RSAConference2020
San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: TECH-R09

Shadow IT and Shadow Remote Access. How to Find It (for free!)

John Strand

Owner
Black Hills Information Security
@strandjs

Goals

- Changes in the vulnerability management landscape
- The explosion of IoT and what it means to findings shadow IP access
- Shadow IT attack case studies
- How to start hunting at scale
- For free

Changes in Vulnerability Management

- We are all real good at fighting security issues of 5-10 years ago
  - Development lead time
  - Management fighting the same things as when they were in the trenches
  - It is "easier"
- Somehow, we stopped well before we should have

Quick Question...

Nessus vulnerability scanner

Nessus Scan Report
Wed, 09 Mar 2016 21:17:48 GMT

Table Of Contents

Vulnerabilities By Plugin

- 85382 (1) - OpenSSH < 7.0 Multiple Vulnerabilities
- 33929 (6) - PCI DSS compliance
- 10081 (5) - FTP Privileged Port Bounce Scan
- 11573 (5) - smallftpd Multiple Vulnerabilities (Traversal, DoS)
- 35690 (5) - ProFTPD Username Variable Substitution SQL Injection
- 36051 (5) - Xlight FTP Server Authentication SQL Injection
- 11580 (1) - Firewall UDP Packet Source Port 53 Ruleset Bypass
- 84638 (1) - OpenSSH < 6.9 Multiple Vulnerabilities

Enterprise Matrix

Below are the tactics and technique representing the MITRE ATT&CK Matrix™ for Enterprise. The Matrix contains information for the following platforms: Windows, macOS, Linux, AWS, GCP, Azure, Azure AD, Office 365, SaaS.

Last Modified: 2019-10-09 18:48:31.906000

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	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Application Access Token	Bash History	Application Window Discovery	Application Access Token	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Application Deployment Software	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	BITS Jobs	Cloud Instance Metadata API	Cloud Service Dashboard	Component Object Model and Distributed COM	Data from Cloud Storage Object	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Bypass User Account Control	Credential Dumping	Cloud Service Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	Clear Command History	Credentials from Web Browsers	Domain Trust Discovery	Internal Spearphishing	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Code Signing	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Removable Media	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compile After Delivery	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data Staged	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Compiled HTML File	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Email Collection	Fallback Channels	Transfer Data to Cloud Account	Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Firmware	Hooking	Password Policy Discovery	Remote File Copy	Input Capture	Multi-hop Proxy		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Peripheral Device Discovery	Remote Services	Man in the Browser	Multi-Stage Channels		Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Connection Proxy	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Screen Capture	Multiband Communication		Service Stop

Quick Question…

Nessus vulnerability scanner

Nessus Scan Report
Wed, 09 Mar 2016 21:17:48 GMT

Table Of Contents

Vulnerabilities By Plugin

- 85382 (1) - OpenSSH < 7.0 Multiple Vulnerabilities
- 33929 (6) - PCI DSS compliance
- 10081 (5) - FTP Privileged Port Bounce Scan
- 11573 (5) - smallftpd Multiple Vulnerabilities (Traversal, DoS)
- 35690 (5) - ProFTPD Username Variable Substitution SQL Injection
- 36051 (5) - Xlight FTP Server Authentication SQL Injection
- 11580 (1) - Firewall UDP Packet Source Port 53 Ruleset Bypass
- 84638 (1) - OpenSSH < 6.9 Multiple Vulnerabilities

Enterprise Matrix

Below are the tactics and technique representing the MITRE ATT&CK Matrix™ for Enterprise. The Matrix contains information for the following platforms: Windows, macOS, Linux, AWS, GCP, Azure, Azure AD, Office 365, SaaS.

Last Modified: 2019-10-09 18:48:31.906000

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	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Application Access Token	Bash History	Application Window Discovery	Application Access Token	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Application Deployment Software	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	BITS			ect Model d COM	Data from Cloud Storage Object	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Bypass U Co			Remote s	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	Clear Com			phishing	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	CM			ipts	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Code			lash	Data from Removable Media	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compile A			icket	Data Staged	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Compiled			Protocol	Email Collection	Fallback Channels	Transfer Data to Cloud Account	Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Compon			Copy	Input Capture	Multi-hop Proxy		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Peripheral Device Discovery	Remote Services	Man in the Browser	Multi-Stage Channels		Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Connection Proxy	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Screen Capture	Multiband Communication		Service Stop

