Black ICE 2.5 Events, False Positives and Custom Attack Signatures

Alan Mercer
**Black ICE 2.5 Events, False Positives and Custom Attack Signatures**  
Alan Mercer, GSEC Practical Version 1.2f

**Introduction**

The major challenge for administrators of Intrusion Detection Systems is distinguishing between events that are genuine malicious activity and those that are false positives.

This paper aims to help BlackICE IDS administrators by identifying and classifying some events frequently seen by IDS agents in two common deployments – on a DMZ web server and on systems within an internal (mainly Microsoft) network.

Network ICE do provide BlackICE event (‘intrusion’) descriptions in an online database [1], but many of these need further research before they can be classified satisfactorily. This paper includes additional research into some common events.

The nature of BlackICE’s detection engine means that certain generic events may be triggered by different attacks (e.g. the HTTP field with binary event). IDS administrators are encouraged to further research all reported events thoroughly and to not assume event X is a result of attack Y.

The last section of the paper covers an unsupported method of creating custom BlackICE attack signatures that may prove useful in certain circumstances. A custom attack signature could be used to detect a new attack in the period between the attack being first identified and the vendor releasing an official attack signature update.

Please note that an in-depth discussion of incident handling and response procedures is not part of this research. Other papers available from SANS [2] address such issues.

**BlackICE IDS Agent Configurations**

These investigations were made using the Enterprise edition (version 2.5) of Network ICE’s BlackICE product and not BlackICE Defender, the personal IDS and firewall. However certain sections are relevant, particularly the custom attack signature definition.

The Agents used in this research were host-based BlackICE Agent for Server 2.5ev and BlackICE Agent for Workstation 2.5ev running on Windows NT/2000. Both agents were reporting to an ICEcap console version 2.5eq. The network-based BlackICE Sentry agent was not used, though a Sentry agent will generate identical events when monitoring passing network traffic.

The Server agents were installed on Internet-facing DMZ IIS web servers offering both web and FTP services. The only traffic allowed into the DMZ from the Internet was on port 80 (Web), port 443 (Secure Web) and port 21 (FTP) to all machines.

Machines on the internal network were running both Server and Workstation agents.
Common BlackICE events generated by Internet-facing IIS web servers agents

As soon as Internet-facing web servers are connected to the Internet they will bombard the IDS administrator with events to investigate and classify.

With only ports 21, 80 and 443 open most of the malicious activity will fall into 3 categories: web-based server attacks (e.g. Nimda worm, Code Red and IIS Printer buffer overflows), FTP activity and Operating System (O/S) fingerprinting attempts.

It is worth noting that if the IDS agents pick up activity on any ports other than ports 21, 80 and 443 it points to a misconfiguration of the firewall. For example some firewalls allow inbound/outbound DNS traffic to pass by default [3].

Note also that Workstation agent event descriptions are simpler than Server agent event descriptions. Certain Workstation agent events may have generic descriptions like HTTP Attack.

Code Red Worm


<table>
<thead>
<tr>
<th>Original Code Red</th>
<th>Code Red II (&amp; Variants)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ISAPI Extension Overflow</strong></td>
<td><strong>ISAPI Extension Overflow</strong></td>
</tr>
<tr>
<td>Parameters:</td>
<td>Parameters:</td>
</tr>
<tr>
<td>length: 362</td>
<td>length: 362</td>
</tr>
<tr>
<td>URL: /default.ida</td>
<td>URL: /default.ida</td>
</tr>
<tr>
<td>arg: NNNNNNNN (cont.)</td>
<td>arg: XXXXXXXX (cont.)</td>
</tr>
</tbody>
</table>

eEye Code Red scan [5]

**ISAPI Extension Overflow**

Parameters:
- length: 222
- URL: /x.ida
- arg: AAAAA (cont.)

Though it is rarer to see Code Red II events anymore, attacks from Code Red still persist and will continue to do so for some time [6]. Note that unlike Nimda, Code Red attacks only trigger one BlackICE event per attack.

Nimda Worm (and variants)

As Code Red activity started to subside a new and highly infectious worm, known as Nimda [7], struck the Internet around the 17th September 2001. From a very high initial attack rate, attack numbers have fallen, though Nimda-infected machines still account for a large proportion of incoming attacks
Black ICE agents report a number of events in response to Nimda attack. These events are generally triggered in batches of 4 from the same IP address over a 1-second interval. Repeated attack is common.

