Responding to a computer abuse complaint?

Now that you have received an abuse report, what should you do?

Note: At any time in this process, if you encounter suspected child pornography, terrorist activity or any other illegal behavior, stop and report to law enforcement.

Here is a list of some common types of problems/incidents that can generate an abuse report:

- Botnet
- Viruses
- Malware
- Spam (including Phishing and other spam variants)
- Copyright Violation
- Network Scan
- Configuration Error
- Open Mail Relay
- Open Proxy
- Intrusion
- Stalking, Harassment, Online Fraud and other Criminal Activities
- Webpage Defacement

Historically, the most common cause for an abuse report is an infected computer that is attempting to compromise others. Organized Crime syndicates now use viruses, spam, botnets and malware in general to make money for themselves. Infected computers should not be treated as only an inconvenience for the owner.

Contents of the abuse report

Hopefully the notice will include the offending IP address and some description of the offending traffic such as IP protocol (tcp, udp, icmp, etc), source and destination TCP or UDP ports and possibly a description of application behavior.

Finding the Offending Computer

Based on the offending IP address, identify the network perimeter security device that the traffic passes through. This device is typically a firewall that is performing network address translation (NAT).

- Ensure that logging is enabled on the perimeter firewall so that a log entry is created for all network traffic flowing through it. The logging level should provide sufficient detail to associate the abuse data with an internal IP address.

- If the abuse report is spam related, an internal mail server may provide the necessary log data to identify the source. In this case, the firewall logs may only indicate the internal mail server as the source.
- If the abuse report is network attack related, firewall logs can usually identify the responsible IP address.
- Review firewall and other system logs as required.
- Identify IP address associated with offending network traffic.

You may encounter difficulties in identifying the offending computer:

- Depending on DHCP lease times and the timeliness of the abuse report, the IP address identified in historical logs may have been assigned to a different computer. DHCP server logs can be used to identify the MAC address the system that was issued a particular IP address.
- Wireless networks may slow the progress of an investigation because of the mobile and intermittent nature of the connection. Wireless access point logs can be helpful to identify the MAC address of the computer in question.
- Many infected computers will only occasionally send malicious traffic. This pattern may require periodic log reviews for several days in order to identify the offending computer.

If historical data does not aid in identifying offending computer:

- Setup Wireshark on a mirrored port to capture packets to aid in identify computers talking on offending source or destination ports.
- Ntop or PRTG can be used to identify top talkers on the network. These will also require a mirror port configured.

Cleanup

Once the computer is identified and if the activity is not related to illegal activity, you are ready to begin corrective action. Because of the varied nature of these problems, only infected computer cleanup is described here:

- Ensure that the computer is running current anti-virus and anti-malware software. Scan the computer and clean infections.
- Apply all critical patches.
- If a critical system has been compromised (such as Active Directory or HR system), it should be evaluated to determine the security impact to credentials and sensitive data.
- Remove computer from the network and rebuild if efforts to clean the system are unsuccessful.

Reporting

Reply to the person reporting the incident regarding the general findings and the corrective actions that were taken. MCNC would also appreciate being included in the correspondence.

General information:

Responding to IT Security Incidents: http://technet.microsoft.com/en-us/library/cc700825.aspx

SANS SCORE Security Checklist for Windows: http://www.sans.org/score/checklists/ID_Windows.pdf

SANS Score Security Checklist for Linux: http://www.sans.org/score/checklists/ID_Linux.pdf

Wireshark: http://www.wireshark.org/

Ntop: http://www.ntop.org/

PRTG: http://www.paessler.com/prtg