Exploit Public-Facing Application

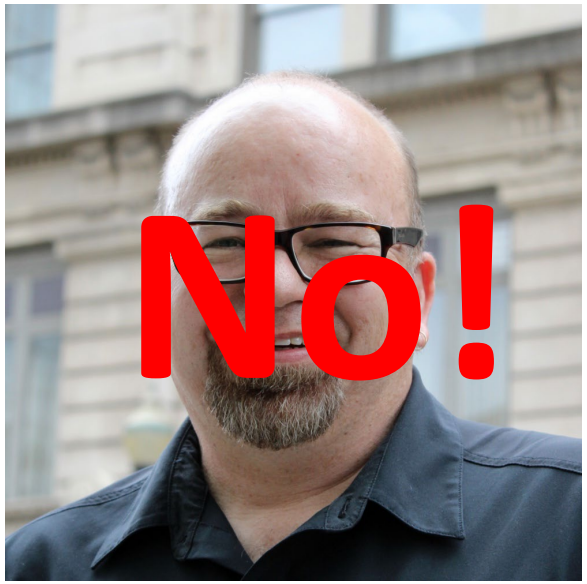
External Remote Services

Far Beyond the Scope of this Presentation...

- We need to move beyond simple patch and configuration checks
- We need to get to threat emulation
- We need to look at lateral movement
- We need to focus on post-exploitation
- We need to do all this some other time
- Shadow IT...

Egypt, Beau, Joff and my Fridge...

Egypt, Beau, Joff and my Fridge...



IoT Case Study: Teamviewer

TeamViewer Confirms Undisclosed Breach From 2016

By Sergiu Gatlan

May 17, 2019 02:02 PM 0

TeamViewer confirmed today that it has been the victim of a cyber attack which was discovered during the autumn of 2016, but was never disclosed. This attack is thought to be of Chinese origins and utilized the Winnti backdoor.

IoT Case Study: Nuance

SALTED HASH- TOP SECURITY NEWS

By Steve Ragan, Senior Staff Writer, CSO | FEB 28, 2018 4:00 AM PST

About

Fundamental security insight to help you minimize risk and protect your organization

NEWS

Nuance says NotPetya attack led to $92 million in lost revenue

Recent SEC filings disclose losses, and predicts additional spend in 2018 for security enhancements and upgrades

