- No Starch Press: www.nostarch.com
- DHS National Checklist Program Repository: http://web.nvd.nist.gov/view/ncp/repository
- NIST Special Publications: http://csrc.nist.gov/publications/nistpubs/index.html
- Microsoft Security Guides for Security Compliance Management Toolkit Series: http://technet.microsoft.com/en-us/library/cc677002.aspx

Appendix B: Incident Response Report

A Naturalis Insident Persent
Network Incident Report United States Secret Service • Financial Crimes Division • Electronic Crimes Branch
Telephone: 202-406-5850 FAX: 202-406-9233 e-mail: ecb@secretservice.gov
Subject:
☐ Site under attack ☐ Incident investigation in progress ☐ Incident closed
What assistance do you require: Immediate call
None needed at this time
☐ Follow-up on all affected sites ☐ Contact the "hacking" site(s)
Site involved (name & acronym):
POC for incident:
Name / Title Organization
Organization F-mail
Alternate POC for incident:
Name / Title Organization
• E-mail • 7 x 24 contact information
Type of Incident:
Malicious code: virus, Trojan horse, worm Probes/scans (non-malicious data gatheringrecurring, massive, unusual)
□ Attack (successful/unsuccessful intrusions including scanning with attack packets)
☐ Denial-of-service event ☐ High embarrassment factor
☐ Deemed significant by site
Date and time incident occurred (specify time zone):
A summary of what happened:
Type of service, information, or project compromised (please provide specifics):
☐ Sensitive unclassified such as privacy, proprietary, or source selection
Other unclassified
Damage done:
Numbers of systems affected Nature of loss, if any
System downtime
Cost of incident: ☐unknown ☐ none ☐<\$10K ☐ \$10K - \$50K ☐ >\$50K
Name other sites contacted
Law Enforcement Other:

Page 1

UNITED STATES SECRET SERVICE

SSF 4017 (03/2002)

