



Homeland
Security

Situational Awareness Threat Report (SATR)

Presenters: Stacie Green & Casey Kahsen

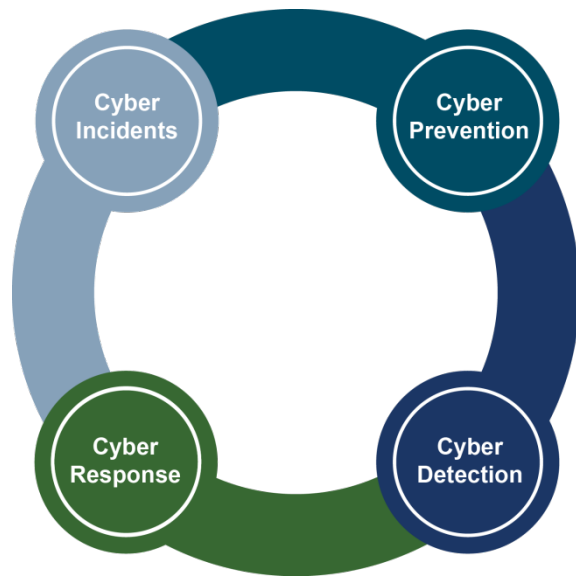
United States Computer Emergency Readiness Team (US-CERT)
13 January 2016

Outline

1. Goal of SATR
2. Overview of SATR
3. Components of SATR
4. Accomplishments of SATR
5. Standardized Reporting
6. Conclusion



Situational Awareness Threat Report Goal



Who is being attacked?
Who is attacking?
What is the impact/magnitude of the attack?
What is the likelihood of attacks and the risks?

ISP validation and awareness
Signature development and deployment

Aware of types of attacks on sectors
Development of means of identifying potential compromises

Machine speed alert capability
Capabilities to enhance computer network defense mitigation actions



.COM Reputation Service & Situational Awareness Threat Report (SATR)

Scripts Pull Data

Extraction and Transformation Scripts



Open Source Feed



GFI



Commercial Feed

Raw Data Storage

Store threat data for analysis



Scripts Ingest

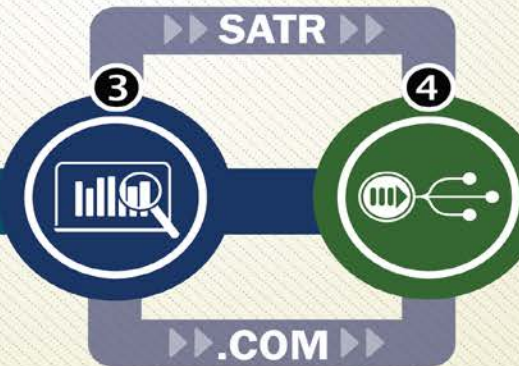
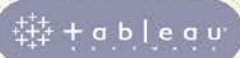
Collected data is parsed into feeds and provided to Northrop Grumman for analysis



Analyze

Situational Awareness Threat Report (SATR)

- Run query scripts
- Generate graphs
- Generate report



.COM Reputation Score

- Query data
- Execute scoring algorithm
- Assign score

Output

Situational Awareness Threat Report (SATR)
Customizable report that captures malicious events and offers information for critical decision making



.COM Reputation Score
Provides insight into active malicious indicators



Homeland Security

National Cybersecurity and Communications Integration Center

Overview: Data Sources

102 total ingested feeds
~750M raw records ingested daily



BIG DATA



GLOBAL THREAT PERSPECTIVE

~250,000 unique IPs processed per day

30-50 malicious domains reported daily



QUERIBLE INDICATORS

- IPs
- MD5
- Domains
- URLs
- APT Activity
- Malware family
- CVEs
- NAICs/Sectors



Overview: Reporting Capabilities



Customizable
Reporting



Correlation of
Federal and
Commercial
Threat Data



Big Data
Visualizations



Reporting on
Critical
Infrastructure
Sectors



Component: Threat Actors

Reporting Example: Threat Actors

APT Indicators Monitored for Activity

- Provides insight into high priority indicators that have been previously associated with threat actors and focused operations
- Illustrates potential threats that haven't been reported
- Offers view of potential focused operations activity from commercial data perspective

2 | Threat Data at a Glance

Pertinent high level data summarized. Identifies threats trending up or down from various feeds.

