Network Analysis of Point of Sale System Compromises

Operation Terminal Guidance

Chicago Electronic & Financial Crimes Task Force

U.S. Secret Service

Outline

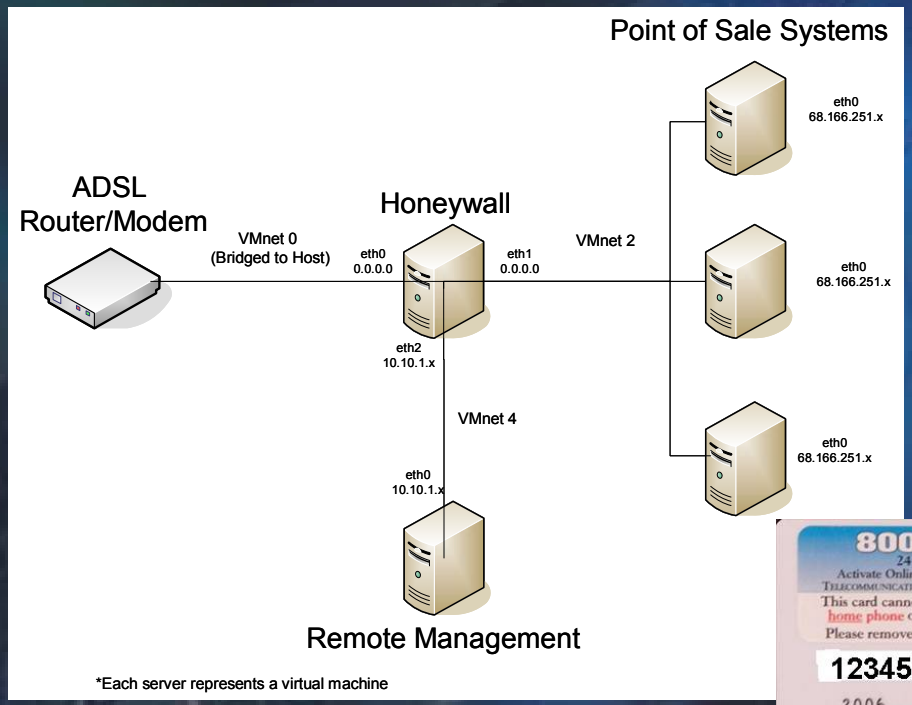
- Background
- Hypothesis
- Deployment Methodology
- Data Analysis
- Findings
- Discussion

Investigative Goals

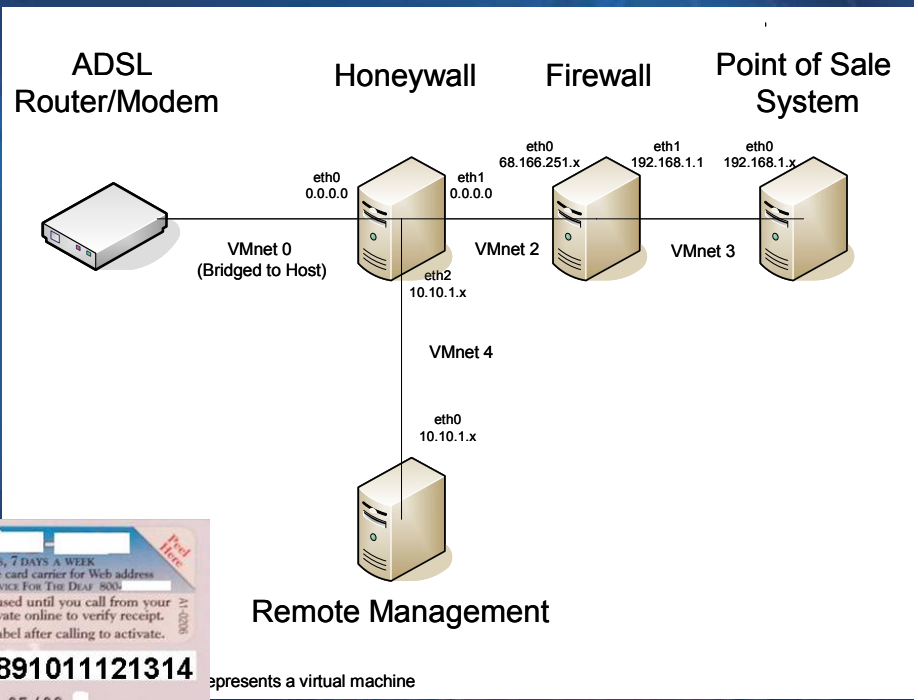
- Hypothesis: Remote attackers were not targeting point of sale (POS) system software, rather POS system compromises are a result of insecure deployment of the underlying operating system by automated scanning and vulnerability exploitation

Deployment Methodology

Test Group Honeynet



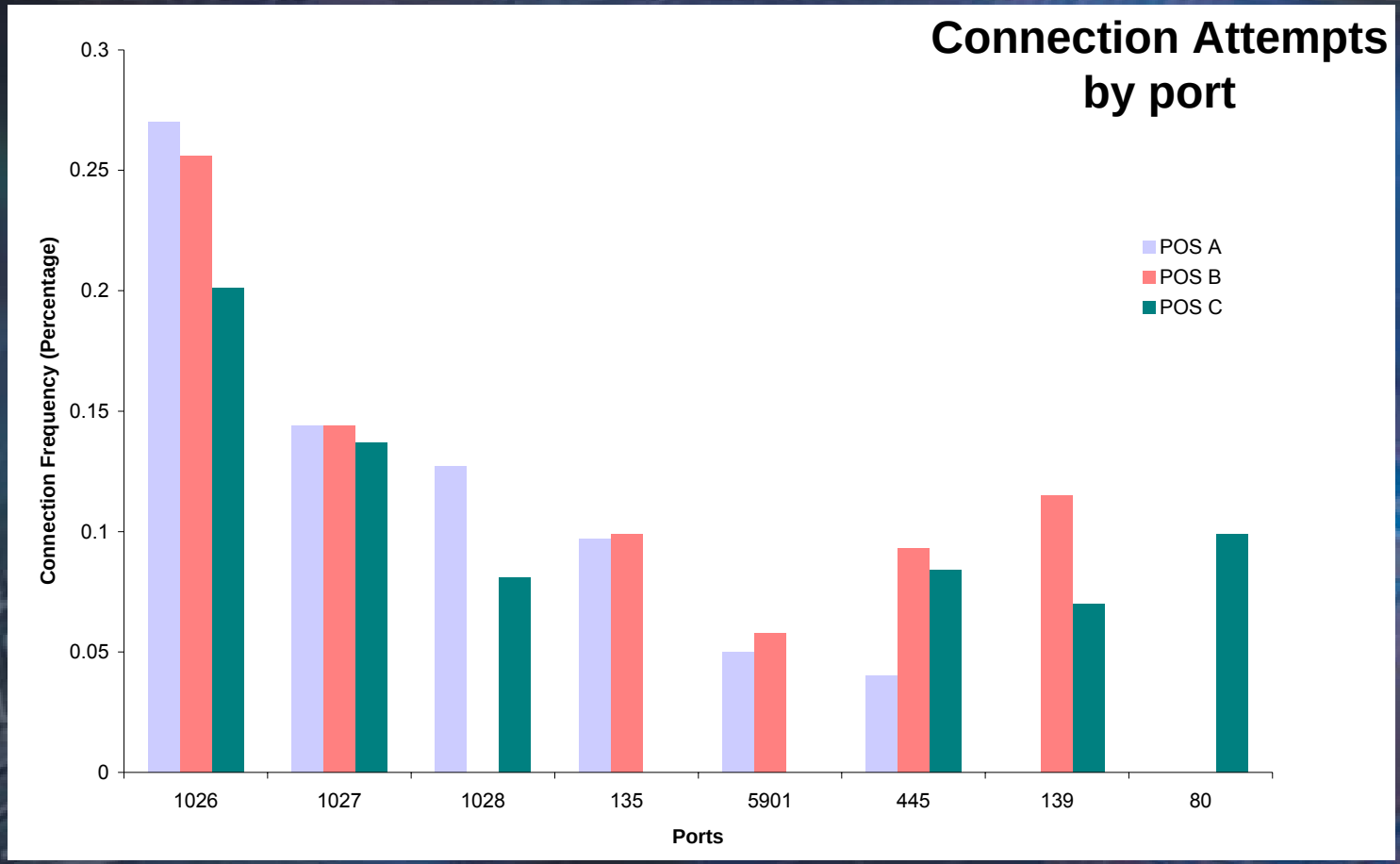
Control Group Honeynet



Honeytoken

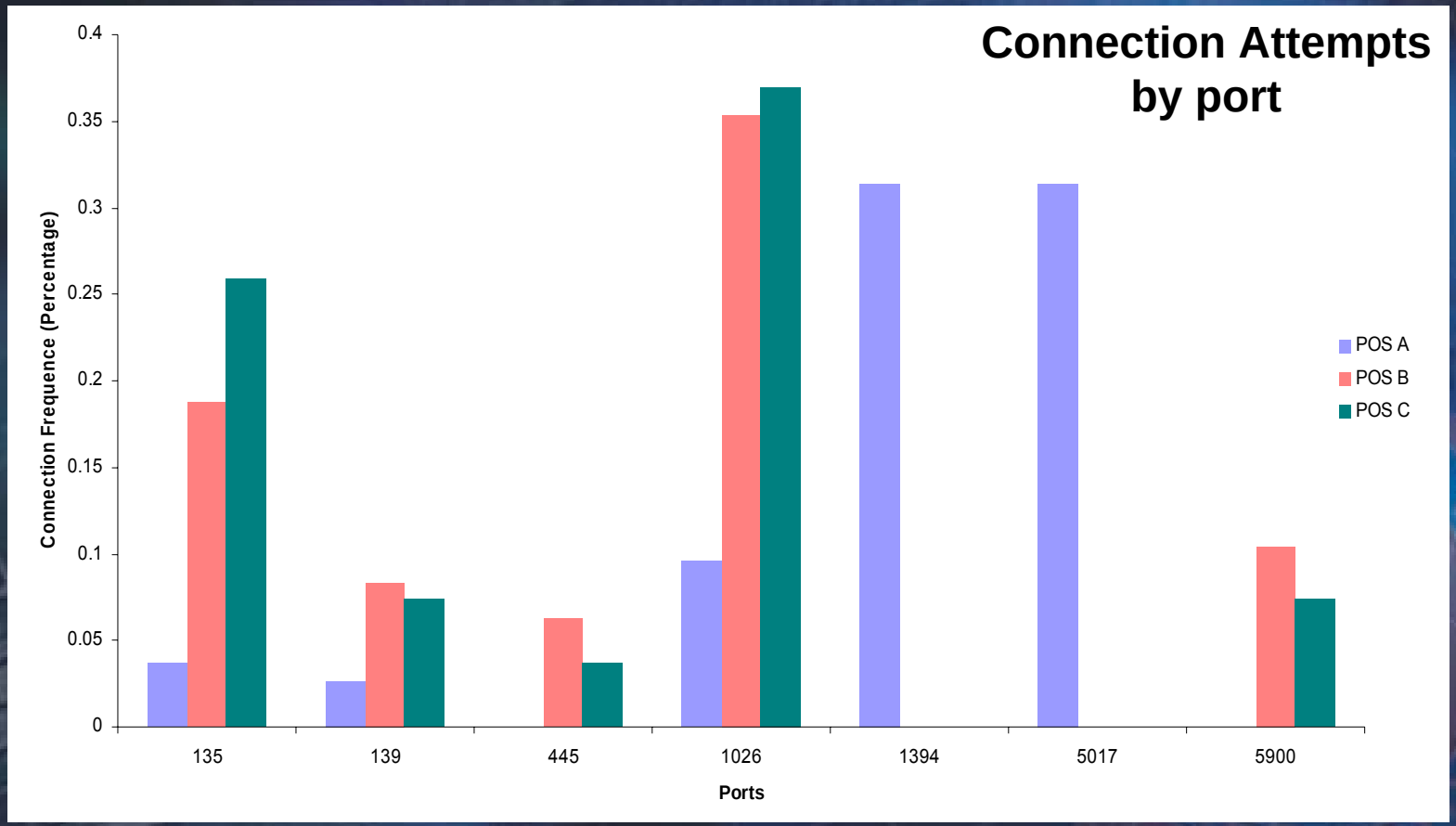
Data Analysis

Control Group



Data Analysis

Test Group



Data Analysis

- Association rules
  - Clustering
    - T: Number of virtual POS systems with connection attempts from a single source
    - n_i: Number of packets from a source to a virtual POS system
    - N: Total number of packets from a source to all three POS systems
    - $N=\sum n_i$

$$\text{Support}(R) = \frac{\#\text{ connections (POS system A, B, and C)}}{\#\text{connections}}$$

Data analysis methodology from F. Pouget and M. Dacier. "Honeypot Based Forensics."

