

Cyber Security:

Threats and Countermeasures

Kah-Kin Ho

Head of Cyber Security Business Development

Global Government Solutions Group

9th Oct 2012

Agenda

- Threat Landscape – Technical, Social, Political
- Lead Methodology
- Cisco Security Intelligence Operations
- Concluding Remarks

Recent Trends

- Security conscious users are targeted.
- Bad guys getting better in evading detection.
- Legitimate sites used by bad guys for profit making activities.
- Overwhelming AV companies.
- Social networks targeting.

Legitimate alert

From: ITS Helpdesk
Sent: Tuesday, March 22, 2011 2:48 PM
To: Howe, Joe
Subject: ACTION REQUIRED: VPN Client Update

This message is to alert you that ITS has posted a new Cisco Systems VPN Client on BevoWare for all operating systems. The certificate for the current VPN client from BevoWare will soon expire and prevent users from logging on. Users of the Cisco AnyConnect VPN Client are not affected.

If you fall into one of the following categories, you must update your client:

- You use the desktop client from BevoWare and you downloaded it prior to March 21, 2011
- You set up an iPhone VPN profile using the iPhone configuration page

Please do one of the following as soon as possible:

- Switch to the Web-based client available at <https://vpn.utexas.edu>. It works for Windows, Mac, and Linux. It provides longer connection times, fewer dropped sessions, and automatic client updates.
- Download and install the updated Cisco Systems VPN Client from BevoWare (<http://www.utexas.edu/its/bevoware/download>) .
- iPhone users should go to the iPhone configuration page and select the Create a UT VPN Profile option to update their configuration <http://webdb.its.utexas.edu/iphone/index.cfm>.

You must have administrative privileges on your computer to install any VPN client. Please contact your desktop support staff if you need assistance.

Effective April 25th, 2011, the vulnerable VPN client will no longer be able to connect to the VPN service.

Please contact your desktop support staff or the ITS Help Desk at 512-475-9400 if you have any questions about this message.

Copied Alert

今日，小弟一開電郵，就收到懷疑中共玩嘢嘅木馬電郵，內容話係VPN Client Update，

「Dear,

If you already have VPN installed on your computer, you'll be asked to download and install update the next time you start VPN. Once the new update is installed, VPN should function normally.

Download and install the updated:<http://www.cisco.com/vpn/upgrade.exe>

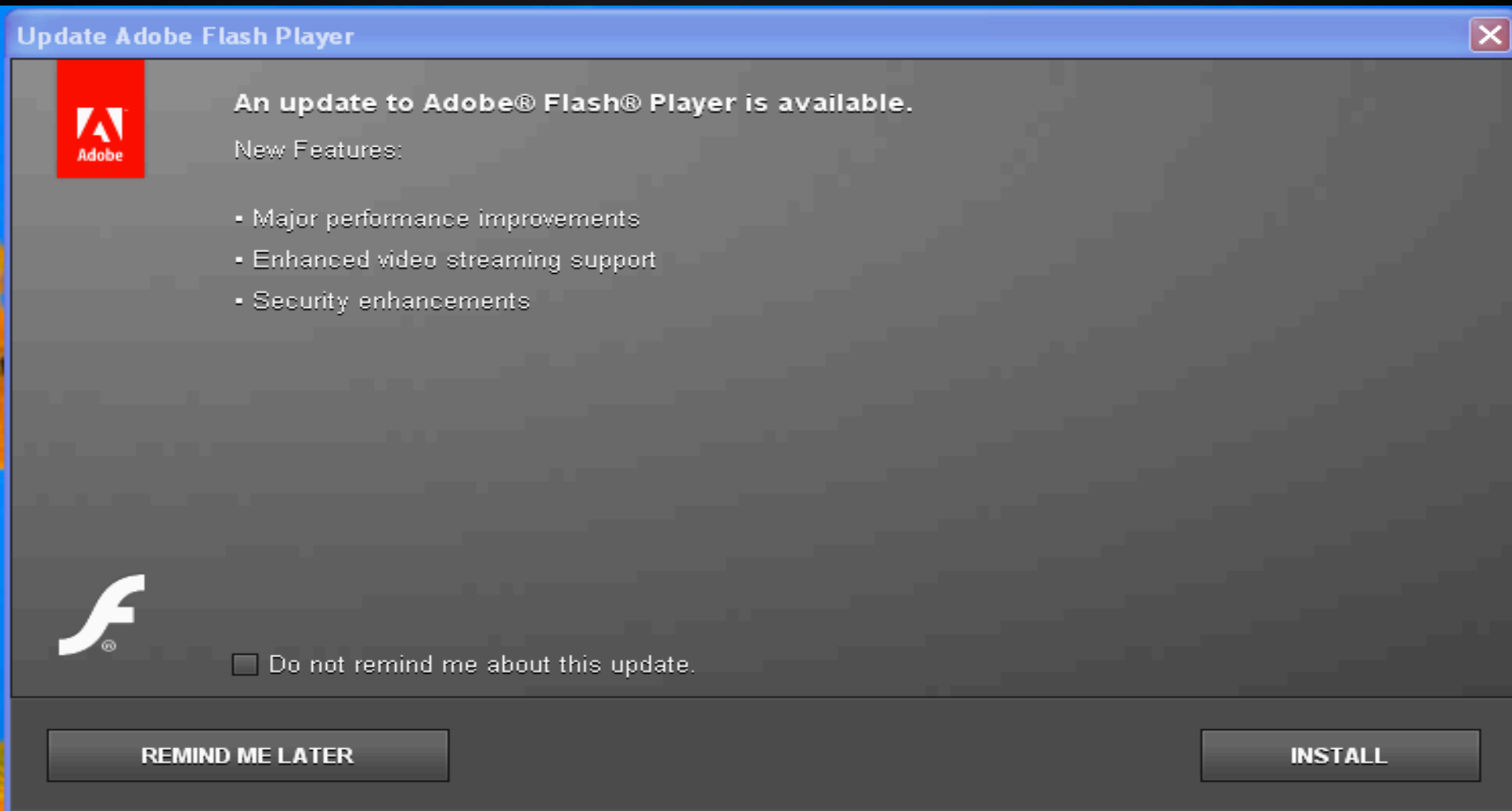
*You must have administrative privileges on your computer to install any VPN client.
Please contact your desktop support staff if you need assistance.*

