Incident Response procedures for new malware

1) Within 30 minutes of activation, the incident response team will submit a sample to http://www.virustotal.com/ to gauge which of our AV vendors currently detect the sample.
2) Within two hours the Incident response team should have completed submission malware samples to all virus vendors. A short description of the malware's actions should be included. This will lessen the chance of confusion by the malware analysts.
3) Alert the security community by making malware submissions to the SANS Internet Storm Center and the ClamAV web sites.
4) Once incident numbers have been granted by the AV vendors, the incident response team will check Virustotal.com every 24 hours to see which of our AV vendors now detect the new malware. The incident response team will follow up every 24 hours with AV vendors who do not detect the malware until virus definitions have been fielded and a manual malware removal procedure has been established.
5) Once virus definitions have been fielded, the incident response team will work with each site security officer to ensure all branches of the company have updated their virus definitions.
6) The incident response team will distribute the manual malware removal procedure to all affected sites using the best available communications method within one hour of its acquisition.
7) The incident response team will remain activated until AV products have been properly updated and all infestations have been removed.

Appendix 1 – Preferred contact methods for AV vendors

Authentium

Preferred Method

Please call our Technical Support staff at +1 (561) 575-3200. At the voice prompt, press menu option number 2 during our daily office hours - 8:00am to 8:00pm EST Monday to Friday. You will be asked for your name, company, phone number, your Authentium product and version number, and known information related to the threat. After recording your information, the technical support person will reply with a tracking number called the "VxER" number. Please keep this number handy for any future inquiries into this incident.

Email

If you are unwilling or unable to call tech support, you can send the file directly to the Authentium virus labs. When sending a file to us, please use PKZIP or PGP to ensure transmission integrity. You can find our PGP key located at the bottom of the web page http://www.authentium.com/threatmatrix/submitsample.html. Send sample to virus@authentium.com

NOTE: For security purposes, please send the sample as a password-protected zip file, and include the password in the email.

FTP

Follow the instructions below. NOTE: Make sure you upload the file in binary mode.

* Connect to ftp://ftp.commandsoftware.com
* Log in as "SAMPLE".
* Change to the "/incoming/virus" directory.
* Upload the files.
* NOTE: You *must* use a Passive FTP client.

McAfee

Preferred method

Log in to McAfee WebImmune web site at https://www.webimmune.net/default.asp and follow instructions. Create a new user if you do not have a current user ID.

Sophos

Preferred method

Use Sophos malware submission web page at http://sophos.com/support/samples/.

Symantec

Preferred method

Use Symantec SecurityResponse malware submissions web page at http://www.symantec.com/business/security_response/submitsamples.jsp. If the ISOC uses Symantec AV, they should receive faster response by using SAV's built-in virus submission software. Information for Gold and Platinum support customers is on the malware submissions web page.

Alternate method

Use the SAV home users manual malware submissions web page listed at https://submit.symantec.com/websubmit/retail.cgi.

Security Community Reporting

Reporting virus incidents to security community resources offer ways to help others deal with fast moving malware and could help in developing manual malware removal procedures. Here are two such sites:

SANS Internet Storm Center

Preferred method

Submit malware samples and malware descriptions to the SANS Internet Storm Center contact page at http://isc.sans.org/contact.html.

ClamAV Open Source Project

Preferred method

Submit malware samples and malware descriptions to the ClamAV Open Source Project malware samples page at http://cgi.clamav.net/sendvirus.cgi.