Data Analysis

Control Group Clusters

Port	Item Sets	Support %	Support % > 1%
80	Cluster 1: T=1, N=3 Cluster 2: T=1, N=1 Cluster 3: T=2, N=8 (n=5, n=3)	43.5% 10.9% 4.3%	1
135	Cluster 4: T=1, N=1 Cluster 5: T=1, N=2	54.5% 22%	2
139	Cluster 6: T=1, N=2 Cluster 7: T=1, N=3	75% 10.1%	1
445	Cluster 8: T=1, N=1 Cluster 9: T=1, N=2 Cluster 10: T=1, N=3	20% 70% 7.1%	2
1026	Cluster 11: T=1, N=1	53.5%	1
1027	Cluster 12: T=1, N=1	98%	1
1028	Cluster 13: T=1, N=1	83%	1
5901	Cluster 14: T=1, N=2	90.9%	1

Data Analysis

Test Group Clusters

Port	Item Sets	Support %	Support % > 1%
445	Cluster 1: T=2, N=34	22.2%	0
1026	Cluster 2: T=2, N=3 Cluster 3: T=3, N=3 (n=1,n=1, n=1) Cluster 4: T=1, N=1	1.8% 20% 50.9%	2
1394	Cluster 5: T=1, N=12 Cluster 6: T=1, N=15 Cluster 7: T=1, N=6 Cluster 8: T=1, N=9	20% 16.7% 1.7% 16.7%	3
2967	Cluster 9: T=3, N=8 (n=2, n=3, n=3) Cluster 10: T=3, N=30 (n=10, n=10, n=10)	10% 10%	0
5900	Cluster 11: T=3, N=3	20%	0

Data Analysis

- Edit Distance Analysis
  - Extract TCP payloads from previous identified cluster members
  - Compare packets from each IP address against all others identified through clustering

Source A	Source B
<mss E..0..@.o.A.;W\. D..s.]..... p...^2..... <mss E..0..@.o.A.;W\. D..s.]..... p...^2.....	<mss E..0.{@.k.l\=.y. D..s.....jd..... p..... <mss E..0.{@.k.l\=.y. D..s.....jd..... p.....

Attack Phrases

Data Analysis

Control Group Phrase Distance

Cluster	Port	Phrase Distance (Lines)	Std Deviation
Cluster 6	139	2	9
Cluster 7	139	1	5
Cluster 8	445	3	10
Cluster 9	445	5	8
Cluster 10	445	4	18
Cluster 11	1026	86	169
Cluster 13	1028	12	65
Cluster 14	5901	32	12

