ATMMalScan

A forensics tool for ATMs

Frank Boldewin
Fiducia & GAD IT AG

EAST EGAF – 22nd Meeting
20th January 2021

Introduction

- ATMMalScan is an incident response tool specifically designed for use on ATMs to identify and collect evidence of an attack on these devices.
- It scans running processes on a system as well as the hard disk for ATM malware and generates memory dumps of suspicious processes, which the analyst can then examine in depth.
- Additionally, it can also help to classify unknown samples.
- Requirements
  - Windows 7 or higher
  - Visual C++ Redistributable for Visual Studio 2015
- Known issues
  - Currently ATMMalScan does not support codepages that require Unicode, this means Windows operating systems that are set to e.g. Cyrillic or Chinese characters, no representative result can be guaranteed. This is due to YARA C-API restrictions.

https://github.com/fboldewin/ATMMalScan

Sample usage - Step1

- Scan process memory and disk.
- Even though standard user rights are sufficient, scanning with Admin privileges provide best results!

```
C:\ATMMalScan>ATMMalScan64.exe -Mem -Disk c:\Users\root\AppData\Local\temp

ATMMalScan v0.1 (c) Frank Boldewin (@r3c0nst)
----------------------------------------------


         ===> ATTENTION: Not running as Admin. For best scanning results execute this tool with Administrator rights!

[*] Scanning System-Memory for malicious patterns now...

Scanning TPOSD.EXE
Scanning sihost.exe
Scanning svchost.exe
Scanning svchost.exe
Scanning svchost.exe
Scanning taskhostw.exe
Scanning SynTPEnh.exe
Scanning igfxEM.exe
Scanning Explorer.EXE
Scanning svchost.exe
Scanning StartMenuExperienceHost.exe
```

Sample usage – Step2

- ATMMalScan detected a malware called XFS_DIRECT in a process, gives details about the thread and its rules matches.
- Further a full processmemory dump has been saved to disk, to catch the malicious process, its modules, as well as its stack and heap pages.
- Malware has been detected on disk as well.

```
Scanning DnGrt4sS$EaL6.exe

        Rule "ATM_Malware_XFS_DIRECT" matched
        -------------------------------------
                Details: ==> https://github.com/fboldewin/ATM-Jackpotting-P4WNP1-style-with-malware-XFS_DIRECT

        Match Dump Information:
        -------------------------

        4E 4F 57 20 45 4E 54 45 52 20 4D 41 53 54 45 52 |  NOW ENTER MASTER
        20 4B 45 59                                     |   KEY

        43 6C 6F 73 69 6E 67 20 61 70 70 2C 20 74 68 61 |  Closing app, tha
        6E 20 64 65 6C 65 74 65 20 6D 79 73 65 6C 66 2E |  n delete myself.

        4E 75 6D 62 65 72 20 6F 66 20 70 68 69 73 69 63 |  Number of phisic
        61 6C 20 63 61 73 68 20 75 6E 69 74 73 20 69 73 |  al cash units is
        3A                                              |  :

        43 4F 55 4C 44 20 4E 4F 54 20 45 4E 41 42 4C 45 |  COULD NOT ENABLE
        20 6F 72 20 44 49 53 41 42 4C 45 20 63 6F 6E 6E |   or DISABLE conn
        65 63 74 69 6F 6E                               |  ection

        58 46 53 5F 44 49 52 45 43 54                   |  XFS_DIRECT

        54 61 6B 65 20 74 68 65 20 6D 6F 6E 65 79 20 79 |  Take the money y
        6F 75 20 73 6E 69 63 6B 79 20 6D 6F 74 68 65 72 |  ou snicky mother
        20 66 75 63 6B 65 72 20 3A 29                   |   fucker :)

        41 00 54 00 4D 00 20 00 49 00 53 00 20 00 54 00 |  A.T.M. .I.S. .T.
        45 00 4D 00 50 00 4F 00 52 00 41 00 52 00 49 00 |  E.M.P.O.R.A.R.I.
        4C 00 59 00 20 00 4F 00 55 00 54 00 20 00 4F 00 |  L.Y. .O.U.T. .O.
        46 00 20 00 53 00 45 00 52 00 56 00 49 00 43 00 |  F. .S.E.R.V.I.C.
        45 00 21 00                                     |  E.!.

        D1 F8 89 44 24 10 DB 44 24 10 DC 0D 80 C3 0E 00 |  ...D$..D$.......
        E8 5B E8 01 00 35 2F 81 0B 00 A3                |  .[...5/....

        8B 54 24 38 68 2E 01 00 00 52 C7 43 06 01 00 00 |  .T$8h....R.C....
        00                                              |  .


                ==> Dumping full processmemory of DnGrt4sS$EaL6.exe (Pid: 1776)
                ==> Dumpfile: C:\ATMMalScan\Dump\FullProcessMemory-PID-1776.dmp

Scanning Calculator.exe
Scanning RuntimeBroker.exe


[ ] Scanning path C:\USERS\ROOT\APPDATA\LOCAL\TEMP for malicious patterns now...


        Rule "ATM_Malware_XFS_DIRECT" triggered for filename: C:\USERS\ROOT\APPDATA\LOCAL\TEMP\DnGrt4sS$EaL6.exe
        Meta Information => https://github.com/fboldewin/ATM-Jackpotting-P4WNP1-style-with-malware-XFS_DIRECT


[*] Scan finished...
```

