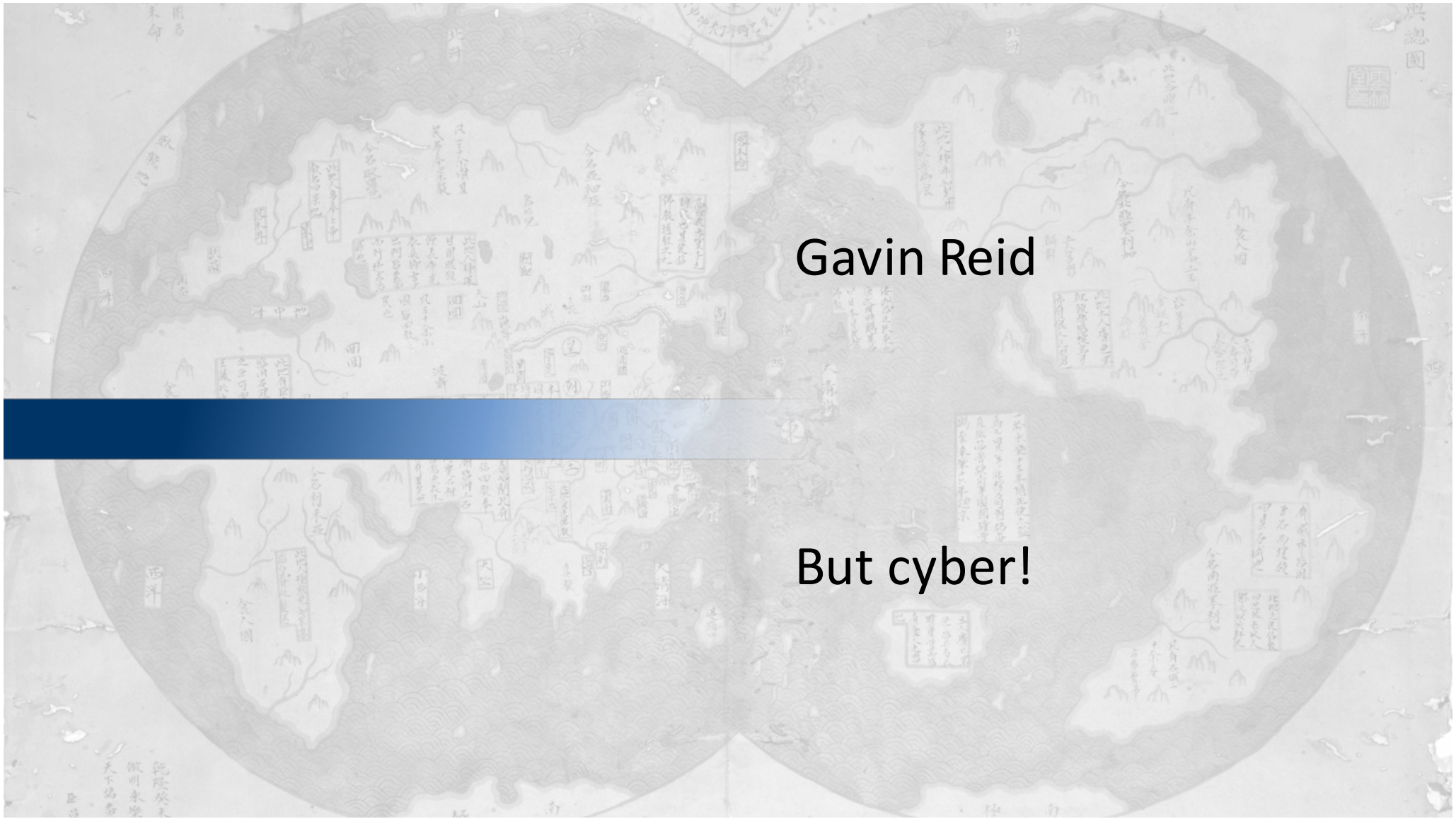
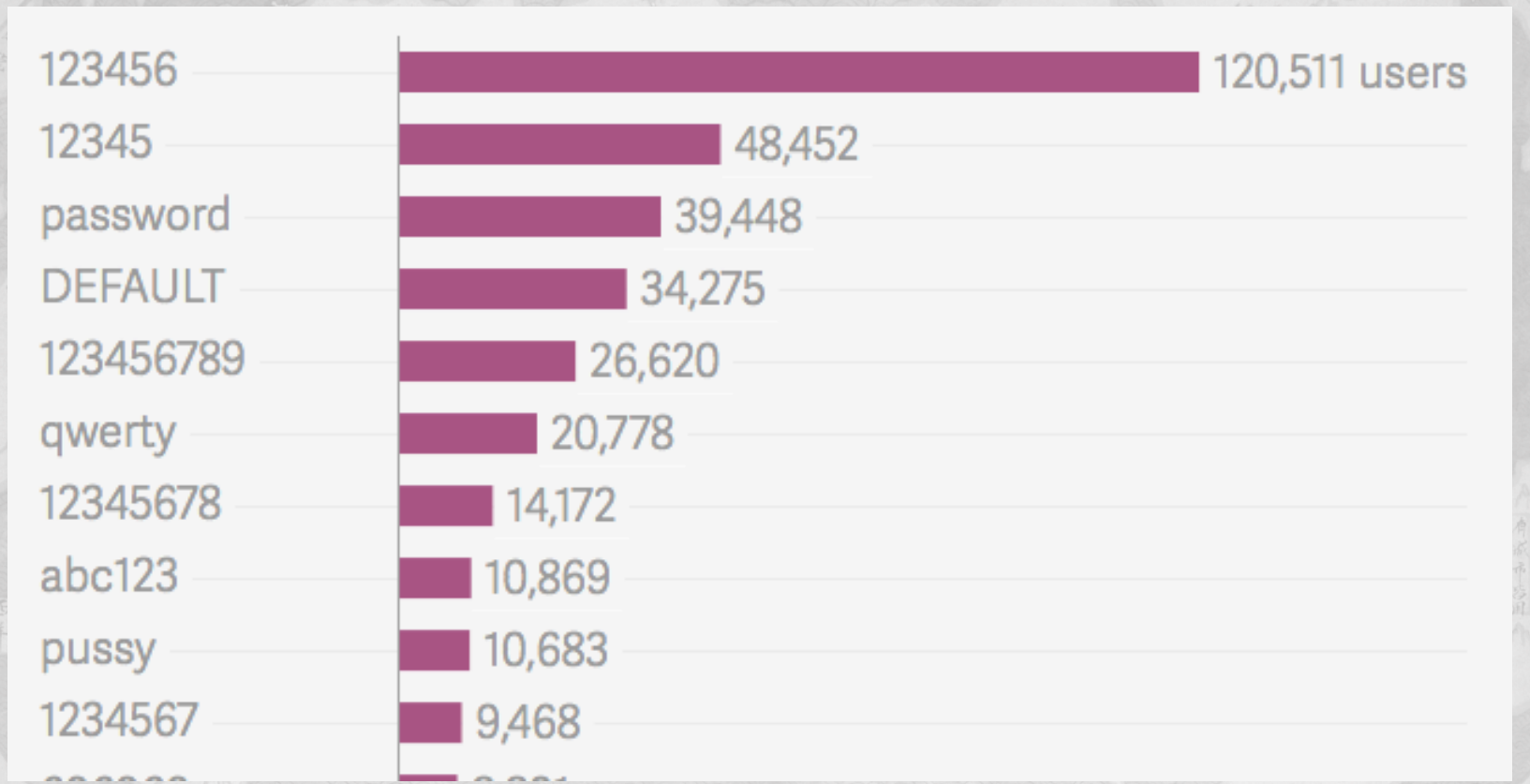


Gavin Reid

But cyber!


