Fall 2003 Wincati Issues

SUMMARY

This document describes the analytical process V/Dops used to identify why the WinCati application was intermittently failing on Met Park 9. The author intends the audience to be data networking professionals.

Met Park

Our analysis identifies an interaction between a bug in the WinCati software and a bug in an EFI Fiery print server which results in intermittent failure of the WinCati application.

Resolution

Local support staff have installed personal firewall software on the machines running the WinCati software, configured to block the offending traffic from the EFI print server. We are researching a longer-term solution, notably, one which will scale to the day when many WinCati users attempt to co-exist with the EFI print server.

OVERVIEW

History

The Cancer Prevention group at the Fred Hutchinson Cancer Research Center gathers information from patients via telephone interviews and employs WinCati ("Windows Computer-Assisted Telephone Interviewing") software from SawTooth Technologies when doing this. From a geek point of view, Wincati installs on the end-user's desktop and is configured to talk to a database server.

CP recently moved staff from the 7th floor of the Met East Building to the 9th floor. These users on the 9th floor are light users of the Wincati application, unlike some of their colleagues on the 7th floor. They began to report intermittent failures in Wincati: the software, once loaded, worked fine, but would sometimes crash on loading. Local staff noticed that only workstation running NT 5.0 (W2K) experienced problems – workstation running NT 4.0 functioned with incident.

Technical Details

FHCRC subnets its 140.107.0.0/16 IP space on the /24 boundary and dedicates a /24 network to each floor. MP7 sits on subnet 140.107.114.0/24; MP9 sits on subnet 140.107.108.0/24; the database server servicing the Wincati application sits on subnet 140.107.107.0/24.

The workstation runs WinCati v4.1; the database server runs Sybase 6.

ANALYSIS

Data-Gathering

V/Dops staff gathered numerous packet traces from workstations on MP7 and MP9 loading the Wincati application, some successful, some resulting in failure.

Results

We discovered two bugs, one in the Wincati application and another in an EFI Fiery Server ZX print server. (http://www.efi.com Electronics for Imaging).

WINCATI

When the Wincati software loads, it emits a classfull UDP broadcast in an effort to find its server. Immediately thereafter (within a few milliseconds), it then sends a unicast packet to the server address which the operator has entered into its configuration. Given that it has been configured to know the address of its server, this initial broadcast-based effort to find its server offers no functionality that I can detect. After receiving a response from the server, it then negotiates a TCP-based connection with the server.

If the Wincati software hears an ICMP port unreachable message from *any* station before it has established a connection with its server, then the Wincati software shuts down.

EFI FIERY SERVER ZX

If the EFI Fiery Server ZX receives a classfull broadcast packet destined to a port on which it is not listening, it returns a unicast ICMP Port Unreachable message. I contend that this is a bug – responding to broadcast packets with ICMP unreachable messages opens up the device to a variety of DoS attacks, in addition to making it a dupe for creating DoS attacks. I note that the EFI print server is the only device, from over a hundred other devices located on this subnet, which responds in this fashion.

What Remains

As of this writing, we have not contacted Sawtooth Technologies nor EFI to request fixes for these bugs.

LESSONS LEARNED

Sniff often and early. Failures can result from a *combination* of errors.

ACKNOWLEGEMENTS

Thanks to Mike Pennachi of Network Protocol Specialists
(http://www.networkprotocolspecialists.com) for analyzing this issue.

TRACES

All traces taken with Network Associates Sniffer Portable loaded on a laptop and plugged into a 10/100 hub shared by the workstation, with the uplink port connected to that floor's local Ethernet switch. Traces have been filtered and then imported into Ethereal for printing. The workstation running Wincati has IP address 140.107.108.213; the EFI print server has IP address 140.107.108.21. The database server hosting the Wincati back-end has IP address 140.107.107.41 and is called "cds.fhcrc.org".

Successful

Here is an example of a successful Wincati load. Notice how in packet 956, the workstation emits a *classfull* broadcast for a box listening on UDP port 2638 … this despite the fact that its IP stack is correctly configured to know that the local subnet mask is 255.255.255.0.