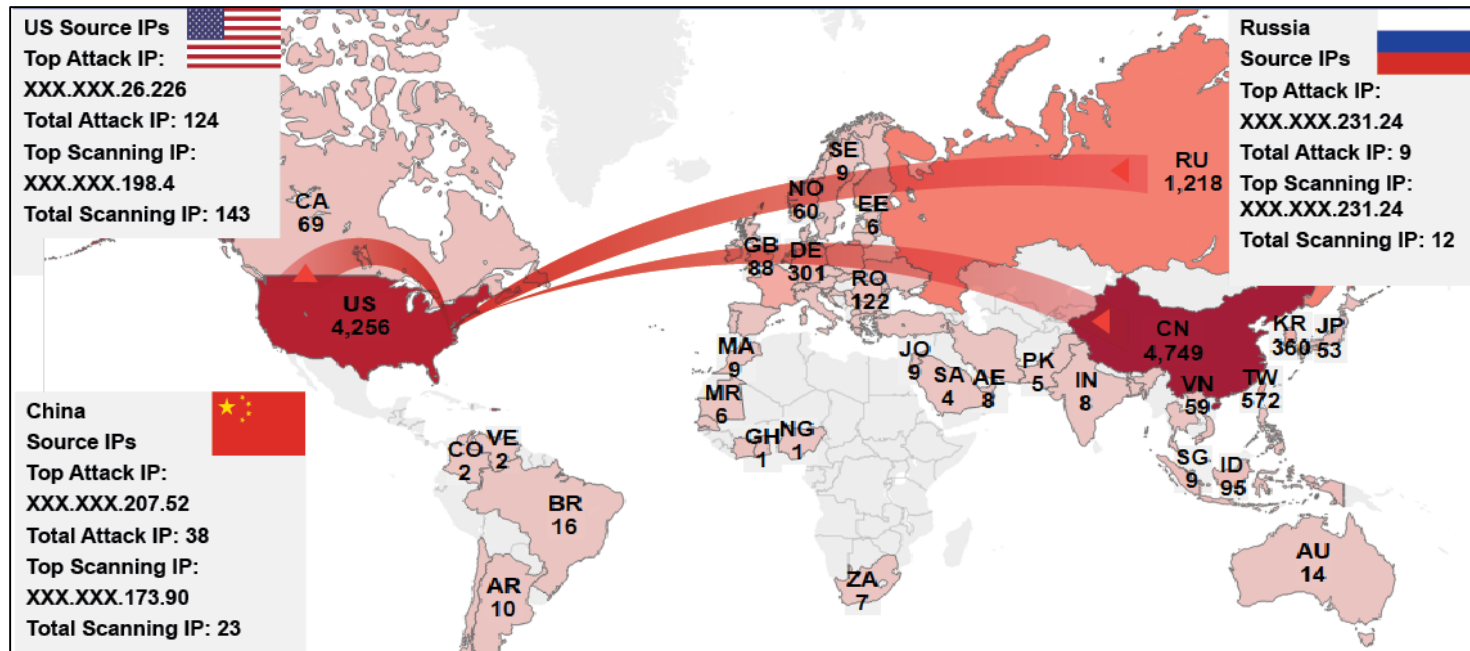
Focused Operations: iSight Cyber Espionage

