Key

Color	Description
	Anti-virus activity
	My commentary
	Event log
	File system timestamps
	IDS logs (mostly Bro)
	Windows Prefetch cache (program execution)
	Web history (cookies, history, etc)

Timeline

time	type	path/details
02/19/09 7:47:25	**comment**	**Here's the beginning of the day in question…it starts with the system booting. See the key above for an explanation of the colors (or look at the "type" column). This is "boiled down" commentary from nearly 2,000 events from a short slice of time from a forensic analysis of a compromised computer, which itself was "boiled down" from hundreds of thousands of events extracted from the computer and our logs.**
02/19/09 7:47:26	event log	The system boots, user logs in, starts to work
02/19/09 9:26:14	**comment**	**The fun (probably) starts here…**
02/19/09 9:26:15	web history	Web history shows that the user went to a high school wrestling web site and apparently got infected through a malicious ad, two PDF files are accessed
02/19/09 9:28:13	**comment**	**Banner[1], [2].pdf are created…these both contain malware (currently not identified by virustotal). The system had a version of Adobe Reader installed that had an exploitable vulnerability.**
02/19/09 9:28:14	file system	Two malicious pdf files are downloaded (file system timestamps)
02/19/09 9:28:17	ids logs	IDS (bro) detects two PDF downloads via web from one of the ad sites references from the aforementioned web site
02/19/09 9:28:20	ids logs	Bro shows download of Windows executable called xrun.tmp
02/19/09 9:28:57	**comment**	**Got xrun.tmp, and apparently runs something called rn.tmp**
02/19/09 9:28:57	prefetch cache	Execute RN.TMP-36CAACC4.pf
02/19/09 9:29:40	web history	A variety of cookies are created, evidence of access to a bunch of sites. not clear what all of these are.
02/19/09 9:37:55	**comment**	**Something apparently created prun.tmp, rasesnet.tmp and winvsnet.tmp, these were deleted by the A-V system**
02/19/09 9:37:56	anti-virus logs	anti-virus deletes prun.tmp (Generix.dx), rasesnet.tmp (Vundo) and winsvnet.tmp (Generic Downloader.X)
02/19/09 9:43:59	web history	More web cookie activity
02/19/09 9:44:07	**comment**	**More bad stuff is created, run…A-V finds what would appear to be a by-product…**
02/19/09 9:44:08	file system	Create prunnet.exe
02/19/09 9:44:24	prefetch cache	prunnet.exe executed (twice?)
02/19/09 9:44:33	anti-virus logs	Cleans ecomsnraxw.tmp (W32/Virut.n.gen)
02/19/09 9:44:37	ids logs	downloads windows executable
02/19/09 9:44:38	ids logs	downloads another windows executable
02/19/09 9:44:48	**comment**	**The seneka rootkit is installed!**
02/19/09 9:44:49	file system	Create senekalhtijurw.sys - part of the Seneka rootkit
02/19/09 9:44:57	anti-virus logs	Deletes wcenoxarms.tmp (Generic Downloader.x)
02/19/09 9:45:00	file system	Create senekafqqjlktq.dll - part of the Seneka rootkit
02/19/09 9:45:10	file system	Create winsinstall.exe
02/19/09 9:45:13	ids logs	Windows executable downloaded
02/19/09 9:46:01	anti-virus logs	Will delete apstpldr.dll[1].htm (Vundo)
02/19/09 9:46:10	web history	Web history shows a lot of random web activity here.
02/19/09 9:47:20	file system	Create prun.tmp, geBtSlyX.dll and ssqQkHBq.dll
02/19/09 9:47:35	file system	Create fccbAQkj.bat and qoMfdaYs.bat
02/19/09 9:47:46	ids logs	Download two Windows executables
02/19/09 9:55:46	file system	Access prun.tmp - executed?
