Low Interaction Honeypot - Dionaea

Features Improvement

Google Summer of Code 2010

By Tan Kean Siong

Mentor : Markus Koetter

Content

- Google Summer of Code 2010
- Dionaea honeypot
- Improvement on Dionaea

- **Interesting facts!!**

Google Summer of Code

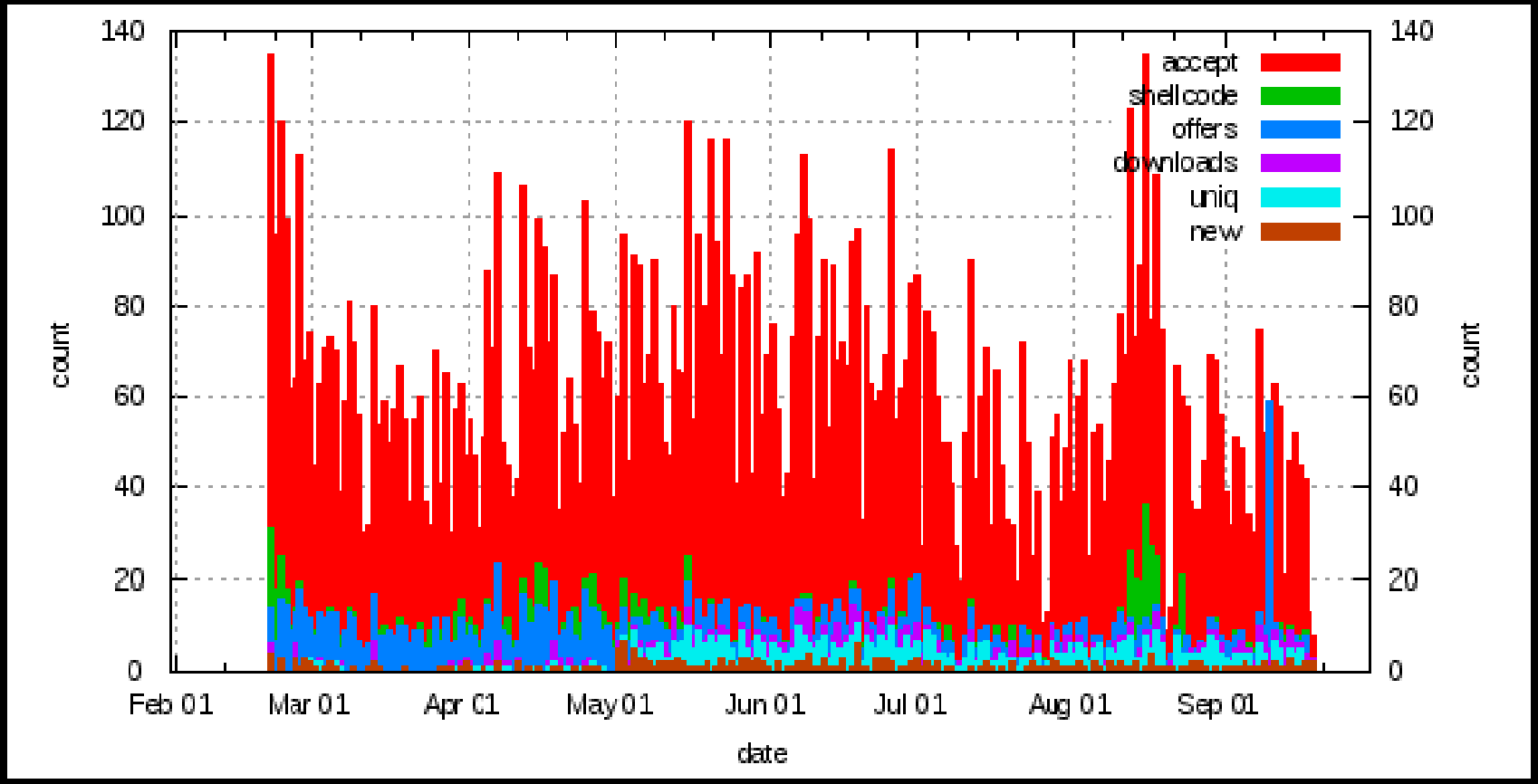
"Google Summer of Code is a global program that inspire young developers to begin participating in open source development, write code for various open source software projects"

