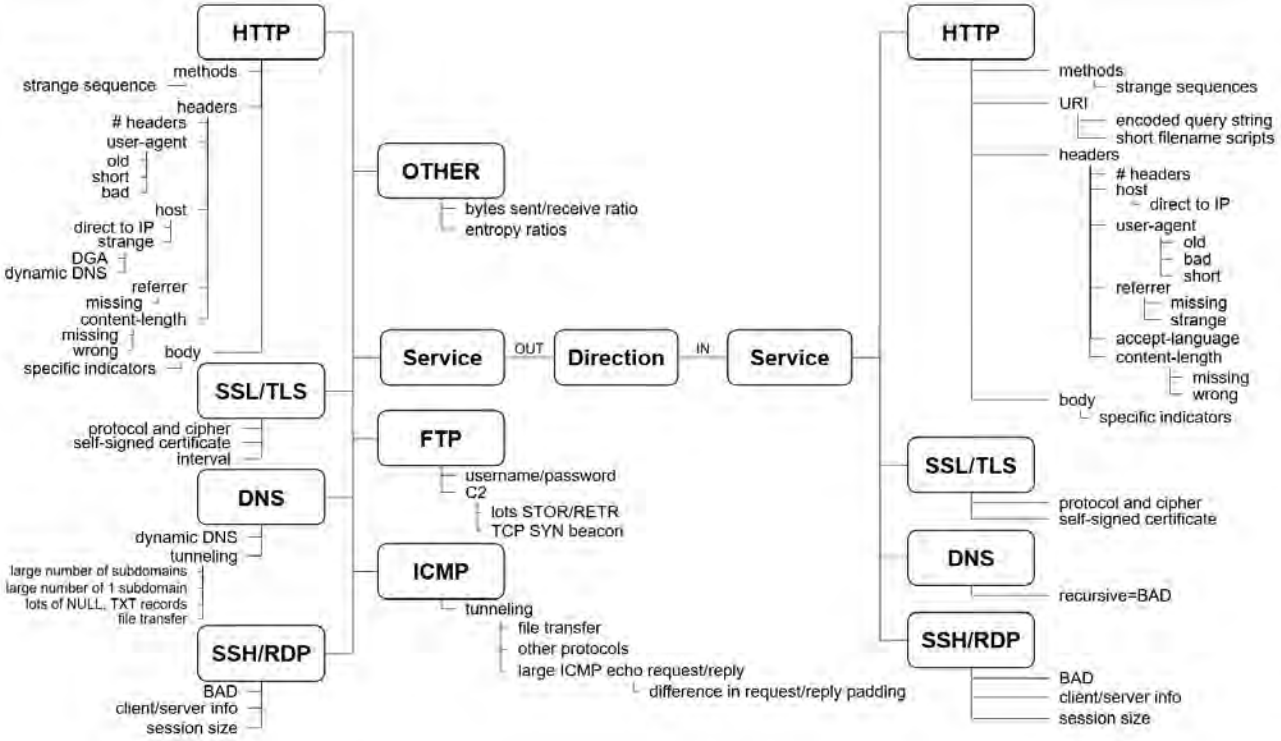
- Service Analysis
  - Begin with the Smallest (IRC, VNC, BITTORRENT, RPC, RDP)
    - Allows for Quick Elimination
    - Continue to Work Backwards
    - Document Area that Each Analyst Covered (Analyst 1 – Outbound/RDP, Outbound/IRC, etc)
- Drill Down on Each Selected Service
- Rinse and Repeat

EXECUTING A HUNT

Care and Feeding

- Investigate, Investigate, Eliminate
- Find the Signal in the Noise
  - Determine what traffic is causing false positives, and manage it.
  - As you tune and dial in your environment, actionable data will become increasingly apparent.
- Build reports and automate the pain away

