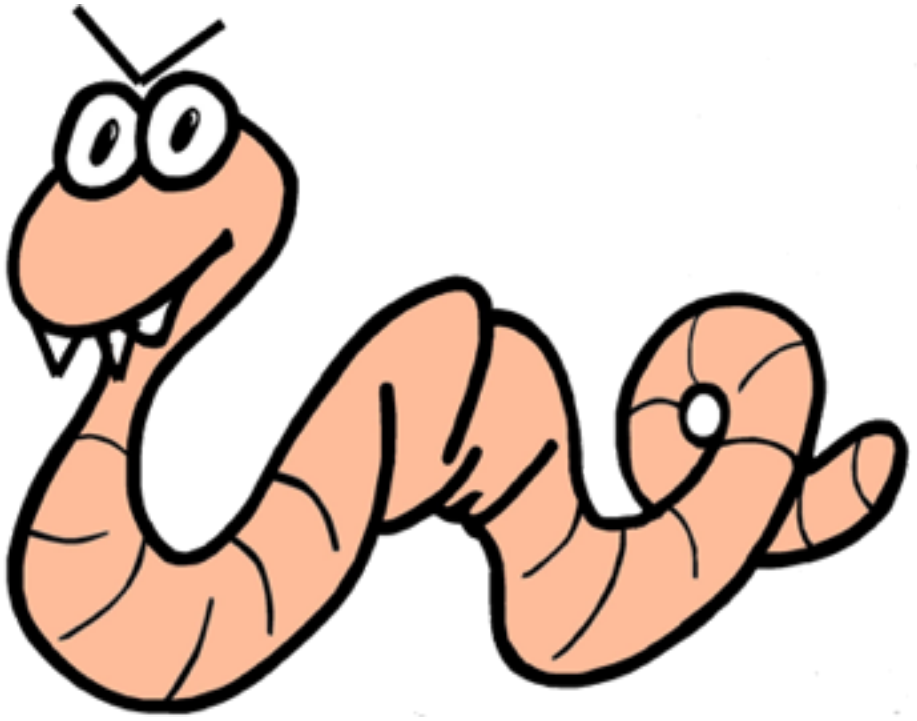
Conficker Worm



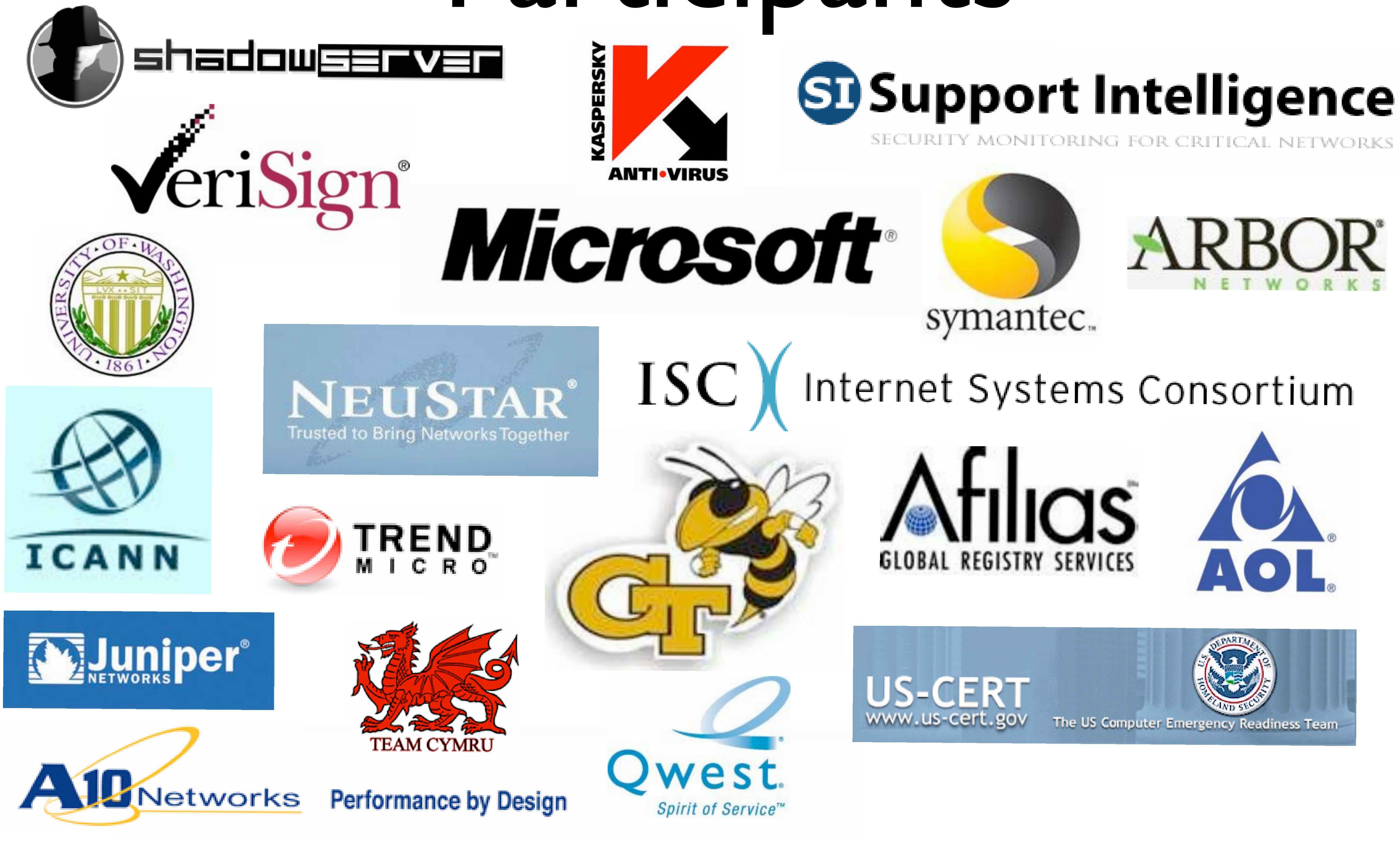
World Federation of Scientists
Erice, Sicily

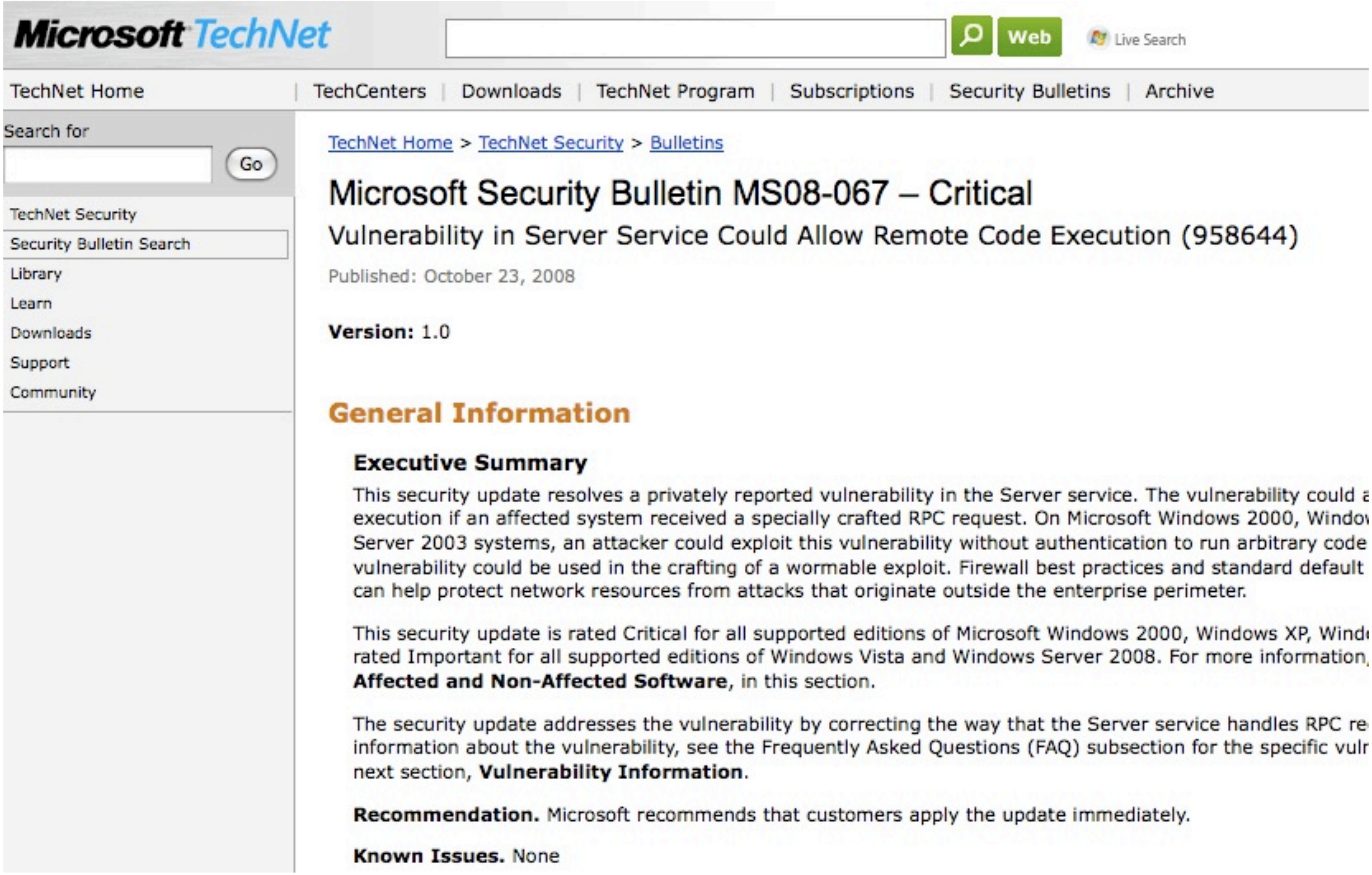
The Conficker Worm

Aug 19-24, 2009
Rick Wesson
CEO, Support Intelligence

KEVIN BACON
They say there's nothing new under the sun.
But under the ground...
CONFICKER
A NO FRILLS/WILSON-MADDOCK Production "TREMORS" KEVIN BACON · FRED WARD · FINN CARTER · MICHAEL GROSS and REBA McENTIRE
Music Composed and Conducted by ERNEST TROOST Edited by O. NICHOLAS BROWN Production Designer IVO CRISTANTE Director of Photography ALEXANDER GRUSZYNSKI
Line Producer GINNY NUGENT Executive Producer GALE ANNE HURD Story by S.S. WILSON & BRENT MADDOCK & RON UNDERWOOD Screenplay by S.S. WILSON & BRENT MADDOCK
PG-13 Produced by BRENT MADDOCK and S.S. WILSON Directed by RON UNDERWOOD A UNIVERSAL RELEASE

Participants





Microsoft Security Bulletin MS08-067 – Critical

Vulnerability in Server Service Could Allow Remote Code Execution (958644)

Published: October 23, 2008

Version: 1.0

General Information

Executive Summary

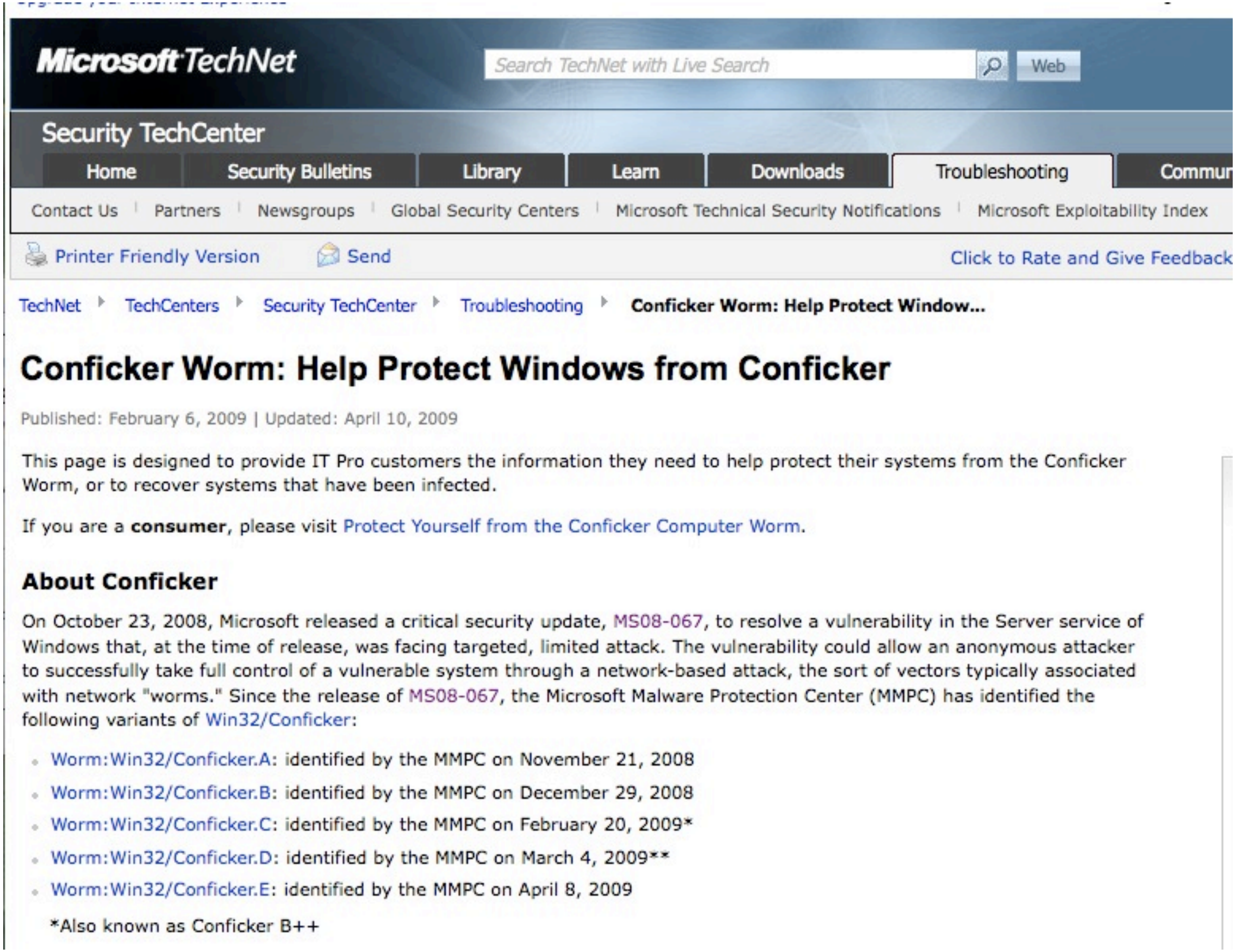
This security update resolves a privately reported vulnerability in the Server service. The vulnerability could a
execution if an affected system received a specially crafted RPC request. On Microsoft Windows 2000, Windo
Server 2003 systems, an attacker could exploit this vulnerability without authentication to run arbitrary code
vulnerability could be used in the crafting of a wormable exploit. Firewall best practices and standard default
can help protect network resources from attacks that originate outside the enterprise perimeter.

This security update is rated Critical for all supported editions of Microsoft Windows 2000, Windows XP, Wind
rated Important for all supported editions of Windows Vista and Windows Server 2008. For more information,
Affected and Non-Affected Software, in this section.

The security update addresses the vulnerability by correcting the way that the Server service handles RPC re
information about the vulnerability, see the Frequently Asked Questions (FAQ) subsection for the specific vulr
next section, **Vulnerability Information**.

Recommendation. Microsoft recommends that customers apply the update immediately.

Known Issues. None



Conficker Worm: Help Protect Windows from Conficker

Published: February 6, 2009 | Updated: April 10, 2009

This page is designed to provide IT Pro customers the information they need to help protect their systems from the Conficker Worm, or to recover systems that have been infected.

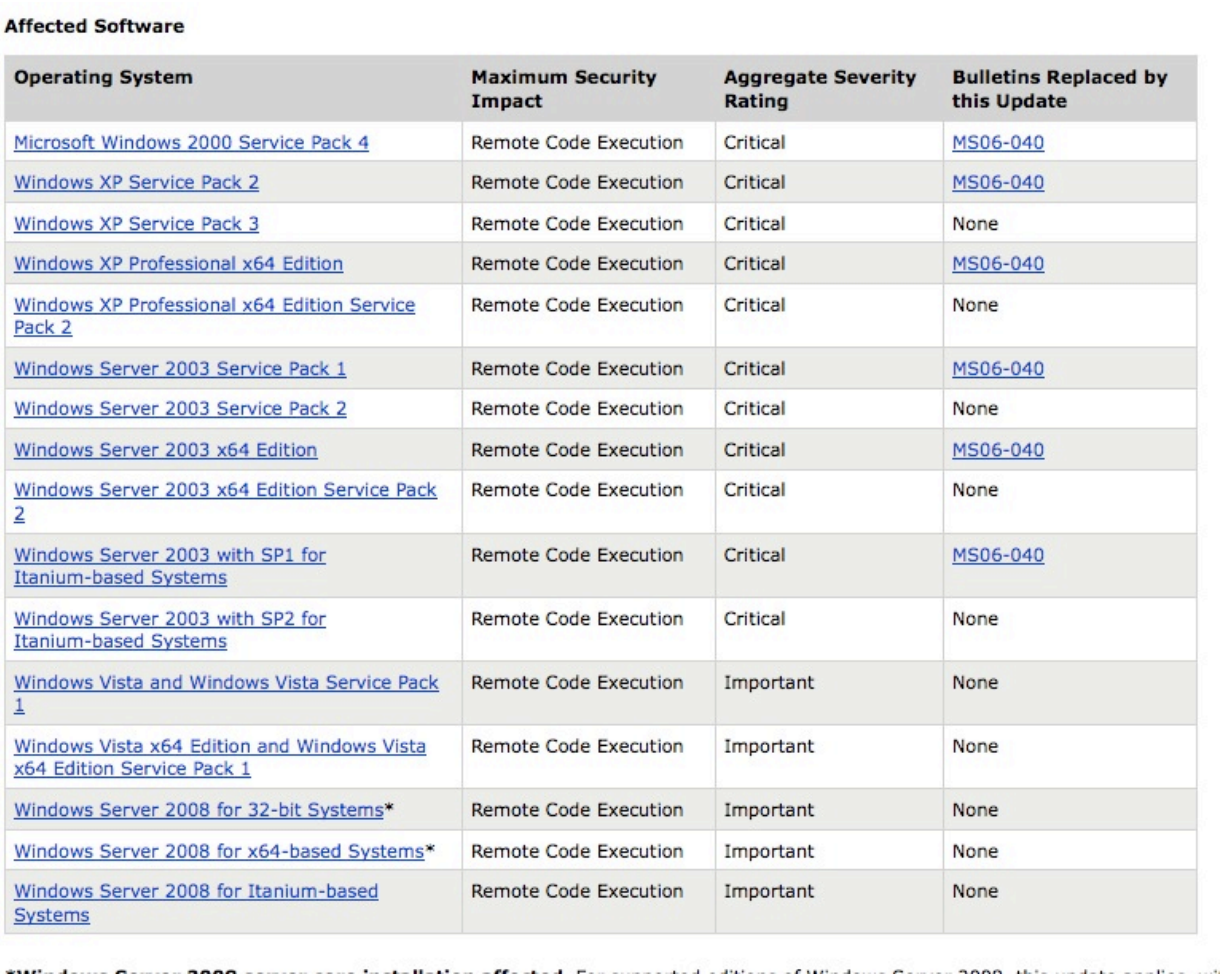
If you are a **consumer**, please visit Protect Yourself from the Conficker Computer Worm.