Dionaea Honeypot

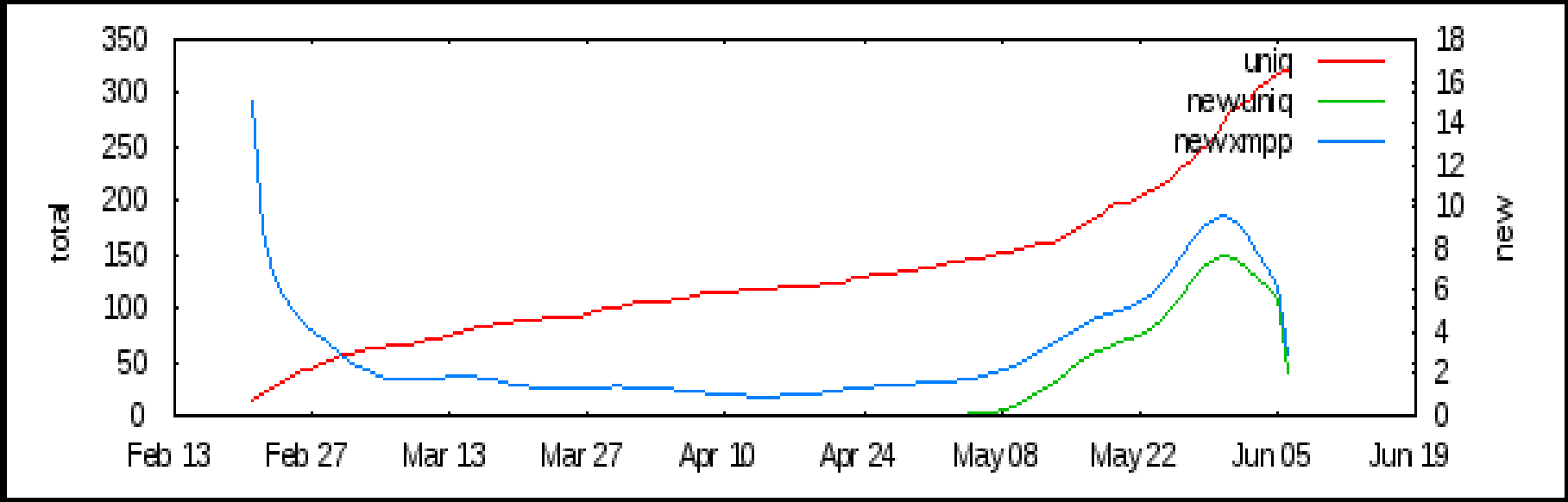
- Nepenthes successor
- Embedding python as scripting language
- Support SMB , http, ftp, tftp, SIP, TDS
- Using libemu to detect shellcodes

Attacks on SMB (port TCP 445)

- Utilities : gnuplotsql



- How many unique binaries captured?



