RSAConference2019
Asia Pacific & Japan

Singapore | 16–18 July | Marina Bay Sands

BETTER.

SESSION ID: SDS-R01

Observing Real-World Carnage: Deconstructing Attacks on Critical Assets

Sharat Nautiyal

Senior Cybersecurity Solutions Architect
ExtraHop

#RSAC

RSAConference2019
Asia Pacific & Japan

- Identifying & Prioritising Your Critical Assets
- Digital Epidemiology
- Real-World Attack Examples
- Key Takeaways

RSAConference2019
Asia Pacific & Japan

- **Identifying & Prioritising Your Critical Assets**
- **Digital Epidemiology**
- **Real-World Attack Examples**
- **Key Takeaways**

Critical Assets

What are your organisation's critical assets? How do you prioritise them?

- E-Ticketing Systems
- Customer Self-Service Portals
- Consumer/Corporate Online Banking
- Mobile Services
- Payment Gateways
- EHR/Patient Record Systems
- IoT/Medical Devices
- Payment/Billing Systems

- CRM
- ERP
- Retail Store Applications: POS
- 3rd Party Partner Interfaces
- Interbank Payment Systems
- Trading Systems
- ATM Systems

- DNS Servers
- Storage Servers
- Databases
- Active Directory
- Radius/Diameter Servers
- Email
- Legacy Mainframes

What are your organisation’s critical assets? How do you prioritise them?

- Most of the critical assets are deep in the network
- Yet, more resources are spent protecting north south and less focus on security controls in east west
- Cloud deployments, BYOD, IoT have made critical assets more vulnerable than ever
- Never loose sight of your key critical assets. Understand their asset value and choose relevant security controls.

RSAConference2019
Asia Pacific & Japan

- Identifying & Prioritising Your Critical Assets
- Digital Epidemiology
- Real-World Attack Examples
- Key Takeaways

Digital Epidemiology: Focused Visibility on Critical Assets

1. Obtain situational awareness for all critical assets
   - Know the types of systems that critical credentials should be accessing
   - Know the methods that users connect to your environment
   - Understand what ports, protocols and peers are acceptable for your critical systems
2. Surface anomalies and deviations from typical behavior
   - Alert on non-human transaction rates
   - Be aware of new ports, protocols and peers
3. Move beyond "treating symptoms": Build out surveillance of critical control points
   - Endpoint solutions
   - Logging and machine data
   - Network traffic analysis

Typical Tools for Surveillance/Digital Epidemiology

Endpoint Detection and Response (EDR)

Log Analysis with SIEM

Network Detection and Response (NDR)

Typical Tools for Surveillance/Digital Epidemiology

- Endpoint (EDR)
- Log Analysis (SIEM)
- Network (NDR)

Pros

- Telemetry & Information about specific system
- Data often closest to root cause

Challenges

- Dependent on Self-Reported data
- System Overhead Concerns
- Compatibility Issues: MacOS, Linux, Kernel Version, Legacy Systems
- Not installable on everything: IoT, BYOD, Appliances, External APIs
- Visibility starts with knowing where to install EDRs

Typical Tools for Surveillance/Digital Epidemiology

- Endpoint (EDR)
- **Log Analysis (SIEM)**
- Network (NDR)

Pros

- SIEM space is a mature industry and technology
- Can deliver transactional details (discrete actions and context)
- Often the “source of truth” for Compliance

Challenges

- Dependent on self-reporting
- Can be stunningly expensive: license & storage
- Disparate data source: has to be mashed up with other data
- Potential overhead concerns
- Must be configured and managed
- Purpose-built for archiving

Typical Tools for Surveillance/Digital Epidemiology

Endpoint (EDR)

Log Analysis (SIEM)

Network (NDR)

Pros

- Less deployment friction (agentless)
- Only prerequisite is an IP Address (Federated Visibility)
- Full accountability for all systems/all transactions/all credentials
- Visibility into encrypted channels