IoT Case Study: Hospital in Wyoming

WY: Gillette hospital targeted in ransomware attack

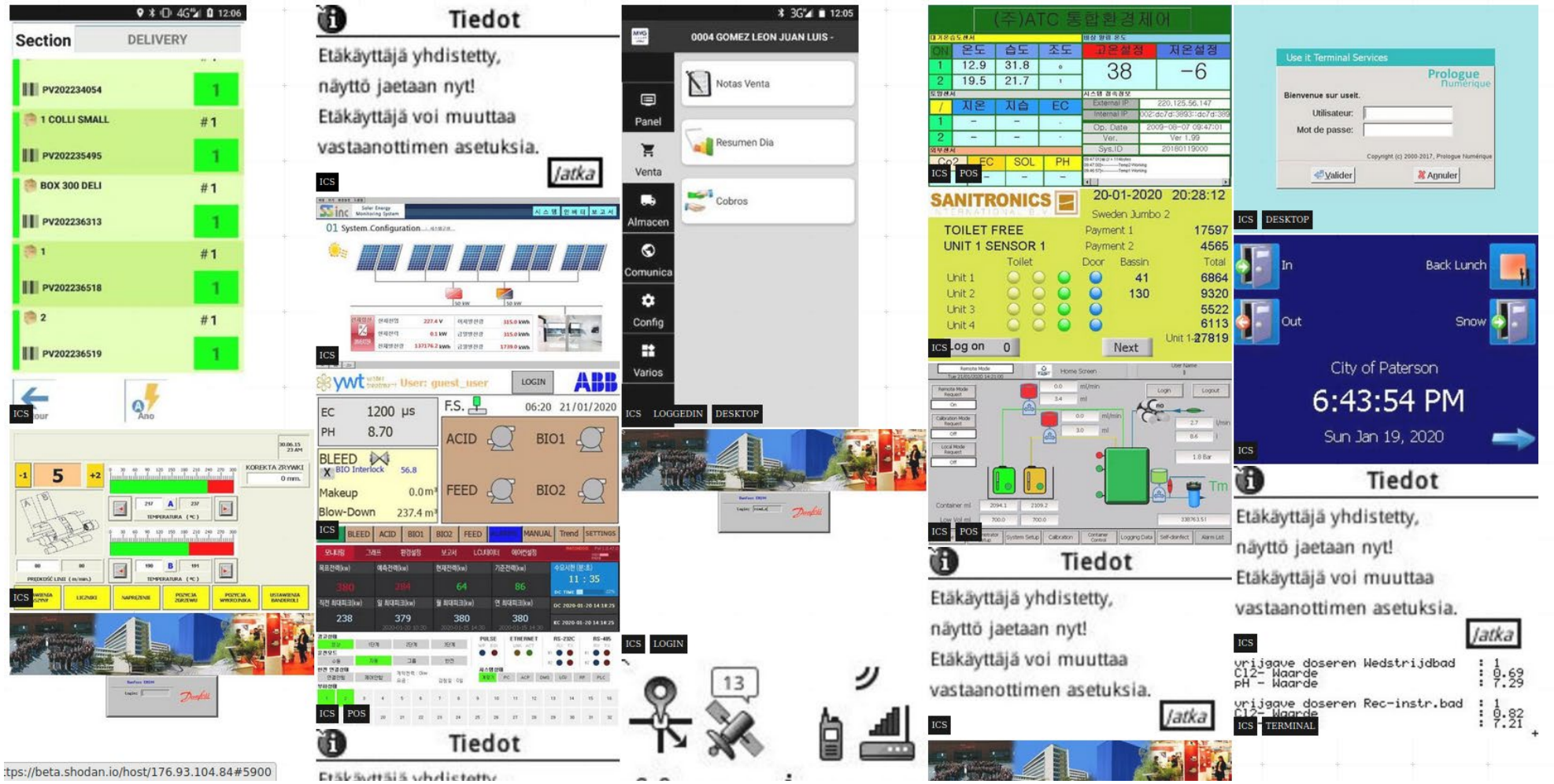
SEPTEMBER 21, 2019 DISSENT

Seth Klamann reports:

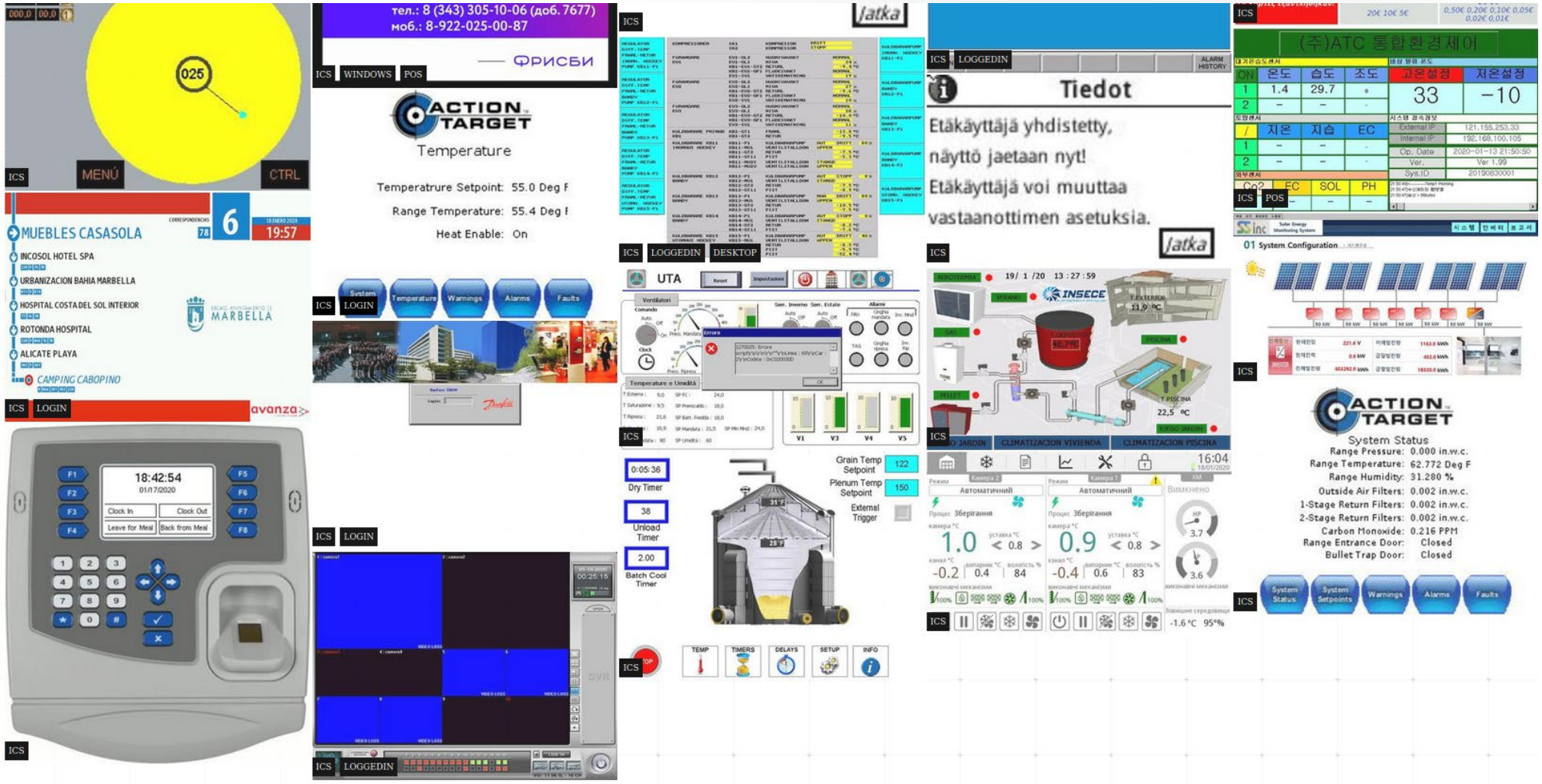
> Campbell County Health in Gillette was targeted in a ransomware attack Friday, according to an alert the state Department of Health sent to health care providers.
>
> The attack occurred early Friday morning, at approximately 3 a.m. The hospital "experienced serious computer issues" due to the attack. This caused a "service disruption" at the facility.

