2024

SECURITY REPORT

Endpoint Forensics with memory dumps on windows os (Mr-Robot)

github.com/Abdibimantara abdibimantara.github.io abdibimantara91@gmail.com

Daftar Isi

Executive Summary

Ditemukannya 3 device yang teinfeksi serangan malware. Dimana serangan malware tersebut berhasil masuk melalui website yang terindikasi sebagai phishing. Device tersebut diketahui sudah berhasil tercompromised dan berhasil di remote oleh attacker

Latar Belakang

Tim Security Opreation Center (SoC) mendapati adanya laporan dari user internal dengan divisi non IT. Dimana user tersebut melaporkan adanya temuan suspicious yaitu device pribadinya (laptop) mulai bertindak aneh setelah menerima email mencurigakan untuk pembaruan keamanan. Dari hasil laporan tersebut, tim SoC mengeskalasikan kepada tier 3 analyst untuk dilalukan proses endpoint forensic guna mengetahui apa yang sebenarnya terjadi.

Lab Environment

Dalam proses forensic tersebut, tim tier 3 analyst dari Security operatin Center (SoC) menggunakan beberapa tools forensic seperti Volatility dan environment terisolasi guna membatasi adanya koneksi internet dari device yang digunakan selama forensic tersebut. Selain itu system operasi yang digunakan sebagai landasan forensic adalah system operasi berbasis linux, yaitu kali linux 2024.

Analysis Incident

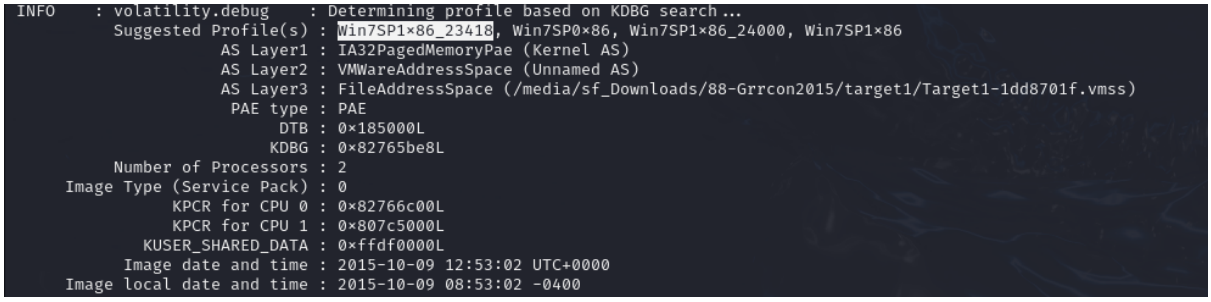
Informasi awal didapatkan dari tier 1 tim Security operation Center (SoC), dimana adanya user internal dari divisi non IT melaporkan adanya anomaly activity pada device (laptop) pribadinya. Anomaly tersebut berupa adanya aktivitas yang tidak seperti biasanya, setelah menerima email mencurigakan untuk pembaruan keamanan. Laporan tersebut ditindaklanjutin secara langsung oleh tim SOC, dengan melakukan eskalasi ke tier 3 untuk dilakukan investigasi secara mendetail.

Untuk rekomendasi awal, tim SoC memberikan saran kepada user internal tersebut untuk memutuskan koneksi internet dari device terinfeksi tersebut. Sehingga meminimalisir adanya penyebaran kepada device lainnya melalui koneksi internet.

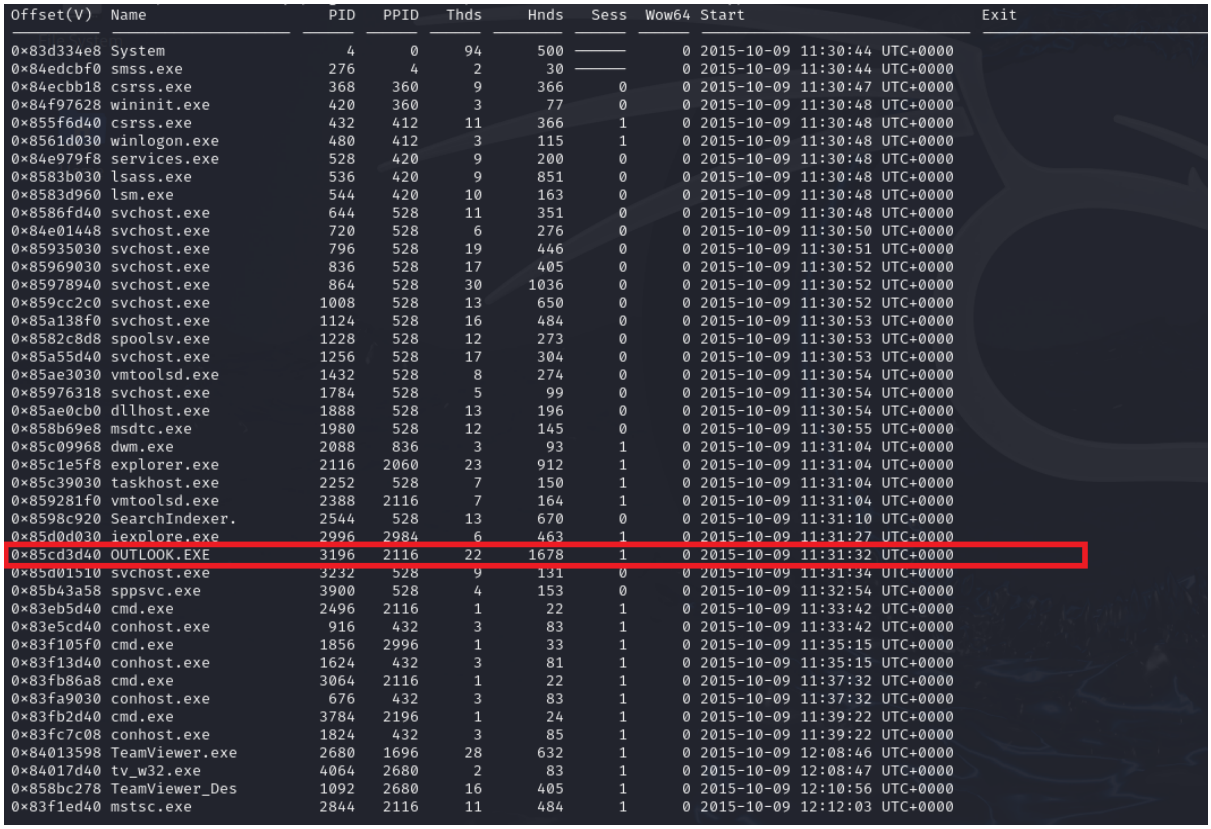
Langkah awal tim SoC melakukan imaging file terlebih dahulu pada device terkait. Dimana proses tersebut akan menghasilkan beberapa file yang dapat digunakan selama masa investigasi.

Setelah membuat file image tersebut, tim SoC memulai fase investigasi. Dalam fase investigasi tersebutm tim SoC umumnya menggunakan tools opensource Volatility. Volatility sendiri digunakan untuk melakukan untuk membantu dalam analisis data memori dari suatu system yang sedang berjalan (RAM dumps).

Penelusuran diawali dengan melakukan analisa pada image file dari device terinfeksi di Machinename Target1. Menggunakan tool volatility, dilakukan identifikasi system operasi yang digunakan, dan diketahui bawah system operasi dari device tersebut adalah Win7SP1x86.

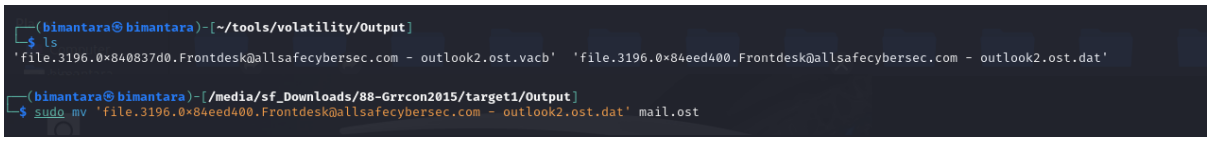


Setelah berhasil mengetahui system operasi yang digunakan pada device tersebut, penelusuran dilanjutkan dengan melakukan identifikasi list proses yang sedang berjalan pada device terinfeksi tersebut. Dimana dari hasil penelusuran, didaptkan hasil bahwa benar terdapat process Outlook.exe yang sedang berjalan di device tersebut. Hal ini memperkuat dugaan bahwa user yang menggunakan device tersebut benar terkena mail phising.

