Homeland Security

Situational Awareness Threat Report (SATR)

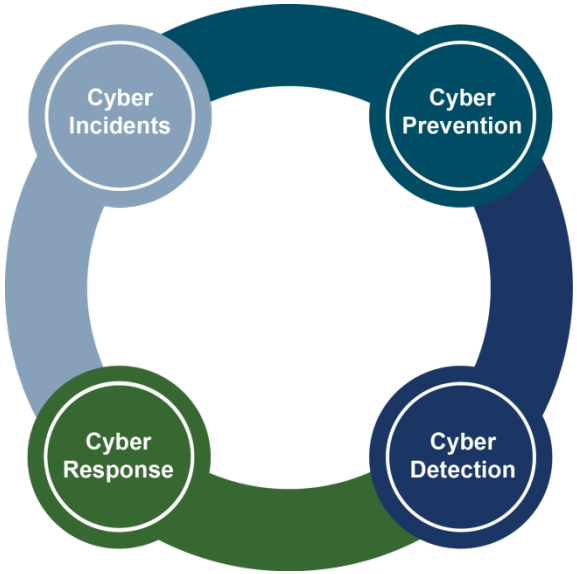
Presenters: Stacie Green & Casey Kahsen

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?

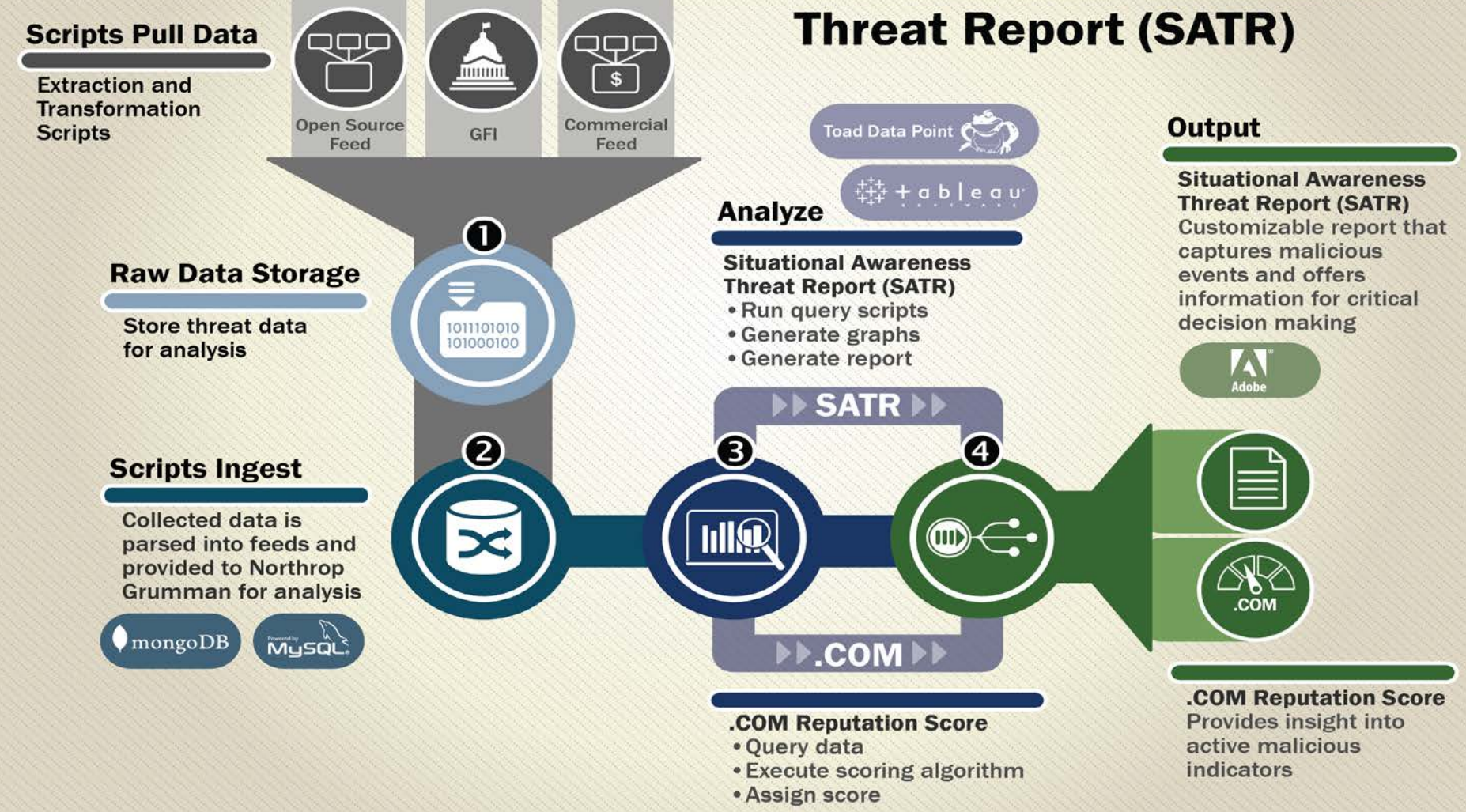
ISP validation and awareness
Signature development and deployment