Read more on Casper Star-Tribune. Updates on the situation are provided on the county's web site. At the time of this posting, there is a notice at the top of the home page saying:

Not.....


Section
DELIVERY
PV202234054
1 COLLI SMALL
PV202235495
BOX 300 DELI
PV202236313
PV202236518
PV202236519
Tiedot
Etäkäyttäjä yhdistetty,
näyttö jaetaan nyt!
Etäkäyttäjä voi muuttaa
vastaanottimen asetuksia.
Jatka
0004 GOMEZ LEON JUAN LUIS -
Notas Venta
Resumen Dia
Cobros
Panel
Venta
Almacen
Comunica
Config
Varios
ICS
LOGGEDIN
DESKTOP
(주)ATC 통합환경제어
SANITRONICS
20-01-2020 20:28:12
Sweden Jumbo 2
TOILET FREE
UNIT 1 SENSOR 1
Payment 1 17597
Payment 2 4565
Next
Use it Terminal Services
Prologue
Bienvenue sur useit.
Utilisateur:
Mot de passe:
Valider
Annuler
DESKTOP
In
Back Lunch
Out
Snow
City of Paterson
6:43:54 PM
Sun Jan 19, 2020
ABB
LOGIN
F.S.
06:20 21/01/2020
ACID
BIO1
FEED
BIO2
BLEED
BIO Interlock
Makeup
Blow-Down
POS
LOGIN
TERMINAL
vrijgave doseren Wedstrijdbad : 1
C12- Waarde : 0.69
pH - Waarde : 7.29
vrijgave doseren Rec-instr.bad : 1
C12- Waarde : 0.82
: 7.21

An Exception..



