Integrating Open Source Information

Rumors & Facts in Early Warning

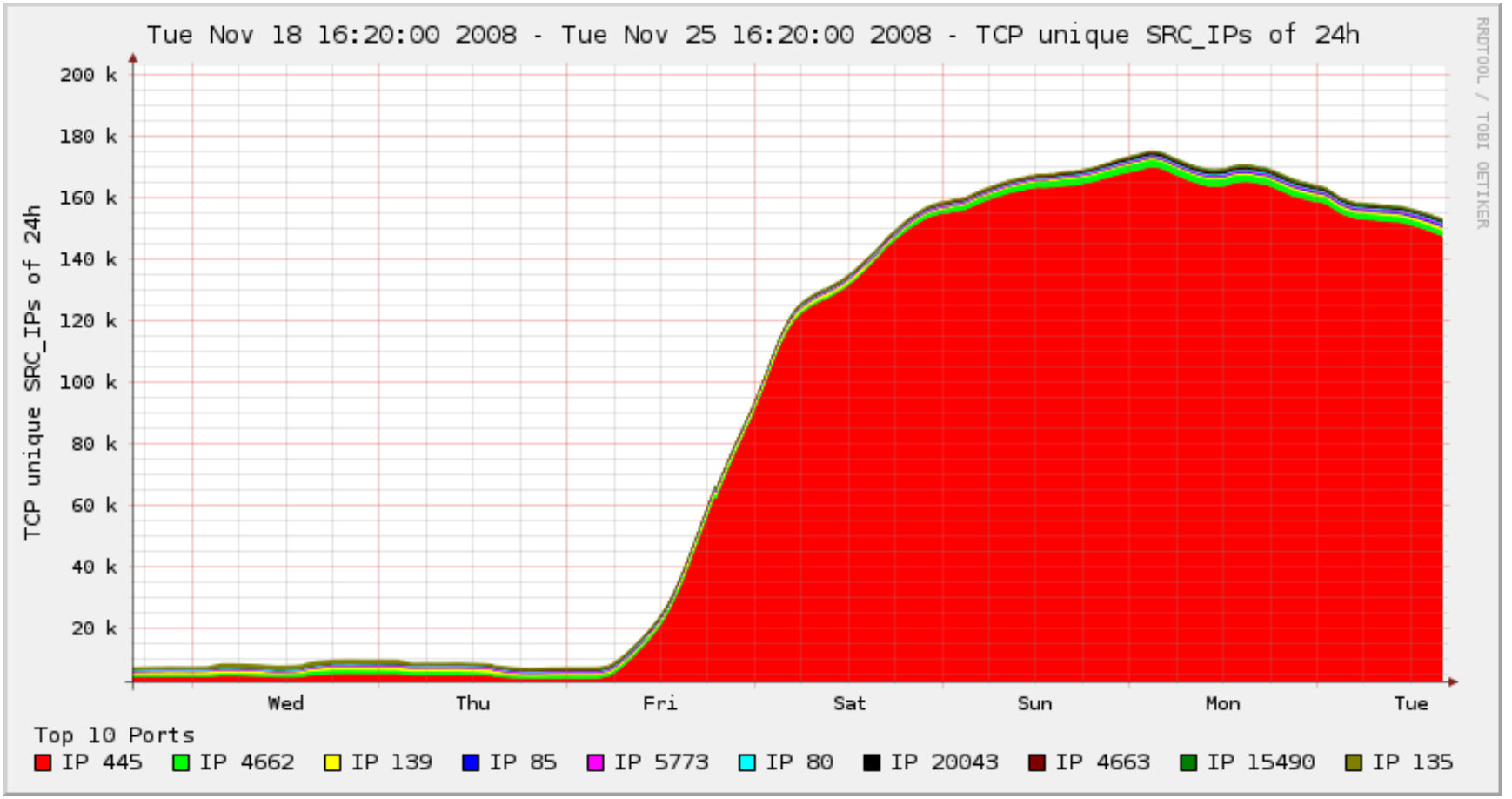
Till Dörges
Jürgen Sander

Table of Contents

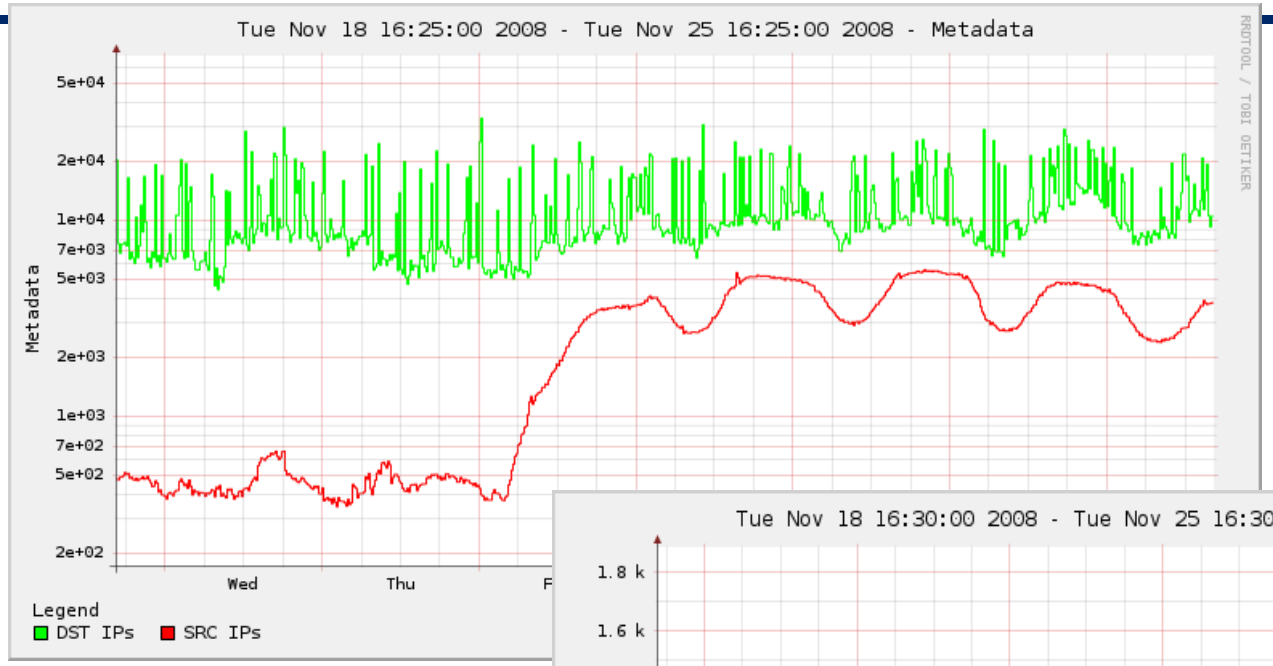
Early Warning – Classical Approach

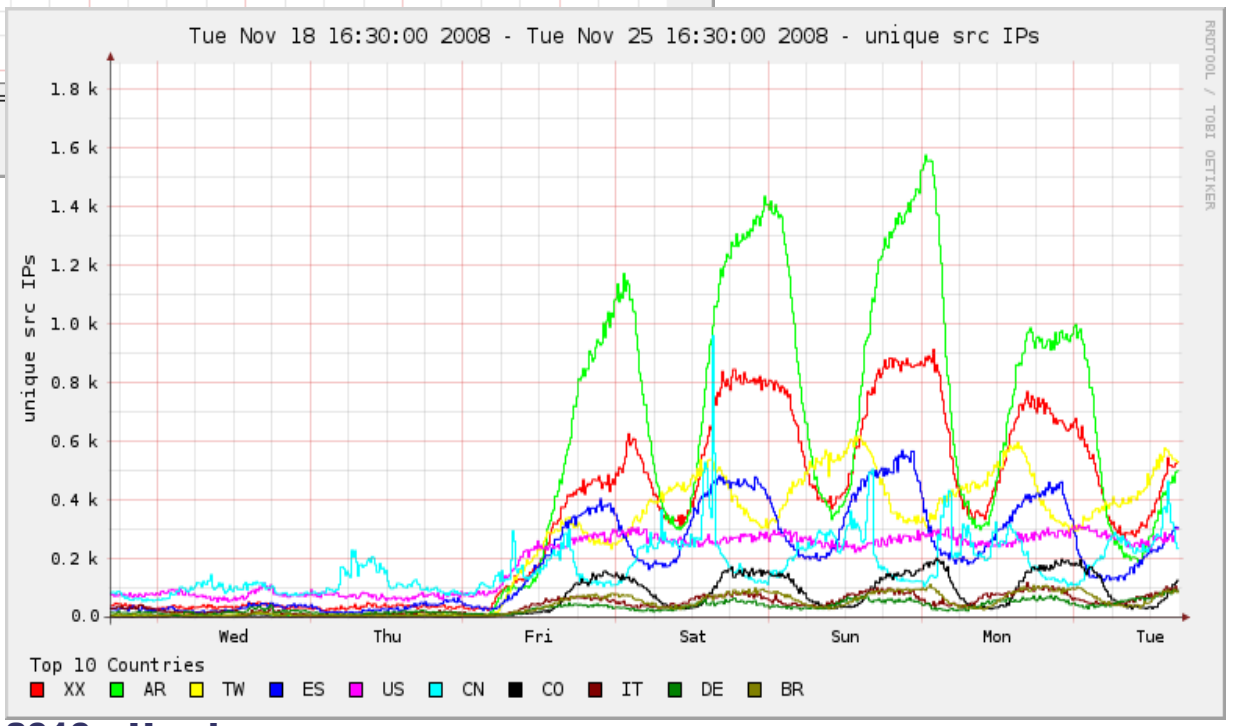
- **Goal**
  - Warn as early as possible
- **Properties**
  - Usually based on sensor data
    - easily collectible
    - sometimes difficult to interpret
  - Often based on incomplete information / facts