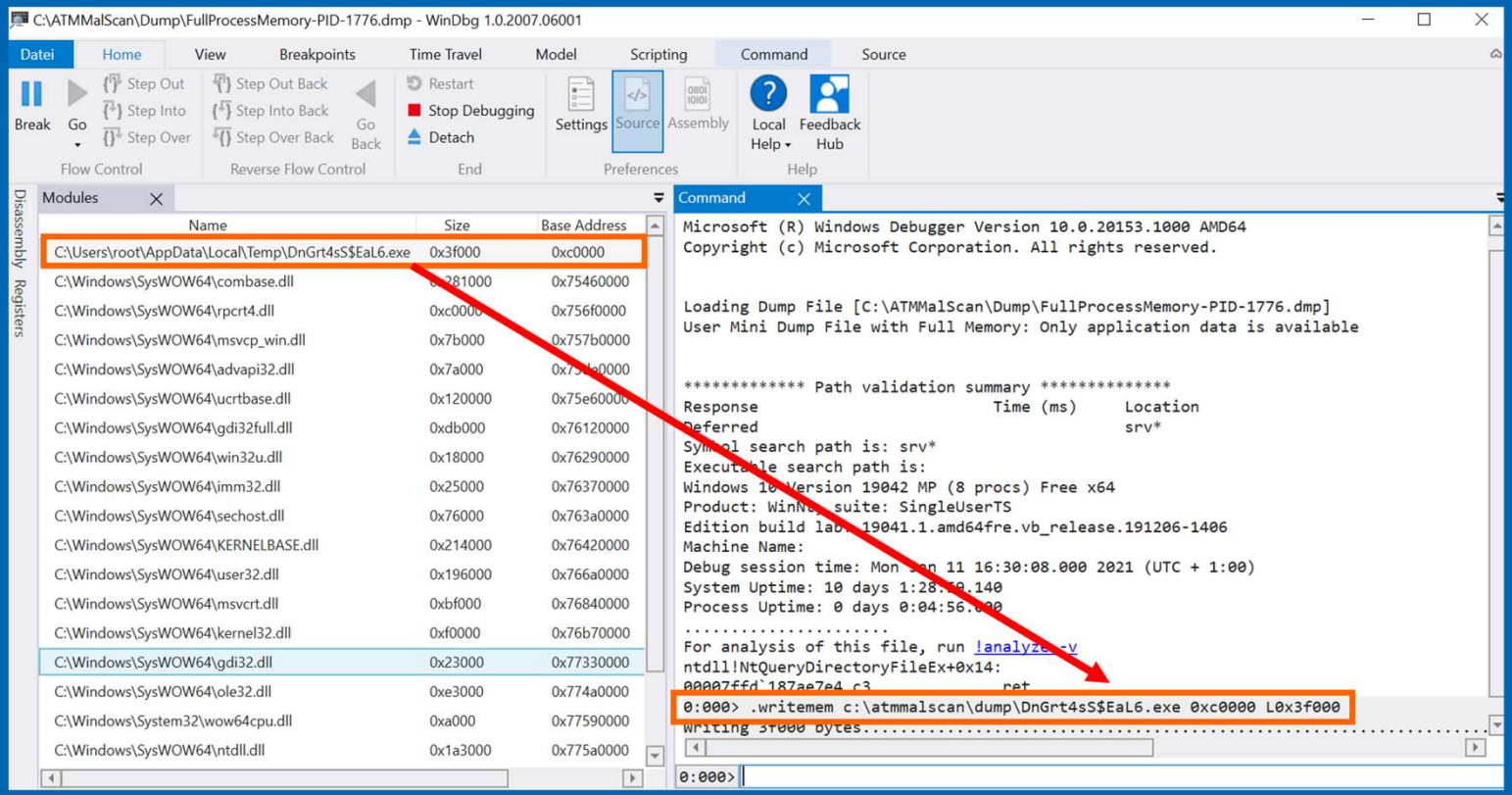
Sample usage – Step3

- The processmemory dump has been saved in ATMMalScan's the subdirectory .\Dump

```
C:\ATMMalScan>cd Dump

C:\ATMMalScan\Dump>dir
 Datenträger in Laufwerk C: ist Windows
 Volumeseriennummer: 1097-7[illegible]40

 Verzeichnis von C:\ATMMalScan\Dump

11.01.2021  16:30    <DIR>          .
11.01.2021  16:30    <DIR>          [illegible]
11.01.2021  16:30        28.556.959 FullProcessMemory-PID-1776.dmp
               1 Datei(en),     28.556.959 Bytes
               2 Verzeichnis(se), 784.063.184.896 Bytes frei
```

Sample usage – Step4

- Open dumpfile with Microsoft Windbg and extract just the malware binary to disk using ".writemem"



Sample usage – Step5

- Repair the dumped PE with one of your favorite PE-Fixers and start analysing the malware in detail.

```
C:\ATMMalScan\Dump>Pe-Dumpfixer.py DnGrt4sS$EaL6__dump.exe DnGrt4sS$EaL6__fixed.exe 0xC0000

        ==> PE-Dumpfile fixed!

C:\ATMMalScan\Dump>ida DnGrt4sS$EaL6__fixed.exe

C:\ATMMalScan\Dump>
```

IDA - DnGrt4sS$EaL6__fixed.exe C:\ATMMalScan\Dump\DnGrt4sS$EaL6__fixed.exe

File Edit Jump Search View Debugger Lumina Options Windows Help

Library function | Regular function | Instruction | Data | Unexplored | External symbol | Lumina function

IDA View-A | Occurrences of: wfsexecute | Hex View-1 | Structures | Enums | Imports | Exports

```
.text:000C50B1                          loc_C50B1:                              ; CODE XREF: sub_C4E80+1A6↑j
.text:000C50B1 8B 54 24 14                      mov     edx, [esp+2Ch+var_18]
.text:000C50B5 66 8B 0D 0E 2C 0F 00             mov     cx, word_F2C0E
