



City of Pittsburgh

Network Situational Awareness

Project Team: Aditya Anil Balapure, Xi Dai, Jorge Medina, Sunil David, Yunxin Li
Project Advisor: Sidney Faber

Agenda

- I. Project Overview
 - a. Business Case
 - b. Project's Objectives
 - c. Project Outcomes
- I. Business Processes
 - A. Profiling
 - B. IOC Analysis
- III. Conclusions and Recommendations
- IV. Lessons Learned

I. Project Overview

Business Case

- Assume that one or more hosts from the City of Pittsburgh have been compromised.
- Existent defenses have failed to detect and prevent the intrusion.
- Case scenario of an Advanced Persistent Threat – APT.

I. Project Overview

Project Objectives

- Analyze and monitor historic and live network flow data in search for Indicators of Compromise (IoC).
- Design, develop and document a process for the collection, detection, and analysis of IoCs
- Recommendations to improve PGH's security posture

I. Project Overview

Project Outcome

- Build network profile, find some interesting network activities.
- Network Profiling Process
- Search for Indicator of Compromise (IoC) Process
- Information Security recommendations

II. Business Processes

Benefits of using BPMN v2.0 - Business Process Model Notation:

- Standard from the BPMI (Not-for-Profit)
- Uses flow diagrams to model complex business processes.
- Provide a notation (syntax and semantics) that is easily understandable by all stakeholders
- Promote the standardization of best practices between the organization.
- Improve knowledge transfer.

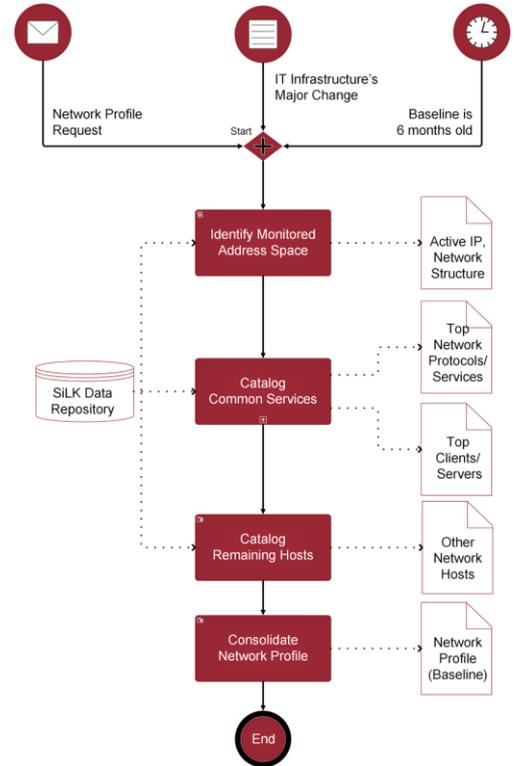
II. Business Processes

Network Profiling Process

Based on the recommendations from CERT's Network Situational Awareness Team.

Process purpose is to...

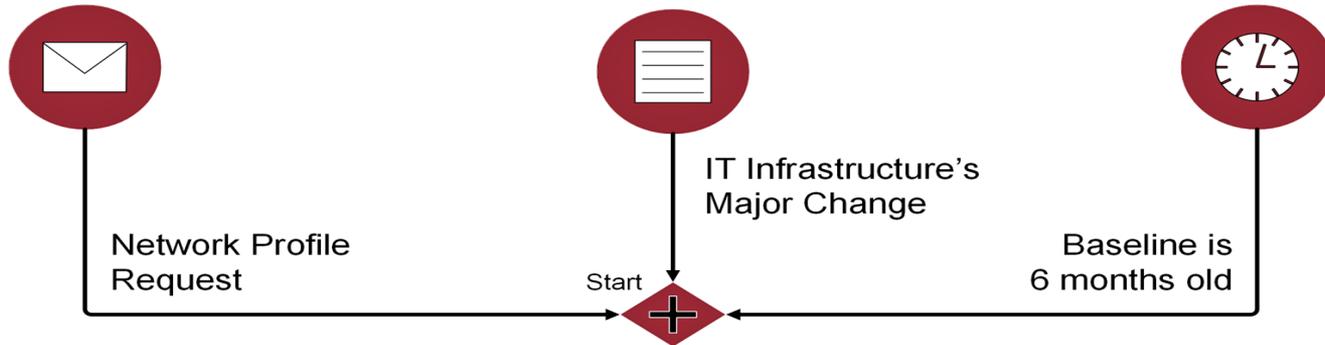
- Create a network profile or network baseline
- Increase the awareness of network normal activities and behavior