Example: Sensor data



Example: Sensor data (cont'd)





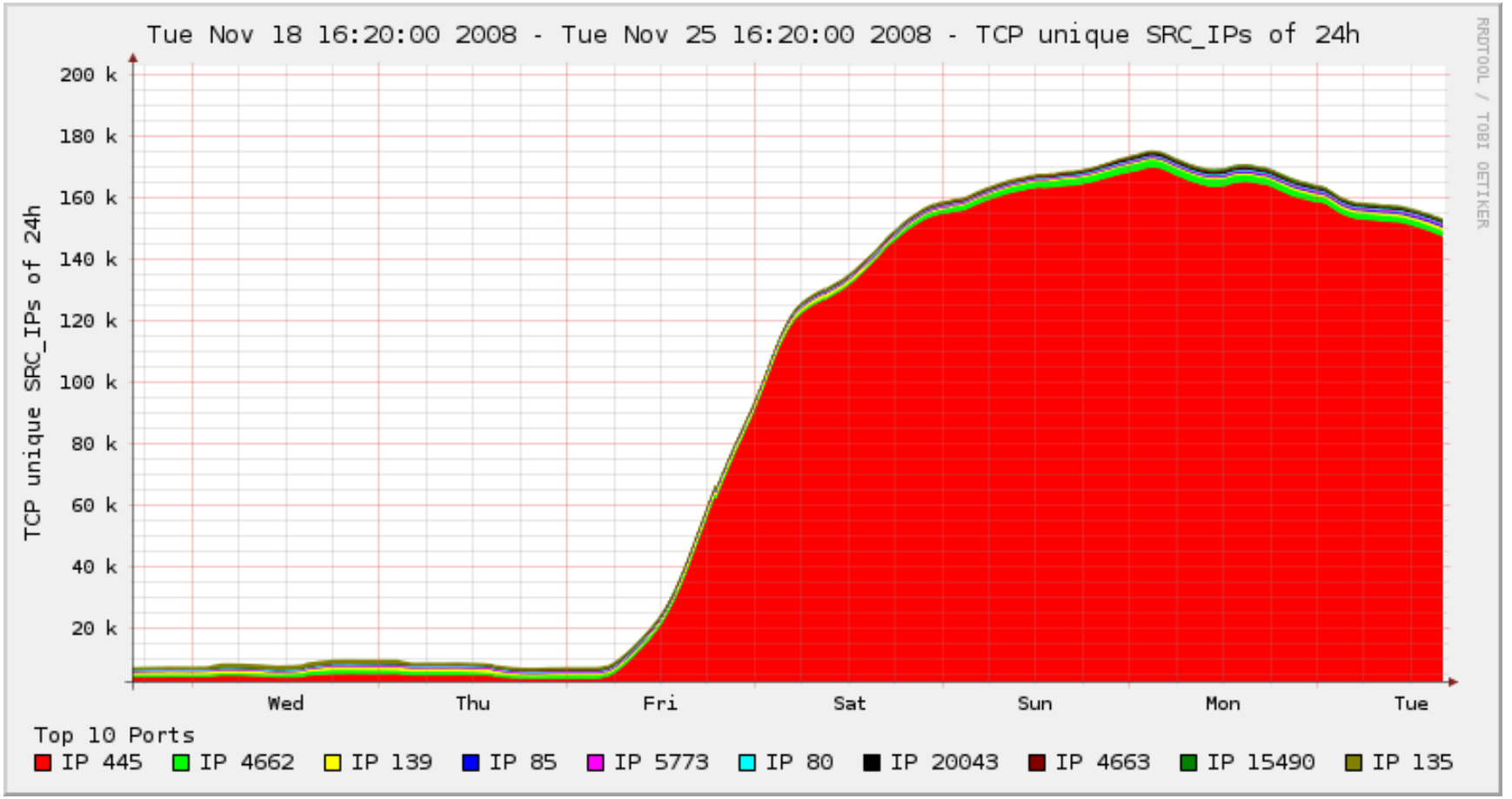
Example: Interpretation

- What caused the peak?

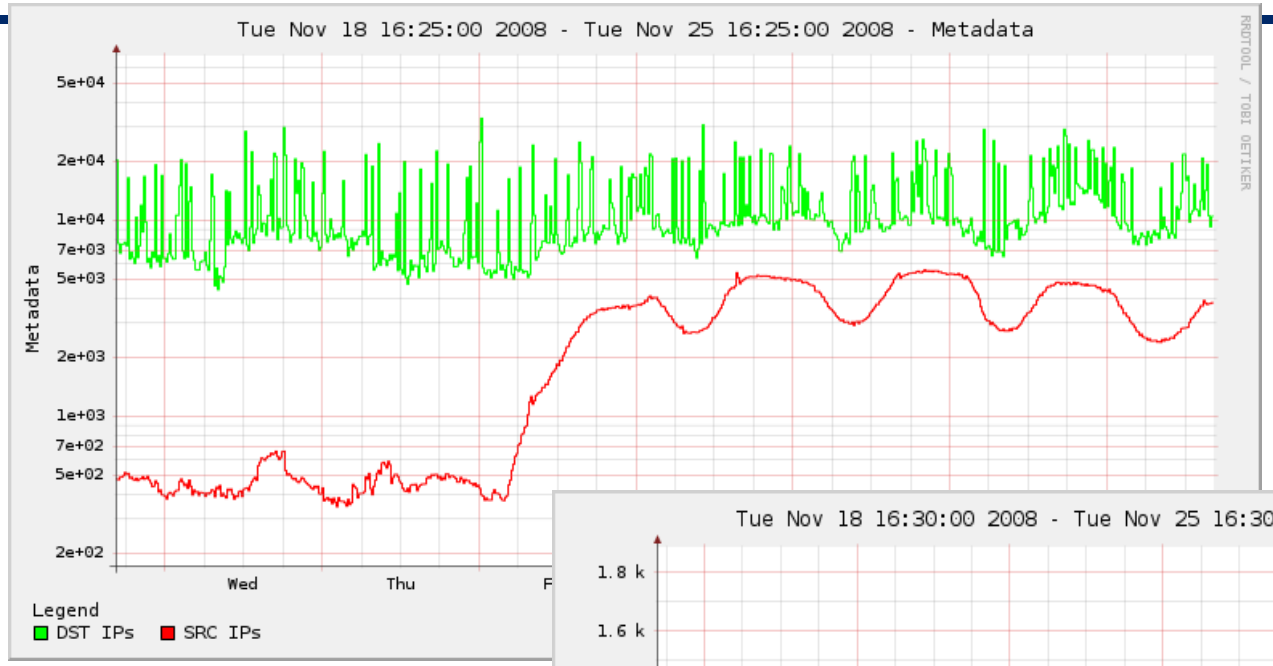
EW – Classical Approach – Revisited

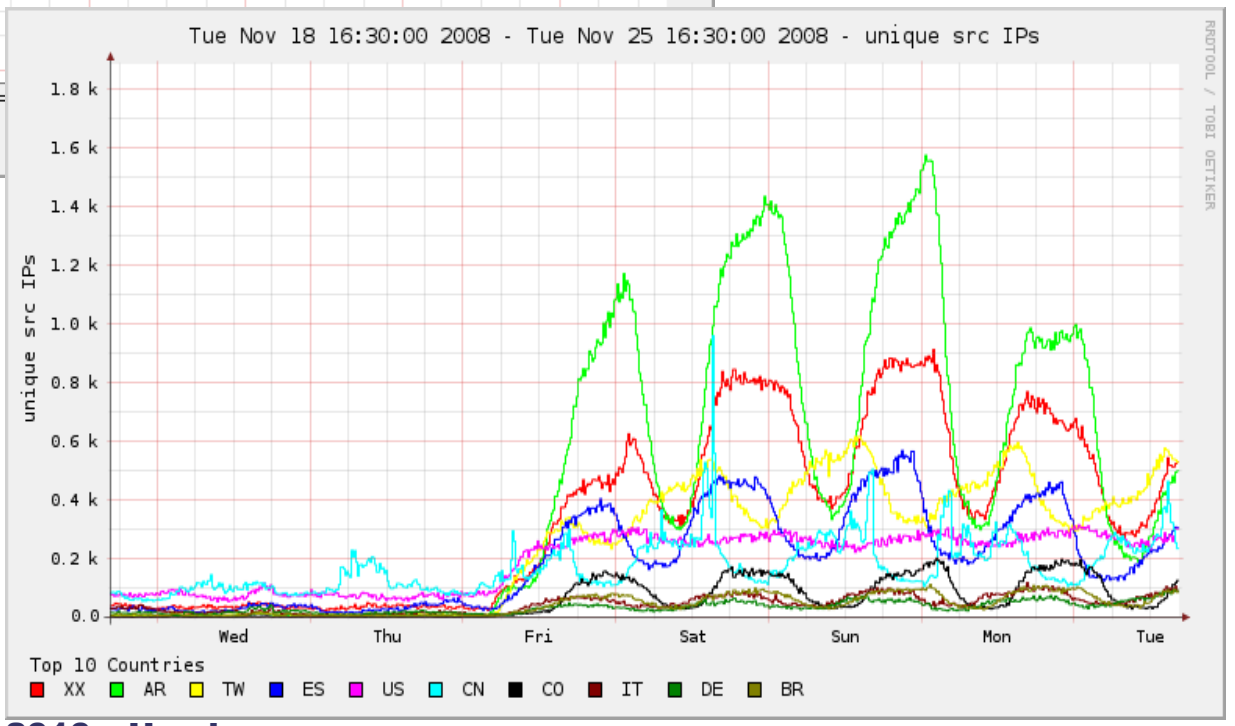
- **Goal**
  - Warn as early as possible
- **Properties**
  - Usually based on sensor data
    - easily collectible
    - sometimes difficult to interpret
  - Often based on incomplete information / facts
- **Missing information / context**
- **How can context be supplied?**
  - Deeper analysis of events
  - Open Source Information