Morris Kristi

Kristi.Morris@cisco.com」

當然，我唔係CISCO嘅客，第一時間睇email header，因為一定中共玩嘢，個header係咁。

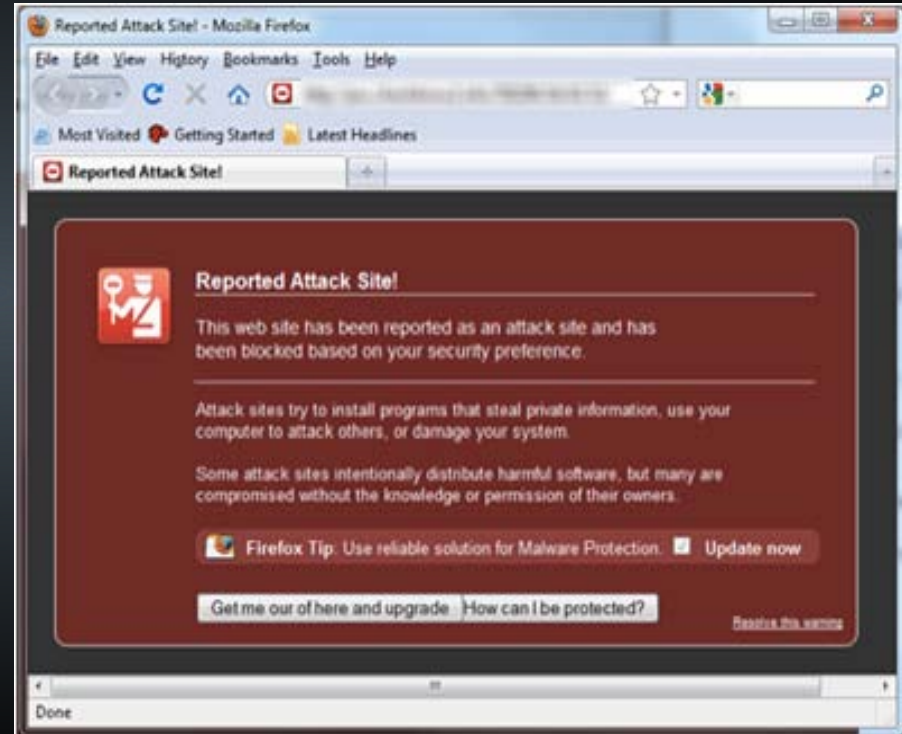
Which one is real?



Or this ?



They are all Fake.





















Intelligence Evasion

Mozilla Firefox

File Edit View History Bookmarks Tools Help

      http://www.zinsecurity.com/

 Most Visited  Getting Started  Latest Headlines  blackrep  milw0rm.com  MalwareDomainList up...  MalwareURL.com - Lat...  Proxywiki New Proxy  Ur I.T. Mate Group hp...

 FoxLingo  Webpage  Text  Services  GrammarCheck  AutoTrans  Search  

 http://www.zinsecurity.com/ 

Intelligence Evasion

SoftVeteran - Online Protection - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.zinsecurity.com/online/994c846805b1b4860d9457c90df47ef6/0478c52e6db101effdb21d3ee40ff7fc/3656b9eddb95cfb9d7f013ed46b015a2

Most Visited Getting Started Latest Headlines blackrep milw0rm.com MalwareDomainList up... MalwareURL.com - Lat... Proxywiky New Proxy Ur I.T. Mate Gro

FoxLingo Webpage Text Services GrammarCheck AutoTrans Search

SoftVeteran - Online Protection

System Tasks

- View system information
- Add or remove programs
- Change a settings

Other Places

- My Network Places
- My Documents
- Shared Documents
- Control Panel

Details

My Computer
System Folder

System folders



Shared Documents



My Documents

5 Viruses found

Hard drive



Hard drive (C:)

Security



Windows Security

Security is affected by virus

Checking: c:\..\Default User\Application Data\ALCW2



Your Computer is infected

Windows Security Alert



To help protect your computer, Windows Web Security have detected Trojans and ready to remove them.

Detected spyware and adware on your computer:	Filename:
Trojan-PSW.Win32.LdPinch.abm	ieframe.dll
W32.Benjamin.Worm	x2.64.exe
Backdoor.Win32.Haxdoor.gu	ds32gt.dll
W32.Nimda.J@mm	kbdhe220.dll
AdvWare.Hotbar	HideWin.exe

**upd4t3**

Follow

aHR0cDovL2JpdC5seS8xN2EzdFMg

about 2 hours ago from web

aHR0cDovL2JpdC5seS9MT2ZSTyBodHRwOi8vYml0Lmx5L0ltZ2

about 2 hours ago from web

aHR0cDovL2JpdC5seS8xN2w0RmEgaHR0cDovL2JpdC5seS8xN

about 4 hours ago from web

aHR0cDovL2JpdC5seS9wbVN1YyBodHRwOi8vYml0Lmx5LzE3b

about 4 hours ago from web

aHR0cDovL2JpdC5seS9HaHVvdSBodHRwOi8vYml0Lmx5L1FqC

about 5 hours ago from web

aHR0cDovL2JpdC5seS9RakFaWQ==

about 5 hours ago from web

aHR0cDovL2JpdC5seS83UGFEOQ==

about 5 hours ago from web

aHR0cDovL2JpdC5seS8zUndBTiBodHRwOi8vYml0Lmx5LzJwU0

about 12 hours ago from web

Name upd4t3

20

following

7

followers

Tweets


25

Favorites

Actions

block upd4t3

Following

 RSS feed of upd4t3's tweets

```
$ echo "aHR0cDovL2JpdC5seS9SNINUViAgaHR0cDovL2JpdC5seS8yS29lbw==" | openssl base64 -d  
hxxp://bit.ly/R6STV hxxp://bit.ly/2KoH
```

CNBC FIRST IN BUSINESS WORLDWIDE

RT REAL-TIME QUOTES Symbol / Company Go Symbol Lookup

SEARCH

HOME **NEWS** MARKETS EARNINGS INVESTING VIDEO CNBC TV CNBC 360 CNBC PRO

U.S. ASIA-PACIFIC EUROPE ECONOMY ENERGY GREEN TECHNOLOGY BLOGS WIRES SLIDESHOWS SPECIAL REPORTS CORRECTIONS

Mom Earns \$7,219/Month Part-Time

Published: | 10:47 A.M. EST

Text Size

By: Colleen Kane, Writer

Jamie Wallace of , never thought she would have a job working at home until one day she filled out a simple form online. Before she knew it, she discovered her secret to beating the recession, and being able to provide for her family by working from home.



I read Jamie's blog last month and decided to feature her story in our Career News segment. In our phone interview she told me her amazing story. "Since getting my **Home Revenue System** I actually make about \$6,000-\$8,700 a month using the internet. It is enough to comfortably

replace my old job's income. And the best thing is that I only work about 10-12 hours a week from home so I now have a lot more time for my family."