II. Business Processes

Process Initiation

Process can start with any of this three events:



II. BP - Network Profiling



Identify the Monitored Address Space:

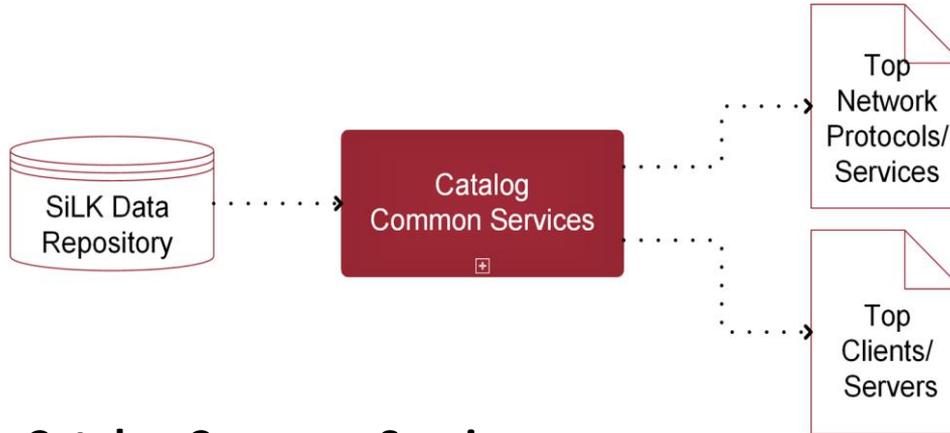
- Active TCP connections;
- Non-trivial amount of traffic on protocols other than TCP;
- Aggregate individual hosts into populated network blocks;
- Verify the list of active hosts

Outcome: Active host list, network structure

Network Structure:

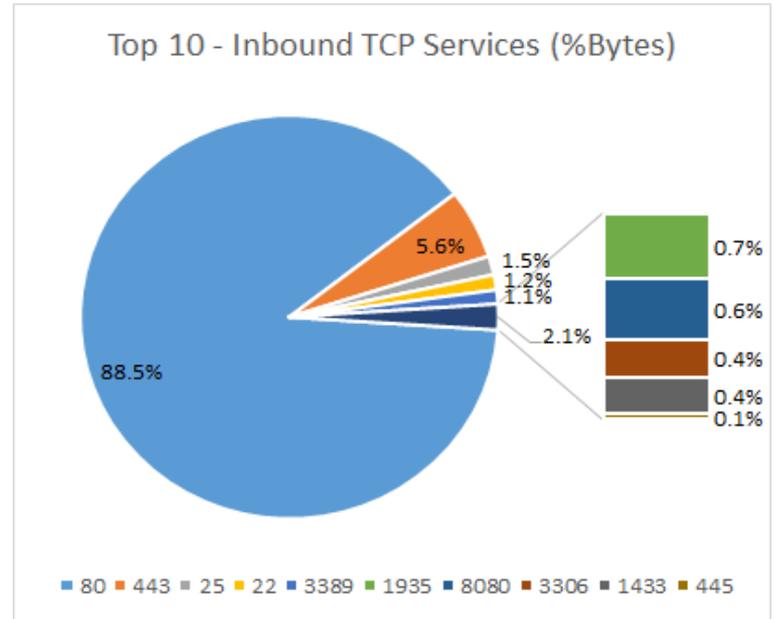
205.141.128.64/27	4
205.141.129.0/27	4
205.141.129.32/27	8
205.141.129.64/27	3
205.141.129.160/27	9
205.141.129.192/27	6
205.141.188.0/27	5
205.141.188.160/27	1
205.141.189.0/27	5
205.141.189.160/27	1
205.141.190.0/27	10
205.141.190.32/27	2
205.141.191.224/27	1
205.141.128.0/18	 59
TOTAL	 59 Active Hosts

II. BP - Network Profiling



Catalog Common Services:

- Top Network Protocols (in/out)
- Top Services
- Top Servers and Clients (Top Talkers)