Conficker: Sensor data (I)

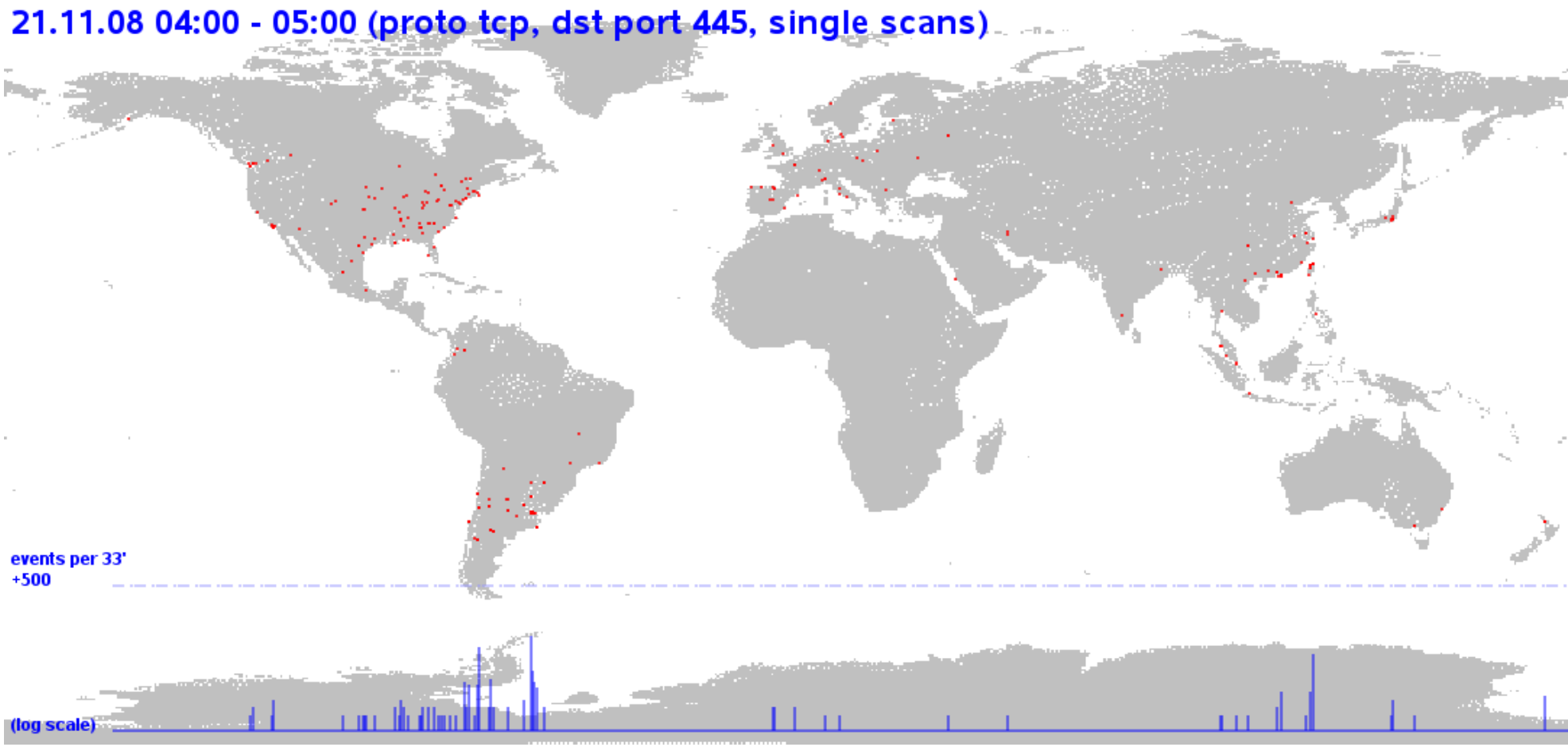


Conficker: Sensor data (II)

