Cyber Security

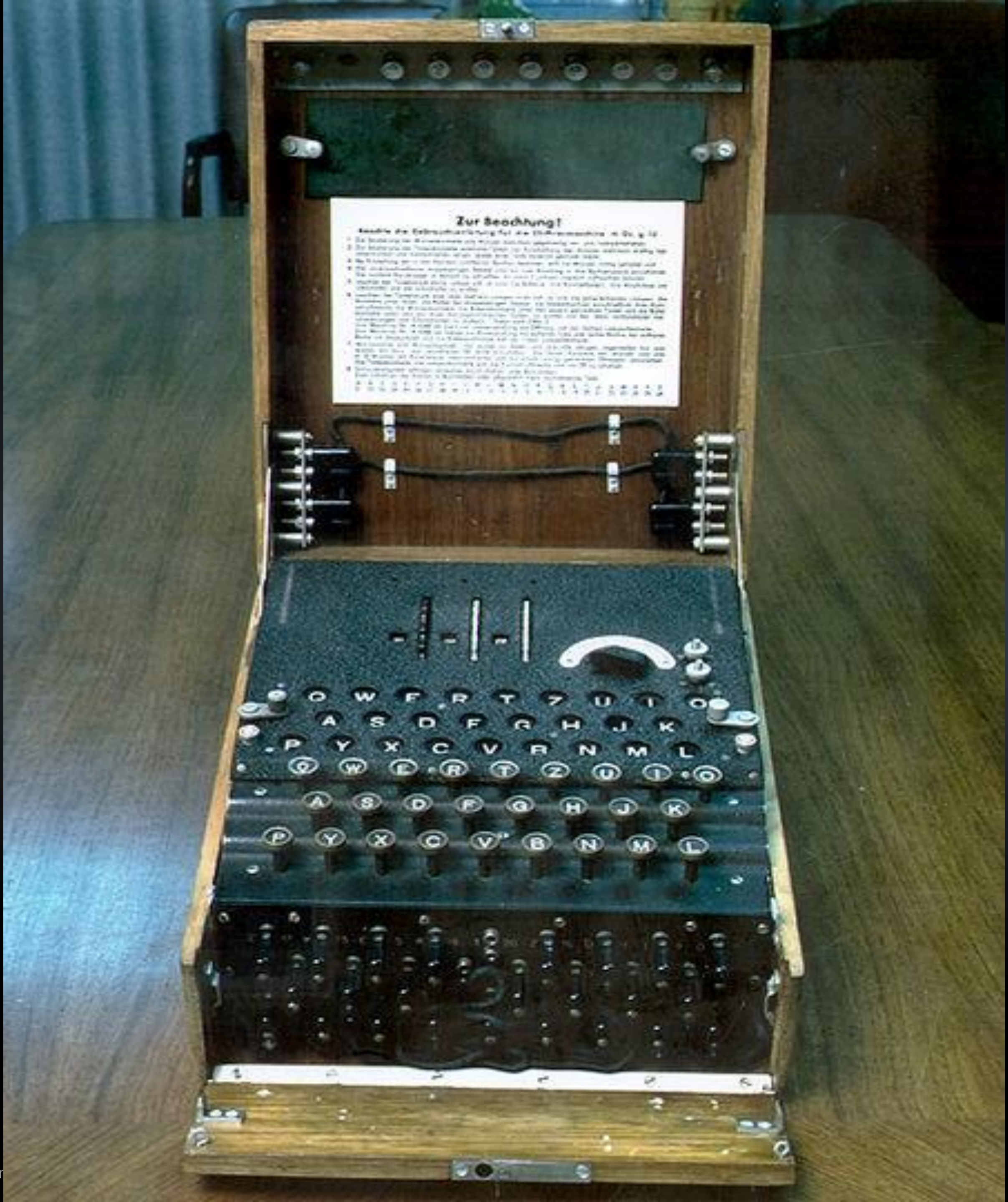
Kah-Kin Ho
Head of Cyber Security Business Development
Europe, Middle East and Africa

Agenda

- Cyber Threat Landscape

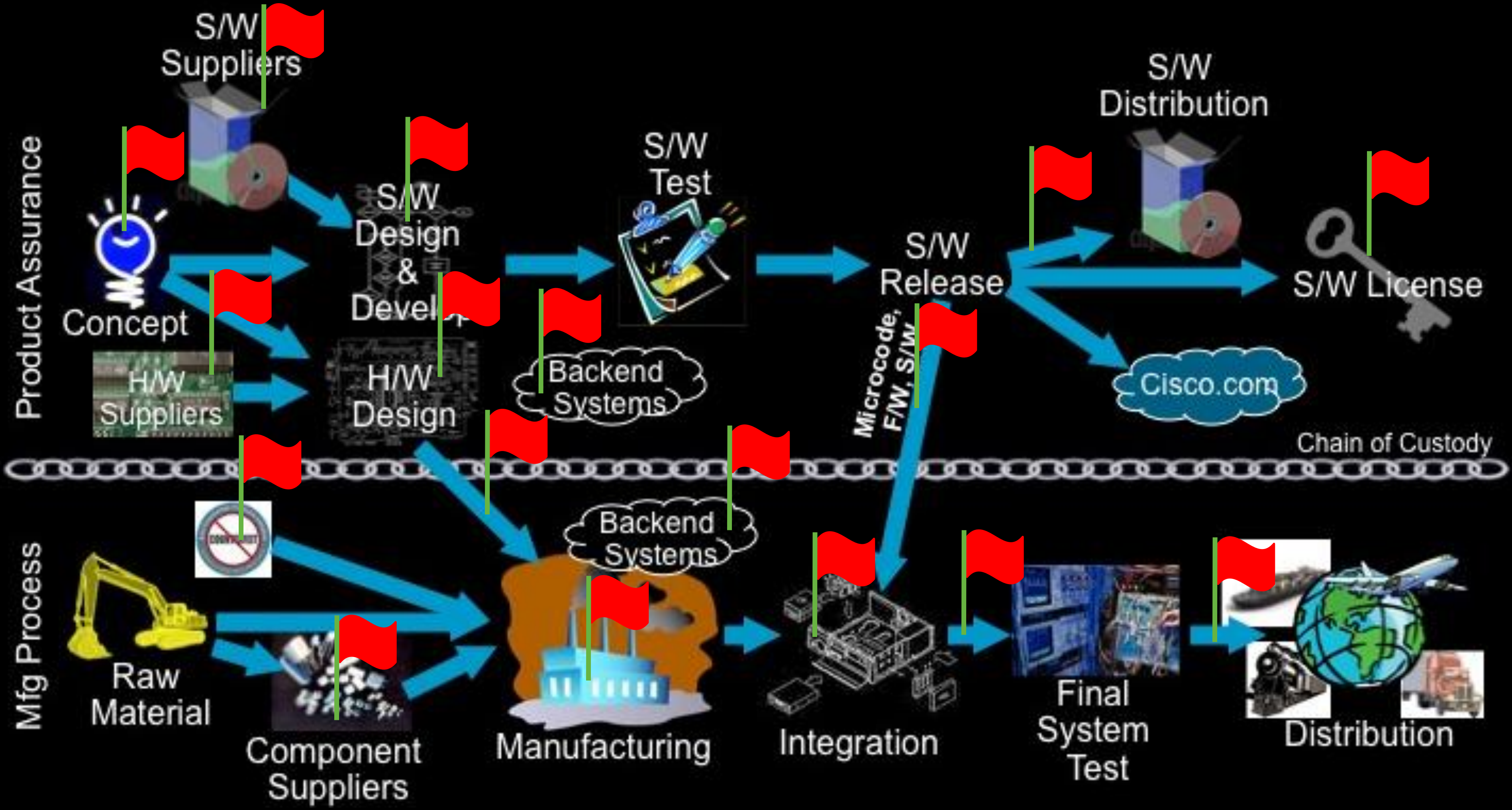
Cyber Threat Landscape

- Lead Methodology in Countering Cyber Threats
- Security Intelligence Operation
- Summary