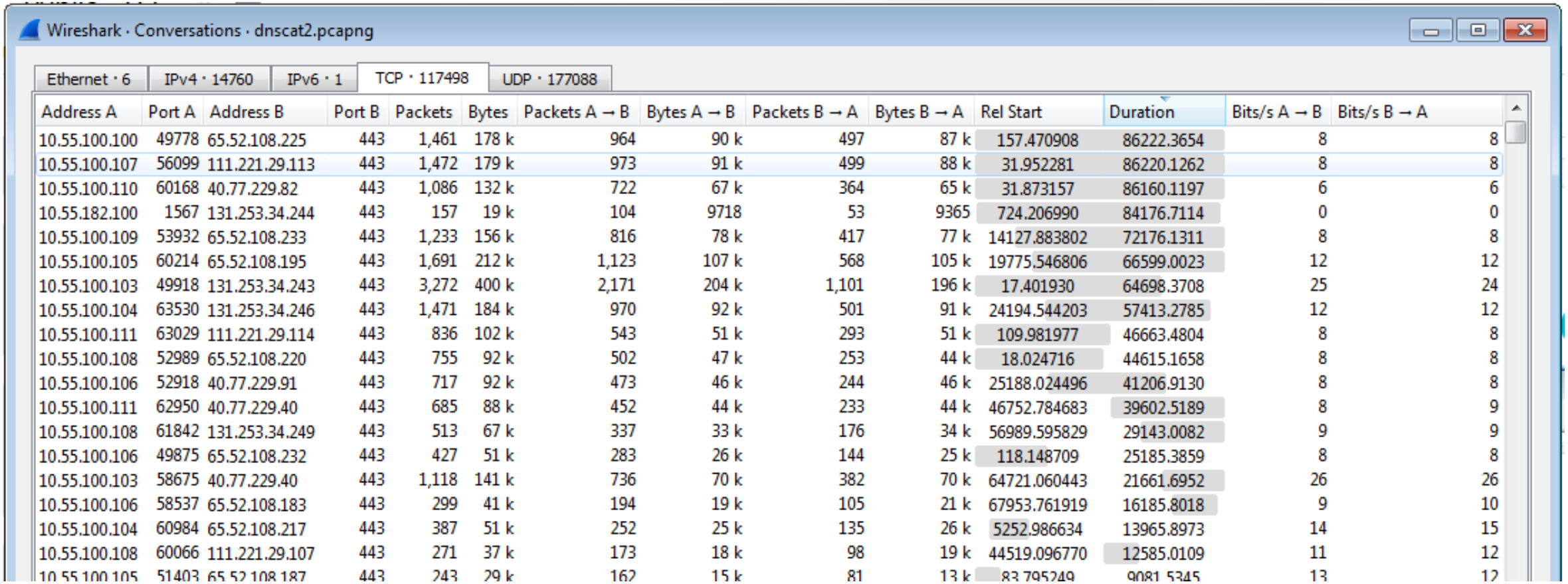
Tshark Hunting

```
cbrenton@cbrenton-lab-testing:~/lab-thunt$ tshark -r data-exfil.pcap -T fields -e ip.
src -e ip.dst -e ip.len ip.src == 192.168.0.0/16 or ip.src == 10.0.0.0/8 or ip.src ==
 172.16.0.0/12 | sort | datamash -g 1,2 sum 3 | sort -k 3 -rn | head -10
10.55.200.10    172.16.200.11   4825837
10.55.100.111   23.38.115.36    1140527
10.55.100.111   165.227.216.194 1042860
10.55.100.111   34.233.92.30    992160
10.55.100.111   24.220.113.58   857202
10.55.100.111   24.220.113.56   825084
10.55.100.111   23.52.163.40    820940
10.55.100.100   23.38.115.36    809700
10.55.100.111   172.217.8.198   795040
10.55.100.111   23.63.220.157   792002
cbrenton@cbrenton-lab-testing:~/lab-thunt$ _
```

Command Used

```
tshark -r data-exfil.pcap -T fields -e ip.src -e ip.dst -e ip.len ip.src == 192.168.0.0/16 or ip.src == 10.
0.0.0/8 or ip.src == 172.16.0.0/12 | sort | datamash -g 1,2 sum 3 | sort -k 3 -rn | head
```