XXX.XXX.78.68

- Wisp Team: Intel
- Sykipot Malware
- YumRAT Payload



Component : Government Targets



Depicts Attacks Against U.S. Government

Illustrates Top Indicators from Countries of Interest

By Source Country

- By most counter-measures triggered
- Two categories: Attacking & Scanning



Component: Vulnerabilities

CVEs Trending Up by Count of Submission

Vulnerability	CVSS Score	Snort Signature (Rule ID)	Vulnerability Type	Observed Increase
CVE-2015-5119	10.0		Denial of Service Execute Code Overflow Memory Corruption	+23 ▲

Image Depicts Report for 8/3/2015

Daily Report Monitors Exploit Usage

- Provide exploit trending
- Indicates usage patterns
- Can drive decision making



Component : Vulnerabilities



Top Cyber News

This section establishes trends in news relating to cyber security and threat incidents in the last 24 hours. This list is generated by reviewing trusted sources and selecting and prioritizing high interest articles.

[Newest RIG exploit kit driven by malicious advertising](#)

August 3, 2015

RIG's author has released version 3.0, which was recently discovered by researchers from Trustwave. The latest version uses malvertising in order to deliver a majority of its traffic, infecting some 1.25 million systems to date.

Tag: Vulnerability & Exploitation

Source: <http://www.csoonline.com>

Reporting Example: Vulnerabilities

Report From Next Day

- Article describes RIG's use of CVE-2015-5119
- Reported previous day with an uptick of activity
- Example of threat forecasting

