Malware Targeting Israelis during "Haravot Barzel" war

Contents

Quick Introduction

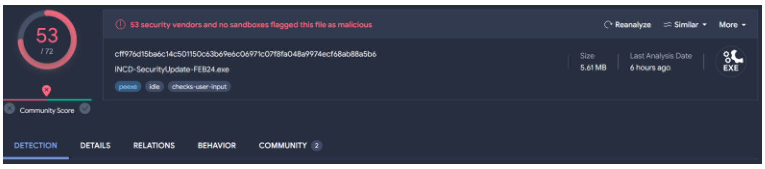
The malware spread through deceptive emails targeted at Israeli entities, linked to the 7th of October War. It disguised itself as a "Software Update" to trick users into downloading and running it. This analysis examines the Windows version of the malware, one of few variations deployed.

Malware Properties

- identified by the following SHA256 hash: cff976d15ba6c14c501150c63b69e6c06971c07f8fa048a9974ecf68ab88a5b6
- VirusTotal: here

Online Tool Analysis (as of today)

The malware is flagged by 53 anti-viruses. Most of them flag the malware as Torjan.



53 / 72

53 security vendors and no sandboxes flagged this file as malicious

cff976d15ba6c14c501150c63b69e6c06971c07f8fa048a9974ecf68ab88a5b6

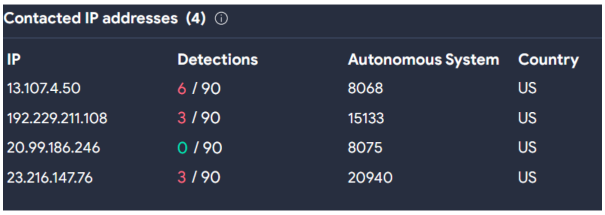
INCD-SecurityUpdate-FEB24.exe

Size: 5.61 MB

Last Analysis Date: 6 hours ago

Figure 1 - Screenshot from VirusTotal; Detections tab.

The malware contacts 4 flagged IP addresses within the US:

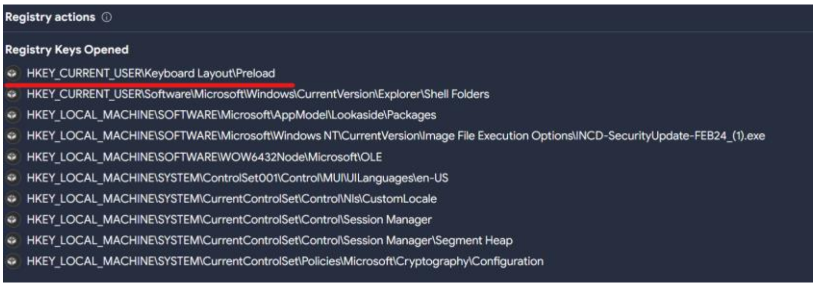


Contacted IP addresses (4)

IP	Detections	Autonomous System	Country
13.107.4.50	6 / 90	8068	US
192.229.211.108	3 / 90	15133	US
20.99.186.246	0 / 90	8075	US
23.216.147.76	3 / 90	20940	US

Figure 2 - Screenshot from VirusTotal; Relations tab.

The malware seems to access odd registries paths:



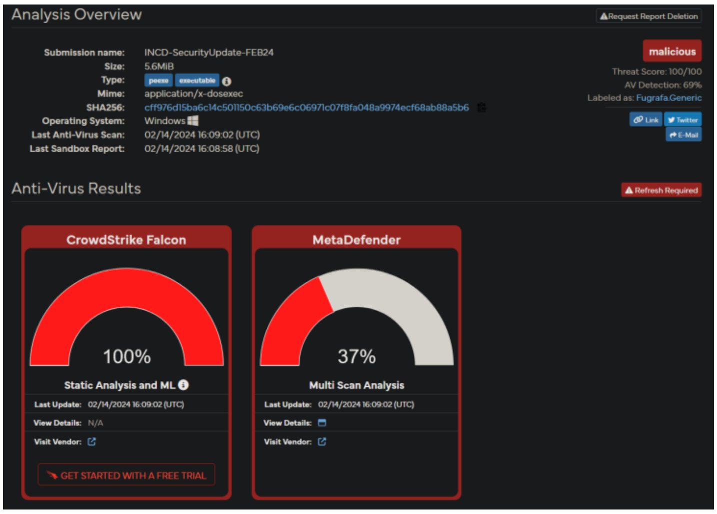
Registry actions

Registry Keys Opened

```
HKEY_CURRENT_USER\Keyboard Layout\Preload
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\AppModel\Lookaside\Packages
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\INCD-SecurityUpdate-FEB24_(1).exe
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\OLE
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\MUI\UILanguages\en-US
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Nls\CustomLocale
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Segment Heap
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Policies\Microsoft\Cryptography\Configuration
```