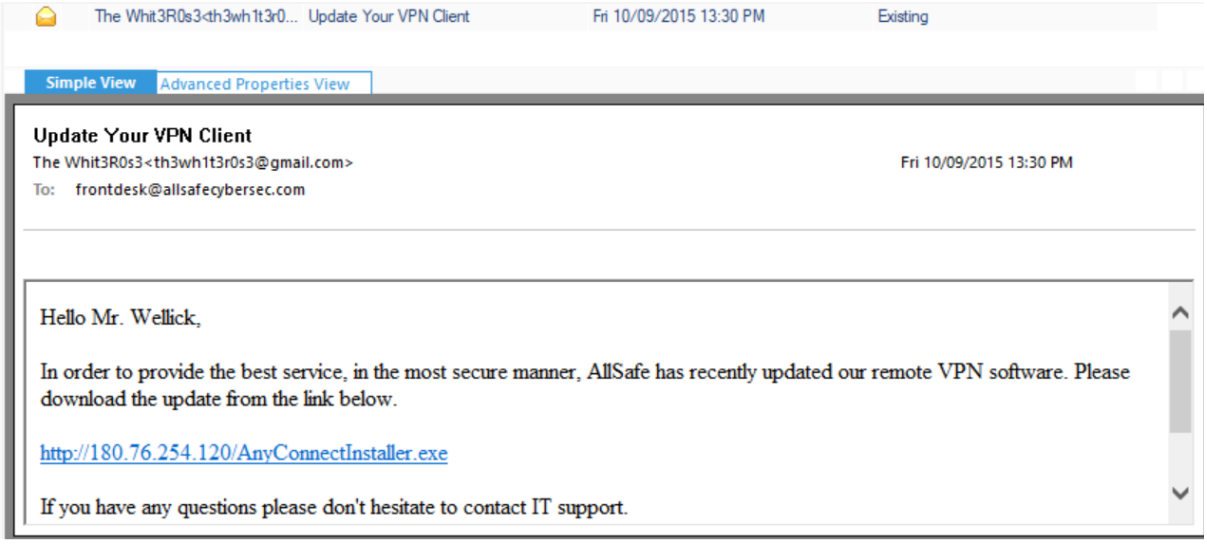


Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
0×83d334e8	System	4	0	94	500	———	0	2015-10-09 11:30:44 UTC+0000	
0×84edcbf0	smss.exe	276	4	2	30	———	0	2015-10-09 11:30:44 UTC+0000	
0×84ecbb18	csrss.exe	368	360	9	366	0	0	2015-10-09 11:30:47 UTC+0000	
0×84f97628	wininit.exe	420	360	3	77	0	0	2015-10-09 11:30:48 UTC+0000	
0×855f6d40	csrss.exe	432	412	11	366	1	0	2015-10-09 11:30:48 UTC+0000	
0×8561d030	winlogon.exe	480	412	3	115	1	0	2015-10-09 11:30:48 UTC+0000	
0×84e979f8	services.exe	528	420	9	200	0	0	2015-10-09 11:30:48 UTC+0000	
0×8583b030	lsass.exe	536	420	9	851	0	0	2015-10-09 11:30:48 UTC+0000	
0×8583d960	lsm.exe	544	420	10	163	0	0	2015-10-09 11:30:48 UTC+0000	
0×8586fd40	svchost.exe	644	528	11	351	0	0	2015-10-09 11:30:48 UTC+0000	
0×84e01448	svchost.exe	720	528	6	276	0	0	2015-10-09 11:30:50 UTC+0000	
0×85935030	svchost.exe	796	528	19	446	0	0	2015-10-09 11:30:51 UTC+0000	
0×85969030	svchost.exe	836	528	17	405	0	0	2015-10-09 11:30:52 UTC+0000	
0×85978940	svchost.exe	864	528	30	1036	0	0	2015-10-09 11:30:52 UTC+0000	
0×859cc2c0	svchost.exe	1008	528	13	650	0	0	2015-10-09 11:30:52 UTC+0000	
0×85a138f0	svchost.exe	1124	528	16	484	0	0	2015-10-09 11:30:53 UTC+0000	
0×8582c8d8	spoolsv.exe	1228	528	12	273	0	0	2015-10-09 11:30:53 UTC+0000	
0×85a55d40	svchost.exe	1256	528	17	304	0	0	2015-10-09 11:30:53 UTC+0000	
0×85ae3030	vmtoolsd.exe	1432	528	8	274	0	0	2015-10-09 11:30:54 UTC+0000	
0×85976318	svchost.exe	1784	528	5	99	0	0	2015-10-09 11:30:54 UTC+0000	
0×85ae0cb0	dllhost.exe	1888	528	13	196	0	0	2015-10-09 11:30:54 UTC+0000	
0×858b69e8	msdtc.exe	1980	528	12	145	0	0	2015-10-09 11:30:55 UTC+0000	
0×85c09968	dwm.exe	2088	836	3	93	1	0	2015-10-09 11:31:04 UTC+0000	
0×85c1e5f8	explorer.exe	2116	2060	23	912	1	0	2015-10-09 11:31:04 UTC+0000	
0×85c39030	taskhost.exe	2252	528	7	150	1	0	2015-10-09 11:31:04 UTC+0000	
0×859281f0	vmtoolsd.exe	2388	2116	7	164	1	0	2015-10-09 11:31:04 UTC+0000	
0×8598c920	SearchIndexer.	2544	528	13	670	0	0	2015-10-09 11:31:10 UTC+0000	
0×85d0d030	iexplore.exe	2996	2984	6	463	1	0	2015-10-09 11:31:27 UTC+0000	
0×85cd3d40	OUTLOOK.EXE	3196	2116	22	1678	1	0	2015-10-09 11:31:32 UTC+0000	
0×85d01510	svchost.exe	3232	528	9	131	0	0	2015-10-09 11:31:34 UTC+0000	
0×85b43a58	sppsvc.exe	3900	528	4	153	0	0	2015-10-09 11:32:54 UTC+0000	
0×83eb5d40	cmd.exe	2496	2116	1	22	1	0	2015-10-09 11:33:42 UTC+0000	
0×83e5cd40	conhost.exe	916	432	3	83	1	0	2015-10-09 11:33:42 UTC+0000	
0×83f105f0	cmd.exe	1856	2996	1	33	1	0	2015-10-09 11:35:15 UTC+0000	
0×83f13d40	conhost.exe	1624	432	3	81	1	0	2015-10-09 11:35:15 UTC+0000	
0×83fb86a8	cmd.exe	3064	2116	1	22	1	0	2015-10-09 11:37:32 UTC+0000	
0×83fa9030	conhost.exe	676	432	3	83	1	0	2015-10-09 11:37:32 UTC+0000	
0×83fb2d40	cmd.exe	3784	2196	1	24	1	0	2015-10-09 11:39:22 UTC+0000	
0×83fc7c08	conhost.exe	1824	432	3	85	1	0	2015-10-09 11:39:22 UTC+0000	
0×84013598	TeamViewer.exe	2680	1696	28	632	1	0	2015-10-09 12:08:46 UTC+0000	
0×84017d40	tv_w32.exe	4064	2680	2	83	1	0	2015-10-09 12:08:47 UTC+0000	
0×858bc278	TeamViewer_Des	1092	2680	16	405	1	0	2015-10-09 12:10:56 UTC+0000	
0×83f1ed40	mstsc.exe	2844	2116	11	484	1	0	2015-10-09 12:12:03 UTC+0000	

Setelah diketahui bahwa terdapat process Outlook.exe yang berjalan pada device terinfeksi, Tim Security segera melakukan pelusuran terkait dengan file.ost. File .ost sendiri merupakan file data yang digunakan Microsoft Outlook untuk menyimpan salinan lokal informasi kotak surat. Sehingga dari file.ost tersebut kita dapat mengetahui Salinan email apa saja yang terkirim kepada device terkait.

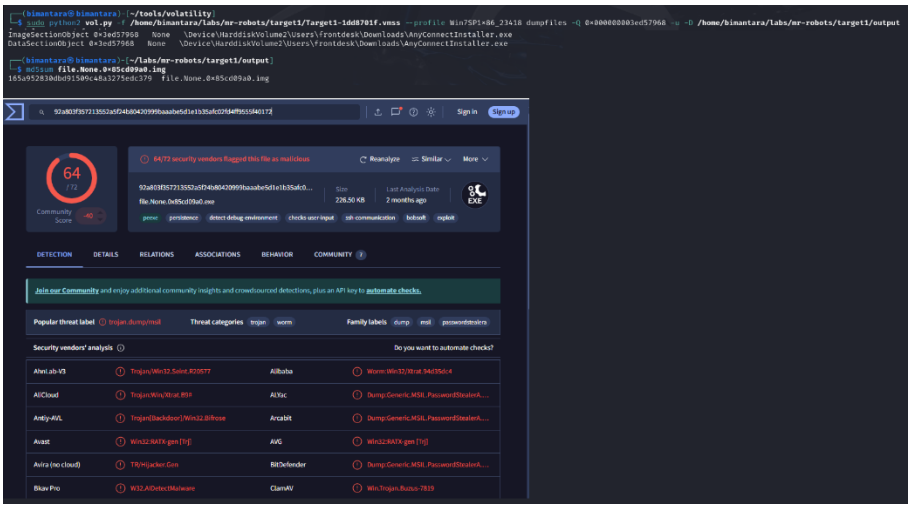


Terdapat file dengan nama “'file.3196.0x84eed400.Frontdesk@allsafecybersec.com - outlook2.ost.dat'”. File data tersebut merupakan file sering digunakan untuk menyimpan data mentah atau metadata tambahan dari file utama. Sehingga dalam penelusuran kali ini, akan berfokus pada file tersebut. File tersebut dilakukan process rename menjadi “mail.ost” sehingga dapat dibuka dengan tools tambahan yaitu kernel view ost.