NEW EPISODE
CN HD

Where are we with security in 2016?


123456
120,511 users
12345
48,452
password
39,448
DEFAULT
34,275
123456789
26,620
qwerty
20,778
12345678
14,172
abc123
10,869
pussy
10,683
1234567
9,468

RISK ASSESSMENT / SECURITY & HACKTIVISM

DHS infosec chief: We should pull clearance of feds who fail phish test

Repeat offenders "should not be holding a TS SCI with the federal government."

by **Sean Gallagher** - Sep 21, 2015 12:00pm EDT

Share Tweet 123

In the wake of the Office of Personnel Management hack this year, which reportedly took advantage of a phishing attack to steal credentials used to gain access to highly sensitive personnel records, US federal agencies have been increasing their security training and employee testing around phishing. In addition to the employee awareness campaign launched by the National Counterintelligence and Security Center, more agencies are using security auditing tools that simulate phishing attacks against employees to test whether the employees abide by their information security training. Those who fall for phishing tests are generally either required to take a security refresher class or at worst are publicly called out for their errors in agency e-mails.

Enlarge / Paul Beckman, the DHS' chief information security officer, thinks repeat phishing failures should get an employee's clearance pulled.

But at least one federal chief information security officer thinks that these steps aren't enough and

The state of the industry…

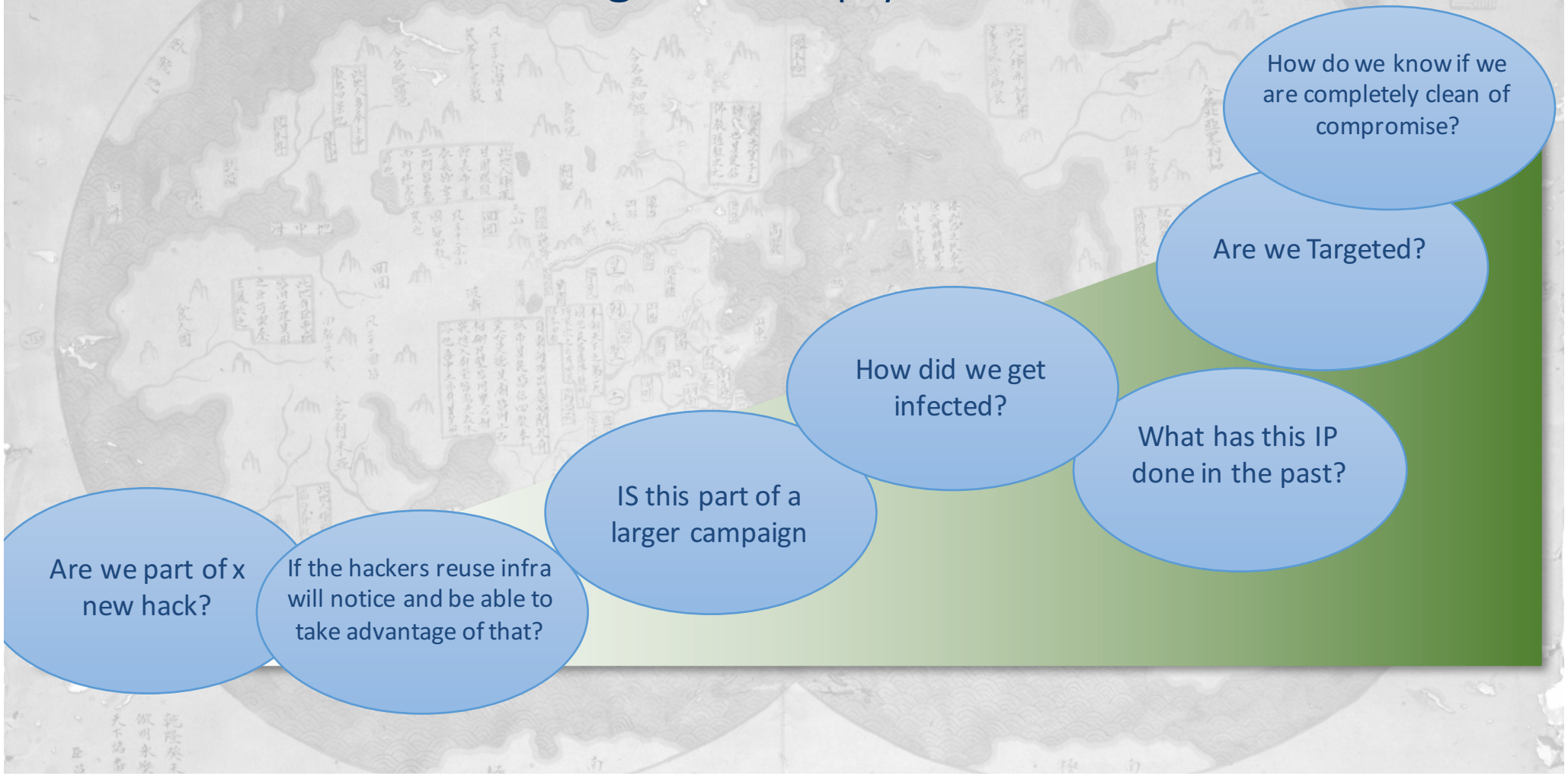
What we need to do differently…

What is threat?