In packet 957, the workstation asks the DNS server for the address of cds.fhcrc.org … in packet 960, the DNS server responds … and in packet 961, the workstation sends a unicast version of its broadcast packet to cds.fhcrc.org … in packet 962, cds.fhcrc.org responds … and in packet 963, the workstation initiates a TCP SYN/SYN/ACK to build a connection with its database server. In packet 966, just after the TCP handshake completes, the EFI print server responds to the classfull broadcast with an ICMP Port Unreachable message, which, I believe, the workstation ignores. From the user point of view, the application loads successfully. Notice how the workstation waited only .002560 seconds after emitting the broadcast before giving up and asking DNS for the address of its configured server.

```
    No. Bytes  Delta T     Source              Destination         Protocol Info
    953 93     0.000550    140.107.107.41      140.107.108.213     SMB      Trans2 Response, QUERY_PATH_INFO, Error: STATUS_OBJECT_NAME_NOT_FOUND
    954 184    0.000193    140.107.108.213     140.107.107.41      SMB      Trans2 Request, QUERY_PATH_INFO, Query File Basic Info, Path:
\sti\WinCati\rasadhlp.dll
    955 93     0.000535    140.107.107.41      140.107.108.213     SMB      Trans2 Response, QUERY_PATH_INFO, Error: STATUS_OBJECT_NAME_NOT_FOUND
    956 56     0.014383    140.107.108.213     140.107.255.255     UDP      Source port: 2689  Destination port: 2638
    957 73     0.002560    140.107.108.213     140.107.92.11       DNS      Standard query A cds.fhcrc.org
    958 60     0.001542    140.107.108.21      Broadcast           ARP      Who has 140.107.108.213?  Tell 140.107.108.21
    959 42     0.000012    140.107.108.213     140.107.108.21      ARP      140.107.108.213 is at 00:08:74:a9:d3:6f
    960 270    0.000229    140.107.92.11       140.107.108.213     DNS      Standard query response A 140.107.107.41
    961 56     0.000566    140.107.108.213     140.107.107.41      UDP      Source port: 2689  Destination port: 2638
    962 60     0.000408    140.107.107.41      140.107.108.213     UDP      Source port: 2638  Destination port: 2689
    963 62     0.000290    140.107.108.213     140.107.107.41      TCP      2691 > 2638 [SYN] Seq=1037375767 Ack=0 Win=64240 Len=0 MSS=1460
    964 60     0.000438    140.107.107.41      140.107.108.213     TCP      2638 > 2691 [SYN, ACK] Seq=1629435376 Ack=1037375768 Win=8760 Len=0
MSS=1460
    965 54     0.000014    140.107.108.213     140.107.107.41      TCP      2691 > 2638 [ACK] Seq=1037375768 Ack=1629435377 Win=64240 Len=0
    966 70     0.001213    140.107.108.21      140.107.108.213     ICMP     Destination unreachable
    967 165    0.003473    140.107.108.213     140.107.107.41      TCP      2691 > 2638 [PSH, ACK] Seq=1037375768 Ack=1629435377 Win=64240
Len=111
    968 165    0.001625    140.107.107.41      140.107.108.213     TCP      2638 > 2691 [PSH, ACK] Seq=1629435377 Ack=1037375879 Win=8649 Len=111
    969 123    0.000833    140.107.108.213     140.107.107.41      TCP      2691 > 2638 [PSH, ACK] Seq=1037375879 Ack=1629435488 Win=64129 Len=69
```

```
    970 68     0.002572    140.107.107.41       140.107.108.213      TCP      2638 > 2691 [PSH, ACK] Seq=1629435488 Ack=1037375948 Win=8580 Len=14
```