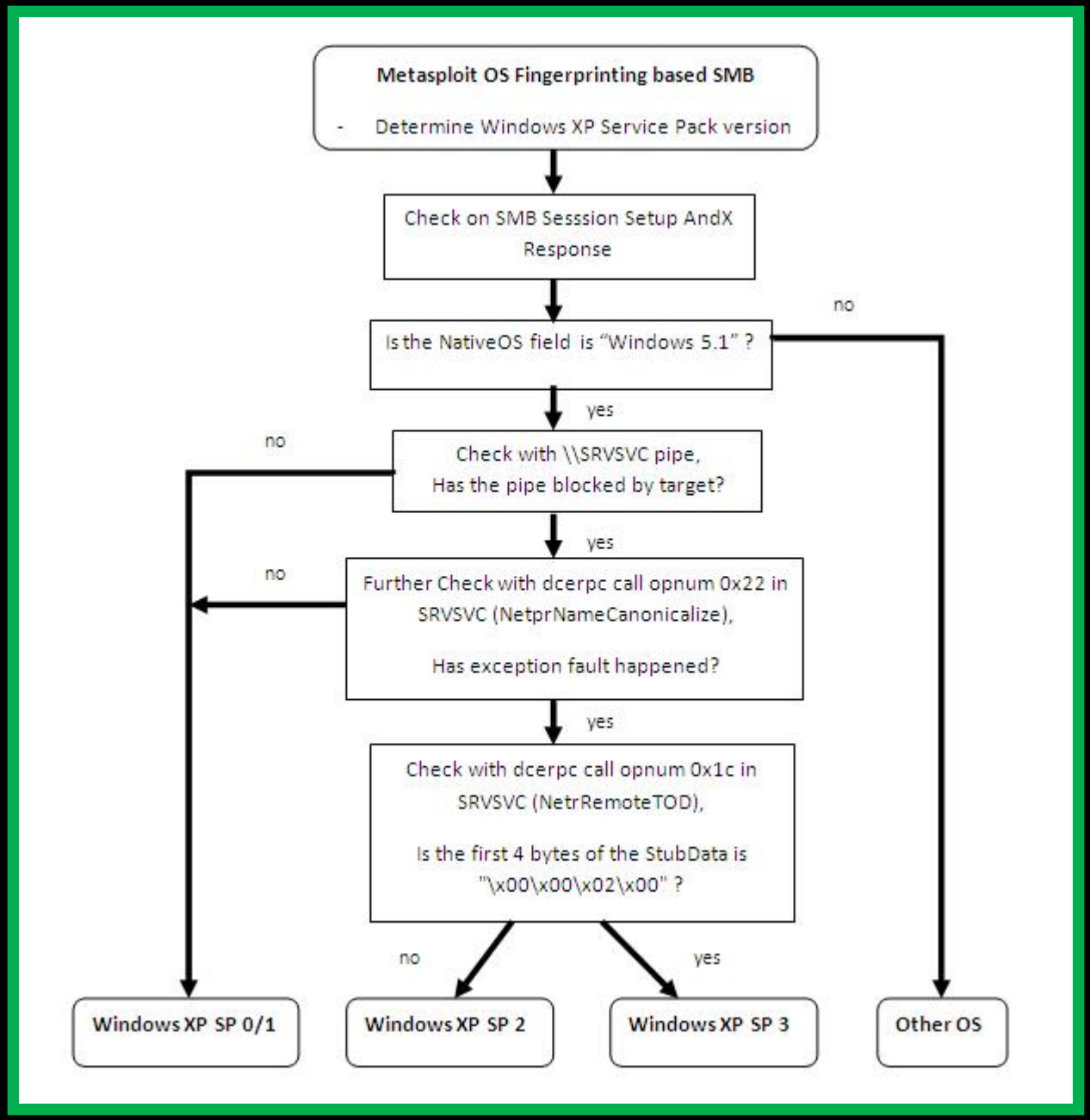
Features Improvement

- SMB stack improvement
  - NTLM authentication
- Metasploit operating system fingerprinting support
  - Nmap NSE support
- Tabular Data Stream (TDS) protocol support

Metasploit OS fingerprinting

- Metasploit OS fingerprint via SMB
- Eg. for windows XP,
  - To determine correct OS and service pack version, only 1 SMB response and 3 DCE RPC calls

    - SMB Sesssion Setup AndX Response
    - SRVSVC : **NetprNameCanonicalize** and **NetrRemoteTOD**
    - SPOOLSS: **EnumPrinter**


Metasploit OS Fingerprinting based SMB
- Determine Windows XP Service Pack version
Check on SMB Sesssion Setup AndX Response
Is the NativeOS field is "Windows 5.1" ?
no
yes
Check with \\SRVSVC pipe, Has the pipe blocked by target?
no
yes
Further Check with dcerpc call opnum 0x22 in SRVSVC (NetprNameCanonicalize), Has exception fault happened?
no
yes
Check with dcerpc call opnum 0x1c in SRVSVC (NetrRemoteTOD), Is the first 4 bytes of the StubData is "\x00\x00\x02\x00" ?
no
yes
Windows XP SP 0/1
Windows XP SP 2
Windows XP SP 3
Other OS

Interesting facts!