.text:000C50BC 8B 42 1E                         mov     eax, [edx+1Eh]
.text:000C50BF 66 0B 0D F0 2B 0F 00             or      cx, word ptr dword_F2BF0
.text:000C50C6 C7 47 12 00 04 00 00             mov     dword ptr [edi+12h], 400h
.text:000C50CD 8B 00                            mov     eax, [eax]
.text:000C50CF 0F B7 D1                         movzx   edx, cx
.text:000C50D2 52                               push    edx             ; wAttributes
.text:000C50D3 6A F5                            push    0FFFFFFF5h      ; nStdHandle
.text:000C50D5 89 47 0A                         mov     [edi+0Ah], eax
.text:000C50D8 FF 15 38 70 0E 00                call    ds:GetStdHandle
.text:000C50DE 50                               push    eax             ; hConsoleOutput
.text:000C50DF FF 15 50 70 0E 00                call    ds:SetConsoleTextAttribute
.text:000C50E5 68 D4 BE 0E 00                   push    offset aWaitingForUser ; "\nWaiting for user input: "
.text:000C50EA 68 38 2A 0F 00                   push    offset dword_F2A38
.text:000C50EF E8 6C 47 00 00                   call    sub_C9860
.text:000C50F4 83 C4 08                         add     esp, 8
.text:000C50F7 8D 44 24 14                      lea     eax, [esp+2Ch+var_18]
.text:000C50FB 50                               push    eax
.text:000C50FC 6A 00                            push    0
.text:000C50FE 57                               push    edi
.text:000C50FF 68 98 01 00 00                   push    198h
.text:000C5104 55                               push    ebp
.text:000C5105 FF 15 90 19 0F 00                call    ds:WFSExecute
.text:000C510B 8B F0                            mov     esi, eax
```