II. BP - Network Profiling

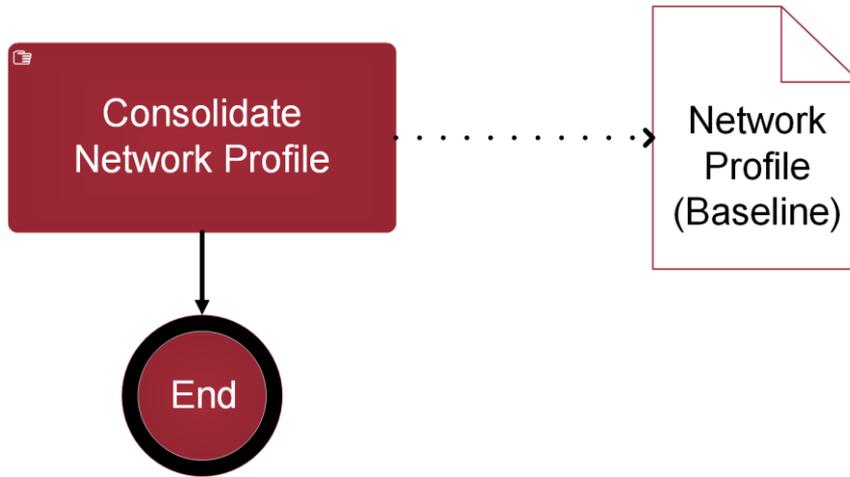


Catalog the remaining hosts:

Identify host with trivial amounts of traffic (host traffic is less than 1% of total protocol traffic)

Outcome: Bottom Talkers.

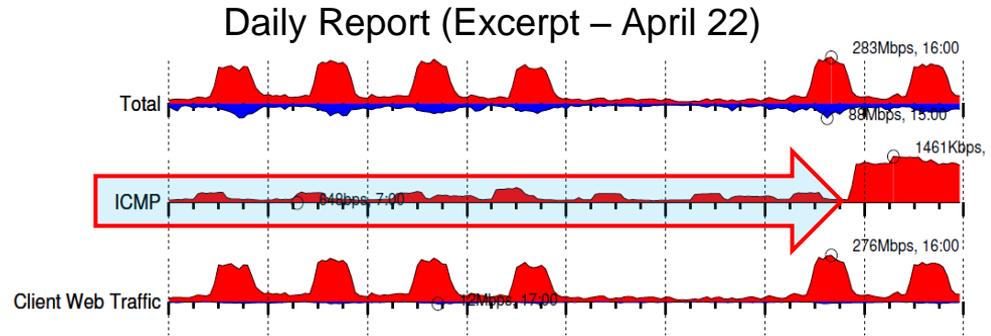
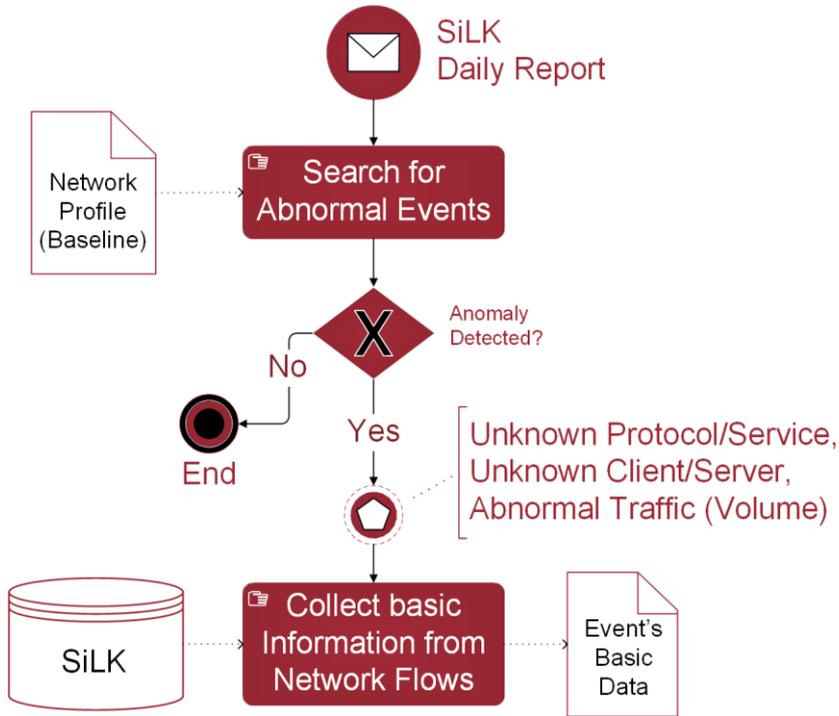
II. BP - Network Profiling



Consolidated Network Profile (Baseline)

- Update twice a year
- Update if there is a big change in IT infrastructure.
- Use the baseline to detect abnormal behaviors.