Working online has been a financial windfall for Jamie, who struggled for months to find a job in a struggling economy through many online job

ADVERTISEMENT

SECTORS

- More



Tesco Growth to Outpace Rivals
A survey says sales growth at Britain's Tesco will outpace its major international rivals including Wal-Mart in coming years.

- Fed may reconsider plan to limit debit card fees
- CNBC Tech Check Blog
- Behind The Wheel with Phil LeBeau
- Consumer Nation Blog

MORE US COMPANIES NEWS

- More

- Video Game Sales Get off to Slow Start in 2012
- J&J Recalled Products Back on Shelves This Year: CEO
- Starbucks CEO Addresses Single-Serve Strategy
- CEOs See Economic Conditions Improving: Survey
- Credibility Shaken, Hedge Funds Are Punished by Investors

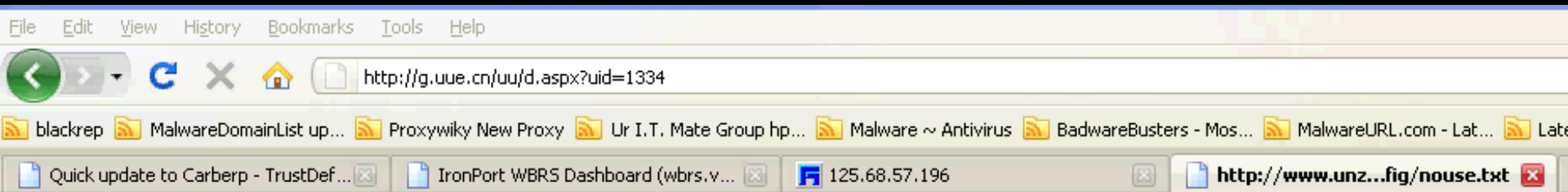
COMPANIES SLIDESHOWS

- More



Victoria's Secret 2012 Fashion Show
Each year, Victoria's Secret kicks off its holiday-selling season with a runway event to build excitement about its products.

Unique Malware Content



PASS<http://www.unzjs.com/software/ausys.exe>
<http://g.uue.cn/uu/d.aspx?uid=1334>
PASS<http://www.unzjs.com/software/QQ.exe>

The Facebook Vector

Advertise on Facebook

1. Design Your Ad

Destination: External URL

URL: canadaneews.3322.org

Title: Canada job cuts

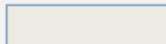
10 characters left

Body: Canadian government to shed 33% of workers



93 characters left

Image:



Browse...

[?]

[Remove uploaded image.](#)

Preview:

Canada job cuts



Canadian government to shed 33% of workers

Estimated Reach

18,540 people

- who live in **Canada**
- age **18** and older
- who work at **Canadian Forces** or **Government of Canada**

Hackerville: The Romanian cybercriminal hotspot Râmnicu Vâlcea



Tallinn Estonia 2007





Russia – Georgia War 2008



China's Emergence



Motivation: Status and Ego



深切哀悼汶川大地震遇难同胞!