What is intelligence?

intent, capability and opportunity

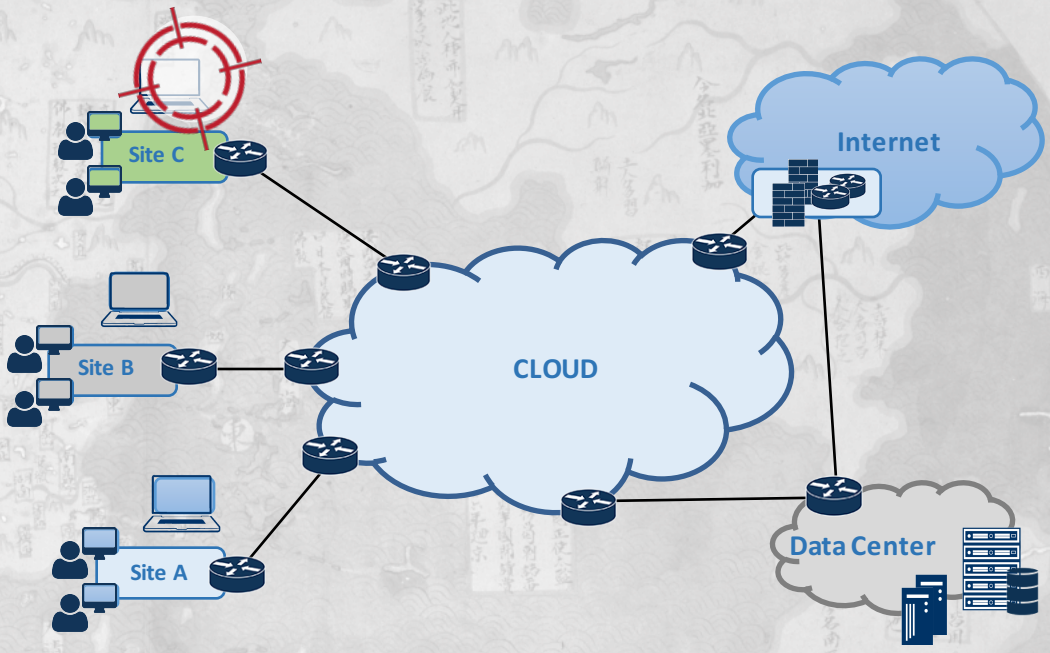
What can threat intelligence help you with?



Indicators of Compromise…

"An IOC is an observable artifact of an intrusion on a host or network. Analysts can use it to trace the steps of an attack and identify what was affected, how long it was active or if there are any persisting elements of the intrusion."

- Observables
- Measurable events
- Stateful properties



What is an indicator?

* Full list at http://openioc.org/terms/Current.iocterms

IP with no (or invalid) context…

IP with context…better

Malware: Dridex

Attachment File Name: RZZA3440.doc

Attachment MD5s:
b4fe7224da594703e78d62d9cb85c5f4c3a00c36
ea51040c3a10c557154bc7b15b9acbcd6555539
8a7e3fd0f0a389cf9582b75b4f8855dbe555bff08
0c57808aBe699ba4855340adf5c9d7092e9df08
b

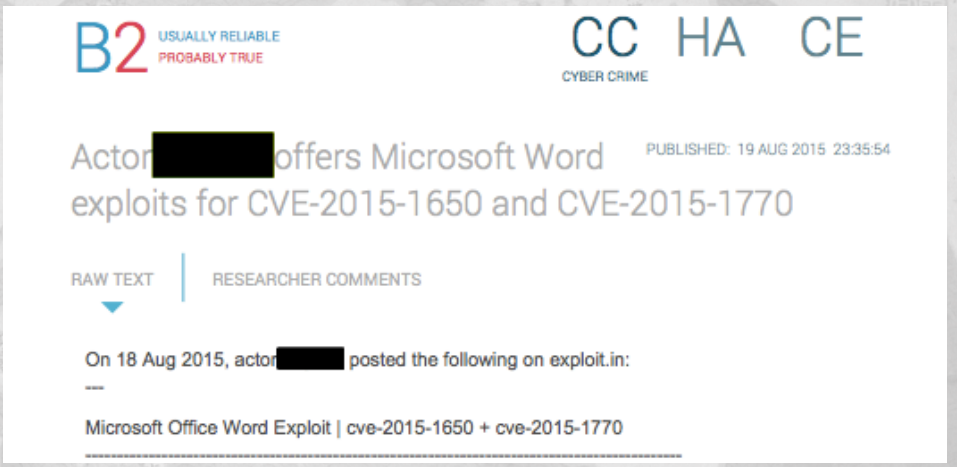
Payload URLs:
hxxp://internetz1[.]com/03/39.exe
hxxp://gggrp[.]com/03/59.exe
hxxp://fefg[.]com/03/39.exe
hxxp://woofe[.]com/03/39.exe
hxxp://contestswin[.]net/03/39.exe

Payload MD5:
5e91af2e44c17de55134ff935c0f30f1

C2:
130.0.133[.]35

Intelligence– best

Investigator finds new malware in word doc used in spearphish
– hashes file 7c47ff87c0frca93e135c9acffee48d3f
– Sandboxes and Finds c2
Query TI dbase (Intel 471) finds that same file/C2 has been used before by a specific hacker group X



Group X uses various hacker forums, IRC, samples , URLS and C2's

Check nF for IRC connections to server. Runs the new IOCS into comparison engine and finds other infections – helping organization completely understand and fix the problem

Progression? of detection capabilities

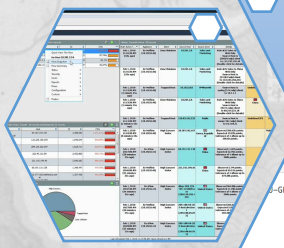
Exploit Sigs (IDS/HIDS)

Anti Virus

Getting hacked

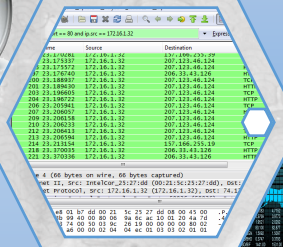
Logging

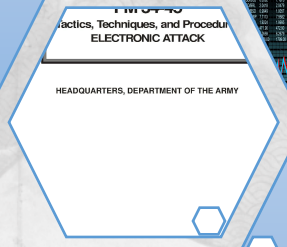
NBAD/nF



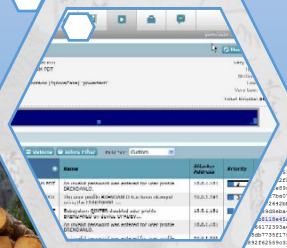
DPI attack sigs (Yara)

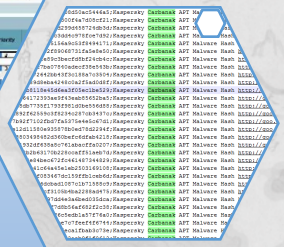
SIEM





IOCs





PCAP

Big Data/Analytics

Nirvana

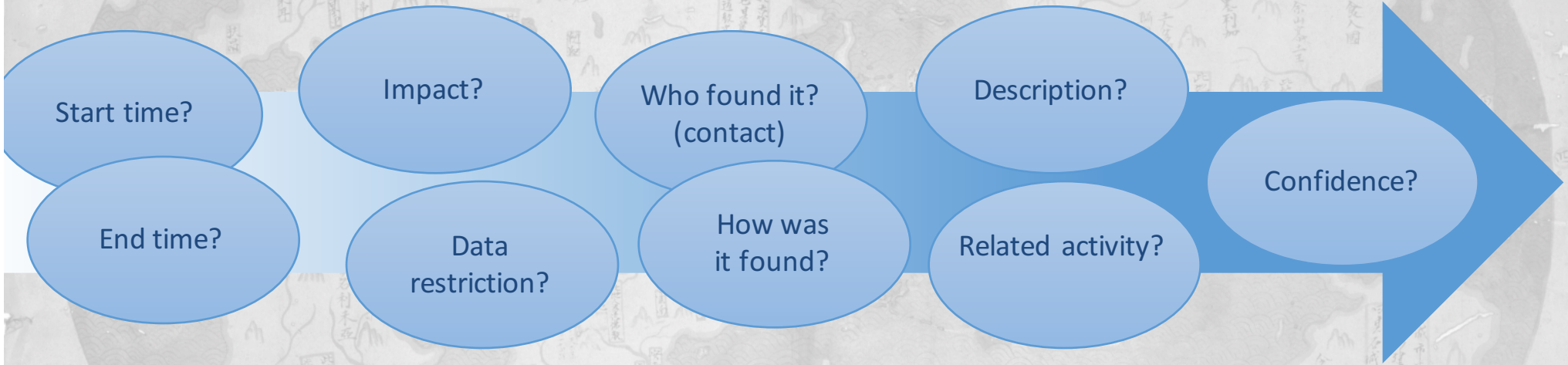
TTPs

Feeds…

Sources…(providers)

