To Be or Not To Be

An Incident Recovery Case Study

Sherman, Xie Chunyan
CCE, CISSP, GCIH

Agenda

- **Incidents in NUS**
- **Incident Handling Decisions**
- **The Recovery Principles**
- **Case Studies**
- **Q&A**

Systems Classification

Affiliated Research Institutes and Centers
School/Faculty Level
- **Academic Systems**
- **Administrative Systems**

University Level
- **Administrative**
- **Academic Systems**

Work Stations
Notebooks
Networked appliances

Attacks Observed

Targeted phishing

Website defacement

Targeted hacking

Virus/Botnet

Lost of end-point devices

Careless handling/accidentally sending

Targeted Phishing

Dear nus.edu.sg Email Owner,

This message is from nus.edu.sg messaging center to all nus.edu.sg Email owners. We are currently upgrading our data base and e-mail center. We are deleting all unused nus.edu.sg to create more space for new one. To prevent your account from closing you will have to update it below so that we will know that it's a present used account.

CONFIRM YOUR EMAIL BELOW
Email Username :.....
EMAIL Password : .....
Date of Birth : .....
Country or Territory : .....

Warning!!! Email owner that refuses to update his or her Email within Seven days of receiving this warning will lose his or her Email permanently.

Regards,
NUS.EDU.SG Beta Team

Web Defacement

Hacked by RedRoLiX Terrorist Crew NOWAR	Hacked by RedRoLiX Terrorist Crew NOWAR	Singapore	13/01/2009	13/01/2009

Targeted Hacking

xxx x xx:42:12 localhost sshd[22746]: Failed password for admin from ::ffff:173.8.119.129 port 57469 ssh2
xxx x xx:42:16 localhost sshd[22748]: Failed password for admin from ::ffff:173.8.119.129 port 58334 ssh2
xxx x xx:42:21 localhost sshd[22750]: Failed password for admin from ::ffff:173.8.119.129 port 59179 ssh2
xxx x xx:42:26 localhost sshd[22752]: Failed password for admin from ::ffff:173.8.119.129 port 60015 ssh2
xxx x xx:42:30 localhost sshd[22754]: Failed password for admin from ::ffff:173.8.119.129 port 60836 ssh2
xxx x xx:42:35 localhost sshd[22756]: Failed password for admin from ::ffff:173.8.119.129 port 33425 ssh2
xxx x xx:42:40 localhost sshd[22758]: Failed password for admin from ::ffff:173.8.119.129 port 34267 ssh2
xxx x xx:42:44 localhost sshd[22760]: Failed password for admin from ::ffff:173.8.119.129 port 35057 ssh2
xxx x xx:43:36 localhost sshd[22782]: Failed password for admin from ::ffff:173.8.119.129 port 43227 ssh2
xxx x xx:43:38 localhost sshd[22784]: Accepted password for admin from ::ffff:173.8.119.129 port 44026 ssh2

Motivation of Attacks

- **Spam generation**
- **Political propaganda**
- **Launch pad**
- **General purpose zombie hosts**

Incident Handling Decisions

To Disconnect?

To Make Forensic Copy?

To Reinstall?

To Redevelopment?

Disconnection -- If the Answer is NO

Damage Containment Measures

- **Blackhole Network**
- **Network Point Disconnection**

Activity Monitoring

- **Log Correlation System**

Forensic Copy – If the answer is NO

Establish Strong Audit Trial

Minimize Analysis Foot Print

Reinstallation – If the answer is NO

OS/Application Verification

Activity Monitoring

Log Correlation System

Redevelopment – If the answer is NO

Penetration Testing

Secure Code Scanning

Recovery Decisions Considerations

Backup Strategy

Responsibility Relationship

The Recovery Priorities

End User Experience

Damage Containment

Rapid Root Cause Identification

Cost

Case Studies

Case 1: Website Defacement

Case 2: System Compromise

Case 3: Website Defacement

Case 1

Web Defacement

Initial information: An website xxx.nus.edu.sg is detected compromised. The IP resolves to an university level server.

To Disconnect?