***Clusters 1,2, 3,4,5, and 12 were discarded as not statistically significant

Data Analysis

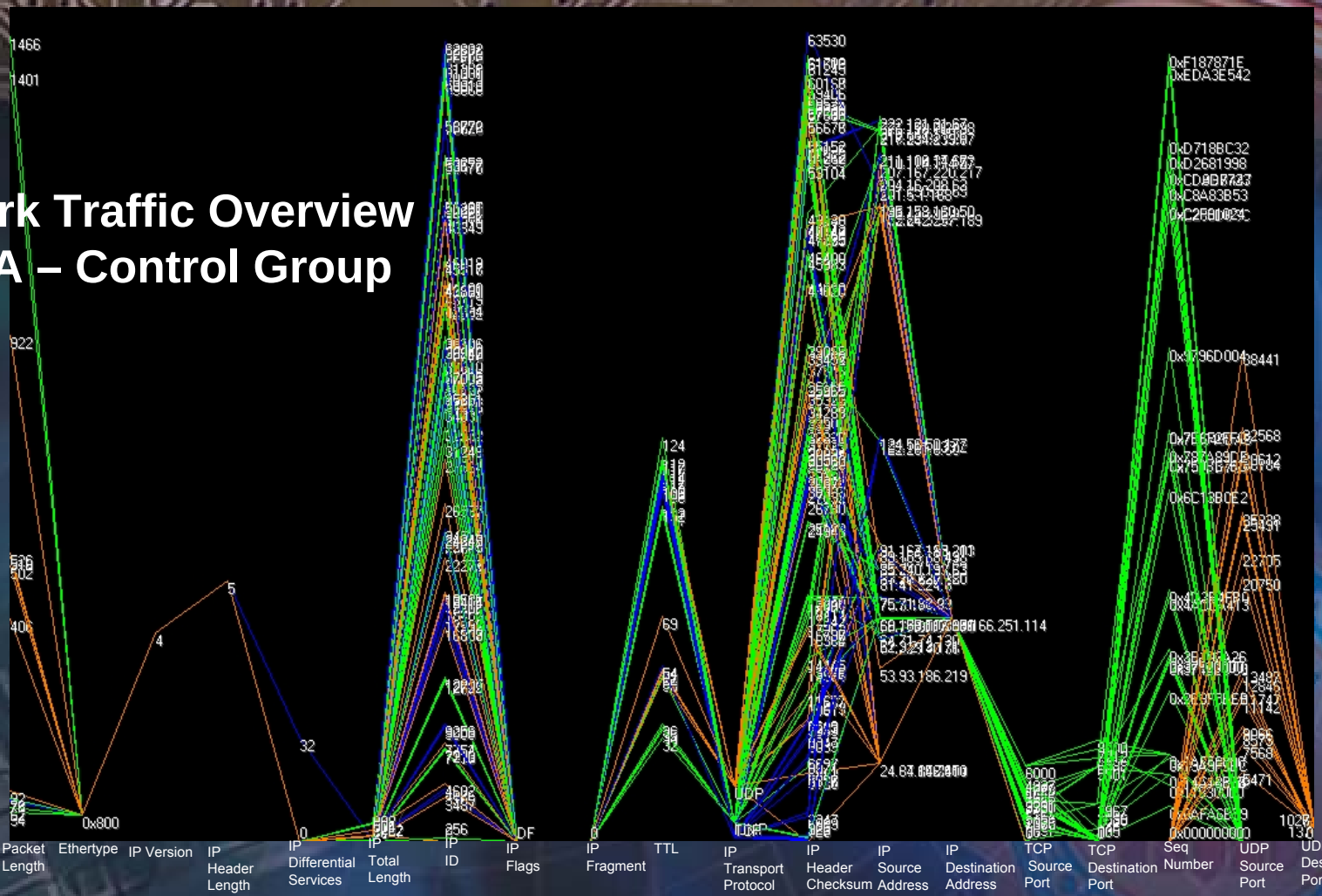
Test Group Phrase Distance

Cluster	Port	Phrase Distance (Lines)	Std Deviation
Cluster 2	1026	324	238
Cluster 5	1394	360	85
Cluster 6	1394	280	170
Cluster 7	1394	529	136
Cluster 8	1394	1422	1143
Cluster 11	5900	240	257