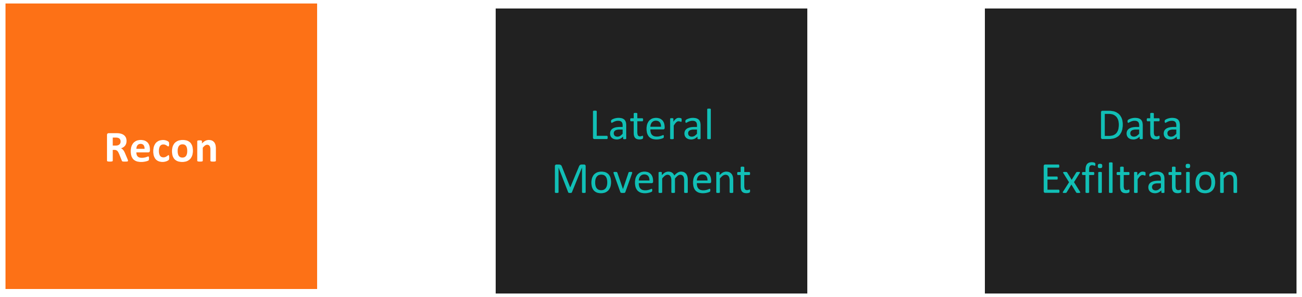
Challenges

- Requires network tap/SPANs (can be expensive)
- Limited to what is on the network
- Most NDR solutions do not provide full encrypted payload analysis

- Identifying & Prioritising Your Critical Assets
- Digital Epidemiology
- Real-World Attack Examples
- Key Takeaways

Deconstructing Real-World Attacks: Reconnaissance

- Reconnaissance - step to obtain information
- Guest computers, mobile devices, IoT devices etc are now being used to run scans and exploit
- BYOD devices are not just the one used by your employees but also by guests users
- They can be used to gather intelligence: OS, make and model, software version, open ports on connected devices



Recon

Lateral Movement

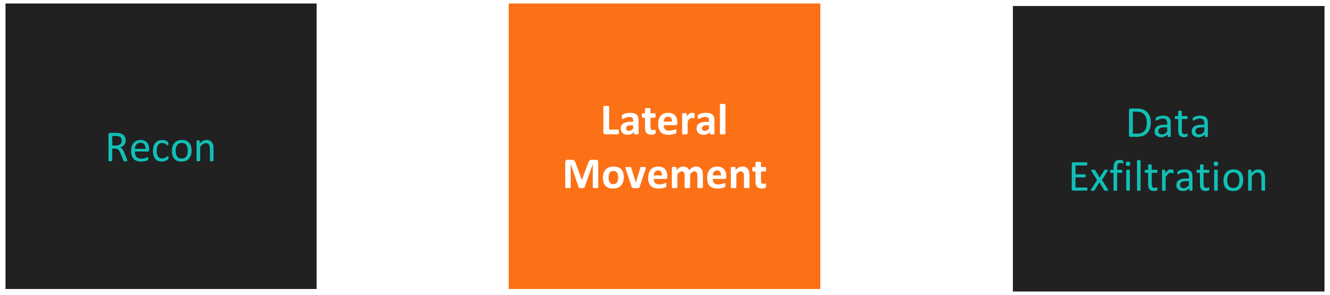
Data Exfiltration

Deconstructing Real-World Attacks: Lateral Movement

- Lateral movement - east - west movement in the network.

Typical techniques

- Service Account Abuse
- Brute Force via Kerberos/LDAP
- PSExec
- CIFS Shares
- New Peers
- New Protocols (new use of SSH, FTP, etc.)
- Uploading Webshells
- SSH Brute Force
- DNS Tunneling