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)



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

QUERIABLE 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

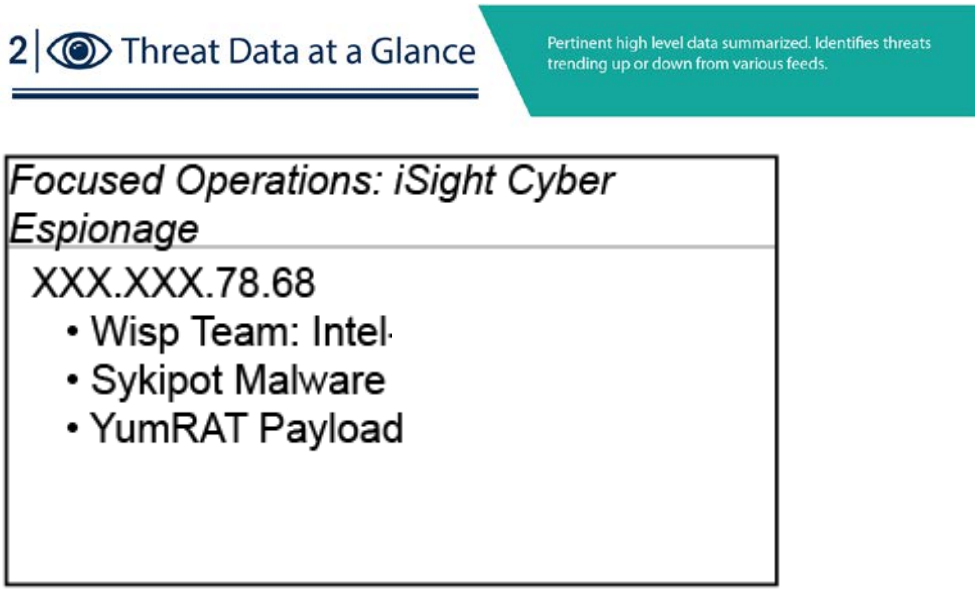
Reporting on Critical Infrastructure Sectors