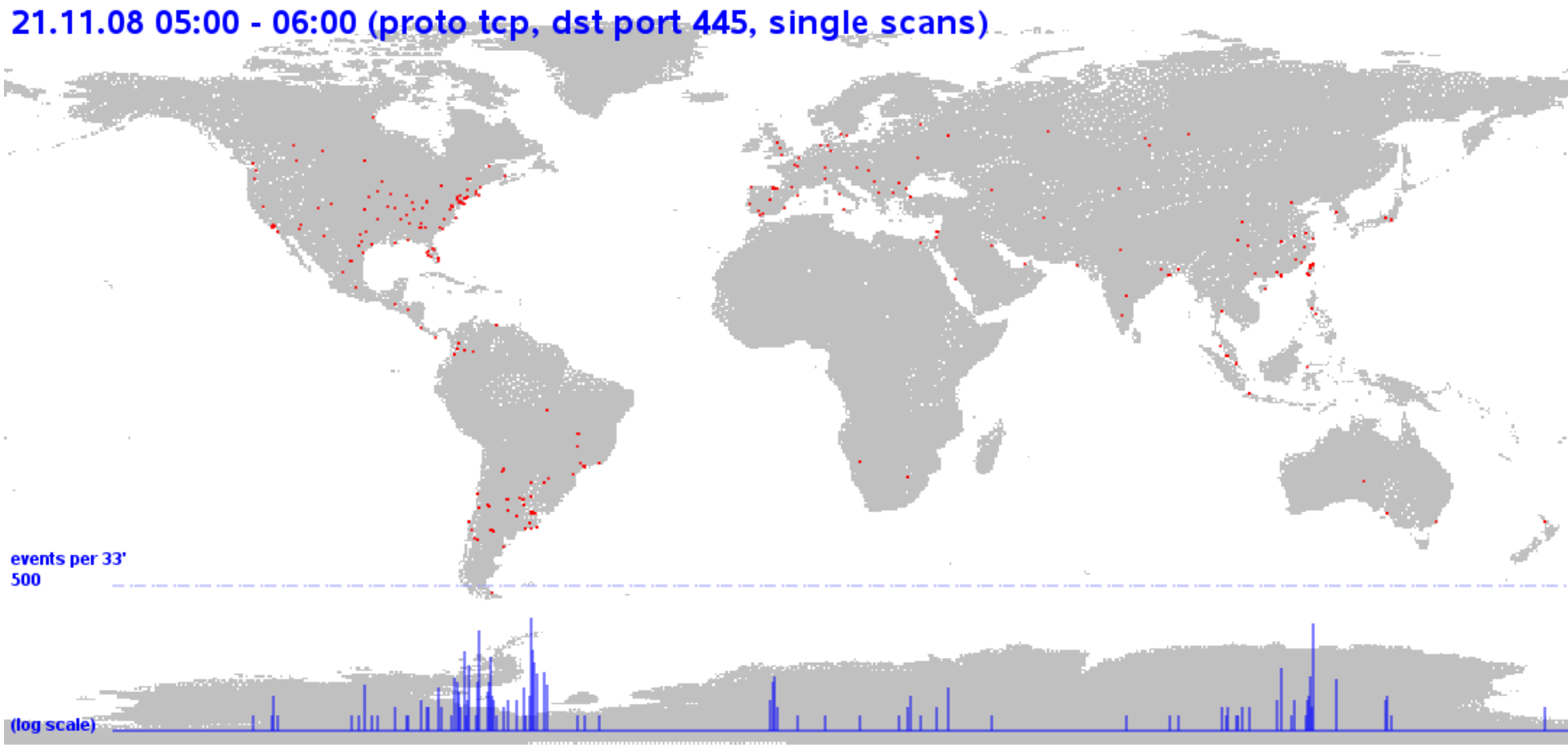




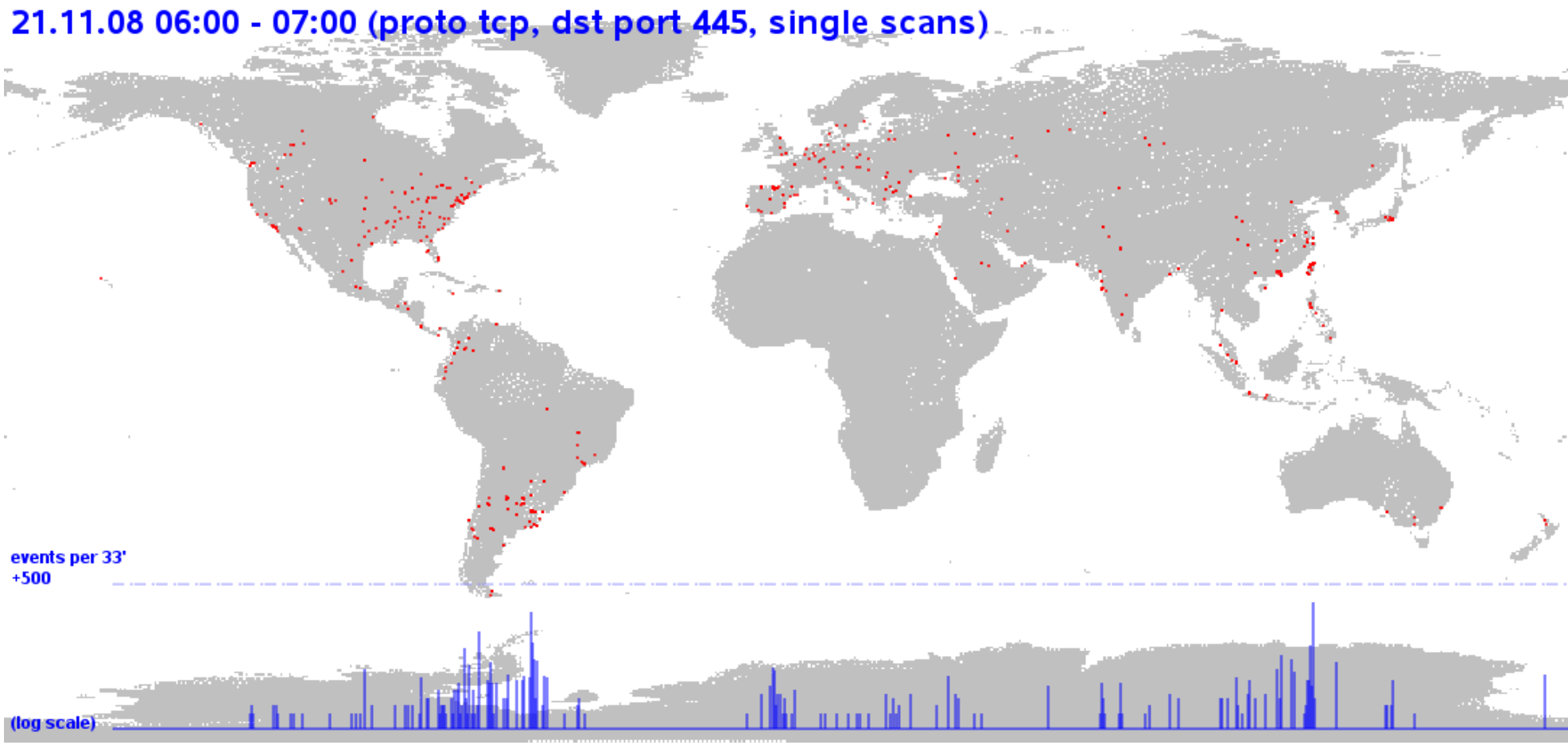
Conficker: Sensor data (III)



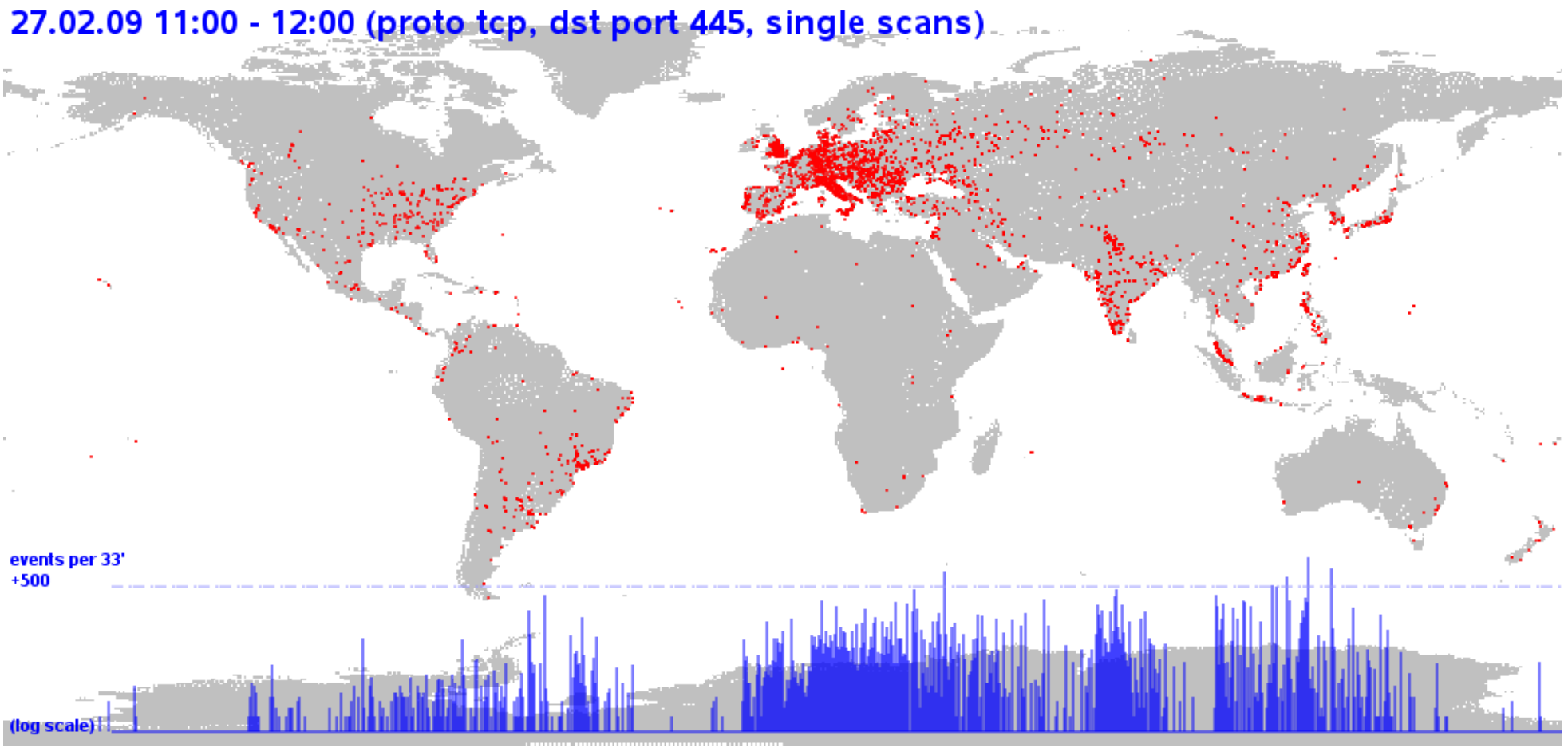
Conficker: Sensor data (III)



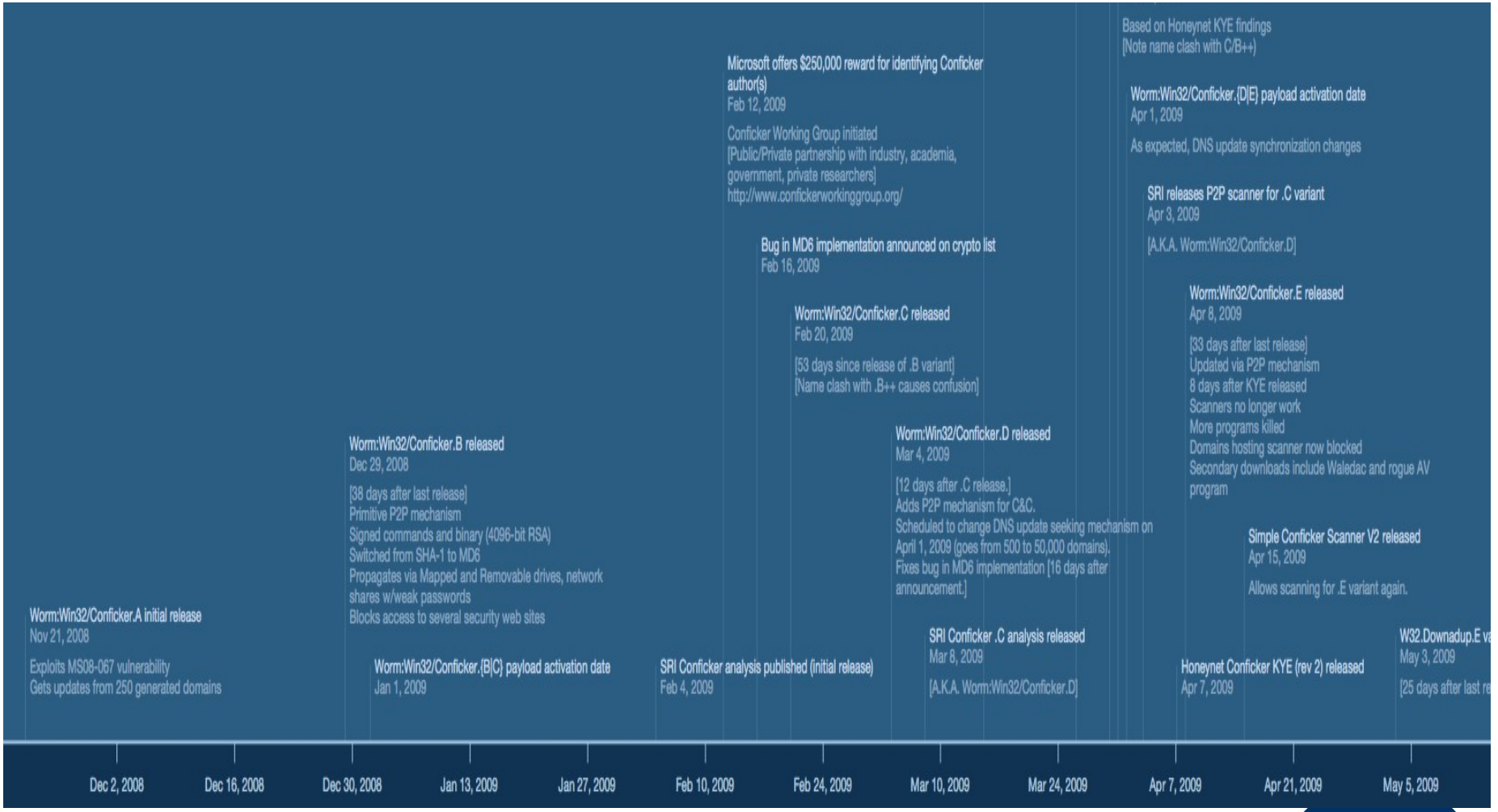
Conficker: Sensor data (III)