***Clusters 1,3,4,9,10 were discarded as not statistically significant

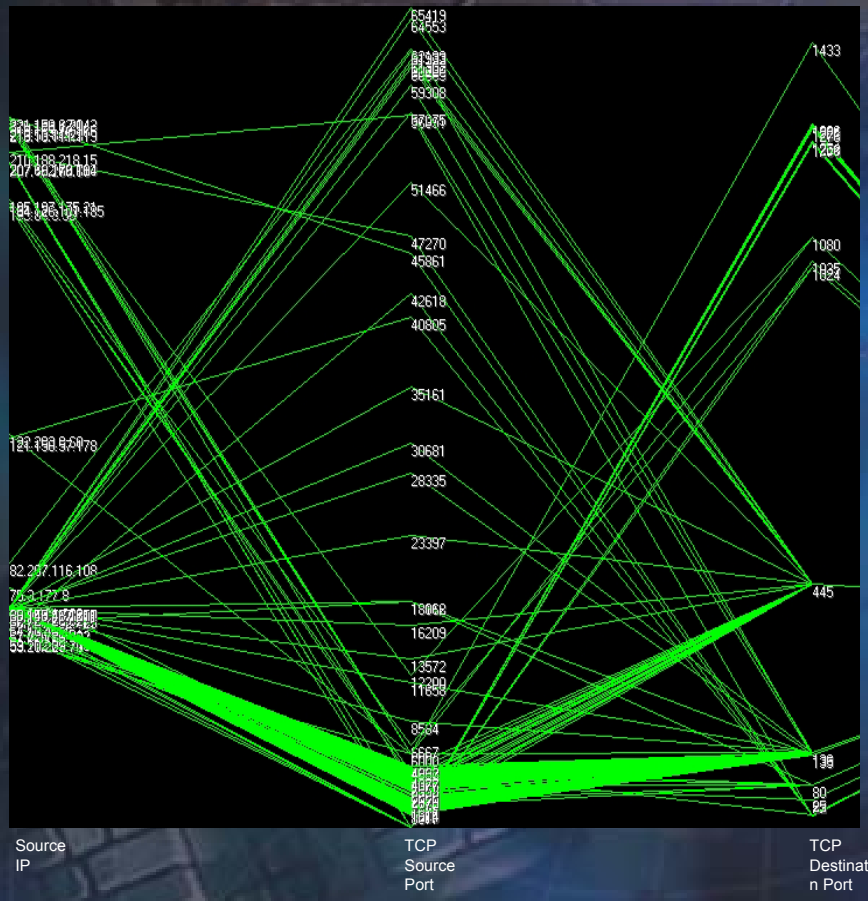
Data Analysis

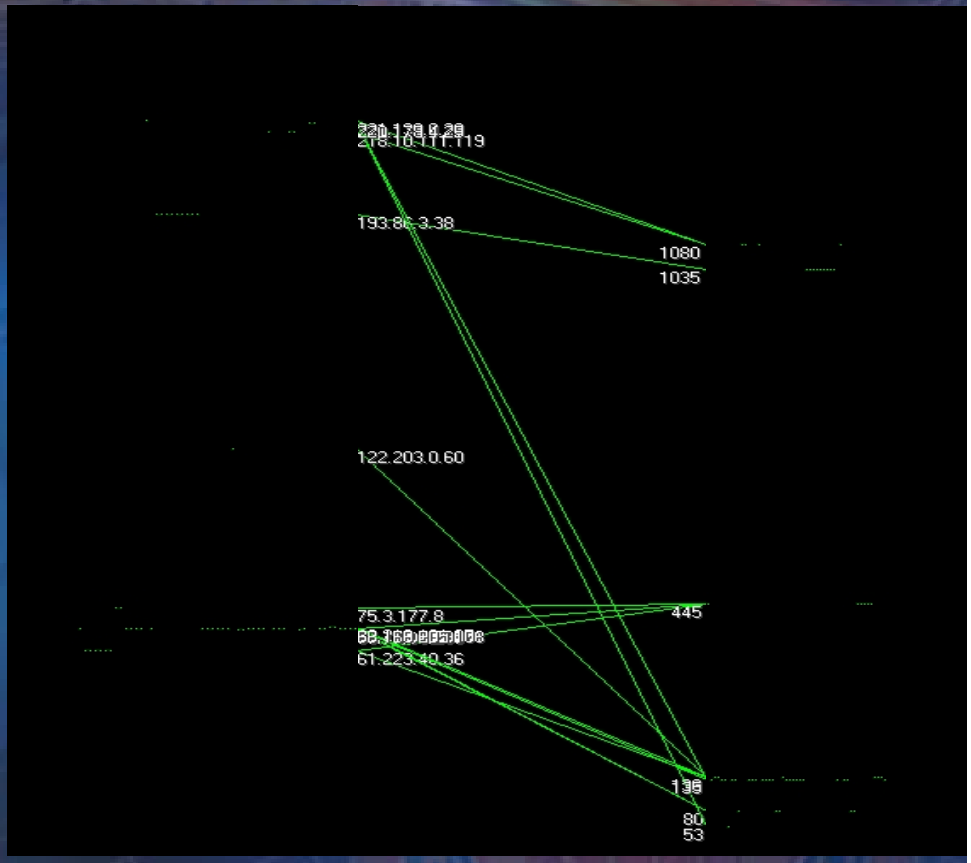
Network Traffic Overview
POS A – Control Group



Visualization methodology from Greg Conti's. "Security Data Visualization."