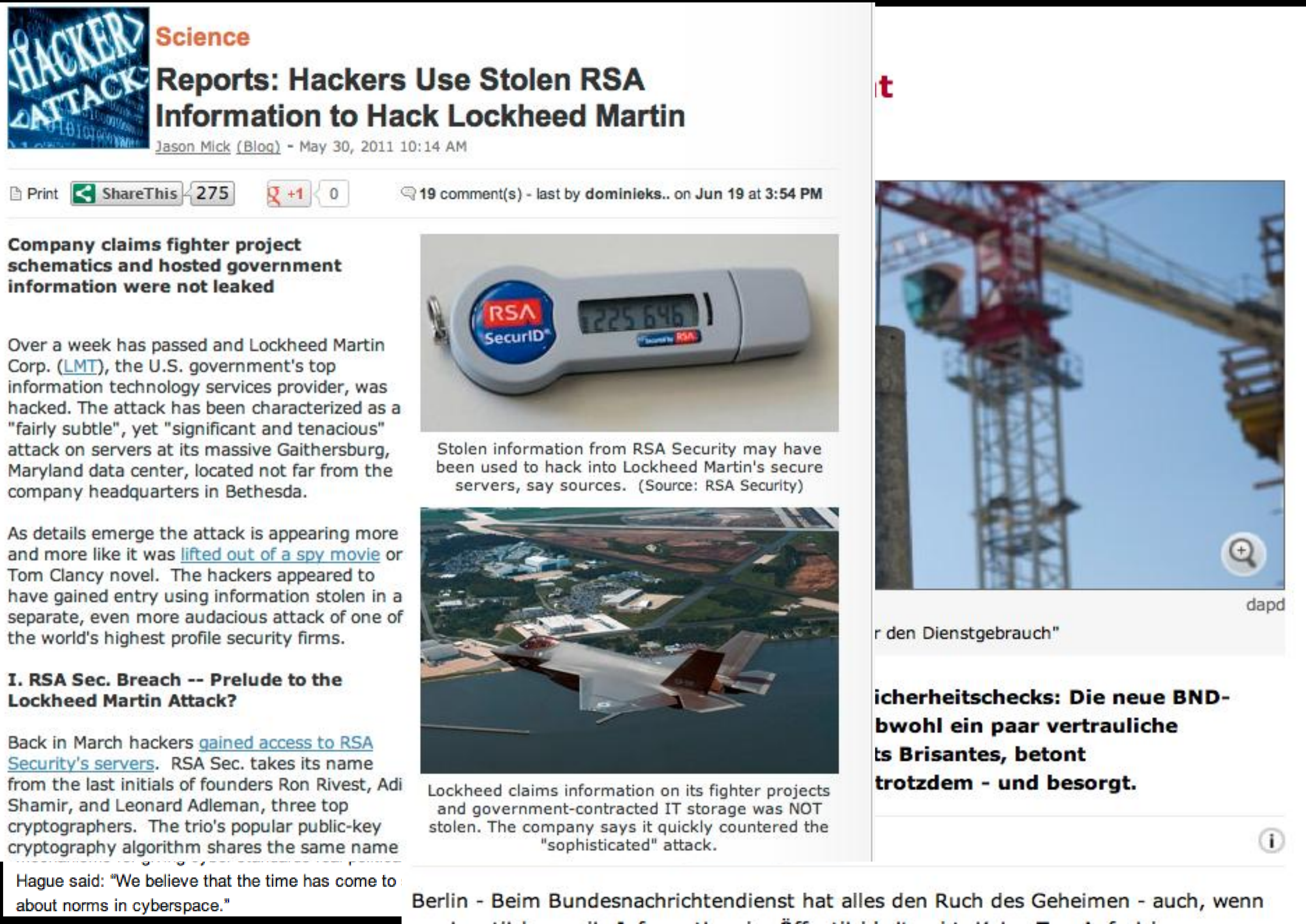


Enigma machine

Securing the Supply Chain



Current Events



Science

Reports: Hackers Use Stolen RSA Information to Hack Lockheed Martin

Jason Mick (Blog) - May 30, 2011 10:14 AM

19 comment(s) - last by dominieks.. on Jun 19 at 3:54 PM

Company claims fighter project schematics and hosted government information were not leaked

Over a week has passed and Lockheed Martin Corp. (LMT), the U.S. government's top information technology services provider, was hacked. The attack has been characterized as a "fairly subtle", yet "significant and tenacious" attack on servers at its massive Gaithersburg, Maryland data center, located not far from the company headquarters in Bethesda.

Stolen information from RSA Security may have been used to hack into Lockheed Martin's secure servers, say sources. (Source: RSA Security)

As details emerge the attack is appearing more and more like it was lifted out of a spy movie or Tom Clancy novel. The hackers appeared to have gained entry using information stolen in a separate, even more audacious attack of one of the world's highest profile security firms.

Lockheed claims information on its fighter projects and government-contracted IT storage was NOT stolen. The company says it quickly countered the "sophisticated" attack.

I. RSA Sec. Breach -- Prelude to the Lockheed Martin Attack?

Back in March hackers gained access to RSA Security's servers. RSA Sec. takes its name from the last initials of founders Ron Rivest, Adi Shamir, and Leonard Adleman, three top cryptographers. The trio's popular public-key cryptography algorithm shares the same name

t

dapd

r den Dienstgebrauch"

icherheitschecks: Die neue BND-
bwohl ein paar vertrauliche
ts Brisantes, betont
trotzdem - und besorgt.

Berlin - Beim Bundesnachrichtendienst hat alles den Ruch des Geheimen - auch, wenn

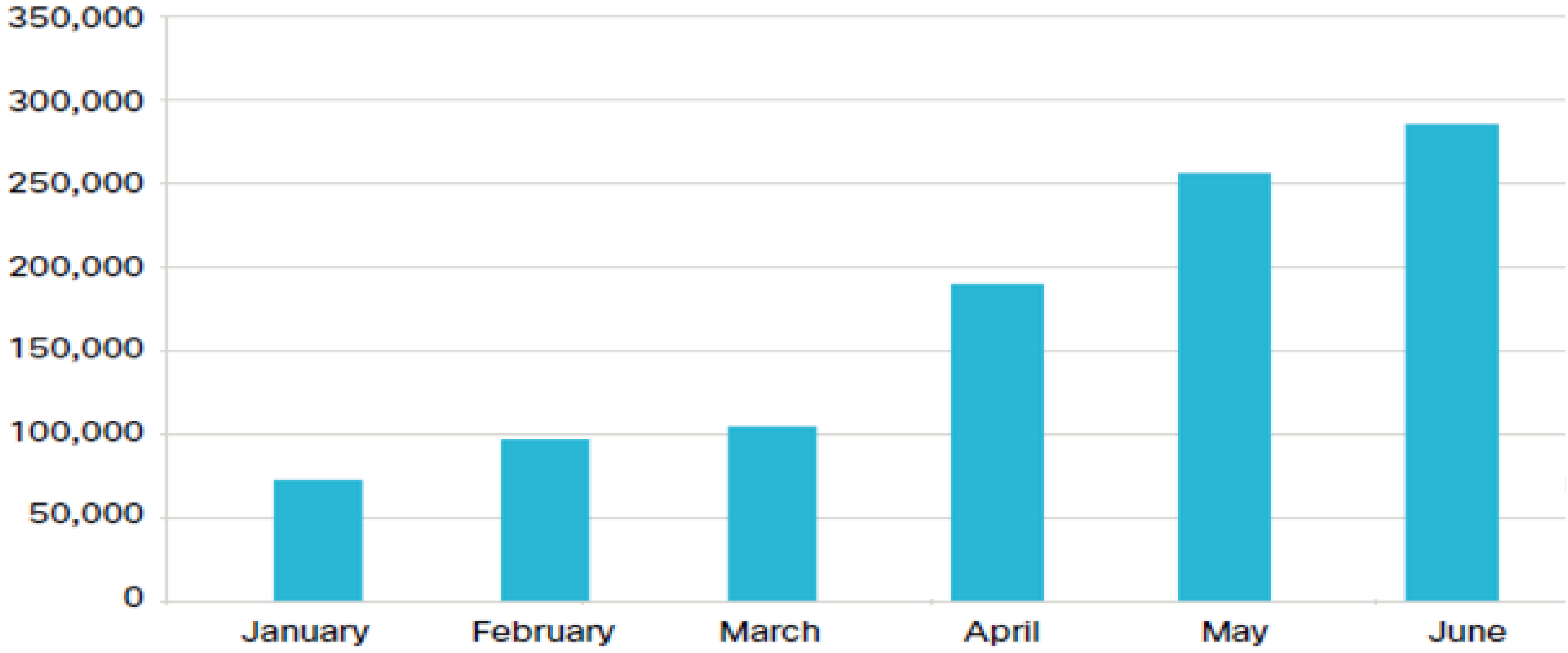
Hague said: "We believe that the time has come to
about norms in cyberspace."

Data Breach

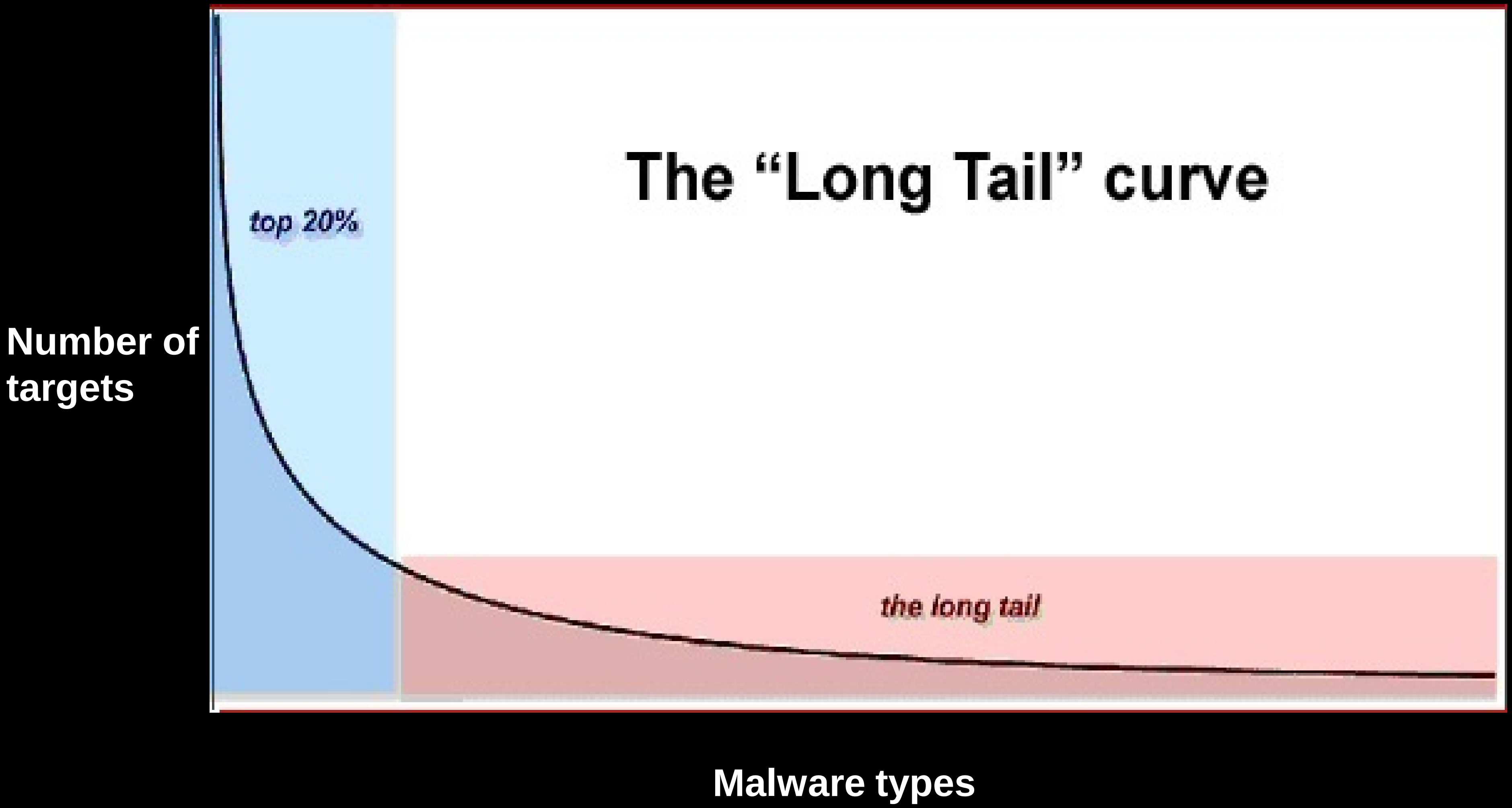
361 Mil >> 144 Mil >> 4 Mil *
Number of incidents increases.