1. MS10-061 Exploitation

- **Microsoft Security Bulletin MS10-061**

" Vulnerability in Print Spooler Service Could Allow Remote Code Execution"

Dionaea emulate the vulnerability!

Dionaea utilities: readlogsqltree.py

2010-09-26 20:53:37

connection 25889 smbd tcp accept ::ffff:127.0.0.1:445 <- ::ffff:127.0.0.1:45470 (25889 None)

dcerpc bind: uuid '12345678-1234-abcd-ef00-0123456789ab' (spoolss)

dcerpc request: uuid '12345678-1234-abcd-ef00-0123456789ab' (spoolss) opnum 69 (OpenPrinter ())

dcerpc request: uuid '12345678-1234-abcd-ef00-0123456789ab' (spoolss) opnum 17 (StartDocPrinter ())

dcerpc request: uuid '12345678-1234-abcd-ef00-0123456789ab' (spoolss) opnum 19 (WritePrinter ())

dcerpc request: uuid '12345678-1234-abcd-ef00-0123456789ab' (spoolss) opnum 19 (WritePrinter ())

dcerpc request: uuid '12345678-1234-abcd-ef00-0123456789ab' (spoolss) opnum 19 (WritePrinter ())

dcerpc request: uuid '12345678-1234-abcd-ef00-0123456789ab' (spoolss) opnum 19 (WritePrinter ())

dcerpc request: uuid '12345678-1234-abcd-ef00-0123456789ab' (spoolss) opnum 19 (WritePrinter ())

dcerpc request: uuid '12345678-1234-abcd-ef00-0123456789ab' (spoolss) opnum 19 (WritePrinter ())

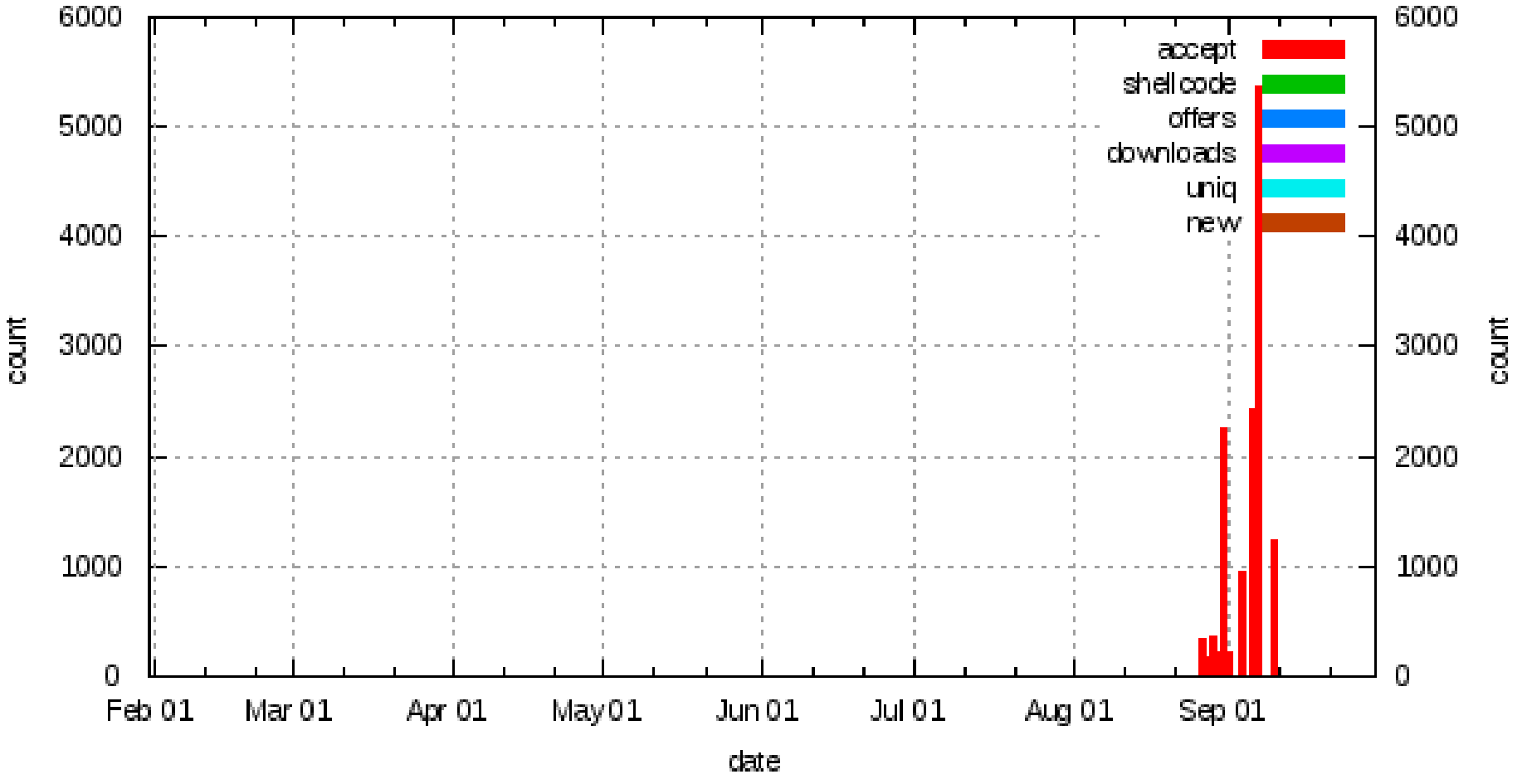
dcerpc request: uuid '12345678-1234-abcd-ef00-0123456789ab' (spoolss) opnum 19 (WritePrinter ())