19日-21日 全国哀悼日



» 您尚未 登录 注册 | 搜索 | 勋章中心 | 黑盟问答 | 帮助

» 中国黑客联盟 » 总站论坛 » 勋章中心

勋章介绍 | 获得勋章名单 | 勋章颁发情况

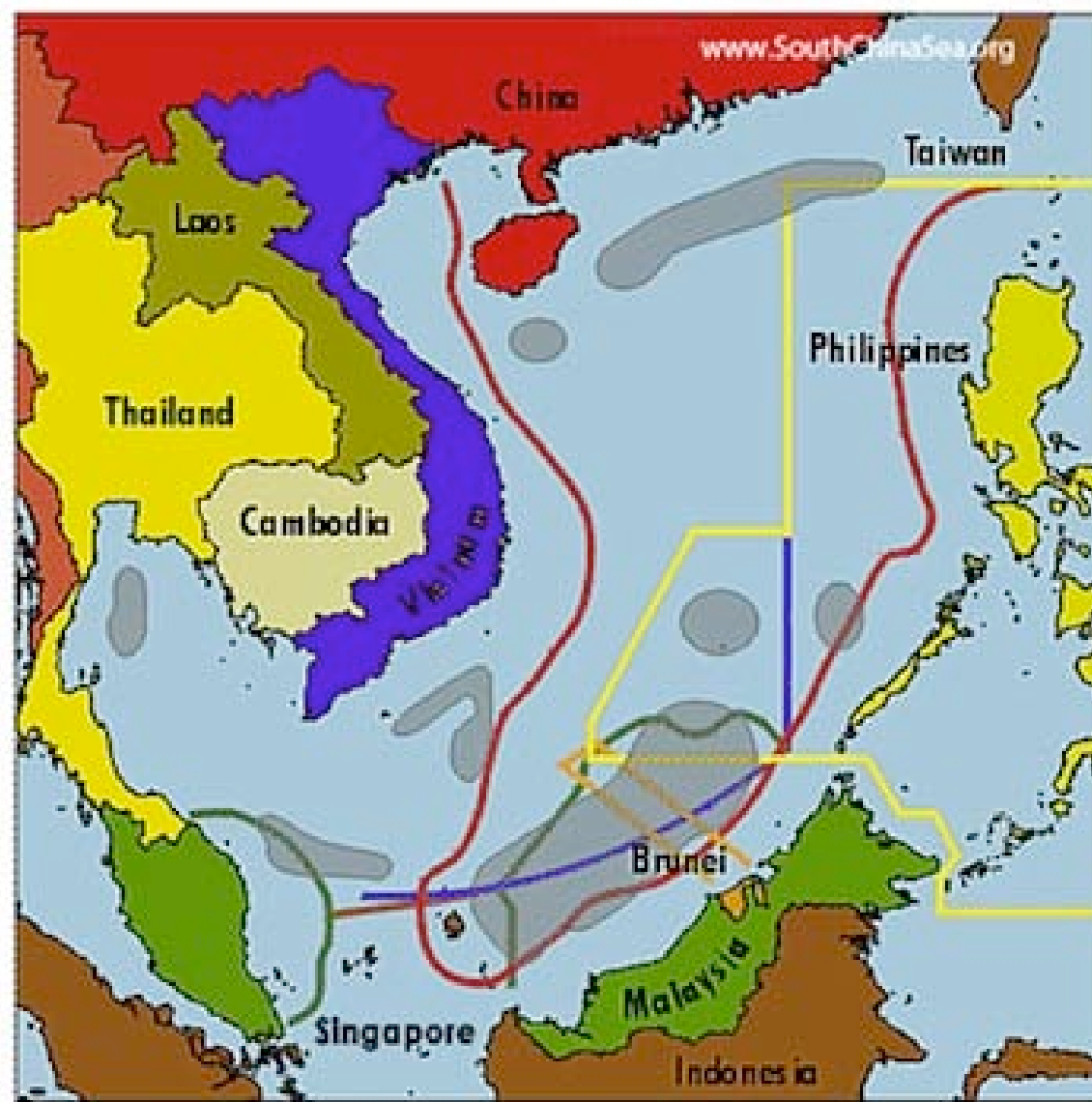
您还没有勋章

勋章介绍

ID	勋章名称	勋章说明	勋章图片
1	终身成就奖	感谢您为论坛发展做出的不可磨灭的贡献!	
2	优秀斑猪奖	辛劳地为论坛付出劳动,收获快乐,感谢您!	
3	宣传大使奖	感谢您为论坛积极宣传,特颁发此奖!	
4	特殊贡献奖	您为论坛做出了特殊贡献,谢谢您!	
5	金点子奖	为论坛提出建设性的建议被采纳,特颁发此奖!	
6	原创先锋奖	感谢您积极发表原创作品,特颁发此奖!	
7	贴图大师奖	贴图高手,堪称大师!	
8	灌水天才奖	能够长期提供优质的论坛水资源者,可得这个奖章!	
9	新人进步奖	新人有很大的进步可以得到这个奖章!	
10	幽默大师奖	您总是能给别人带来欢乐,谢谢您!	