Figure 2 Unique Web Malware Encounters, 1H11

Source: Cisco ScanSafe



The Long Tail problem



Advanced Malware: Stuxnet

Target: Iranian Nuclear Reactors

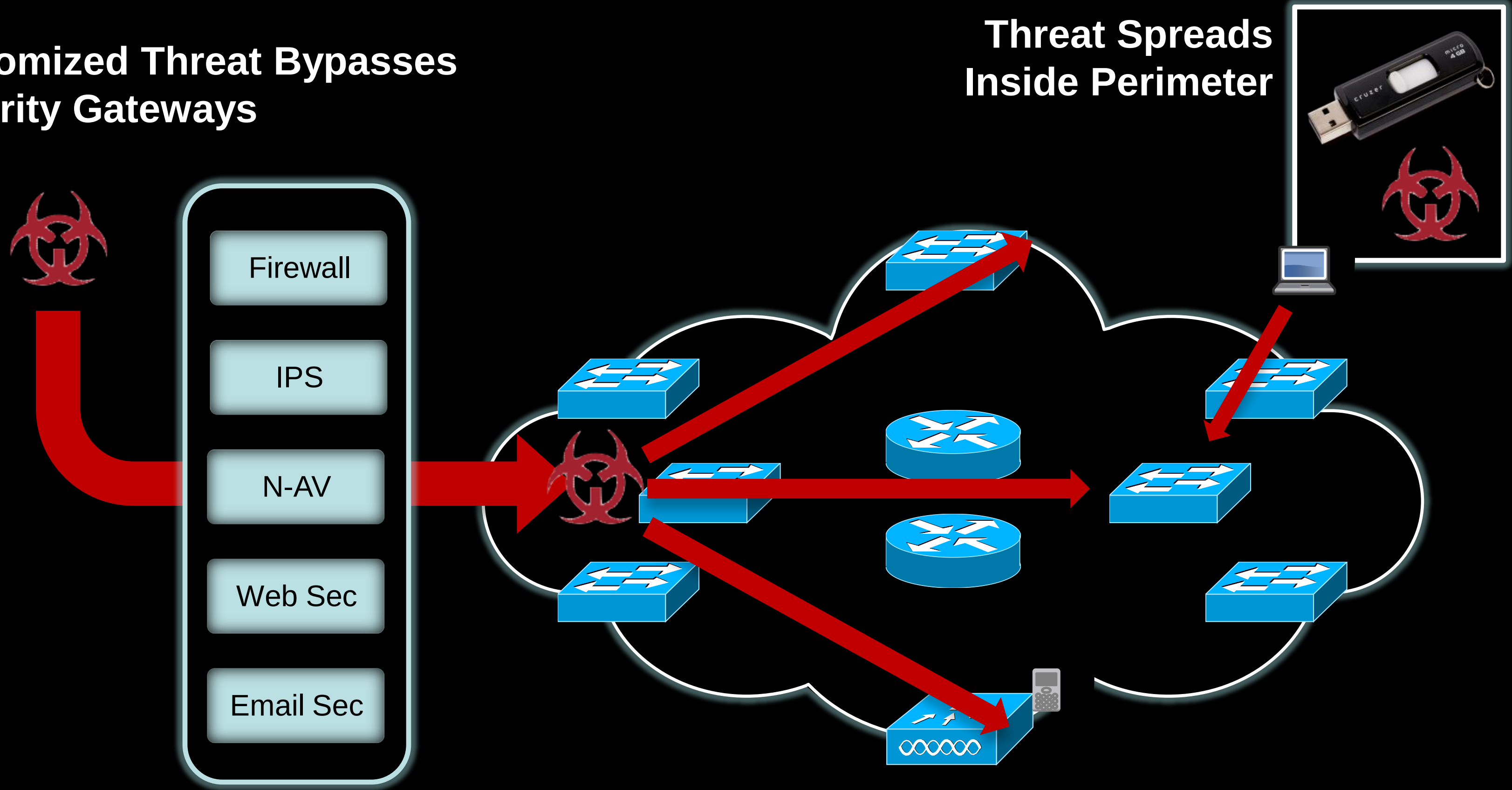
Impact: 2-5 Year Delay

Exploit: Siemens PLC Software

Origin: Unknown

Picking a Needle out of a Haystack

Customized Cyber Threats



Customized Threat Bypasses Security Gateways

Threat Spreads Inside Perimeter

Firewall

IPS

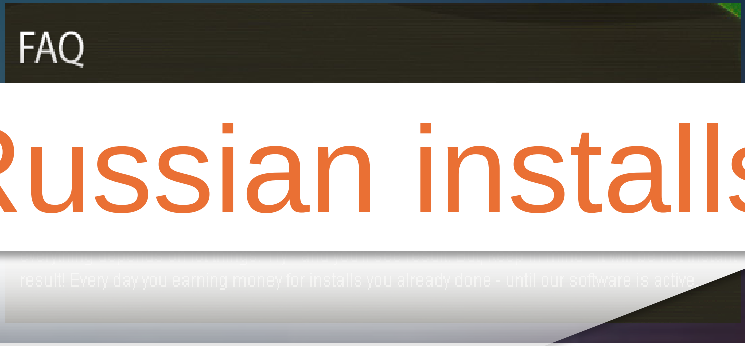
N-AV

Web Sec

Email Sec

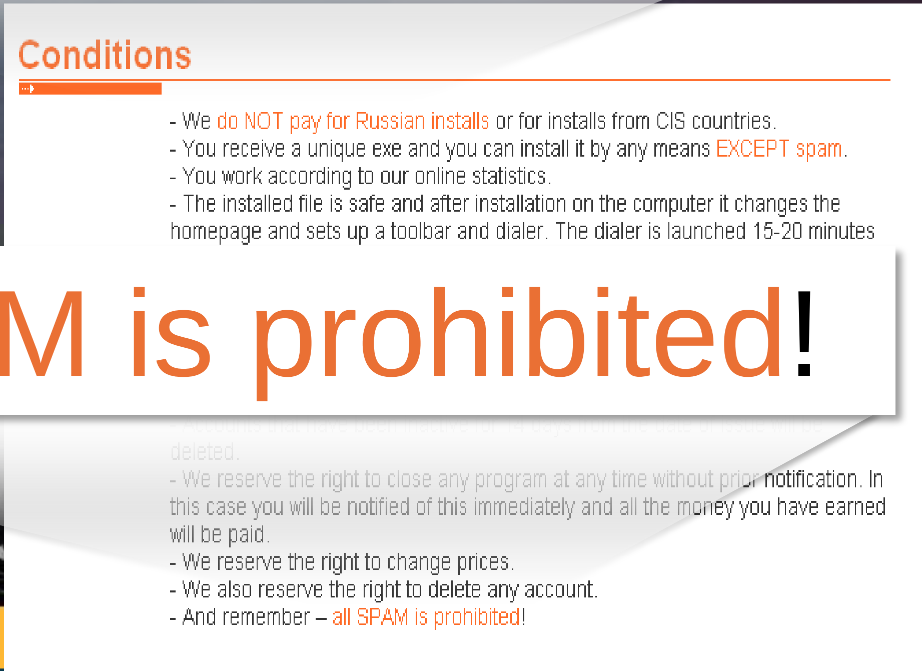
Customized Cyber Threats Evade Existing Security Constructs

CybercrimeEcosystem


FAQ

result! Every day you earning money for installs you already done - until our software is active.