Figure 3 - Screenshot from VirusTotal; Behavior tab.

The malware also flagged by Hybrid Analysis:



Analysis Overview

Submission name: INCD-SecurityUpdate-FEB24
Size: 5.6MiB
Type: peexe executable
Mime: application/x-dosexec
SHA256: cff976d15ba6c14c501150c63b69e6c06971c07f8fa048a9974ecf68ab88a5b6
Operating System: Windows
Last Anti-Virus Scan: 02/14/2024 16:09:02 (UTC)
Last Sandbox Report: 02/14/2024 16:08:58 (UTC)

malicious
Threat Score: 100/100
AV Detection: 69%
Labeled as: Fugrafa.Generic

Anti-Virus Results

CrowdStrike Falcon
100%
Static Analysis and ML
Last Update: 02/14/2024 16:09:02 (UTC)
View Details: N/A
Visit Vendor:

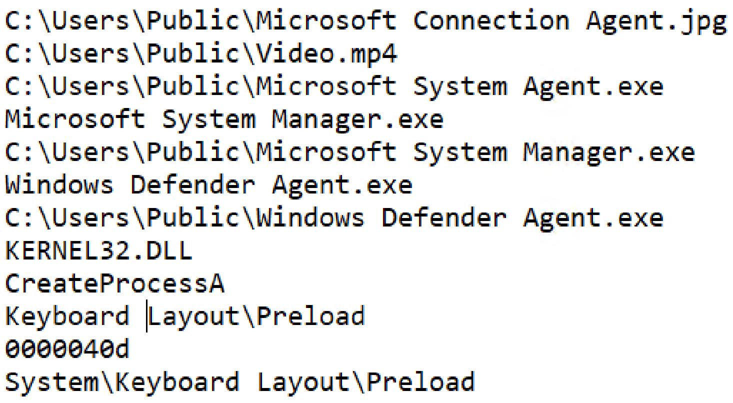
MetaDefender
37%
Multi Scan Analysis
Last Update: 02/14/2024 16:09:02 (UTC)
View Details:
Visit Vendor:

Figure 4 - Screenshot from Hybrid Analysis.

Static analysis

We found strings within the malware that explicitly mention .NET. However, when using a file detector on the malware, it appears that the malware is not .NET. This discrepancy could suggest that the file is a loader or downloader. Additionally, it's worth noting that this malicious loader is a console application.

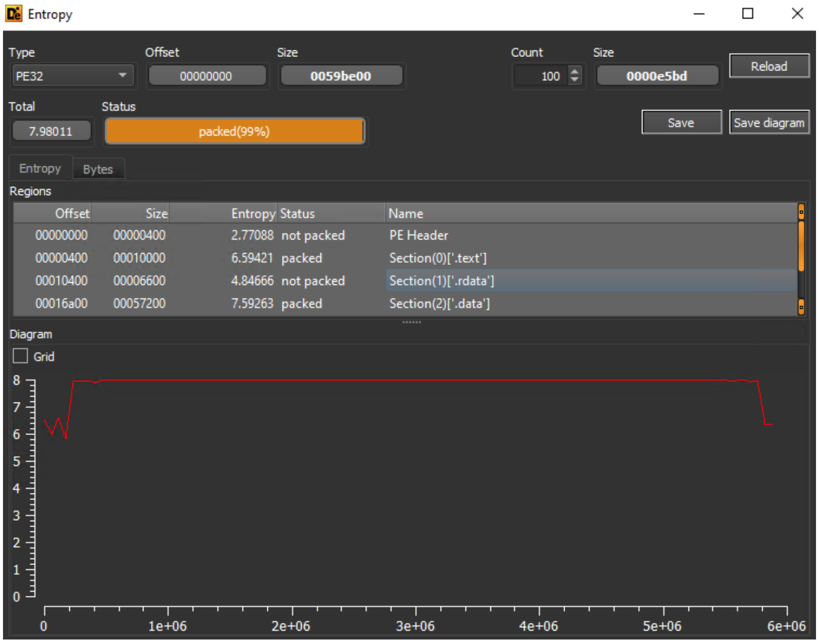
The malware's strings mention access to anything related to keyboard layout, as well as references to video or media in general:



```
C:\Users\Public\Microsoft Connection Agent.jpg
C:\Users\Public\Video.mp4
C:\Users\Public\Microsoft System Agent.exe
Microsoft System Manager.exe
C:\Users\Public\Microsoft System Manager.exe
Windows Defender Agent.exe
C:\Users\Public\Windows Defender Agent.exe
KERNEL32.DLL
CreateProcessA
Keyboard Layout\Preload
0000040d
System\Keyboard Layout\Preload
```