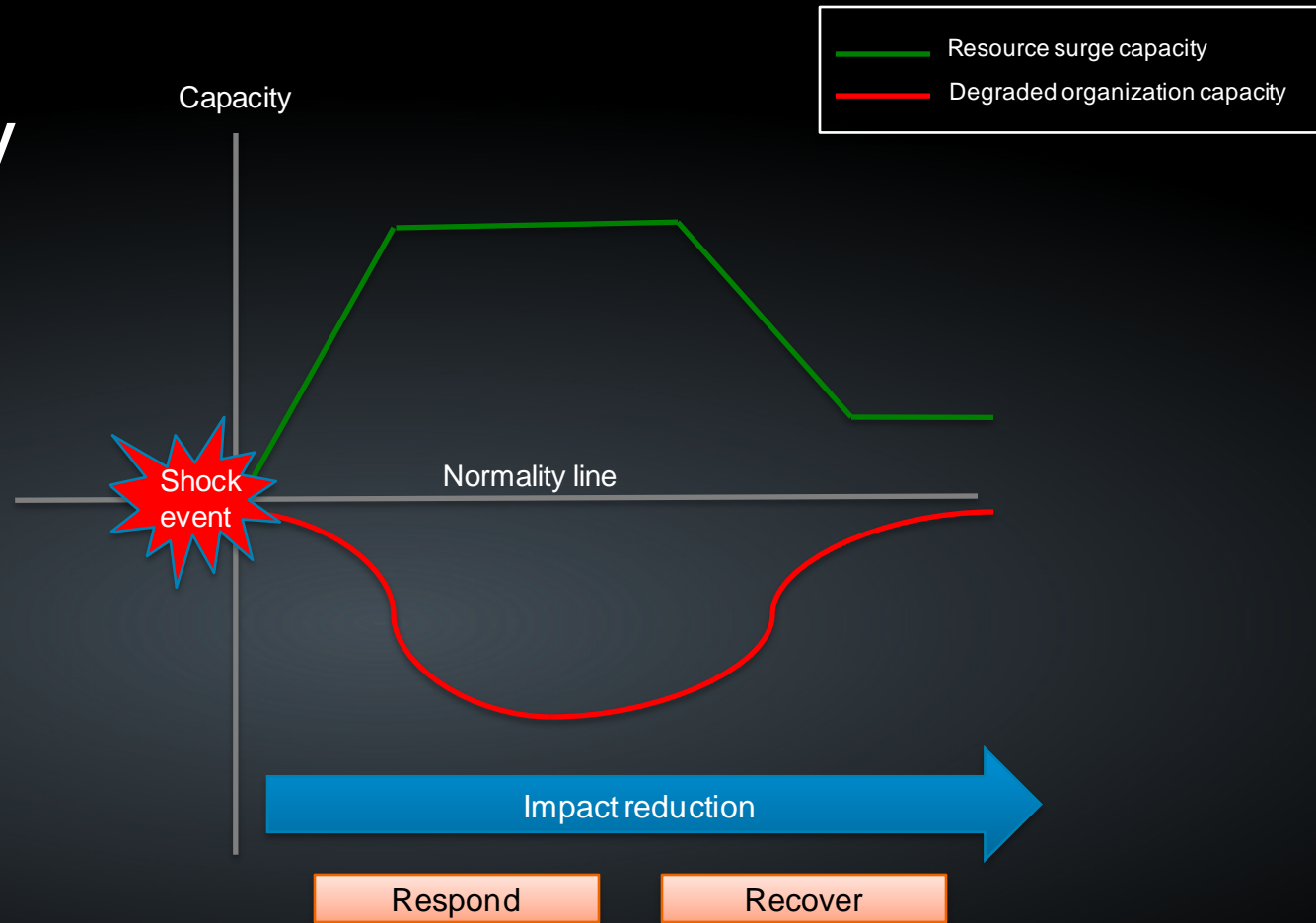
Countries Claiming Ownership

- China
- Vietnam
- Malaysia
- Brunei
- Philippines

Gas/ Oil fields

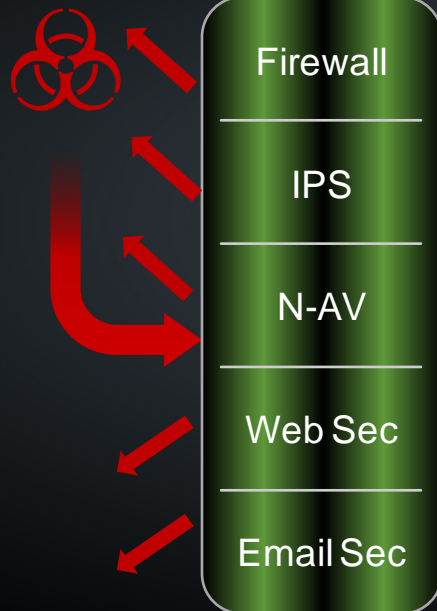
0 500 1000 km

Lead Methodology

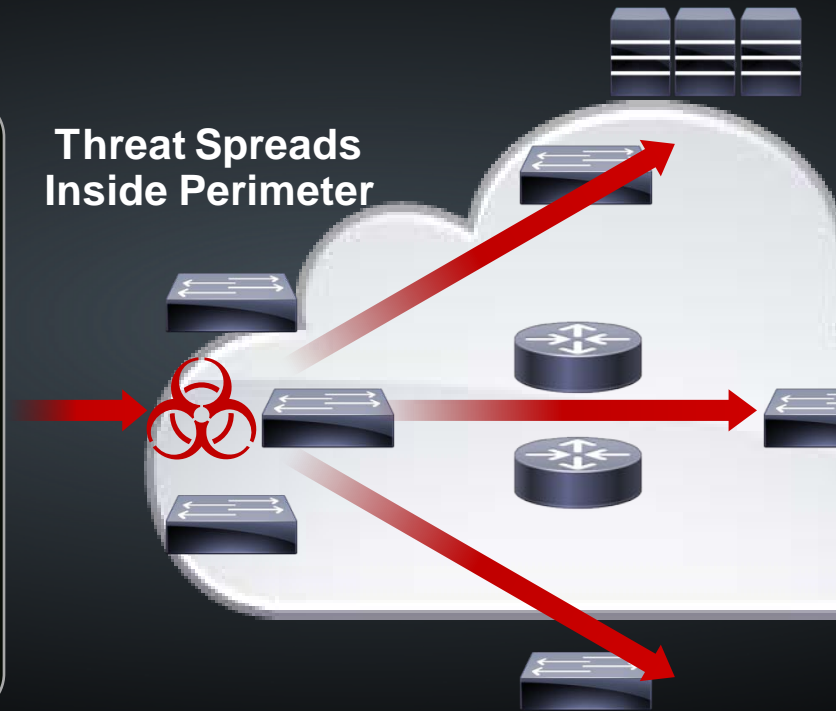


Picking a Needle out of a Haystack

**Customized Threat
Bypasses Security
Gateways**



**Threat Spreads
Inside Perimeter**



**Customized Threat
Enters from Inside**



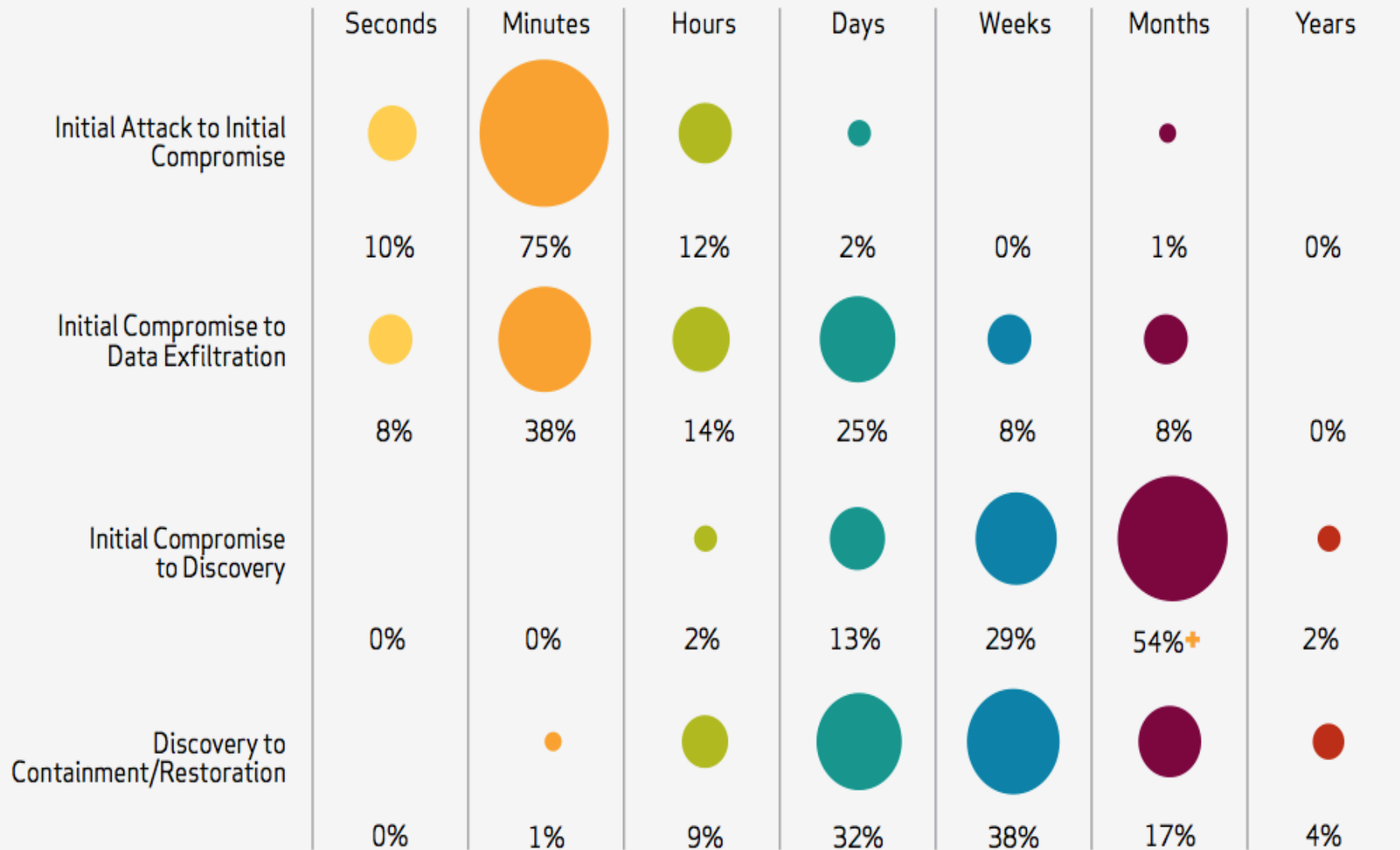
**Threat Spreads
to Devices**



Perimeter security stops many threats but
Sophisticated Cyber Threats Evade Existing Security Constructs

Fingerprints of Threat are Found Only in Network Fabric

Detection is key to Respond and Recover



Cisco Cyber Threat Defense



Visibility

Cisco Cyber Threat Defense



Traffic: P2P
Destination: badsite.com
Reputation: -6
Malware: Zeus
User: Jane Smith
Access Group: Guest
Device: Laptop
Location: Campus HQ
Access Method: Wireless

Threat

Context



User: John Doe
Access Group: Finance
Device: Android Phone
Location: Remote
Access Method: VPN

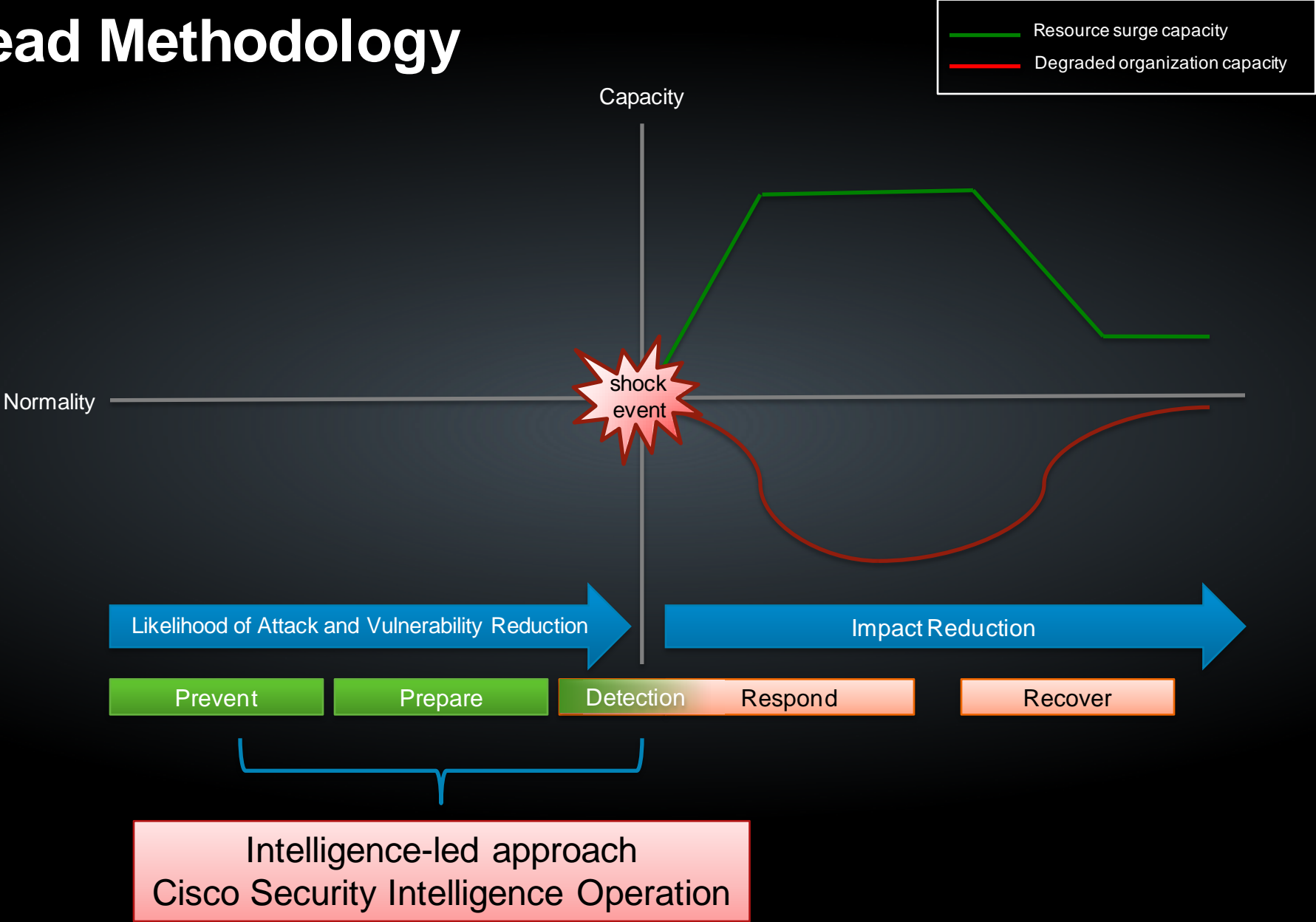
Context



Threat
Profile

Visibility

Lead Methodology





slo

$$X_{i+1}^{(t)} \quad m+n = \sum \quad f_i = \sum_{i=0}^{(N-1)} F(x_{i+1} x_i) \quad \frac{X_i^{(t+1)} + 2X_i^{(t)} + X_{i+1}^{(t)}}{4}$$



SensorBase



Threat Operations Center



Dynamic Updates



SIO

100 TB

DATA RECEIVED PER DAY

2 Mil+

GLOBALLY DEPLOYED DEVICES

30B

WEB REQUESTS

HTTP://

1B

MAIL BOXES



35%

WORLDWIDE TRAFFIC



SensorBase

Threat Operations Center

Dynamic Updates



SIO



\$200M

**SPENT IN DYNAMIC RESEARCH
AND DEVELOPMENT**

24x7x365

OPERATIONS

500

**ENGINEERS, TECHNICIANS
AND RESEARCHERS**

40+

LANGUAGES

80+

Ph.D.s, CCIE, CISSPs, MSCEs

SensorBase

Threat Operations Center

Dynamic Updates

Security Support Operations

Current SSO Presence in the Following Regions:

- California
- Texas
- Ohio
- Idaho
- China
- Ukraine
- UK
- Canada
- India
- Australia



Languages: Arabic, Farsi/Persian, Hebrew, Syriac, Urdu, Bengali, Gujarati, Gurmukhi, Hindi, Marathi, Sinhala, Tamil, Thai, Chinese, Japanese, Korean, Belarusian, Bulgarian, Kazakh, Macedonian, Russian, Ukrainian, Greek, Armenian, Georgian, Basque, Catalan, Croatian, Czech, Danish, Dutch, English, Estonian, Filipino, Finnish, French, German, Hungarian, Icelandic, Indonesian, Italian, Malay, Norwegian, Polish, Portuguese, Romanian, Slovak, Slovene, Spanish, Swedish, Turkish, Vietnamese