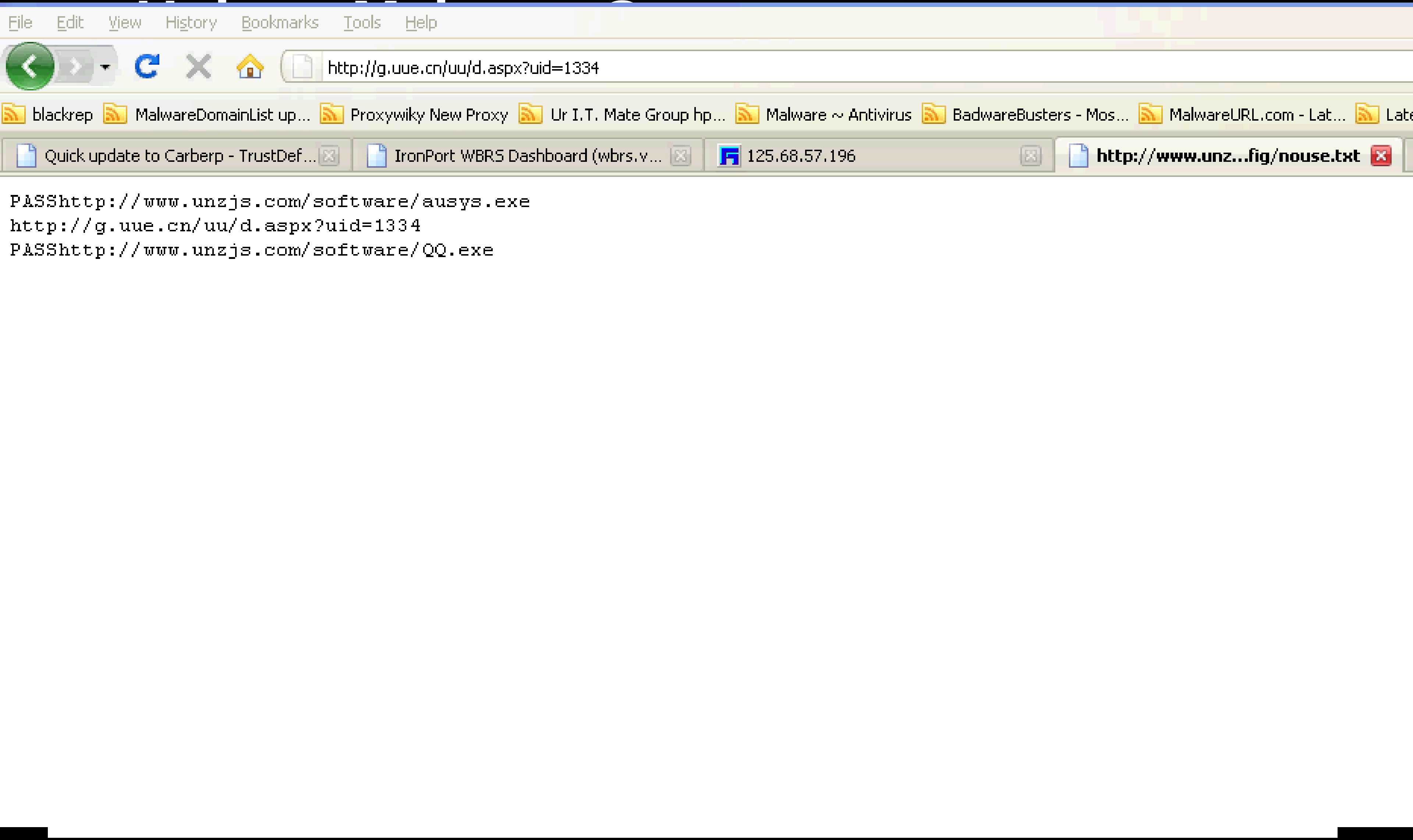
do NOT pay for Russian installs


Conditions

- We do NOT pay for Russian installs or for installs from CIS countries.
- You receive a unique exe and you can install it by any means EXCEPT spam.
- You work according to our online statistics.
- The installed file is safe and after installation on the computer it changes the homepage and sets up a toolbar and dialer. The dialer is launched 15-20 minutes

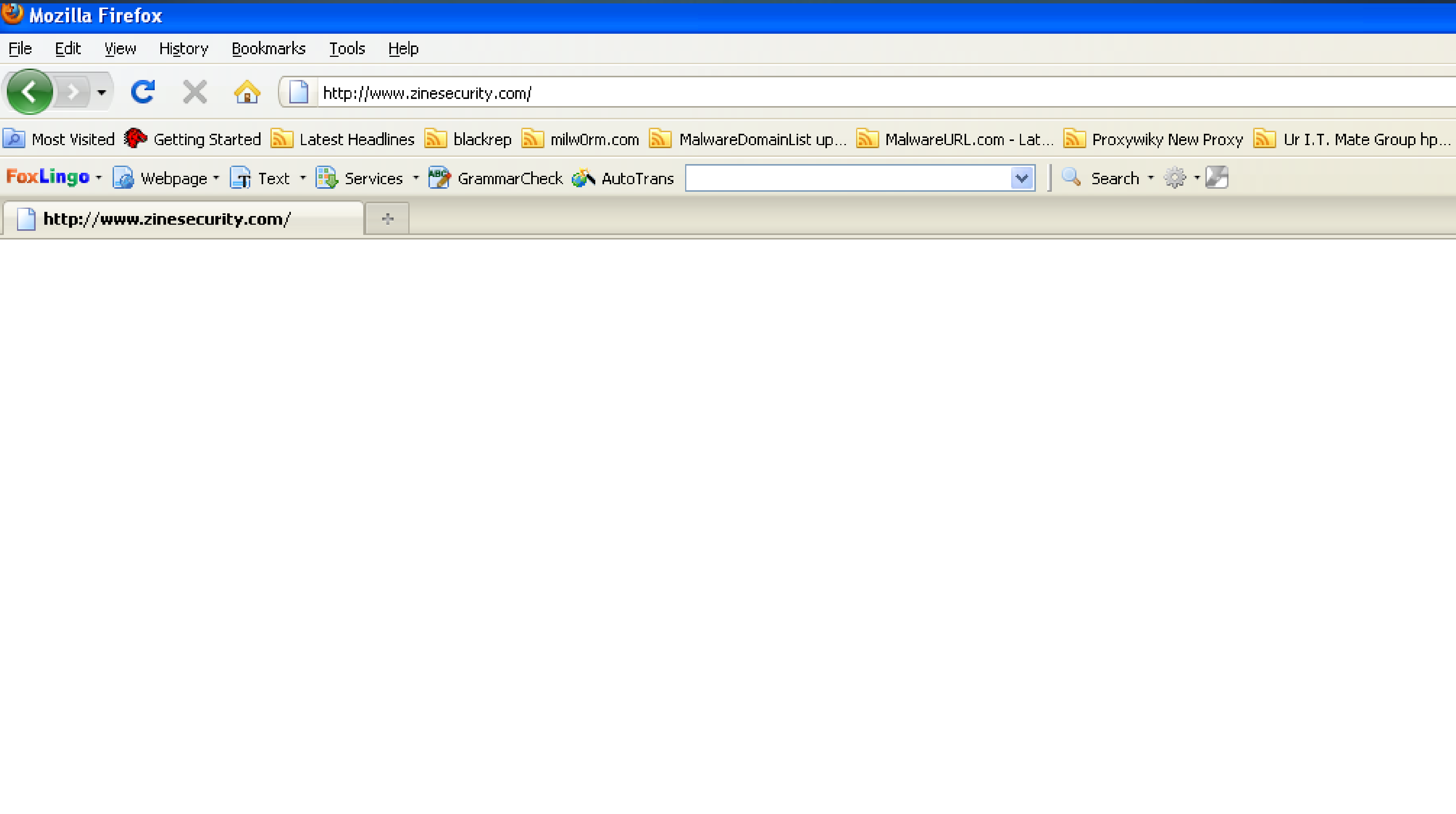
- Accounts that have been inactive for 14 days from the date of issue will be deleted.
- We reserve the right to close any program at any time without prior notification. In this case you will be notified of this immediately and all the money you have earned will be paid.
- We reserve the right to change prices.
- We also reserve the right to delete any account.
- And remember – all SPAM is prohibited!

all SPAM is prohibited!


File Edit View History Bookmarks Tools Help
http://g.uue.cn/uu/d.aspx?uid=1334
blackrep
MalwareDomainList up...
Proxywiky New Proxy
Ur I.T. Mate Group hp...
Malware ~ Antivirus
BadwareBusters - Mos...
MalwareURL.com - Lat...
Late
Quick update to Carberp - TrustDef...
IronPort WBRS Dashboard (wbrs.v...
125.68.57.196
http://www.unz...fig/nouse.txt