Recon

Lateral Movement

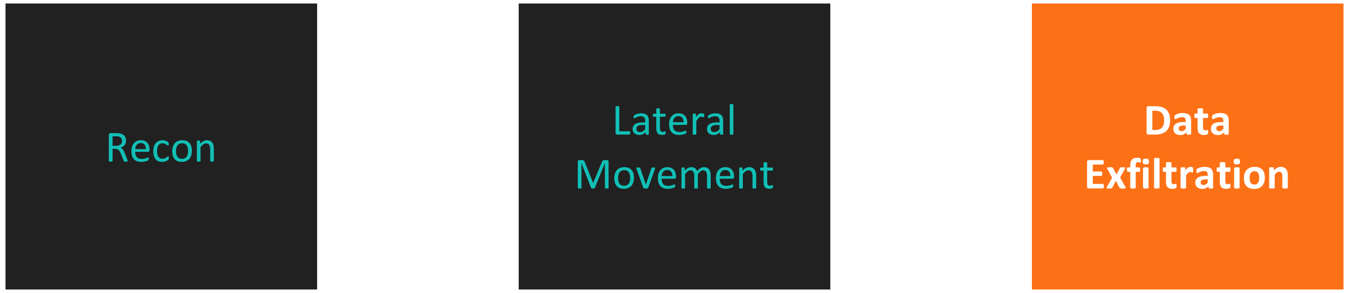
Data Exfiltration

Deconstructing Real-World Attacks: Data Exfiltration

- Data Exfil - unauthorized data movement

Typical techniques

- Encrypted channels
- Use of Let’s Encrypt (Cerbot)-derived certificates
- Several odd ports (Non-443)
- Open ports (HTTP/SSL/SMTP/etc.)
- DNS exfiltration via tunneling
- ICMP exfiltration (IoT Device)
- Port knocking (SANS PORTKnockOut)
- Exfiltration via dozens and in some cases, hundreds of ports