- Industry Orgs
- Secret Groups
- Vendor Threat Intel
- First Party Data
- Government Orgs
- Peer Groups
- Open Source
- CIRTS
- ISACS

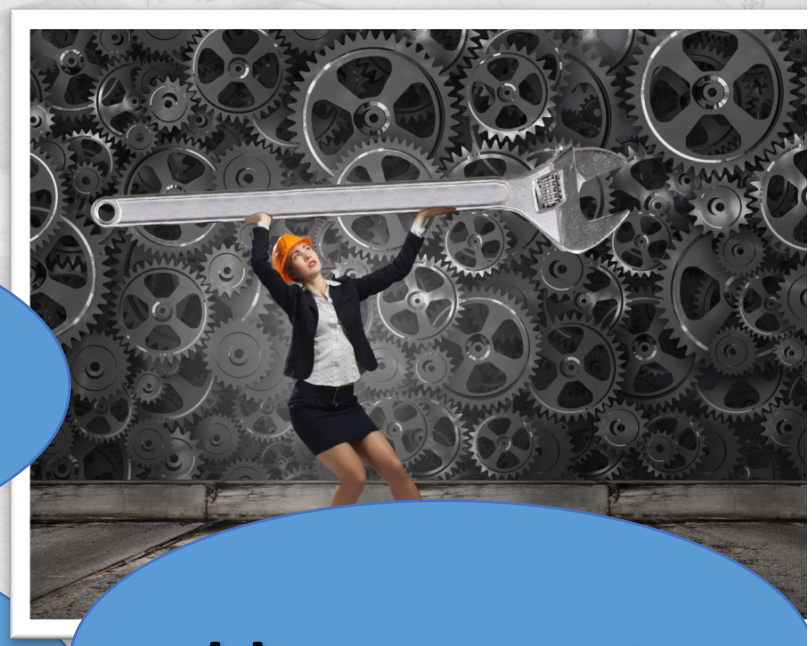
What IS context?



Data Enrichment…

- Whois
- GeoLocation
- ★★★ Reputation
- History
- Hash
- PDNS
- VirusTotal
- Sandboxing
- Confidence