Berdasarkan bantuan dari tools Kerner OST viewer, diketahui bahwa terdapat mail masuk pada folder inbox dengan subject mail yaitu “Update your VPN Client” pada 10 September 2015 jam 13.30 PM dengan pengirimnya berasal dari email **th3wh1t3 r0s3@gmail(.)com.** Dimana dari hasil temuan tersebut diketahui bahwa bad actor tersebut meminta kepada korban untuk segera melakukan installasi update aplikasi VPN client dengan mengklik malicious url dengan nama “AnyConnectInstaller.exe”

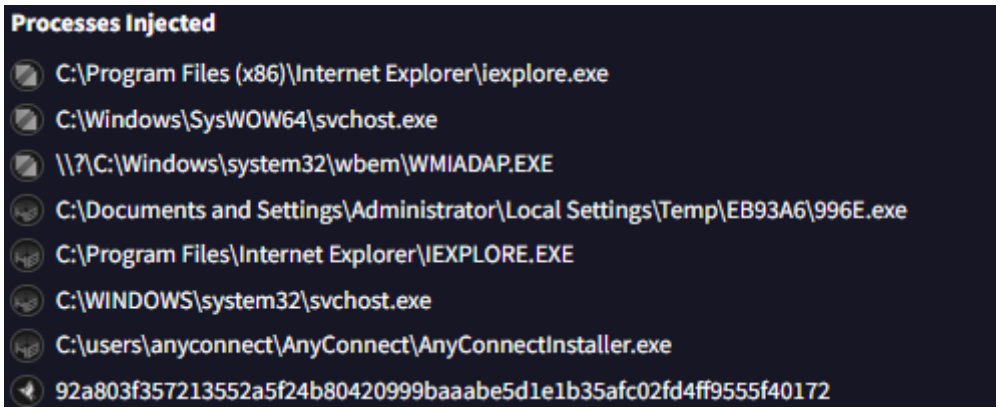
Setelah berhasil mengidentifikasi terkait dengan email phishing tersebut, didapatkan malicious file yang teridentifikasi sebagai “AnyConnectInstaller.exe”. File .exe tersebut selanjutnya akan dilakukan process dump untuk dilakukan Analisa secara singkat untuk mengentahui file tersebut termasuk jenis malware apa.



Berdasarkan penelusuran, diketahui bahwa hash dari file .exe tersebut adalah 165a952830dbd91509c48a3275edc379, dan setelah dilakukan pengecekkan melalui

virustotals, didapatkan bahwa file tersebut berhubungan dengan jenis malware Xrat atau biasa disebut dengan Extreme RAT.

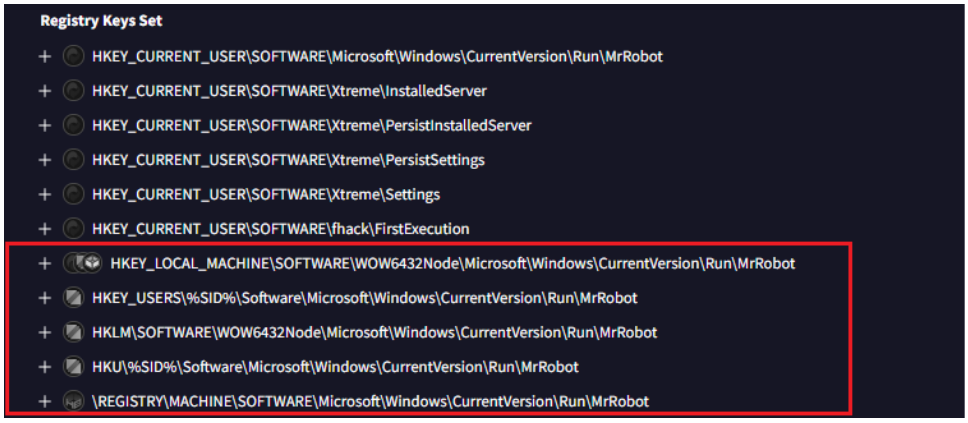
DIlihat dari informasi virustotals, terdapat process injection yang dilakukan oleh jenis malware ini. Process injection merupakan teknik yang digunakan untuk menyuntikkan (inject) kode berbahaya ke dalam proses yang sedang berjalan di memori sistem. Teknik ini sering digunakan oleh penyerang, malware, atau software untuk menyembunyikan aktivitasnya, meningkatkan hak akses, atau menghindari deteksi oleh solusi keamanan seperti antivirus atau endpoint detection and response (EDR). Umumnya process injection dimulai dari iexplore.exe dengan memanfaatkan javascript yang biasa digunakan pada web yang berisi konten phishing.




```
┌──(bimantara㉿bimantara)-[~/tools/volatility]
└─$ python2 vol.py -f /home/bimantara/labs/mr-robots/target1/Target1-1dd8701f.vmss --profile Win7SP1x86_23418 pstree
 0x85d0d030:iexplore.exe                2996   2984      6    463 2015-10-09 11:31:27 UTC+0000
. 0x83f105f0:cmd.exe                    1856   2996      1     33 2015-10-09 11:35:15 UTC+0000
```

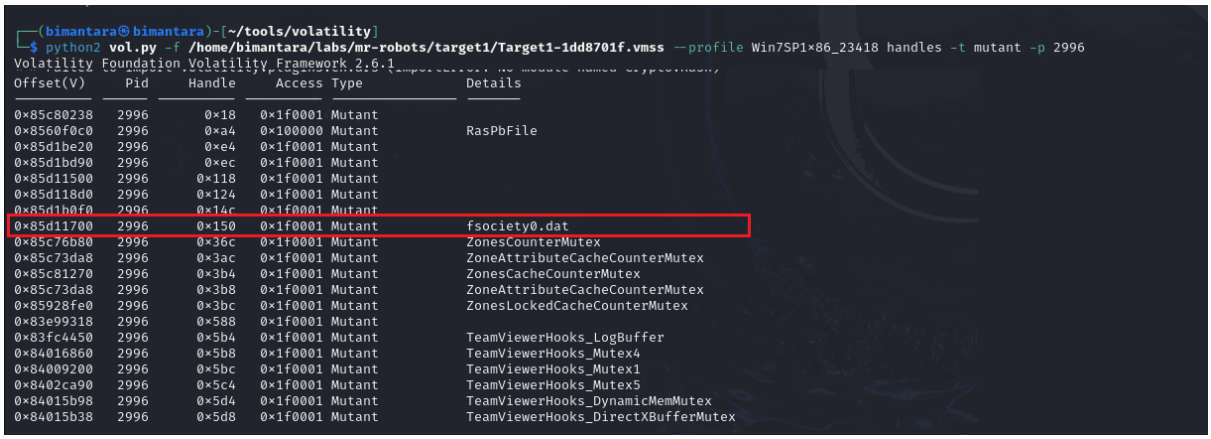
Penelusuran dilakukan, dimulai dengan berfokus pada process tree menggunakan command pstree. Berdasarkan command pstree, didapatkan adanya process yang dimulai dari iexplore.exe dengan memanggil suatu process cmd.exe hal ini sama dengan process yang sering digunakan oleh threat actor. Dimana process ID tersebut diketahui adalah 2996.

Process Analisa juga berfokus pada menemukan adanya maintain persistence yang umum dilakukan oleh malware. Process tersebut digunakan oleh threat actor untuk menjaga agar malware yang telah dimasukkan ke dalam device terinfeksi akan selalu berjalan dan dapat berkomunikasi dengam threat actor.