Component: Threat Actors

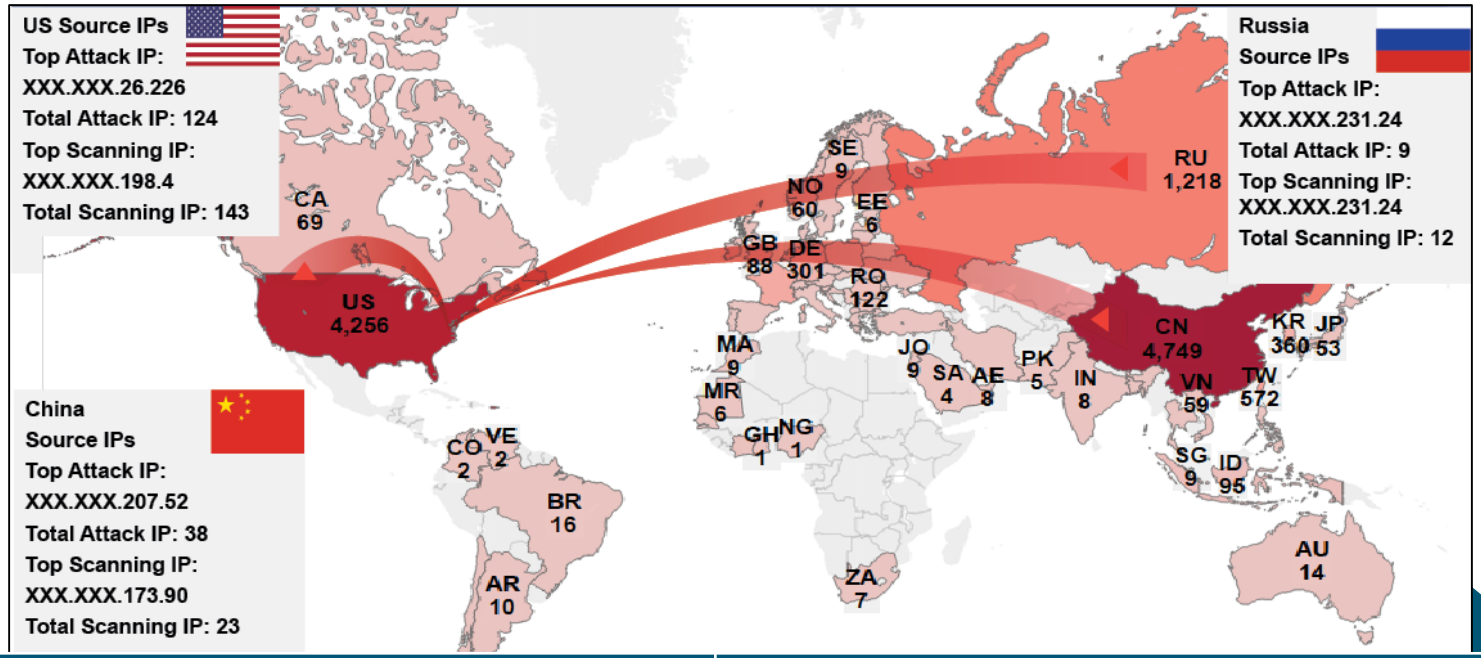
Reporting Example: Threat Actors

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



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