Image Depicts Report for 8/4/2015

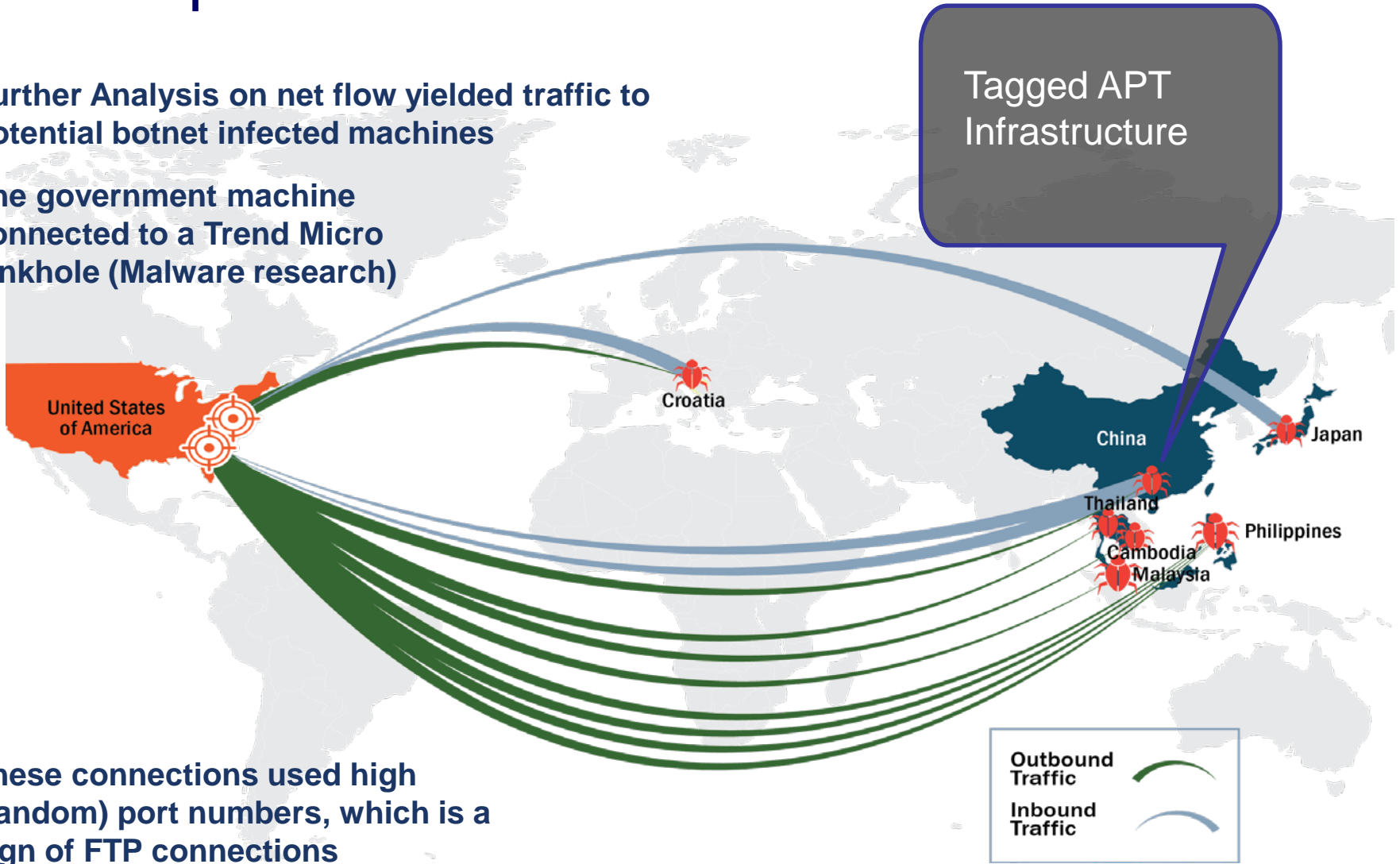


Accomplishments of SATR

Further Analysis on net flow yielded traffic to potential botnet infected machines

The government machine connected to a Trend Micro sinkhole (Malware research)

These connections used high (random) port numbers, which is a sign of FTP connections



Accomplishments of SATR

Operational Success Use Cases



Potential reduction in data exfiltration from public facing government FTP servers



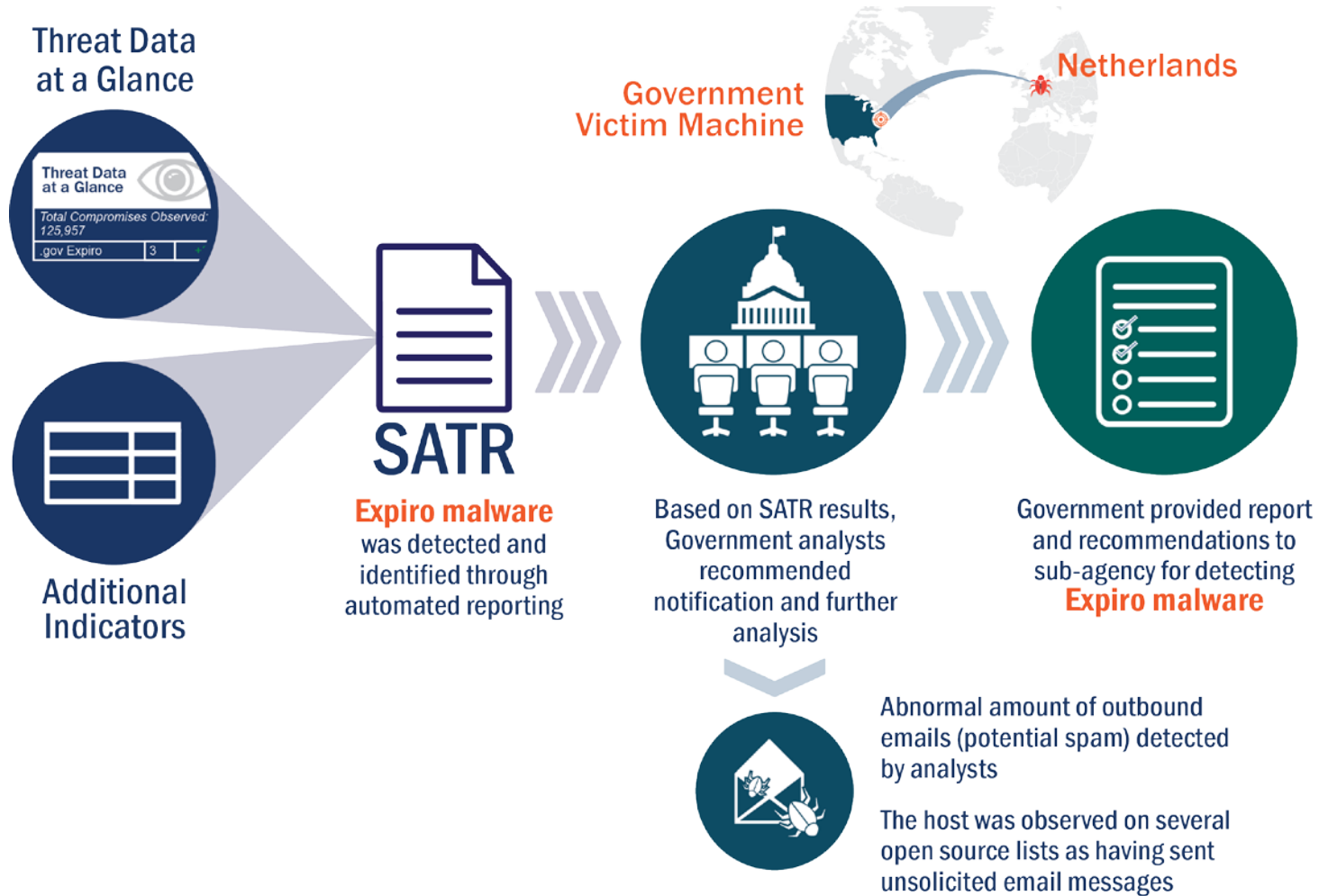
SATR analysis, alerted USG department a device was observed communicating with potential APT actors