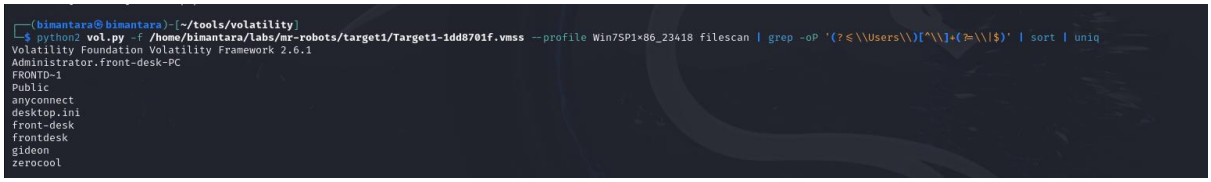


Dilihat dari informasi diatas, terdapat adanya konfigurasi yang digunakan oleh malware tersebut dalam melakukan maintain persistence. Dimana malware tersebut melakukan konfigurasi pada registry **Microsoft\Windows\CurrentVersion\Run**, path registry tersebut berisi daftar aplikasi yang akan dijalankan secara otomatis setiap kali sistem atau pengguna masuk (boot-up). Sehingga didapatkan bahwa threat actor berusaha menjalankan MrRobot setiap kali pengguna melakukan booting.

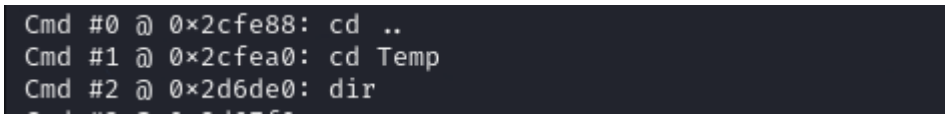
Setiap malware umumnya akan menjalankan suatu process yang memungkinkan malware memastikan hanya satu instance dari dirinya yang berjalan pada satu waktu di sistem korban. Process tersebut sering disebut dengan mutant atau mutex. Untuk mengeahui mutant atau mutex yang digunakan oleh threat actor, dapat diketahui dengan mudah melalui process .exe yang dimulai dari malware tersebut yaitu iexplore.exe dengan bantuan command handles. Dilihat pada gambar dibawah, terdapat file fsociety0.dat yang bertype Mutant, file ini diasumsikan sebagai file mutant atau mutex dari malware yang meninfeksi device tersebut.



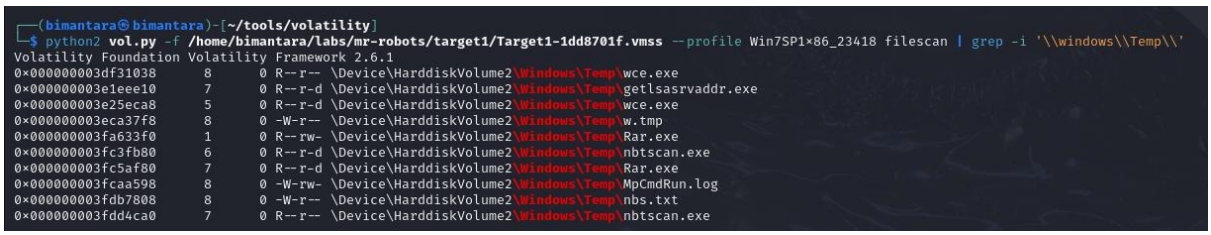
Investigasi kami berlanjut dengan menemukan adanya beberapa user yang sepertinya dibuat oleh threat actor. Disini kami menggunakan plugin filescan dengan berfokus melakukan pencarian string berdasarkan username. Disini kami menemukan beberapa user, namun kami berfokus pada username Gideon dan Zerocool yang sedikit berbeda dari yang lainnya.



Selnajutnya terdapat informasi mengenai attacker yang berusaha memindahkan beberapa tools yang berada pada device terinfeksi. Hal ini bis akita ketahui dengan melalukan pengecekkan pada history commanline.

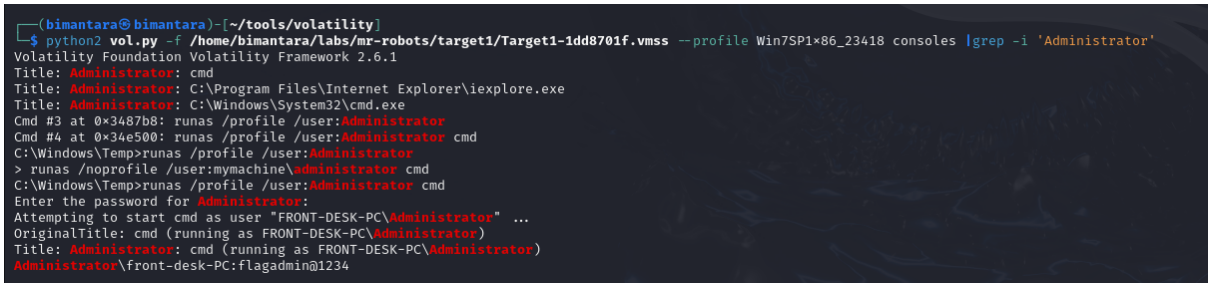


Berdasarkan historical dari command yang dijalankan oleh threat actor, diketahui bahwa adanya process masuk ke direktori Temp. Sehingga kami berasumsi bahwa threat actor tersebut menyembunyikan beberapa tools yang berada pada direktori temp. Kami menemukan terdapat beberapa tools yang digunakan oleh threat actor dalam direktori temp.



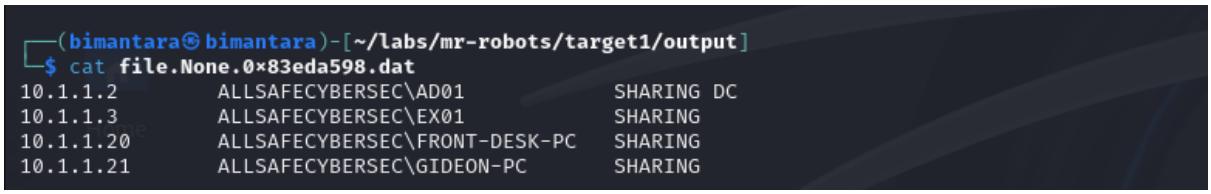
- wce.exe
- getlsasrvaddr.exe
- Rar.exe
- nbtscan.exe

Selanjutnya kami menemukan adanya proses yang dijalankan melalui cmd, disini kami mendapatkan adanya aktivitas menjalankan user local administrator. Disini kami mendapati adanya informasi berupa password seperti pada gambar dibawah ini.

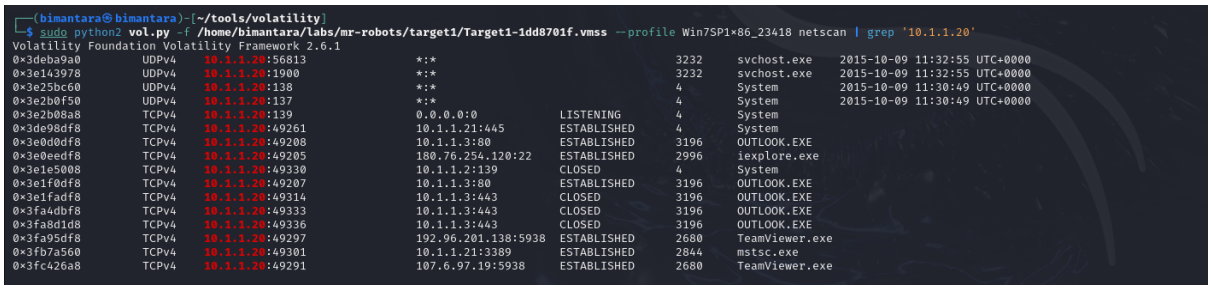


Berdasarkan hasil investigasi sebelumnya, diketahui terdapat beberapa tools yang digunakan oleh threa actor seperti nbtscan.exe. Dimana file nbtscan.exe tersebut berguna untuk tujuan tertentu dalam serangan mereka, terutama dalam tahap **reconnaissance** atau pengintaian jaringan.