**HTTP UTF8 backtick**
Parameters:
```
URL: = /scripts/../../winnt/system32/cmd.exe | /scripts/../../winnt/system32/cmd.exe
```

**HTTP URL with double encoded ../*
Parameters:
```
URL: = /_mem_bin/./.././.././winnt/system32/cmd.exe | /_vti_bin/./.././.././winnt/system32/cmd.exe | /msadc/./.././.././winnt/system32/cmd.exe | /scripts/./.././.././winnt/system32/cmd.exe
```

**HTTP URL Scan**
Parameters:
```
URL: = /_mem_bin/./.././.././winnt/system32/cmd.exe | /_vti_bin/./.././.././winnt/system32/cmd.exe | /c/winnt/system32/cmd.exe | /d/winnt/system32/cmd.exe
```

**IIS System 32 Command**
Parameters:
```
URL: = /_mem_bin/./.././.././winnt/system32/cmd.exe | /_vti_bin/./.././.././winnt/system32/cmd.exe | /c/winnt/system32/cmd.exe | /msadc/./.././.././winnt/system32/cmd.exe
```

Note these events are generic and can be triggered by attacks other than the Nimda worm.

**IIS 5.0 Printer Buffer Overflow Attack**

Seen less frequently are attempts to exploit an IIS 5.0 buffer-overflow reported in May 2001 [8]. Like Nimda, these IIS printer buffer overflow attacks trigger more than one event. The event pairs, generated from 1 IP address at the same time, are

**IIS .printer overflow**

**HTTP field with binary**

Parameters:
```
length = 356
URL= /NULL.printer
```
```
field_length = 356 | 779
binary_count = 93 | 124
```

Note the **HTTP field with binary** event is a heuristic signature for the detection of buffer overflows and format string attacks. This event can therefore be generated in response to other types of attack, though as stated in the Network ICE support site the event often appears in pairs [9].
Other malicious web activity

If web sites are using password authentication, failed attempts to access them will generate the following event

*HTTP login failed*
- Parameters:
  - count = varies (see below)
  - login = URL being attacked (e.g. /extranet)

A query the Security event log on Windows system for failure audit events (logon type 2) will identify the account used for the failed logons.

FTP Activity

It is likely that every day FTP scanning activity will be detected. Often attackers scan a ranges of IP addresses so if you have IDS agents installed on a number of Internet-facing machines you will see the following event reported over a short period of time from the same IP address by each agent in turn (assuming FTP services are not running).

*FTP port probe*
- Parameters:
  - port = 21
  - reason = RSTsent or NOanswer

If your servers are hosting FTP services you may see attempts to guess legitimate passwords,

*FTP login failed*
- Parameters:
  - count = 4
  - victim = IP Address
  - login = anonymous@ftp.microsoft.com

By default this event is generated after 4 failed logins in a configurable 3600-second period.

O/S Fingerprinting

From time to time the Internet-facing machine will be OS fingerprinted [10] from another machine on the Internet. Such activity can trigger the following events.

*TCP OS fingerprint*
- Parameters:
  - port = varies (e.g. 21, 80 etc depending on open ports)
  - flags = varies (e.g. SF, SFPU depends on fingerprinting method)
  - options = varies (e.g. 3-0x;2-0x01;8-0x3F3F3F3F000000)
NMAP OS fingerprint
Parameters:
port = varies (e.g. 21)
flags = varies (e.g. S)
options = varies (e.g. 3-0x;2-0x01;8-0x3F3F3F000000)

Common BlackICE false positives seen on an internal Microsoft network

Unlike agents running on the DMZ web servers – exposed only to external attacks on port 21, 80 and 443 – agents running on an internal network will see a lot more activity across a broad range of ports. Identifying and classifying the nature of this activity – malicious or false positive – is a big challenge for IDS administrators.

Every internal network configuration is different so the purpose of this section is to point BlackICE IDS administrators in the general direction event classification. Ports used by different applications vary as much as the network activity generated by different applications.

Some of these events will be seen by DMZ server agents, though this will depend on the types of network traffic allowed into the DMZ from the internal network and other DMZs e.g. network backups, Enterprise monitoring systems etc.

Identifying and classifying these false positives allows the IDS administrator to use the built-in BlackICE facilities for managing false positives.