Where does the data come from



Customer data

Web

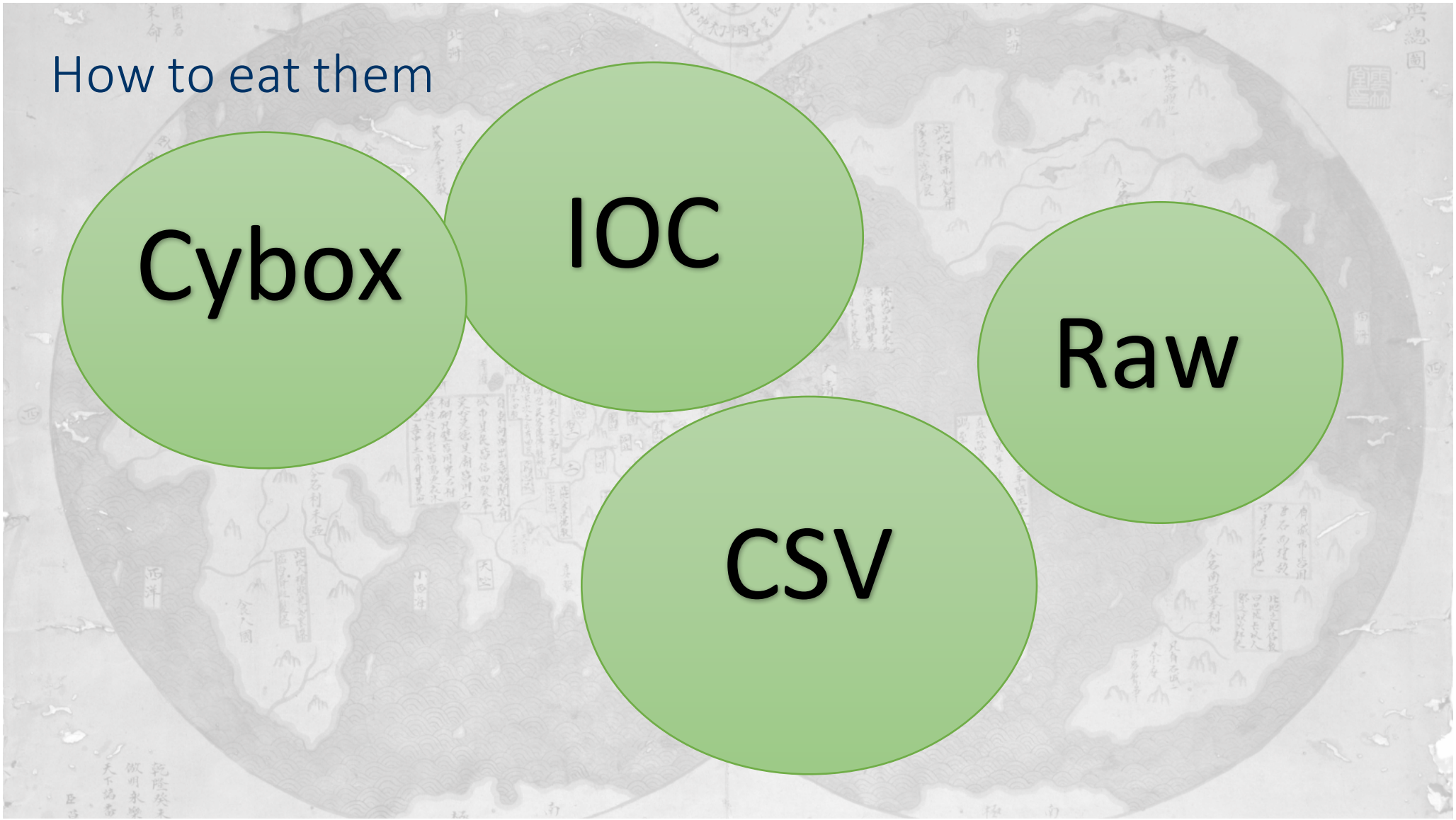
Honeynets

Scanning
Crawling

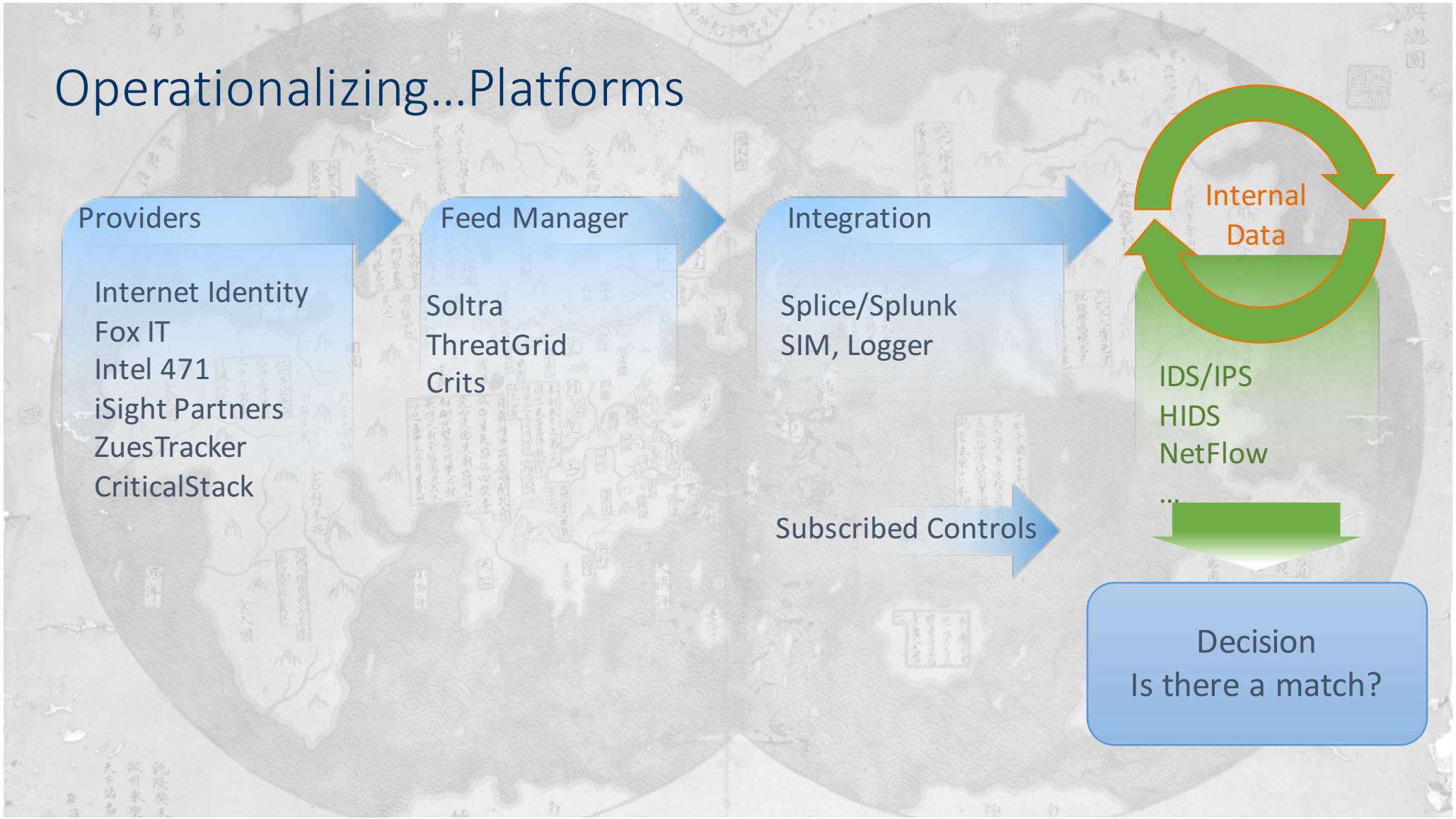
Malware processing

Human INT

How to eat them

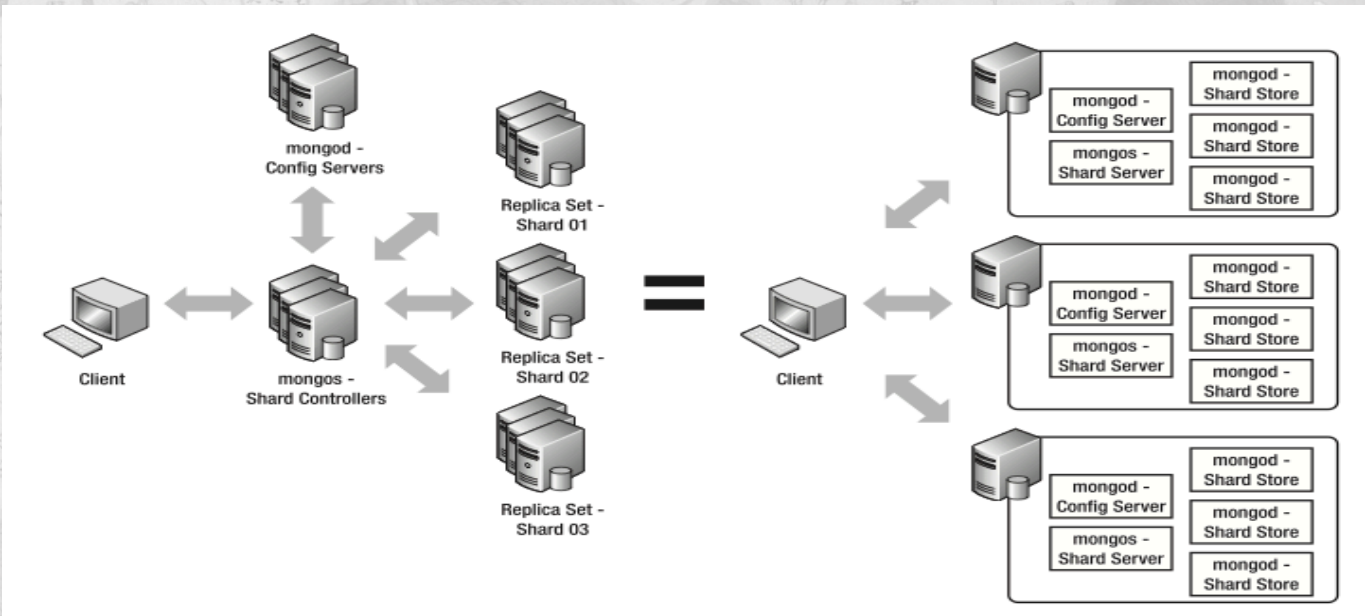


Operationalizing…Platforms



How does Cisco do it

- Python/Django front end UI
  - Apache or Django runserver
- MongoDB backend
  - Fault Tolerant
  - High Performance
  - NO SQL
  - Mongo FS for files
- Document based
  - Files and metadata