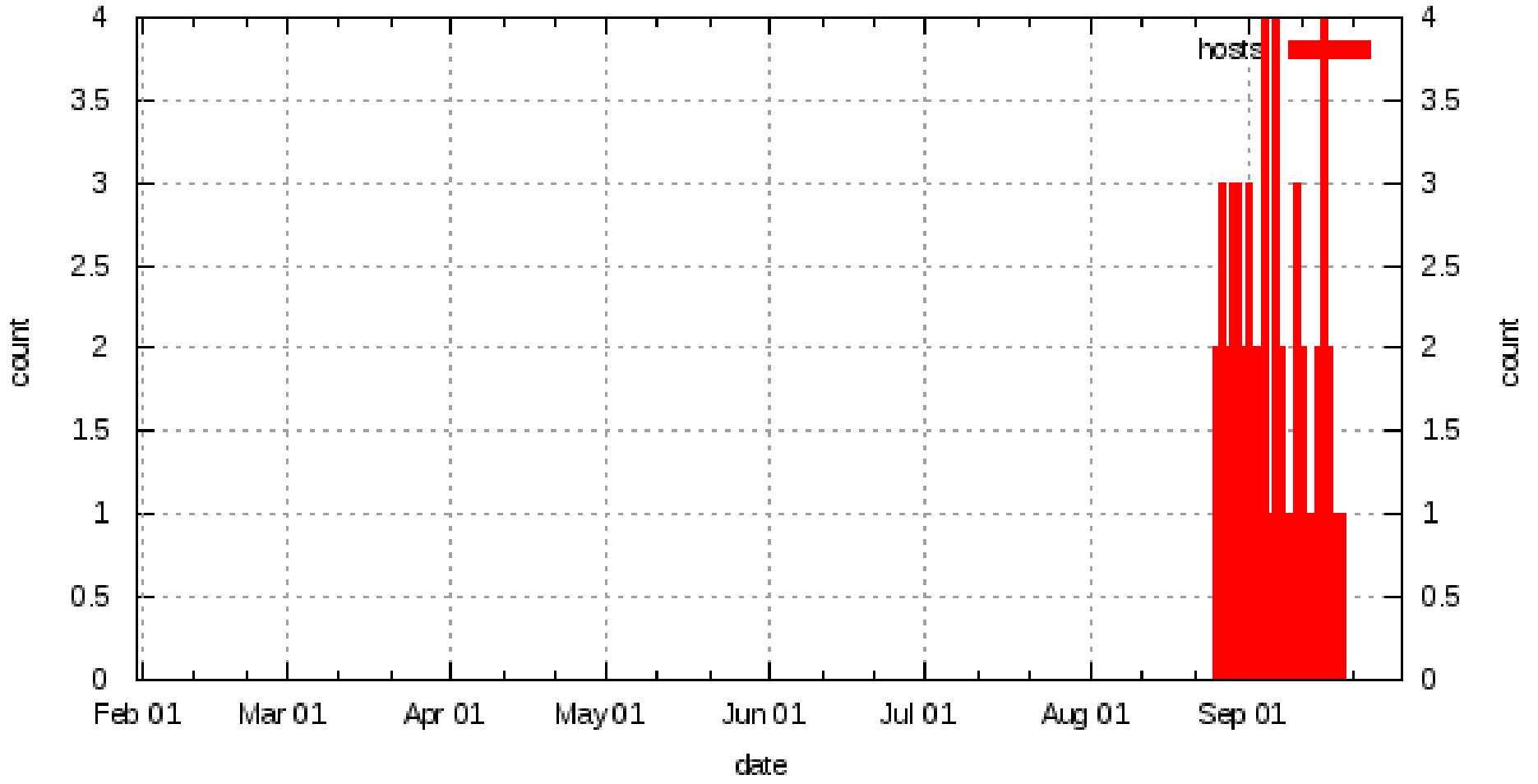
dcerpc request: uuid '12345678-1234-abcd-ef00-0123456789ab' (spoolss) opnum 19 (WritePrinter ())