Conficker: Sensor data (III)



Conficker: Timeline (after the fact)



Conficker: Deeper Analysis (I)

- Analysis of Argos data

packetdump.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: ip.addr == 190.51.61.86 | Expression... | Leeren | Anwenden

No.	Time	Source	Destination	Protocol	Info
17888	2008-11-26 13:41:19.571749	190.51.61.86	[redacted]	TCP	1691 > 445 [SYN] Seq=0 Len=0 MSS=1440
17889	2008-11-26 13:41:19.572336	[redacted]	190.51.61.86	TCP	445 > 1691 [SYN, ACK] Seq=0 Ack=1 Win=17280 Len=0 MSS=1460
17891	2008-11-26 13:41:19.859890	190.51.61.86	[redacted]	TCP	[illegible] Ack=1 Win=65535 Len=0
17892	2008-11-26 13:41:19.869509	190.51.61.86	[redacted]	SMB	Negotiate Protocol Request
17893	2008-11-26 13:41:19.869934	[redacted]	190.51.61.86	SMB	Negotiate Protocol Response
17894	2008-11-26 13:41:20.195229	190.51.61.86	[redacted]	SMB	Session Setup AndX Request, User: anonymous
17895	2008-11-26 13:41:20.196470	[redacted]	190.51.61.86	SMB	Session Setup AndX Response
17896	2008-11-26 13:41:20.489190	190.51.61.86	[redacted]	TCP	[illegible] Ack=226 Win=65310 Len=0
17897	2008-11-26 13:41:20.489699	[redacted]	190.51.61.86	TCP	445 > 1691 [FIN, ACK] Seq=226 Ack=130 Win=17152 Len=0
17898	2008-11-26 13:41:20.495300	190.51.61.86	[redacted]	TCP	1706 > 445 [SYN] Seq=0 Len=0 MSS=1440
17899	2008-11-26 13:41:20.495809	[redacted]	190.51.61.86	TCP	445 > 1706 [SYN, ACK] Seq=0 Ack=1 Win=17280 Len=0 MSS=1460
17900	2008-11-26 13:41:20.851944	190.51.61.86	[redacted]	TCP	1691 > 445 [ACK] Seq=130 Ack=227 Win=65310 Len=0
17901	2008-11-26 13:41:20.870307	190.51.61.86	[redacted]	TCP	[illegible] Seq=1 Ack=1 [illegible] Len=0
17902	2008-11-26 13:41:20.886177	190.51.61.86	[redacted]	SMB	Negotiate Protocol Request
17903	2008-11-26 13:41:20.888798	[redacted]	190.51.61.86	SMB	Negotiate Protocol Response
17904	2008-11-26 13:41:21.276643	190.51.61.86	[redacted]	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
17905	2008-11-26 13:41:21.278385	[redacted]	190.51.61.86	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MOR
17906	2008-11-26 13:41:21.679293	190.51.61.86	[redacted]	SMB	Session Setup AndX Request, NTLMSSP_AUTH, User: \
17907	2008-11-26 13:41:21.683171	[redacted]	190.51.61.86	SMB	Session Setup AndX Response
17909	2008-11-26 13:41:22.274448	190.51.61.86	[redacted]	SMB	Tree Connect AndX Request, Path: \\[redacted]IPC$
17910	2008-11-26 13:41:22.275369	[redacted]	190.51.61.86	SMB	Tree Connect AndX Response
17911	2008-11-26 13:41:23.154651	190.51.61.86	[redacted]	SMB	NT Create AndX Request, FID: 0x4000, Path: \srvsvc

```
    Error Code: No Error
  ▷ Flags: 0x00
  ▷ Flags2: 0x0000
    Process ID High: 0
    Signature: 0000000000000000
    Reserved: 0000
    Tree ID: 0
    Process ID: 604
    User ID: 0
```

```
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0050  00 00 00 00 5c 02 00 00  00 00 00 0c 00 02 4e 54   ....\... ......NT
0060  20 4c 4d 20 30 2e 31 32  00                         LM 0.12 .
```

Process ID (smb.pid), 2 bytes | P: 19395 D: 83 M: 0

Conficker: OSINF (I)

CVE LIST | COMPATIBLE PRODUCTS | NEWS – JANUARY 15, 2010

Celebrating 10 Years

HOME > CVE > CVE-2008-4250 (UNDER REVIEW)

About CVE
Terminology
Documents
FAQs
CVE List
About CVE Identifiers
Obtain a CVE Identifier
Search CVE
Search NVD
CVE In Use
CVE Adoption
CVE-Compatible Products
NVD for CVE Fix Information
More . . .
News & Events
Calendar
Free Newsletter
Community
CVE Editorial Board
Sponsor
Contact Us
Search the Site

CVE-ID

CVE-2008-4250
(under review)

Learn more at National Vulnerability Database (NVD)
• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 200
allows remote attackers to execute arbitrary code via a crafted RPC request that triggers the overflow during path canonicalizat
wild by Gimmiv.A in October 2008. aka "Server Service Vulnerability."

References

Note: References are provided for t … tended to be com

- BUGTRAQ:20081026 Windows RP
- URL:http://www.securityfocus.c
- BUGTRAQ:20081027 Windows RP
- URL:http://www.securityfocus.c
- MILW0RM:6824
- URL:http://www.milw0rm.com/e
- MILW0RM:6841
- URL:http://www.milw0rm.com/e
- MILW0RM:7104
- URL:http://www.milw0rm.com/e
- MILW0RM:7132
- URL:http://www.milw0rm.com/e
- MISC:http://blogs.securiteam.c
- URL:http://xforce.iss.net/xforce/xfdb/46040

Status

Candidate — This CVE Identifier has "Can… updated to official "Entry" st…

Phase

Assigned (20080925)

Votes

Comments

Conficker: OSINF (II)

Microsoft TechNet

Search Microsoft.com bing Web

TechNet Home | TechCenters | Downloads | TechNet Program | Subscriptions | Security Bulletins | Archive

Search for Go

TechNet Security
Security Bulletin Search
Library
Learn
Downloads
Support
Community

TechNet Home > TechNet Security > Bulletins

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
request. On Microsoft Windows 2000, Windows XP, and Windows Server 2003 systems, an attacker could exp
this vulnerability could be used in the crafting of a wormable exploit. Firewall best practices and standard def
originate outside the enterprise perimeter.

This security update is rated Critical for all supported editions of Microsoft Windows 2000, Windows XP, Wind
and Windows Server 2008. For more information, see the subsection, **Affected and Non-Affected Software**

The security update addresses the vulnerability by correcting the way that the Server service handles RPC re
Questions (FAQ) subsection for the specific vulnerability entry under the next section, **Vulnerability Inform**

Recommendation. Microsoft recommends that customers apply the update immediately.

Known Issues. None

Top of section

Affected and Non-Affected Software

The following software have been tested to determine which versions or editions are affected. Other versions
the support life cycle for your software version or edition, visit Microsoft Support Lifecycle.

Affected Software

Operating System	Maximum Security Impact	Aggregat
Microsoft Windows 2000 Service Pack 4	Remote Code Execution	Critical

Conficker: OSINF (0) ???

- Hints even before reservation of CVE no.?

Table of Contents

Definitions

- **Information**
  - Anything relevant to your goals / tasks
- **Data**
  - Measurements
  - Machine recordable/processable information
- **Sensor data**
  - Data measured/recorded by sensor(s) (e.g. NetFlow or IDS)
- **Early Warning (System)**
  - (System to) Warn people not affected, yet

Definitions (cont'd)

- **Open Source Information**
  - Everything that's publicly available (news, ...)
  - Explicitly comprises rumors
- **Open Source Intelligence**
  - Collection of openly available information
  - Analysis of information → intelligence (i.e. “understanding”)
- **Context**
  - Information necessary to fully understand sensor data

Table of Contents

Open Source Information

- **OSINF: Helps interpret sensor data**
  - “Something going on with product A“
  - ➔ Pay specific attention to sensor data related product A
- **Sensor data: Helps to look for/judge OSINF**
  - Unexplained sensor data possibly related to product A
  - ➔ Look for OS information related to product A

Open Source Inf.: Different Sources

- **Simply use a search engine?**
  - Not sufficient
- **Mailinglists**
- **RSS / Atom**
- **Online Forums**
- **Chat / IRC**
- **News sites**
- **Web pages**
- **Rumors**
- **…**

Table of Contents

Collecting information

- **Partially back to sensor data problem**
  - Crawlers
  - E-Mail
  - ...
- **But some things just can't be automated**
  - “Gut feeling” as input?
  - Understanding information ...