What does CRiTs look like

Welcome, Mike Scheck. | Role: Administrator | A | Go

Top Backdoors

Name	Samples
DPD	1
PIVY	

Top Campaigns

Name	Emails	Indicators	Samples
Group 3	0	2067	1
Group 17	0	818	11
Group 16	0	68	0
Group 13	0	13	0
Group 10	0	0	0

Latest Indicators

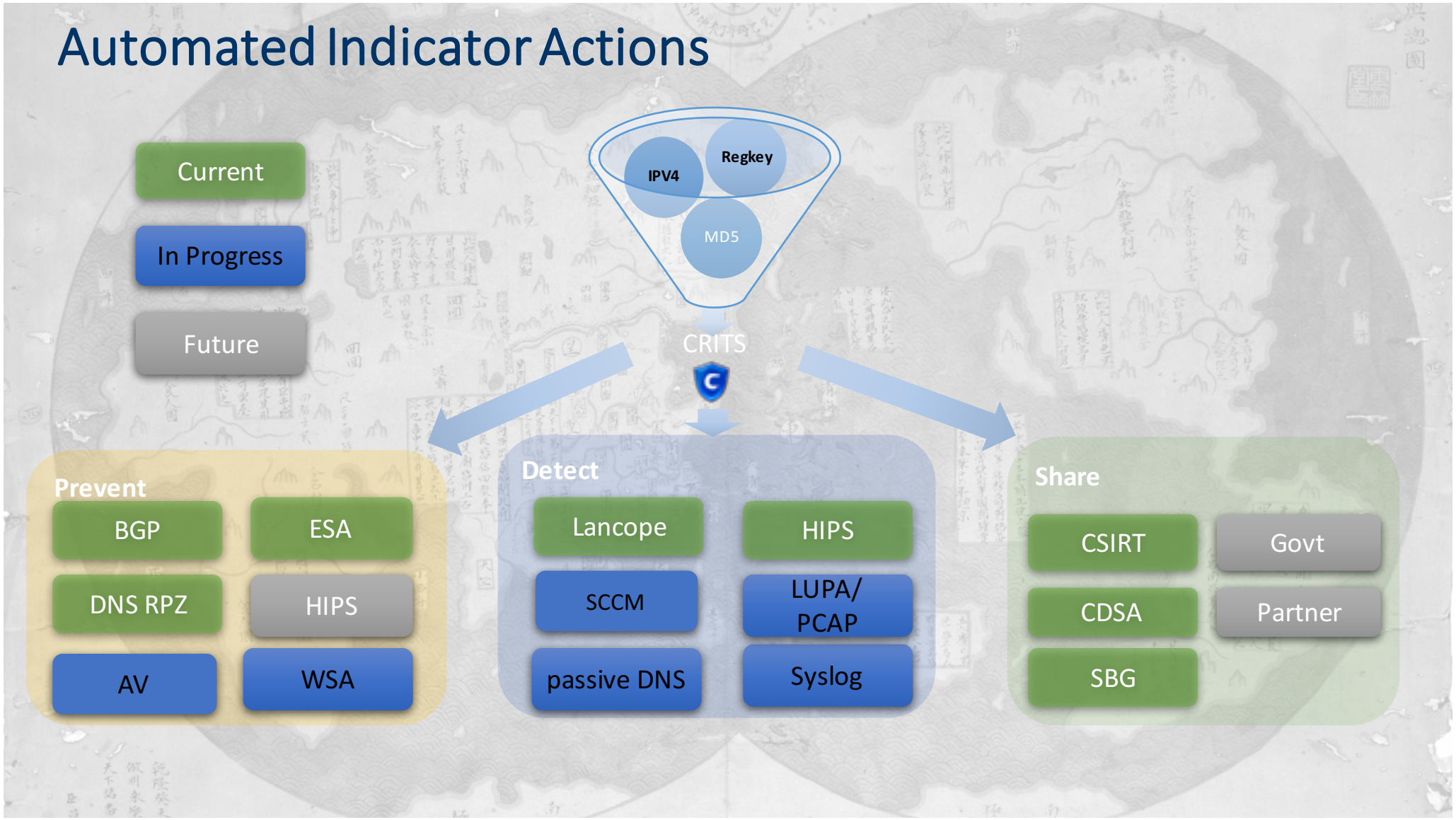
Value	Type	Date Added	Campaign	Source	Status
mx.xmlflash.net	Domain	2013-11-14	Group 3	OTHER	New
www.nbsd.k12.ms.us	Domain	2013-11-14	Group 4	OTHER	New
/serv/pte.exe	Domain	2013-11-14	Group 4	OTHER	New
www.myspace-login.com	Domain	2013-11-14	Group 4	OTHER	New
2014 individual income tax credit policy	String	2013-11-14	Group 4	OTHER	New

Recently Added/Modified Samples

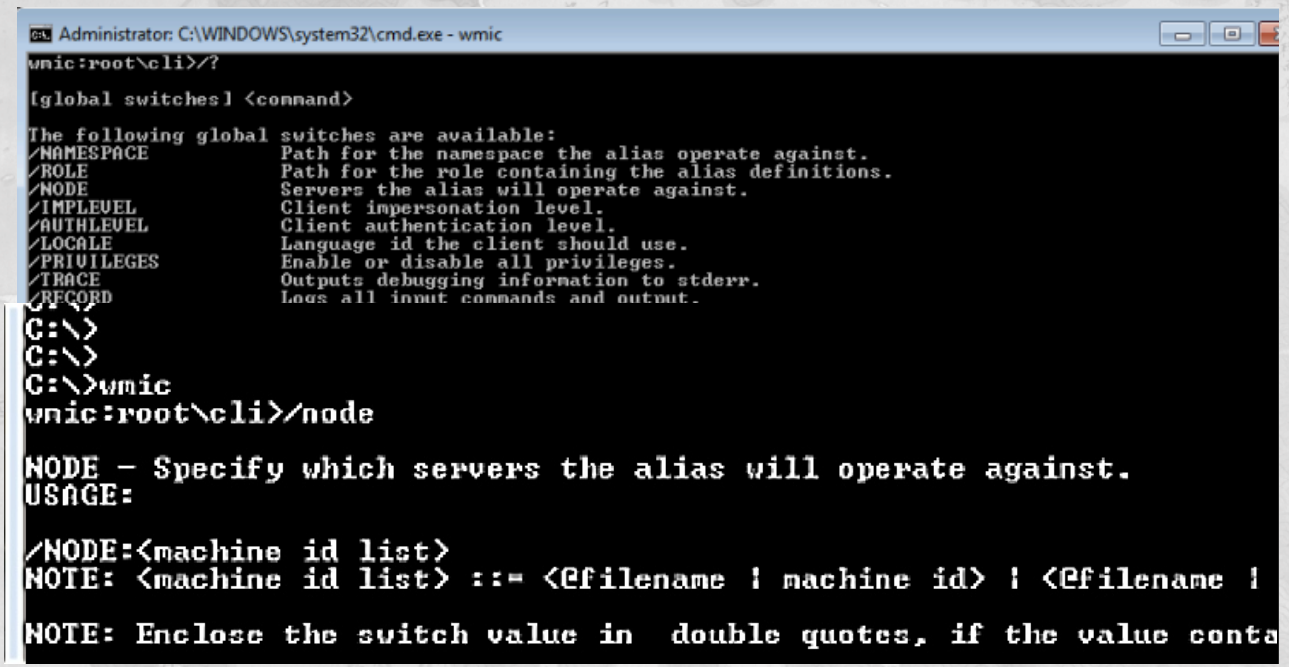
Filename	Size	Filetype	Receive	Backdoor(v)[C]	CVE
jack246.exe			08/12/2013		
Sample 60eed7a7c5f4f4aeace594e2e4d180a0.exe_carver			08/12/2013		
c5eb1cff314e4d682b1315dfab44e7dd			08/12/2013		
Sample 68aee94684ba33d1e5d97d7d27d0fe13.exe_carver			08/12/2013		