02/19/09 9:55:48	file system	Create rqRKEUkK.dll
02/19/09 9:55:49	file system	Create vtUkhiHb.bat
02/19/09 9:55:54	ids logs	Download another Windows executable
02/19/09 10:01:20	file system	Create cbXQiFxw.dll
02/19/09 10:01:23	ids logs	Download Windows executable
02/19/09 10:01:25	file system	Create ojacobk.sys
02/19/09 10:01:26	**comment**	**Uh-oh…strange services starting are always a Bad Sign**
02/19/09 10:01:26	event log	The irzylwcf started
02/19/09 10:01:26	file system	Create irzylwcf
02/19/09 10:01:41	file system	Create, access romxwcenas.tmp
02/19/09 10:01:45	prefetch cache	Execute ROMXWCENAS.TMP-3639D719.pf
02/19/09 10:01:57	prefetch cache	Execute SXAEWRMCON.TMP-234ED43A.pf
02/19/09 10:02:01	file system	Create, access swxaoermnc.tmp
02/19/09 10:02:04	file system	Create wvUmjlbx.dll
02/19/09 10:02:08	prefetch cache	Execute SWXAOERMNC.TMP-316E61E9.pf
02/19/09 10:02:11	ACMW	Create jkkHBTJD.bat
02/19/09 10:02:12	file system	Create mcrh.tmp
02/19/09 10:02:17	prefetch cache	Execute NMOXWAESRC.TMP-0868916F.pf
02/19/09 10:02:26	ids logs	Download Windows executable
02/19/09 10:02:27	file system	Create mcrh.tmp
02/19/09 10:02:29	**comment**	**Anti-virus is stopped…sigh**
02/19/09 10:02:29	event log	Anti-virus is paused, then stopped
02/19/09 10:02:29	ids logs	Download Windows executable
02/19/09 10:02:30	file system	Create VRT140.tmp
02/19/09 10:02:30	file system	Create gcnogcva.sys
02/19/09 10:02:32	file system	Create VRT140.tmp
02/19/09 10:02:33	ids logs	Download Windows executable
02/19/09 10:02:34	file system	Create xccef090131.exe
02/19/09 10:02:34	file system	Create xccefb090131.scr
02/19/09 10:02:35	ids logs	Download Windows executable
02/19/09 10:02:36	prefetch cache	Execute VRT13F.TMP-19B35236.pf
02/19/09 10:02:37	file system	Create 143.tmp
02/19/09 10:02:39	prefetch cache	execute VRT141.TMP-153583A6.pf
02/19/09 10:02:40	**comment**	**Some strange service failed to start - also a Bad Sign**
02/19/09 10:02:40	event log	The zmzfozjg service failed to start
02/19/09 10:02:44	file system	Create xccwinsys.ini
02/19/09 10:02:48	prefetch cache	Execute VRT141.TMP-153583A6.pf
02/19/09 10:02:50	file system	Create xccef090131.exe
02/19/09 10:02:50	file system	Create phqghume.sys
02/19/09 10:02:51	file system	Create lgate[1].htm
02/19/09 10:02:52	file system	Create lgate[1].htm
02/19/09 10:02:52	file system	Create xccefb090131.scr
02/19/09 10:02:52	file system	Create 143.tmp
02/19/09 10:02:54	file system	Create irzylwcf
02/19/09 10:02:54	file system	Create xccdf16_090131a.dll
02/19/09 10:02:54	file system	Create xccdfb16_090131.dll
02/19/09 10:02:55	**comment**	**Another strange service fails to start…**
02/19/09 10:02:55	event log	The aylnlfdx service failed to start
02/19/09 10:02:56	file system	Create ge[1].txt (Windows executable)
02/19/09 10:02:56	file system	Modify imapi.exe
02/19/09 10:02:58	file system	Modify, access ge[1].txt
02/19/09 10:02:58	file system	Create 145.tmp
02/19/09 10:02:58	file system	Modify services.exe
02/19/09 10:02:59	file system	Create, access em[1].txt
02/19/09 10:02:59	file system	Modify werclsid.exe
02/19/09 10:02:59	ids logs	Download Windows executable (ge[1].txt)
02/19/09 10:03:00	file system	Modify 145.tmp
02/19/09 10:03:00	file system	Modify CcEvtSvc.exe
02/19/09 10:03:02	ids logs	Download Windows executable
02/19/09 10:03:04	file system	Create CcEvtSvc.exe
02/19/09 10:03:10	**comment**	**The firewall has stopped and the CcEvtSvc service starts…**
02/19/09 10:03:10	event log	Application layer gateway service entered stopped state
02/19/09 10:03:10	event log	Windows firewall service entered the stopped state
02/19/09 10:03:13	event log	CcEvtSvc service started
02/19/09 10:03:14	file system	Create abb[1].txt (Windows executable)
02/19/09 10:03:14	file system	Create services.exe
02/19/09 10:03:14	file system	Create netsh.exe
02/19/09 10:03:16	file system	Modify abb[1].txt
02/19/09 10:03:17	file system	Create 147.tmp
02/19/09 10:03:17	file system	Create reader_s.exe
02/19/09 10:03:17	ids logs	Download Windows executable (abb.txt)
02/19/09 10:03:18	file system	Create reader_s.exe
02/19/09 10:03:23	file system	Create, access al[1].txt
02/19/09 10:03:24	file system	Create 148.tmp
02/19/09 10:03:24	file system	Create index[1]
02/19/09 10:03:24	file system	Modify 147.tmp
02/19/09 10:03:24	file system	Modify al[1].txt
02/19/09 10:03:25	file system	Modify index[1]
02/19/09 10:03:25	file system	Create doc[1].txt
02/19/09 10:03:25	file system	Create pydesepr.dll
02/19/09 10:03:25	file system	Write jdfjpl.dll
02/19/09 10:03:26	file system	Modify jdfjpl.dll
02/19/09 10:03:26	file system	Modify pydesepr.dll
02/19/09 10:03:26	ids logs	Download Windows executable (al[1].txt)
02/19/09 10:03:27	ids logs	Download Windows executable
02/19/09 10:03:27	file system	Create jdfjpl.dll
02/19/09 10:03:28	ids logs	Download Windows Executable (doc.txt)
02/19/09 10:03:30	**comment**	**Automatic updates have been disabled…**
02/19/09 10:03:46	prefetch cache	Execute WUAUCLT.EXE-1360D60A.pf
02/19/09 10:03:49	event log	Automatic update service entered the stopped state
02/19/09 10:05:08	ids logs	Connections to web services on strange ports on 3 external IPs
02/19/09 10:05:28	web history	More random web traffic
02/19/09 10:05:31	file system	Modify msmsgs.exe
02/19/09 10:05:57	file system	Create, access upd105320[1]
02/19/09 10:05:57	file system	Create vgyixcnu.dll
02/19/09 10:06:00	ids logs	Download Windows Executable
02/19/09 10:06:07	file system	Modify, access doc[1].txt
02/19/09 10:06:07	file system	Modify 148.tmp
02/19/09 10:06:12	file system	Create uncxiygv.ini
02/19/09 10:06:12	file system	Create lgsztotz.exe
02/19/09 10:06:22	file system	Modify uncxiygv.ini
02/19/09 10:16:11	**comment**	**The system reboots after a crash**
02/19/09 10:16:12	event log	Reboot events due to a bug check
02/19/09 10:17:05	file system	Create ethqqaeg.sys
02/19/09 10:17:11	file system	Modify SbClientManager.exe
02/19/09 10:17:19	ids logs	Web traffic on strange ports to 2 external IPs
02/19/09 10:17:25	file system	Modify mdm.exe
02/19/09 10:17:45	**comment**	**System starts sending spam…I forget how we knew that (probably observed)**
02/19/09 10:17:52	file system	Modify acrodist.exe
02/19/09 10:17:52	file system	Modify fxsvc.exe
02/19/09 10:17:58	file system	Modify agent.exe
02/19/09 10:18:16	file system	Modify xccwinsys.ini
02/19/09 10:18:52	**comment**	**Due to the concurrent spam/SMTP sessions…**
02/19/09 10:18:53	event log	Too many concurrent TCP sessions
02/19/09 10:19:14	file system	Modify dumprep.exe
02/19/09 10:19:15	web history	More web activity
02/19/09 10:20:00	event log	system rebooted?
02/19/09 10:20:04	ids logs	Web traffic on strange ports to 2 external IPs
02/19/09 10:20:27	file system	Modify userinit.exe
02/19/09 10:20:59	file system	Modify dwwin.exe
02/19/09 10:21:13	ids logs	Download Windows executable
02/19/09 10:21:25	event log	DSProct service started?
02/19/09 10:21:37	file system	Modify senekakjlpapjct.dat
02/19/09 10:23:21	ids logs	Web traffic on strange ports to 1 external IP
02/19/09 10:23:54	ids logs	SMTP protocol violation detected
02/19/09 10:25:07	ids logs	Web traffic on strange ports to 2 external IPs
02/19/09 10:26:52	event log	CcEvtSvc service terminated unexpectedly.
02/19/09 10:27:24	ids logs	Web traffic on strange ports to 1 external IP
02/19/09 10:28:55	ids logs	Web traffic on strange ports to 2 external IPs
02/19/09 10:30:23	file system	Modify MPNOTIFY.EXE
02/19/09 10:30:38	prefetch cache	Execute WGATRAY.EXE-350D4455.pf
02/19/09 10:30:51	**comment**	**At this point Bro is detecting many thousands of spam messages sent from this computer**