Apparent source: Diskette, CD, etc. E-mail attachment Software download	Details for Malicious Code	
□ E-mail attachment □ Software download Primary system or network involved: □ Paddresses or sub-net addresses □ OS version(s) □ NOS version(s) □ Other affected systems or networks (IPs and OSs): Type of malicious code (include name if known): □ Virus □ Trojan horse □ Worm □ Joke program □ Other □ Copy sent to □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □		
Software download Primary system or network involved: • IP addresses or sub-net addresses • OS version(s) • NOS version(s) • NOS version(s) • Other		
Primary system or network involved: IP addresses or sub-net addresses OS version(s) NOS version(s) Other Other affected systems or networks (IPs and OSs): Type of malicious code (include name if known): Virus Trojan horse Worm Joke program Other Copy sent to Method of Operation (for new malicious code): Type: macro, boot, memory resident, polymorphic, self encrypting, stealth Payload Software infected Files erased, modified, deleted, encrypted (any special significance to these files) Self propagating via e-mail Detectable changes Other features How detected: Remediation (what was done to return the system(s) to trusted operation): Anti-virus product gotten, updated, or installed for automatic operation New policy instituted on attachments Firewall or routers or e-mail servers updated to detect and scan attachments		
IP addresses or sub-net addresses OS version(s) NOS version(s) Other Other Other affected systems or networks (IPs and OSs): Type of malicious code (include name if known): Virus Trojan horse Worm Joke program Other Copy sent to Copy sent to Copy sent to Software infected Files erased, modified, deleted, encrypted (any special significance to these files) Self propagating via e-mail Detectable changes Other features How detected: Remediation (what was done to return the system(s) to trusted operation): Anti-virus product gotten, updated, or installed for automatic operation New policy instituted on attachments Firewall or routers or e-mail servers updated to detect and scan attachments Firevall or routers or e-mail servers updated to detect and scan attachments	□ Software download	
OS version(s) NOS version(s) Other affected systems or networks (IPs and OSs): Type of malicious code (include name if known): Virus Trojan horse Worm Joke program Other Copy sent to Method of Operation (for new malicious code): Type: macro, boot, memory resident, polymorphic, self encrypting, stealth Payload Software infected Files erased, modified, deleted, encrypted (any special significance to these files) Self propagating via e-mail Detectable changes Other features How detected: Remediation (what was done to return the system(s) to trusted operation): Anti-virus product gotten, updated, or installed for automatic operation New policy instituted on attachments Firewall or routers or e-mail servers updated to detect and scan attachments		
Not version(s) Other affected systems or networks (IPs and OSs): Type of malicious code (include name if known): Virus Trojan horse Worm Joke program Other Copy sent to Payload Software infected Files erased, modified, deleted, encrypted (any special significance to these files) Self propagating via e-mail Detectable changes Other features How detected: Remediation (what was done to return the system(s) to trusted operation): Anti-virus product gotten, updated, or installed for automatic operation New policy instituted on attachments Firewall or routers or e-mail servers updated to detect and scan attachments	IP addresses or sub-net addresses	
Not version(s) Other affected systems or networks (IPs and OSs): Type of malicious code (include name if known): Virus Trojan horse Worm Joke program Other Copy sent to Payload Software infected Files erased, modified, deleted, encrypted (any special significance to these files) Self propagating via e-mail Detectable changes Other features How detected: Remediation (what was done to return the system(s) to trusted operation): Anti-virus product gotten, updated, or installed for automatic operation New policy instituted on attachments Firewall or routers or e-mail servers updated to detect and scan attachments	OS version(s)	
Other affected systems or networks (IPs and OSs): Type of malicious code (include name if known): Virus Trojan horse Worm Joke program Other Copy sent to Method of Operation (for new malicious code): Type: macro, boot, memory resident, polymorphic, self encrypting, stealth Payload Software infected Files erased, modified, deleted, encrypted (any special significance to these files) Self propagating via e-mail Detectable changes Other features How detected: Remediation (what was done to return the system(s) to trusted operation): Anti-virus product gotten, updated, or installed for automatic operation New policy instituted on attachments Firewall or routers or e-mail servers updated to detect and scan attachments	NOS version(s)	