Failure

In this trace, we see the workstation emit its classfull broadcast in packet 5102 and immediately thereafter receive the ICMP Port Unreachable packet from the EFI print server, in packet 5103. The workstation then emits a unicast version of the packet, directed to cds.fhcrc.org (presumably, the workstation had the DNS—IP address mapping for this name in its local cache) … but when cds.fhcrc.org responds, the workstation, rather inexplicably, delivers its own ICMP Port Unreachable message back to cds.fhcrc.org … and it does not initiate the three-way TCP handshake which we see in the Successful trace above. I believe that the EFI print server's Port Unreachable message has "broken" the workstation's ability to negotiate a connection with cds.fhcrc.org. From the user point of view, the Wincati application fails to load.

```
    No. Bytes  Delta T     Source               Destination          Protocol Info
   5095 93     0.000384    140.107.107.41       140.107.108.213      SMB      Trans2 Response, QUERY_PATH_INFO, Error: STATUS_OBJECT_NAME_NOT_FOUND
   5096 184    0.000269    140.107.108.213      140.107.107.41       SMB      Trans2 Request, QUERY_PATH_INFO, Query File Basic Info, Path:
\sti\WinCati\DHCPCSVC.DLL
   5097 93     0.000330    140.107.107.41       140.107.108.213      SMB      Trans2 Response, QUERY_PATH_INFO, Error: STATUS_OBJECT_NAME_NOT_FOUND
   5098 184    0.011973    140.107.108.213      140.107.107.41       SMB      Trans2 Request, QUERY_PATH_INFO, Query File Basic Info, Path:
\sti\WinCati\rasadhlp.dll
   5099 93     0.000374    140.107.107.41       140.107.108.213      SMB      Trans2 Response, QUERY_PATH_INFO, Error: STATUS_OBJECT_NAME_NOT_FOUND
   5100 184    0.000425    140.107.108.213      140.107.107.41       SMB      Trans2 Request, QUERY_PATH_INFO, Query File Basic Info, Path:
\sti\WinCati\rasadhlp.dll
   5101 93     0.000385    140.107.107.41       140.107.108.213      SMB      Trans2 Response, QUERY_PATH_INFO, Error: STATUS_OBJECT_NAME_NOT_FOUND
   5102 60     0.011921    140.107.108.213      140.107.255.255      UDP      Source port: 1061  Destination port: 2638
   5103 70     0.000030    140.107.108.21       140.107.108.213      ICMP     Destination unreachable
   5104 60     0.000702    140.107.108.213      140.107.107.41       UDP      Source port: 1061  Destination port: 2638
   5105 60     0.000418    140.107.107.41       140.107.108.213      UDP      Source port: 2638  Destination port: 1061
   5106 70     0.000270    140.107.108.213      140.107.107.41       ICMP     Destination unreachable
   5107 60     0.023612    Cisco_42:41:b5       Spanning-tree-(for-bridges)_00 STP      Conf. Root = 8189/00:50:3e:9c:48:6b  Cost = 4  Port = 0x8048
   5108 117    0.012804    140.107.108.213      140.107.107.41       SMB      Read AndX Request, FID: 0x1804, 16384 bytes at offset 1118208
   5109 1514   0.015713    140.107.107.41       140.107.108.213      SMB      Read AndX Response, FID: 0x1804, 16384 bytes
   5110 1514   0.000022    140.107.107.41       140.107.108.213      NBSS     NBSS Continuation Message
   5111 1514   0.000286    140.107.107.41       140.107.108.213      NBSS     NBSS Continuation Message
   5112 1514   0.000018    140.107.107.41       140.107.108.213      NBSS     NBSS Continuation Message
```

For those who like detail, here are the decode and hex windows from selected packets above.

```
Frame 5102 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 00:08:74:a9:d3:6f, Dst: ff:ff:ff:ff:ff:ff
Internet Protocol, Src Addr: 140.107.108.213 (140.107.108.213), Dst Addr: 140.107.255.255 (140.107.255.255)
User Datagram Protocol, Src Port: 1061 (1061), Dst Port: 2638 (2638)
Data (14 bytes)

0000  ff ff ff ff ff ff 00 08 74 a9 d3 6f 08 00 45 00   ........t..o..E.
0010  00 2a 07 ce 00 00 80 11 ad 49 8c 6b 6c d5 8c 6b   .*.......I.kl..k
0020  ff ff 04 25 0a 4e 00 16 25 96 53 54 52 4d 42 52   ...%.N..%.STRMBR
```

```
0030  4f 41 44 63 61 74 69 00 00 00 00 00               OADcati.....
```

Frame 5103 (70 bytes on wire, 70 bytes captured)

```
Ethernet II, Src: 00:c0:85:2a:23:72, Dst: 00:08:74:a9:d3:6f
Internet Protocol, Src Addr: 140.107.108.21 (140.107.108.21), Dst Addr: 140.107.108.213 (140.107.108.213)
Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 3 (Port unreachable)
    Checksum: 0xd583 (correct)
    Internet Protocol, Src Addr: 140.107.108.213 (140.107.108.213), Dst Addr: 140.107.255.255 (140.107.255.255)
    User Datagram Protocol, Src Port: 1061 (1061), Dst Port: 2638 (2638)

0000  00 08 74 a9 d3 6f 00 c0 85 2a 23 72 08 00 45 00   ..t..o...*#r..E.
0010  00 38 65 18 00 00 ff 01 64 eb 8c 6b 6c 15 8c 6b   .8e.....d..kl..k
0020  6c d5 03 03 d5 83 00 00 00 00 45 00 00 2a ce 07   l.........E..*..
0030  00 00 80 11 00 00 8c 6b 6c d5 8c 6b ff ff 04 25   .......kl..k...%
0040  0a 4e 00 16 00 00                                 .N....
```