Figure 5 – Strange strings found in the malware's loader.

We then used DIE (Detected it easy) to calculate the entropy of the malware. However, it's important to note that even if the entropy is high, it doesn't necessarily mean the malware is packed. In this case, the high entropy was likely due to the video and picture embedded within the malware executable:



Entropy

Type: PE32 · Offset: 00000000 · Size: 0059be00 · Count: 100 · Size: 0000e5bd

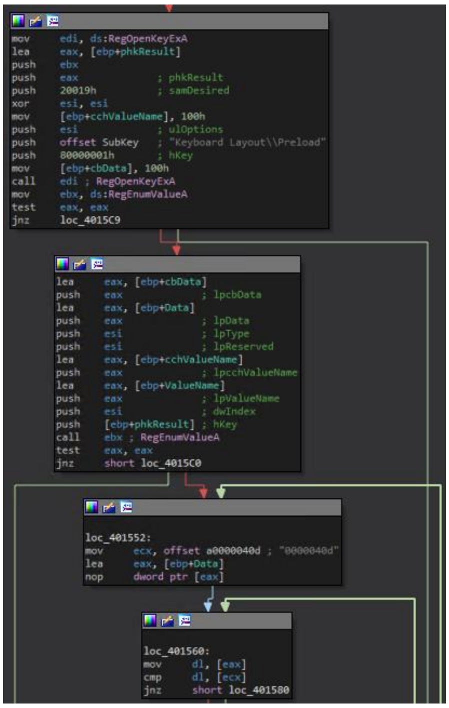
Total: 7.98011 · Status: packed(99%)

Regions

Offset	Size	Entropy	Status	Name
00000000	00000400	2.77088	not packed	PE Header
00000400	00010000	6.59421	packed	Section(0)['.text']
00010400	00006600	4.84666	not packed	Section(1)['.rdata']
00016a00	00057200	7.59263	packed	Section(2)['.data']

Figure 6 - Screenshot of entropy window within DIE

Using IDA to disassemble the loader, I searched for references to that keyboard registry path. I found something interesting: The malware won't load the malicious payload if a specific keyboard language isn't present, which is 0000040d. A quick Google search helped me determine that the language is Hebrew.



```
mov     edi, ds:RegOpenKeyExA
lea     eax, [ebp+phkResult]
push    ebx
push    eax                 ; phkResult
push    20019h              ; samDesired
xor     esi, esi
mov     [ebp+cchValueName], 100h
push    esi                 ; ulOptions
push    offset SubKey       ; "Keyboard Layout\\Preload"
push    80000001h           ; hKey
mov     [ebp+cbData], 100h
call    edi ; RegOpenKeyExA
mov     ebx, ds:RegEnumValueA
test    eax, eax
jnz     loc_4015C9
```