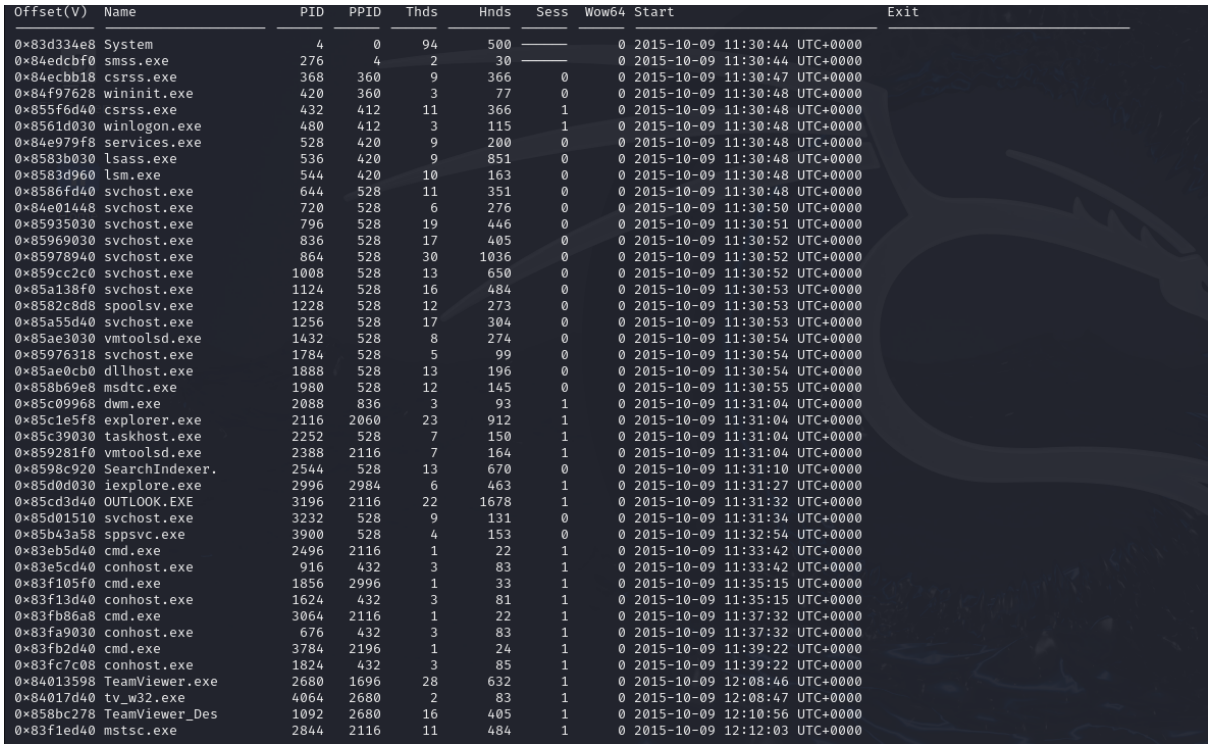
Dari hasil penggunaan tools nbtscan.exe tersebut, dapat diketahui hasilnya. Hasil scanning tersebut tersimpan dalam direktori \Device\HarddiskVolume2\Windows \Temp\nbs.txt. melalui penggunaan plugin dumpfiles kami mendapati informasi seperti ini :



Selanjutnya dilakukan validasi penelusuran pada sisi network. Dimana dari sisi network ditemukan adanya konesik dari device terinfeksi yaitu FRONT-DESK-PC (10.1.1.20) mengarah ke IP public yang terasosiasi dengan process iexplore.exe yaitu 180.76.254.120 dengan port 22 dan statsus eshtablished.

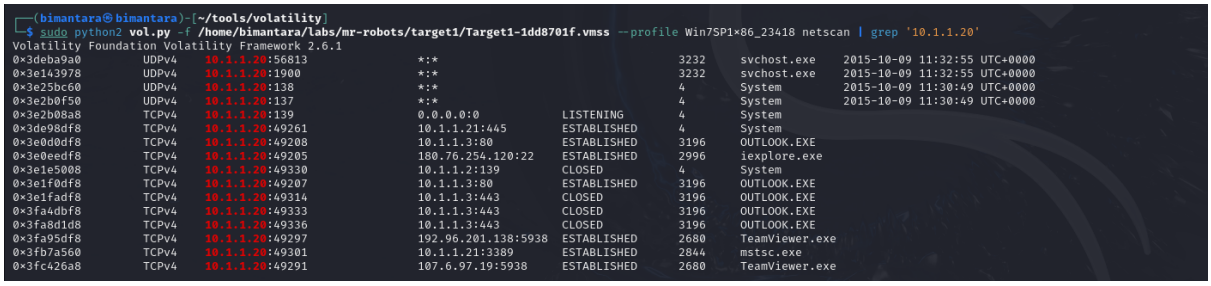


Dalam proses malicious activity yang dijalankan oleh malware tersebut, terdeteksi adanyan penggunaan remote access tool yang bersifat legitimate. Dimana tools remoted access tool tersebut sering digunakan oleh orang awam. Setelah validasi yang dilakukan, diketahui software remote access tersebut adalah TeamViewer.exe



Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
0×83d334e8	System	4	0	94	500	———	0	2015-10-09 11:30:44 UTC+0000	
0×84edcbf0	smss.exe	276	4	2	30	———	0	2015-10-09 11:30:44 UTC+0000	
0×84ecbb18	csrss.exe	368	360	9	366	0	0	2015-10-09 11:30:47 UTC+0000	
0×84f97628	wininit.exe	420	360	3	77	0	0	2015-10-09 11:30:48 UTC+0000	
0×855f6d40	csrss.exe	432	412	11	366	1	0	2015-10-09 11:30:48 UTC+0000	
0×8561d030	winlogon.exe	480	412	3	115	1	0	2015-10-09 11:30:48 UTC+0000	
0×84e979f8	services.exe	528	420	9	200	0	0	2015-10-09 11:30:48 UTC+0000	
0×8583b030	lsass.exe	536	420	9	851	0	0	2015-10-09 11:30:48 UTC+0000	
0×8583d960	lsm.exe	544	420	10	163	0	0	2015-10-09 11:30:48 UTC+0000	
0×8586fd40	svchost.exe	644	528	11	351	0	0	2015-10-09 11:30:48 UTC+0000	
0×84e01448	svchost.exe	720	528	6	276	0	0	2015-10-09 11:30:50 UTC+0000	
0×85935030	svchost.exe	796	528	19	446	0	0	2015-10-09 11:30:51 UTC+0000	
0×85969030	svchost.exe	836	528	17	405	0	0	2015-10-09 11:30:52 UTC+0000	
0×85978940	svchost.exe	864	528	30	1036	0	0	2015-10-09 11:30:52 UTC+0000	
0×859cc2c0	svchost.exe	1008	528	13	650	0	0	2015-10-09 11:30:52 UTC+0000	
0×85a138f0	svchost.exe	1124	528	16	484	0	0	2015-10-09 11:30:53 UTC+0000	
0×8582c8d8	spoolsv.exe	1228	528	12	273	0	0	2015-10-09 11:30:53 UTC+0000	
0×85a55d40	svchost.exe	1256	528	17	304	0	0	2015-10-09 11:30:53 UTC+0000	
0×85ae3030	vmtoolsd.exe	1432	528	8	274	0	0	2015-10-09 11:30:54 UTC+0000	
0×85976318	svchost.exe	1784	528	5	99	0	0	2015-10-09 11:30:54 UTC+0000	
0×85ae0cb0	dllhost.exe	1888	528	13	196	0	0	2015-10-09 11:30:54 UTC+0000	
0×858b69e8	msdtc.exe	1980	528	12	145	0	0	2015-10-09 11:30:55 UTC+0000	
0×85c09968	dwm.exe	2088	836	3	93	1	0	2015-10-09 11:31:04 UTC+0000	
0×85c1e5f8	explorer.exe	2116	2060	23	912	1	0	2015-10-09 11:31:04 UTC+0000	
0×85c39030	taskhost.exe	2252	528	7	150	1	0	2015-10-09 11:31:04 UTC+0000	
0×859281f0	vmtoolsd.exe	2388	2116	7	164	1	0	2015-10-09 11:31:04 UTC+0000	
0×8598c920	SearchIndexer.	2544	528	13	670	0	0	2015-10-09 11:31:10 UTC+0000	
0×85d0d030	iexplore.exe	2996	2984	6	463	1	0	2015-10-09 11:31:27 UTC+0000	
0×85cd3d40	OUTLOOK.EXE	3196	2116	22	1678	1	0	2015-10-09 11:31:32 UTC+0000	
0×85d01510	svchost.exe	3232	528	9	131	0	0	2015-10-09 11:31:34 UTC+0000	
0×85b43a58	sppsvc.exe	3900	528	4	153	0	0	2015-10-09 11:32:54 UTC+0000	
0×83eb5d40	cmd.exe	2496	2116	1	22	1	0	2015-10-09 11:33:42 UTC+0000	
0×83e5cd40	conhost.exe	916	432	3	83	1	0	2015-10-09 11:33:42 UTC+0000	
0×83f105f0	cmd.exe	1856	2996	1	33	1	0	2015-10-09 11:35:15 UTC+0000	
0×83f13d40	conhost.exe	1624	432	3	81	1	0	2015-10-09 11:35:15 UTC+0000	
0×83fb86a8	cmd.exe	3064	2116	1	22	1	0	2015-10-09 11:37:32 UTC+0000	
0×83fa9030	conhost.exe	676	432	3	83	1	0	2015-10-09 11:37:32 UTC+0000	
0×83fb2d40	cmd.exe	3784	2196	1	24	1	0	2015-10-09 11:39:22 UTC+0000	
0×83fc7c08	conhost.exe	1824	432	3	85	1	0	2015-10-09 11:39:22 UTC+0000	
0×84013598	TeamViewer.exe	2680	1696	28	632	1	0	2015-10-09 12:08:46 UTC+0000	
0×84017d40	tv_w32.exe	4064	2680	2	83	1	0	2015-10-09 12:08:47 UTC+0000	
0×858bc278	TeamViewer_Des	1092	2680	16	405	1	0	2015-10-09 12:10:56 UTC+0000	
0×83f1ed40	mstsc.exe	2844	2116	11	484	1	0	2015-10-09 12:12:03 UTC+0000	

