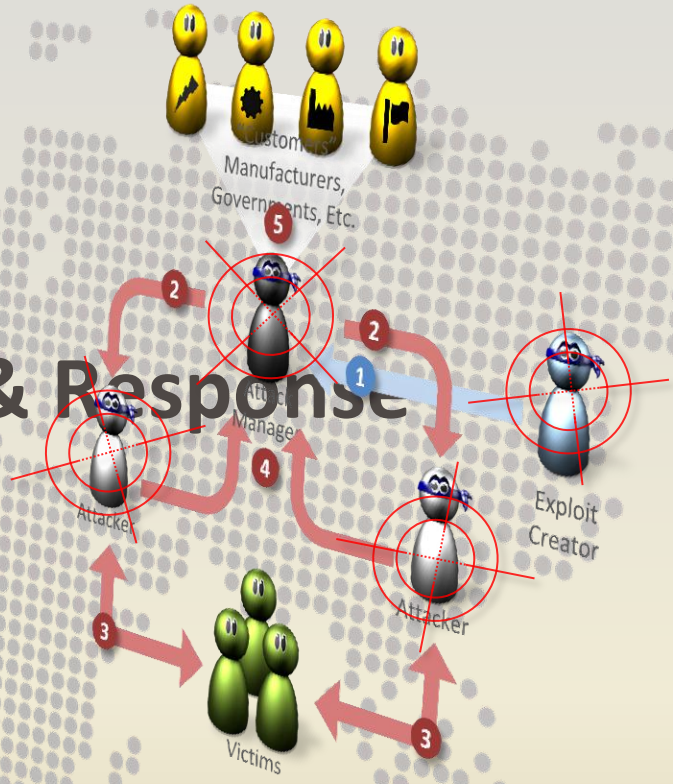
Security Threat Intelligence & Response



Deepak Maheshwari
Head – Government Affairs, India Region

Combo, Sri Lanka **March 26, 2015**

Symantec Security Response – Major Investigations

ESPIONAGE: TURLA (2014)

A campaign which has systematically targeted the governments and embassies of former Eastern Bloc countries

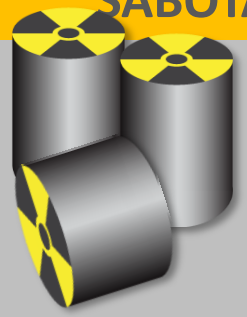
TARGETS	GOVERNMENT EMBASSIES
METHODS	SPEAR PHISHING, WATER HOLE

ESPIONAGE: REGIN (2014)

A complex and stealthy spying tool used for mass surveillance and intelligence gathering by nation states.

TARGETS	MASS SURVEILLENCE, COMMUNICATIONS
METHODS	SOCIAL ENGINEERING, WATER HOLE

SABOTAGE: STUXNET (2010)



The first computer software threat that was used as a cyber-weapon. Targeted nuclear facility in Iran. Used multiple zero-day exploits.

TARGETS	NUCLEAR FACILITY
METHODS	ZERO-DAY EXPLOITS, SUPPLY CHAIN

FINANCIAL FRAUD: PLOUTUS (2013)

Criminals compromising ATMs with customer Trojan and mobile phone. Can command ATM to issue cash using SMS

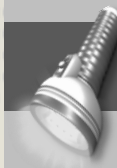
TARGETS	BANKS
METHODS	PHYSICAL ACCESS

Symantec Security Response – Leaders in Protection & Intelligence

GLOBAL REACH ROUND THE CLOCK

7 SITES, 24 x 7 x 365

WEB REQUESTS



13 BILLION DAILY

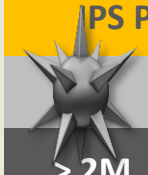
THREAT INTELLIGENCE

100s OF INVESTIGATIONS

MALWARE DETECTION

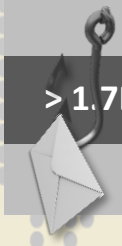
> 31M SIGNATURES

IPS PROTECTION



> 2M BLOCKED DAILY

EMAIL PROTECTION



> 1.7B BLOCKED DAILY

SOME OF LANDMARK INVESTIGATIONS

STUXNET	REGIN	DRAGONFLY	TURLA
HIDDEN LYNX	RAMNIT	NITRO	PLOUTUS ATM

SYMANTEC BIG DATA ANALYTICS PLATFORM

Programs downloaded/run

336 million/day - Windows, Android

Web sites visited

2 billion/day

Attacks seen

15 million/day

Machine activity

Static features

Behaviors

Symantec
Data Analytics Platform
(SDAP)

Predictive analytics
using machine learning

1 7 0 0 0 0 0 0 0
0 0 0 0 rows of data

300k rows added every second

- Malicious files
- Malicious web sites
- Malicious IP addresses
- Malicious e-mail sources
- C&C servers
- Attribution