Type of malicious code (include name if known): Virus Trojan horse Worm Joke program Other Copy sent to polymorphic, self encrypting, stealth Payload Software infected Files erased, modified, deleted, encrypted (any special significance to these files) Self propagating via e-mail Detectable changes Other features How detected: Remediation (what was done to return the system(s) to trusted operation): Anti-virus product gotten, updated, or installed for automatic operation New policy instituted on attachments Firewall or routers or e-mail servers updated to detect and scan attachments	Other	
Virus Trojan horse Worm Joke program Other Copy sent to Project Projec	Other affected systems or networks (IPs and O	Ss):
Joke program		
Joke program Other Copy sent to Gopy sent to G	Urus	
Joke program Other Copy sent to Gopy sent to G	☐ Trojan horse	
Copy sent to Copy sent to Details: Method of Operation (for new malicious code): Type: macro, boot, memory resident, polymorphic, self encrypting, stealth Payload Software infected Files erased, modified, deleted, encrypted (any special significance to these files) Self propagating via e-mail Detectable changes Other features How detected: Remediation (what was done to return the system(s) to trusted operation): Anti-virus product gotten, updated, or installed for automatic operation New policy instituted on attachments Firewall or routers or e-mail servers updated to detect and scan attachments	U worm	
Copy sent to Copy sent to Details: Method of Operation (for new malicious code): Type: macro, boot, memory resident, polymorphic, self encrypting, stealth Payload Software infected Files erased, modified, deleted, encrypted (any special significance to these files) Self propagating via e-mail Detectable changes Other features How detected: Remediation (what was done to return the system(s) to trusted operation): Anti-virus product gotten, updated, or installed for automatic operation New policy instituted on attachments Firewall or routers or e-mail servers updated to detect and scan attachments	Joke program	
Copy sent to Copy sent to Copy se	U Other	
Method of Operation (for new malicious code): Type: macro, boot, memory resident, polymorphic, self encrypting, stealth Payload Software infected Files erased, modified, deleted, encrypted (any special significance to these files) Self propagating via e-mail Detectable changes Other features How detected: Remediation (what was done to return the system(s) to trusted operation): Anti-virus product gotten, updated, or installed for automatic operation New policy instituted on attachments Firewall or routers or e-mail servers updated to detect and scan attachments		
Method of Operation (for new malicious code): Type: macro, boot, memory resident, polymorphic, self encrypting, stealth Payload Software infected Files erased, modified, deleted, encrypted (any special significance to these files) Self propagating via e-mail Detectable changes Other features How detected: Remediation (what was done to return the system(s) to trusted operation): Anti-virus product gotten, updated, or installed for automatic operation New policy instituted on attachments Firewall or routers or e-mail servers updated to detect and scan attachments		
Method of Operation (for new malicious code): Type: macro, boot, memory resident, polymorphic, self encrypting, stealth Payload Software infected Files erased, modified, deleted, encrypted (any special significance to these files) Self propagating via e-mail Detectable changes Other features How detected: Remediation (what was done to return the system(s) to trusted operation): Anti-virus product gotten, updated, or installed for automatic operation New policy instituted on attachments Firewall or routers or e-mail servers updated to detect and scan attachments		
□ Type: macro, boot, memory resident, polymorphic, self encrypting, stealth □ Payload □ Software infected □ Files erased, modified, deleted, encrypted (any special significance to these files) □ Self propagating via e-mail □ Detectable changes □ Other features How detected: Remediation (what was done to return the system(s) to trusted operation): □ Anti-virus product gotten, updated, or installed for automatic operation □ New policy instituted on attachments □ Firewall or routers or e-mail servers updated to detect and scan attachments		
□ Type: macro, boot, memory resident, polymorphic, self encrypting, stealth □ Payload □ Software infected □ Files erased, modified, deleted, encrypted (any special significance to these files) □ Self propagating via e-mail □ Detectable changes □ Other features How detected: Remediation (what was done to return the system(s) to trusted operation): □ Anti-virus product gotten, updated, or installed for automatic operation □ New policy instituted on attachments □ Firewall or routers or e-mail servers updated to detect and scan attachments	Method of Operation (for new malicious code):	Details:
polymorphic, self encrypting, stealth Payload Software infected Files erased, modified, deleted, encrypted (any special significance to these files) Self propagating via e-mail Detectable changes Other features How detected: Remediation (what was done to return the system(s) to trusted operation): Anti-virus product gotten, updated, or installed for automatic operation New policy instituted on attachments Firewall or routers or e-mail servers updated to detect and scan attachments		
□ Payload □ Software infected □ Files erased, modified, deleted, encrypted (any special significance to these files) □ Self propagating via e-mail □ Detectable changes □ Other features How detected: Remediation (what was done to return the system(s) to trusted operation): □ Anti-virus product gotten, updated, or installed for automatic operation □ New policy instituted on attachments □ Firewall or routers or e-mail servers updated to detect and scan attachments		
□ Software infected □ Files erased, modified, deleted, encrypted (any special significance to these files) □ Self propagating via e-mail □ Detectable changes □ Other features How detected: Remediation (what was done to return the system(s) to trusted operation): □ Anti-virus product gotten, updated, or installed for automatic operation □ New policy instituted on attachments □ Firewall or routers or e-mail servers updated to detect and scan attachments		
(any special significance to these files) Self propagating via e-mail Detectable changes Other features How detected: Remediation (what was done to return the system(s) to trusted operation): Anti-virus product gotten, updated, or installed for automatic operation New policy instituted on attachments Firewall or routers or e-mail servers updated to detect and scan attachments		
(any special significance to these files) Self propagating via e-mail Detectable changes Other features How detected: Remediation (what was done to return the system(s) to trusted operation): Anti-virus product gotten, updated, or installed for automatic operation New policy instituted on attachments Firewall or routers or e-mail servers updated to detect and scan attachments	☐ Files erased, modified, deleted, encrypted	
□ Detectable changes □ Other features How detected: Remediation (what was done to return the system(s) to trusted operation): □ Anti-virus product gotten, updated, or installed for automatic operation □ New policy instituted on attachments □ Firewall or routers or e-mail servers updated to detect and scan attachments		
□ Detectable changes □ Other features How detected: Remediation (what was done to return the system(s) to trusted operation): □ Anti-virus product gotten, updated, or installed for automatic operation □ New policy instituted on attachments □ Firewall or routers or e-mail servers updated to detect and scan attachments	☐ Self propagating via e-mail	
Other features How detected: Remediation (what was done to return the system(s) to trusted operation): Anti-virus product gotten, updated, or installed for automatic operation New policy instituted on attachments Firewall or routers or e-mail servers updated to detect and scan attachments	□ Detectable changes	
Remediation (what was done to return the system(s) to trusted operation): Anti-virus product gotten, updated, or installed for automatic operation New policy instituted on attachments Firewall or routers or e-mail servers updated to detect and scan attachments		
the system(s) to trusted operation): Anti-virus product gotten, updated, or installed for automatic operation New policy instituted on attachments Firewall or routers or e-mail servers updated to detect and scan attachments	How detected:	
the system(s) to trusted operation): Anti-virus product gotten, updated, or installed for automatic operation New policy instituted on attachments Firewall or routers or e-mail servers updated to detect and scan attachments		
☐ Anti-virus product gotten, updated, or installed for automatic operation ☐ New policy instituted on attachments ☐ Firewall or routers or e-mail servers updated to detect and scan attachments		Details:
for automatic operation New policy instituted on attachments Firewall or routers or e-mail servers updated to detect and scan attachments		
☐ New policy instituted on attachments ☐ Firewall or routers or e-mail servers updated to detect and scan attachments		
☐ Firewall or routers or e-mail servers updated to detect and scan attachments		
to detect and scan attachments		
Additional comments:	** ************************************	
	Additional comments:	
UNITED STATES SECRET SERVICE Page 2 SSF 4017 (03/20	UNITED STATES SECRET SERVICE	SSF 4017 (03/2002)