Another use case

- Quick identification of ATM malware samples for family classification within seconds

```
Verzeichnis von C:\Malware

9.01.2021  15:42    <DIR>          .
9.01.2021  15:42    <DIR>          ..
9.01.2021  13:39         1.160.192 009b677564b3ebb0831171edf3fb0deb0fa3b0010b74586e01d8df4af965ef3f
9.01.2021  13:39            37.888 0106757fac9d10a8e2a22dce5337f404bfa1c44d3cc0c53af3c7539888bc4025
9.01.2021  13:39           261.112 0149667c0f8cbfc216ef9d1f3154643cbbf6940e6f24a09c92a82dd7370a5027
9.01.2021  13:39         1.128.960 03bb8decefc540bff5b08425adddb404b345452c8adedee0c8af13572891865b
9.01.2021  13:39            18.432 04f25013eb088d5e8a6e55bdb005c464123e6605897bd80ac245ce7ca12a7a70
9.01.2021  13:39         1.918.464 05fae4bef32daf78a8fa42f8c25fdf481f13dfbbbd3048e5b89190822bc470cd
9.01.2021  13:39            12.800 1065502d7171df7be3776b839410a227c540cd977e5e856bbbcd837b0872bdb6
9.01.2021  13:39           118.784 16166533c69f2f04110e8b8e9cc45ed2aeaf7850fa68845c64d92ff907dd44f0
9.01.2021  13:39           444.928 21f3c0bf3fc05685ec5b7bf3c98103761894d7c6783c2c12afae958eb103598e
9.01.2021  15:20           172.032 26b2daa6fbf5ec13599d24e6819202ddb3f770428d732100be15c23be317bd47
9.01.2021  13:39            52.736 4035d977202b44666885f9781ac8755c799350a03838ff782eb730c0d7069958
9.01.2021  13:39            15.360 4a75be18a3fe0033a9ebdb8f4af81c94e03581d19b5b4373e74e41283fd2615f
9.01.2021  13:39           319.488 5cc18fa2204e0bee1f70b53af1fabe03ecce2b2b5e8baecb6fcfc76d2e8395c7
9.01.2021  13:39            18.656 7bd2c97ac5027c360011dc5aa8f2371cd934f73e885e41f7e80152332b3af1db
9.01.2021  13:39           233.472 85652bbd0379d73395102edc299c892f21a4bba3378aa3b0aaea9b1130022bdd
9.01.2021  13:39            26.112 867991ade335186baa19a227e3a044c8321a6cef96c23c98eef21fe6b87edf6a
              16 Datei(en),      5.939.416 Bytes
```

```
C:\Malware>\ATMMalScan\ATMMalScan64.exe -Disk C:\Malware

ATMMalScan v0.1 (c) Frank Boldewin (@r3c0nst)
---------------------------------------------


[*] Scanning path C:\MALWARE for malicious patterns now...

        Rule "ATM_Malware_Winpotv3" triggered for filename: C:\MALWARE\009b677564b3ebb0831171edf3fb0deb0fa3b0010b74586e01d8df4af965ef3f
        Meta Information => https://securelist.com/atm-robber-winpot/89611/

        Rule "ATM_Malware_Ploutus" triggered for filename: C:\MALWARE\0106757fac9d10a8e2a22dce5337f404bfa1c44d3cc0c53af3c7539888bc4025
        Meta Information => https://malpedia.caad.fkie.fraunhofer.de/details/win.ploutus_atm

        Rule "ATM_Malware_JavaDispCash" triggered for filename: C:\MALWARE\0149667c0f8cbfc216ef9d1f3154643cbbf6940e6f24a09c92a82dd7370a5027
        Meta Information => https://malpedia.caad.fkie.fraunhofer.de/details/jar.javadispcash

        Rule "ATM_Malware_KDIAG_Patched" triggered for filename: C:\MALWARE\03bb8decefc540bff5b08425adddb404b345452c8adedee0c8af13572891865b
        Meta Information => https://securelist.com/koffeymaker-notebook-vs-atm/89161/

        Rule "ATM_Malware_ALICE" triggered for filename: C:\MALWARE\04f25013eb088d5e8a6e55bdb005c464123e6605897bd80ac245ce7ca12a7a70
        Meta Information => https://malpedia.caad.fkie.fraunhofer.de/details/win.alice_atm

        Rule "ATM_Malware_CutletMaker" triggered for filename: C:\MALWARE\05fae4bef32daf78a8fa42f8c25fdf481f13dfbbbd3048e5b89190822bc470cd
        Meta Information => https://securelist.com/atm-malware-is-being-sold-on-darknet-market/81871/

        Rule "ATM_Malware_ATMITCH" triggered for filename: C:\MALWARE\1065502d7171df7be3776b839410a227c540cd977e5e856bbbcd837b0872bdb6
        Meta Information => https://malpedia.caad.fkie.fraunhofer.de/details/win.atmitch

        Rule "ATM_Malware_Tyupkin" triggered for filename: C:\MALWARE\16166533c69f2f04110e8b8e9cc45ed2aeaf7850fa68845c64d92ff907dd44f0
        Meta Information => https://www.lastline.com/labsblog/tyupkin-atm-malware/

        Rule "ATM_Malware_Ripper" triggered for filename: C:\MALWARE\21f3c0bf3fc05685ec5b7bf3c98103761894d7c6783c2c12afae958eb103598e
        Meta Information => https://malpedia.caad.fkie.fraunhofer.de/details/win.ripper_atm

        Rule "ATM_Malware_Atmosphere" triggered for filename: C:\MALWARE\26b2daa6fbf5ec13599d24e6819202ddb3f770428d732100be15c23be317bd47
        Meta Information => https://www.group-ib.com/resources/threat-research/silence_moving-into-the-darkside.pdf

        Rule "ATM_Malware_ATMSpitter" triggered for filename: C:\MALWARE\4035d977202b44666885f9781ac8755c799350a03838ff782eb730c0d7069958
        Meta Information => https://malpedia.caad.fkie.fraunhofer.de/details/win.atmspitter

        Rule "ATM_Malware_Dispcash19_USB_Logger" triggered for filename: C:\MALWARE\4a75be18a3fe0033a9ebdb8f4af81c94e03581d19b5b4373e74e41283fd2615f
        Meta Information => https://twitter.com/r3c0nst/status/1129651569006383104

        Rule "ATM_Malware_Prilex" triggered for filename: C:\MALWARE\5cc18fa2204e0bee1f70b53af1fabe03ecce2b2b5e8baecb6fcfc76d2e8395c7
        Meta Information => https://securelist.com/goodfellas-the-brazilian-carding-scene-is-after-you/84263/

        Rule "ATM_Malware_CNGTester_ATMWizX" triggered for filename: C:\MALWARE\7bd2c97ac5027c360011dc5aa8f2371cd934f73e885e41f7e80152332b3af1db
        Meta Information => http://atm.cybercrime-tracker.net/index.php?x=threat&hash=a4b42f503090cd3cd53963ddaf0be3e4eeedbd81ff02664668e68612816e727f

        Rule "ATM_Malware_Neopocket" triggered for filename: C:\MALWARE\85652bbd0379d73395102edc299c892f21a4bba3378aa3b0aaea9b1130022bdd
        Meta Information => https://www.s21sec.com/en/blog/2014/04/neopocket-a-new-atm-malware/

        Rule "ATM_Malware_DispenserXFS_Silence2" triggered for filename: C:\MALWARE\867991ade335186baa19a227e3a044c8321a6cef96c23c98eef21fe6b87edf6a
        Meta Information => https://www.group-ib.com/resources/threat-research/silence_2.0.going_global.pdf

[*] Scan finished...
```

Update v0.2 from 7th March 2021

[+] Added support to include external YARA rules
[+] Added new internal rules
[+] Fixed a bug in the 32bit version

```
ATMMalScan v0.2 (c) Frank Boldewin (@r3c0nst)
---------------------------------------------


==> Choose at least -Mem or -Disk as Parameter!


Usage:
        ATMMalScan -Mem
        ATMMalScan -Disk C:\
        ATMMalScan -Mem -Disk C:\ -Ext c:\myrules\ATMMalware.yar

Parameters:
 -Mem                          Scans systems processmemory for ATMMalware patterns.
 -Disk <path to scan>          Recursively scans a given directory path for ATMMalware patterns.
 -Ext <path_to_YARA_rule_file> Takes an external YARA rule file to scan
```