RSA CONFERENCE CHINA 2011
NOVEMBER 2-3 | CHINA WORLD HOTEL | BEIJING

Intelligence Based Cyber Defense

Speaker：Richard Zhao

PhD, CISSP

Chief Strategy Officer, NSFOCUS, ichard.zhao@nsfocus.com

Board Director, Cloud Security Alliance Greater China Coordination Body

Agenda

I. DDoS and APT Incidents

II. Security Intelligence System

III. Next Generation Security

IV. Intelligence Based Cyber Defense

OPERATION MALAYSIA

Malaysia Official Government Website [link] – [Down]

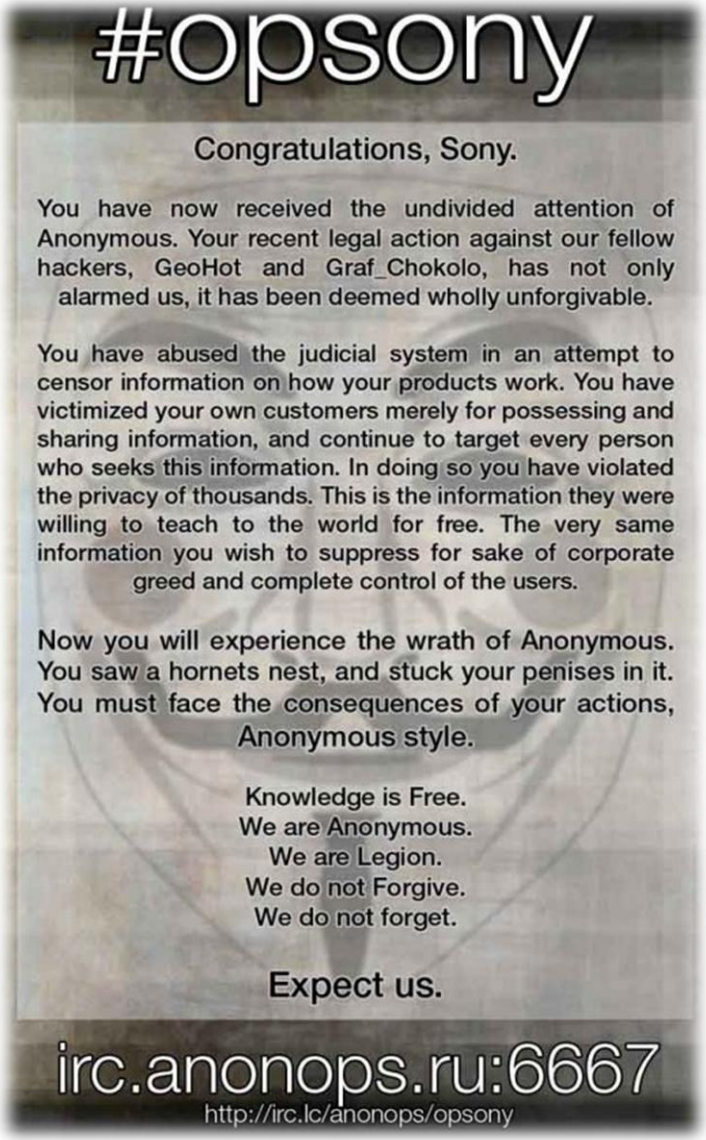
- SabahTourism.com [link] [Hacked][Leaked]
- CIDB [link] [Hacked] [Up]
- Land Public Transport Commision [link] [Suspected]
- Malaysian Meteorological Service [link] [Down]
- ASEANconnect [link] [Suspected]
- Hollywood-Artist.info [link] [Suspected]
- Ministry of Education [link] [Down]

– Suruhanjaya Pilihanraya Malaysia [link] [Down]

- Bomba [link][Down]
- TMNet [link] [Down]
- Perbendaharaan Malaysia [link] [Down]
- Kementerian Kerja Raya Malaysia [link] [Down]
- Parlimen Malaysia [link] [Down]
- JobsMalaysia [link] [Down]
- Kementerian Penerangan, Komunikasi dan Kebudayaan [link] [Down]

DDoS Attacks Strands Traditional Firewall/IPS

Cyber Attacks to Sony PlayStation Network



Cyber Attacks to Sony PlayStation Network -2

[user12] if sony is watching this channel they should know that running an older version of apache on a redhat server with known vulnerabilities is not wise, especially when that server freely reports its version and its the auth server