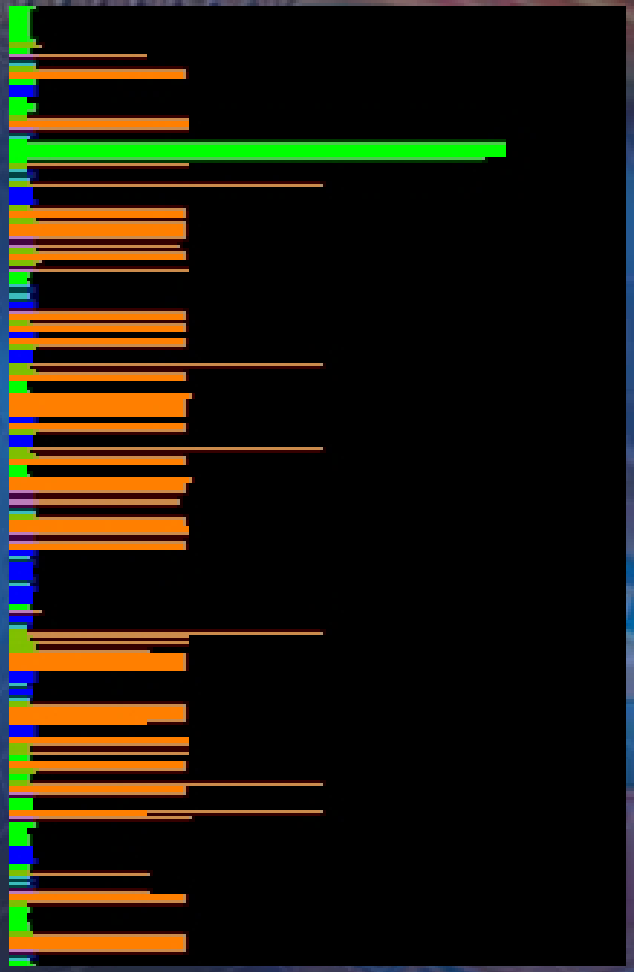
Data Analysis





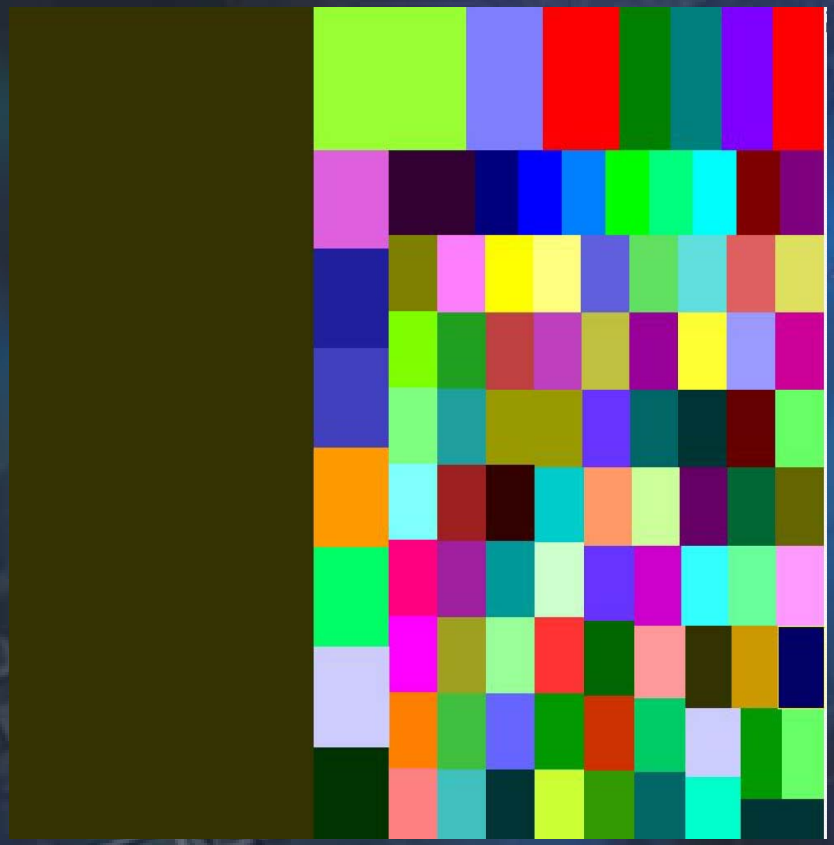
Data Analysis

- The TCP outlier is associated with browsing public web site to ensure connectivity
- Uniform length of packets