THE LABYRINTH



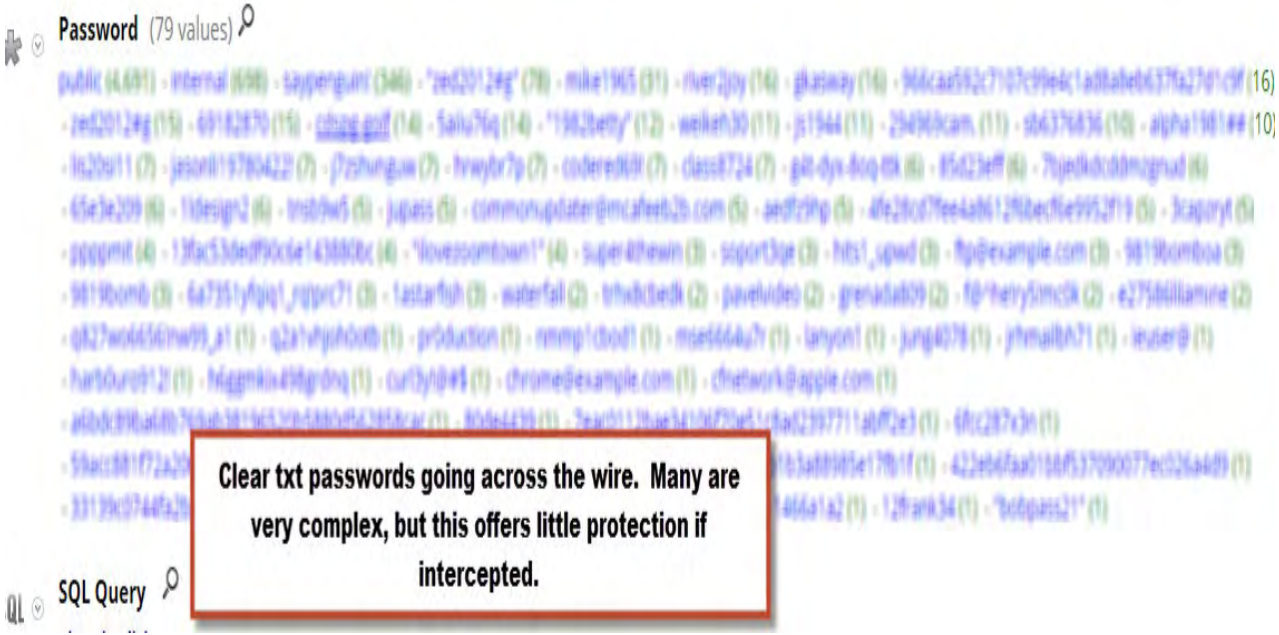
SO, WHAT DO WE FIND?

CLEARTEXT OR ENCRYPTED?

PERCENTAGE OF TRAFFIC ENCRYPTED – NO DECRYPTION

CLEARTEXT OR ENCRYPTED?

STRONG PASSWORDS OVER UNENCRYPTED TRANSPORTS?