Wireshark

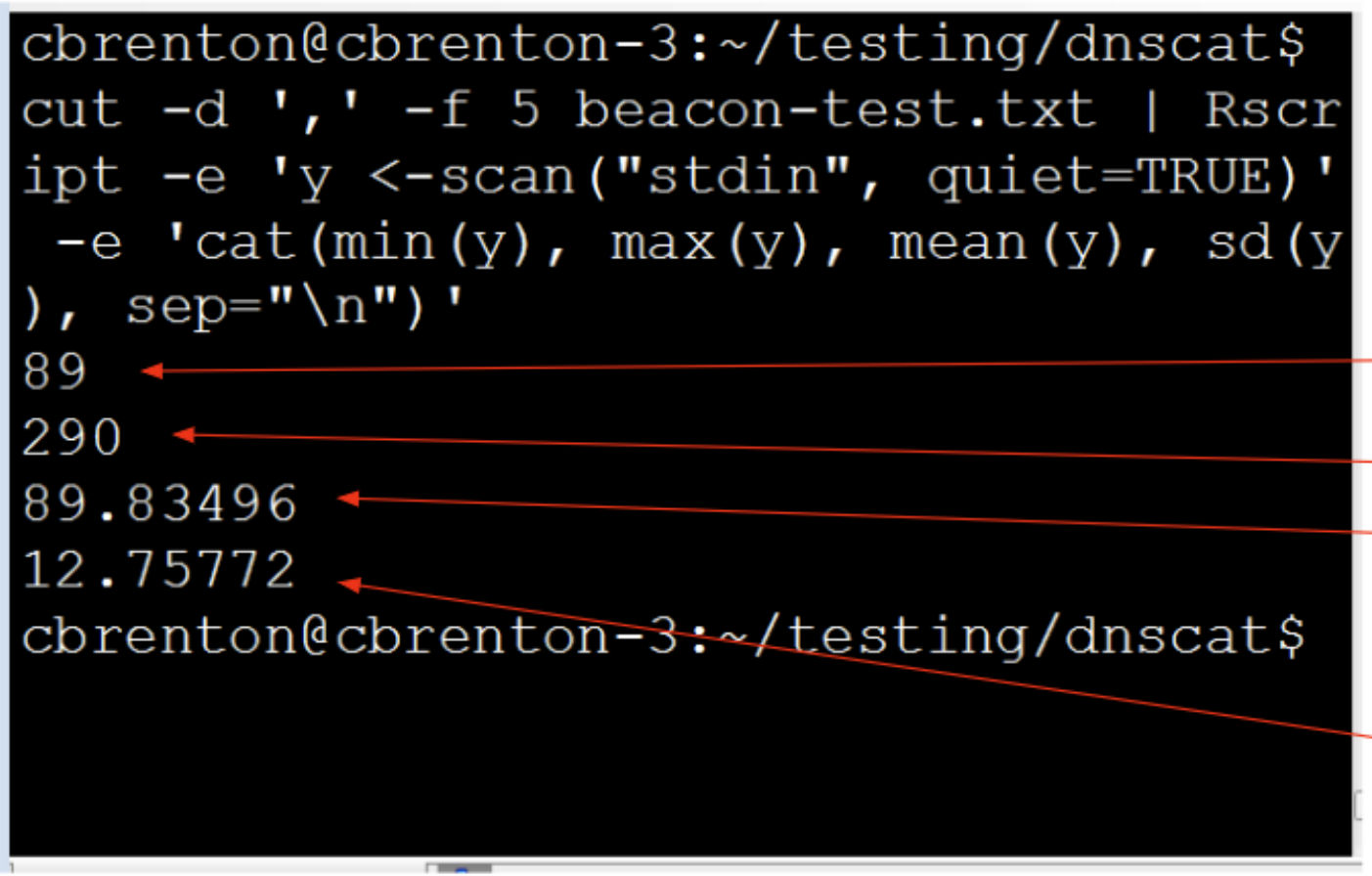


Wireshark · Conversations · dnscat2.pcapng

Ethernet · 6 | IPv4 · 14760 | IPv6 · 1 | TCP · 117498 | UDP · 177088

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
10.55.100.100	49778	65.52.108.225	443	1,461	178 k	964	90 k	497	87 k	157.470908	86222.3654	8	8
10.55.100.107	56099	111.221.29.113	443	1,472	179 k	973	91 k	499	88 k	31.952281	86220.1262	8	8
10.55.100.110	60168	40.77.229.82	443	1,086	132 k	722	67 k	364	65 k	31.873157	86160.1197	6	6
10.55.182.100	1567	131.253.34.244	443	157	19 k	104	9718	53	9365	724.206990	84176.7114	0	0
10.55.100.109	53932	65.52.108.233	443	1,233	156 k	816	78 k	417	77 k	14127.883802	72176.1311	8	8
10.55.100.105	60214	65.52.108.195	443	1,691	212 k	1,123	107 k	568	105 k	19775.546806	66599.0023	12	12
10.55.100.103	49918	131.253.34.243	443	3,272	400 k	2,171	204 k	1,101	196 k	17.401930	64698.3708	25	24
10.55.100.104	63530	131.253.34.246	443	1,471	184 k	970	92 k	501	91 k	24194.544203	57413.2785	12	12
10.55.100.111	63029	111.221.29.114	443	836	102 k	543	51 k	293	51 k	109.981977	46663.4804	8	8
10.55.100.108	52989	65.52.108.220	443	755	92 k	502	47 k	253	44 k	18.024716	44615.1658	8	8
10.55.100.106	52918	40.77.229.91	443	717	92 k	473	46 k	244	46 k	25188.024496	41206.9130	8	8
10.55.100.111	62950	40.77.229.40	443	685	88 k	452	44 k	233	44 k	46752.784683	39602.5189	8	9
10.55.100.108	61842	131.253.34.249	443	513	67 k	337	33 k	176	34 k	56989.595829	29143.0082	9	9
10.55.100.106	49875	65.52.108.232	443	427	51 k	283	26 k	144	25 k	118.148709	25185.3859	8	8
10.55.100.103	58675	40.77.229.40	443	1,118	141 k	736	70 k	382	70 k	64721.060443	21661.6952	26	26