About Conficker

On October 23, 2008, Microsoft released a critical security update, MS08-067, to resolve a vulnerability in the Server service of Windows that, at the time of release, was facing targeted, limited attack. The vulnerability could allow an anonymous attacker to successfully take full control of a vulnerable system through a network-based attack, the sort of vectors typically associated with network "worms." Since the release of MS08-067, the Microsoft Malware Protection Center (MMPC) has identified the following variants of Win32/Conficker:

- Worm:Win32/Conficker.A: identified by the MMPC on November 21, 2008
- Worm:Win32/Conficker.B: identified by the MMPC on December 29, 2008
- Worm:Win32/Conficker.C: identified by the MMPC on February 20, 2009*
- Worm:Win32/Conficker.D: identified by the MMPC on March 4, 2009**
- Worm:Win32/Conficker.E: identified by the MMPC on April 8, 2009

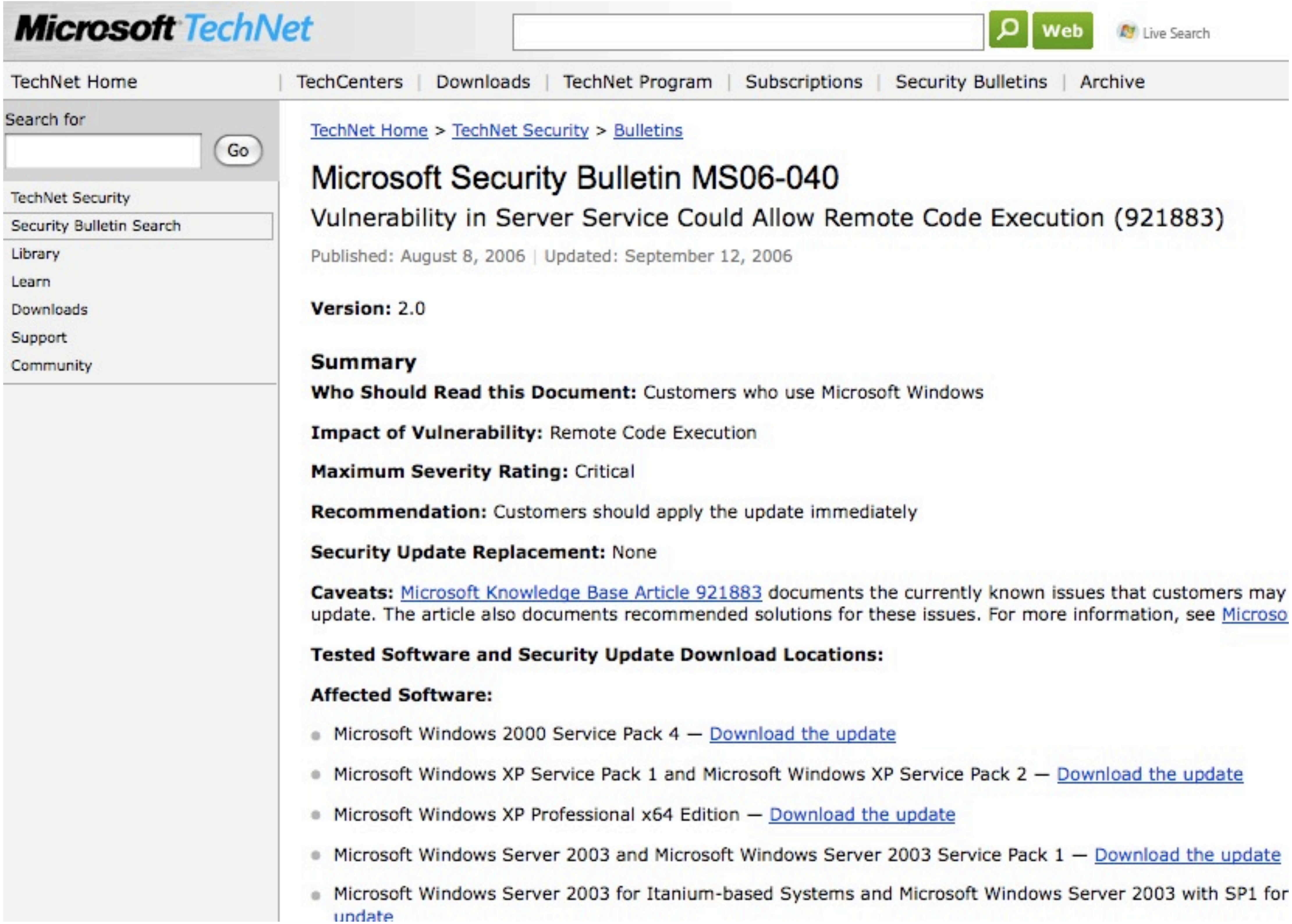
*Also known as Conficker B++



Affected Software

Operating System	Maximum Security Impact	Aggregate Severity Rating	Bulletins Replaced by this Update
Microsoft Windows 2000 Service Pack 4	Remote Code Execution	Critical	MS06-040
Windows XP Service Pack 2	Remote Code Execution	Critical	MS06-040
Windows XP Service Pack 3	Remote Code Execution	Critical	None
Windows XP Professional x64 Edition	Remote Code Execution	Critical	MS06-040
Windows XP Professional x64 Edition Service Pack 2	Remote Code Execution	Critical	None
Windows Server 2003 Service Pack 1	Remote Code Execution	Critical	MS06-040
Windows Server 2003 Service Pack 2	Remote Code Execution	Critical	None
Windows Server 2003 x64 Edition	Remote Code Execution	Critical	MS06-040
Windows Server 2003 x64 Edition Service Pack 2	Remote Code Execution	Critical	None
Windows Server 2003 with SP1 for Itanium-based Systems	Remote Code Execution	Critical	MS06-040
Windows Server 2003 with SP2 for Itanium-based Systems	Remote Code Execution	Critical	None
Windows Vista and Windows Vista Service Pack 1	Remote Code Execution	Important	None
Windows Vista x64 Edition and Windows Vista x64 Edition Service Pack 1	Remote Code Execution	Important	None
Windows Server 2008 for 32-bit Systems*	Remote Code Execution	Important	None
Windows Server 2008 for x64-based Systems*	Remote Code Execution	Important	None
Windows Server 2008 for Itanium-based Systems	Remote Code Execution	Important	None

***Windows Server 2008 server core installation affected.** For supported editions of Windows Server 2008, this update applies, wi



TechNet Home > TechNet Security > Bulletins

Microsoft Security Bulletin MS06-040

Vulnerability in Server Service Could Allow Remote Code Execution (921883)

Published: August 8, 2006 | Updated: September 12, 2006

Version: 2.0

Summary

Who Should Read this Document: Customers who use Microsoft Windows

Impact of Vulnerability: Remote Code Execution

Maximum Severity Rating: Critical

Recommendation: Customers should apply the update immediately

Security Update Replacement: None

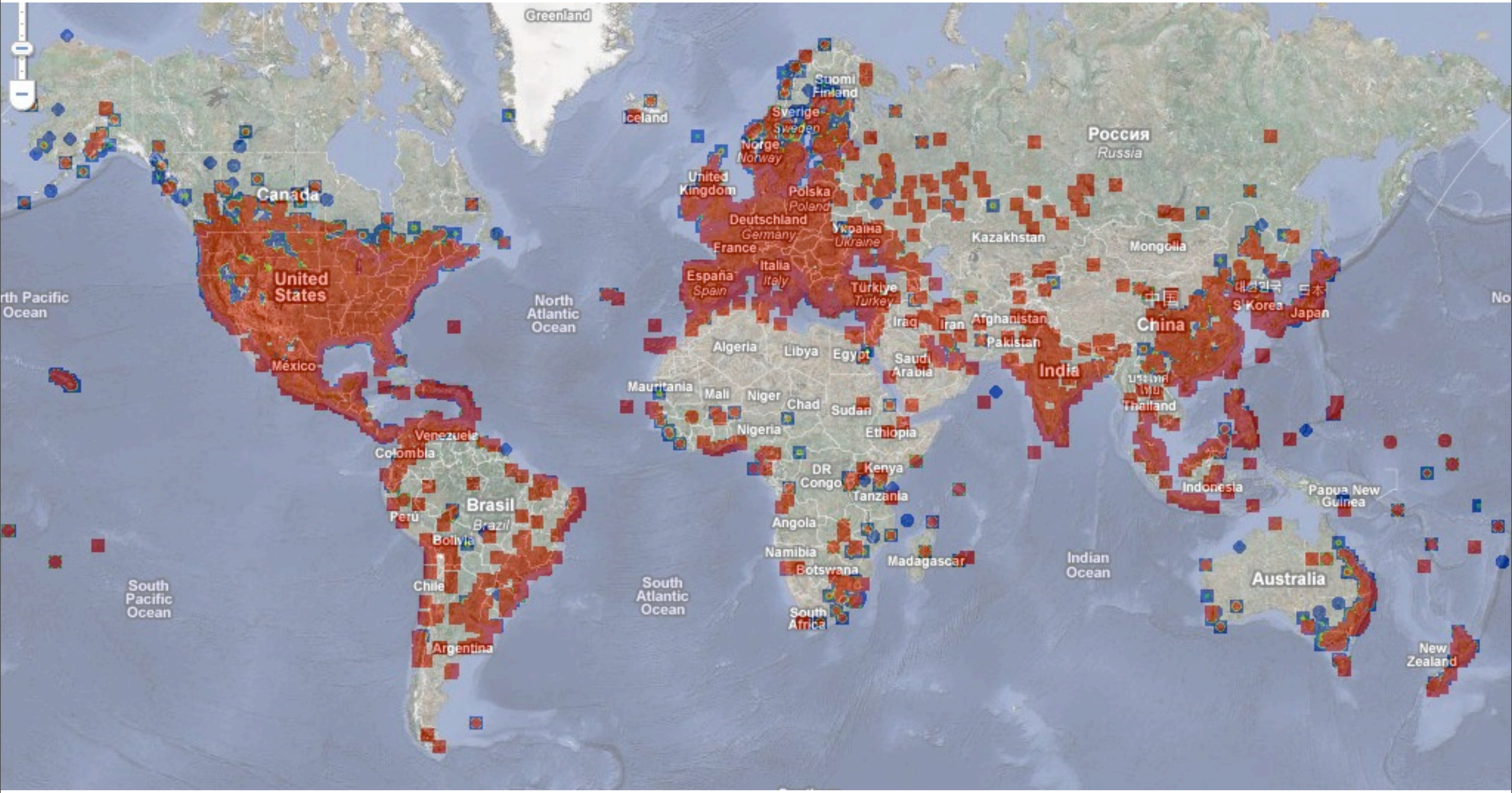
Caveats: Microsoft Knowledge Base Article 921883 documents the currently known issues that customers may update. The article also documents recommended solutions for these issues. For more information, see Microso