Selain installasi tools remote access tools, teridentifikasi juga menggunakan tools lain yaitu mstc.exe. Tools ini memungkinkan pengguna untuk terhubung ke komputer atau server lain melalui Remote Desktop Protocol (RDP). Ini biasanya digunakan untuk manajemen jarak jauh atau pengelolaan server.



```
┌──(bimantara㉿bimantara)-[~/tools/volatility]
└─$ sudo python2 vol.py -f /home/bimantara/labs/mr-robots/target1/Target1-1dd8701f.vmss --profile Win7SP1x86_23418 netscan | grep '10.1.1.20'
Volatility Foundation Volatility Framework 2.6.1
0×3deba9a0         UDPv4    10.1.1.20:56813                *:*                                     3232     svchost.exe    2015-10-09 11:32:55 UTC+0000
0×3e143978         UDPv4    10.1.1.20:1900                 *:*                                     3232     svchost.exe    2015-10-09 11:32:55 UTC+0000
0×3e25bc60         UDPv4    10.1.1.20:138                  *:*                                     4        System         2015-10-09 11:30:49 UTC+0000
0×3e2b0f50         UDPv4    10.1.1.20:137                  *:*                                     4        System         2015-10-09 11:30:49 UTC+0000
0×3e2b08a8         TCPv4    10.1.1.20:139                  0.0.0.0:0              LISTENING        4        System
0×3de98df8         TCPv4    10.1.1.20:49261                10.1.1.21:445          ESTABLISHED      4        System
0×3e0d0df8         TCPv4    10.1.1.20:49208                10.1.1.3:80            ESTABLISHED      3196     OUTLOOK.EXE
0×3e0eedf8         TCPv4    10.1.1.20:49205                180.76.254.120:22      ESTABLISHED      2996     iexplore.exe
0×3e1e5008         TCPv4    10.1.1.20:49330                10.1.1.2:139           CLOSED           4        System
0×3e1f0df8         TCPv4    10.1.1.20:49207                10.1.1.3:80            ESTABLISHED      3196     OUTLOOK.EXE
0×3e1fadf8         TCPv4    10.1.1.20:49314                10.1.1.3:443           CLOSED           3196     OUTLOOK.EXE
0×3fa4dbf8         TCPv4    10.1.1.20:49333                10.1.1.3:443           CLOSED           3196     OUTLOOK.EXE
0×3fa8d1d8         TCPv4    10.1.1.20:49336                10.1.1.3:443           CLOSED           3196     OUTLOOK.EXE
0×3fa95df8         TCPv4    10.1.1.20:49297                192.96.201.138:5938    ESTABLISHED      2680     TeamViewer.exe
0×3fb7a560         TCPv4    10.1.1.20:49301                10.1.1.21:3389         ESTABLISHED      2844     mstsc.exe
0×3fc426a8         TCPv4    10.1.1.20:49291                107.6.97.19:5938       ESTABLISHED      2680     TeamViewer.exe
```

Process investigasi dilanjutkan kepada mesin kedua. Dimana pada mesin kedua juga dilakukan veifikasi imaging yang telah didapatkan oleh tim. Didapatkan bahwa profile dari device terkait berupa Win7SP1x86_23418.

```
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86_24000, Win7SP1x86
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : VMWareAddressSpace (Unnamed AS)
                     AS Layer3 : FileAddressSpace (/home/bimantara/labs/mr-robots/target2/target2-6186fe9f.vmss)
                      PAE type : PAE
                           DTB : 0x185000L
                          KDBG : 0x82730be8L
          Number of Processors : 2
     Image Type (Service Pack) : 0
                KPCR for CPU 0 : 0x82731c00L
                KPCR for CPU 1 : 0x807c5000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2015-10-09 12:53:12 UTC+0000
     Image local date and time : 2015-10-09 08:53:12 -0400
```

Proses invesitagasi dilanjutkan dengan mencari tahu terkait dengan password dari user Gideoon sebagai security admins. WCE adalah tools yang sering digunakan dalam pengujian penetrasi atau kegiatan berbahaya oleh threat actors. Alat ini dirancang untuk bekerja dengan kredensial pengguna Windows di memori.

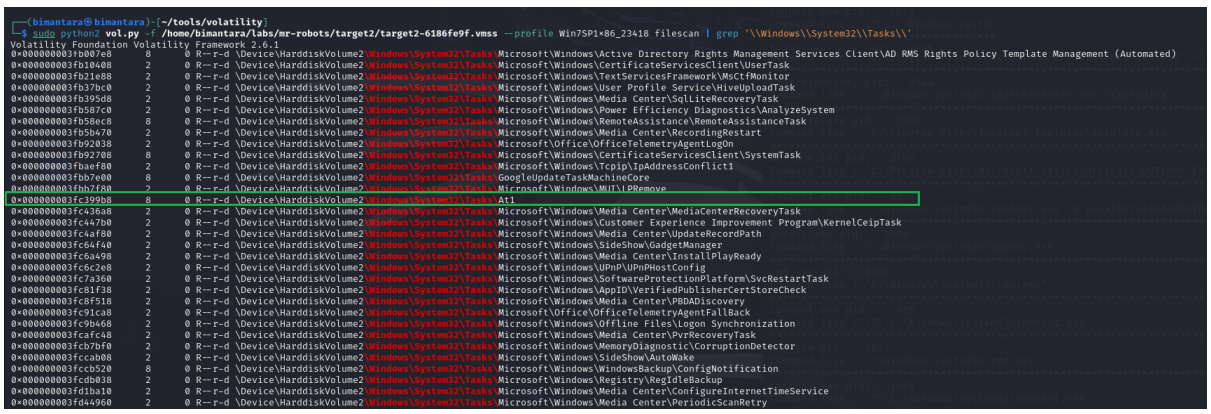
```
ProcessHandle: 0x60
Cmd #0 at 0xe6030: cd C:\Users
Cmd #1 at 0xe6ea8: dir
Cmd #2 at 0xee3d0: wce.exe -w > gideon/w.tmp
Cmd #3 at 0xe0170: who ami
Cmd #4 at 0xe0188: whoami
Cmd #5 at 0xea3c8: net use z: \\10.1.1.2\c$
Cmd #6 at 0xe01b8: cd z:
Cmd #7 at 0xe6ed8: dir
Cmd #8 at 0xe6070: cd gideon

┌──(bimantara㉿bimantara)-[~/labs/mr-robots/target2/output]
└─$ cat file.None.0x85a35da0.dat
WCE v1.42beta (Windows Credentials Editor) - (c) 2010-2013 Amplia Security - by Hernan Ochoa (hernan@ampliasecurity.
com)
Use -h for help.


gideon\ALLSAFECYBERSEC:t76fRJhS
GIDEON-PC$\ALLSAFECYBERSEC:s9O3t%sd1q>:u5Za8Xrx_3Eg;(\qapu<"Rn$#QQJlsD m#;z2hbJkr*tLe>0)F[S)'USh3BKJILn3-?vt]q=s-Cp.
ws9wVik[]5?#F\*l/J19+`PYco:au;T
```

Selanjutnya Setelah penyerang mendapatkan akses ke "Gideon", mereka beralih ke pengontrol domain AllSafeCyberSec untuk mencuri file. Hal ini dapat ditemukan pada histori dari commandline yang dijalankan oleh thret actor tersebut.

```
CommandHistory: 0×e9198 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 18 LastAdded: 17 LastDisplayed: 17
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0×60
Cmd #0 at 0×e6030: cd C:\Users
Cmd #1 at 0×e6ea8: dir
Cmd #2 at 0×ee3d0: wce.exe -w > gideon/w.tmp
Cmd #3 at 0×e0170: who ami
Cmd #4 at 0×e0188: whoami
Cmd #5 at 0×ea3c8: net use z: \\10.1.1.2\c$
Cmd #6 at 0×e01b8: cd z:
Cmd #7 at 0×e6ed8: dir
Cmd #8 at 0×e6070: cd gideon
Cmd #9 at 0×e6ef8: dir
Cmd #10 at 0×e6f08: z:
Cmd #11 at 0×e6f18: dir
Cmd #12 at 0×f2418: copy c:\users\gideon\rar.exe z:\crownjewels
Cmd #13 at 0×e0cb8: cd crownjewels
Cmd #14 at 0×e6f28: dir
Cmd #15 at 0×e6f38: rar
Cmd #16 at 0×f2478: rar crownjewlez.rar *.txt -hp123qwe!@#
Cmd #17 at 0×f24d0: rar a -hp123!@#qwe crownjewlez.rar *.txt
```

Threat actor menggunakan RAR untuk membuat crownjewlez.rar dengan sakelar -HP (yang digunakan untuk mengatur kata sandi untuk arsip yang sedang dibuat) dan menambahkan semua file dengan ekstensi .txt ke arsip.

