X-Force Exchange

Threat Intelligence Collection and Sharing

Ron Williams, STSM, Principal Architect
Chenta Lee, Senior Software Engineer
IBM

Agenda

- Threat Analyst Operations - ‘Getting to Go’
  - Threat evaluation, investigation, and mitigation
- The Power of Community - Getting in front of active Campaigns
- Demo - Identifying, Analyzing, Mitigating, and Sharing Active Threats
- Q&A

‘Getting to Go’ - Mitigating Active Infiltration

Alert - Business Relevant Investigation Candidates

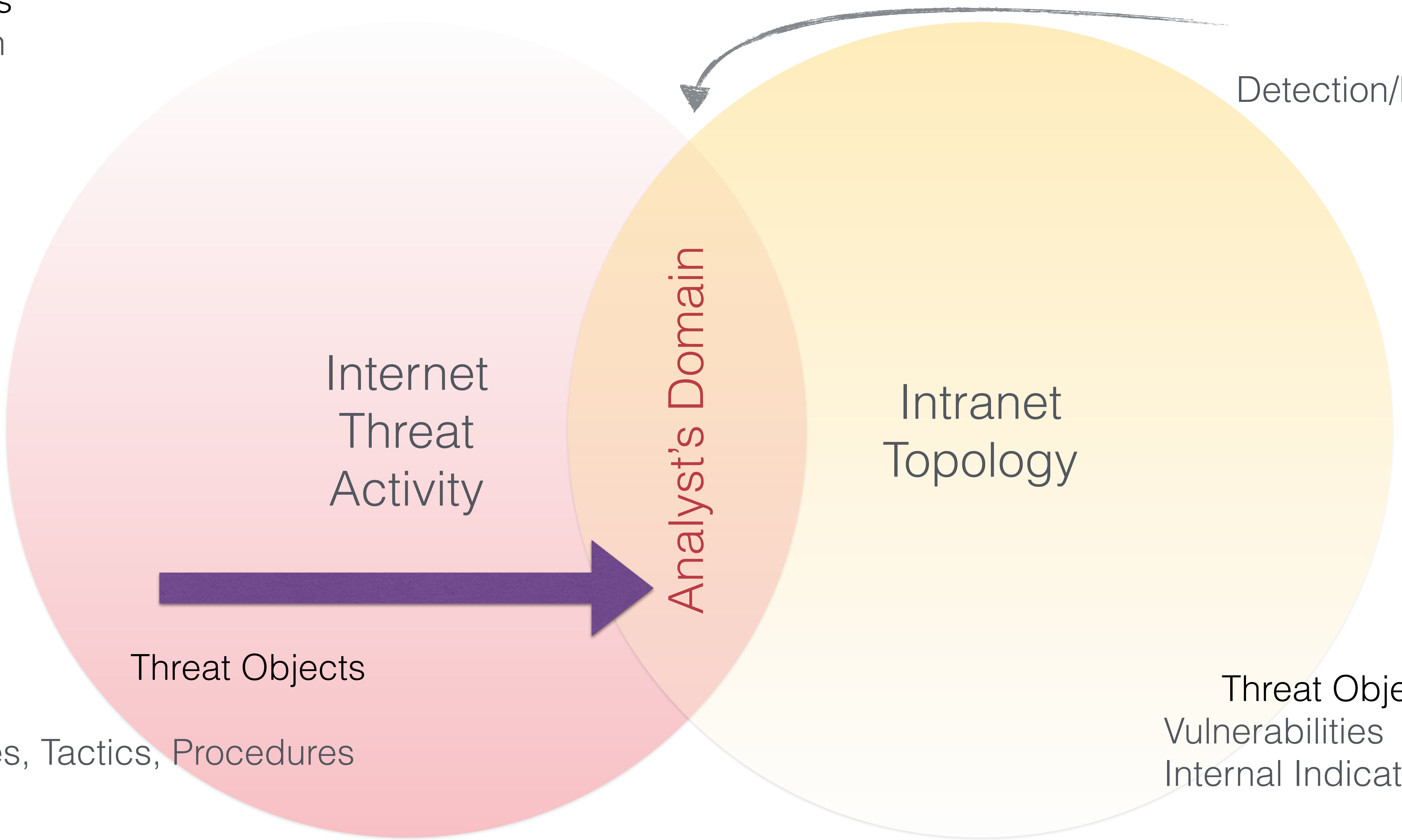
Research - History, Related IOCs, IPs, URLs, Malware - history & current activity

Mitigation - Business Risk Prioritization

Action Required - Analyst Coordination with IT & Network Operations

Use Cases
Prevention
Detection
Response

Analyst’s
Scope:
Detection/Response



Internet
Threat
Activity

Analyst’s Domain

Intranet
Topology

Threat Objects

Actors
Techniques, Tactics, Procedures
Indicators

Threat Objects
Vulnerabilities
Internal Indicators

Analyst Workflow

1. Potential Threat Identified

   (SIEM Alert, SPAM ID, Malware Scan)