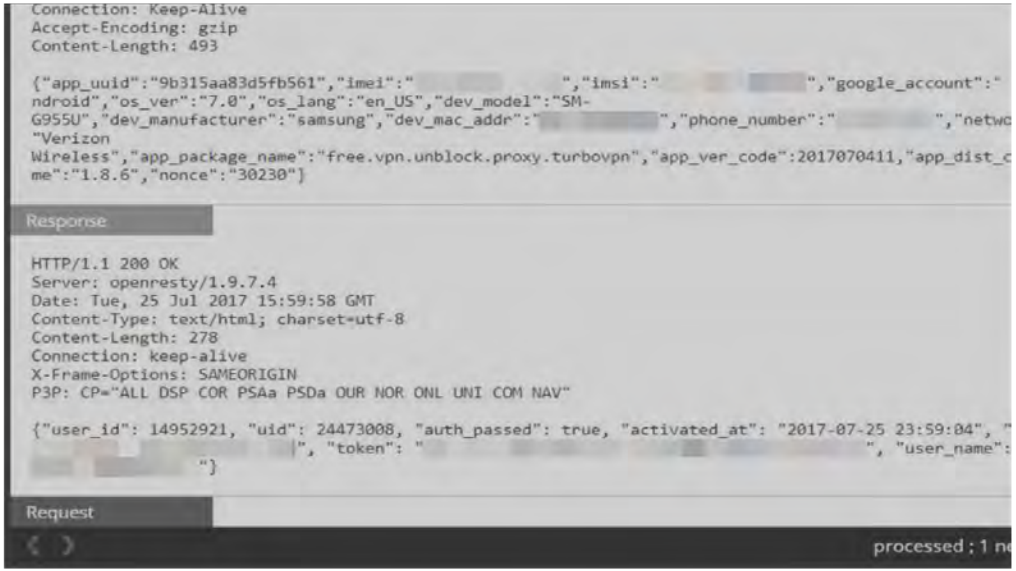


Clear txt passwords going across the wire. Many are very complex, but this offers little protection if intercepted.

CLEARTEXT OR ENCRYPTED?

WEBCAMS

ALWAYS USE A VPN!



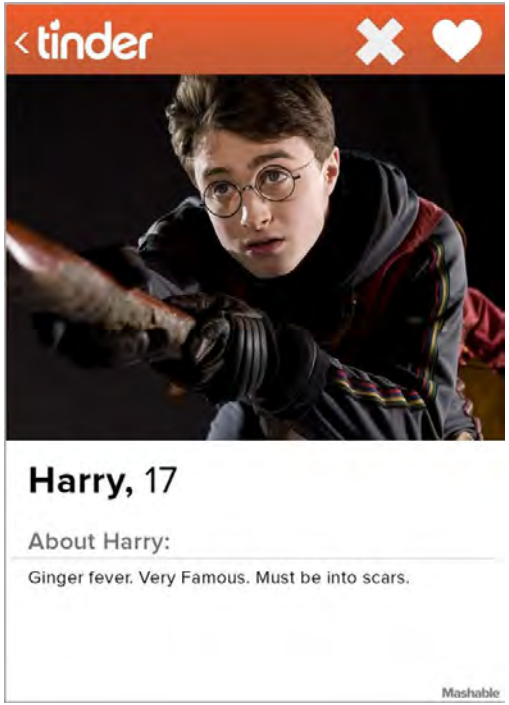
BIG FIX…OR BIG BROKEN?