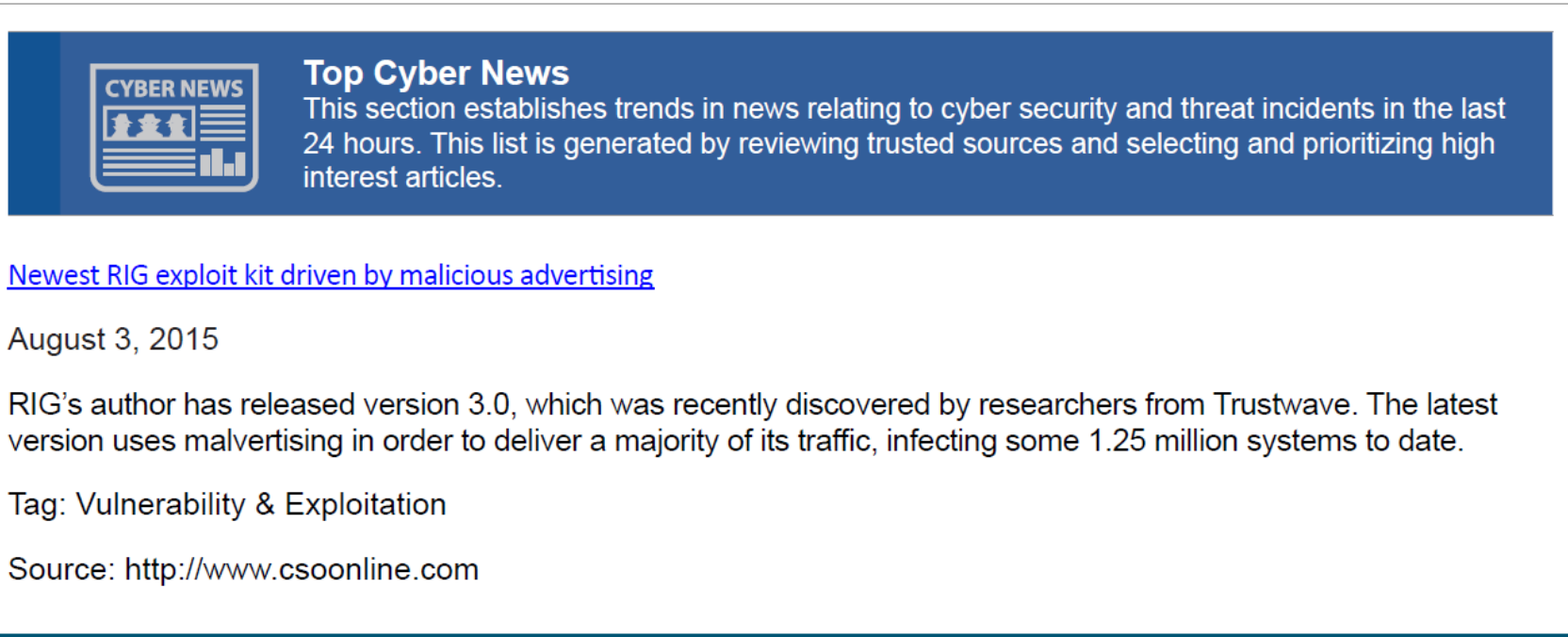
Vulnerability	CVSS Score	Snort Signature (Rule ID)	Vulnerability Type	Observed Increase
CVE-2015-5119	10.0		Denial of Service Execute Code Overflow Memory Corruption	+23 ▲

Image Depicts Report for 8/3/2015

Daily Report Monitors Exploit Usage

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

Component : Vulnerabilities



Reporting Example: Vulnerabilities

Report From Next Day

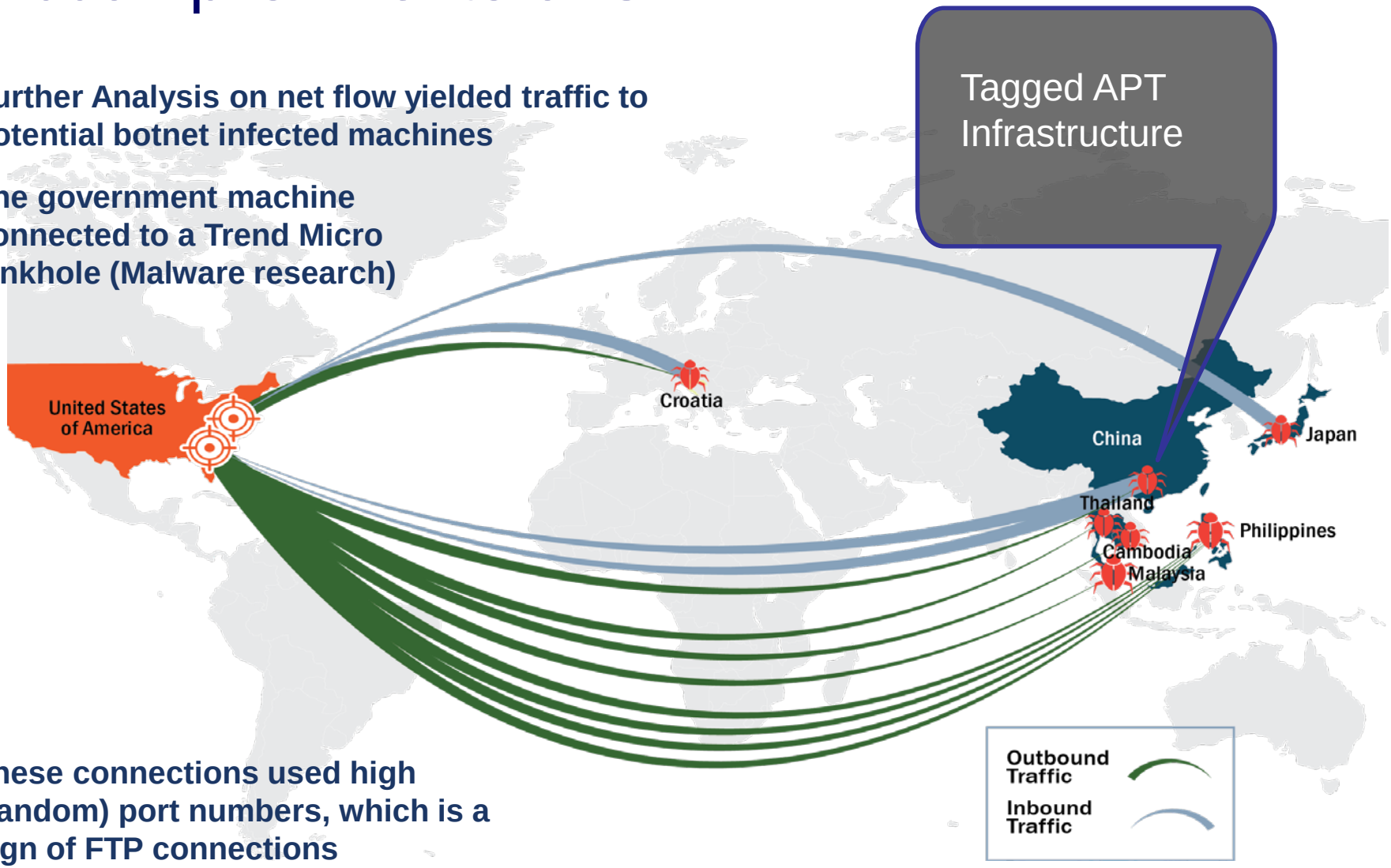
- Article describes RIG's use of CVE-2015-5119
- Reported previous day with an uptick of activity
- Example of threat forecasting