SIO

3 to 5

MINUTE UPDATES

6,500+

IPS SIGNATURES PRODUCED

20+

PUBLICATIONS PRODUCED

200+

PARAMETERS TRACKED

8M+

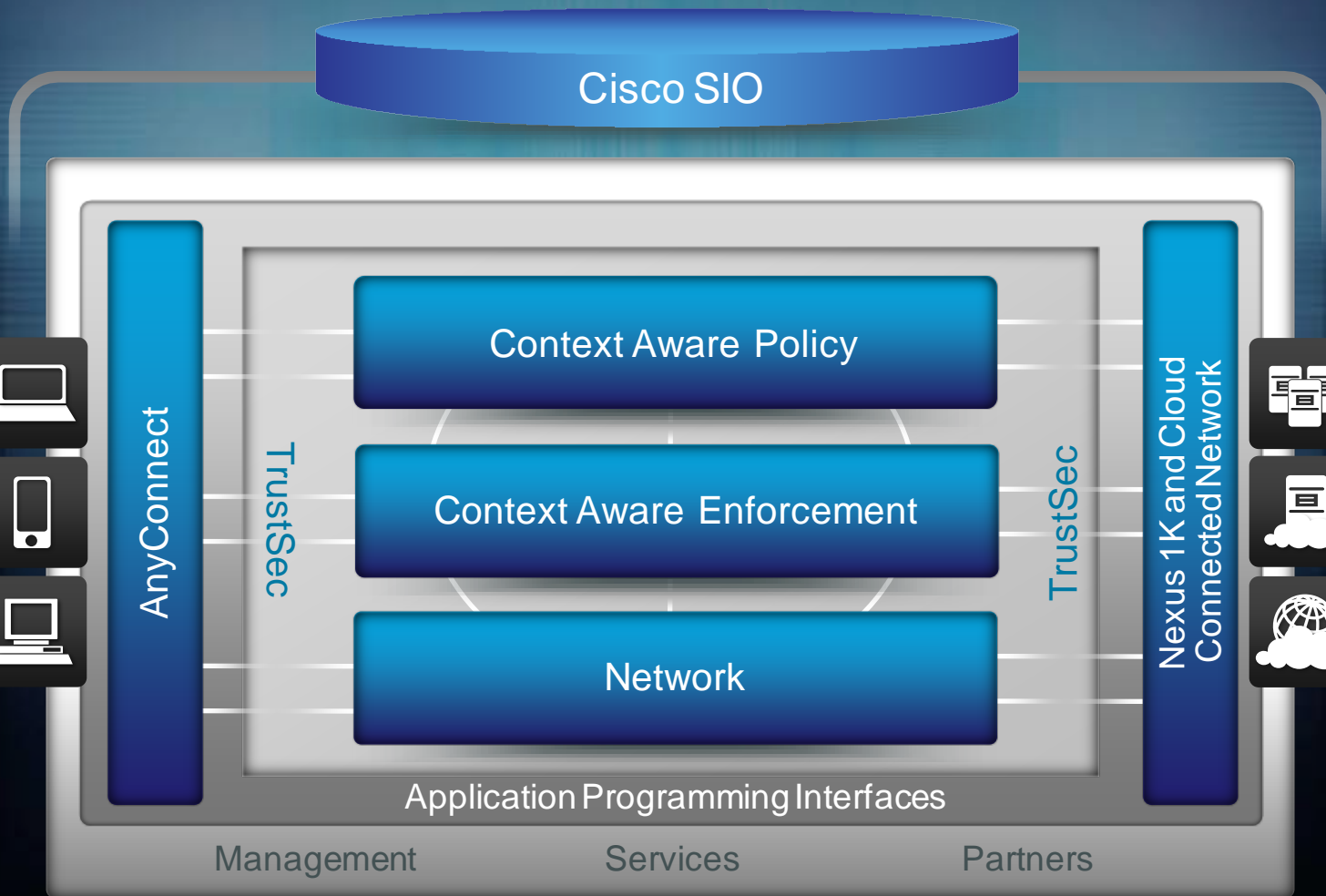
RULES per DAY

SensorBase

Threat Operations Center

Dynamic Updates

Global Context: Data Makes a Difference





US HYBRID SMISHING SLAMMER
MATION ACTIVE CONTENT DANGERO
STER VIRUS EMBEDDED URLS VIS
WELCHIA WORM PHISHING CONER
SOBIG DISRUPTIVE TROJAN EX
MYTOB MALICIOUS PROPAGATION INF
PLICATING CODE RED EXPLOIT BUGE

US HYBRID SMISHING SLAMMER
MATION ACTIVE CONTENT DANGEROUS
STER VIRUS EMBEDDED URLS VIS
WELCHIA WORM PHISHING CONER
SOBIG DISRUPTIVE TROJAN EX
MYTOB MALICIOUS PROPAGATION INF
PLICATING CODE RED EXPLOIT BUGE



AGATION NIMDA FILE EXPLOIT II

BRID MALWARE CODE RED GONER

PHISHING ATTACK VISHING BUGBEAR

FILE SELF REPLICATING CLAMMER

EXPLOIT SPREADING RAPIDLY I MY

INFECTIOUS BLASTER DENIAL OF SER

PHISHING ACTIVE CONTENT GONER

BLENDDED



CONTEXT

Context Inspection

- Where's it coming from?
- How many others have seen it?
- How new is it?
- Who owns the package?
- What else have they sent us?
- Is the sender even a real person?

From

Aunt Jenny
234 Any St.
Anytown, CA



From:

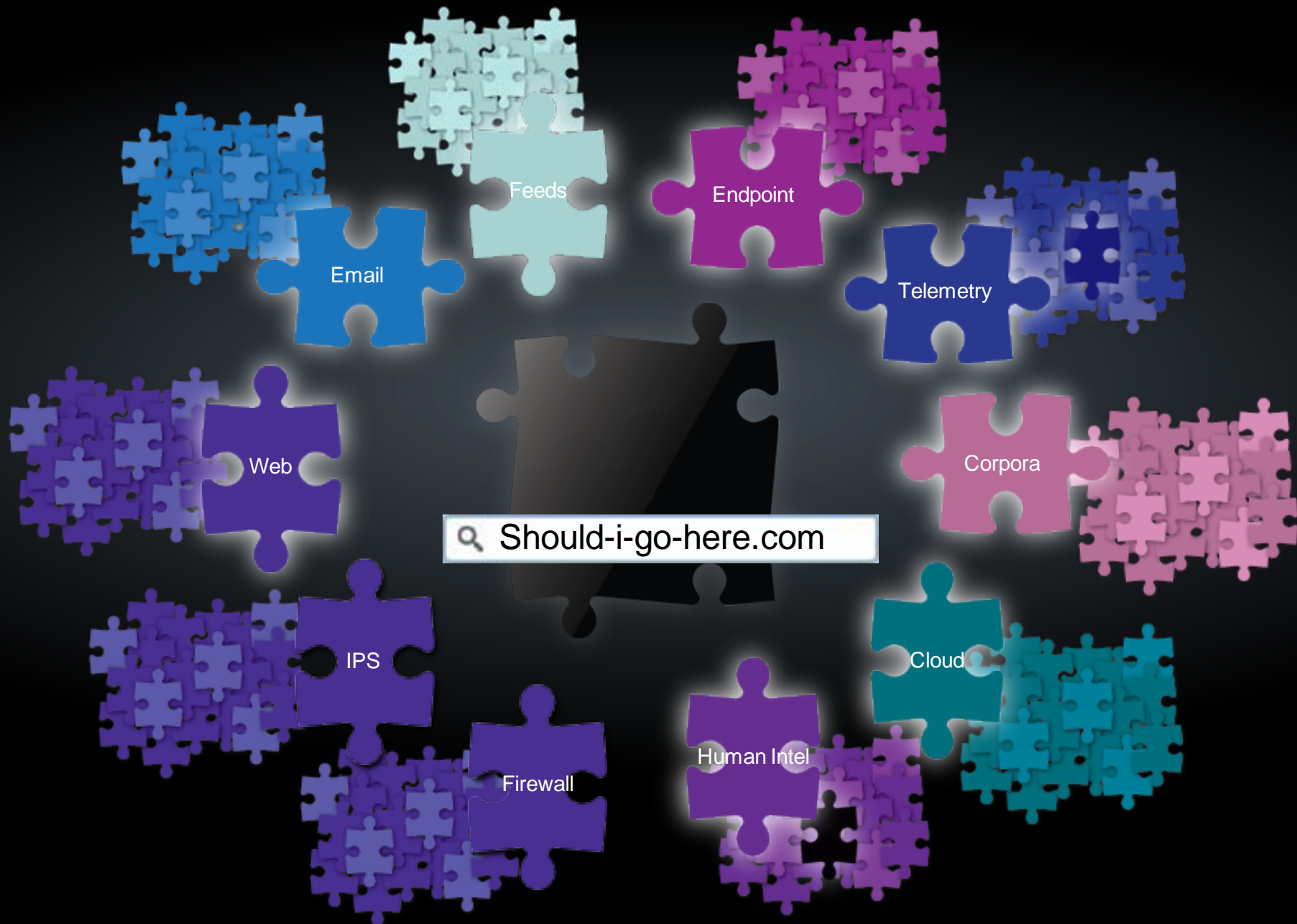
Aunt Jenny
234 Any St.
Anytown, CA

HANDLE WITH CARE



Deny 13. Allow Everything Else.

1A 13 1C



Targeted attacks

Cisco Security Intelligence Operations has detected significant activity related to spam e-mail messages that claim to contain a file sharing tool download link for the recipient. The text in the e-mail message may attempt to convince the recipient to open the link and view the details. However, the link references a malicious .exe file that, when executed, attempts to infect the system with malicious code. E-mail messages that are related to this threat (RuleID4414) may contain the following file:

Flashfxp.exe

The *Flashfxp.exe* file has a file size of 53,248 bytes. The MD5 checksum, which is a unique identifier of this executable file, is the following string: 0x01EC264B82D938B5D7FDD6A51D73DECD

The following text is an example of the e-mail messages that are associated with this threat outbreak:

Subject Line: **Important File**

Message Body:

Dear,

I want to sent you some files, but they are too large to send as email attachments, so I create an ftp server. I will give you an ftp client software and you can download these files through it.

The FTP tools Download in: <ftp://59.120.154.62/documents/Flashfxp.exe>

username:alcoouser

password:alcoap@ssw0rd

These files are confidential and please keep them secret, including the username and the password.

Cisco Security Intelligence Operations analysts examine real-world e-mail traffic data that is collected from over 100,000 contributing organizations worldwide. This data helps provide a range of information about and analysis of global e-mail security threats and trends. Cisco will continue to monitor this threat and automatically adapt IronPort systems to protect customers. This report will be updated if there are significant changes or if the risk to end users increases.

Virus Name	Cisco	Sophos	McAfee	Trend Micro	Symantec
Troj/Bredo-LX	<div><div>FIRST</div><div>11/17/2011 12:03</div></div>	<div><div></div><div>+0d 4h 52m</div></div>	<div><div></div><div>Not Published</div></div>	<div><div></div><div>Not Published</div></div>	<div><div></div><div>+0d 12h 12m</div></div>
W32/Gamarue-F	<div><div>FIRST</div><div>11/17/2011 09:01</div></div>	<div><div></div><div>+0d 4h 4m</div></div>	<div><div></div><div>Not Published</div></div>	<div><div></div><div>+0d 18h 9m</div></div>	<div><div></div><div>+0d 15h 14m</div></div>
Troj/Agent-UBN	<div><div>FIRST</div><div>11/16/2011 20:07</div></div>	<div><div></div><div>+0d 5h 23m</div></div>	<div><div></div><div>Not Published</div></div>	<div><div></div><div>Not Published</div></div>	<div><div></div><div>+0d 10h 38m</div></div>
Troj/Agent-UBK	<div><div>FIRST</div><div>11/16/2011 16:51</div></div>	<div><div></div><div>+0d 2h 59m</div></div>	<div><div></div><div>+1d 1h 4m</div></div>	<div><div></div><div>Not Published</div></div>	<div><div></div><div>+0d 6h 54m</div></div>
Trojan variant	<div><div>FIRST</div><div>11/16/2011 15:14</div></div>	<div><div></div><div>Not Published</div></div>	<div><div></div><div>Not Published</div></div>	<div><div></div><div>Not Published</div></div>	<div><div></div><div>+0d 8h 31m</div></div>
Troj/Agent-UBJ	<div><div>FIRST</div><div>11/16/2011 11:25</div></div>	<div><div></div><div>+0d 5h 0m</div></div>	<div><div></div><div>Not Published</div></div>	<div><div></div><div>+0d 18h 40m</div></div>	<div><div></div><div>+0d 12h 20m</div></div>
Troj/Zbot-BDU	<div><div>FIRST</div><div>11/16/2011 09:01</div></div>	<div><div></div><div>+0d 7h 24m</div></div>	<div><div></div><div>+0d 9h 4m</div></div>	<div><div></div><div>Not Published</div></div>	<div><div></div><div>+0d 14h 44m</div></div>
Troj/Zbot-BDV	<div><div>FIRST</div><div>11/16/2011 07:32</div></div>	<div><div></div><div>+0d 12h 18m</div></div>	<div><div></div><div>Not Published</div></div>	<div><div></div><div>Not Published</div></div>	<div><div></div><div>Not Published</div></div>
Troj/Agent-TYS	<div><div>FIRST</div><div>11/16/2011 00:44</div></div>	<div><div></div><div>+0d 7h 11m</div></div>	<div><div></div><div>Not Published</div></div>	<div><div></div><div>Not Published</div></div>	<div><div></div><div>Not Published</div></div>
Troj/Agent-TYS	<div><div>FIRST</div><div>11/16/2011 00:44</div></div>	<div><div></div><div>+0d 7h 11m</div></div>	<div><div></div><div>Not Published</div></div>	<div><div></div><div>Not Published</div></div>	<div><div></div><div>Not Published</div></div>