Tested Software and Security Update Download Locations:

Affected Software:

- Microsoft Windows 2000 Service Pack 4 — Download the update
- Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2 — Download the update
- Microsoft Windows XP Professional x64 Edition — Download the update
- Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1 — Download the update
- Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows Server 2003 with SP1 for update

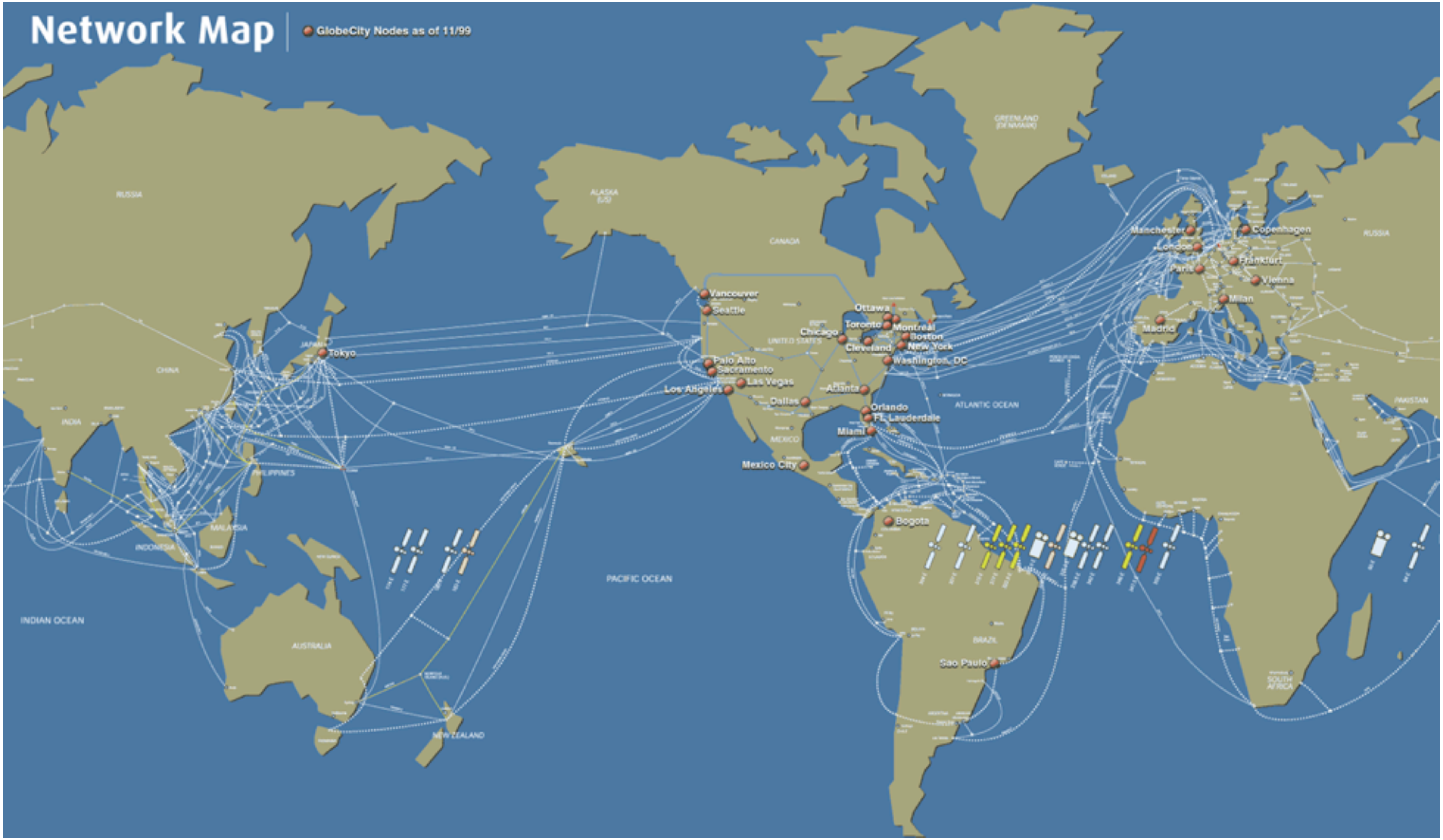
Global Infection Base

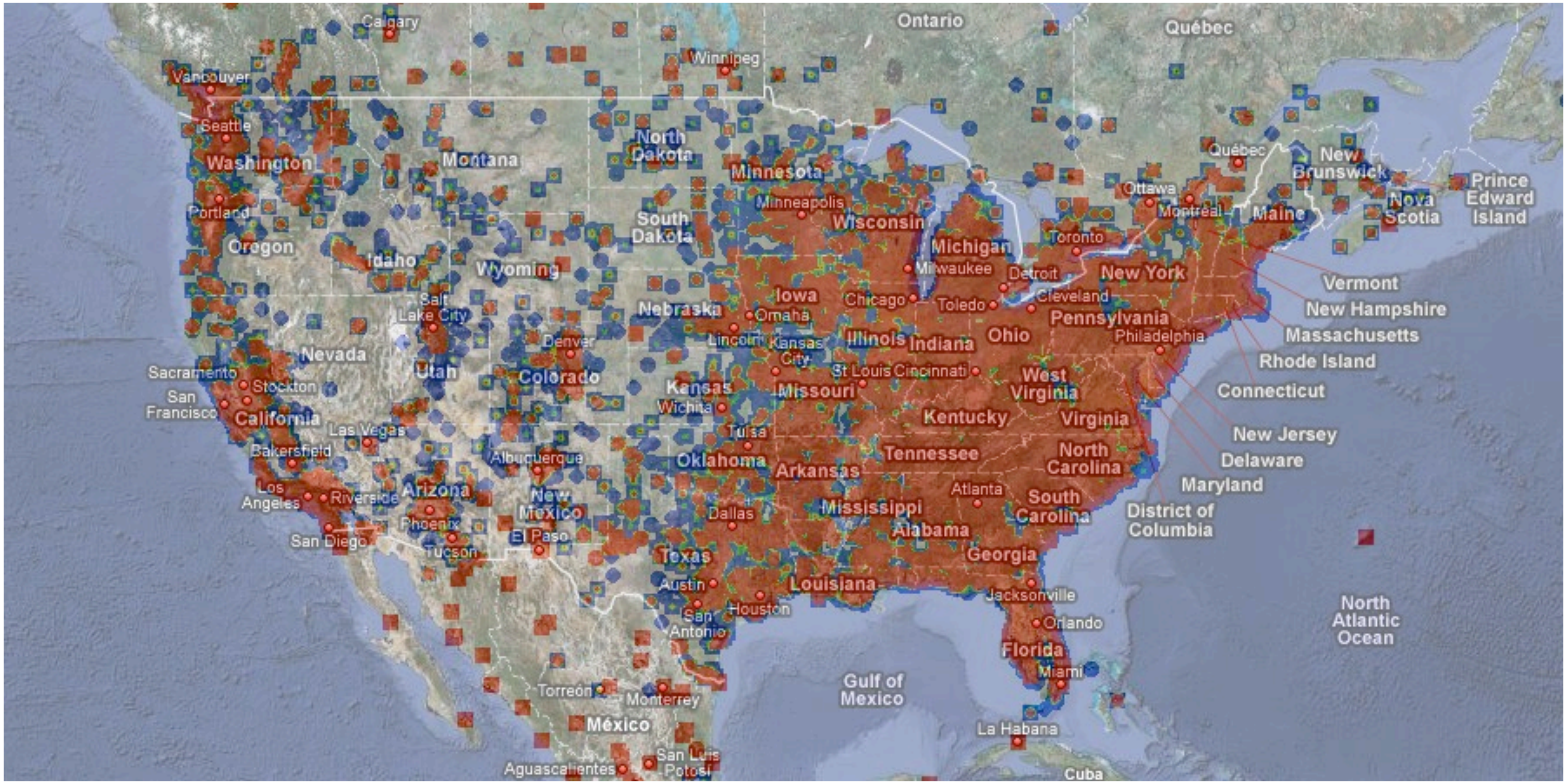


Support Intelligence

SECURITY MONITORING FOR CRITICAL NETWORKS