Such facilities include

• Using ICEcap policies to create policy issues that drop the severity of common false positive events.

• Defining trusted hosts, trusted issues and trust pairs (trusted issues from certain hosts) to prevent event generation in the first place.

• Modifying the thresholds beyond which an event is generated.

A discussion of these techniques is not covered in detail here.

Probes and Scans

A port probe event is generated when a failed connection is made to a network service. The connection fails because the service is not running, is temporarily unavailable or a firewall rule on the IDS agent rejects the connection request.

HTTP port probe
Parameters:
port = 80
reason = varies (e.g. RSTsent=connection rejected, Noanswer=no response)

Cause: Failed connections to TCP port 80.
Example(s): Windows 2000 can trigger these when mapping drives. Also seen if
web-based attacks (Nimda or Code Red) are directed against non-web DMZ servers.

**NetBIOS port probe**

Parameters:
- port = 139
- reason = varies (e.g. RST sent, No answer)

*Cause*: A connection to TCP port 139.

*Example(s)*: Mapping a drive with 'Net Use' (or with Windows Explorer) to a machine when NetBIOS file and print services (on TCP 139) are unavailable.

**SNMP port probe**

Parameters:
- port = 161
- reason = varies (e.g. ICMP sent, Firewalled by Agent)

*Cause*: A failed connection to UDP port 161.

*Example(s)*: Microsoft's SMS and Enterprise management and monitoring systems can generate many of these probes during data collection.

**TCP port probe & UDP port probe**

Parameters:
- port = varies (port of service probed)
- reason = varies (ICMP sent [UDP], RST sent [TCP], Firewalled, No answer)

*Cause*: Failed connections to services running on TCP/UDP ports that are unknown by the Black ICE agent.

*Example(s)*: They will often be seen when legitimate services are too busy to respond to connection attempts. Examples include monitoring agents talking to collection servers, browsers connecting to busy secure web sites (TCP 443) and very commonly in Windows 2000 environments when machines probe the Direct Host port [11] or TCP 445.

**TCP port scan & UDP port scan**

Parameters:
- port = varies (e.g. port 1 | port 2 | port 3 | port 4….)
- reason = varies (ICMP sent [UDP], RST sent [TCP], Firewalled, No answer)

*Cause*: Triggered by a sequential connection to 4 unique TCP or UDP ports (this is configurable).

*Example(s)*: Network backup agents communicating with backup servers or by network mapping tools.

**Microsoft networking activity**

**MS share dump**

Parameters:
- (null)

*Example(s)*: Seen frequently in a Microsoft domain environment - it can be
generated through browsing the share list on a domain machine in Network Neighbourhood.

**SMB empty password**

Parameters:
- account = varies
- share = \MACHINENAME\SHARE

*Cause:* A connection made to a share with no password.
*Examples:* Automated services may connect to, say SMS or anti-virus update shares that have no password protection. Also seen if a user logged on with a Windows domain account connects to another Windows machine that is not part of the domain, but the credentials match local credentials (username and password).

**MS security ID lookup**

Parameters:
- (null)

*Example(s):* Normal domain activity including viewing user rights in User Manager, viewing logged on users in Server Manager and opening remote event logs.

**SMB login failed**

Parameters:
- count = varies (number of failed attempts - 4, 6 etc)
- login = e.g. Administrator
- victim = IP address

*Cause:* 4 failed logins within a configurable 3600-second period.
*Example(s):* Frequently seen if services (e.g. SMS, monitoring tools etc) are running as a user account and the password has changed or expired.

**MS name lookup**

Parameters:
- (null)

*Example(s):* Generated during domain member to domain controller communication. Viewing user details with a domain management tool like Hyena can generate it (along with an *MS security ID lookup* event).

**Network discovery/management activity**

**SNMP backdoor**

Parameters:
- community = varies (e.g. admin | openview | password etc)

*Cause:* SNMP connect to a machine with one of a list of default passwords.
*Example(s):* Your network uses default SNMP passwords

**SNMP discovery broadcast**

Parameters:
command = varies (e.g. community = public)

_Cause_: SNMP GET commands.
_Examples_: Enterprise management and monitoring systems broadcasts.

**Other network activity**

**ICMP subnet mask request**
Parameters:
(null)

_Examples_: Network management and monitoring discovery broadcasts.

**RPC bad credentials**
Parameters:
reason = varies (e.g. credlen&length=500)

_Cause_: Unusual sets of credentials that do not match the RPC specifications.
_Example(s)_: Backup software such as Legato.

**Ping sweep**
Parameters:
(null)

_Examples_: Network management and monitoring systems when mapping networks.

**Telnet abuse**
Parameters:
port = varies (e.g. 25 | 80 | 100 etc)

_Cause_: Telnet connection attempts to FTP (21), SMTP (25), HTTP (80), POP (110) or IMAP (143).
_Example(s)_: Testing to see if a service is running.

**TCP SYN flood**
Parameters:
percentfromintruder = percentage of SYN connects originating from one host

_Cause_: 100 failed TCP connections over a configurable 1-second period.
_Example(s)_: Scanning tools, or services that were offline coming back online.

**Creating a Custom BlackICE Attack Signature [12]**

Custom attack signatures (or ‘Intrusions’) can be created for all Black ICE agents. The process differs slightly if the agents are standalone (BlackICE Defender) or part of an Enterprise deployment (using an ICEcap console).

The two issues to note are firstly that custom signatures will be overwritten if the agent software is updated, for example by downloading the latest version of Defender or by pushing the latest agent updates from the ICEcap console.
The second issue is that changing the configuration files may have a support implication with your reseller or vendor.

Attack signatures can be written that look for specific patterns in network traffic. The types of patterns include URLs, SMB filenames, FTP filenames, HTTP GET requests, HTTP PUT requests and so on.

The custom attack signature created below will trigger an event when a request to access a “payroll.txt” file over an SMB connection is seen by the IDS agent. Note that this procedure has been tested on agents running on NT machines only.

**Creating a BlackICE Defender 2.5 Custom Attack Signature**

(1) Stop the BlackICE service and close the BlackICE GUI (tray icon)

(2) Remove the read-only attribute from the ‘issuelist.csv’ file found in the /program files/Network ICE/BlackICE folder.

(3) Open the ‘issuelist.csv’ file and add a row below (for example) issue 2009201 – the ISS Scan issue.

(4) Enter an unused issue number of 2009202 and give the issue a name (say, *Payroll Access*). Enter a type of 0, an impact of 0, a pk-severity of –1, a di-severity of 4 (up to you), leave roots blank, add a class of Suspicious file and a summary of ‘Someone is trying to access the Payroll file’ i.e.

```
2009202,Payroll Access,0,0,-1,4,,Suspicious file,Someone is trying to access the Payroll file,
```

(5) Save the ‘issuelist.csv’ file and make it read-only again.

(6) Open the ‘blackice.ini’ file also found under /program files/Network ICE/BlackICE folder and add the following line

```
smb.filename.2009202=*/payroll.txt
```

(7) Restart the BlackICE service and the BlackICE GUI.

(8) Create a c:\payroll.txt file, map a drive to the NT share \machinename\c$ from another machine. Open the payroll.txt file from the remote machine and check the GUI on the target machine for a *Payroll Access* event.

**Creating an Enterprise BlackICE Agent 2.5 Custom Attack Signature**

Carry out the following steps on the ICEcap console.

(1) Stop the ICEcap service, BlackICE service and BlackICE GUI (if installed).
(2) Edit the both the ‘issuelist.csv’ files found in the \program files\Network
ICE\ICEcap\infobase\issues folder (not read-only) and the ‘issuelist.csv’ file found
under \program files\Network ICE\ICEcap\versions\{agent version}\blackd folder
(which is read-only).

(3) Carry out steps 3, 4 as above on both ‘issuelist.csv’ files.

(4) Make the agent ‘issuelist.csv’ file read-only again.

(5) Restart the ICEcap, BlackICE services and BlackICE GUI (if installed).

(6) Login to the web-based ICEcap console with administrative rights. Under the
Agent Configuration screen of the target agent add a Custom parameter with a name
of smb.filename.2009202, a value of */payroll.txt and a comment of ‘Someone is
trying to access the Payroll file’.

(7) Uninstall the remote agents and then reinstall them again from the ICEcap
console using the Agent Install mechanism.

(8) Carry out step 8 as above to test the custom attack signature. Look for the
Payroll Access event in the BlackICE GUI of the local agent and also check the
same event is recorded at the ICEcap console.