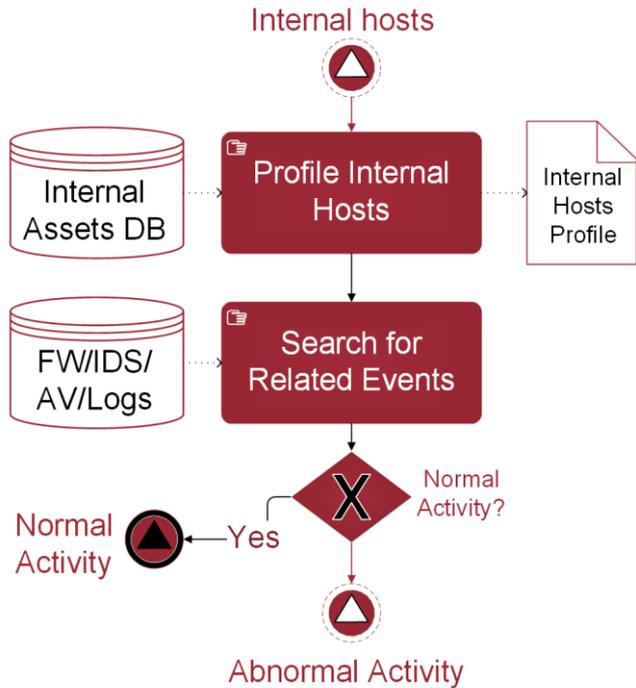
III. BPM - Indicators of Compromise



Collect basic information about the event

- Date / Time of the event
- Event type
- Protocol / Service
- IP source and destination
- Source or Destination Country Codes

III. BPM - Indicators of Compromise



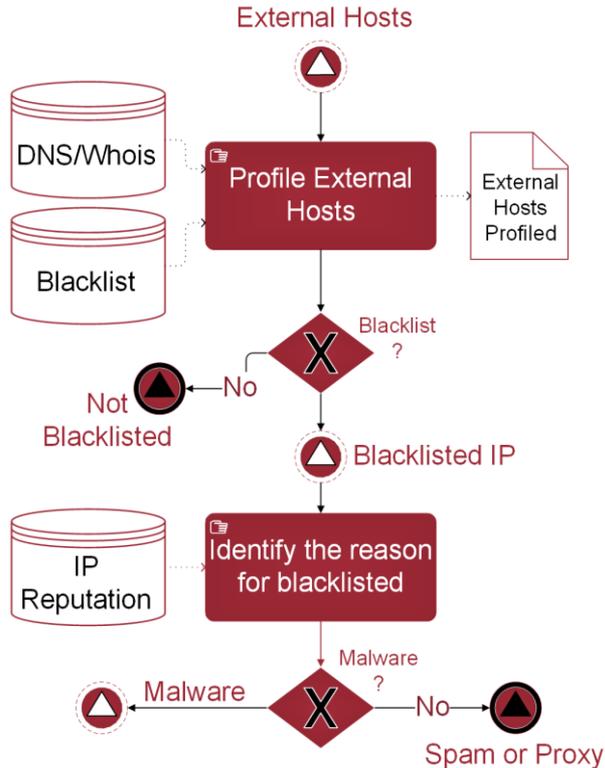
Internal Host Profile

- Hostname
- Business Unit / Responsible / Owner
- Related Business Service or Product
- OS / Software Base
- Risk Profile (Recommended)

Related Events

- Firewall
- IDS/IPS
- Antivirus Logs
- ElasticSearch
- Patch Management / SW Inventory
- Vulnerability Management

III. BPM - Indicators of Compromise



External Host Profile

- Hostname
- Network Owner
- Country
- Risk Profile (Reputation)