Details for Probes and Scans		
Apparent source: • IP address		
Host name		
Location of attacking host:		
☐ Domestic		
☐ Foreign		
☐ Insider		
Primary system(s) / network(s) involved:		
IP addresses or sub-net addresses		
OS version(s)		
NOS version(s)		
Other affected systems or networks (IPs and O	Ss):	
Method of Operation:	Details:	
☐ Ports probed/scanned		
☐ Order of ports or IP addresses scanned		
☐ Probing tool		
☐ Anything that makes this probe unique		
- rayaning anat manor and proof anique		
How detected:	Details:	
☐ Another site		
☐ Incident response team		
☐ Log files		
☐ Packet sniffer		
☐ Intrusion detection system		
□ Anomalous behavior		
□ User		
Log file excerpts:		
Additional comments:		
Additional comments.		
UNITED STATES SECRET SERVICE		SSF 4017 (03/2002)

Page 3

How detected:	Deteiler
	Details:
☐ Another site	
☐ Incident response team	
☐ Log files	
 Packet sniffer/intrusion detection software 	
☐ Intrusion detection software	
☐ Anomalous behavior	
User	
☐ Alarm tripped	
☐ TCP Wrappers	
☐ TRIPWRED	
☐ Other	
Log file excerpts:	
Remediation (what was done to return the system(s) to trusted operation): Patches applied Scanners run	Details:
system(s) to trusted operation): Patches applied Scanners run Security software installed:	Details:
system(s) to trusted operation): Patches applied Scanners run Security software installed: Unneeded services and applications removed	Details:
system(s) to trusted operation): Patches applied Scanners run Security software installed: Unneeded services and applications removed OS reloaded	Details:
system(s) to trusted operation): Patches applied Scanners run Security software installed: Unneeded services and applications removed OS reloaded Restored from backup	Details:
system(s) to trusted operation): Patches applied Scanners run Security software installed: Unneeded services and applications removed OS reloaded Restored from backup Application moved to another system	Details:
system(s) to trusted operation): Patches applied Scanners run Security software installed: Unneeded services and applications removed OS reloaded Restored from backup Application moved to another system Memory or disk space increased	Details:
system(s) to trusted operation): Patches applied Scanners run Security software installed: Unneeded services and applications removed OS reloaded Restored from backup Application moved to another system Memory or disk space increased Moved behind a filtering router or firewall	Details:
system(s) to trusted operation): Patches applied Scanners run Security software installed: Unneeded services and applications removed OS reloaded Restored from backup Application moved to another system Memory or disk space increased	Details:
system(s) to trusted operation): Patches applied Scanners run Security software installed: Unneeded services and applications removed OS reloaded Restored from backup Application moved to another system Memory or disk space increased Moved behind a filtering router or firewall Hidden files detected and removed	Details:
system(s) to trusted operation): Patches applied Scanners run Security software installed: Unneeded services and applications removed OS reloaded Restored from backup Application moved to another system Memory or disk space increased Moved behind a filtering router or firewall Hidden files detected and removed Trojan software detected and removed	Details:
system(s) to trusted operation): Patches applied Scanners run Security software installed: Unneeded services and applications removed OS reloaded Restored from backup Application moved to another system Memory or disk space increased Moved behind a filtering router or firewall Hidden files detected and removed Trojan software detected and removed Left unchanged to monitor hacker	Details:
system(s) to trusted operation): Patches applied Scanners run Security software installed: Unneeded services and applications removed OS reloaded Restored from backup Application moved to another system Memory or disk space increased Moved behind a filtering router or firewall Hidden files detected and removed Trojan software detected and removed Left unchanged to monitor hacker Other	Details:
system(s) to trusted operation): Patches applied Scanners run Security software installed: Unneeded services and applications removed OS reloaded Restored from backup Application moved to another system Memory or disk space increased Moved behind a filtering router or firewall Hidden files detected and removed Trojan software detected and removed Left unchanged to monitor hacker	Details:
system(s) to trusted operation): Patches applied Scanners run Security software installed: Unneeded services and applications removed OS reloaded Restored from backup Application moved to another system Memory or disk space increased Moved behind a filtering router or firewall Hidden files detected and removed Trojan software detected and removed Left unchanged to monitor hacker Other	Details:
system(s) to trusted operation): Patches applied Scanners run Security software installed: Unneeded services and applications removed OS reloaded Restored from backup Application moved to another system Memory or disk space increased Moved behind a filtering router or firewall Hidden files detected and removed Trojan software detected and removed Left unchanged to monitor hacker Other	Details:
system(s) to trusted operation): Patches applied Scanners run Security software installed: Unneeded services and applications removed OS reloaded Restored from backup Application moved to another system Memory or disk space increased Moved behind a filtering router or firewall Hidden files detected and removed Trojan software detected and removed Left unchanged to monitor hacker Other	Details:
system(s) to trusted operation): Patches applied Scanners run Security software installed: Unneeded services and applications removed OS reloaded Restored from backup Application moved to another system Memory or disk space increased Moved behind a filtering router or firewall Hidden files detected and removed Trojan software detected and removed Left unchanged to monitor hacker Other	Details:
system(s) to trusted operation): Patches applied Scanners run Security software installed: Unneeded services and applications removed OS reloaded Restored from backup Application moved to another system Memory or disk space increased Moved behind a filtering router or firewall Hidden files detected and removed Trojan software detected and removed Left unchanged to monitor hacker Other	Details:

National CyberWatch Center Preparing for the Collegiate Cyber Defense Competition (CCDC): A Guide for New Teams and Recommendations for Experienced Players

Apparent source:	
IP address	
Location of host: Domestic	
☐ Foreign	
☐ Insider	
Primary system(s) involved:	
IP addresses or sub-net address	
OS version(s)	
NOS version(s)	
Other affected systems or networks (IPs and	IOSs):
Method of Operation:	Details:
☐ Tool used	
☐ Packet flood	
☐ Malicious packet ☐ IP Spoofing	
☐ Ports attacked	
Anything that makes this event unique	
Remediation	Details:
what was done to protect the system(s)):	
Application moved to another system	
Memory or disk space increased	
☐ Shadow server installed	
Moved behind a filtering router or firewall	
☐ Other	
og file excerpts:	
dditional comments:	