Semantically

- **What about duplicates?**
  - Information is hard to interpret by machines
- **What is the information about?**
  - Information is hard to interpret by machines
- **Quality of the information**
  - Information is hard to interpret by machines
- **Quality of the sources**
  - …
- **Human knowledge and information is needed!**

Requirements for OSINF processing tool

- Modular
- Workflow support
- Quality assurance
- Internationalization
- Cooperative working environment
- Integration with publication / advisory system
- Aggregation and classification of information

Workflow

- Managing Open Source Information

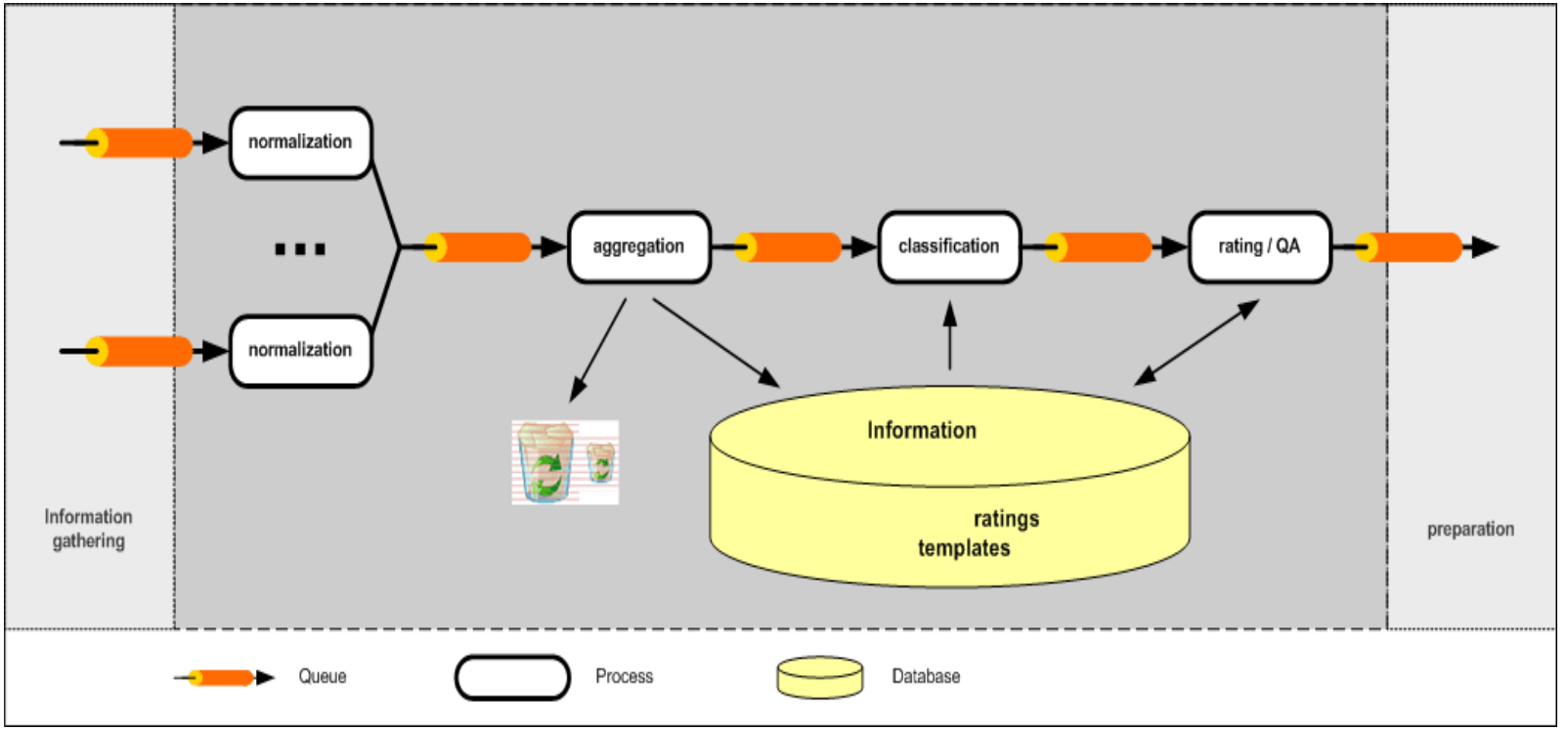


Table of Contents

Realization (prototype)

- **Backend**
  - Independent
  - Modular
  - Scalable
  - Ruby
- **Greetings from Sisyphus ...**

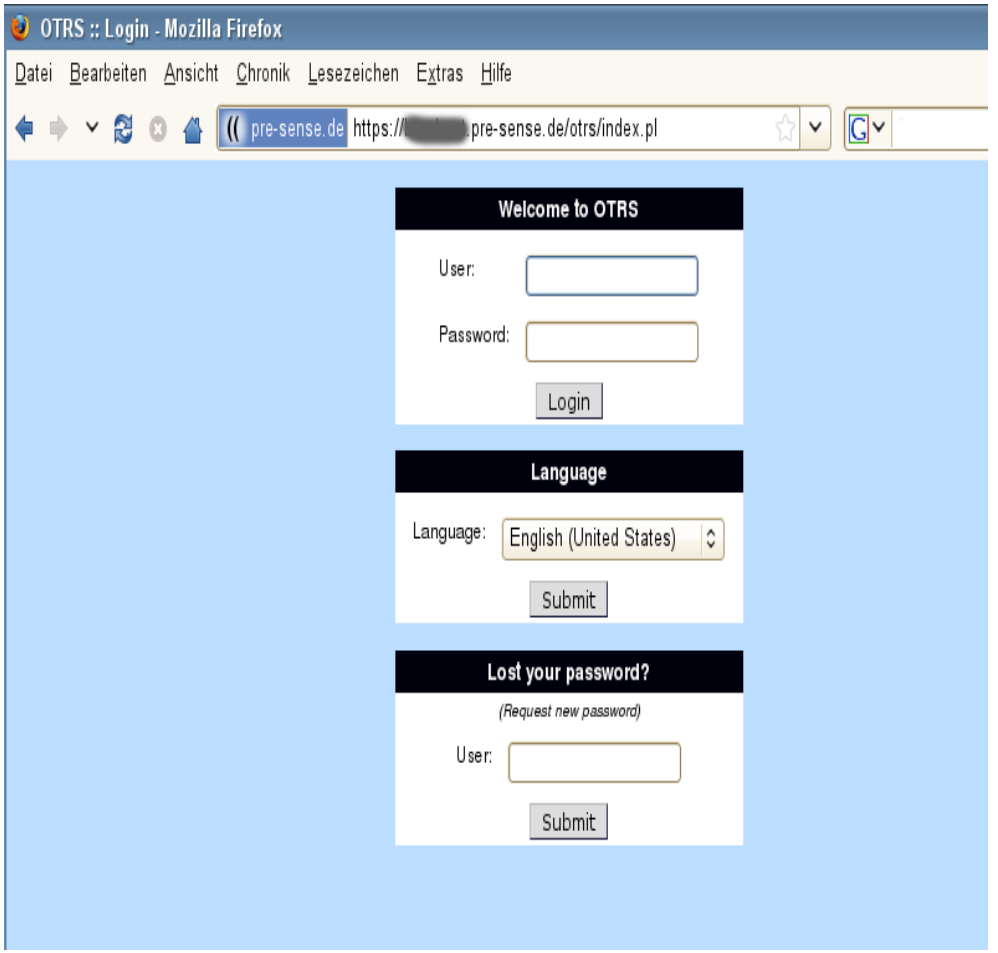
td@merceile:~ - Shell - Konsole

Sitzung Bearbeiten Ansicht Lesezeichen Einstellungen Hilfe

```
$  run-backend.sh
No config file given. Using default value (etc/config.yaml)
theinvisiblething - started
        2 new element(s)
theinvisiblething - finished
schneier - started
        5 new element(s)
schneier - finished
googlesecurity - started
        0 new element(s)
googlesecurity - finished
securityfocus - started
        5 new element(s)
securityfocus - finished
seclist - started
        4 new element(s)
seclist - finished
xorl - started
        10 new element(s)
xorl - finished
securiteam - started
        4 new element(s)
securiteam - finished
milw0rm - started
        0 new element(s)
milw0rm - finished
metasploit - started
        6 new element(s)
metasploit - finished
glasblog - started
        3 new element(s)
glasblog - finished
heisewww - started
        15 new element(s)
```

Frontend

- **Based on OTRS 2.4.x**
  - Perl, XML
  - Decent module system
  - Internationalization
  - Web based
- **Key modeling elements**
  - Tickets
  - Queues



Processing

- Information is presented as tickets

[OTRS] {first

Logout Dashboard Ticket Stats Customer Preferences QueueView Phone-Ticket Email-Ticket Search

[QueueView: Rated::HIGH]

Queues: My Queues (101) - Junk (17) - Rated (101)
HIGH (99) - MEDIUM (2)