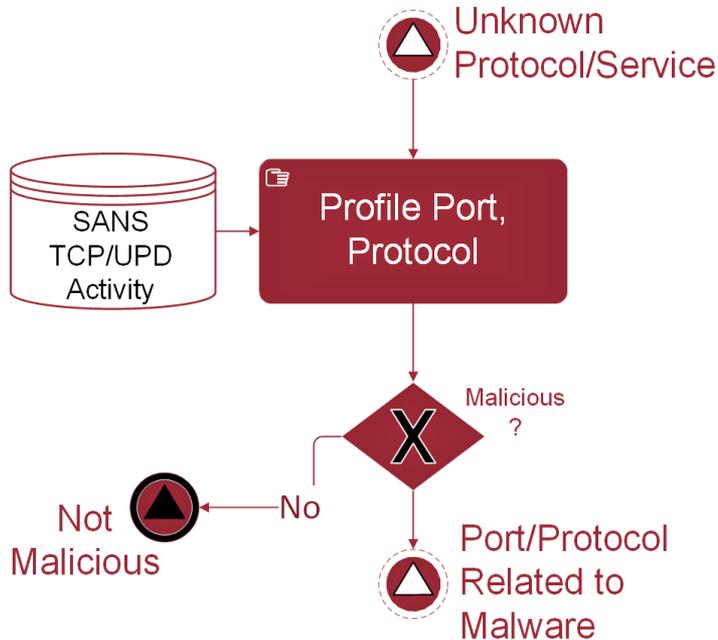
Possible reason for bad reputation:

- Spammer, Proxy
- Malware infected, Botnet

Suggested Blacklist resources:

- SANS - Suspicious domains
https://isc.sans.edu/suspicious_domains.html
- Spamhaus - ZEN DNSBL
<https://www.spamhaus.org/zen/>

III. BPM - Indicators of Compromise



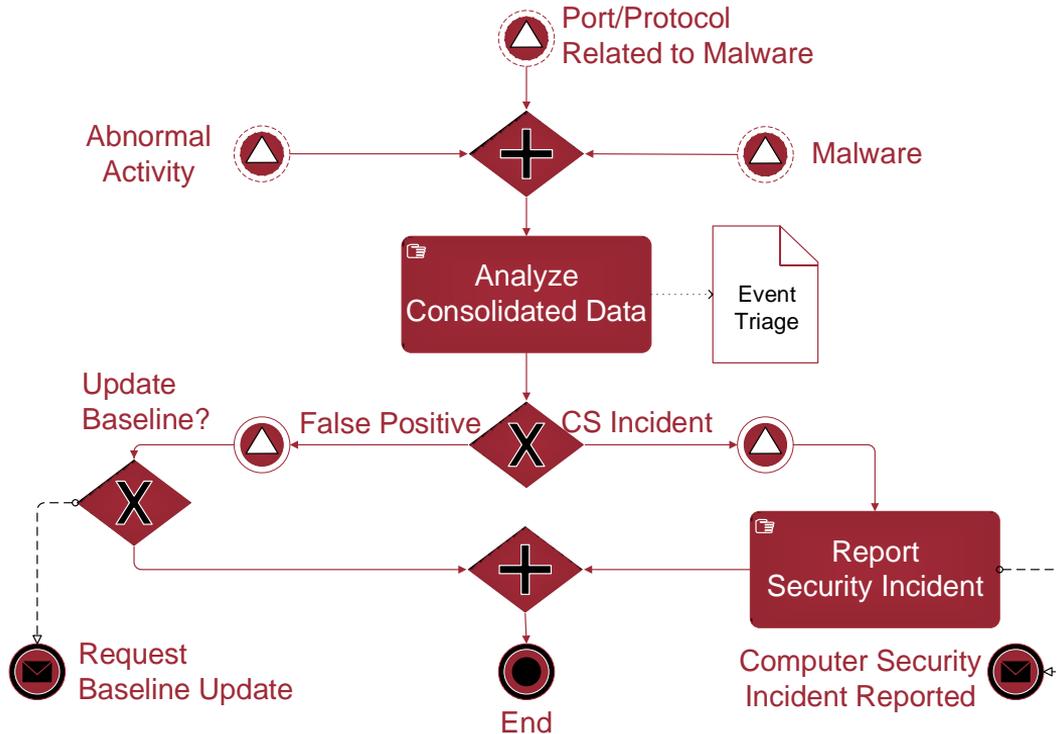
Port/Protocol Profile

- Identify the network protocol (TCP/UDP)
- Identify what applications/malware use the port/protocol

Suggested resource

- TCP/UDP Port Activity
<https://isc.sans.edu/port.html>

III. BPM - Indicators of Compromise



Process Outcome:

- Abnormal behavior and unknown events are analyzed and triaged.
- Computer security incidents are reported.
- False positives are used as feedback for the baseline.