Hosted by: CISCO | CSIRT Instance (DB: crits) | Last login: 2013-11-08

Automated Indicator Actions



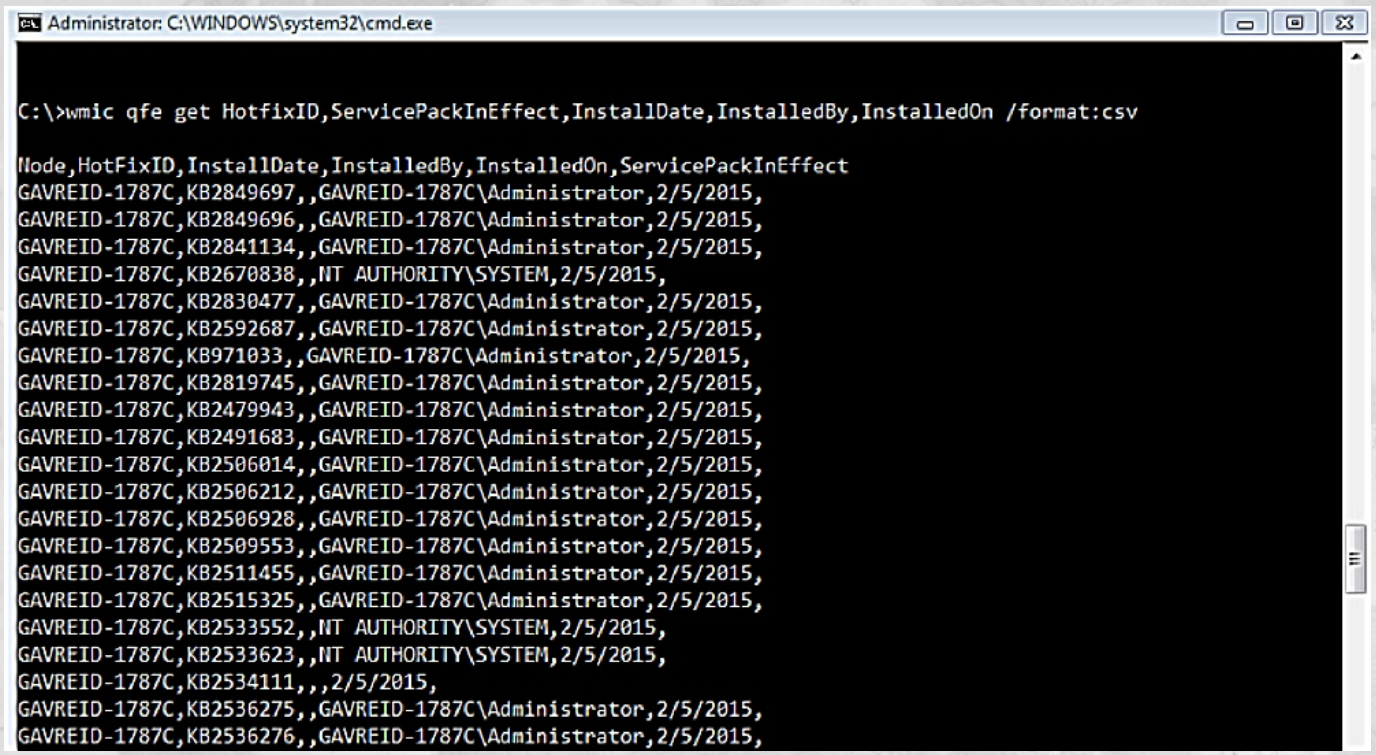
What about techniques



wmic /node:"@server-targets.txt" service get name

wmic /node:"machine-FQDN" service get name

So what could you do

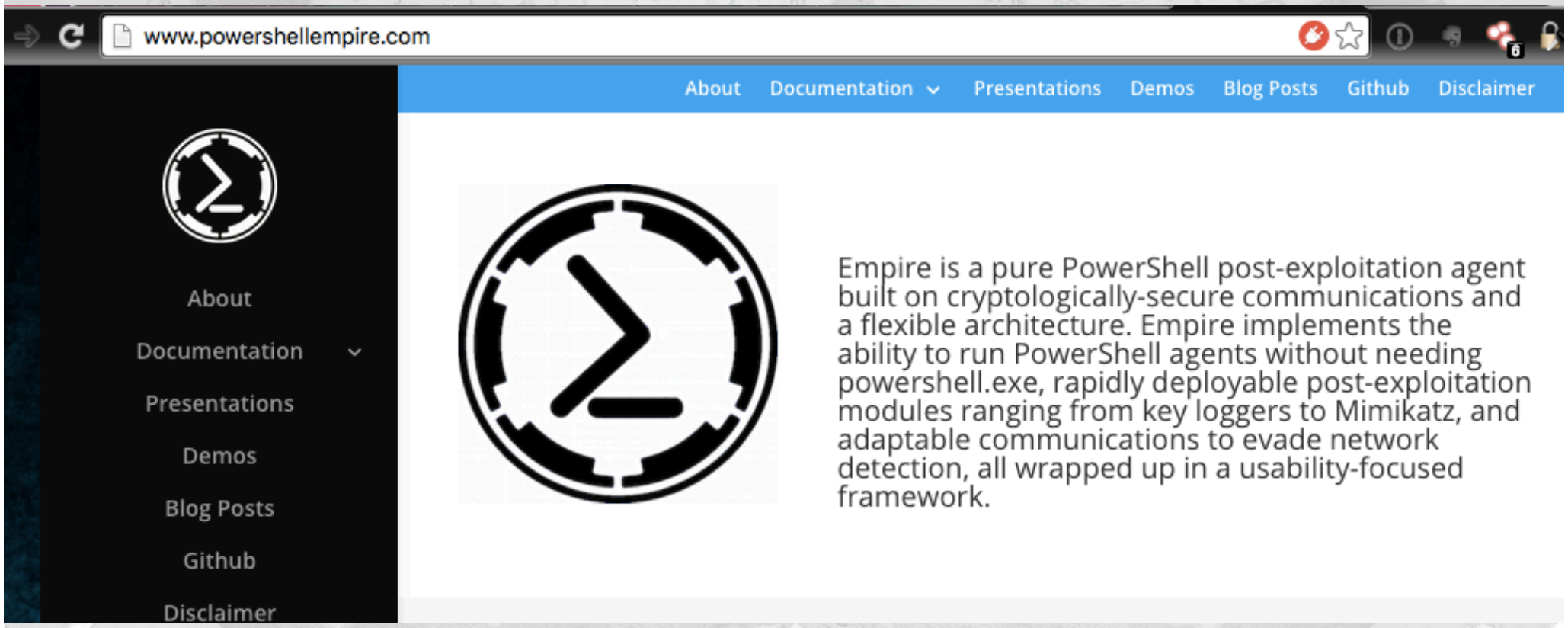


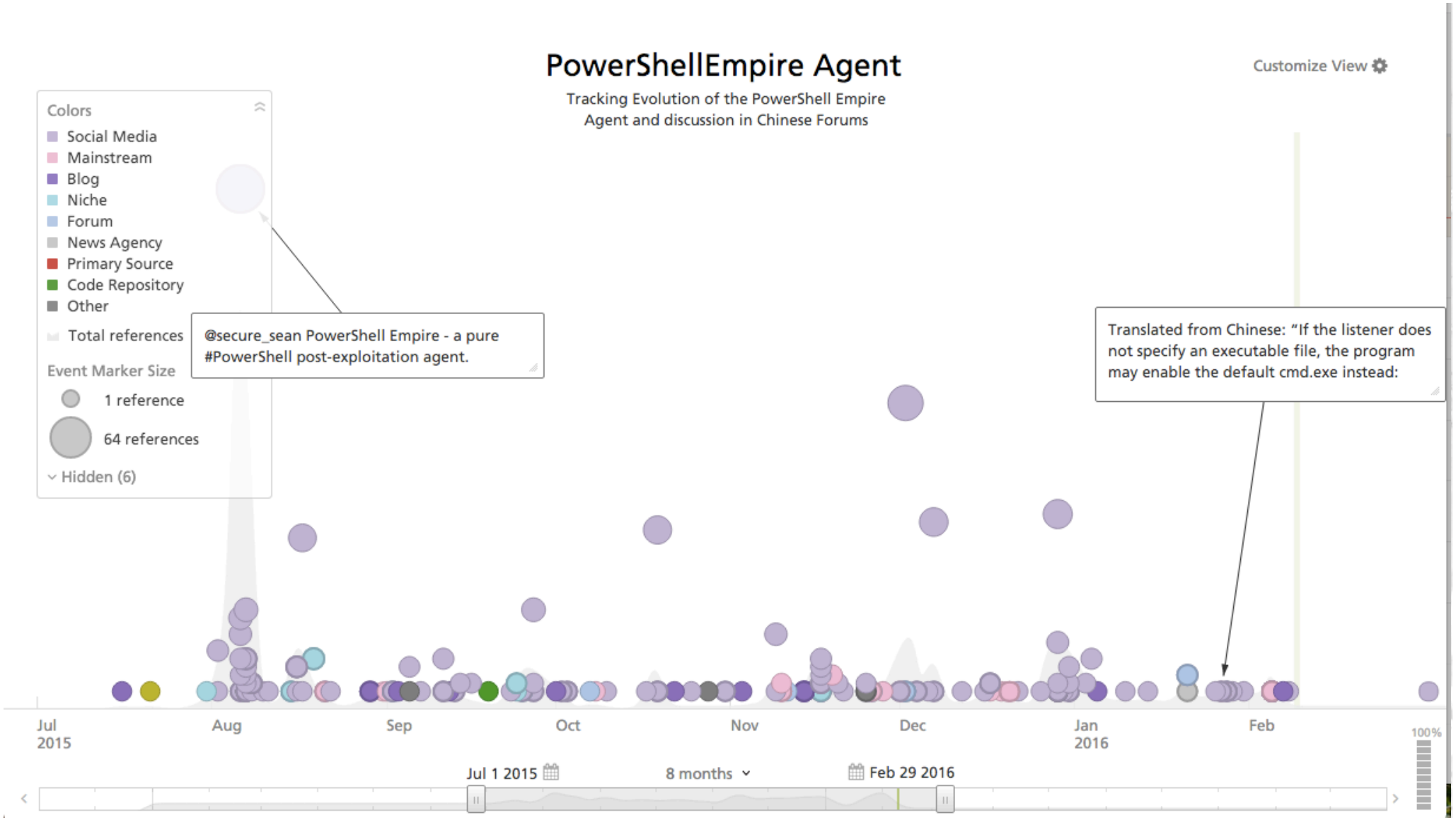
C:\>wmic qfe get HotfixID,ServicePackInEffect,InstallDate,InstalledBy,InstalledOn /format:csv

Powers(hell)

Set-ExecutionPolicy	Mimikatz	EncodedCommand	Find-AVSignature
DllInjection	Invoke-Shellcode	Get-Keystrokes	Get-TimedScreenshot
Invoke-CredentialInjection	Invoke-PSInject	Invoke-ServiceStart	Get-RegAutoLogon
Add-ScrnSaveBackdoor	Invoke-ServiceUserAdd	Write-ServiceEXE	Invoke-TokenManipulation

Where?


www.powershellempire.com
About
Documentation
Presentations
Demos
Blog Posts
Github
Disclaimer
About
Documentation
Presentations
Demos
Blog Posts
Github
Disclaimer
Empire is a pure PowerShell post-exploitation agent built on cryptologically-secure communications and a flexible architecture. Empire implements the ability to run PowerShell agents without needing powershell.exe, rapidly deployable post-exploitation modules ranging from key loggers to Mimikatz, and adaptable communications to evade network detection, all wrapped up in a usability-focused framework.