- 4 different organizations
- Over 150 posts over the course of BH, including FULL system inventory with versions, process lists, registry keys …

```
321: ipv4 address
32m: 10.18.112.0
294m:
294i: application
294m: "AAH Updates Notifier.app" "9.0.0.281" "AAH Updates Notifier" "9.0.0.281" "Adobe Application Manager Updates Notifier 9.0.0.281, © 2009-2015 Adobe Systems Incorporated and its licensors. All rights reserved."
294m: "Calculator.app" "10.8" "Calculator" "10.8" "10.8, Copyright © 2001-2013, Apple Inc."
294m: "Calendar.app" "9.0" "Calendar" "9.0" ""
294m: "Adobe Reader.app" "11.0.23" "Adobe Reader" "11.0.23" "Adobe Reader X 11.0.23, ©1984-2012 Adobe Systems Incorporated. All rights reserved."
294m: "Microsoft Outlook.app" "16.13.1" "Microsoft Outlook" "16.13.1" "16.13.1 (180523 :4), © 2018 Microsoft Corporation. All rights reserved."
294m: "Microsoft Word.app" "16.13.1" "Microsoft Word" "16.13.1" "16.13.1 (180523 :4), © 2018 Microsoft Corporation. All rights reserved."
294m: "Microsoft OneNote.app" "16.13.1" "Microsoft OneNote" "16.13.1" "16.13.1 (180523 :4), © 2018 Microsoft Corporation. All rights reserved."
294m: "HipChat.app" "4.30.1" "HipChat" "4.30.1" "Copyright © 2015 Atlassian. All rights reserved."
294m: "WhatsApp.app" "0.3.1649" "WhatsApp" "0.3.1649" ""
294m: "Google Chrome.app" "70.0.3538.110" "Google Chrome" "70.0.3538.110" ""
294m: "System Preferences.app" "14.0" "System Preferences" "14.0" ""
294m: "About This Mac.app" "1.0" "About This Mac" "1.0" "Copyright © 2016 Apple Inc. All rights reserved."
294m: "Skype.app" "8.34" "Skype" "8.34" ""
294m: "Microsoft Teams.app" "1.00.129053" "Microsoft Teams" "1.00.129053" "1.00.129053"
294m: "Microsoft PowerPoint.app" "16.13.1" "Microsoft PowerPoint" "16.13.1" "16.13.1 (180523 :4), © 2018 Microsoft Corporation. All rights reserved."
294m: "Microsoft Excel.app" "16.13.1" "Microsoft Excel" "16.13.1" "16.13.1 (180523 :4), © 2018 Microsoft Corporation. All rights reserved."
294m: "Skype for Business.app" "16.17.65" "Skype for Business" "16.17.65" ""
294m: "Captive Network Assistant.app" "4.0" "Captive Network Assistant" "4.0" ""
294m: "Sublime Text.app" "Build 3176" "Sublime Text" "Build 3176" "Copyright © 2006-2018 Sublime HQ Pty Ltd"
294m: "Preview.app" "9.0" "Preview" "9.0" "9.0, Copyright 2002-2016 Apple Inc."
294m: "OmniGraffle.app" "6.6.2" "OmniGraffle" "6.6.2" "OmniGraffle 6.6.2, version 169.23.0.276662, Copyright 2000-2017 The Omni Group"
294m: "CCXProcess.app" "1.4.1" "CCXProcess" "1.4.1" "Copyright 2015-2016 Adobe Systems Incorporated. All rights reserved."
294m: "Core Sync.app" "2.5.0.197" "Core Sync" "2.5.0.197" "Copyright © 2001-2016, Adobe Systems Incorporated. All rights reserved."
294m: "Adobe Desktop Service.app" "3.9" "Adobe Desktop Service" "3.9" "Copyright 2013-2016 Adobe Systems Incorporated. All rights reserved."
294m: "Spotify.app" "1.0.93.244.g1e3a05e7" "Spotify" "1.0.93.244.g1e3a05e7" ""
294m: "GlobalMeet Guest Desktop.app" "3.9.4" "GlobalMeet Guest Desktop" "3.9.4" "3.9.4,"
294m: "ESET Endpoint Antivirus.app" "6.4.168.0" "ESET Endpoint Antivirus" "6.4.168.0" ""(C) 2017 ESET, spol. s r. o.""
294m: "Cisco Webex Meetings.app" "33.6.4.15" "Cisco Webex Meetings" "33.6.4.15" "© 2018 Cisco and/or its affiliates. All rights reserved."
294m: "Cisco AnyConnect Secure Mobility Client.app" "4.5.1044" "Cisco AnyConnect Secure Mobility Client" "4.5.1044" "Copyright (c) 2017 Cisco Systems, Inc."
294m: "Hate Translate.app" "5.1.2" "Hate Translate" "5.1.2" "Copyright © 2015 Andrii Liakh. All rights reserved."
294m: "Archive Utility.app" "81.0" "Archive Utility" "81.0" "© 2003-2014 Apple Inc. All Rights Reserved."