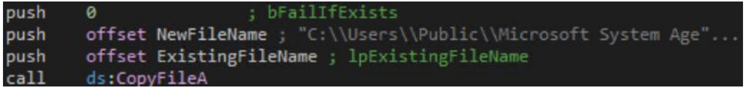
```
lea     eax, [ebp+cbData]
push    eax                 ; lpcbData
lea     eax, [ebp+Data]
push    eax                 ; lpData
push    esi                 ; lpType
push    esi                 ; lpReserved
lea     eax, [ebp+cchValueName]
push    eax                 ; lpcchValueName
lea     eax, [ebp+ValueName]
push    eax                 ; lpValueName
push    esi                 ; dwIndex
push    [ebp+phkResult] ; hKey
call    ebx ; RegEnumValueA
test    eax, eax
jnz     short loc_4015C0
```

```
loc_401552:
mov     ecx, offset a0000040d ; "0000040d"
lea     eax, [ebp+Data]
nop     dword ptr [eax]
```

```
loc_401560:
mov     dl, [eax]
cmp     dl, [ecx]
jnz     short loc_401580
```

Figure 7 - IDA View of conditioned malware loading.

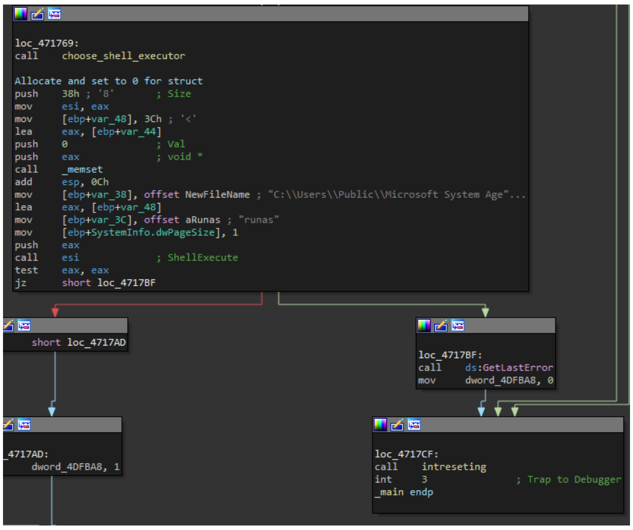
If Hebrew is indeed one of the languages that Windows uses, the loader will copy itself to a path under the public user directory, disguised as "Microsoft System Agent" to deceive the victim into believing that the loader is part of Microsoft's applications:



```
push    0               ; bFailIfExists
push    offset NewFileName ; "C:\\Users\\Public\\Microsoft System Age"...
push    offset ExistingFileName ; lpExistingFileName
call    ds:CopyFileA
```

Figure 8 - The loader copies itself.

As we delve deeper into the code, we uncover that the malware's loader executes a shell command. Specifically, it attempts to execute the "runas" command to run the copied loader with elevated permissions.



```
loc_471769:
call    choose_shell_executor

Allocate and set to 0 for struct
push    38h ; '8'       ; Size
mov     esi, eax
mov     [ebp+var_48], 3Ch ; '<'
lea     eax, [ebp+var_44]
push    0               ; Val
push    eax             ; void *
call    _memset
add     esp, 0Ch
mov     [ebp+var_38], offset NewFileName ; "C:\\Users\\Public\\Microsoft System Age"...
lea     eax, [ebp+var_48]
mov     [ebp+var_3C], offset aRunas ; "runas"
mov     [ebp+SystemInfo.dwPageSize], 1
push    eax
call    esi             ; ShellExecute
test    eax, eax
jz      short loc_4717BF
```

```
        short loc_4717AD
```

```
loc_4717BF:
call    ds:GetLastError
mov     dword_4DFBA8, 0
```

```
_4717AD:
        dword_4DFBA8, 1
```

```
loc_4717CF:
call    intreseting
int     3                       ; Trap to Debugger
_main endp
```

Figure 9 - IDA view of the malware's loader try to run with elevated permissions.

We then came across with interesting function, which mentions EXE files or media files like MP4 and JPG files. This function oversees loading the real malicious stuff that the malware is doing.