2. Research Information Collection
   a. IP Reputation
   b. URL Reputation
   c. Malware History, Shared Information?
3. Validate - Edit - Report
4. Action - Report/Remediate/Share

KEEP

CALM

AND

WAIT FOR IT

infiltrating an enterprise

A. At hotel, want WiFi access in Lobby

B. Presented with ‘Hotel’s’ WiFi Finder App and promise of Free WiFi

C. Select ‘Connect’ - authenticate to O/S to permit installation

Powned

D. Urgent phone call - close laptop - leave town

back home in SOC

SIEM Alert - SRC 172.10.34.17   DEST **216.158.85.49**

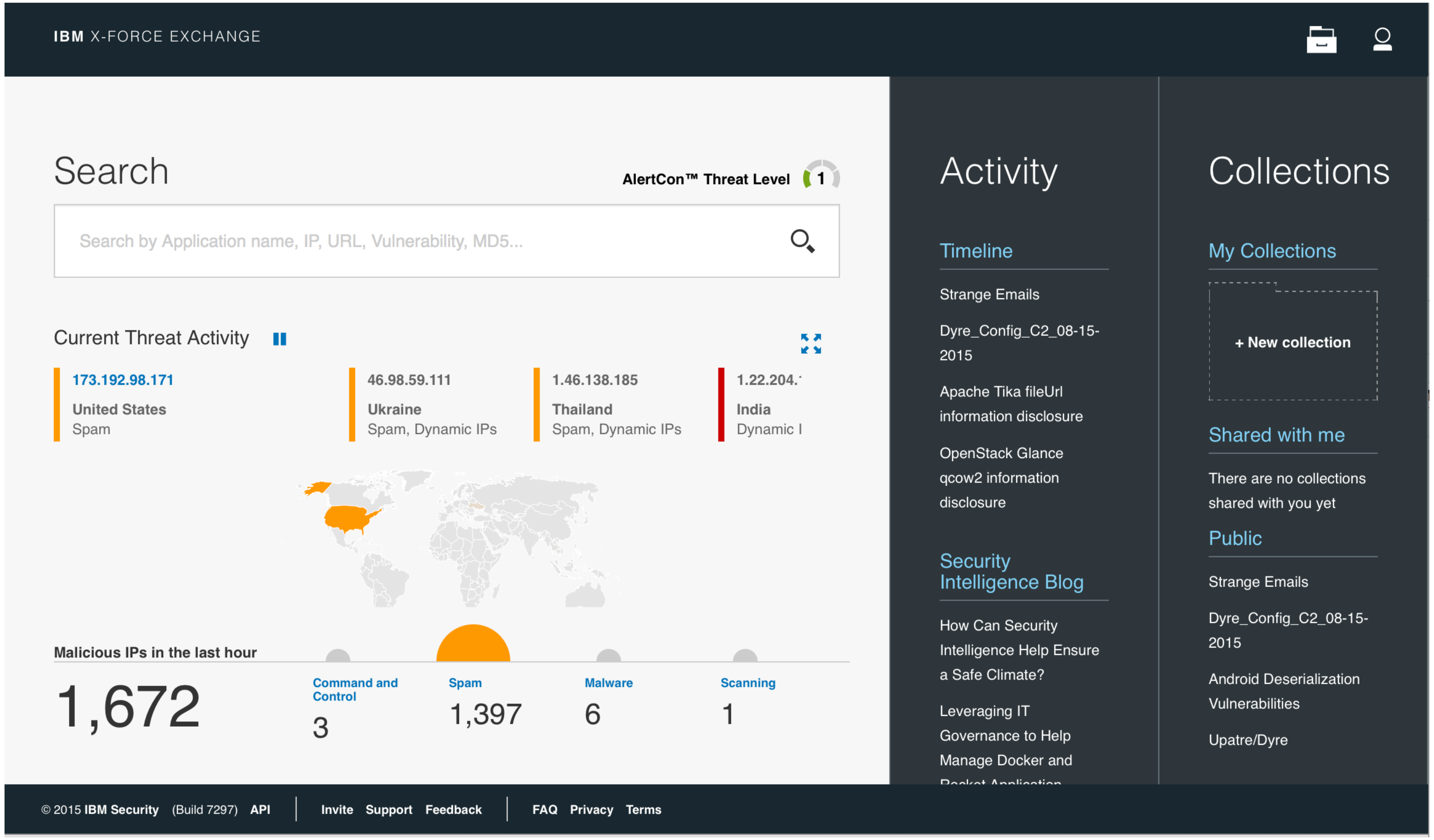
Identified C2 Communications

Response

- Identify SRC Machine from Asset Repository/Network
- Institute Malware Scan

Found Suspicious File MD5: 560d68c31980c26d2adab7406b61c651

demonstration



IBM X-FORCE EXCHANGE

Search

AlertCon™ Threat Level 1

Search by Application name, IP, URL, Vulnerability, MD5...