Recon

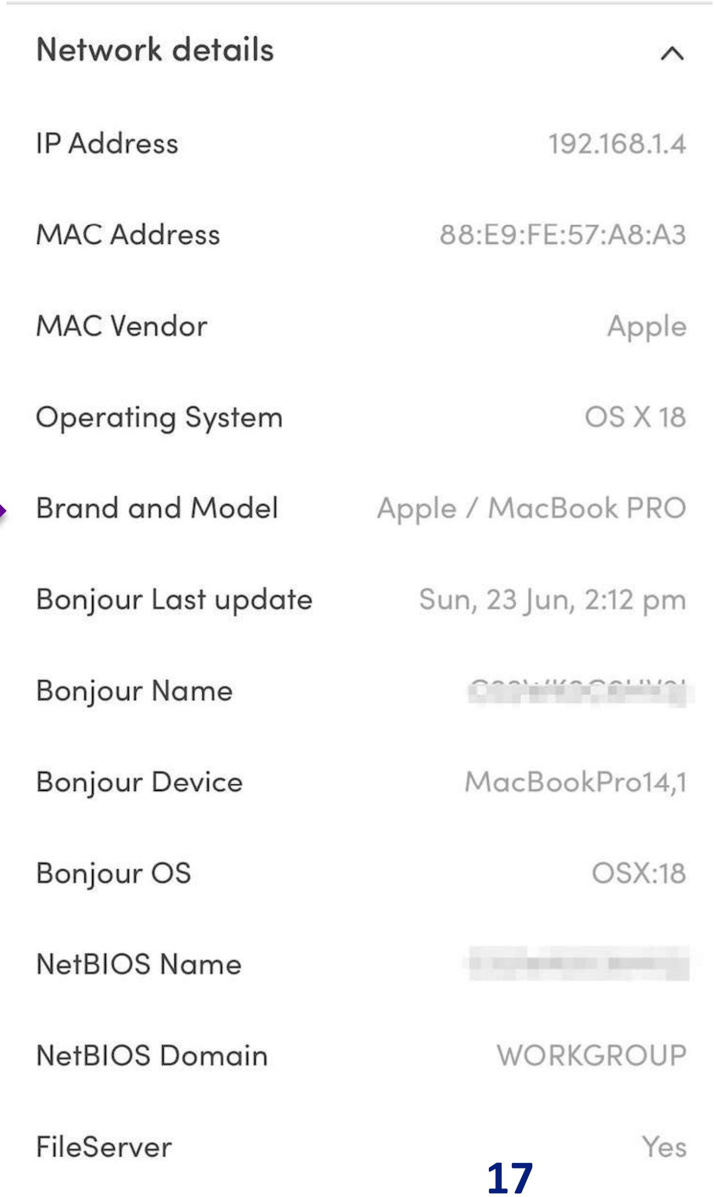
Lateral Movement

Data Exfiltration

Deconstructing Real-World Attacks: BYOD Menace

Free mobile App

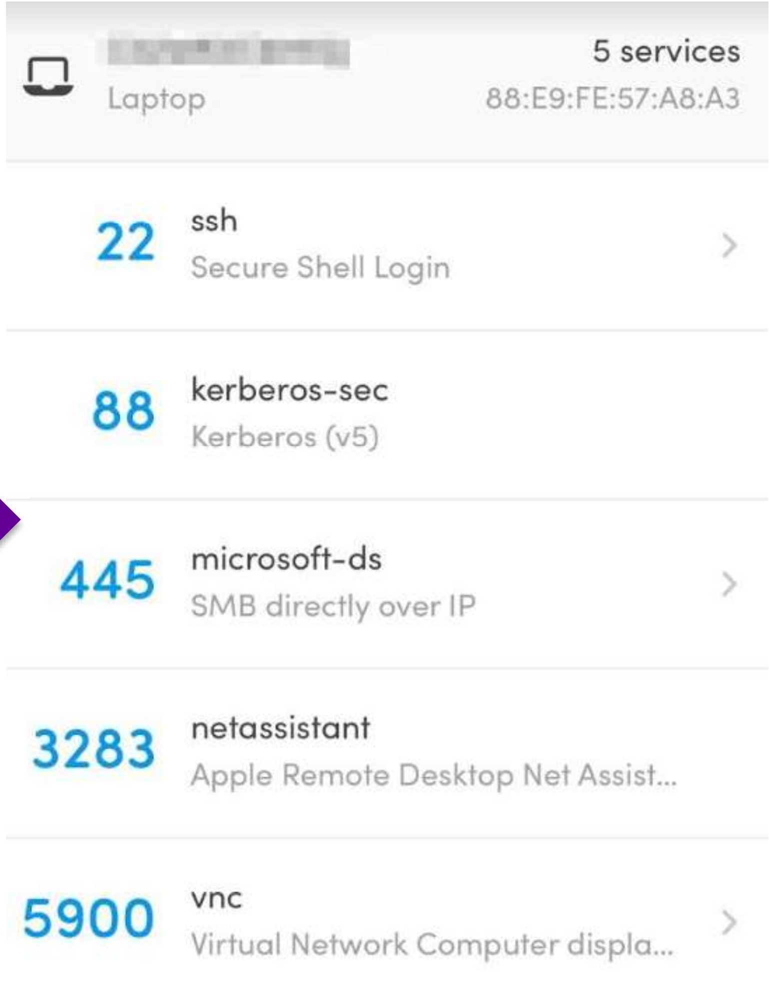
Reconnaissance



Network details

IP Address	192.168.1.4
MAC Address	88:E9:FE:57:A8:A3
MAC Vendor	Apple
Operating System	OS X 18
Brand and Model	Apple / MacBook PRO
Bonjour Last update	Sun, 23 Jun, 2:12 pm
Bonjour Name	[redacted]
Bonjour Device	MacBookPro14,1
Bonjour OS	OSX:18
NetBIOS Name	[redacted]
NetBIOS Domain	WORKGROUP
FileServer	Yes