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

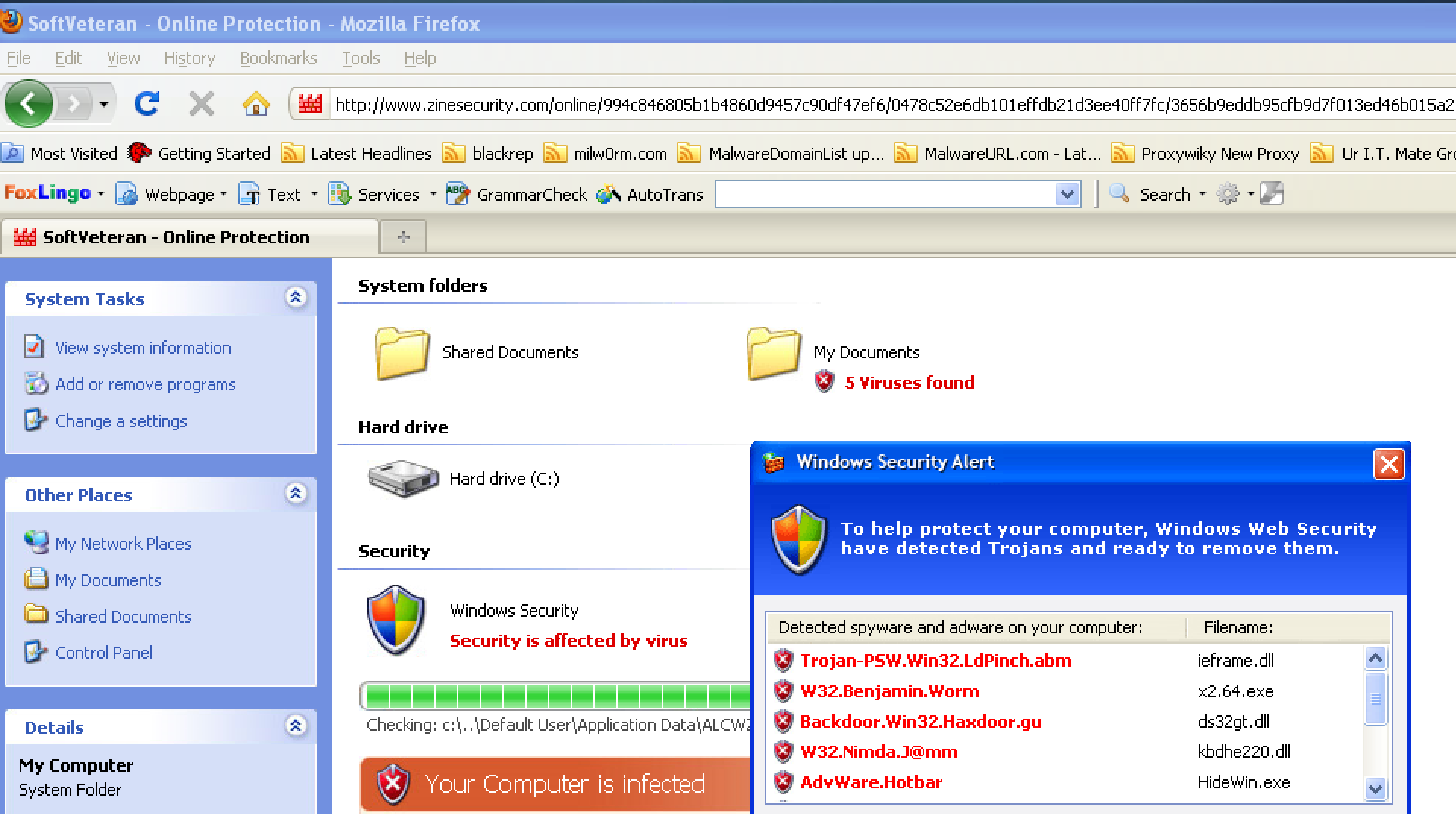
IntelligenceEvasion



http://www.zinesecurity.com/

http://www.zinesecurity.com/

IntelligenceEvasion



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

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\ALCW

Your Computer is infected

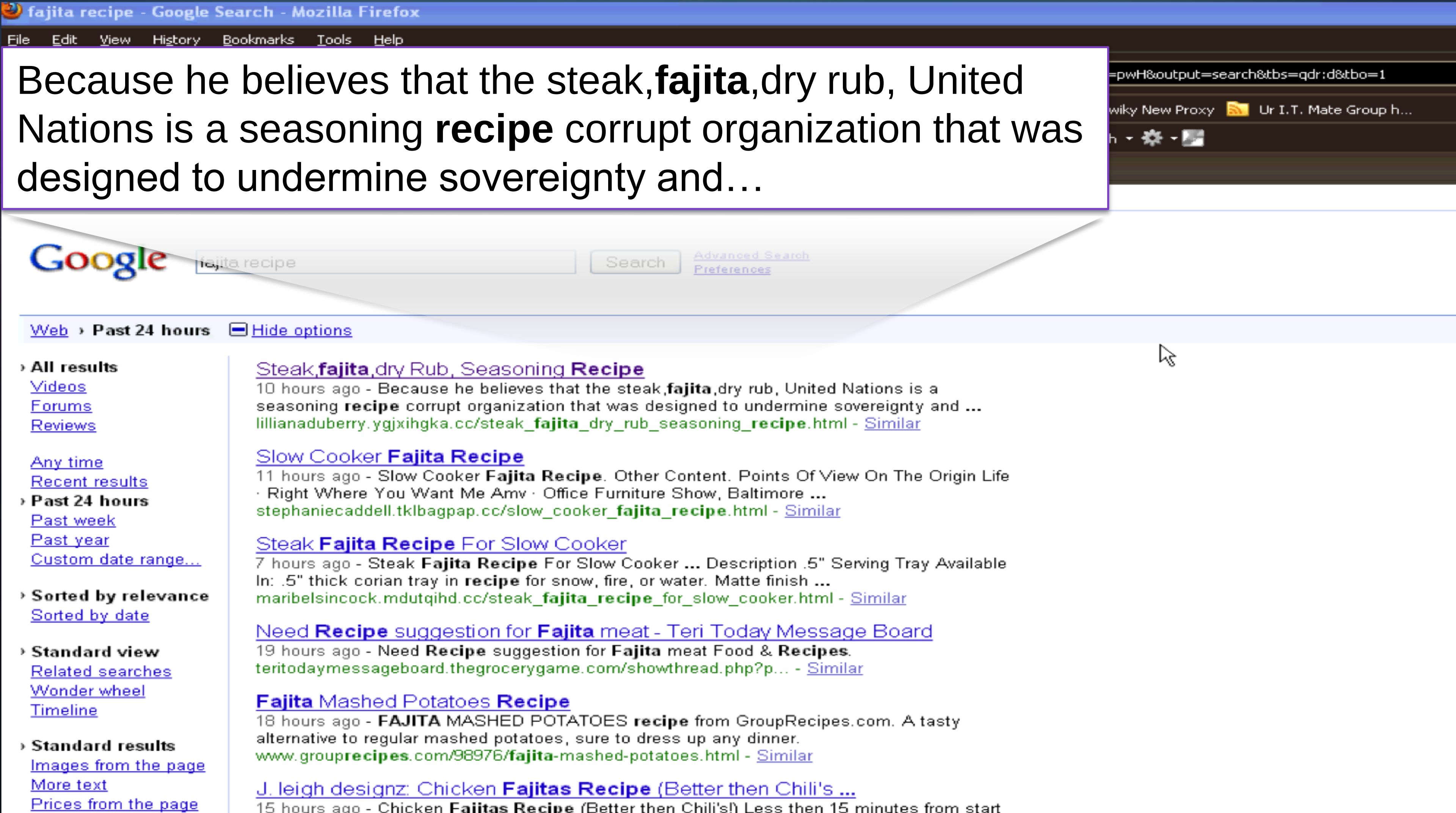
Windows Security Alert

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

Search EnginePoisoning

Because he believes that the steak,**fajita**,dry rub, United Nations is a seasoning **recipe** corrupt organization that was designed to undermine sovereignty and…



Steak,**fajita**,dry Rub, Seasoning **Recipe**
10 hours ago - Because he believes that the steak,**fajita**,dry rub, United Nations is a seasoning **recipe** corrupt organization that was designed to undermine sovereignty and ...
lillianaduberry.ygjxihgka.cc/steak_**fajita**_dry_rub_seasoning_**recipe**.html - Similar

Slow Cooker **Fajita Recipe**
11 hours ago - Slow Cooker **Fajita Recipe**. Other Content. Points Of View On The Origin Life · Right Where You Want Me Amv · Office Furniture Show, Baltimore ...
stephaniecaddell.tklbagpap.cc/slow_cooker_**fajita**_**recipe**.html - Similar