Current Threat Activity

173.192.98.171 United States Spam	46.98.59.111 Ukraine Spam, Dynamic IPs	1.46.138.185 Thailand Spam, Dynamic IPs	1.22.204. India Dynamic I

Malicious IPs in the last hour

1,672

Command and Control	Spam	Malware	Scanning
3	1,397	6	1

Activity

Timeline

Strange Emails

Dyre_Config_C2_08-15-2015

Apache Tika fileUrl information disclosure

OpenStack Glance qcow2 information disclosure

Security Intelligence Blog

How Can Security Intelligence Help Ensure a Safe Climate?

Leveraging IT Governance to Help Manage Docker and Packet Application

Collections

My Collections

+ New collection

Shared with me

There are no collections shared with you yet

Public

Strange Emails

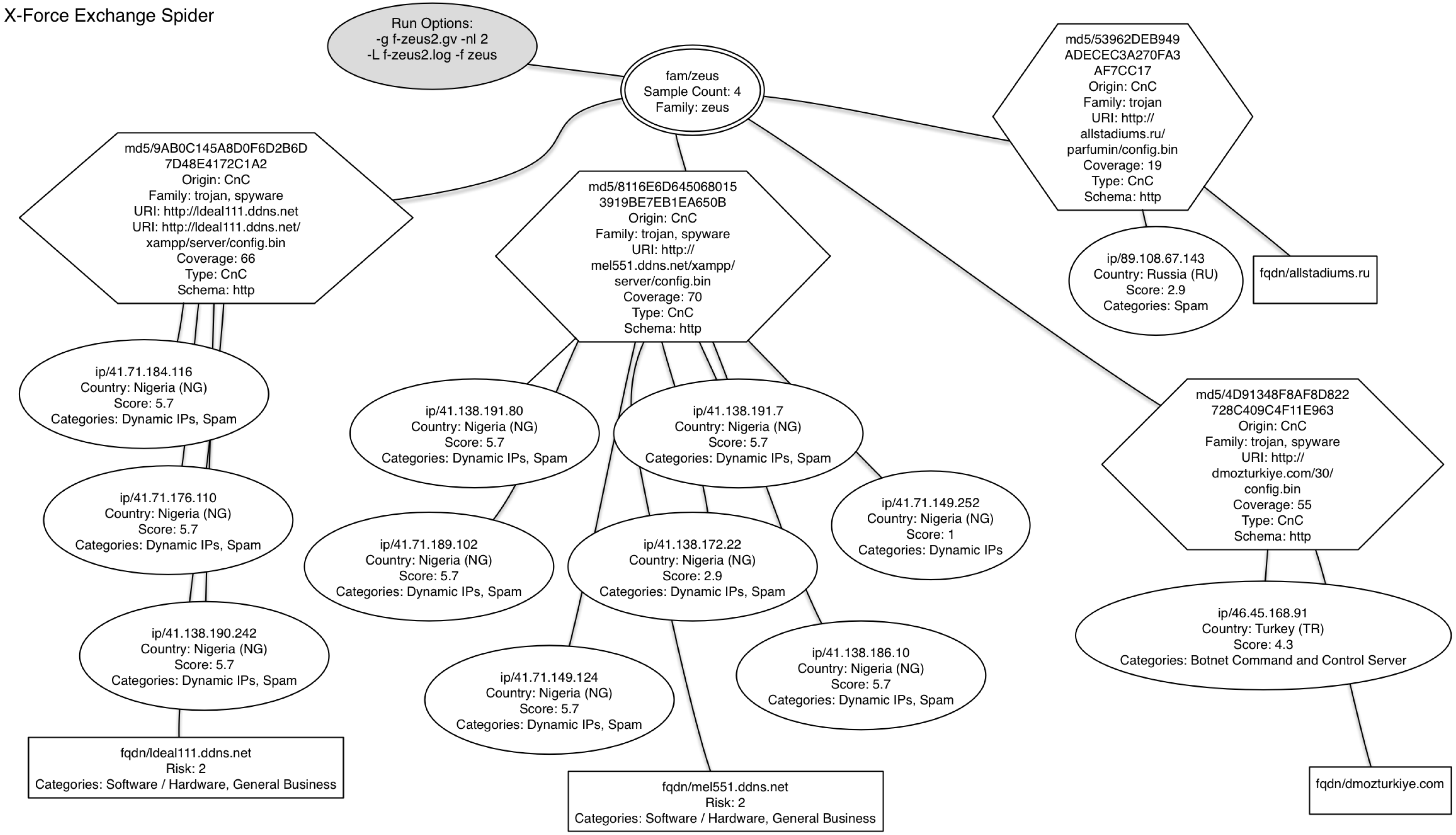
Dyre_Config_C2_08-15-2015

Android Deserialization Vulnerabilities

Upatre/Dyre

© 2015 IBM Security (Build 7297) API | Invite Support Feedback | FAQ Privacy Terms