End User Experience

- **Website is used by one student society**
- **Impact is small since currently it's school holiday**

Damage Containment

- **Damage can be contained by taking down the virtual host**

Root Cause Analysis

Line 9559: 2009-xx-xx xx:09:09 W3SVC1 137.132.xx.xx GET /xxxxxx/index.php ***option=com_content&view=article&id=7:yih&catid=38:home*** *80 - 201.209.97.224 Mozilla/5.0+(Windows;+U;+Windows+NT+5.1;+es-ES;+rv:1.9.0.10)+Gecko/2009042316+Firefox/3.0.10 200 0 0*

Root Cause Analysis

Line 9583: 2009-xx-xx xx:09:19 W3SVC1 137.132.xx.xx POST /xxxxx/index.php option=com_user&task=confirmreset 80 - 201.209.97.224 Mozilla/5.0+(Windows;+U;+Windows+NT+5.1;+es-ES;+rv:1.9.0.10)+Gecko/2009042316+Firefox/3.0.10 301 0 0

Line 9584: 2009-xx-xx xx:09:21 W3SVC1 137.132.xx.xx GET /xxxxx/index.php option=com_user&view=reset&layout=complete 80 - 201.209.97.224 Mozilla/5.0+(Windows;+U;+Windows+NT+5.1;+es-ES;+rv:1.9.0.10)+Gecko/2009042316+Firefox/3.0.10 200 0 0

Line 9585: 2009-xx-xx xx:09:25 W3SVC1 137.132.xx.xx POST /xxxxx/index.php option=com_user&task=completereset 80 - 201.209.97.224 Mozilla/5.0+(Windows;+U;+Windows+NT+5.1;+es-ES;+rv:1.9.0.10)+Gecko/2009042316+Firefox/3.0.10 301 0 0

Line 9586: 2009-xx-xx xx:09:26 W3SVC1 137.132.xx.xx GET /xxxxx/index.php option=com_user&view=login 80 - 201.209.97.224 Mozilla/5.0+(Windows;+U;+Windows+NT+5.1;+es-ES;+rv:1.9.0.10)+Gecko/2009042316+Firefox/3.0.10 200 0 0

…

Line 9589: 2009-xx-xx xx:09:31 W3SVC1 137.132.xx.xx GET /xxxxx/administrator/index.php - 80 - 201.209.97.224 Mozilla/5.0+(Windows;+U;+Windows+NT+5.1;+es-ES;+rv:1.9.0.10)+Gecko/2009042316+Firefox/3.0.10 200 0 0

…

Line 9610: 2009-xx-xx xx:09:38 W3SVC1 137.132.xx.xx POST /xxxxx/administrator/index.php - 80 - 201.209.97.224 Mozilla/5.0+(Windows;+U;+Windows+NT+5.1;+es-ES;+rv:1.9.0.10)+Gecko/2009042316+Firefox/3.0.10 301 0 0

…

Root Cause Analysis

Line 9707: 2009-xx-xx xx:10:34 W3SVC1 137.132.xx.xx GET /xxxxx/administrator/index.php option=com_templates&task=edit&cid[]=rhuk_cyberia&client=0 80 - 201.209.97.224 Mozilla/5.0+(Windows;+U;+Windows+NT+5.1;+es-ES;+rv:1.9.0.10)+Gecko/2009042316+Firefox/3.0.10 200 0 0

...

Line 9713: 2009-xx-xx xx:10:41 W3SVC1 137.132.xx.xx GET /xxxxx/administrator/index.php option=com_templates&client=0&task=edit&cid[]=rhuk_cyberia 80 - 201.209.97.224 Mozilla/5.0+(Windows;+U;+Windows+NT+5.1;+es-ES;+rv:1.9.0.10)+Gecko/2009042316+Firefox/3.0.10 200 0 0

...