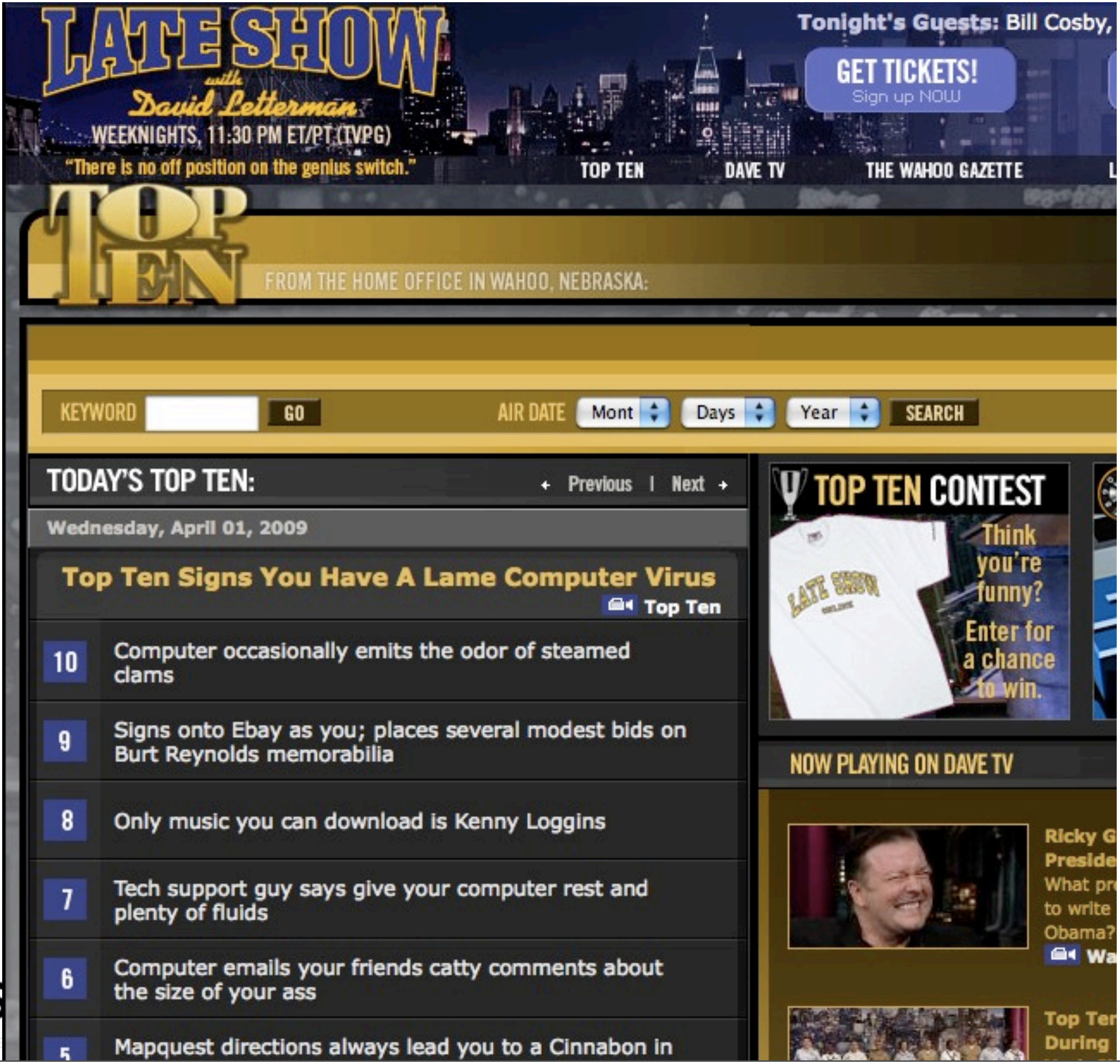
Potential to attack international fiber links





Support Intelligence

SECURITY MONITORING FOR CRITICAL NETWORKS



TODAY'S TOP TEN:

Wednesday, April 01, 2009

Top Ten Signs You Have A Lame Computer Virus

Top Ten

10 Computer occasionally emits the odor of steamed clams

9 Signs onto Ebay as you; places several modest bids on Burt Reynolds memorabilia

8 Only music you can download is Kenny Loggins

7 Tech support guy says give your computer rest and plenty of fluids

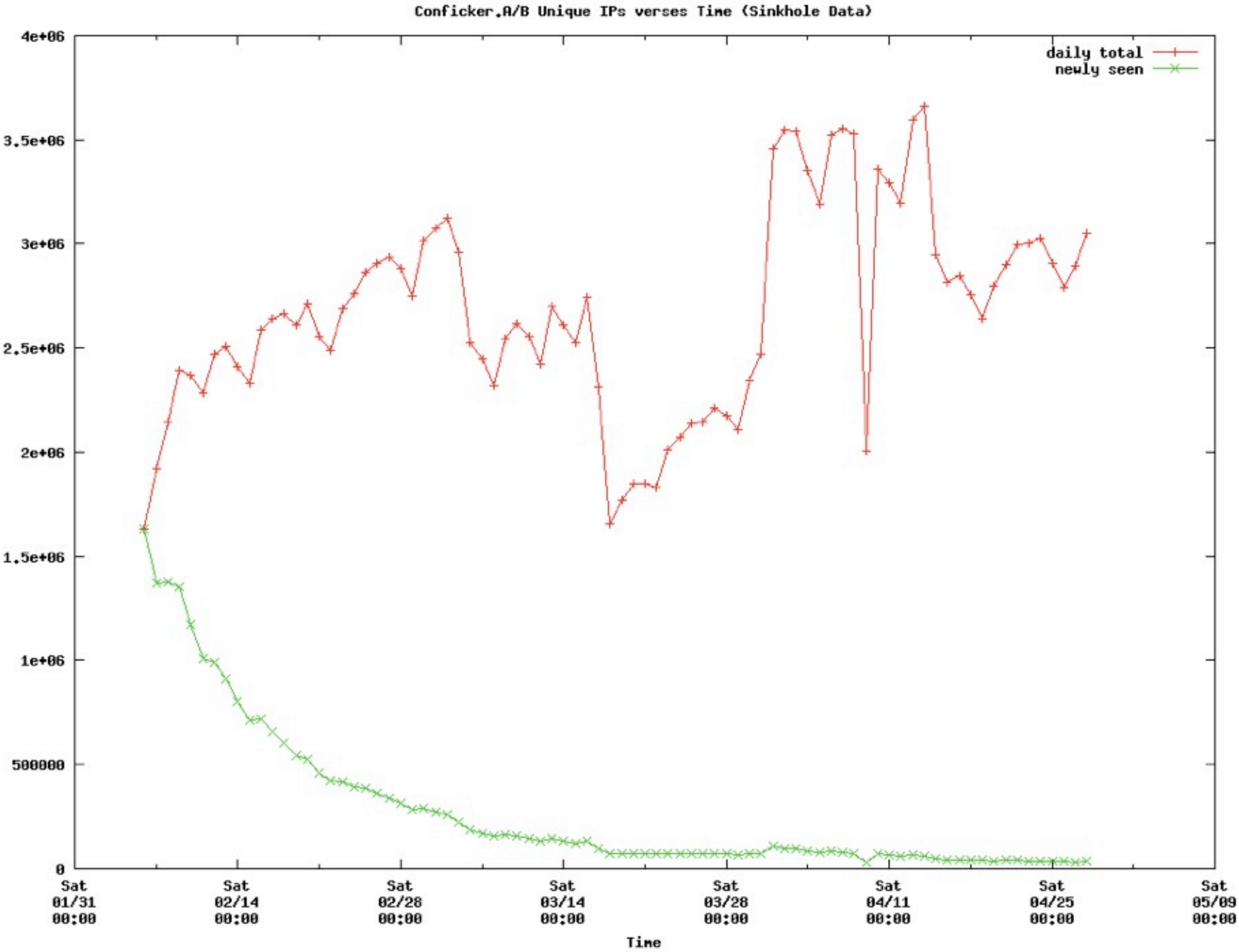
6 Computer emails your friends catty comments about the size of your ass