dcerpc request: uuid '12345678-1234-abcd-ef00-0123456789ab' (spoolss) opnum 23 (EndDocPrinter ())
dcerpc request: uuid '12345678-1234-abcd-ef00-0123456789ab (spoolss) opnum 17 (StartDocPrinter ())
dcerpc request: uuid '12345678-1234-abcd-ef00-0123456789ab' (spoolss) opnum 19 (WritePrinter ())
dcerpc request: uuid '12345678-1234-abcd-ef00-0123456789ab' (spoolss) opnum 19 (WritePrinter ())
dcerpc request: uuid '12345678-1234-abcd-ef00-0123456789ab' (spoolss) opnum 19 (WritePrinter ())
dcerpc request: uuid '12345678-1234-abcd-ef00-0123456789ab' (spoolss) opnum 23 (EndDocPrinter ())
dcerpc request: uuid '12345678-1234-abcd-ef00-0123456789ab' (spoolss) opnum 29 (ClosePrinter ())

profile: [] offer:spoolss://::ffff:127.0.0.1/Xhbqy5httERSXV.exe
download: 6b07a937c7a89f30206cfdf25b8331de spoolss://::ffff:127.0.0.1

2. Attacks on MS-SQL (Port TCP1433)




hosts
count
count
4
3.5
3
2.5
2
1.5
1
0.5
0
Feb 01
Mar 01
Apr 01
May 01
Jun 01
Jul 01
Aug 01
Sep 01
date

Interesting facts!

no. logins	username
2244	sa
347	root

no. of logins	password
21	
17	123
13	sa
13	system
11	1234

Count	command
2465	exec sp_server_info 1 exec sp_server_info 2 exec sp_server_info 500 select 501,NULL,1 where 'a'='A' select 504,c.name,c.description,c.definition from master.dbo.syscharsets c,master.dbo.syscharsets c1,master.dbo.sysconfigures f where f.config=123 and f.value=c1.id and c1.csid=c.id set textsize 2147483647 set arithabort on

What else?

- Dionaea Honeypot Project :
  - http://dionaea.carnivore.it/
- Project blog :
  - http://carnivore.it/