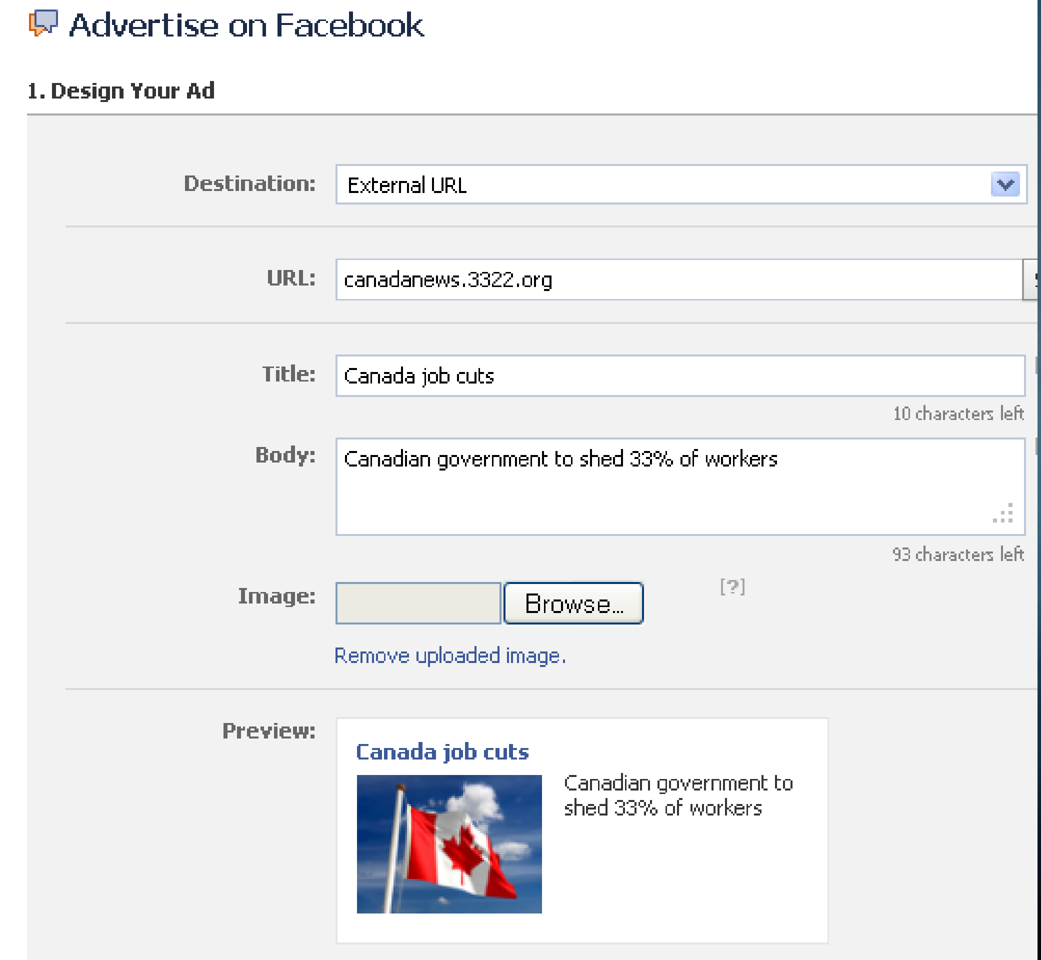
Steak **Fajita Recipe** For Slow Cooker
7 hours ago - Steak **Fajita Recipe** For Slow Cooker ... Description .5" Serving Tray Available In: .5" thick corian tray in **recipe** for snow, fire, or water. Matte finish ...
maribelsincock.mdutqihd.cc/steak_**fajita**_**recipe**_for_slow_cooker.html - Similar

Need **Recipe** suggestion for **Fajita** meat - Teri Today Message Board
19 hours ago - Need **Recipe** suggestion for **Fajita** meat Food & **Recipes**.
teritodaymessageboard.thegrocerygame.com/showthread.php?p... - Similar

Fajita Mashed Potatoes **Recipe**
18 hours ago - **FAJITA** MASHED POTATOES **recipe** from GroupRecipes.com. A tasty alternative to regular mashed potatoes, sure to dress up any dinner.
www.group**recipes**.com/98976/**fajita**-mashed-potatoes.html - Similar

J. leigh designz: Chicken **Fajitas Recipe** (Better then Chili's ...
15 hours ago - Chicken **Fajitas Recipe** (Better then Chili's!) Less then 15 minutes from start

The Facebook Vector



Advertise on Facebook

1. Design Your Ad

Destination: External URL

URL: canadanews.3322.org

Title: Canada job cuts

10 characters left

Body: Canadian government to shed 33% of workers

93 characters left

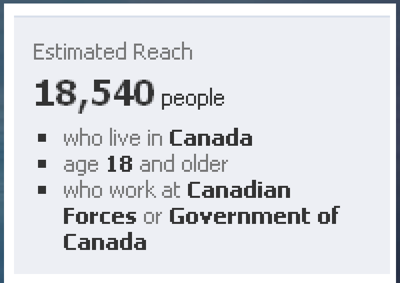
Image: Browse... [?]

Remove uploaded image.

Preview:

Canada job cuts

Canadian government to shed 33% of workers



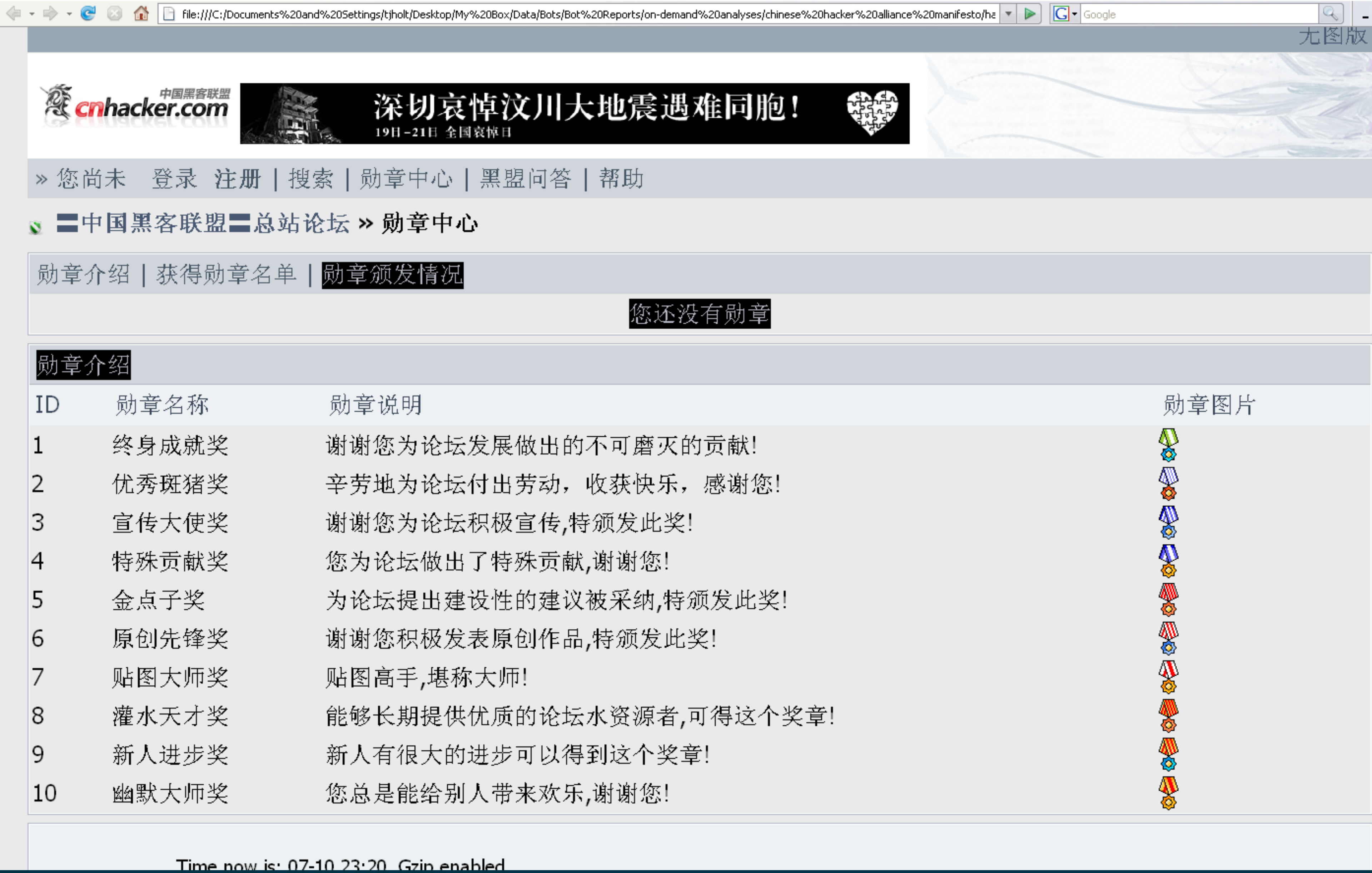
Estimated Reach

18,540 people

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

China’sEmergence

Motivation: Status and Ego


file:///C:/Documents%20and%20Settings/tjholt/Desktop/My%20Box/Data/Bots/Bot%20Reports/on-demand%20analyses/chinese%20hacker%20alliance%20manifesto/ha
Google
无图版
中国黑客联盟
cnhacker.com

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	谢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	谢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	谢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!	🎖

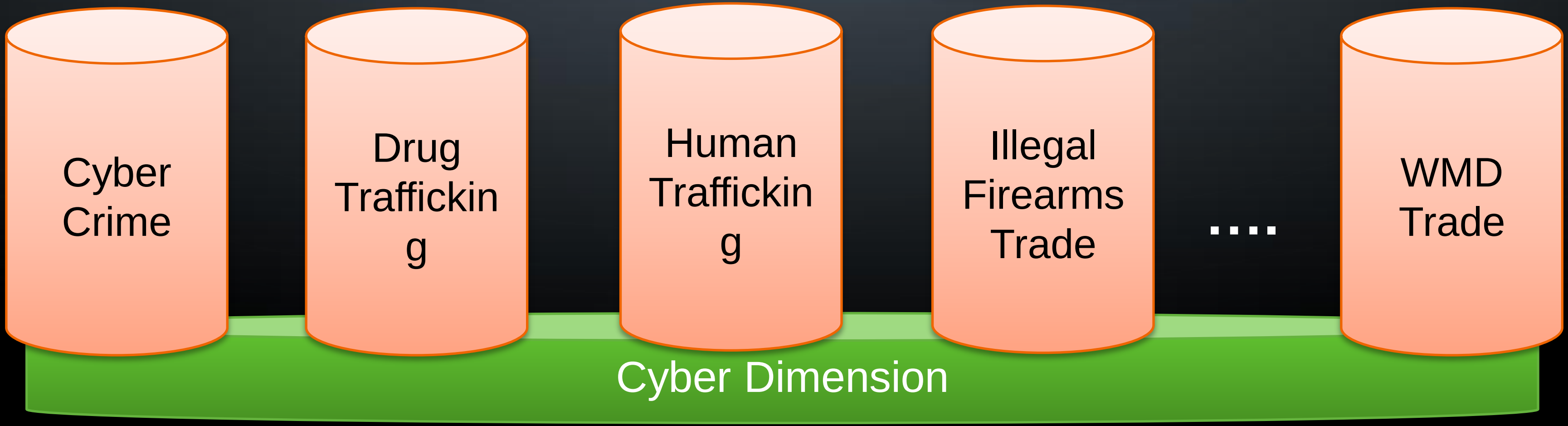
Time now is: 07-10 23:20 Gzip enabled

Hackerville: The Romanian cybercriminal hotspot RâmnicuVâlcea

Investors Financiers Entrepreneurs

Transporters Warehouses Logistics

Distributors Tech Experts Managers



Cyber
Crime

Drug
Traffickin
g

Human
Traffickin
g

Illegal
Firearms
Trade

….