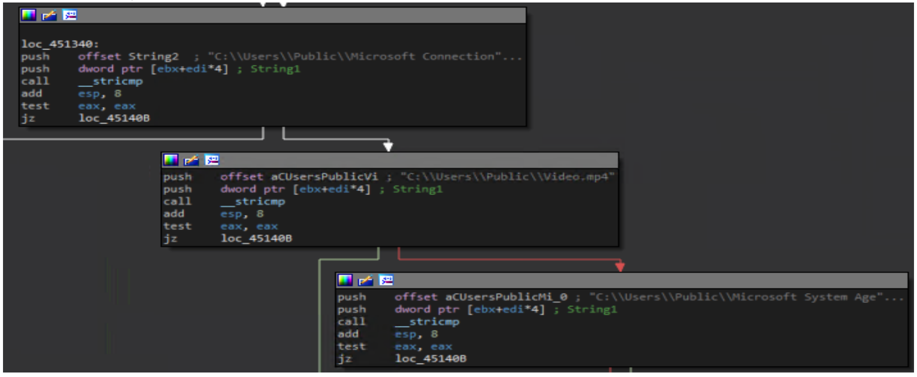
After conducting some investigation, I discovered that there is a video and picture embedded within the executable file. Essentially, the video contains anti-Netanyahu content and is intended to instill fear in Israeli citizens, the picture contains propaganda also. **I will not share the video**. Additionally, there are 2 additional malwares embedded in the loader.

First malware dropped

For the first malware, the loader checks for a domain controller; if none is found, it will not deploy it. The malware is saved once again under the public user path, labeled as "Windows Defender Agent", aiming to further confuse the victim. The dropped malware is in .NET format, confirming initial suspicions. Analysis of the malware's strings and the loader's conditions suggests that the malware may target Windows PCs within active directory. Currently, the malware dropped does not have many detections on VirusTotal (Link).

Second malware dropped

For the second malware dropped, the loader runs it unconditionally. The malware is saved once again under the public user path, labeled as "Microsoft System Manager", aiming to further confuse the victim. This one is not .NET. This malware is a wiper, it will write random bytes into all files but the malware files. This one can be found here.

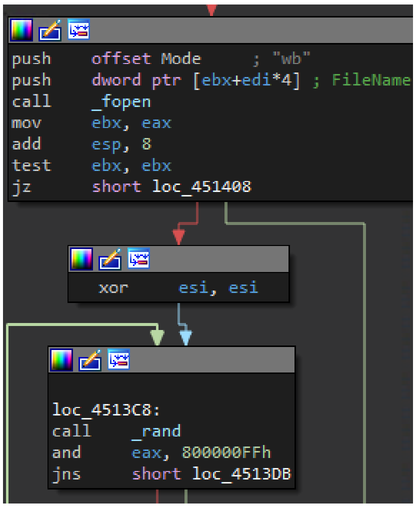


```
loc_451340:
push    offset String2  ; "C:\\Users\\Public\\Microsoft Connection"...
push    dword ptr [ebx+edi*4] ; String1
call    __stricmp
add     esp, 8
test    eax, eax
jz      loc_45140B
```

```
push    offset aCUsersPublicVi ; "C:\\Users\\Public\\Video.mp4"
push    dword ptr [ebx+edi*4] ; String1
call    __stricmp
add     esp, 8
test    eax, eax
jz      loc_45140B
```

```
push    offset aCUsersPublicMi_0 ; "C:\\Users\\Public\\Microsoft System Age"...
push    dword ptr [ebx+edi*4] ; String1
call    __stricmp
add     esp, 8
test    eax, eax
jz      loc_45140B
```

Figure 10 - The malware compares the path given with its file paths.



```
push    offset Mode     ; "wb"
push    dword ptr [ebx+edi*4] ; FileName
call    _fopen
mov     ebx, eax
add     esp, 8
test    ebx, ebx
jz      short loc_451408
```

```
xor     esi, esi
```

```
loc_4513C8:
call    _rand
and     eax, 800000FFh
jns     short loc_4513DB
```