Port Scan



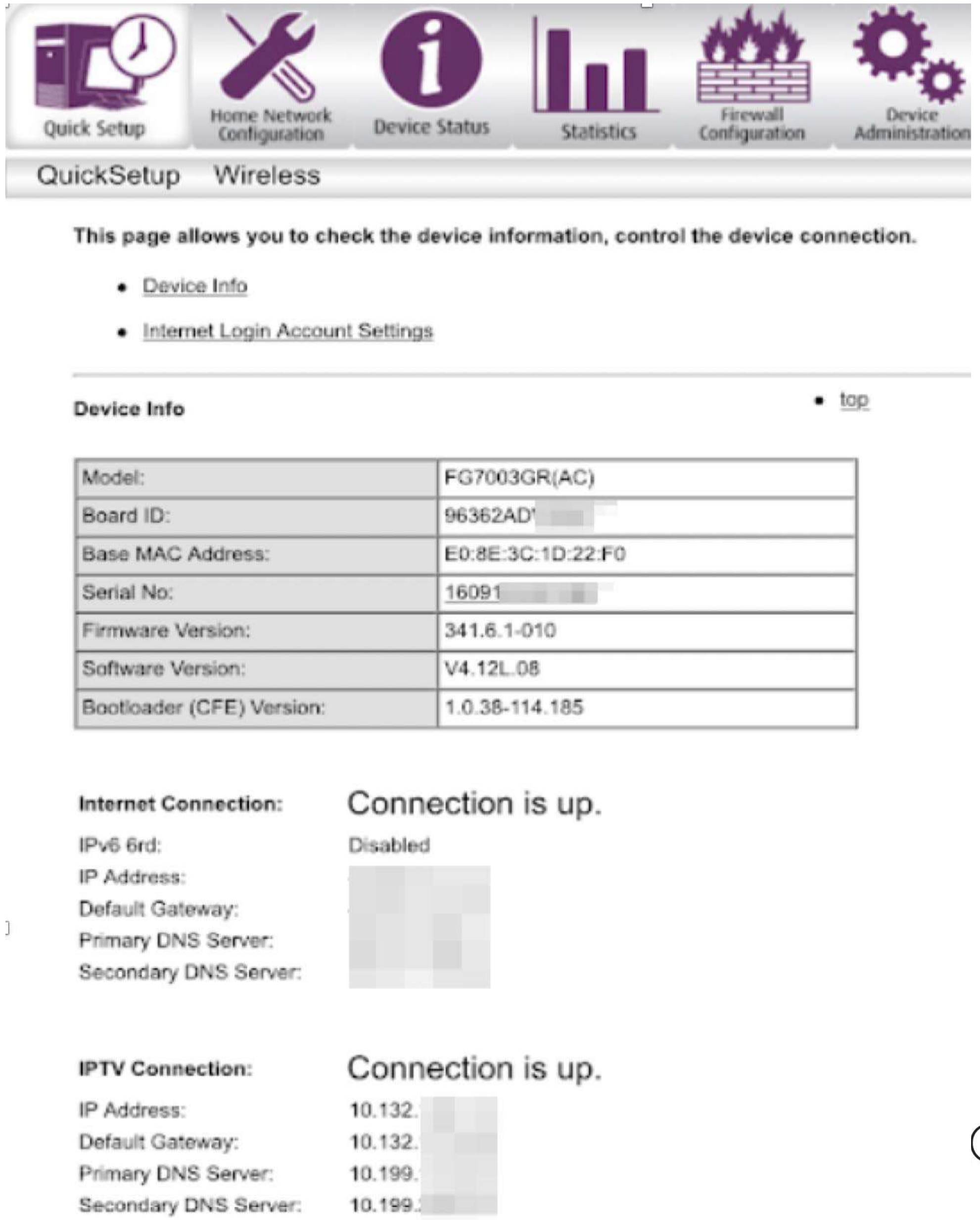
[redacted] 5 services
Laptop 88:E9:FE:57:A8:A3

22	ssh	Secure Shell Login
88	kerberos-sec	Kerberos (v5)
445	microsoft-ds	SMB directly over IP
3283	netassistant	Apple Remote Desktop Net Assist...
5900	vnc	Virtual Network Computer displa...

Deconstructing Real-World Attacks: BYOD Menace

- Easy access to device information from an app running on mobile devices.

- An unsophisticated threat actor also can now fiddle with device settings and at the least cause DOS.



This page allows you to check the device information, control the device connection.

- Device Info
- Internet Login Account Settings

Device Info

- top

Model:	FG7003GR(AC)
Board ID:	96362AD'[redacted]
Base MAC Address:	E0:8E:3C:1D:22:F0
Serial No:	16091[redacted]
Firmware Version:	341.6.1-010
Software Version:	V4.12L.08
Bootloader (CFE) Version:	1.0.38-114.185

Internet Connection: Connection is up.

IPv6 6rd: Disabled
IP Address: [redacted]
Default Gateway:
Primary DNS Server:
Secondary DNS Server:

IPTV Connection: Connection is up.

IP Address: 10.132.[redacted]
Default Gateway: 10.132.
Primary DNS Server: 10.199.
Secondary DNS Server: 10.199.

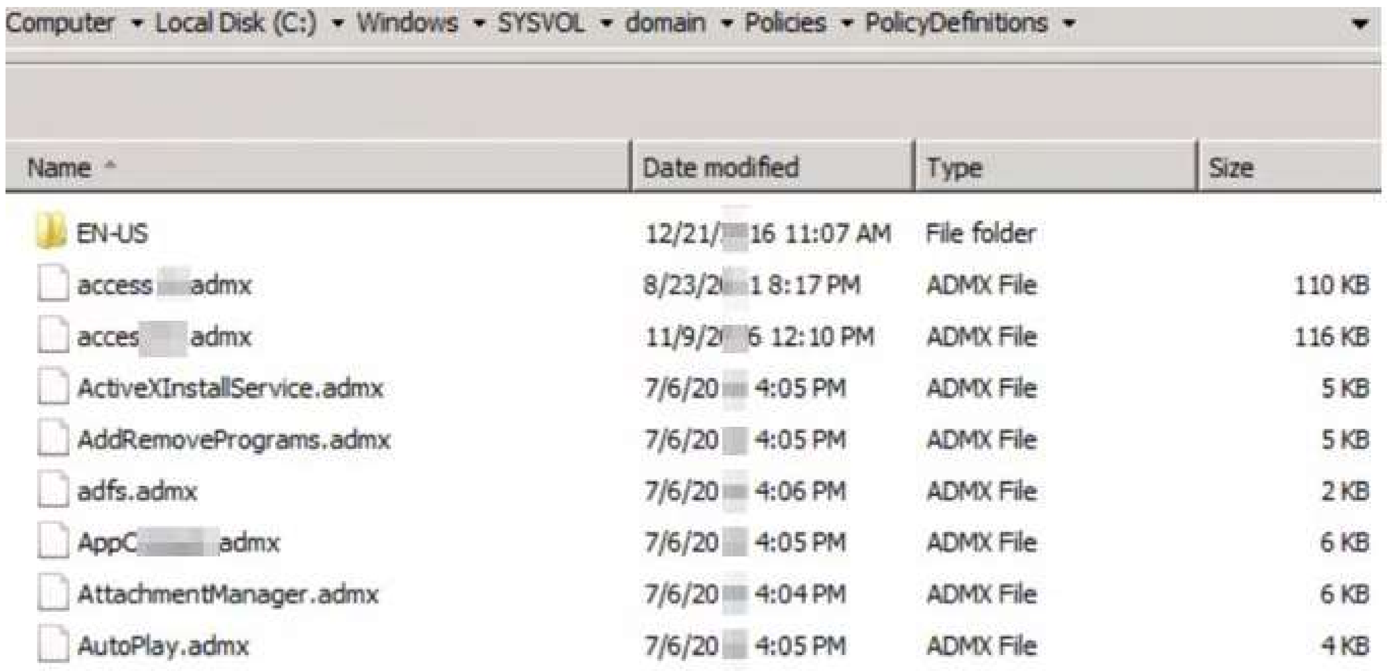
Deconstructing Real-World Attacks: Rogue Domain Controller Exploiting via Lateral Movement

- Anomalous activities on Domain Controller server
- Malware spreading via Domain Controller (SysVol) to the end users
- Any user connecting to Domain Controller was impacted
- Domain Controller attempting lateral movement to internal database servers

Impact

Data exfil with over 20+ connections to unauthorized IP Address via NTP

Sample SysVol



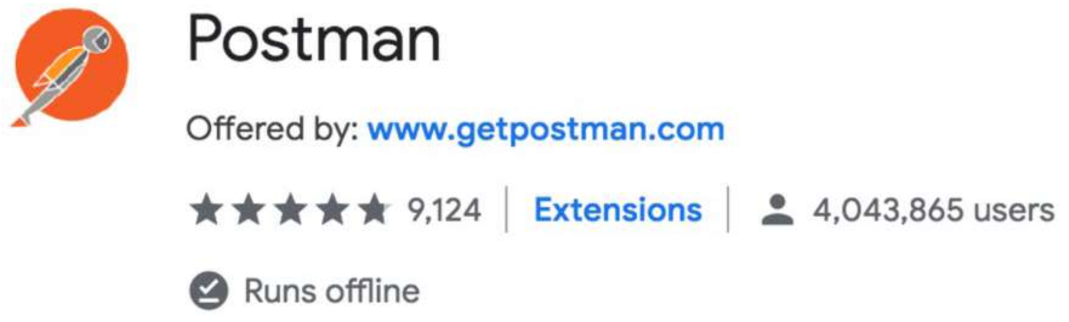
Computer ▸ Local Disk (C:) ▸ Windows ▸ SYSVOL ▸ domain ▸ Policies ▸ PolicyDefinitions ▸