Selanjutnya process investigasi dilanjutkan pada schedule task yang dibuat oleh malware. Dimana process investigasi berfokus pada path C:\Windows\System32\Tasks dengan menggunakan plugin filescan.



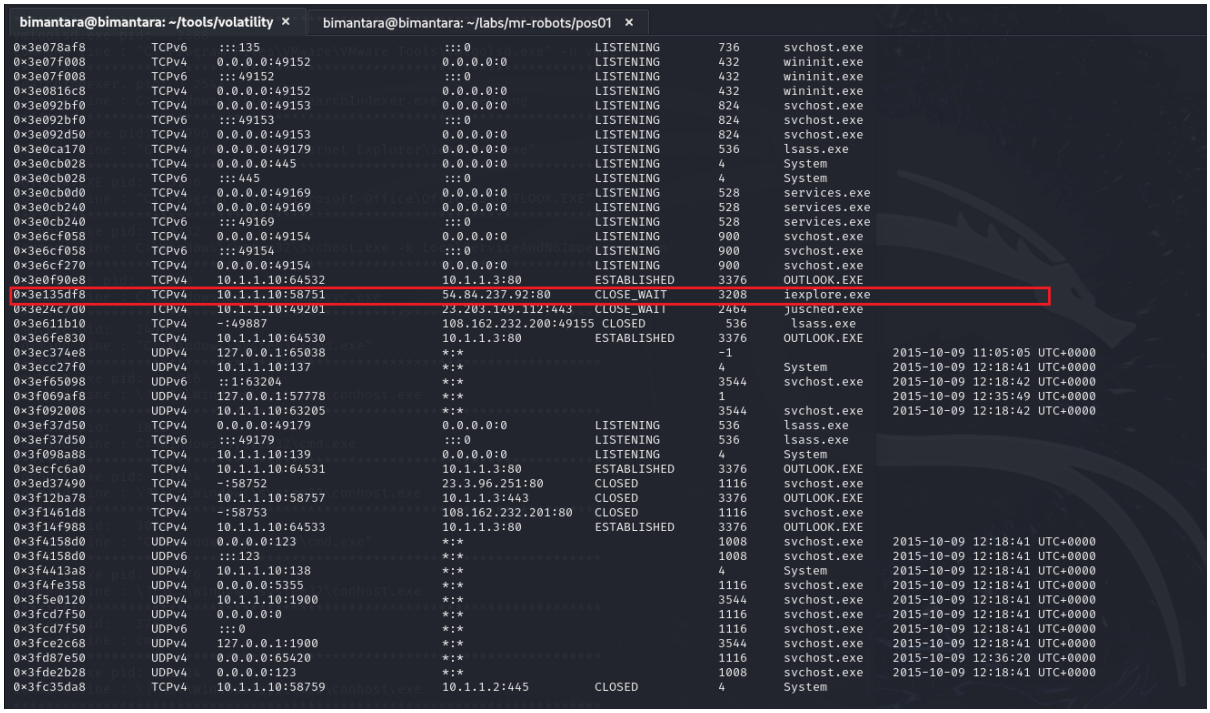
Terlihat adanya schedule task yang dibuat terlihat seperti anomaly. Sehingga temuan ini perlu dilakukan pengecekkan lebih detail. Dan setelah dilakukan dumpfiles, terlihat awah schedule task dengan nama AT1 berisikan automation running script yang dengan nama 1.bat

```
┌──(bimantara㉿bimantara)-[~/…/mr-robots/target2/output/output]
└─$ cat file.None.0x85a86af0.dat
ÿþ<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.0" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo />
  <Triggers>
    <TimeTrigger>
      <StartBoundary>2015-10-09T08:00:00</StartBoundary>
    </TimeTrigger>
  </Triggers>
  <Principals>
    <Principal id="Author">
      <UserId>@AtServiceAccount</UserId>
      <LogonType>InteractiveTokenOrPassword</LogonType>
      <RunLevel>HighestAvailable</RunLevel>
    </Principal>
  </Principals>
  <Actions Context="Author">
    <Exec>
      <Command>c:\users\gideon\1.bat</Command>
    </Exec>
  </Actions>
</Task>
```

Proses investigasi dilanjutkan pada device ketigas yaitu POS. dimana Process validasi dilakukan untuk mengetahui profile dari mesin tersebut.

```
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86_24000, Win7SP1x86
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : VMWareAddressSpace (Unnamed AS)
                     AS Layer3 : FileAddressSpace (/home/bimantara/labs/mr-robots/pos01/POS-01-c4e8f786.vmss)
                      PAE type : PAE
                           DTB : 0x185000L
                          KDBG : 0x82763be8L
          Number of Processors : 2
     Image Type (Service Pack) : 0
                KPCR for CPU 0 : 0x82764c00L
                KPCR for CPU 1 : 0x807c5000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2015-10-09 12:52:56 UTC+0000
     Image local date and time : 2015-10-09 08:52:56 -0400
```

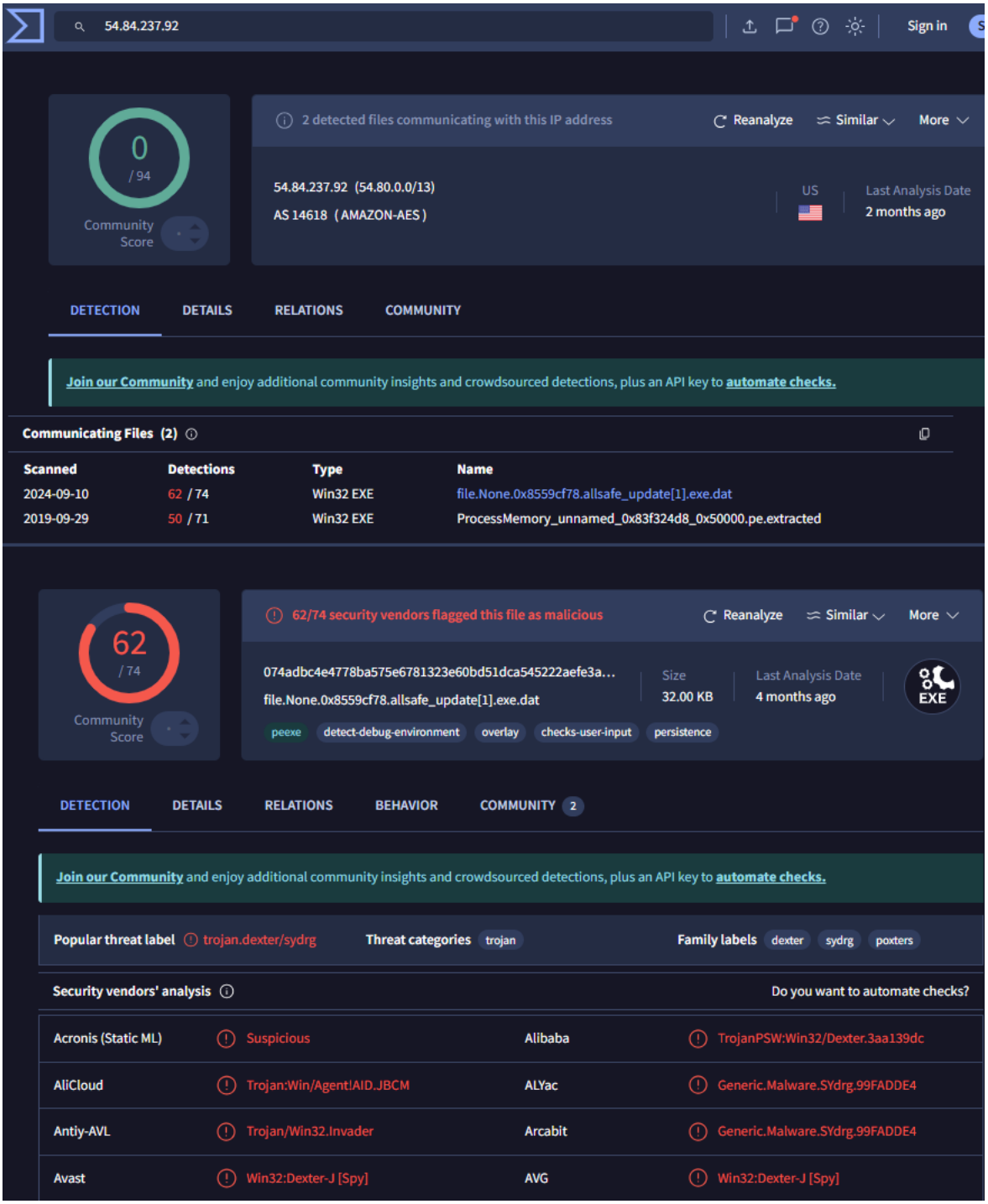
Setelah mengetaui profile dari mesin tersebut selanjutnya adalah melakukan idenftifikasi terkait dengan Malware CNC Server. Process identifikasi tersebut menggunakan plugin netscan. Dikarenakan pada mesin sebelumnya process terinfeksi malware melalui iexplorer.exe maka dalam identifikasi kali ini kami berfokus pada iexplorer.exe juga.