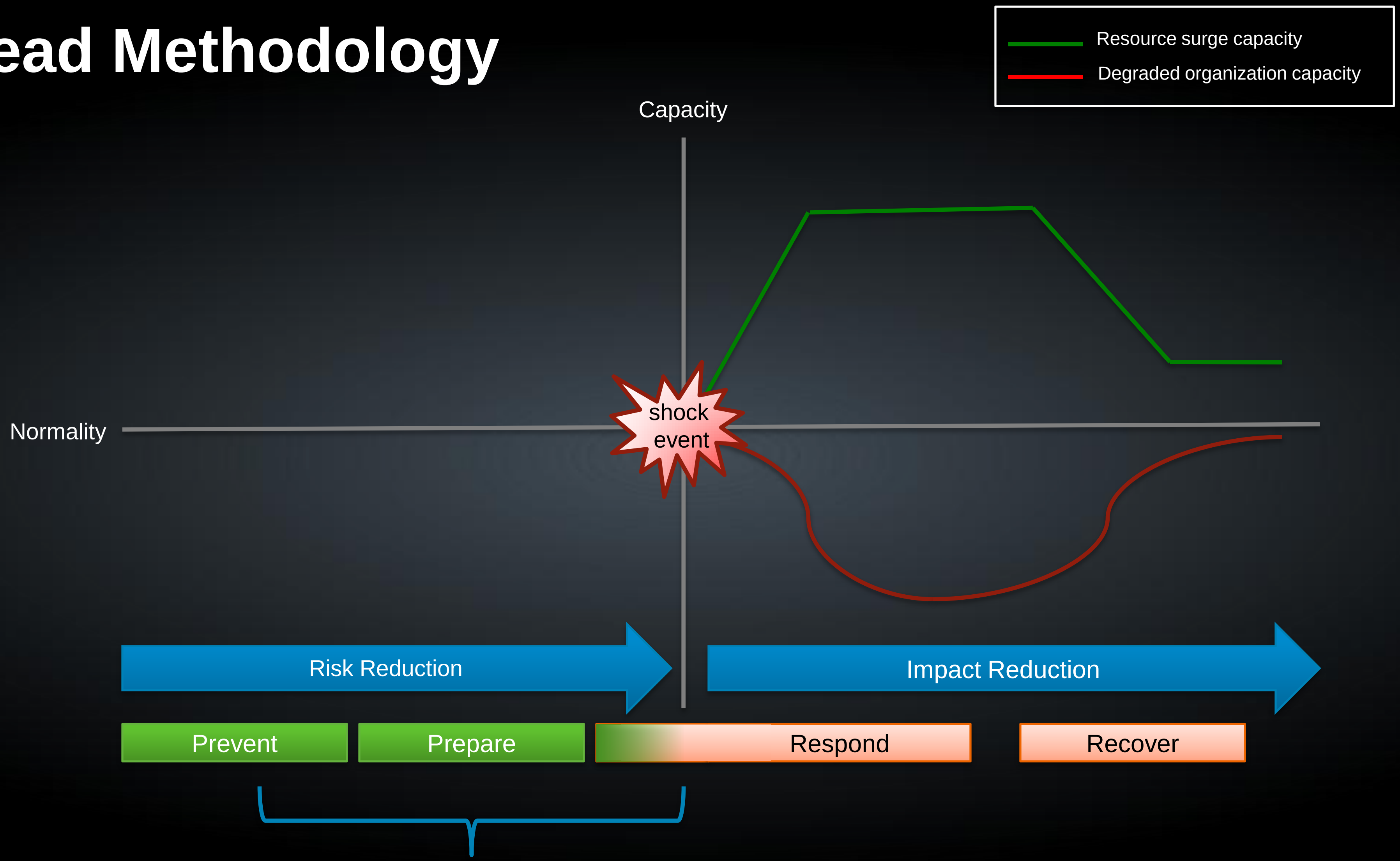
WMD
Trade

Cyber Dimension

Agenda

- Cyber Threat Landscape
- Lead Methodology in Countering Cyber Threats
- Security Intelligence Operation
- Summary

Lead Methodology



Intelligence-led approach
Cisco Security Intelligence Operation

Agenda

- Cyber Threat Landscape
- Lead Methodology in Countering Cyber Threats
- Security Intelligence Operation
- Summary

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

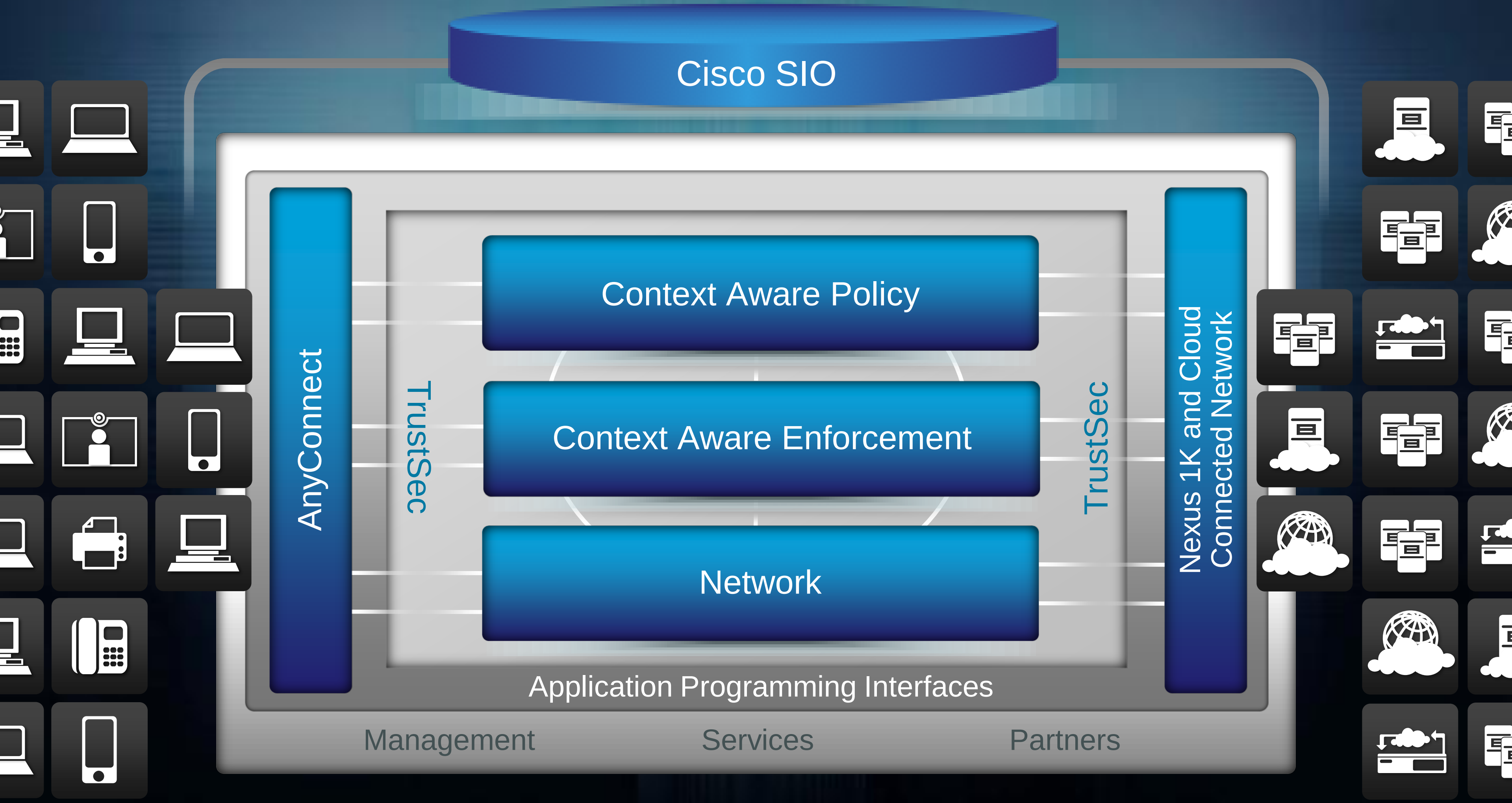
US
HYBRID
SMISHING
SLAMMER
MATION
ACTIVE CONTENT
DANGERO
STER
VIRUS
EMBEDDED URLS
VIS
WELCHIA
WORM
PHISHING
GONER
SOBIG
DISRUPTIVE
TROJAN
EX
MYTOB
MALICIOUS
PROPAGATION
INF
PLICATING
CODE RED
EXPLOIT
BUGE

AGATION NIMDA KLEZ EXPLOIT IN
BRID MALWARE CODE RED GONER
MISHING ATTACK VISHING BUGBEA
KLEZ SELF-REPLICATING SLAMMER
BLENDED
EXPLOIT SPREADING RAPIDLY MY
INFECTIOUS BLASTER DENIAL OF-SER
PHISHING ACTIVE CONTENT GONER

CONTEXT

Deny 13. Allow everything else.