Name	Date modified	Type	Size
EN-US	12/21/[redacted]16 11:07 AM	File folder	
access[redacted]admx	8/23/2[redacted]1 8:17 PM	ADMX File	110 KB
acces[redacted]admx	11/9/2[redacted]6 12:10 PM	ADMX File	116 KB
ActiveXInstallService.admx	7/6/20[redacted] 4:05 PM	ADMX File	5 KB
AddRemovePrograms.admx	7/6/20[redacted] 4:05 PM	ADMX File	5 KB
adfs.admx	7/6/20[redacted] 4:06 PM	ADMX File	2 KB
AppC[redacted]admx	7/6/20[redacted] 4:05 PM	ADMX File	6 KB
AttachmentManager.admx	7/6/20[redacted] 4:04 PM	ADMX File	6 KB
AutoPlay.admx	7/6/20[redacted] 4:05 PM	ADMX File	4 KB

Deconstructing Real-World Attacks: Fake Extensions/Apps

- Watch out for fake websites, authentication pages, extensions
- Example: 2 extensions in the Chrome Extension store with the same name of a popular API development environment

Original Extension



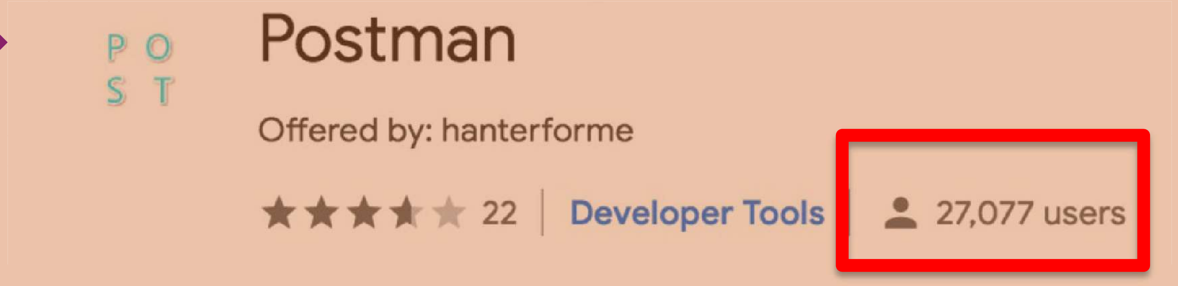
Postman

Offered by: www.getpostman.com

★★★★★ 9,124 | Extensions | 4,043,865 users

Runs offline

Fake Extension



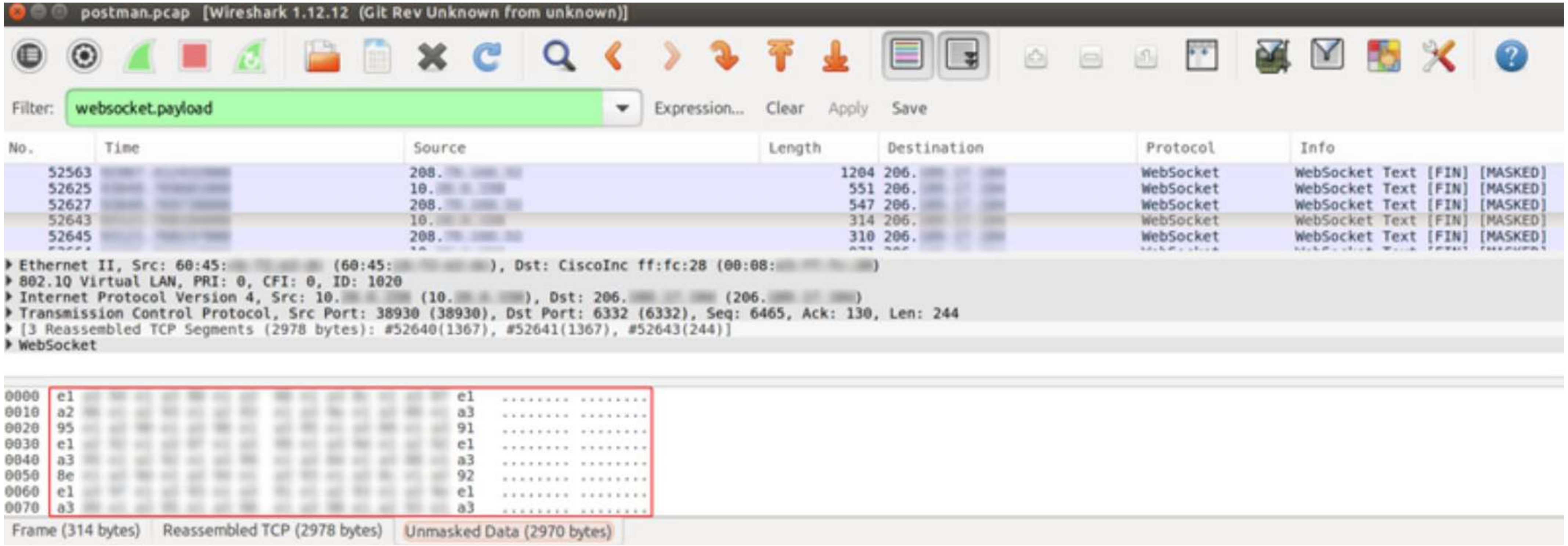
Postman

Offered by: hanterforme

★★★★☆ 22 | Developer Tools | 27,077 users

Deconstructing Real-World Attacks: Fake Extensions/Apps

- A C2 connection from the fake Postman extension detected based on behavioral learning
- Further investigation revealed ”data exfil”
- Fake extension was ultimately removed from Chrome Extension store


postman.pcap [Wireshark 1.12.12 (Git Rev Unknown from unknown)]
Filter:
Expression...
Clear
Apply
Save

Filter: websocket.payload

```
No.    Time           Source           Length Destination  Protocol   Info
52563  [redacted]     208.[redacted]   1204 206.[redacted] WebSocket  WebSocket Text [FIN] [MASKED]