bimantara@bimantara: ~/tools/volatility × bimantara@bimantara: ~/labs/mr-robots/pos01 ×

0×3e078af8	TCPv6	:::135	:::0	LISTENING	736	svchost.exe	
0×3e07f008	TCPv4	0.0.0.0:49152	0.0.0.0:0	LISTENING	432	wininit.exe	
0×3e07f008	TCPv6	:::49152	:::0	LISTENING	432	wininit.exe	
0×3e0816c8	TCPv4	0.0.0.0:49152	0.0.0.0:0	LISTENING	432	wininit.exe	
0×3e092bf0	TCPv4	0.0.0.0:49153	0.0.0.0:0	LISTENING	824	svchost.exe	
0×3e092bf0	TCPv6	:::49153	:::0	LISTENING	824	svchost.exe	
0×3e092d50	TCPv4	0.0.0.0:49153	0.0.0.0:0	LISTENING	824	svchost.exe	
0×3e0ca170	TCPv4	0.0.0.0:49179	0.0.0.0:0	LISTENING	536	lsass.exe	
0×3e0cb028	TCPv4	0.0.0.0:445	0.0.0.0:0	LISTENING	4	System	
0×3e0cb028	TCPv6	:::445	:::0	LISTENING	4	System	
0×3e0cb0d0	TCPv4	0.0.0.0:49169	0.0.0.0:0	LISTENING	528	services.exe	
0×3e0cb240	TCPv4	0.0.0.0:49169	0.0.0.0:0	LISTENING	528	services.exe	
0×3e0cb240	TCPv6	:::49169	:::0	LISTENING	528	services.exe	
0×3e6cf058	TCPv4	0.0.0.0:49154	0.0.0.0:0	LISTENING	900	svchost.exe	
0×3e6cf058	TCPv6	:::49154	:::0	LISTENING	900	svchost.exe	
0×3e6cf270	TCPv4	0.0.0.0:49154	0.0.0.0:0	LISTENING	900	svchost.exe	
0×3e0f90e8	TCPv4	10.1.1.10:64532	10.1.1.3:80	ESTABLISHED	3376	OUTLOOK.EXE	
0×3e135df8	TCPv4	10.1.1.10:58751	54.84.237.92:80	CLOSE_WAIT	3208	iexplore.exe	
0×3e24c7d0	TCPv4	10.1.1.10:49201	23.203.149.112:443	CLOSE_WAIT	2464	jusched.exe	
0×3e611b10	TCPv4	-:49887	108.162.232.200:49155	CLOSED	536	lsass.exe	
0×3e6fe830	TCPv4	10.1.1.10:64530	10.1.1.3:80	ESTABLISHED	3376	OUTLOOK.EXE	
0×3ec374e8	UDPv4	127.0.0.1:65038	*:*		-1		2015-10-09 11:05:05 UTC+0000
0×3ecc27f0	UDPv4	10.1.1.10:137	*:*		4	System	2015-10-09 12:18:41 UTC+0000
0×3ef65098	UDPv6	::1:63204	*:*		3544	svchost.exe	2015-10-09 12:18:42 UTC+0000
0×3f069af8	UDPv4	127.0.0.1:57778	*:*		1		2015-10-09 12:35:49 UTC+0000
0×3f092008	UDPv4	10.1.1.10:63205	*:*		3544	svchost.exe	2015-10-09 12:18:42 UTC+0000
0×3ef37d50	TCPv4	0.0.0.0:49179	0.0.0.0:0	LISTENING	536	lsass.exe	
0×3ef37d50	TCPv6	:::49179	:::0	LISTENING	536	lsass.exe	
0×3f098a88	TCPv4	10.1.1.10:139	0.0.0.0:0	LISTENING	4	System	
0×3ecfc6a0	TCPv4	10.1.1.10:64531	10.1.1.3:80	ESTABLISHED	3376	OUTLOOK.EXE	
0×3ed37490	TCPv4	-:58752	23.3.96.251:80	CLOSED	1116	svchost.exe	
0×3f12ba78	TCPv4	10.1.1.10:58757	10.1.1.3:443	CLOSED	3376	OUTLOOK.EXE	
0×3f1461d8	TCPv4	-:58753	108.162.232.201:80	CLOSED	1116	svchost.exe	
0×3f14f988	TCPv4	10.1.1.10:64533	10.1.1.3:80	ESTABLISHED	3376	OUTLOOK.EXE	
0×3f4158d0	UDPv4	0.0.0.0:123	*:*		1008	svchost.exe	2015-10-09 12:18:41 UTC+0000
0×3f4158d0	UDPv6	:::123	*:*		1008	svchost.exe	2015-10-09 12:18:41 UTC+0000
0×3f4413a8	UDPv4	10.1.1.10:138	*:*		4	System	2015-10-09 12:18:41 UTC+0000
0×3f4fe358	UDPv4	0.0.0.0:5355	*:*		1116	svchost.exe	2015-10-09 12:18:41 UTC+0000
0×3f5e0120	UDPv4	10.1.1.10:1900	*:*		3544	svchost.exe	2015-10-09 12:18:41 UTC+0000
0×3fcd7f50	UDPv4	0.0.0.0:0	*:*		1116	svchost.exe	2015-10-09 12:18:41 UTC+0000
0×3fcd7f50	UDPv6	:::0	*:*		1116	svchost.exe	2015-10-09 12:18:41 UTC+0000
0×3fce2c68	UDPv4	127.0.0.1:1900	*:*		3544	svchost.exe	2015-10-09 12:18:41 UTC+0000
0×3fd87e50	UDPv4	0.0.0.0:65420	*:*		1116	svchost.exe	2015-10-09 12:36:20 UTC+0000
0×3fde2b28	UDPv4	0.0.0.0:123	*:*		1008	svchost.exe	2015-10-09 12:18:41 UTC+0000
0×3fc35da8	TCPv4	10.1.1.10:58759	10.1.1.2:445	CLOSED	4	System	

Berdasarkan informasi diatas, IP yan terduga sebagai IP malware CnC adalah 54.84.237(.)92. Validasi juga dilakukan pada virustotals, dan benar ip tersebut memiliki hubungan dengan malicious file yang terdeteksi sebagai malware yaitu dexter.



Selanjutnya dikarenakan kami mendapati process CnC malware melalui process iexplore.exe sehingga kami melakukan dump process menggunakna memdump. Dari hasil tersebut kami mencari tahu aplikasi yang berhubngan dengan allsafecybersec dan kami melakukan pencarian melalui string

Selanjutnya kami mencari tahu file apa yang didownload dari ip bad reputation tersebut. Untuk mengetahui hal ini, kami dapat menggunakan plugin iehistory yang mengarah ke ip 54.84.237(.)92.

Berdasarkan hasil investigasi diatas, diketahui bahwa malicious file pertama kali ynag didownoad pada device terinfeksi adalah allsafe_update.exe.

Incident of Compromise

Network :

54.84.237(.)92

180.76.254(.)120

Recomendation

- Gunakan Antivirus dan EDR (Endpoint Detection and Response) untuk mendeteksi dan memblokir malware.
- Lakukan Backup Secara Berkala dengan aturan 3-2-1 (3 salinan, 2 media berbeda, 1 offsite).
- Perbarui Sistem dan Aplikasi dengan patch keamanan terbaru.
- Aktifkan Multi-Factor Authentication (MFA) untuk semua akses penting.
- Nonaktifkan Makro pada dokumen Microsoft Office.
- Segmentasi Jaringan untuk membatasi penyebaran ransomware.
- Batasi Hak Akses menggunakan prinsip least privilege.
- Edukasi Pengguna tentang phishing dan ancaman keamanan lainnya.

- Gunakan Firewall dan IDS/IPS untuk memonitor dan memblokir aktivitas mencurigakan.
- Nonaktifkan Protokol Tidak Aman seperti SMBv1 atau RDP tanpa autentikasi yang kuat.

Referrence

https://medium.com/@mo4de1/mrrobot-blue-team-challenge-cyberdefenders-fdbf1fa0c7ed

https://responderj01.medium.com/mrrobot-walkthrough-cyberdefenders-7694e3120897