5 Mapquest directions always lead you to a Cinnabon in

Malware makes the news

Support Intelligence

SECURITY MONITORING FOR CRITICAL NETWORKS

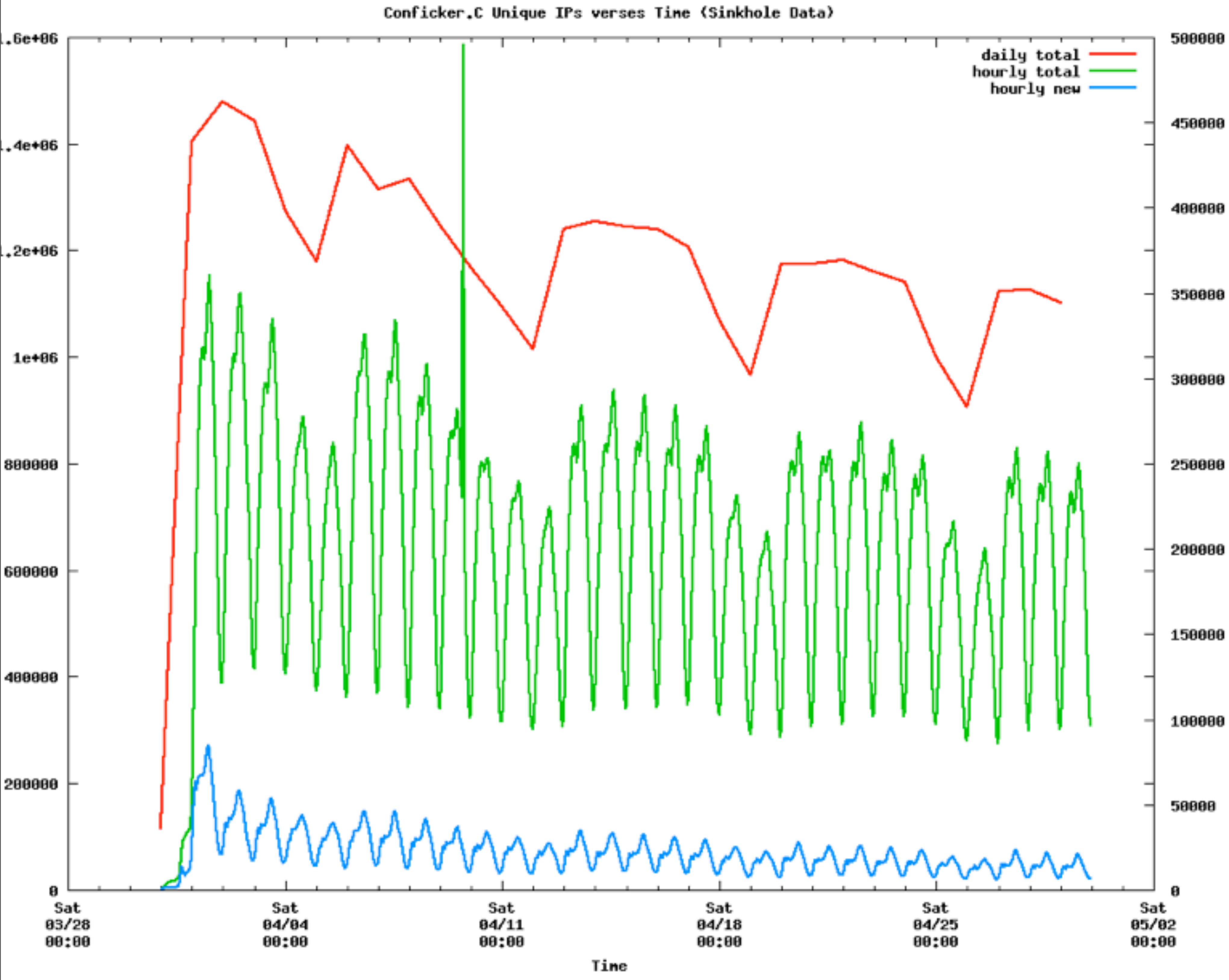


Support Intelligence

SECURITY MONITORING FOR CRITICAL NETWORKS

A+B Variant

Date	Total HTTP Hits	Unique IP's	Unique ASN's	Unique GEO's
2009-05-31	137,760,817	3,721,599	9,141	219
2009-05-30	149,408,605	3,821,993	9,408	218
2009-05-29	187,807,224	4,106,476	10,274	221
2009-05-28	199,562,868	4,065,092	10,331	221
2009-05-27	244,955,856	4,362,696	10,456	220
2009-05-26	271,487,213	4,293,576	10,421	218
2009-05-25	231,494,675	3,989,667	10,174	218
2009-05-24	264,121,645	3,830,624	9,484	215
2009-05-23	92,701,516	2,662,905	9,130	213
2009-05-22	343,097,269	4,151,147	10,377	219



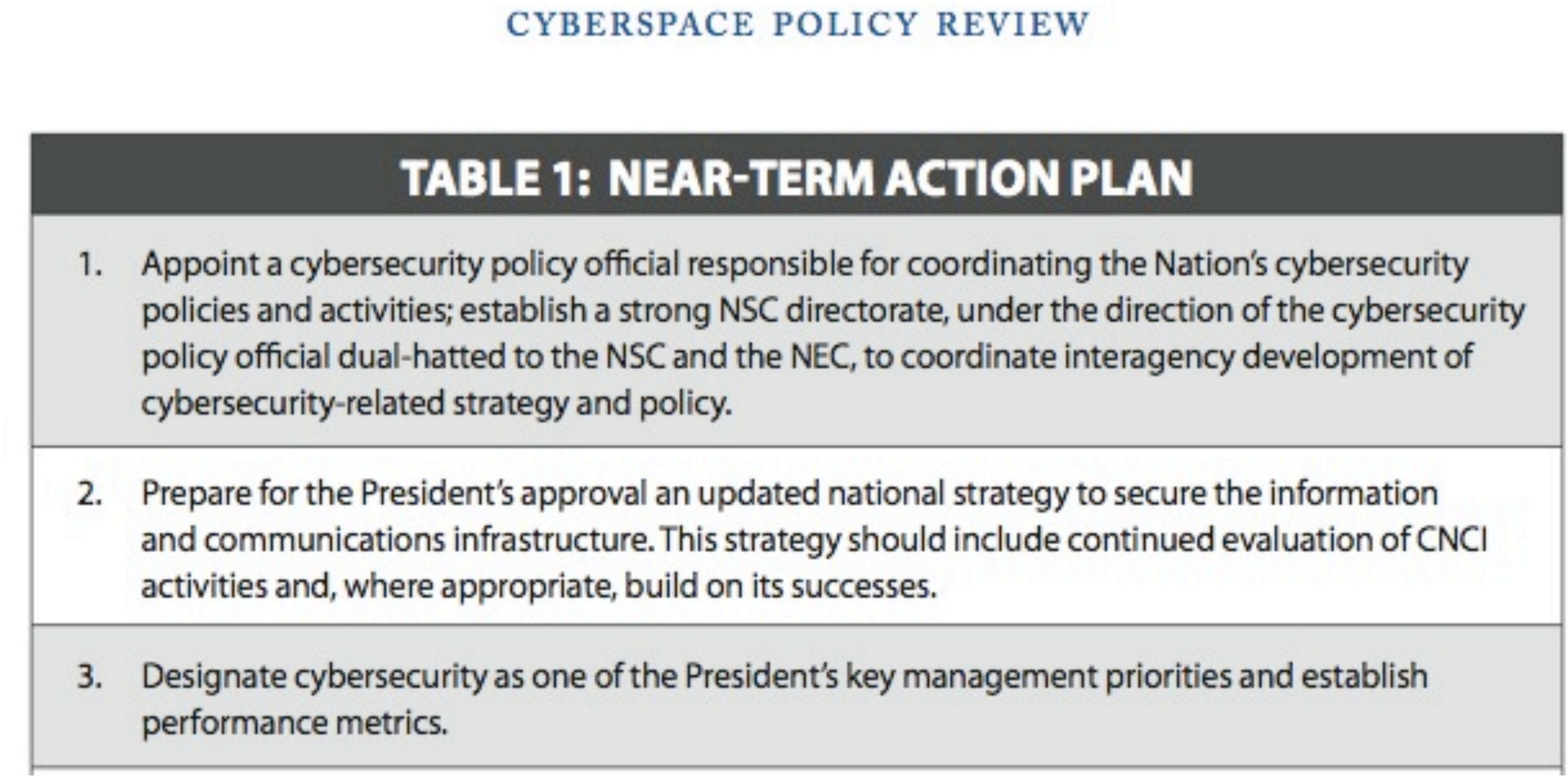
Support Intelligence
SECURITY MONITORING FOR CRITICAL NETWORKS

C Variant (p2p)

Date	Total HTTP Hits	Unique IP's	Unique ASN's	Unique GEO's
2009-05-31	46,251,794	717,049	8,075	202
2009-05-30	48,603,924	762,981	8,209	203
2009-05-29	55,997,707	859,918	8,867	207
2009-05-28	55,334,297	879,569	8,919	208
2009-05-27	65,295,232	917,259	8,950	208
2009-05-26	66,272,183	935,420	8,961	208
2009-05-25	63,242,556	928,934	8,800	207
2009-05-24	44,870,662	739,788	8,080	201
2009-05-23	24,562,643	577,035	7,665	199
2009-05-22	66,496,004	928,830	8,835	207