threat data -> intelligence



X-Force Exchange Spider

Run Options:
-g f-zeus2.gv -nl 2
-L f-zeus2.log -f zeus

fam/zeus
Sample Count: 4
Family: zeus

md5/9AB0C145A8D0F6D2B6D
7D48E4172C1A2
Origin: CnC
Family: trojan, spyware
URI: http://ldeal111.ddns.net
URI: http://ldeal111.ddns.net/
xampp/server/config.bin
Coverage: 66
Type: CnC
Schema: http

md5/8116E6D645068015
3919BE7EB1EA650B
Origin: CnC
Family: trojan, spyware
URI: http://
mel551.ddns.net/xampp/
server/config.bin
Coverage: 70
Type: CnC
Schema: http

md5/53962DEB949
ADECEC3A270FA3
AF7CC17
Origin: CnC
Family: trojan
URI: http://
allstadiums.ru/
parfumin/config.bin
Coverage: 19
Type: CnC
Schema: http

ip/89.108.67.143
Country: Russia (RU)
Score: 2.9
Categories: Spam

fqdn/allstadiums.ru

md5/4D91348F8AF8D822
728C409C4F11E963
Origin: CnC
Family: trojan, spyware
URI: http://
dmozturkiye.com/30/
config.bin
Coverage: 55
Type: CnC
Schema: http

ip/41.71.184.116
Country: Nigeria (NG)
Score: 5.7
Categories: Dynamic IPs, Spam

ip/41.71.176.110
Country: Nigeria (NG)
Score: 5.7
Categories: Dynamic IPs, Spam

ip/41.138.190.242
Country: Nigeria (NG)
Score: 5.7
Categories: Dynamic IPs, Spam

fqdn/ldeal111.ddns.net
Risk: 2
Categories: Software / Hardware, General Business

ip/41.138.191.80
Country: Nigeria (NG)
Score: 5.7
Categories: Dynamic IPs, Spam

ip/41.138.191.7
Country: Nigeria (NG)
Score: 5.7
Categories: Dynamic IPs, Spam

ip/41.71.149.252
Country: Nigeria (NG)
Score: 1
Categories: Dynamic IPs

ip/41.71.189.102
Country: Nigeria (NG)
Score: 5.7
Categories: Dynamic IPs, Spam

ip/41.138.172.22
Country: Nigeria (NG)
Score: 2.9
Categories: Dynamic IPs, Spam

ip/41.71.149.124
Country: Nigeria (NG)
Score: 5.7
Categories: Dynamic IPs, Spam

ip/41.138.186.10
Country: Nigeria (NG)
Score: 5.7
Categories: Dynamic IPs, Spam

fqdn/mel551.ddns.net
Risk: 2
Categories: Software / Hardware, General Business

ip/46.45.168.91
Country: Turkey (TR)
Score: 4.3
Categories: Botnet Command and Control Server

fqdn/dmozturkiye.com

“We can’t share our threat findings …”

– An International Bank’s CISO

We’ve got an IOC, Don’t Tell Anyone

‘Anyone’ already knows

If we share it, it might get used against us

It’s already been used against you

Maybe it’s not that bad …

A public breach doesn’t improve with age.

‘It’ has already happened.

Let’s just deal with it.

what we can share (our experience)

Attack Flow

Suspect Internet IP’s & URLs

Identified Malware Signatures

Other IOC’s (Registry Keys, dropped files, command files, executables, etc.)

Meaningful Correlations

Significant data to assist the 2nd analyst

what we (typically) don’t share

- internal infrastructure (internal networks, ip’s)
- 0day application and system vulnerabilities (unublished)
- target specific data (individuals, accounts, etc)

Q&A

https://exchange.xforce.ibmcloud.com

Ideas

‘What is the role of Threat Intelligence Sharing?
Won’t the Attackers Use it against us?
Why ‘Collections?’
How do I know good intel from bad?
What about misdirection?
What about privacy?

The Unthinkable or Unacceptable is not the same as the Impossible.

Plan for it - or it will plan for you.

– Anonymous

https://exchange.xforce.ibmcloud.com

ron williams, senior technical staff member
chenta lee, sr. programming engineer
ibm security