[user2] its not old version, they just didnt update the banner

[user12] I consider apache 2.2.15 old

[user2] which server

[user12] it also has known vulnerabilities

[user12] auth.np.ac.playstation.net

[user2] ya the displayed version u see via banner is not the real version

[user12] unless they updated it in the last couple weeks

[user12] I doubt that since its not trivial to change that

[user12] its a bit more invasive than just setting it to Prod like they do on their other servers

[user11] you know, watching this conversation makes me think about whether it was a good idea after all to buy a couple of games from psn using a visa card

[user2] its just backported security patches

[user11] i did remove all my info after downloading the games though

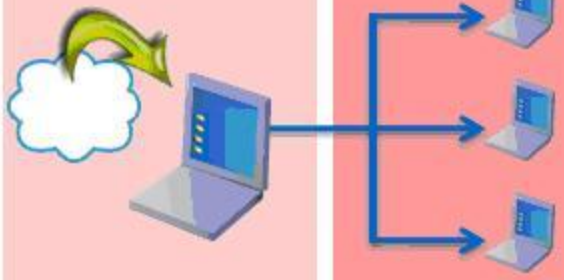
[user12] that is just psn not the store

[user12] they are running linux 2.6.9-2.6.24 on that box too

[user12] that too is old

APT Attack to RSA SecurID

1	2	3	4	5
Phishing and Zero day attack	Back door	Lateral movement	Data gathering	Exfiltrate
A handful of users are targeted by two phishing attacks; one user opens Zero day payload (CVE-02011-0609)	*The user machine is accessed remotely by Poison Ivy tool*	*Attacker elevates access to important user, service and admin accounts, and specific systems*	*Data is acquired from target servers and staged for exfiltration*	*Data is exfiltrated via encrypted files over ftp to external, compromised machine at a hosting provider*



APT Attacks Worldwide

General commercial security devices can't help on those APT and other sort of advanced targeted attacks!

Data Source: Revealed - Operation Shady RAT, By Dmitri Alperovitch, McAfee

Picture of Security Today

- Clear perimeter between security zone and insecurity zone (and DMZ)
- Security policy mostly based on IP addresses, ports, etc.

- Silos of various security devices
- Mission impossible for signatures update to catch up with zero-day threats
- Infidelity of communications from users to vendors
- …

