	Timestamp		Device	User	Event	Explanation
	Beginning	***End***				
	All times are UCT					
1	***12/29/2017 20:58:00***	***01/04/2018 16:40:49***				*The entire incident*
	12/29/2017 00:00:00					
2	12/29/2017 20:58:23	12/29/2017 20:58:31		P. Brand (p.brand@at-usa[.]com)	email	A spearphishing email was received by P. Brand, D. Walker, M. Land, and S. Adams.
2			LAB-Win7-01	S. Adams (s.adams@at-usa[.]co)	email	A spearphishing email was received by P. Brand, D. Walker, M. Land, and S. Adams.
2			LAB-Win10-03	M. Land (m.land@at-usa[.]co)	email	A spearphishing email was received by P. Brand, D. Walker, M. Land, and S. Adams.
2			LAB-Win10-04	D. Walker (d.walker@at-usa[.]co)	email	A spearphishing email was received by P. Brand, D. Walker, M. Land, and S. Adams.
3	12/29/2017 21:24:23	12/29/2017 21:49:14	LAB-Win7-01	S. Adams (s.adams@at-usa[.]co)	Execution Event	The employee was targeted by the attacker's spearphish email and was exposed to a watering hole website (ciso[.]guide) re-directing traffic to the EK (Rig) landing page. While the re-direction was successful the attempted infection failed. Four payloads (bilo439.exe, bilo494.exe, bilo161.exe, bilo467.exe) were delivered. None of these payloads were executed, and LAB-Win7-01 remained uninfected.
4	12/29/2017 21:40:33	12/29/2017 21:57:06	LAB-Win10-03	M. Land (m.land@at-usa[.]co)	Execution Event	The employee was targeted by the attacker's spearphish email and was exposed to a watering hole website (ciso[.]guide) re-directing traffic to the EK (Rig) landing page.
5	12/29/2017 22:50:07	12/29/2017 23:11:16	Daniel-PC	Daniel (Daniel@at-usa[.]co)	Execution Event	A single payload (bilo400.exe) was manually delivered / implemented onto Daniel-PC\Daniel.
6	12/29/2017 23:14:33		Daniel-PC	Daniel (Daniel@at-usa[.]co)	Execution Event	The payload executed resulting in the infection of the device with the Ramnit banking trojan.
7	12/29/2017 23:15:03	12/29/2017 23:21:49	Daniel-PC	Daniel (Daniel@at-usa[.]co)	Execution Event	Copies of Ramnit executables created (Daniel-PC\Daniel)
8	12/29/2017 23:15:03	01/04/2018 14:54:07	Daniel-PC	Daniel (Daniel@at-usa[.]co)	Execution Event	Ramnit registry modifications
9	12/29/2017 23:16:10	12/29/2017 23:37:17	LAB-Win10-04	D. Walker (d.walker@at-usa[.]co)	Execution Event	The employee was targeted by the attacker's spearphish email and was exposed to a watering hole website (ciso[.]guide) re-directing traffic to the EK (Rig) landing page.
10	12/29/2017 23:16:32	12/29/2017 23:17:25	Daniel-PC	Daniel (Daniel@at-usa[.]co)	C2 Activity	Modules downloaded from Ramnit C2 server
11	12/29/2017 23:16:34	12/29/2017 23:45:51	Daniel-PC	Daniel (Daniel@at-usa[.]co)	C2 Activity	The Ramnit malware established persistence on Daniel-PC and initially connected to the Ramnit C2 server (ckkxyupextanlvcrdig[.]com
	01/02/2018 00:00:00					
12	01/02/2018 04:13:28	01/02/2018 04:19:15	Daniel-PC	Waxwing (waxwing@at-usa[.]co)	Execution Event	Copies of Ramnit executables created (Daniel-PC\Waxwing)
13	01/02/2018 04:13:58	01/02/2018 04:14:51	Daniel-PC	Waxwing (waxwing@at-usa[.]co)	C2 Activity	Modules downloaded from Ramnit C2 server
14	01/02/2018 04:14:00	01/02/2018 04:42:44	Daniel-PC	Waxwing (waxwing@at-usa[.]co)	C2 Activity	Ramnit second persistent execution (Waxwing user profile infected)
15	01/02/2018 05:39:20	01/02/2018 05:39:55	Daniel-PC	Daniel (Daniel@at-usa[.]co) Waxwing (waxwing@at-usa[.]co)	C2 Activity	Last successful connection with the malware (Ramnit) server
	01/04/2018 00:00:00					
16		1/4/2018 16:40:49	Daniel-PC	Daniel (Daniel@at-usa[.]co) Waxwing (waxwing@at-usa[.]co)	C2 Activity	Last attempted (but unsuccessful) connection with the malware (Ramnit) server
17	1/4/2018 16:40:55		Daniel-PC	C:\dfir-files\memory\infected_Daniel-PC[.]vmem	Memory	Memory image of Daniel-PC acquired