294m: "App Store.app" "2.2.1" "App Store" "2.2.1" ""
294m: "VMware Fusion.app" "8.5.10" "VMware Fusion" "8.5.10" "Copyright © 1998-2018 VMware, Inc."
294m: "TextEdit.app" "1.12" "TextEdit" "1.12" "Copyright © 1995-2016, Apple Inc.%0aAll rights reserved."
294m: "WebExPluginAgent.app" "33.4" "WebExPluginAgent" "33.4" "© 2018 Cisco and/or its affiliates. All rights reserved."
294m: "Maps.app" "2.0" "Maps" "2.0" "Copyright © 2012-2016 Apple Inc.\nAll rights reserved."
294m: "Path Finder.app" "7.3.3" "Path Finder" "7.3.3" "Path Finder 7.3.3 - Copyright © 2001-2016, Cocoatech"
294m: "Meeting Center.app" "" "Meeting Center" "" ""
294m: "Moom.app" "3.2.6" "Moom" "3.2.6" "© 2011-2016 Many Tricks"
294m: "AdobeGCClient.app" "6.1.0.91" "AdobeGCClient" "6.1.0.91" ""
294m: "Adobe Flash Player Install Manager.app" "31.0.0.153" "Adobe Flash Player Install Manager" "31.0.0.153" ""
294m: "Windows Contacts - Windows 7 x64 - Mandiant.app" "VMware Fusion 8.5.10" "Windows Contacts - Windows 7 x64 - Mandiant" "VMware Fusion 8.5.10" "Windows 10 x64 - Mandiant%0ac:/program files/windows mail/wab.exe"
294m: "Windows Media Player - Windows 7 x64 - Mandiant.app" "VMware Fusion 8.5.10" "Windows Media Player - Windows 7 x64 - Mandiant" "VMware Fusion 8.5.10" "Windows 10 x64 - Mandiant%0ac:/program files (x86)/windows media player/wmplay
294m: "Microsoft Office 2013 - Windows 7 x64 - Mandiant.app" "VMware Fusion 8.5.10" "Microsoft Office 2013 - Windows 7 x64 - Mandiant" "VMware Fusion 8.5.10" "Windows 10 x64 - Mandiant%0ac:/program files/microsoft office/office15/proto
294m: "Support exe for Internet Printing - Windows 7 x64 - Mandiant.app" "VMware Fusion 8.5.10" "Support exe for Internet Printing - Windows 7 x64 - Mandiant" "VMware Fusion 8.5.10" "Windows 10 x64 - Mandiant%0ac:/windows/system32/wpng
294m: "Java(TM) Web Start Launcher 3 - Windows 7 x64 - Mandiant.app" "VMware Fusion 8.5.10" "Java(TM) Web Start Launcher 3 - Windows 7 x64 - Mandiant" "VMware Fusion 8.5.10" "Windows 10 x64 - Mandiant%0ac:/program files (x86)/java/jre1
294m: "PrintBrm Application - Windows 7 x64 - Mandiant.app" "VMware Fusion 8.5.10" "PrintBrm Application - Windows 7 x64 - Mandiant" "VMware Fusion 8.5.10" "Windows 10 x64 - Mandiant%0ac:/windows/system32/printbrmui.exe"
294m: "Windows Wordpad Application - Windows 7 x64 - Mandiant.app" "VMware Fusion 8.5.10" "Windows Wordpad Application - Windows 7 x64 - Mandiant" "VMware Fusion 8.5.10" "Windows 10 x64 - Mandiant%0ac:/program files/windows nt/accessor
294m: "Paint - Windows 7 x64 - Mandiant.app" "VMware Fusion 8.5.10" "Paint - Windows 7 x64 - Mandiant" "VMware Fusion 8.5.10" "Windows 10 x64 - Mandiant%0ac:/windows/system32/mspaint.exe"
294m: "IME search module - Windows 7 x64 - Mandiant.app" "VMware Fusion 8.5.10" "IME search module - Windows 7 x64 - Mandiant" "VMware Fusion 8.5.10" "Windows 10 x64 - Mandiant%0ac:/windows/system32/ime/shared/imesearch.exe"
294m: "Windows® Installer - Windows 7 x64 - Mandiant.app" "VMware Fusion 8.5.10" "Windows® Installer - Windows 7 x64 - Mandiant" "VMware Fusion 8.5.10" "Windows 10 x64 - Mandiant%0ac:/windows/system32/msiexec.exe"
294m: "Wireshark - Windows 10 x64 - Mandiant.app" "VMware Fusion 8.5.10" "Wireshark - Windows 10 x64 - Mandiant" "VMware Fusion 8.5.10" "Windows 10 x64 - Mandiant%0ac:/program files/wireshark/wireshark.exe"
294m: "Microsoft Application Compatibility Manager - Windows 7 x64 - Mandiant.app" "VMware Fusion 8.5.10" "Microsoft Application Compatibility Manager - Windows 7 x64 - Mandiant" "VMware Fusion 8.5.10" "Windows 10 x64 - Mandiant%0ac:/p
application compatibility toolkit/application compatibility manager/acm.exe"
```