Line 9724: 2009-xx-xx xx:11:39 W3SVC1 137.132.xx.xx GET /xxxxx/administrator/index.php option=com_templates&client=0&task=edit&cid[]=rhuk_cblc 80 - 201.209.97.224 Mozilla/5.0+(Windows;+U;+Windows+NT+5.1;+es-ES;+rv:1.9.0.10)+Gecko/2009042316+Firefox/3.0.10 200 0 0

Root Cause Analysis

Line 9725: 2009-xx-xx xx:11:42 W3SVC1 137.132.xx.xx POST /nussucblc/administrator/index.php - 80 - 201.209.97.224 Mozilla/5.0+(Windows;+U;+Windows+NT+5.1;+es-ES;+rv:1.9.0.10)+Gecko/2009042316+Firefox/3.0.10 301 0 0

Line 9726: 2009-xx-xx xx:11:45 W3SVC1 137.132.xx.xx GET /nussucblc/administrator/index.php option=com_templates&client=0 80 - 201.209.97.224 Mozilla/5.0+(Windows;+U;+Windows+NT+5.1;+es-ES;+rv:1.9.0.10)+Gecko/2009042316+Firefox/3.0.10 200 0 0

Line 9729: 2009-xx-xx xx:12:41 W3SVC1 137.132.xx.xx GET /nussucblc/administrator/index.php option=com_templates 80 - 201.209.97.224 Mozilla/5.0+(Windows;+U;+Windows+NT+5.1;+es-ES;+rv:1.9.0.10)+Gecko/2009042316+Firefox/3.0.10 200 0 0

Line 9731: 2009-xx-xx xx:12:43 W3SVC1 137.132.xx.xx GET /nussucblc/index.php option=com_user&view=login 80 - 201.209.97.224 Mozilla/5.0+(Windows;+U;+Windows+NT+5.1;+es-ES;+rv:1.9.0.10)+Gecko/2009042316+Firefox/3.0.10 200 0 0

…

Other decisions

Forensic Copy – NO

Reinstallation – NO

Case 2

System Compromise

Initial information: A system is reported to attack IPs in Huston, US. This system is a departmental level server.

To Disconnect?

End User Experience

- **It’s a development server**
- **No impact to end user**

Damage Containment

- **Damage can not be contained unless disconnection**

To Make Forensic Copy?

There was no backup

Outsource vendor is evolved

No impact to end user

Root Cause Analysis

:xxx xx 07:45:56 tegus1.nus.edu.sg %FWSM-6-302014 Teardown TCP connection 145861783990550207 for outside:173.8.119.129/41200 to inside:137.132.xxx.xxx/22 duration 0:00:04 bytes 3618 TCP FINs

:xxx xx 07:46:00 tegus1.nus.edu.sg %FWSM-6-302013 Built inbound TCP connection 145861783990550209 for outside:173.8.119.129/43269 (173.8.119.129/43269) to inside:137.132.xxx.xxx/22 (137.132.xxx.xxx/22)

:xxx xx 07:46:00 tegus1.nus.edu.sg %FWSM-6-302014 Teardown TCP connection 145861783990550208 for outside:173.8.119.129/42259 to inside:137.132.xxx.xxx/22 duration 0:00:04 bytes 3618 TCP FINs

:xxx xx 07:46:05 tegus1.nus.edu.sg %FWSM-6-302013 Built inbound TCP connection 145861783990550210 for outside:173.8.119.129/44377 (173.8.119.129/44377) to inside:137.132.xxx.xxx/22 (137.132.xxx.xxx/22)

:xxx xx 07:46:05 tegus1.nus.edu.sg %FWSM-6-302014 Teardown TCP connection 145861783990550209 for outside:173.8.119.129/43269 to inside:137.132.xxx.xxx/22 duration 0:00:05 bytes 3618 TCP FINs

:xxx xx 07:46:10 tegus1.nus.edu.sg %FWSM-6-302013 Built inbound TCP connection 145861783990550211 for outside:173.8.119.129/45457 (173.8.119.129/45457) to inside:137.132.xxx.xxx/22 (137.132.xxx.xxx/22)

:xxx xx 07:46:10 tegus1.nus.edu.sg %FWSM-6-302014 Teardown TCP connection 145861783990550210 for outside:173.8.119.129/44377 to inside:137.132.xxx.xxx/22 duration 0:00:04 bytes 3618 TCP FINs

:xxx xx 07:46:15 tegus1.nus.edu.sg %FWSM-6-302014 Teardown TCP connection 145861783990550211 for outside:173.8.119.129/45457 to inside:137.132.xxx.xxx/22 duration 0:00:04 bytes 3618 TCP FINs

The Brute Force Attacker is from IP in Minneapolis, US.