III. Information Security Recommendations

- Implement IT Governance to avoid rogue IT, and unsecure implementations.
- Implement a VPN model for remote administration.
- Update network profile every 6 months, or when major IT changes occurs
- Subscribe to a reliable blacklist to flag off malicious IP addresses for further forensics

III. Conclusions

- Improved network situational awareness of City of Pittsburgh
- Proposed a business process approach to improve the network security posture, analysis capabilities and knowledge transfer.
- Proposed enhanced security configurations, and network design

III. Recommendations - Network Forensics

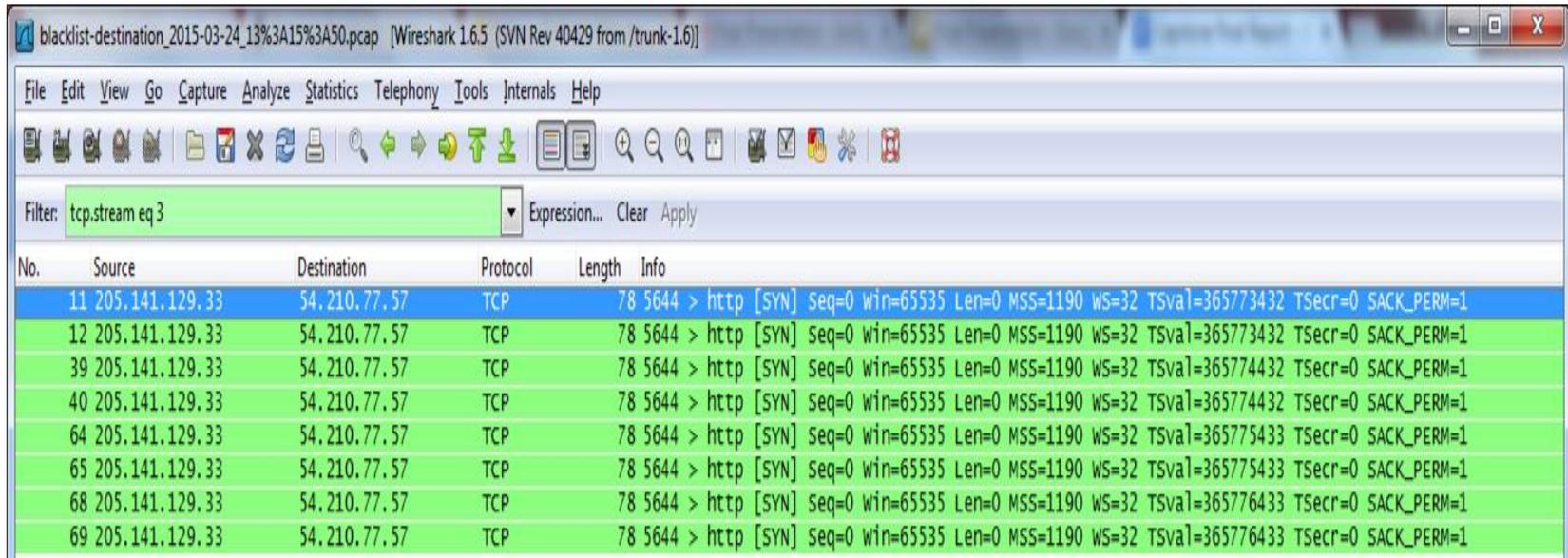
blacklist-destination_2015-03-24_13%3A15%3A50.pcap [Wireshark 1.6.5 (SVN Rev 40429 from /trunk-1.6)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp.stream eq 2 Expression... Clear Apply

No.	Source	Destination	Protocol	Length	Info
5	205.141.129.33	173.192.42.190	TCP	78	14477 > http [SYN] seq=0 win=65535 Len=0 MSS=1190 WS=32 TSval=365768498 TSecr=0 SACK_PERM=1
6	205.141.129.33	173.192.42.190	TCP	78	14477 > http [SYN] seq=0 win=65535 Len=0 MSS=1190 WS=32 TSval=365768498 TSecr=0 SACK_PERM=1
7	173.192.42.190	205.141.129.33	TCP	74	http > 14477 [SYN, ACK] seq=0 Ack=1 win=7240 Len=0 MSS=1460 SACK_PERM=1 TSval=2596202163 TSecr=36576
8	173.192.42.190	205.141.129.33	TCP	74	http > 14477 [SYN, ACK] seq=0 Ack=1 win=7240 Len=0 MSS=1460 SACK_PERM=1 TSval=2596202163 TSecr=36576
9	205.141.129.33	173.192.42.190	TCP	66	14477 > http [ACK] seq=1 Ack=1 win=131200 Len=0 TSval=365768536 TSecr=2596202163
10	205.141.129.33	173.192.42.190	TCP	66	[TCP Dup ACK 9#1] 14477 > http [ACK] seq=1 Ack=1 win=131200 Len=0 TSval=365768536 TSecr=2596202163