A small selection of other custom parameter examples include

<table>
<thead>
<tr>
<th>Event</th>
<th>Parameters</th>
<th>Possible cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP port probe</td>
<td>port = 80</td>
<td>Attempted web connection to a machine without web services running.</td>
</tr>
<tr>
<td>NetBIOS port probe</td>
<td>port = 139</td>
<td>Attempted drive mapping to a machine without NetBIOS services running.</td>
</tr>
<tr>
<td>SNMP port probe</td>
<td>port = 161</td>
<td>Enterprise management &amp; monitoring systems.</td>
</tr>
<tr>
<td>TCP/UDP port probes</td>
<td>port = varies (e.g. TCP 443 TCP 445)</td>
<td>Monitoring agents failing to connect to busy collection servers. Browsers failing to</td>
</tr>
</tbody>
</table>

Appendix – Summary of BlackICE false positives seen on an internal Microsoft network

<table>
<thead>
<tr>
<th>Event</th>
<th>Parameters</th>
<th>Possible cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP port探测</td>
<td>port = 80</td>
<td>尝试与没有Web服务的机器建立Web连接。</td>
</tr>
<tr>
<td>NetBIOS端口探测</td>
<td>port = 139</td>
<td>尝试映射驱动到没有NetBIOS服务的机器。</td>
</tr>
<tr>
<td>SNMP端口探测</td>
<td>port = 161</td>
<td>企业管理和监控系统。</td>
</tr>
<tr>
<td>TCP/UDP端口探测</td>
<td>port = varies (e.g. TCP 443 TCP 445)</td>
<td>监控代理无法连接到繁忙的收集服务器。浏览器无法连接到。</td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>TCP/UDP port scans</td>
<td>port = varies (e.g. port1</td>
<td>port2</td>
</tr>
<tr>
<td>MS share dump</td>
<td>(null) Browsing a share list on a machine.</td>
<td></td>
</tr>
<tr>
<td>SMB empty password</td>
<td>account = varies share = varies Connection to non-password protected shares.</td>
<td></td>
</tr>
<tr>
<td>MS security ID lookup</td>
<td>(null) Normal MS domain activity. Remote viewing of event logs, viewing user rights in user manager.</td>
<td></td>
</tr>
<tr>
<td>SMB login failed</td>
<td>count = varies login = varies victim = varies Services running as user accounts and password has changed or expired.</td>
<td></td>
</tr>
<tr>
<td>MS name lookup</td>
<td>(null) Normal MS domain activity. MS domain management tools.</td>
<td></td>
</tr>
<tr>
<td>SNMP backdoor</td>
<td>community = varies Network using default SNMP passwords.</td>
<td></td>
</tr>
<tr>
<td>SNMP discovery broadcast</td>
<td>command = varies Enterprise management and monitoring system broadcasts.</td>
<td></td>
</tr>
<tr>
<td>ICMP subnet mask request</td>
<td>(null) Network management and monitoring tools.</td>
<td></td>
</tr>
<tr>
<td>RPC bad credentials</td>
<td>reason = varies Network backup agents communicating with backup servers.</td>
<td></td>
</tr>
<tr>
<td>Ping sweep</td>
<td>(null) Network management and monitoring tools.</td>
<td></td>
</tr>
<tr>
<td>Telnet abuse</td>
<td>port = varies Testing of service availability.</td>
<td></td>
</tr>
<tr>
<td>TCP SYN flood</td>
<td>percent from intruder = varies Offline services returns online (e.g. email services).</td>
<td></td>
</tr>
</tbody>
</table>

References

[1] Database of Intrusions detected by Network ICE
   http://advice.networkice.com/Advice/Intrusions/default.htm

[2] SANS reading room: Incident Handling and Forensics
   http://www.sans.org/infosecFAQ/incident/incident_list.htm

   http://www.codetalker.com/advisories/misc/dil981024.html


[6] A Snapshot of Global Internet Worm Activity
http://www.monkey.org/~dugsong/papers/worms/

[7] Nimda Worm

[8] Buffer Overflow Vulnerability in Microsoft IIS 5.0
http://www.cert.org/advisories/CA-2001-10.html

[9] HTTP field with Binary
http://advice.networkice.com/advice/Intrusions/2000646/default.htm

[10] Remote OS detection via TCP/IP Stack Finger Printing
http://www.insecure.org/nmap/nmap-fingerprinting-article.html


[12] Discussions with BlackICE support staff.