Big Data: Symantec Data Analytics Platform

Customer Protection and Response

End-to-End Protection Content

- Anti-virus and IPS signatures
- Anti-spam and anti-phishing rules
- Blocking targeted attack emails
- URL blocking

Operations Assistance & Incident Response

- 24x7x365
- Emergency response
- Threat analysis
- Attack containment and remediation

Threat Intelligence and Response

Attacks on Energy Sector

Financial Trojans

Strategic Research

- Top attack campaigns
- Trends
- Industry sectors

HiddenLynx

ZeroAccess

Bespoke Research

- Research conducted for customers
- Law enforcement investigations

Bitcoins

Threat Intelligence Collection

Data Sources

- Product telemetry
- Honeypots
- Email
- Malware analysis
- OSINT & private sources

Processing Systems

- RATS
- Pokemon
- MTAN
- Symdroid

Threat Intelligence Analysis

WHO?

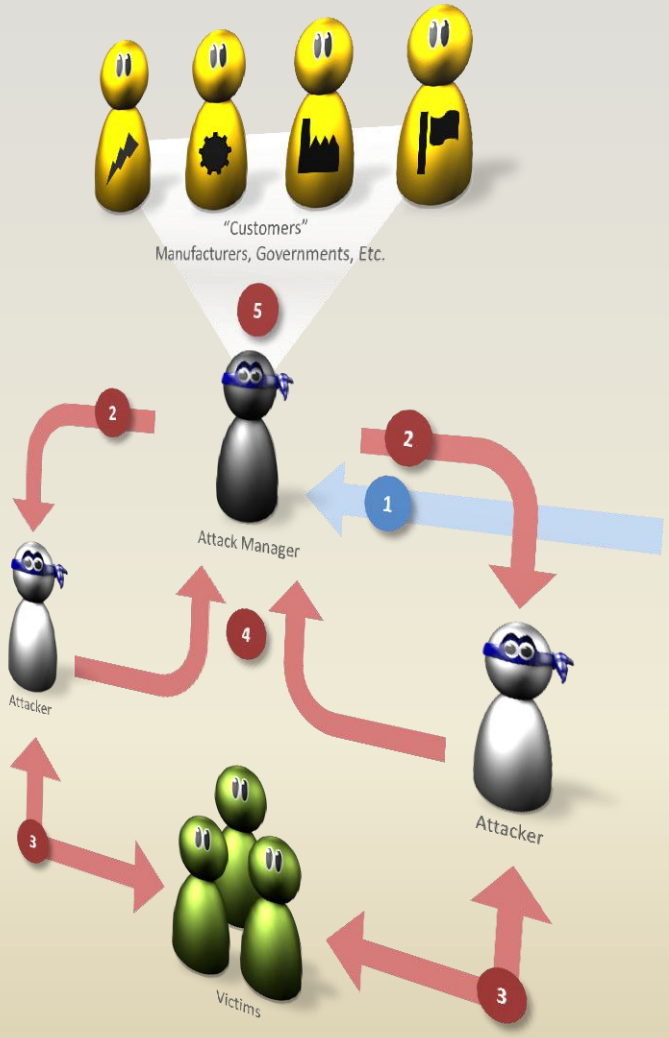
- Identify attackers

WHY?

- Identify motives

WHEN?

- Correlate attacks and campaigns



How does *Insight* Reputation Help?

Insight knows…

…about virtually every software file, good or bad, on the planet.

We use this intelligence to…

…block new and unknown attacks automatically.

…drive investigations into new targeted attacks…

Intelligence Sharing

Customers

- Custom reports
- Intelligence briefings

General Public

- Blogs & videos
- Whitepapers
- Social media
- Media engagements

Internal Customers

- Briefings and newsletters

Global Security Intelligence

- Symantec's **Global Intelligence Network (GIN)** has global visibility into the threat landscape including big data from:
  - More than 41.5 million attack sensors in 157 countries
  - Extensive anti-fraud community of enterprises, security vendors and end users
  - More than 8 billion emails per month from 5 million decoy accounts
  - Over 13 billion web requests a day
- **Breadth and depth of data.** The GIN offers visibility into empirical, real-world customer data from enterprises and consumers, Symantec .cloud meta-data, forums, vendors, honeypots and other third-party data combined with the largest collection of end-point sensors in the industry. We monitor, analyze and process more than 10 trillion security events per year worldwide using data analytics to find common threads. This helps design new ways of detection and prevention.
- **Anticipate.** The best way to protect from threats is to understand what and who is likely to attack, and also to learn what newly identified vulnerabilities may be exploited to attack your network.
- **Shift from reactive security.** Adding visibility into the global threat landscape enables a more proactive posture.

More Information

Blog
http://www.symantec.com/connect/symantec-blogs/sr

Twitter
http://twitter.com/threatintel

Whitepapers
http://www.symantec.com/security_response/whitepapers.jsp

Thanks!