Root Cause Analysis

xxx x xx:42:12 localhost sshd[22746]: Failed password for admin from ::ffff:173.8.119.129 port 57469 ssh2
xxx x xx:42:16 localhost sshd[22748]: Failed password for admin from ::ffff:173.8.119.129 port 58334 ssh2
xxx x xx:42:21 localhost sshd[22750]: Failed password for admin from ::ffff:173.8.119.129 port 59179 ssh2
xxx x xx:42:26 localhost sshd[22752]: Failed password for admin from ::ffff:173.8.119.129 port 60015 ssh2
xxx x xx:42:30 localhost sshd[22754]: Failed password for admin from ::ffff:173.8.119.129 port 60836 ssh2
xxx x xx:42:35 localhost sshd[22756]: Failed password for admin from ::ffff:173.8.119.129 port 33425 ssh2
xxx x xx:42:40 localhost sshd[22758]: Failed password for admin from ::ffff:173.8.119.129 port 34267 ssh2
xxx x xx:42:44 localhost sshd[22760]: Failed password for admin from ::ffff:173.8.119.129 port 35057 ssh2
xxx x xx:43:36 localhost sshd[22782]: Failed password for admin from ::ffff:173.8.119.129 port 43227 ssh2
xxx x xx:43:38 localhost sshd[22784]: Accepted password for admin from ::ffff:173.8.119.129 port 44026 ssh2
xxx x xx:43:49 localhost sshd[22822]: Failed password for admin from ::ffff:173.8.119.129 port 45538 ssh2
xxx x xx:43:54 localhost sshd[22825]: Failed password for admin from ::ffff:173.8.119.129 port 46312 ssh2
xxx x xx:43:58 localhost sshd[22827]: Failed password for admin from ::ffff:173.8.119.129 port 47085 ssh2

Root Cause Analysis

:xxx x xx:49:11 tegus1.nus.edu.sg %FWSM-6-302013 Built inbound TCP connection 146277824587520702 for outside:85.122.96.140/4063 (85.122.96.140/4063) to inside:137.132.xxx.xxx/22 (137.132.xxx.xxx/22)

:xxx x xx:49:54 tegus1.nus.edu.sg %FWSM-6-302013 Built outbound TCP connection 146277824587520703 for inside:137.132.xxx.xxx/50075 (137.132.xxx.xxx/50075) to outside:125.56.199.16/80 (125.56.199.16/80)

:xxx x xx:50:05 tegus1.nus.edu.sg %FWSM-6-302014 Teardown TCP connection 146277824587520703 for inside:137.132.xxx.xxx/50075 to outside:125.56.199.16/80 duration 0:00:10 bytes 2666084 TCP FINs

:xxx x xx:51:41 tegus1.nus.edu.sg %FWSM-6-302015 Built inbound UDP connection 146277824587520704 for outside:190.137.72.82/11218 (190.137.72.82/11218) to inside:137.132.xxx.xxx/60257 (137.132.xxx.xxx/60257)

:xxx x xx:52:42 tegus1.nus.edu.sg %FWSM-6-302016 Teardown UDP connection 146277824587520704 for outside:190.137.72.82/11218 to inside:137.132.xxx.xxx/60257 duration 0:01:01 bytes 167

:xxx x xx:53:35 tegus1.nus.edu.sg %FWSM-6-302013 Built inbound TCP connection 146277824587520705 for outside:85.122.96.140/4065 (85.122.96.140/4065) to inside:137.132.xxx.xxx/22 (137.132.xxx.xxx/22)

:xxx x xx:56:03 tegus1.nus.edu.sg %FWSM-6-302013 Built inbound TCP connection 146277824587520706 for outside:85.122.96.140/4066 (85.122.96.140/4066) to inside:137.132.xxx.xxx/22 (137.132.xxx.xxx/22)

