



Network Incident Report

United States Secret Service • Financial Crimes Division • Electronic Crimes Branch
Telephone: 202-406-5850 FAX: 202-406-9233 e-mail: ecb@secretsservice.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 _____
 • E-mail _____ • 7 x 24 contact information _____

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 gathering--recurring, 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: _____

Details for Malicious Code

Apparent source:

- Diskette, CD, etc.
- E-mail attachment
- Software download

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

Details:

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

Details:

Additional comments:

Details for Probes and Scans

Apparent source: <ul style="list-style-type: none">• IP address _____• Host name _____• Location of attacking host: _____<ul style="list-style-type: none"><input type="checkbox"/> Domestic<input type="checkbox"/> Foreign<input type="checkbox"/> Insider	
Primary system(s) / network(s) involved: <ul style="list-style-type: none">• IP addresses or sub-net addresses _____• OS version(s) _____• NOS version(s) _____	
Other affected systems or networks (IPs and OSs): 	
Method of Operation: <ul style="list-style-type: none"><input type="checkbox"/> Ports probed/scanned<input type="checkbox"/> Order of ports or IP addresses scanned<input type="checkbox"/> Probing tool<input type="checkbox"/> Anything that makes this probe unique	Details:
How detected: <ul style="list-style-type: none"><input type="checkbox"/> Another site<input type="checkbox"/> Incident response team<input type="checkbox"/> Log files<input type="checkbox"/> Packet sniffer<input type="checkbox"/> Intrusion detection system<input type="checkbox"/> Anomalous behavior<input type="checkbox"/> User	Details:
Log file excerpts: 	
Additional comments: 	

Details for Unauthorized Access

Apparent source: <ul style="list-style-type: none">• IP address _____• Host name _____• Location of attacking host: _____<ul style="list-style-type: none"><input type="checkbox"/> Domestic<input type="checkbox"/> Foreign<input type="checkbox"/> Insider	
Primary system(s) involved: <ul style="list-style-type: none">• IP addresses or sub-net addresses _____• OS version(s) _____• NOS version(s) _____	
Other affected systems or networks (IPs and OSs): 	
Avenue of attack: <ul style="list-style-type: none"><input type="checkbox"/> Sniffed/guessed/cracked password<input type="checkbox"/> Trusted host access<input type="checkbox"/> Vulnerability exploited<input type="checkbox"/> Hacker tool used<input type="checkbox"/> Utility or port targeted<input type="checkbox"/> Social engineering	Details:
Level of access gained-root/administrator, user 	
Method of operation of the attack (more detailed description of what was done): <ul style="list-style-type: none"><input type="checkbox"/> Port(s) or protocol(s) attacked<input type="checkbox"/> Attack tool(s) used, if known<input type="checkbox"/> Installed hacker tools such as rootkit, sniffers, 10phtcrack, zap<input type="checkbox"/> Site(s) hacker used to download tools<input type="checkbox"/> Where hacker tools were installed<input type="checkbox"/> Established a service such as IRC<input type="checkbox"/> Looked around at who is logged on<input type="checkbox"/> Trojanned, listed, examined, deleted, modified, created, or copied files<input type="checkbox"/> Left a backdoor<input type="checkbox"/> Names of accounts created and passwords used<input type="checkbox"/> Left unusual or unauthorized processes running<input type="checkbox"/> Launched attacks on other systems or sites<input type="checkbox"/> Other	Details:

Details for Unauthorized Access (continued)

<p>How detected:</p> <ul style="list-style-type: none"><input type="checkbox"/> Another site<input type="checkbox"/> Incident response team<input type="checkbox"/> Log files<input type="checkbox"/> Packet sniffer/intrusion detection software<input type="checkbox"/> Intrusion detection software<input type="checkbox"/> Anomalous behavior<input type="checkbox"/> User<input type="checkbox"/> Alarm tripped<input type="checkbox"/> TCP Wrappers<input type="checkbox"/> TRIPWIRED<input type="checkbox"/> Other	<p>Details:</p>
<p>Log file excerpts:</p>	
<p>Remediation (<i>what was done to return the system(s) to trusted operation</i>):</p> <ul style="list-style-type: none"><input type="checkbox"/> Patches applied<input type="checkbox"/> Scanners run<input type="checkbox"/> Security software installed:<input type="checkbox"/> Unneeded services and applications removed<input type="checkbox"/> OS reloaded<input type="checkbox"/> Restored from backup<input type="checkbox"/> Application moved to another system<input type="checkbox"/> Memory or disk space increased<input type="checkbox"/> Moved behind a filtering router or firewall<input type="checkbox"/> Hidden files detected and removed<input type="checkbox"/> Trojan software detected and removed<input type="checkbox"/> Left unchanged to monitor hacker<input type="checkbox"/> Other	<p>Details:</p>
<p>Additional comments:</p>	

Details for Denial-of-Service Incident

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 OSs):

Method of Operation:

- Tool used
- Packet flood
- Malicious packet
- IP Spoofing
- Ports attacked
- Anything that makes this event unique

Details:

Remediation

(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

Details:

Log file excerpts:

Additional comments: