

**Attachment**  
**Table 1 – Malicious Software, Tools, Hash(s) Value, and Registry Key**  
**January 29, 2009**

<b>Filename</b>	<b>Purpose</b>	<b>MD5/SHA-1 Hash(s) or Registry Key</b>
appsqlio.exe	Reverse shell tool	387cda6eb91f0b3a054de20c02320338
obsqlio.exe	SQL output redirector	f640e53718bc83cb8bb10b1eafb50edf
blobsqlio.exe	Packed version of gsecdump	959523fc10584da9bfb31a524ff472aa
sn.exe	Packet sniffer	e07b83abda5b566b3e9a30515a59ecc3
msdtsc.exe	Packet sniffer	4724103b13e6ce832fbb2c08a419eac6
svclhost.exe	Network communication tool	da4ab50185c7b246d1d2c8fa7bd7a5ed
rexesvr.exe	Command line execution	003f6cda98a40529cc87fd1387714fd7
svcl.exe	Renamed version of sn.exe	e07b83abda5b566b3e9a30515a59ecc3
eqslquery.exe	Script that automates the installation of rexesvr.exe	bc354dcf5221aea9fae8a3283c09504d
rarx.exe	Compression tool	fd729427144044730c572fd5b9be7dd9
Soft.exe	Backdoor	ea75939da539a3879e5b442b11b51f24
Isasstd.exe	Backdoor	07536e77ece9e70f5bf3d6f357c77b04
Isasstm.exe	Backdoor	e2736b8e0628a07fc3a6dcccad99245e
smn.exe	Backdoor	b0ff54c190455feda3f67b53c4a4453d
mstsk.exe	Utility to inject code on running processes	ddfd9073a5f222e223f5f2156c71629d