10.55.100.106	58537	65.52.108.183	443	299	41 k	194	19 k	105	21 k	67953.761919	16185.8018	9	10
10.55.100.104	60984	65.52.108.217	443	387	51 k	252	25 k	135	26 k	5252.986634	13965.8973	14	15
10.55.100.108	60066	111.221.29.107	443	271	37 k	173	18 k	98	19 k	44519.096770	12585.0109	11	12
10.55.100.105	51403	65.52.108.187	443	243	29 k	162	15 k	81	13 k	83.795249	9081.5345	13	12

Using R



"cut" extracts session size, passes through "R" for analysis

Min sessions size

Max sessions size

Mean very close to min could indicate a heartbeat

Standard deviation is small and close in value to "mean minus min". Indicator this could be a heartbeat

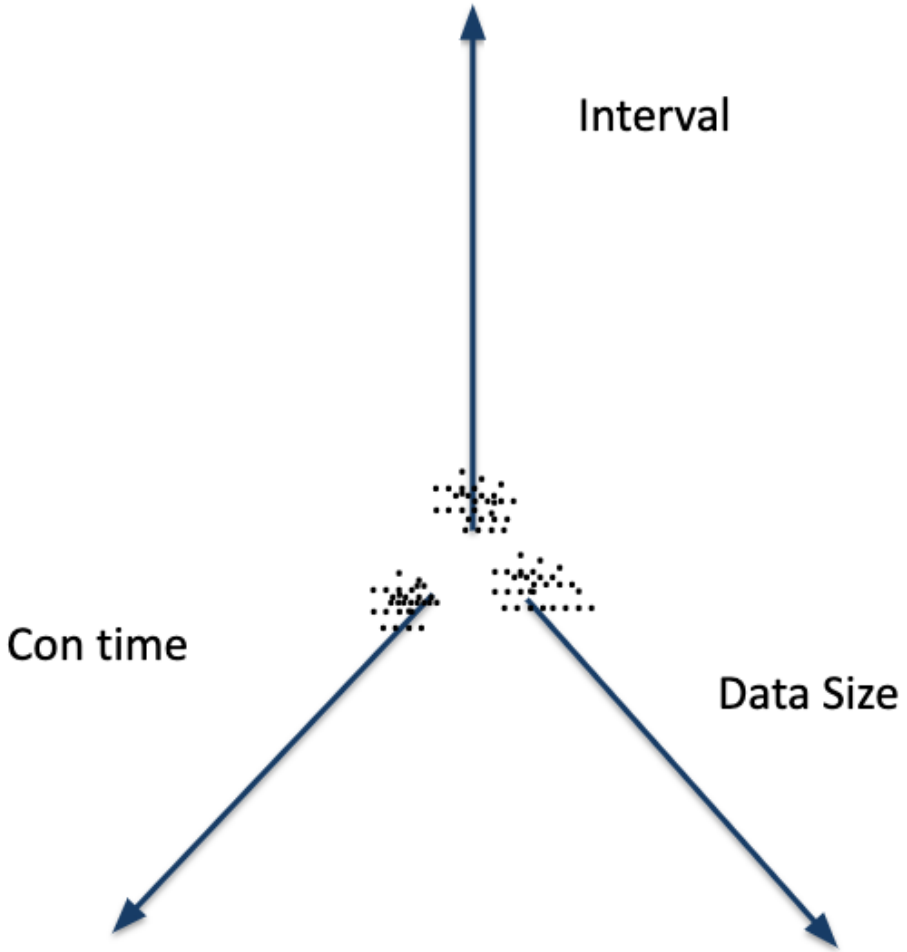
Zeek and User Agent Strings

```
cbrenton@aih-3-3-rc2:~/test/testing$ cat http.08_33_18-09_00_00.log | bro-cut user_agent
 | sort | uniq -c | sort
      1 -
      1 Python-urllib/3.5
     22 Microsoft-WNS/10.0
     26 Microsoft-CryptoAPI/10.0
     30 Microsoft BITS/7.8
     55 Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17134.590
     72 Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
cbrenton@aih-3-3-rc2:~/test/testing$
cbrenton@aih-3-3-rc2:~/test/testing$
cbrenton@aih-3-3-rc2:~/test/testing$ grep Python http.08_33_18-09_00_00.log
1552574001.145136       CLLPdJ1nLAOdIIwyHe      10.55.254.107   42292   91.189.95.15
80      1       GET     changelogs.ubuntu.com   /meta-release-lts       -       1.1
Python-urllib/3.5       0       4386    200     OK      -       -       (empty) -
-       -       -       -       -       FhGf5d4pejzo7Ob3ll      -       text/plain
cbrenton@aih-3-3-rc2:~/test/testing$ _
```