Please refer to :
http://www.nsfocus.com/images/6_about/journal/6_10_014_j.pdf

Security Intelligence System

General Logs
DNS Query | Login/Auth | Firewall /Router/Switch | Web proxy

Security Alerts
IDS/IPS | Firewall | AntiVirus | UTM | …

HoneyNet

Web Resources
Vulnerability and Patches | Attacks | Tools | …

Security Intelligence

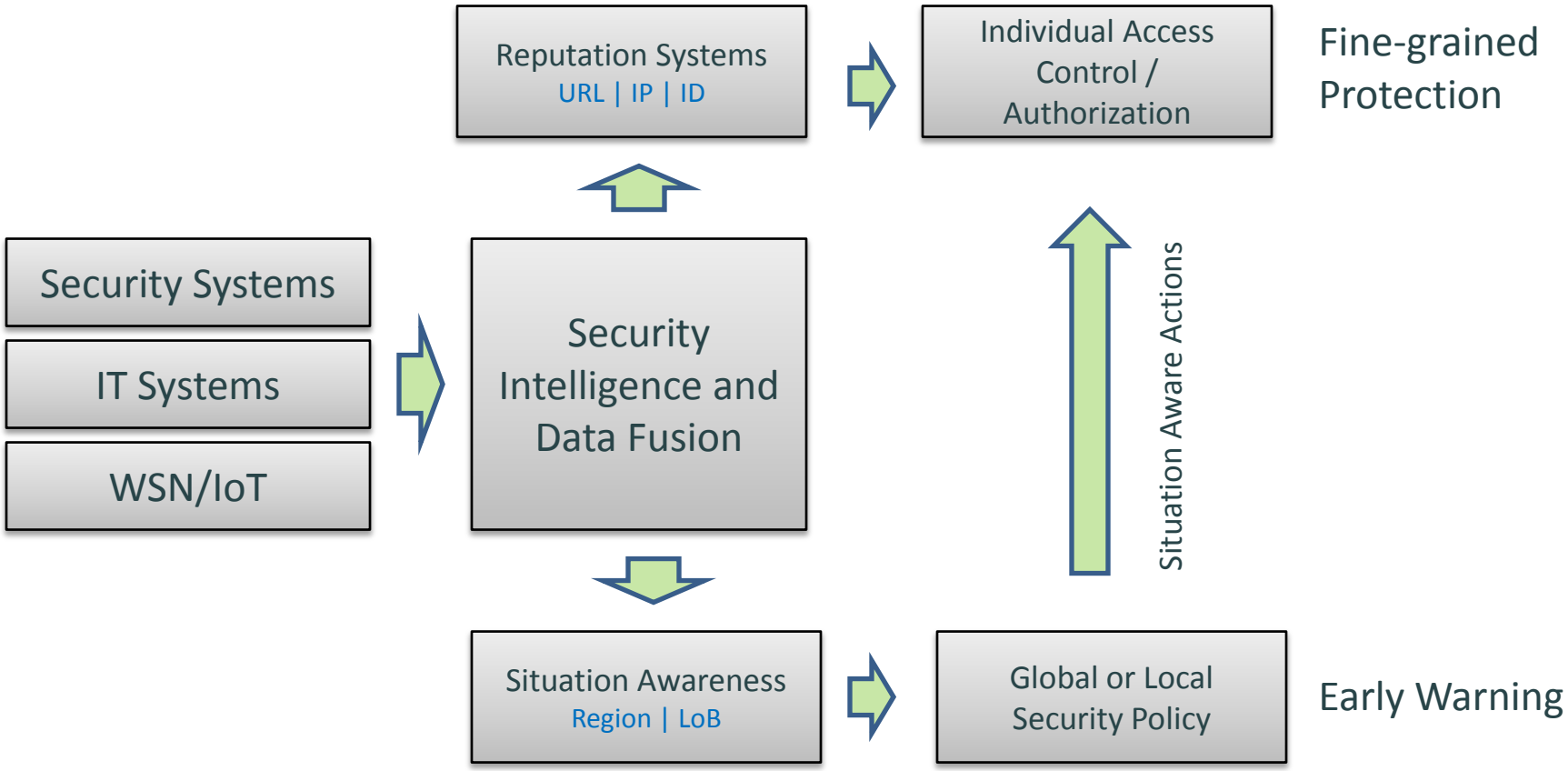
Log Correlation | Malware Analysis | Forensics Reporting | Data Mining Reputation | Situational Awareness | …

Security Policy Update

Ruleset /Knowledgebase /Configuration Update

Communications and Training

Security Intelligence Enables Advanced Features



Talking About Next Generation Security

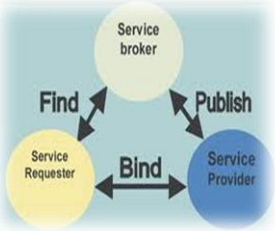
Business

- Intimate Partnership between customer and providers

Knowledge

- Cloud Intelligence

Architecture



- Service Oriented
- Open Plugin-enabled

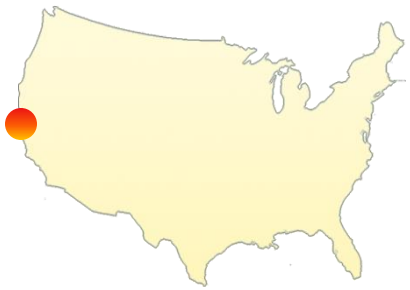
Team

- Real Time Response
- Global Operated

Intelligence Based Cyber Defense

	Technology	Policy
Government	• Develop nation-level security intelligence system, including monitoring, collecting, analyzing, sharing, distributing, covering vulnerability, reputation, honeynet and malware, etc. • Early warning & emergency response system	• Laws/Regulations • Public/private sector collaboration, identifying a few trustworthy providers and develop deep collaborations • Awareness education • International collaboration and agreements
Enterprise	• Choose security devices with adequate dynamic update capability • Enable logging and build correlation/data mining capability or purchase MSS. • Be open to share security data with authority and MSSP	• Regular self check on compliance • Awareness education

谢谢 Thank You 謝謝 Vielen Dank Gracias Merci Beaucoup
ありがと 감사합니다 Obrigado ขอบคุณ Terima kasih



NSFOCUS