Frame 5104 (60 bytes on wire, 60 bytes captured)

```
Ethernet II, Src: 00:08:74:a9:d3:6f, Dst: 00:00:0c:07:ac:6c
Internet Protocol, Src Addr: 140.107.108.213 (140.107.108.213), Dst Addr: 140.107.107.41 (140.107.107.41)
User Datagram Protocol, Src Port: 1061 (1061), Dst Port: 2638 (2638)
Data (14 bytes)

0000  00 00 0c 07 ac 6c 00 08 74 a9 d3 6f 08 00 45 00   .....l..t..o..E.
0010  00 2a 07 d0 00 00 80 11 42 1e 8c 6b 6c d5 8c 6b   .*......B..kl..k
0020  6b 29 04 25 0a 4e 00 16 ba 6c 53 54 52 4d 42 52   k).%.N...lSTRMBR
0030  4f 41 44 63 61 74 69 00 00 00 00 00               OADcati.....
```

Frame 5105 (60 bytes on wire, 60 bytes captured)

```
Ethernet II, Src: 00:d0:bc:ef:bf:24, Dst: 00:08:74:a9:d3:6f
Internet Protocol, Src Addr: 140.107.107.41 (140.107.107.41), Dst Addr: 140.107.108.213 (140.107.108.213)
User Datagram Protocol, Src Port: 2638 (2638), Dst Port: 1061 (1061)
Data (14 bytes)

0000  00 08 74 a9 d3 6f 00 d0 bc ef bf 24 08 00 45 00   ..t..o.....$..E.
0010  00 2a 57 98 00 00 7f 11 f3 55 8c 6b 6b 29 8c 6b   .*W......U.kk).k
0020  6c d5 0a 4e 04 25 00 16 b8 5a 53 54 52 4d 42 52   l..N.%...ZSTRMBR
0030  45 53 50 63 61 74 69 00 00 00 00 00               ESPcati.....
```

Frame 5106 (70 bytes on wire, 70 bytes captured)

```
Ethernet II, Src: 00:08:74:a9:d3:6f, Dst: 00:00:0c:07:ac:6c
Internet Protocol, Src Addr: 140.107.108.213 (140.107.108.213), Dst Addr: 140.107.107.41 (140.107.107.41)
Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 3 (Port unreachable)
    Checksum: 0x3619 (correct)
    Internet Protocol, Src Addr: 140.107.107.41 (140.107.107.41), Dst Addr: 140.107.108.213 (140.107.108.213)
    User Datagram Protocol, Src Port: 2638 (2638), Dst Port: 1061 (1061)
```

```
0000  00 00 0c 07 ac 6c 00 08 74 a9 d3 6f 08 00 45 00   .....l..t..o..E.
0010  00 38 07 d1 00 00 80 01 42 1f 8c 6b 6c d5 8c 6b   .8......B..kl..k
0020  6b 29 03 03 36 19 00 00 00 00 45 00 00 2a 57 98   k)..6.....E..*W.
0030  00 00 7f 11 f3 55 8c 6b 6b 29 8c 6b 6c d5 0a 4e   .....U.kk).kl..N
0040  04 25 00 16 b8 5a                                 .%...Z
```

Successful with ARP Cache Poisoning

At this point, we used a copy of Fluke's Surveyor software to emit a gratuitous ARP packet, with the destination MAC address of the EFI print server, telling the EFI print server that 140.107.108.213's MAC address is really `00:20:af:12:34:56`. That is inaccurate, of course … as you can see from the detail of packet 5102, the MAC address of 140.107.108.213 is really `00:08:74:a9:d3:6f`. However, the EFI print server is evidently running an operating system which accepts gratuitous ARPs (likely some flavor of Windows), and we can see the effects in the following trace.