Real Intelligence Threat Analytics

- Finds patterns in large-scale network traffic
  - Well over one Terabyte at a time
- Specifically looks for beacons
- Also, Blacklist checking, DNS views, Long Connections
- All for free
- Check it out!
- https://github.com/activecm/rita

Math!



RITA and Long Connections

```
thunt@thunt-one-day:~/lab1$ rita show-long-connections lab1 | head
Source IP,Destination IP,Port:Protocol:Service,Duration
10.55.100.100,65.52.108.225,443:tcp:-,86222.4
10.55.100.107,111.221.29.113,443:tcp:-,86220.1
10.55.100.110,40.77.229.82,443:tcp:-,86160.1
10.55.100.109,65.52.108.233,443:tcp:ssl,72176.1
10.55.100.105,65.52.108.195,443:tcp:ssl,66599
10.55.100.103,131.253.34.243,443:tcp:-,64698.4
10.55.100.104,131.253.34.246,443:tcp:ssl,57413.3
10.55.100.111,111.221.29.114,443:tcp:-,46638.5
10.55.100.108,65.52.108.220,443:tcp:-,44615.2
thunt@thunt-one-day:~/lab1$ _
```

RITA and Beacons

```
thunt@thunt-one-day:~/lab1$ rita show-beacons lab1 | head
Score,Source IP,Destination IP,Connections,Avg Bytes,Intvl Range,Size Range,
Top Intvl,Top Size,Top Intvl Count,Top Size Count,Intvl Skew,Size Skew,Intvl
 Dispersion,Size Dispersion
1,192.168.88.2,165.227.88.15,108858,199,860,230,1,89,53341,108319,0,0,0,0
1,10.55.100.111,165.227.216.194,20054,92,29,52,1,52,7774,20053,0,0,0,0
0.838,10.55.200.10,205.251.194.64,210,308,29398,4,300,70,109,205,0,0,0,0
0.835,10.55.200.11,205.251.197.77,69,308,1197,4,300,70,38,68,0,0,0,0
0.834,192.168.88.2,13.107.5.2,27,198,2,33,12601,73,4,15,0,0,0,0
0.834,10.55.100.111,34.239.169.214,34,704,5,4517,1,156,15,30,0,0,0,0
0.833,10.55.100.106,23.52.161.212,27,940,38031,52,1800,505,19,19,0,0,0,0
0.833,10.55.100.111,23.52.162.184,27,2246,37828,52,1800,467,23,25,0,0,0,0
0.833,10.55.100.100,23.52.161.212,26,797,36042,52,1800,505,16,25,0,0,0,0
thunt@thunt-one-day:~/lab1$
```

Apply!

- IoT is exploding
- This is actually a compliance requirement
  - NIST 800, CSC, etc.
- Start hunting rogue IT
- Many tools to use
  - Tshark, R, RITA, Zeek
- Low leval of technical skill required
- However, a high level of curiosity is required

Process

- Just as we started with vulnerability management
  - Monthly or quarterly then continuous
- The first few times will serve as house cleaning
  - Identify: Beacons, IoT, old operating systems, remote access, DNS misconfigurations, video streaming, browser-based bitcoin mining, etc.
- Move towards automated and ongoing anomaly analysis
- All anomaly analysis requires a clean baseline

Thanks!

- Questions?