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

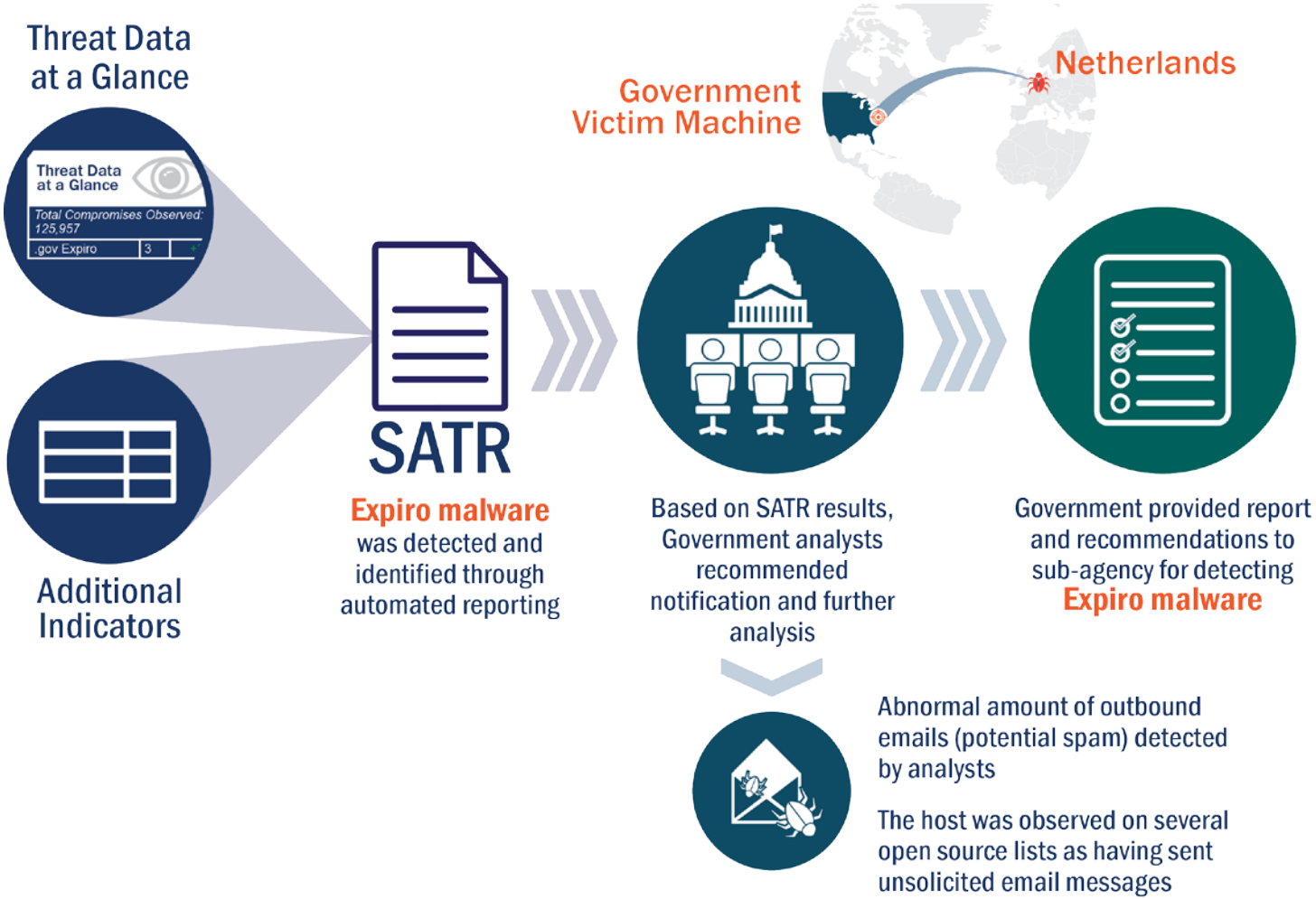
Operational Success Use Cases

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

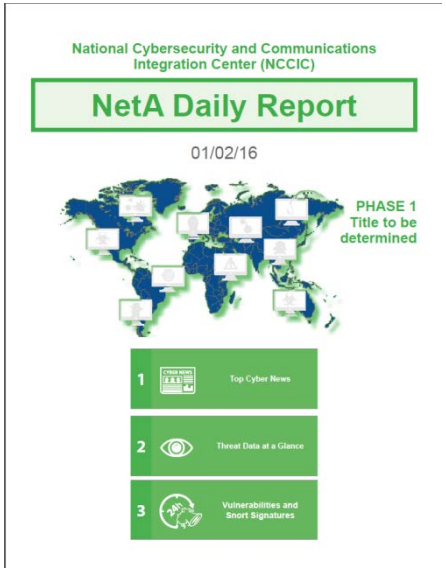
iSIGHTPARTNERS℠
Security beyond the edge℠

TEAM CYMRU

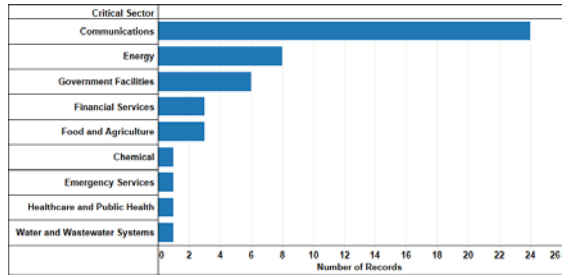
LOOKINGGLASS
Transforming the Art of Threat Intelligence