RSA

THE RSAC DATING POOL



ALL THINGS ARE NOT CONFIGURED EQUALLY

[redacted]: 12:30AM: Arrive SFO Signature Flight Support
12:30AM: Five Emerald Limo (*confirmation [redacted]) will p/u and take [redacted] to the SF Four Seasons (conf. # [redacted])
1:00AM: Arrive at Four Season, ([redacted] will be pre-registered)

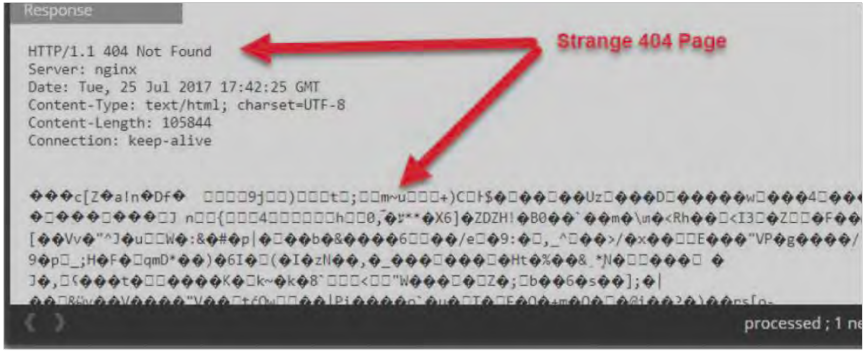
10:45AM: Five Emerald (conf.# [redacted]) will p/u [redacted] at Four Seasons and take to Moscone West (This is actually the loading dock entrance on Howard St. between 4th and 5th St. I will meet the car as it comes down the ramp)
11:10AM-11:30AM: Blocking Rehearsal
11:30AM -12:45: Lunch/relax in private dressing room
1:00PM-1:45 PM: [redacted] presentation
1:55PM-2:15PM: Photo Op
2:20PM: Five Emerald (conf. # [redacted]) will p/u [redacted] and take to SFO (Signature Flight Support)
3:00PM: Flight Leaves SFO ([redacted])
11:30PM: Arrive at [redacted]

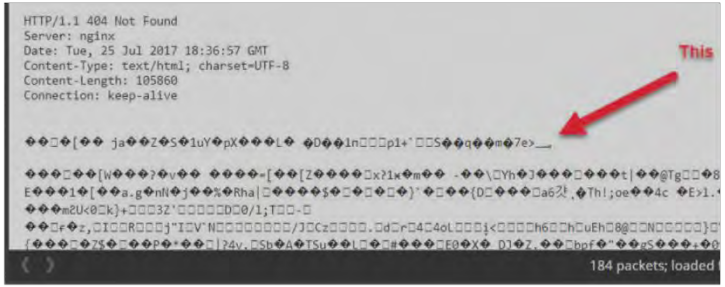
PATCH MANAGEMENT

Top 10 Websites / Concentrator

	Hostname Aliases	Total session size in bytes
1	au.download.windowsupdate.com	145.39 GB
2	au.b1.download.windowsupdate.com	79.81 GB
3	2.tlu.dl.delivery.mp.microsoft.com	77.75 GB
4	archive-7.kali.org	77.43 GB
5	download.windowsupdate.com	62.87 GB
6	iosapps.itunes.apple.com	57.03 GB
7	3.tlu.dl.delivery.mp.microsoft.com	46.54 GB
8	7.tlu.dl.delivery.mp.microsoft.com	44.52 GB
9	us.archive.ubuntu.com	35.49 GB
10	officecdn.microsoft.com	25.15 GB

ZERO DAY, O -DAY OR SAME DAY?





LUXO RF

Event Reconstruction

service	id	type	source	destination	service	first packet time
rsa-bh-pcon.none - Concentrator	3742619	Network Session	172.16.31.3 : 49815	192.186.157.43 : 6667	6667	2016-07-30T14:58:56.696

Request & Response | Top To Bottom | View Text | Actions | Open Event in New Tab | Cancel

Request

```
WHO ##stuffedninja
```

Response

```
:tepper.freenode.net 352 m1m ##stuffedninja ~math_aeta unaffiliated/mimatas tepper.freenode.net m1m H@ :0 New Now Know How
:tepper.freenode.net 352 m1m ##stuffedninja ~s7oneghos pdpc/supporter/active/s7oneghos7 sendak.freenode.net s7oneghos7 H@ :0 s7oneghos7
:tepper.freenode.net 352 m1m ##stuffedninja 424b2611 gateway/web/freenode/ip.66.75.38.17 herbert.freenode.net peacefrogturtle H@ :0
cpe-66-75-38-17.san.res.rr.com/66.75.38.17
:tepper.freenode.net 352 m1m ##stuffedninja ChanServ services. services. ChanServ H@ :0 Channel Services
:tepper.freenode.net 315 m1m ##stuffedninja :End of /WHO list.
```

Request

```
PING :ALIVECHECK
```

Response

```
:tepper.freenode.net PONG tepper.freenode.net :ALIVECHECK
```

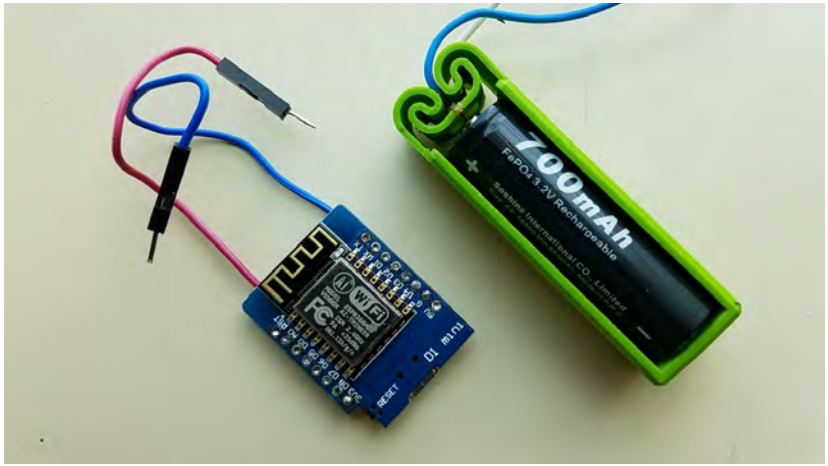
Request

```
PRIVMSG ##stuffedninja :s7oneghos7: do you still have that RF pager script?
PRIVMSG ##stuffedninja :rotoruter has a HackRF now as well
PRIVMSG ##stuffedninja :I'm thinking it might be worth trying it out at the luxor
```

14 packets; loaded from cache | Show Reconstruction Log

RSA

“DEVICES”



Thank You

Neil “ Grifter ” Wyler
@grifter801

RSA