:xxx x xx:58:43 tegus1.nus.edu.sg %FWSM-6-302013 Built outbound TCP connection 146277824587520707 for inside:137.132.xxx.xxx/50078 (137.132.xxx.xxx/50078) to outside:208.100.61.101/80 (208.100.61.101/80)

:xxx x xx:58:48 tegus1.nus.edu.sg %FWSM-6-302014 Teardown TCP connection 146277824587520707 for inside:137.132.xxx.xxx/50078 to outside:208.100.61.101/80 duration 0:00:04 bytes 656374 TCP FINs

The attacker accessed the system from 85.122.96.140 (Romania) and downloaded files to the system from 125.56.199.16(Boston) and 208.100.61.101 (Chicago)

Root Cause Analysis

The system is a development server for a department.

Remote access via SSH is open for vendor to access the system from outside of NUS network.

The Attacker successfully used Brute Force Attack to crack the account “admin” on the system. The password of the account “admin” is the name of the software installed.

Other decisions

Reinstallation – Yes

Redevelopment – No

Case 3

Web Defacement

Initial information: An website xxx.nus.edu.sg is detected defaced. The IP resolves to a school level server. The event registration system of the website seems to be compromised.

To Disconnect?

End User Experience

- **Site can not be taken down**
- **Huge impact to users**

Damage Containment

- **Damage can be contained by remove the affected module.**

Risk: The attacker could have planted other malicious software on the system.

Root Cause Analysis

2009-xx-xx xx:01:25 W3SVC844950 137.132.146.115 GET /index.asp - 80 - 85.133.177.15 Mozilla/5.0+(Windows;+U;+Windows+NT+5.1;+en-US;+rv:1.9.0.8)+Gecko/2009032609+Firefox/3.0.8 200 0 0

2009-xx-xx xx:03:18 W3SVC844950 137.132.146.115 GET /admin/index.asp - 80 - 85.133.177.15 Mozilla/5.0+(Windows;+U;+Windows+NT+5.1;+en-US;+rv:1.9.0.8)+Gecko/2009032609+Firefox/3.0.8 302 0 0

2009-xx-xx xx:03:47 W3SVC844950 137.132.146.115 GET /admin/index.asp d=login 80 - 85.133.177.15 Mozilla/5.0+(Windows;+U;+Windows+NT+5.1;+en-US;+rv:1.9.0.8)+Gecko/2009032609+Firefox/3.0.8 200 0 0

2009-xx-xx xx:04:53 W3SVC844950 137.132.146.115 POST /admin/index.asp d=login 80 - 85.133.177.15 Mozilla/5.0+(Windows;+U;+Windows+NT+5.1;+en-US;+rv:1.9.0.8)+Gecko/2009032609+Firefox/3.0.8 302 0 0

The attacker was from 85.133.177.15 (Iran).

The attacker accessed the log in page (/admin/index.asp d=login) of the in-house CMS. The user used POST command to send password string to the server.

Root Cause Analysis

2009-xx-xx xx:08:07 W3SVC844950 137.132.146.115 GET /admin/index.asp d=add_event 80 - 85.133.177.15 Mozilla/5.0+(Windows;+U;+Windows+NT+5.1;+en-US;+rv:1.9.0.8)+Gecko/2009032609+Firefox/3.0.8 200 0 64

2009-xx-xx xx:08:07 W3SVC844950 137.132.146.115 GET /admin/index.asp d=add_event 80 - 85.133.177.15 Mozilla/5.0+(Windows;+U;+Windows+NT+5.1;+en-US;+rv:1.9.0.8)+Gecko/2009032609+Firefox/3.0.8 200 0 0

The authentication code in the login page is vulnerable to SQL injection attack.

The attacker used modified the event information (*/admin/index.asp d=add_event)* in the database

Redevelopment

End User Experience

- **All event registration switches to manual**

Cost Consideration

Other decisions

Forensic copy -- NO

Reinstallation – NO

Tips

It’s always a balancing act.

Don’t jump to conclusion.

Take calculated risk.

There’s no hard and fast rule.

Q & A

Thank You

ccecert@nus.edu.sg