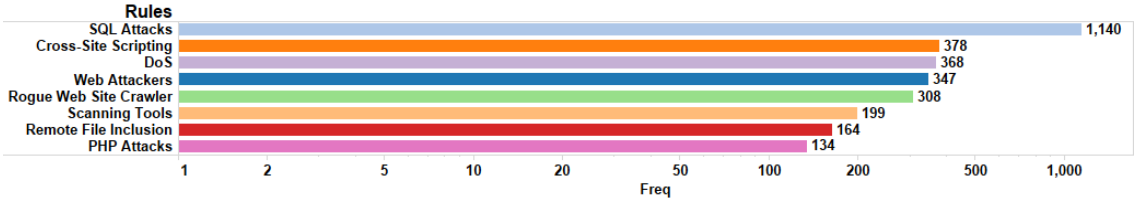
shadowserver

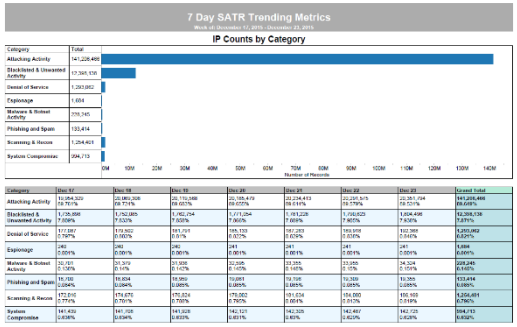
Reporting Aspects



IP Address	Threat Type(s)	Tags	AS Number	Country Code	Company
XXX.XXX.199.216	System Compromise ; Attacking Activity	[LG OPTICROBOT] Conficker B	23969	TH	TOT-NET TOT Public Company Limited
XXX.XXX.129.126	Attacking Activity ; System Compromise	Event not labeled by Looking Glass	22258	US	Comcast Cable Communications Holdings, Inc
XXX.XXX.46.241	Attacking Activity ; System Compromise	Event not labeled by Looking Glass	7029	US	Windstream Communications Inc
XXX.XXX.56.109	Attacking Activity ; System Compromise	Event not labeled by Looking Glass	7155	US	ViaSat Inc.
XXX.XXX.85.74	Attacking Activity ; System Compromise	[LG OPTICROBOT] Sality P2P	46652	US	Total Server Solutions L.L.C.
XXX.XXX.195.217	Attacking Activity ; System Compromise	[LG OPTICROBOT] APT APT1	8075	US	Microsoft Corporation
XXX.XXX.41.129	Attacking Activity	Event not labeled by Looking Glass	6327	CA	Shaw Communications Inc
XXX.XXX.204.242	Attacking Activity	Event not labeled by Looking Glass	8386	TR	KOCNET-VODAFONE NET ILETISIM HIZMETLERI A.S.
XXX.XXX.7.4	Attacking Activity	Event not labeled by Looking Glass	17974	ID	TELKOMNET-AS2-AP PT Telekomunikasi Indonesia
XXX.XXX.217.73	Attacking Activity	[LG OPTICROBOT] Conficker B	45595	PK	PKTELECOM-AS-PK Pakistan Telecom Company Limited