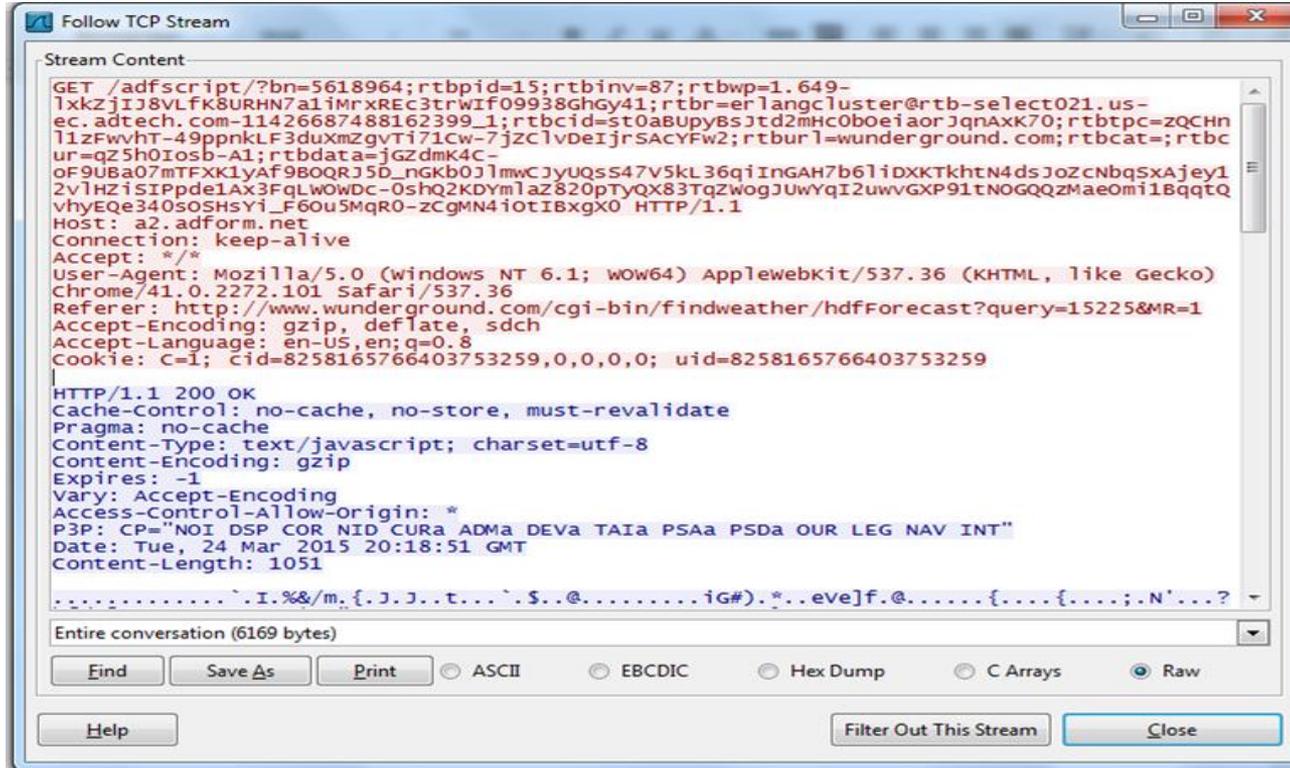
III. Recommendations - Network Forensics



The image shows a Wireshark window titled "blacklist-destination_2015-03-24_13%3A15%3A50.pcap [Wireshark 1.6.5 (SVN Rev 40429 from /trunk-1.6)]". The filter bar contains the expression "tcp.stream eq 3". The packet list pane displays the following data:

No.	Source	Destination	Protocol	Length	Info
11	205.141.129.33	54.210.77.57	TCP	78	5644 > http [SYN] Seq=0 win=65535 Len=0 MSS=1190 WS=32 TSval=365773432 TSecr=0 SACK_PERM=1
12	205.141.129.33	54.210.77.57	TCP	78	5644 > http [SYN] Seq=0 win=65535 Len=0 MSS=1190 WS=32 TSval=365773432 TSecr=0 SACK_PERM=1
39	205.141.129.33	54.210.77.57	TCP	78	5644 > http [SYN] Seq=0 win=65535 Len=0 MSS=1190 WS=32 TSval=365774432 TSecr=0 SACK_PERM=1
40	205.141.129.33	54.210.77.57	TCP	78	5644 > http [SYN] Seq=0 win=65535 Len=0 MSS=1190 WS=32 TSval=365774432 TSecr=0 SACK_PERM=1
64	205.141.129.33	54.210.77.57	TCP	78	5644 > http [SYN] Seq=0 win=65535 Len=0 MSS=1190 WS=32 TSval=365775433 TSecr=0 SACK_PERM=1
65	205.141.129.33	54.210.77.57	TCP	78	5644 > http [SYN] Seq=0 win=65535 Len=0 MSS=1190 WS=32 TSval=365775433 TSecr=0 SACK_PERM=1
68	205.141.129.33	54.210.77.57	TCP	78	5644 > http [SYN] Seq=0 win=65535 Len=0 MSS=1190 WS=32 TSval=365776433 TSecr=0 SACK_PERM=1
69	205.141.129.33	54.210.77.57	TCP	78	5644 > http [SYN] Seq=0 win=65535 Len=0 MSS=1190 WS=32 TSval=365776433 TSecr=0 SACK_PERM=1

III. Recommendations - Network Forensics



The screenshot shows a network analysis tool window titled "Follow TCP Stream". The main area displays the "Stream Content" of an HTTP transaction. The request is a GET for a weather forecast page, and the response is a 200 OK with gzipped content. The interface includes a text area for the stream content, a status bar for the entire conversation (6169 bytes), and various control buttons like Find, Save As, Print, and Close.

```
Follow TCP Stream
Stream Content
GET /adfscript/?bn=5618964;rtbpid=15;rtbinv=87;rtbwp=1.649-
1xkzjI38VLFkBURHN7a1mrxREc3trwif09938GhGy41;rtbr=erlangcluster@rtb-select021.us-
ec.adtech.com-11426687488162399_1;rtbcid=st0aBUpYBSjtd2mHc0b0ei aorJqnAxk70;rtbtpc=ZQCHN
11zFvwhT-49ppnkLF3duxmZgyTi71Cw-7jZClvDeIjrSACyFw2;rtbur1=wunderground.com;rtbcac=;rtbc
ur=qZ5h0Iosb-A1;rtbdata=jGZdmk4C-
oF9UBa07mTFXK1yAf9BOQRJ5D_ngkb0JlmcCJyUqS547V5kL36qiNGAH7b61iDXKtkhtN4dsJozCNbqSxAjey1
2v1HZiSIPpde1Ax3FQLWOWdc-0shQ2KDYmlaz820pTyQX83TqZwogJUWYqI2uWvGXP91tNOGQQZmaeOm1lBqqTQ
vhyEQe340sOSHSyI_F6ou5MqR0-zcGMN4iotIBxgX0 HTTP/1.1
Host: a2.adform.net
Connection: keep-alive
Accept: */*
User-Agent: Mozilla/5.0 (windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/41.0.2272.101 Safari/537.36
Referer: http://www.wunderground.com/cgi-bin/findweather/hdfForecast?query=15225&MR=1
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8
Cookie: c=i; cid=8258165766403753259,0,0,0,0; uid=8258165766403753259

HTTP/1.1 200 OK
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Content-Type: text/javascript; charset=utf-8
Content-Encoding: gzip
Expires: -1
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
P3P: CP="NOI DSP COR NID CURA ADMA DEVA TAIa PSAa PSDa OUR LEG NAV INT"
Date: Tue, 24 Mar 2015 20:18:51 GMT
Content-Length: 1051
.....`I.%&/m.{.J.J..t...`.S.@.....ig#)*..eve]f.@.....{....{.....;N'!...?

Entire conversation (6169 bytes)
Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw
Help Filter Out This Stream Close
```

IV. Future Work

- Automate IP analysis and malicious attribution
- Automate blacklist queries and correlation with SiLK
- Activate the internal SiLK sensor and profile the internal network.
- Improve SiLK data visualization

V. Lessons Learned

- Applied acquired knowledge about Network Situational Awareness in a real-life scenario
- Sought solutions from different perspectives and managed to combine different resources together to make critical decisions
- Improved communication and project management skills

Questions/Comments?