A/B/C Totals

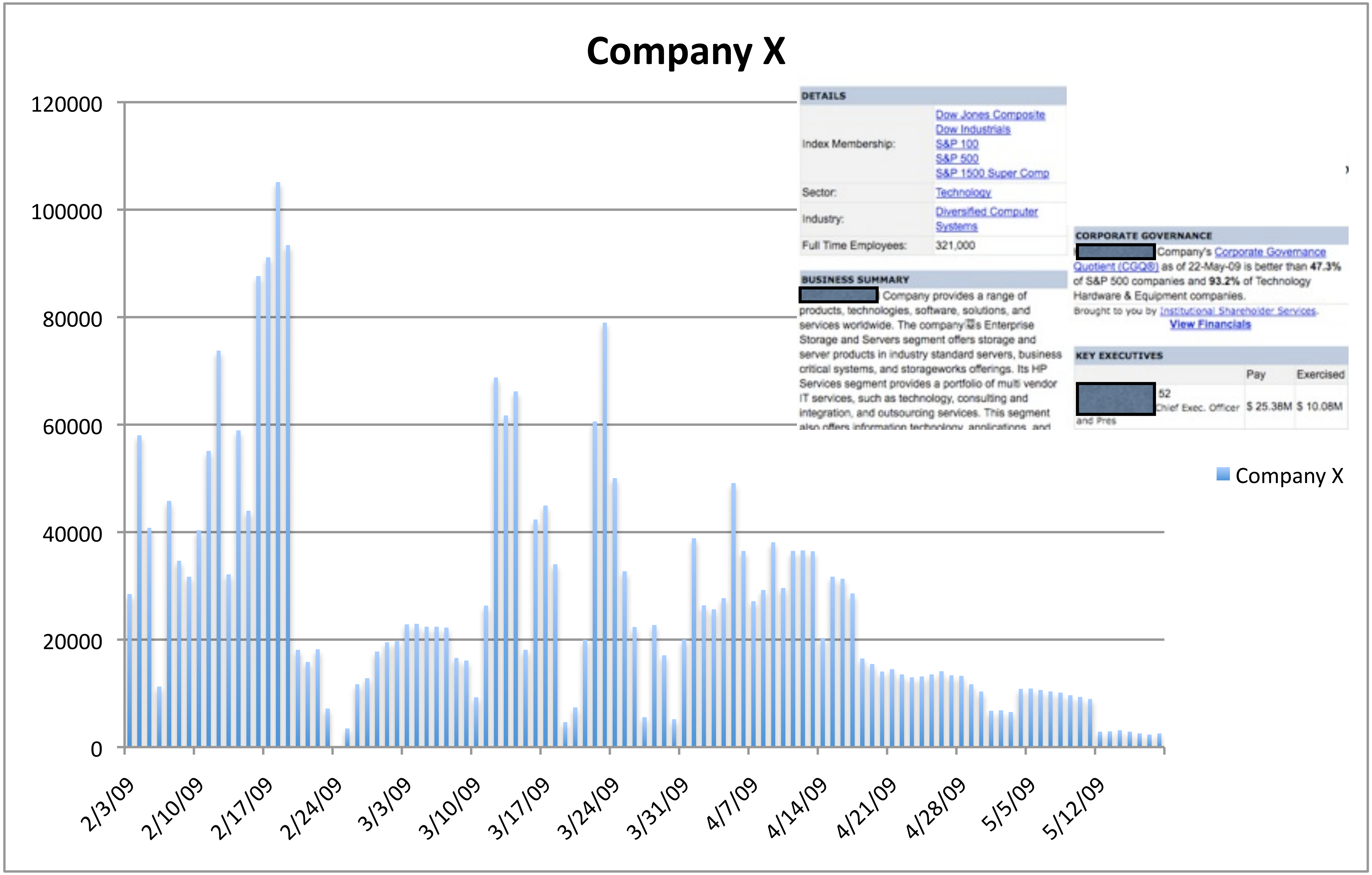
Date	Total HTTP Hits	Unique IP's	Unique ASN's	Unique GEO's
2009-05-31	184,012,611	4,297,992	10,256	219
2009-05-30	198,012,529	4,428,578	10,430	219
2009-05-29	243,804,931	4,768,850	11,216	221
2009-05-28	254,897,165	4,743,616	11,228	222
2009-05-27	313,250,726	5,055,360	11,326	220
2009-05-26	337,759,396	4,999,421	11,337	220
2009-05-25	304,515,914	4,789,953	11,081	219
2009-05-24	308,992,307	4,425,925	10,378	216
2009-05-23	117,264,159	3,121,204	9,992	215
2009-05-22	409,593,273	4,854,546	11,228	220



CYBERSPACE POLICY REVIEW

TABLE 1: NEAR-TERM ACTION PLAN

1. Appoint a cybersecurity policy official responsible for coordinating the Nation's cybersecurity policies and activities; establish a strong NSC directorate, under the direction of the cybersecurity policy official dual-hatted to the NSC and the NEC, to coordinate interagency development of cybersecurity-related strategy and policy.
2. Prepare for the President's approval an updated national strategy to secure the information and communications infrastructure. This strategy should include continued evaluation of CNCI activities and, where appropriate, build on its successes.
3. Designate cybersecurity as one of the President's key management priorities and establish performance metrics.



DETAILS

Index Membership:	Dow Jones Composite Dow Industrials S&P 100 S&P 500 S&P 1500 Super Comp
Sector:	Technology
Industry:	Diversified Computer Systems
Full Time Employees:	321,000

BUSINESS SUMMARY

[redacted] Company provides a range of products, technologies, software, solutions, and services worldwide. The company s Enterprise Storage and Servers segment offers storage and server products in industry standard servers, business critical systems, and storageworks offerings. Its HP Services segment provides a portfolio of multi vendor IT services, such as technology, consulting and integration, and outsourcing services. This segment also offers information technology, applications, and

CORPORATE GOVERNANCE

[redacted] Company's Corporate Governance Quotient (CGQ®) as of 22-May-09 is better than **47.3%** of S&P 500 companies and **93.2%** of Technology Hardware & Equipment companies.

Brought to you by Institutional Shareholder Services.

View Financials

KEY EXECUTIVES

	Pay	Exercised
[redacted] 52 Chief Exec. Officer and Pres	$ 25.38M	$ 10.08M

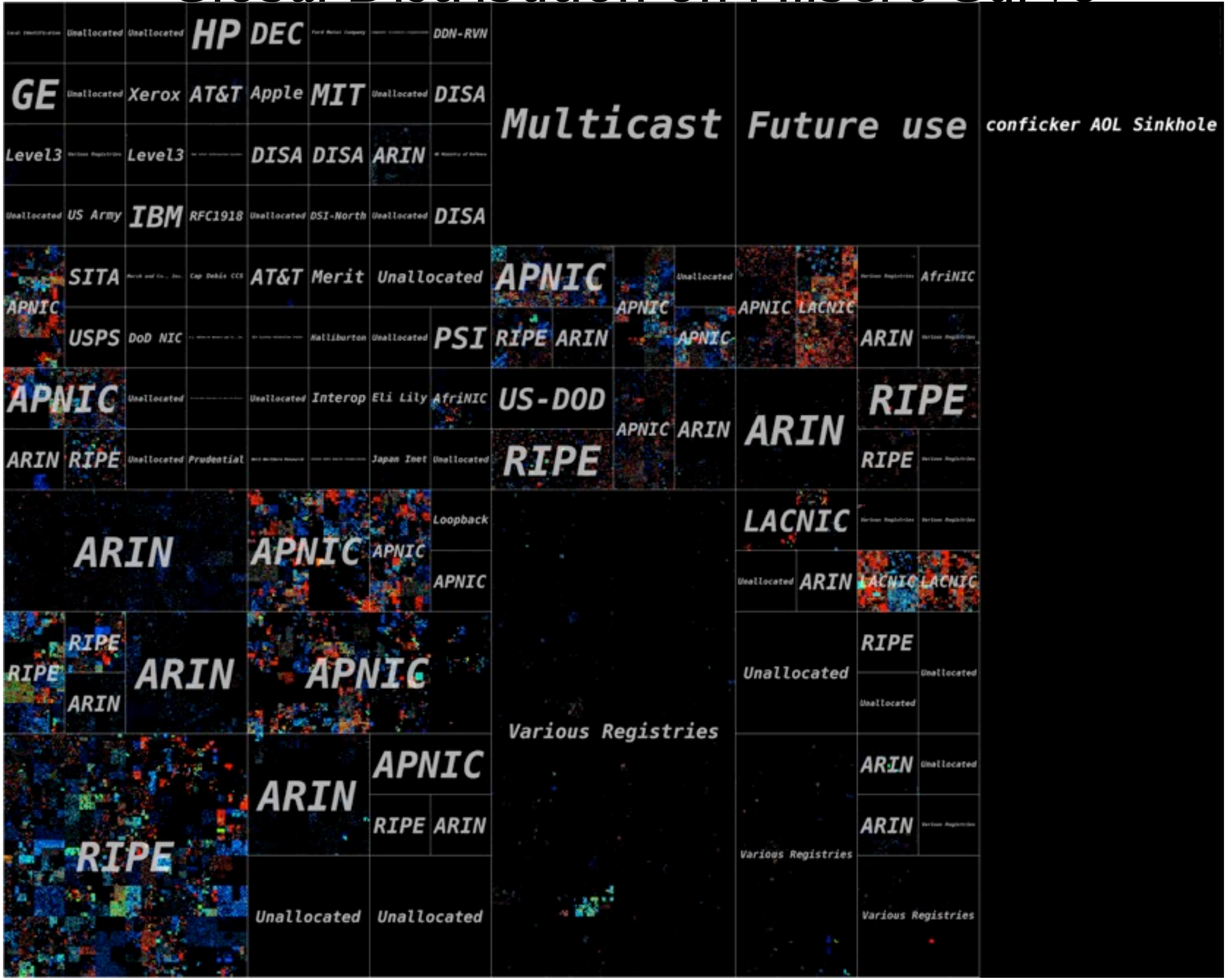
SI Support Intelligence

SECURITY MONITORING FOR CRITICAL NETWORKS

Conficker

- 3 primary variants A/B/C
- Capabilities:
    - impede global commerce or information exchange.
    - challenge stability of state (Estonia, Georgia)
    - dynamically update itself
    -

Global Distribution on Hilbert Curve



Conficker

- ms08-064 vulnerability (RPC buffer over flow)
- uses intelligent scanning/infect
- avoids CERT and Security company address space
- brute forces Administrator accounts
- USB share with social engineered attack