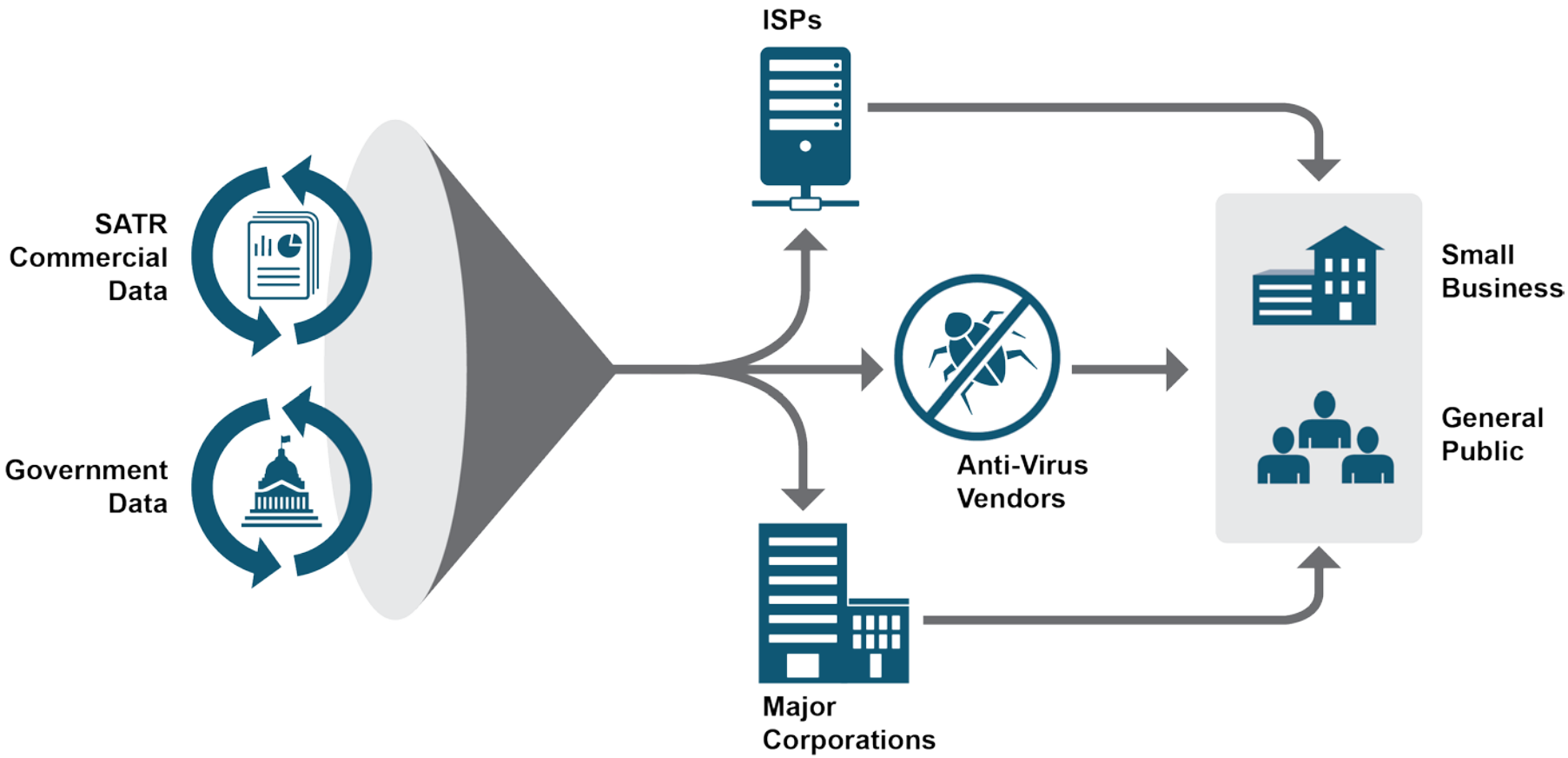




Top Attributed Botnets Observed Targeting the Federal Government

gameover-zeus-dga	12	-5 ↓
zeus	11	1 ↑
securityscorecard-nivdort	2	-1 ↓
zeus3np2p	1	-2 ↓
securityscorecard-bedep	1	0 —

Conclusion


ISPs
SATR
Commercial
Data
Government
Data
Anti-Virus
Vendors
Small
Business
General
Public
Major
Corporations

QUESTIONS?