Possible identification of botnet machines used for data exfiltration campaigns



Accomplishments of SATR



Accomplishments of SATR



This analysis resulted in a reduction of potentially unsolicited email traffic (spam)



This use case potentially increased government reputation as the machine was on two known blacklists



Standardized Reporting

**REVERSING
LABS**

SOURCEfire®

Akamai

IID

iSIGHTPARTNERSSM
Security beyond the edge™

TEAM CYMRU

LOOKINGGLASS
Transforming the Art of Threat Intelligence

shadowSERVER



**Homeland
Security**

National Cybersecurity and
Communications Integration Center

Reporting Aspects

SATR 01/05/16
Situational Awareness Threat Report
DAILY REPORT

National Cybersecurity and Communications Integration Center (NCCIC)

- 1 Top Cyber News
- 2 Threat Data at a Glance
- 3 Most Observed IP Indicators
- 4 Vulnerabilities and Snort Signatures
- 5 Active Malware C2
- 6 Federal Government
- 7 Critical Infrastructure

1 Top Cyber News

Android security update fixes 5 critical flaws, removes unneeded_permissions
January 05, 2016

Google has released the January security update for Android for its Nexus devices. The update fixes 12 issues, five of which are critical.

The most important hole that's been plugged is a remote code execution flaw in mediaplayer (CVE-2015-6535).

Tag: Vulnerability and Exploitation
Source: <http://www.reliasecurity.org/>

First known hacker caused power outage, causes troubling escalation
January 04, 2016

A new type of ransomware that still goes undetected by the great majority of AV solutions has been spotted and analyzed by @misploit's researchers.