Conficker 2nt Stage

- domain used for rendezvous crypto generated daily
  - A/B 500 domains per day
  - C 50,000 domains per day
- second stage download used PKI to verify binary.
- A: 1024 bit key
- B: 2048 bit key
- current attempted takeovers

Conficker Census

- Conficker A at 3,898,326 infected IPs
- Conficker B at 4,731,225 infected IPs,
- with 726,017 overlapped IPs
- 214 countries

Support Intelligence
SECURITY MONITORING FOR CRITICAL NETWORKS

Variants

- A: com net org biz info
- B: com net org biz info cc cn ws
- 500 domains/day to blacklist
- C: 110 TLDs over 50,000 domains/day

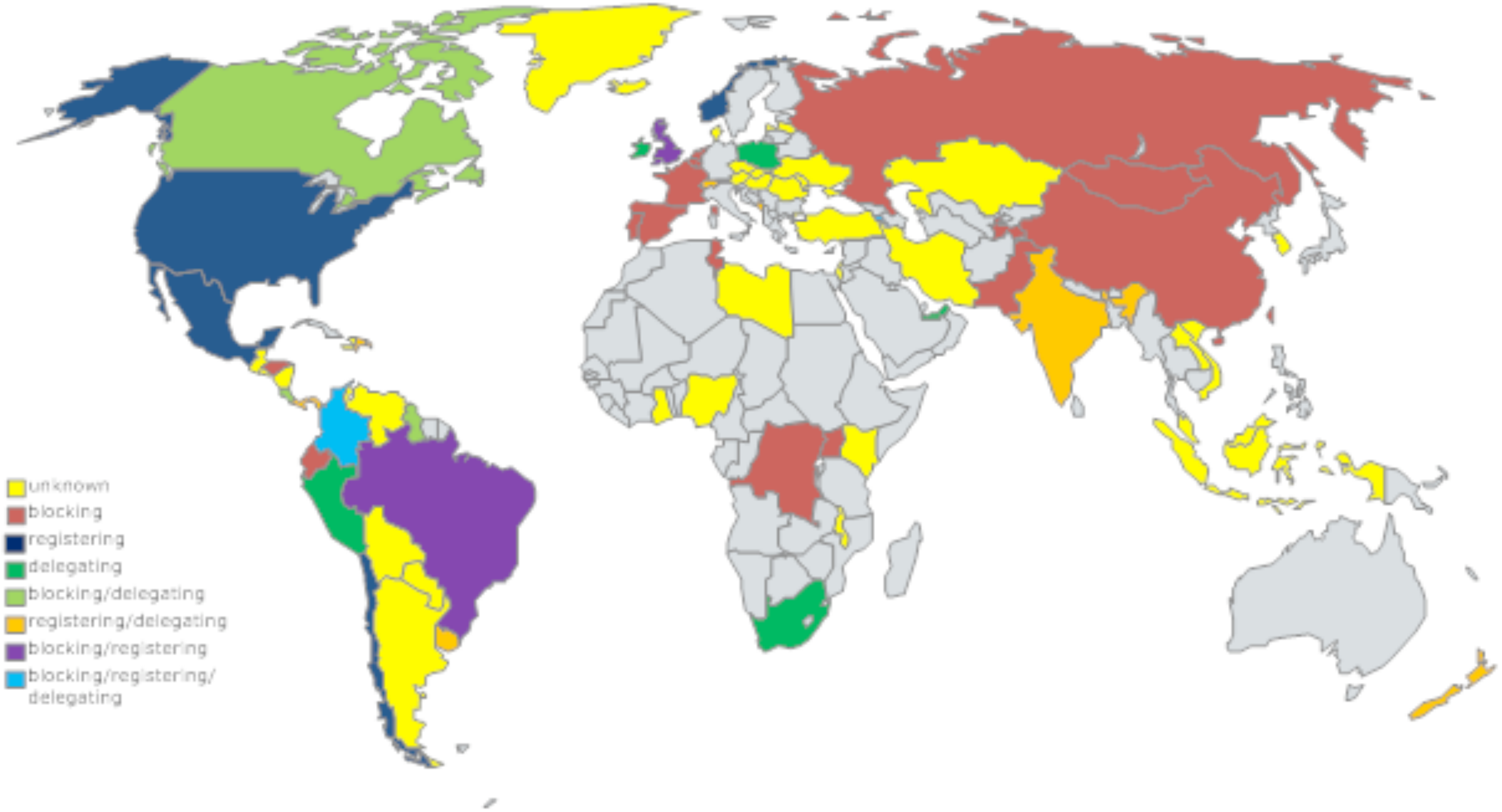
sinkhole reports

- available of you want data share
- currently doing 12 mb/s and growing
- produces 500,000,000 events per day
- 116 Billion data points from Feb ’09

Participants

- ICANN, Verisign, NeuLevel, Afilias, PIR
- Symantec, AOL, ISC, Support Intelligence
- Shadow Server, SRI
- CNNIC, .CA, .IL, .US,

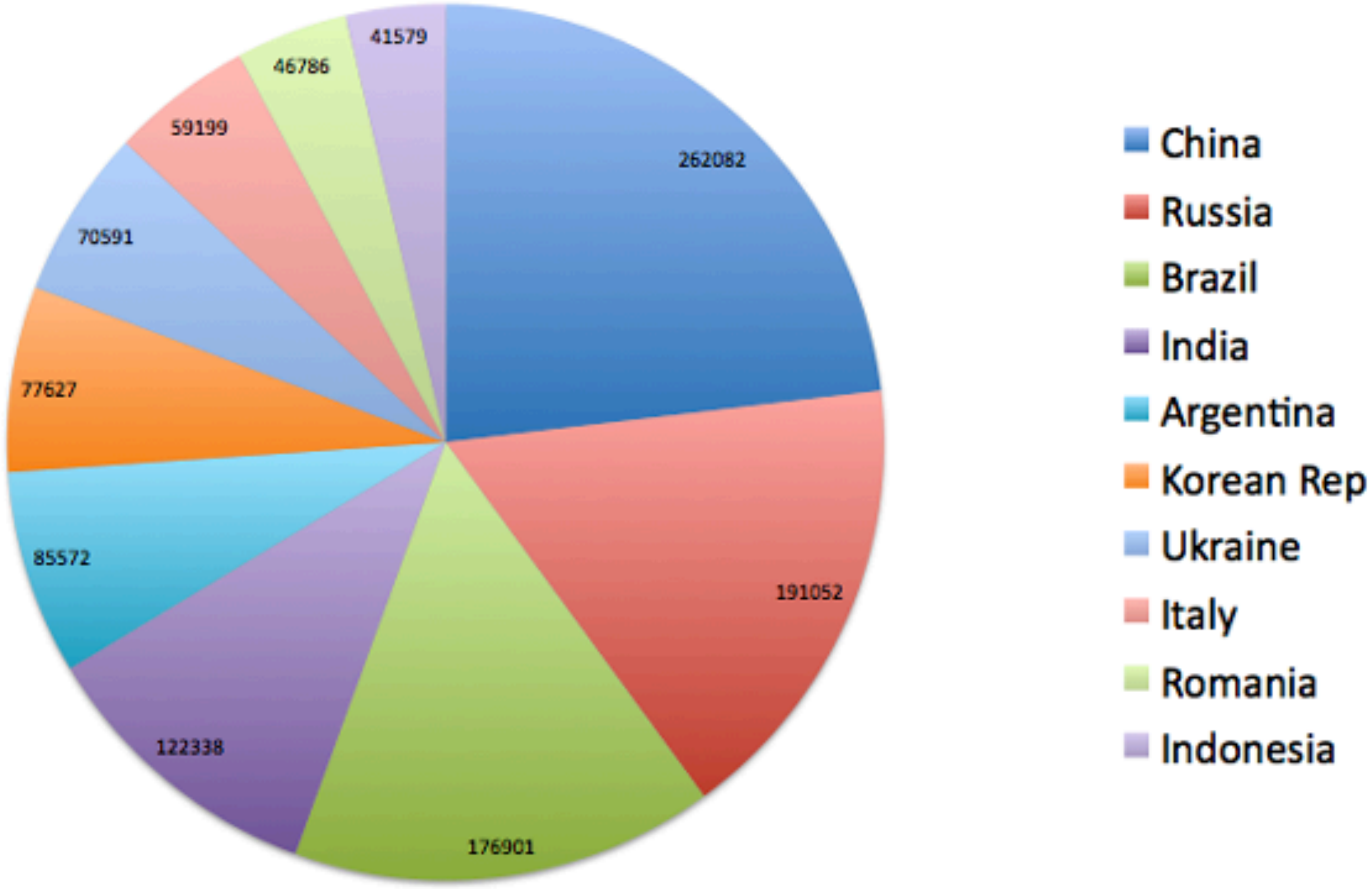
C Variant Targets



Variant C

- 110 country code top level domains
- 500 selected of 50,000 domains per day
- peer to peer file distribution
- direct takeover exploit, botnet could be subverted by 3rd party.

Infection Distribution



Support Intelligence

SECURITY MONITORING FOR CRITICAL NETWORKS

Remediation

- Millions of systems need code updates
- Distributed into hard to reach businesses.
  - Internet Cafe, School computer labs, small business.
  - Laptops, USB sticks infection vectors

Forward

- Significant populations continue to exist
- A/B continue to grow though we continue to contain it.
- We have no remediation strategy beyond Fortune 1000 companies
- The poor and uneducated have no way out.

Conclusion

- Information Security research on global infectons needs encouragement and financial support. The CWG is completely unfunded.
- International cooperation is required
- Conficker is not the last botnet to gain global advantage