This trace begins in the same way as the 'Failure' trace above … the workstation emits its classfull broadcast, and the EFI print server responds with its ICMP Port Unreachable … except that the workstation seems unaffected by the ICMP Port Unreachable. By examining the detail in frame 934, we can see why: the EFI print server believes the workstation's MAC address is `00:20:af:12:34:56`, which is not correct. The local Ethernet switch, on receiving this unknown MAC address, likely flooded the packet to all ports … the workstation received this ICMP Port Unreachable message … but because the destination MAC address does not match the MAC address of its NIC, the workstation's NIC discarded the packet, and thus it never reached the upper layers, where it would have messed things up.

```
    No. Bytes  Delta T     Source              Destination         Protocol Info
    928 93     0.000382    140.107.107.41      140.107.108.213     SMB      Trans2 Response, QUERY_PATH_INFO, Error: STATUS_OBJECT_NAME_NOT_FOUND
    929 184    0.011589    140.107.108.213     140.107.107.41      SMB      Trans2 Request, QUERY_PATH_INFO, Query File Basic Info, Path:
\sti\WinCati\rasadhlp.dll
    930 93     0.000380    140.107.107.41      140.107.108.213     SMB      Trans2 Response, QUERY_PATH_INFO, Error: STATUS_OBJECT_NAME_NOT_FOUND
    931 184    0.000319    140.107.108.213     140.107.107.41      SMB      Trans2 Request, QUERY_PATH_INFO, Query File Basic Info, Path:
\sti\WinCati\rasadhlp.dll
    932 93     0.000383    140.107.107.41      140.107.108.213     SMB      Trans2 Response, QUERY_PATH_INFO, Error: STATUS_OBJECT_NAME_NOT_FOUND
    933 60     0.011731    140.107.108.213     140.107.255.255     UDP      Source port: 1115  Destination port: 2638
    934 70     0.000135    140.107.108.21      140.107.108.213     ICMP     Destination unreachable
    935 60     0.000534    140.107.108.213     140.107.107.41      UDP      Source port: 1115  Destination port: 2638
    936 60     0.000372    140.107.107.41      140.107.108.213     UDP      Source port: 2638  Destination port: 1115
    937 62     0.000316    140.107.108.213     140.107.107.41      TCP      1116 > 2638 [SYN] Seq=474847002 Ack=0 Win=64240 Len=0 MSS=1460
    938 60     0.000219    140.107.107.41      140.107.108.213     TCP      2638 > 1116 [SYN, ACK] Seq=2347846660 Ack=474847003 Win=8760 Len=0
MSS=1460
    939 60     0.000222    140.107.108.213     140.107.107.41      TCP      1116 > 2638 [ACK] Seq=474847003 Ack=2347846661 Win=64240 Len=0
    940 165    0.004775    140.107.108.213     140.107.107.41      TCP      1116 > 2638 [PSH, ACK] Seq=474847003 Ack=2347846661 Win=64240 Len=111
    941 165    0.001325    140.107.107.41      140.107.108.213     TCP      2638 > 1116 [PSH, ACK] Seq=2347846661 Ack=474847114 Win=8649 Len=111
    942 123    0.001047    140.107.108.213     140.107.107.41      TCP      1116 > 2638 [PSH, ACK] Seq=474847114 Ack=2347846772 Win=64129 Len=69
    943 68     0.002449    140.107.107.41      140.107.108.213     TCP      2638 > 1116 [PSH, ACK] Seq=2347846772 Ack=474847183 Win=8580 Len=14
    944 148    0.000240    140.107.108.213     140.107.107.41      TCP      1116 > 2638 [PSH, ACK] Seq=474847183 Ack=2347846786 Win=64115 Len=94
```

Here is the detail on selected packets:

```
Frame 933 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 00:08:74:a9:d3:6f, Dst: ff:ff:ff:ff:ff:ff
Internet Protocol, Src Addr: 140.107.108.213 (140.107.108.213), Dst Addr: 140.107.255.255 (140.107.255.255)
User Datagram Protocol, Src Port: 1115 (1115), Dst Port: 2638 (2638)
Data (14 bytes)

0000  ff ff ff ff ff ff 00 08 74 a9 d3 6f 08 00 45 00   ........t..o..E.
0010  00 2a 49 da 00 00 80 11 6b 3d 8c 6b 6c d5 8c 6b   .*I.....k=.kl..k
0020  ff ff 04 5b 0a 4e 00 16 25 60 53 54 52 4d 42 52   ...[.N..%`STRMBR
0030  4f 41 44 63 61 74 69 00 00 00 00 00               OADcati.....


Frame 934 (70 bytes on wire, 70 bytes captured)
Ethernet II, Src: 00:c0:85:2a:23:72, Dst: 00:20:af:12:34:56
Internet Protocol, Src Addr: 140.107.108.21 (140.107.108.21), Dst Addr: 140.107.108.213 (140.107.108.213)
Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 3 (Port unreachable)
    Checksum: 0xc90b (correct)
    Internet Protocol, Src Addr: 140.107.108.213 (140.107.108.213), Dst Addr: 140.107.255.255 (140.107.255.255)
    User Datagram Protocol, Src Port: 1115 (1115), Dst Port: 2638 (2638)

0000  00 20 af 12 34 56 00 c0 85 2a 23 72 08 00 45 00   . ..4V...*#r..E.
0010  00 38 7e 64 00 00 ff 01 4b 9f 8c 6b 6c 15 8c 6b   .8~d....K..kl..k
0020  6c d5 03 03 c9 0b 00 00 00 00 45 00 00 2a da 49   l.........E..*.I
0030  00 00 80 11 00 00 8c 6b 6c d5 8c 6b ff ff 04 5b   .......kl..k...[
0040  0a 4e 00 16 00 00                                 .N....
```