Tag: Critical Infrastructure
Source: <http://www.reliasecurity.org/>

National Cybersecurity and Communications Integration Center (NCCIC)

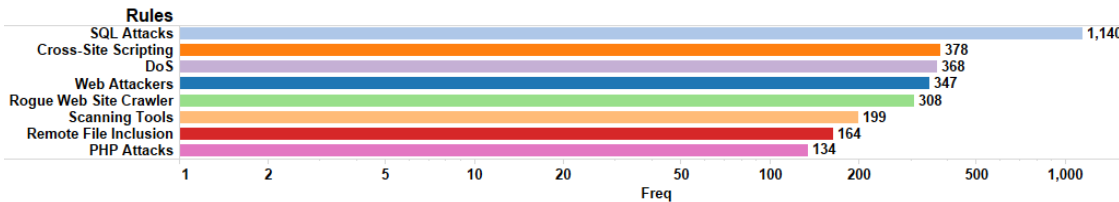
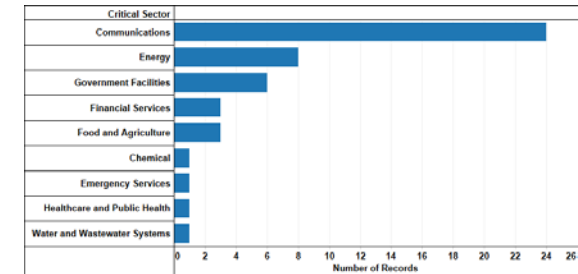
NetA Daily Report

01/02/16

PHASE 1
Title to be determined

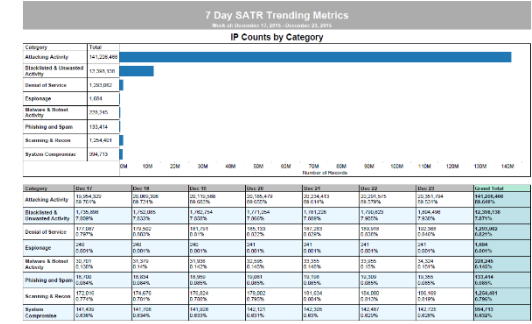
- 1 Top Cyber News
- 2 Threat Data at a Glance
- 3 Vulnerabilities and Snort Signatures

IP Address	Threat Type(s)	Tags	AS Number	Country Code	Company
XXX.XXX.199.216	System Compromise - Attacking Activity	[E.G OPTICROBOT] Conficker B	23969	TH	TOT-MET TOT Public Company Limited
XXX.XXX.129.125	Attacking Activity - System Compromise	Event not labeled by Looking Glass	22268	US	Comcast Cable Communications Holdings, Inc.
XXXXXXXX.46.241	Attacking Activity - System Compromise	Event not labeled by Looking Glass	7029	US	Windstream Communications Inc.
XXXXXXXX.56.109	Attacking Activity - System Compromise	Event not labeled by Looking Glass	7165	US	ViaSat Inc.
XXX.XXX.65.74	Attacking Activity - System Compromise	[E.G OPTICROBOT] Sany P2P	46662	US	Total Server Solutions L.L.C.
XXX.XXX.195.217	Attacking Activity - System Compromise	[E.G OPTICROBOT]APT APT1	8675	US	Microsoft Corporation
XXXXXXXX.4.129	Attacking Activity	Event not labeled by Looking Glass	6527	CA	Shaw Communications Inc.
XXX.XXX.294.342	Attacking Activity	Event not labeled by Looking Glass	6196	TR	KOCNET YODAFONE NET ELETRONIK MENKUL DEGERLER A.S.
XXX.XXX.7.4	Attacking Activity	Event not labeled by Looking Glass	17924	ID	TELKOMNET AS2-AR PT Telekomunikasi Indonesia
XXX.XXX.217.71	Attacking Activity	[E.G OPTICROBOT] Conficker B	45596	PK	PKTELECOM AS-PAK Pakistan Telecom Company Limited