Tickets: 1-25 of 99 - Page: 1 2 3 4

Ticket#	Age	From/Subject	State	Locked	Queue
2010011342000055	12 days 22 hours	kanese@pre-sense.de schneier: The Power Law of Ter[..]	new	unlock	Rated::HIGH
2010011342000064	12 days 22 hours	kanese@pre-sense.de schneier: Friday Squid Bloggin[..]	new	unlock	Rated::HIGH
2010011342000073	12 days 22 hours	kanese@pre-sense.de schneier: The Comparative Risk[..]	new	unlock	Rated::HIGH
2010011342000082	12 days 22 hours	kanese@pre-sense.de schneier: 768-bit Number Facto[..]	new	unlock	Rated::HIGH
2010011342000091	12 days 22 hours	kanese@pre-sense.de securityfocus: Brief: NIST inv[..]	new	unlock	Rated::HIGH
2010011342000108	12 days 22 hours	kanese@pre-sense.de securityfocus: Brief: Cyber ex[..]	new	unlock	Rated::HIGH
2010011342000117	12 days 22 hours	kanese@pre-sense.de securityfocus: News: Malicious[..]	new	unlock	Rated::HIGH
2010011342000135	12 days 22 hours	kanese@pre-sense.de xorl: Linux kernel print-fatal[..]	new	unlock	Rated::HIGH
2010011342000144	12 days 22 hours	kanese@pre-sense.de xorl: CVE-2010-0012: Transmiss[..]	new	unlock	Rated::HIGH
2010011342000153	12 days 22 hours	kanese@pre-sense.de xorl: CVE-2009-4593: bftpd Rem[..]	new	unlock	Rated::HIGH
2010011342000162	12 days 22 hours	kanese@pre-sense.de schneier: My Second CNN.com Es[..]	new	unlock	Rated::HIGH
2010011342000171	12 days 22 hours	kanese@pre-sense.de heisewww: Sicherheits-Update f[..]	new	unlock	Rated::HIGH
2010011342000181	12 days 22 hours	kanese@pre-sense.de heisewww: Open-Source-Projektb[..]	new	unlock	Rated::HIGH
2010011342000199	12 days 22 hours	kanese@pre-sense.de heisewww: Sicherheitsrelevante[..]	new	unlock	Rated::HIGH
2010011342000206	12 days 22 hours	kanese@pre-sense.de heisewww: Support-Zeiträume fü[..]	new	unlock	Rated::HIGH
2010011342000215	12 days 22 hours	kanese@pre-sense.de	new	unlock	Rated::HIGH

Tickets

- One piece of information

Logout Dashboard Ticket Stats Customer Preferences QueueView Phone-Ticket Email-Ticket Search New message (0) Locked Tickets (0)

[Zoom Ticket#: 2010012542000738] idefenselabs: Adobe Reader and Acrobat JpxDecode Memory Corr[..] [Age: 3 minutes]

Back - Lock - History - Print - Priority - Free Fields - Link - Owner - Customer - Note - Merge - Pending - Close

Created:01/25/2010 01:53:06

|--> 1. customer (email-external) kanese@pre-sense.de: idefenselabs: Adobe Reader and Acrob[..] 01/25/2010 01:53

From: kanese@pre-sense.de
To: OS3 <otrs@breakout.pre-sense.de>
Subject: idefenselabs: Adobe Reader and Acrobat JpxDecode Memory Corruption Vulnerability
Created: 01/25/2010 01:53:06
Attachment: TicketState.yaml 6 Bytes

```
I. BACKGROUND


Adobe Reader and Acrobat are Portable Document Format (PDF) reader and processors. For
more information, please visit following pages:

http://www.adobe.com/products/reader/ http://www.adobe.com/products/acrobat/ II.
DESCRIPTION


Remote exploitation of a memory corruption vulnerability in multiple versions of Adobe
Systems Inc.'s Reader and Acrobat PDF reader and processor could allow an attacker to
execute arbitrary code with the privileges of the current user.
```

State: new
Locked: unlock
Priority: 3 normal
Queue: Rated::HIGH
CustomerID: 1
Accounted time: 0
Owner: root@localhost (Admin OTRS)

Ratings:
Topicality: 1
Credibility: 1
Relevance: 1

Linked:
Normal: T:2010011342000448

Quality management

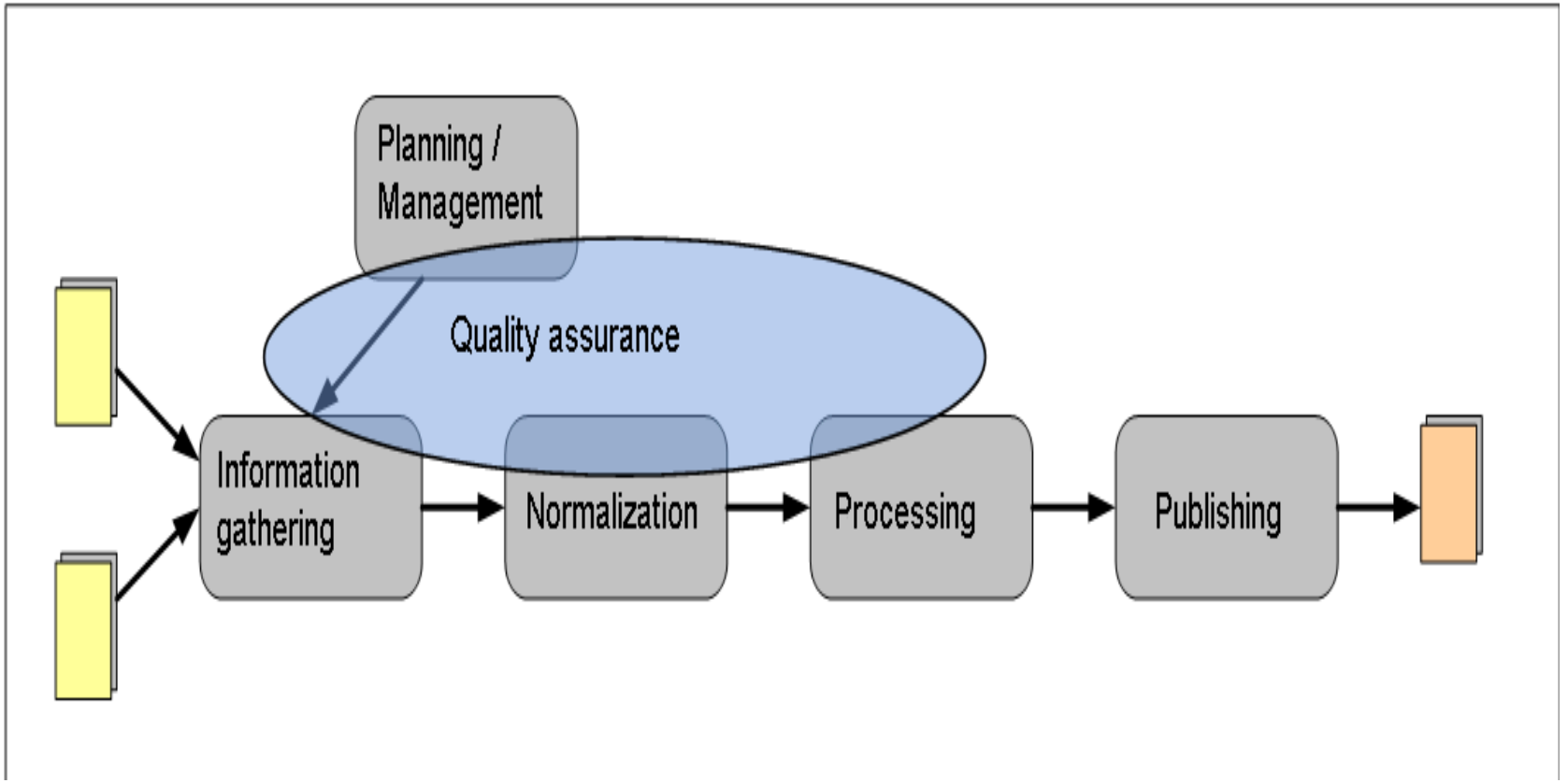
- Quality of information
- Quality of sources
- Quality of the entire process

QM of Information/Sources

- **QM of information**
  - Rating strictly human domain
    - topicality
    - credibility
    - relevance
  - Duplicate detection
- **QM of sources**
  - Feedback loop from rating information
  - Human intervention possible

QM of the process

- Workflow parts concerned



Rating

- Tickets are pre-rated

[OTRS] {firstname} {lirs

Logout Dashboard Ticket Stats Customer Preferences QueueView Phone-Ticket Email-Ticket Search

[QueueView: Rated::MEDIUM]

Queues: My Queues (91) - Junk (10) - Rated (91)
HIGH (89) - MEDIUM (2)