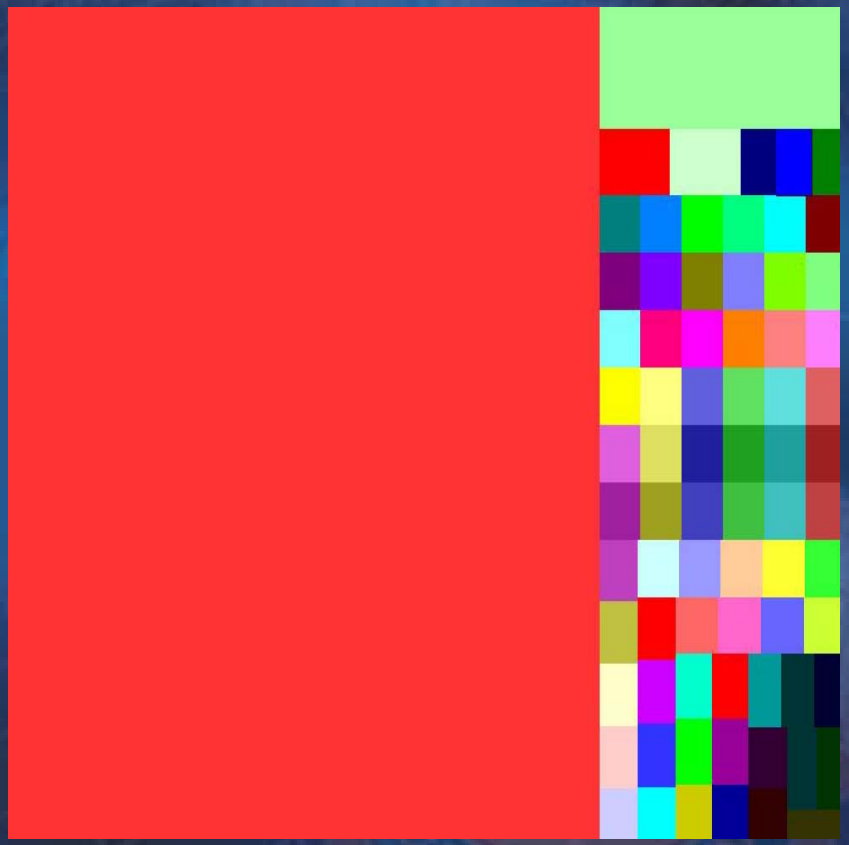


Data Analysis

TCP Packet Tree Map



UDP Packet Tree Map



Data Analysis

- Examination of the UDP packets identified in the previous tree map revealed them to be spam targeting messenger applications

```
- REGISTRY DAMAGED AND CORRUPTED.To FIX this problem:Open Internet Explorer and type:  www.registrycleanerxp.comOnce
- REGISTRY DAMAGED AND CORRUPTED.To FIX this problem:Open Internet Explorer and type:  www.registrycleanerxp.comOnce
- REGISTRY DAMAGED AND CORRUPTED.To FIX this problem:Open Internet Explorer and type:  www.registrycleanerxp.comOnce
NTION REQUIRED   Windows has found CRITICAL SYSTEM ERRORS. Download Registry Cleaner from: www.key32.comFAILURE TO A
- REGISTRY DAMAGED AND CORRUPTED.To FIX this problem:Open Internet Explorer and type:  www.registrycleanerxp.comOnce
- REGISTRY DAMAGED AND CORRUPTED.To FIX this problem:Open Internet Explorer and type:  www.registrycleanerxp.comOnce
- REGISTRY DAMAGED AND CORRUPTED.To FIX this problem:Open Internet Explorer and type:  www.registrycleanerxp.comOnce
- REGISTRY DAMAGED AND CORRUPTED.To FIX this problem:Open Internet Explorer and type:  www.registrycleanerxp.comOnce
- REGISTRY DAMAGED AND CORRUPTED.To FIX this problem:Open Internet Explorer and type:  www.registrycleanerxp.comOnce
- REGISTRY DAMAGED AND CORRUPTED.To FIX this problem:Open Internet Explorer and type:  www.registrycleanerxp.comOnce
- REGISTRY DAMAGED AND CORRUPTED.To FIX this problem:Open Internet Explorer and type:  www.registrycleanerxp.comOnce
- REGISTRY DAMAGED AND CORRUPTED.To FIX this problem:Open Internet Explorer and type:  www.registrycleanerxp.comOnce
- REGISTRY DAMAGED AND CORRUPTED.To FIX this problem:Open Internet Explorer and type:  www.registrycleanerxp.comOnce
- REGISTRY DAMAGED AND CORRUPTED.To FIX this problem:Open Internet Explorer and type:  www.registrycleanerxp.comOnce
- REGISTRY DAMAGED AND CORRUPTED.To FIX this problem:Open Internet Explorer and type:  www.registrycleanerxp.comOnce
```

Findings

- Automated scanning of select set of ports
- Multiple exploits targeting multiple OS's from single source IP address
- Attackers not aware compromised system is a POS system until after compromise and exploit
- Insecure installation of operating system and applications lead to compromise

Discussion

All references available upon request

Ryan E. Moore
Special Agent
U.S. Secret Service
312-353-5431
ryan.moore@usss.dhs.gov

U.S. Secret Service