52625  [redacted]     10.[redacted]     551 206.[redacted] WebSocket  WebSocket Text [FIN] [MASKED]
52627  [redacted]     208.[redacted]    547 206.[redacted] WebSocket  WebSocket Text [FIN] [MASKED]
52643  [redacted]     10.[redacted]     314 206.[redacted] WebSocket  WebSocket Text [FIN] [MASKED]
52645  [redacted]     208.[redacted]    310 206.[redacted] WebSocket  WebSocket Text [FIN] [MASKED]
```

```
▸ Ethernet II, Src: 60:45:[redacted] (60:45:[redacted]), Dst: CiscoInc ff:fc:28 (00:08:[redacted])
▸ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 1020
▸ Internet Protocol Version 4, Src: 10.[redacted] (10.[redacted]), Dst: 206.[redacted] (206.[redacted])
▸ Transmission Control Protocol, Src Port: 38930 (38930), Dst Port: 6332 (6332), Seq: 6465, Ack: 130, Len: 244
▸ [3 Reassembled TCP Segments (2978 bytes): #52640(1367), #52641(1367), #52643(244)]
▸ WebSocket
```

```
0000  e1 [redacted] e1   ........ ........
0010  a2 [redacted] a3   ........ ........
0020  95 [redacted] 91   ........ ........
0030  e1 [redacted] e1   ........ ........
0040  a3 [redacted] a3   ........ ........
0050  8e [redacted] 92   ........ ........
0060  e1 [redacted] e1   ........ ........
0070  a3 [redacted] a3   ........ ........
```

Frame (314 bytes) | Reassembled TCP (2978 bytes) | Unmasked Data (2970 bytes)

Key Take-Aways

Digital Epidemiology: Focused Visibility on Critical Assets

1. Obtain situational awareness for all critical assets
2. Surface anomalies and deviations from typical behaviour
3. Move beyond “treating symptoms”: Build out surveillance of critical control points
4. Focus on “complete visibility”
5. Do not ignore BYOD and IoT devices

RSAConference2019
Asia Pacific & Japan

THANK YOU!