Tickets: 1-2 of 2 - Page: 1

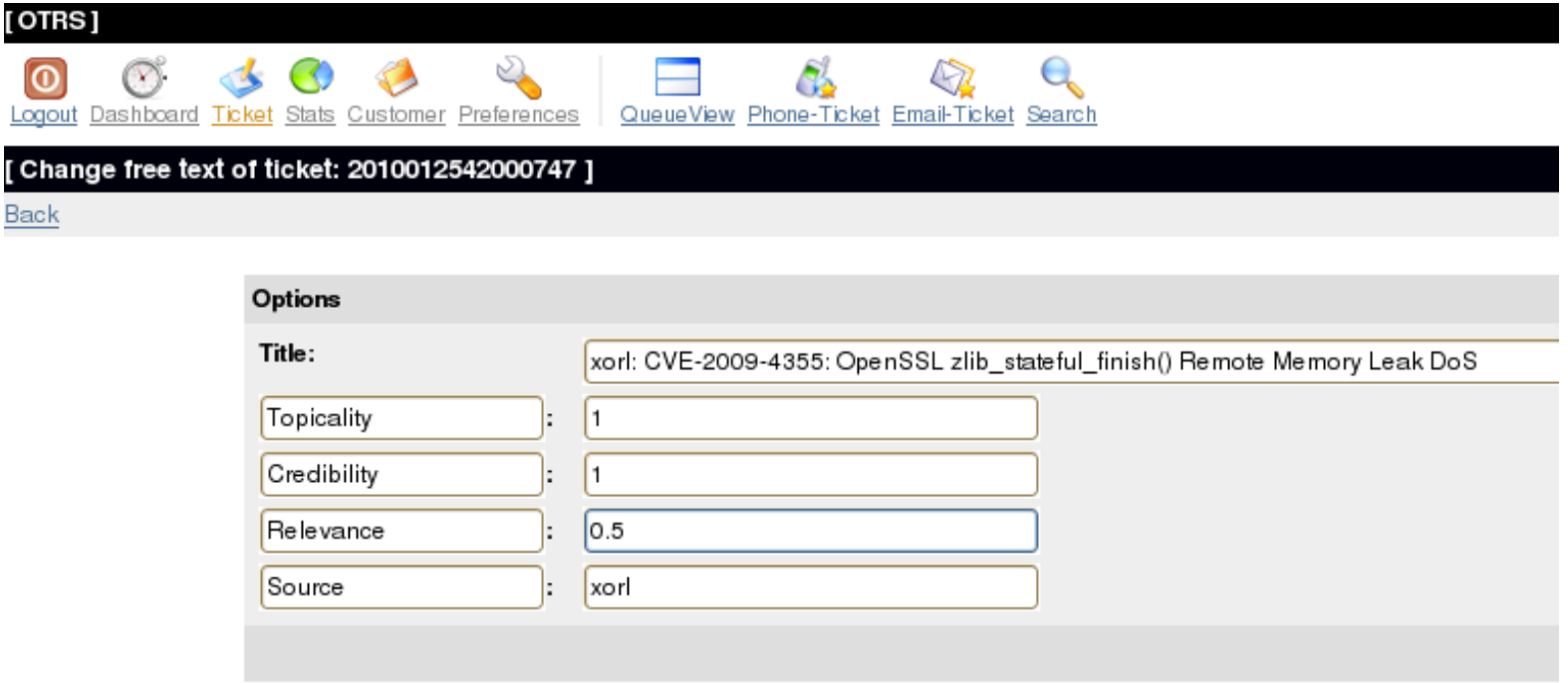
	Ticket#	Age	From/Subject	State	Locked	Queue
☐	2010012542000596	13 minutes	kanese@pre-sense.de sans: The necessary evils: Po[..]	new	unlock	Rated::MEDIUM
☐	2010012542000551	13 minutes	kanese@pre-sense.de heisewww: Elektronischer Perso[..]	new	unlock	Rated::MEDIUM

☐ Bulk Action

Tickets: 1-2 of 2 - Page: 1

Rating (cont'd)

- Manual rating of tickets
- Feedback loop to automatic (source) rating



Categorizing

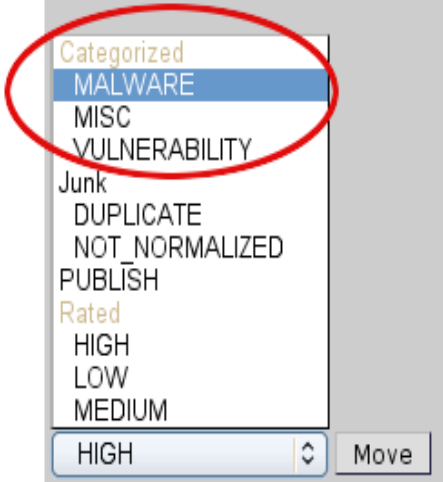
- Queues can be customized

But Andy Grimm discovered that mod_php was calling an SSL cleaning routine from cURL library which was this: void Curl_ossl_cleanup(void) { /* Free the SSL error strings */ ERR_free_strings(); /* EVP_cleanup() removes all ciphers and digests from the table. */ EVP_cleanup(); #ifdef HAVE_ENGINE_cleanup ENGINE_cleanup(); #endif #ifdef HAVE_CRYPTO_CLEANUP_ALL_EX_DATA /* this function was not present in 0.9.6b, but was added sometimes later */ CRYPTO_cleanup_all_ex_data(); #endif }

So, in case of 'HAVE_CRYPTO_CLEANUP_ALL_EX_DATA' enabled cURL library the previously mentioned OpenSSL routine will be invoked. Of course, the above OpenSSL patch fixes this bug since it removes that function but cURL should also be updated to remove this call: #endif - -#ifdef HAVE_CRYPTO_CLEANUP_ALL_EX_DATA - /* this function was not present in 0.9.6b, but was added sometimes - later */ - CRYPTO_cleanup_all_ex_data(); -#endif }

Since this is no longer available from OpenSSL, I don't think that this is an important vulnerability since there are many constraints that have to be met in order to be able to perform a remote DoS because of memory consumption. There are obviously easier ways to perform much more reliable remote DoS. P.S.: Dear reader, my apologies for the delayed post but I almost forgot it and since [6]I was having a look at a forensic challenge :P

[1] <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4355>
[2] <https://issues.rpath.com/browse/RPL-3157>
[3] <https://bugzilla.redhat.com/show_bug.cgi?id=546707#c3>
[4] <https://issues.rpath.com/secure/attachment/17979/CVE-2009-4355.patch>
[5] <https://bugzilla.redhat.com/show_bug.cgi?id=546707#c6>
[6] <http://twitter.com/xorlgr/status/7953670328>



Duplicates

- **Simhash**
  - Manassas' "shingleprinting" algorithm
  - http://wiki.cs.pdx.edu/forge/simhash.html

[OTRS] {firstname} {lirstname} (kanese@pre-sense.de) 14:58:26 - 01/25/2010

Logout Dashboard Ticket Stats Customer Preferences QueueView Phone-Ticket Email-Ticket Search New message (0) Locked Tickets (0)

[Zoom Ticket#: 2010012542000443] heisewww: Hacker haben Spanien im Visier [Age: 13 hours 6 minutes]

Back - Lock - History - Print - Priority - Free Fields - Link - Owner - Customer - Note - Merge - Pending - Close

Created:01/25/2010 01:51:42

|-> 1. customer (email-external) kanese@pre-sense.de: heisewww: Hacker haben Spanien im Vi[..] 01/25/2010 01:51

From: kanese@pre-sense.de
To: OS3 <otrs@breakout.pre-sense.de>
Subject: heisewww: Hacker haben Spanien im Visier
Created: 01/25/2010 01:51:42
Attachment: TicketState.yaml 8 Bytes

Wichtige Ministerien und Behörden in Spanien sind im vergangenen Jahr mindestens 40 Mal das Ziel von Angriffen professioneller Computer-Hacker geworden. Hinter den Attacken werden vor allem ausländische Spionagedienste vermutet, [1]berichtete die Madrider Zeitung El Pais am heutigen Sonntag unter Berufung auf den spanischen Geheimdienst Centro Nacional de Inteligencia ([2]CNI).

Ziel der Internet-Spione seien unter anderem der CNI selbst sowie das dazugehörige Nationale Kryptographische Zentrum (CCN) gewesen. Dieses kümmert sich um die Verschlüsselung vertraulicher Daten der gesamten Staatsverwaltung. Nach Angaben des Geheimdienstes blieben die Cyber-Attacken jedoch ohne Erfolg.

Bei den Angriffen seien zumeist Trojaner eingesetzt worden. In einigen Fällen habe es Warnungen anderer Regierungen gegeben. Experten beklagen, Spanien hinke beim Schutz wichtiger Infrastrukturen vor "Cyber-Spionen" im internationalen Vergleich weit hinterher. (dpa) / ([3]anw)

[1] <http://www.elpais.com/articulo/reportajes/Espana/blanco/cuarenta/ciberataqu[..]>
[2] <http://www.cni.es/>
[3] <mailto:anw@ct.de>

This ticket is a duplicate of ticket #2010012542000818 (confidence: 100%).

State: new
Locked: unlock
Priority: 3 normal
Queue: Junk::DUPLICATE
CustomerID: –
Accounted time: 0
Owner: root@localhost (Admin OTRS)

Ratings:
Topicality: 1
Credibility: 1
Relevance: 1

Linked:
Normal: T:2010012542000818

Customer Info:
Firstname: OS3
Lastname: Zulieferer
Username: OS3Backend
Email: kanese@pre-sense.de
Open Tickets (127)

Compose Answer (email):

Contact customer (phone):
Phone call

Article:
Print Forward Bounce Split

Change queue:
DUPLICATE
Move

Publication

- **Single Queue**
- **Hierarchy of queues**
- **Can be customized (modules)**
  - E-Mail
  - Input for advisory system
  - ...

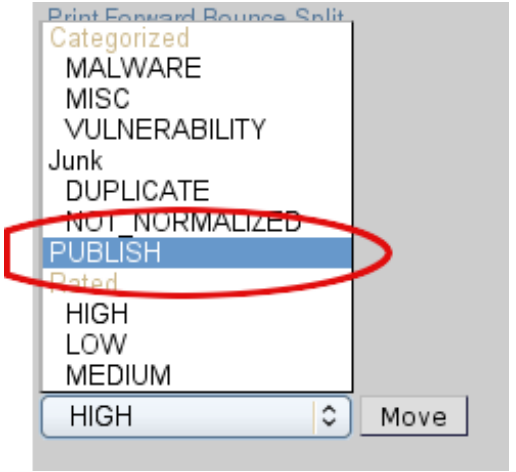


Table of Contents

Conclusions / Outlook

- **Integration of OS information**
- **Prototypical implementation**
- **Human interaction necessary**
- **Source handling difficult**
  - Generic parser modules difficult
  - Web site changes
- **Workflow „finetuning“**
- **Correlation with sensor data**
- **Generation of profiles**

Thanks …

… for your attention!

Questions?

Till Dörges, Jürgen Sander
PRESENSE Technologies GmbH
{doerges,sander}@pre-sense.de