Top Attributed Botnets Observed Targeting the Federal Government

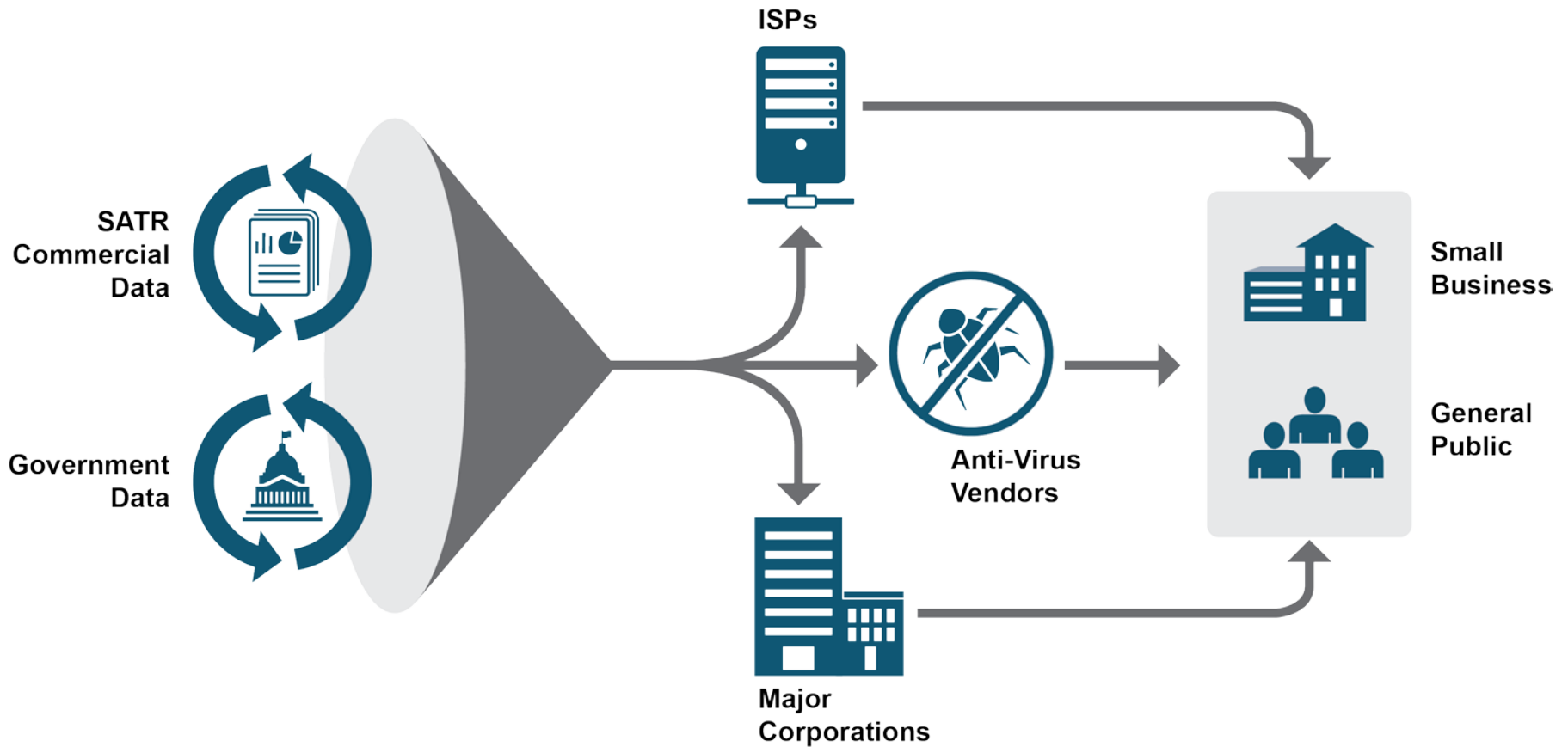
Botnet	Obs. IP	Delta
gameover-zeus-dga	12	-5 ↓
zeus	11	1 ↑
securityscorecard-nivdort	2	-1 ↓
zeus3np2p	1	-2 ↓
securityscorecard-bedep	1	0 —



Homeland Security

National Cybersecurity and Communications Integration Center

Conclusion



QUESTIONS?