PowerShellEmpire Agent
Tracking Evolution of the PowerShell Empire
Agent and discussion in Chinese Forums
Customize View
Colors
Social Media
Mainstream
Blog
Niche
Forum
News Agency
Primary Source
Code Repository
Other
Total references
Event Marker Size
1 reference
64 references
Hidden (6)
@secure_sean PowerShell Empire - a pure #PowerShell post-exploitation agent.
Translated from Chinese: "If the listener does not specify an executable file, the program may enable the default cmd.exe instead:
Jul 2015
Aug
Sep
Oct
Nov
Dec
Jan 2016
Feb
100%
Jul 1 2015
8 months
Feb 29 2016

Making it intelligent

What do you do with this data to help your organization

- Detecting this technique means logging WMIC & Powershell
- Pull logs from at least your server environment
- Whitelist know good and alerting on all else
- Empire commands get investigated immediately

Maturity…

Low: most indicator-based; IP-based blocking; only able to consume tactical products.

Medium: indicators are grouped and have context; Indicator to internal data comparisons automated. Mix of 3rd party with some first party

High: production of unique and relevant products for different internal customers; Used for prioritization of security arch. Automatic subscription of high fidelity data to security controls. HI-FIDELITY FIRST-PARTY

Can you protect what you can't see?

Thanks!