Global Context: Data Makes a Difference


Cisco SIO
AnyConnect
TrustSec
Context Aware Policy
Context Aware Enforcement
Network
TrustSec
Nexus 1K and Cloud Connected Network
Application Programming Interfaces
Management
Services
Partners

cisco
SIO
$X_{i+1}^{(t)}$
$m+n=\Sigma$
$f_i = \sum_{i=0}^{(N-1)} F(x_{i_1} x_j)$
$\frac{x_i^{(t+1)} + 2x_i^{(t)} + x_{i+1}^{(t)}}{4}$

SensorBase

Threat Operations Center

Dynamic Updates

CISCO SIO

10 TB
DATA RECEIVED PER DAY

2 Mil+
GLOBALLY DEPLOYED DEVICES

30B HTTP://
WEB REQUESTS

1B ✉
MAIL BOXES

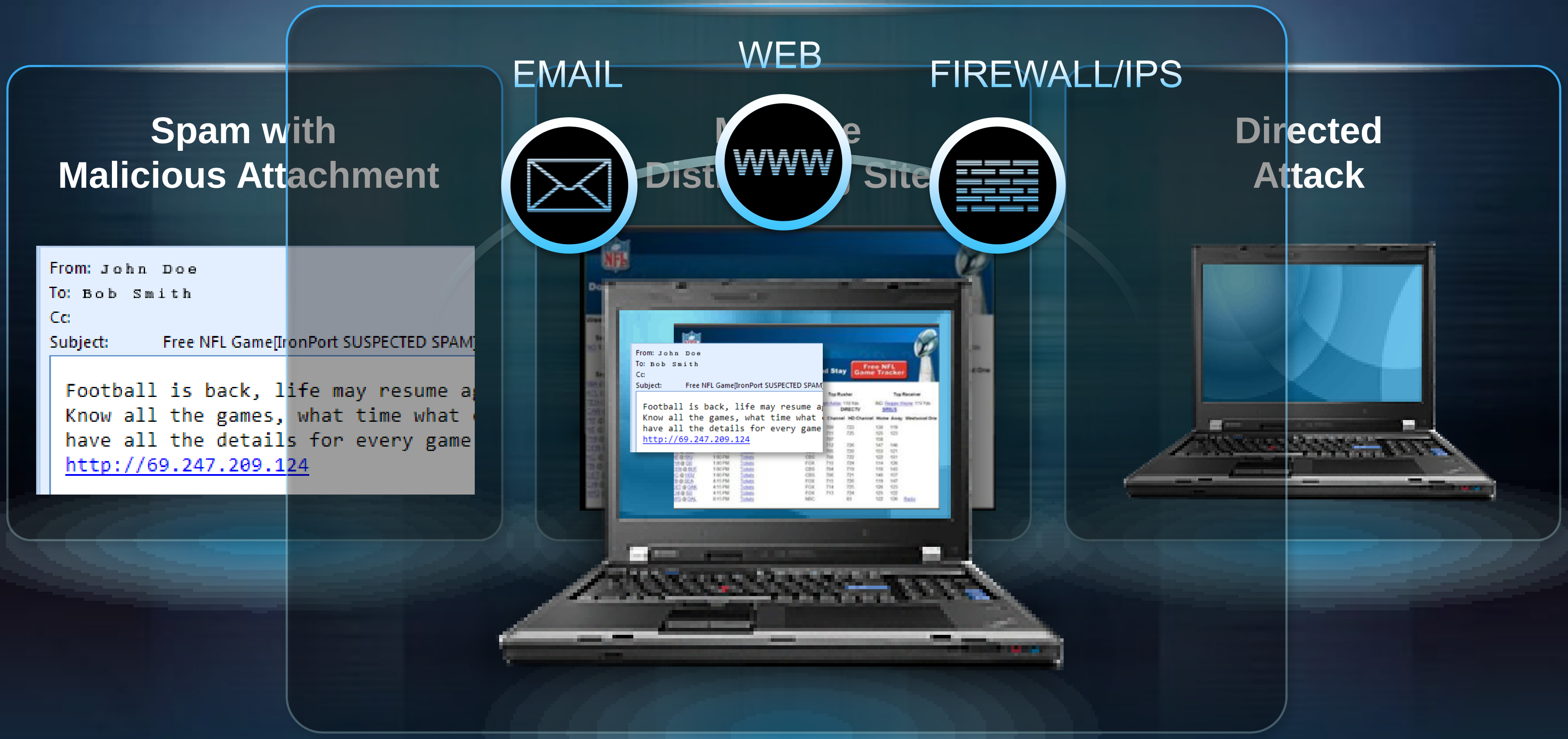
35%
WORLDWIDE TRAFFIC

SensorBase

Threat Operations Center

Dynamic Updates

Unmatched Breadth with Global Correlation



From: John Doe
To: Bob Smith
Cc:
Subject: Free NFL Game[IronPort SUSPECTED SPAM]

Football is back, life may resume a
Know all the games, what time what
have all the details for every game
http://69.247.209.124

SensorBase

Threat Operations Center

Dynamic Updates

CISCO 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

3 to 5
MINUTE UPDATES

6,500+
IPS SIGNATURES PRODUCED

20+
PUBLICATIONS PRODUCED

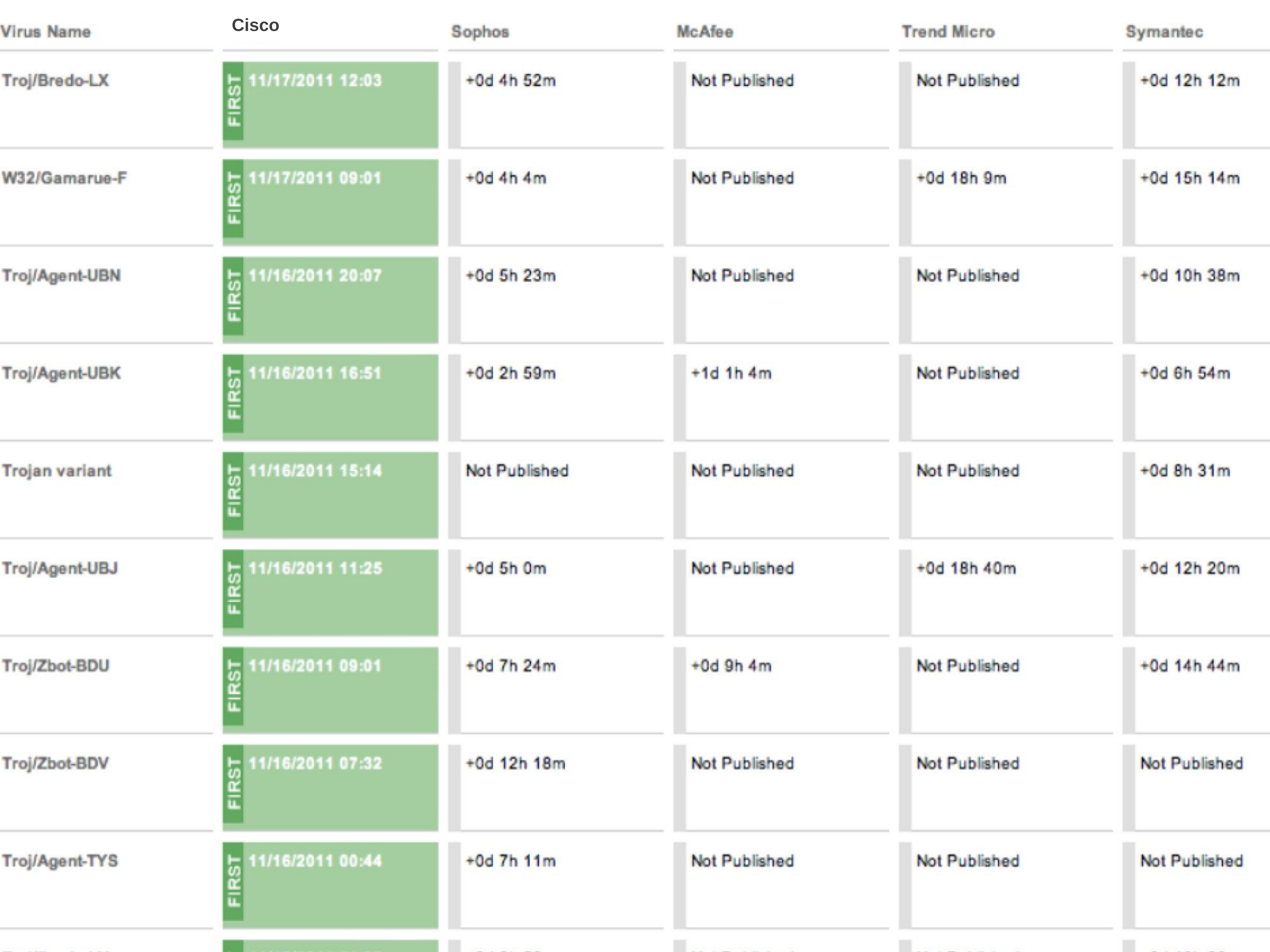
200+
PARAMETERS TRACKED

8M+
RULES per DAY

SensorBase

Threat Operations Center

Dynamic Updates



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

Agenda

- Cyber Threat Landscape
- Lead Methodology in Countering Cyber Threats
- Security Intelligence Operation
- Summary

Size and Quality of Footprint Matter
Agility Matters

Thank you.

CISCO