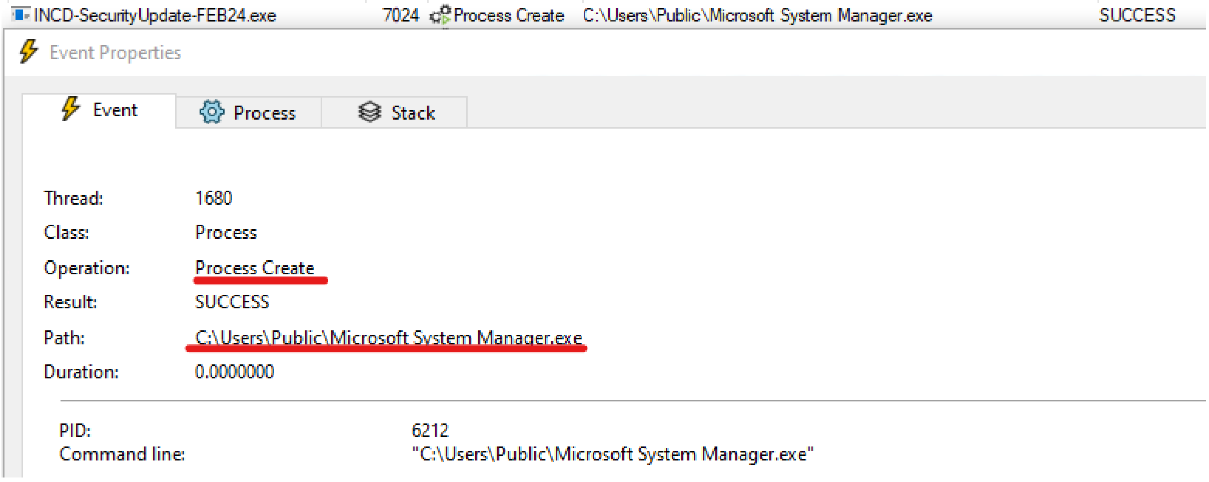
Figure 11 - The malware writes random bytes into all files.

Dynamic analysis

Running the malware did indeed meet our expectations. The video runs repeatedly, and the picture we found is now the wallpaper. Our files were wiped with random bytes.

It's important to note that I ran the malware on a Windows system with a Hebrew keyboard layout and that it wasn't within the Active Directory.

Using Procmon, we can now observe the process creation of the wiper by the loader:

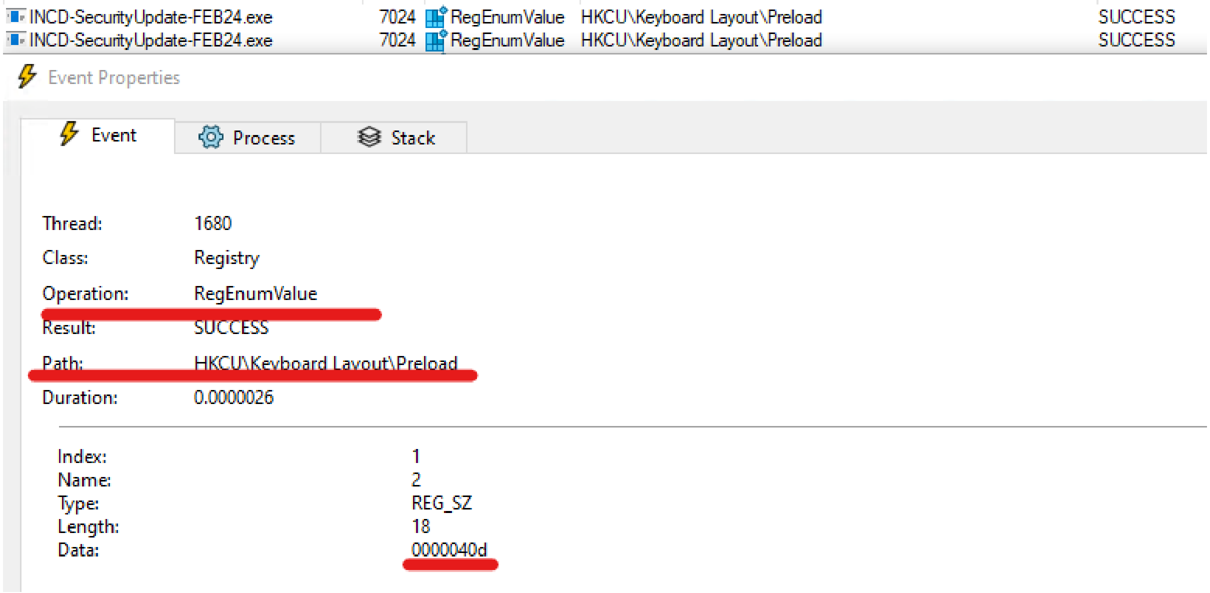


```
INCD-SecurityUpdate-FEB24.exe    7024  Process Create  C:\Users\Public\Microsoft System Manager.exe    SUCCESS
```

```
Thread:      1680
Class:       Process
Operation:   Process Create
Result:      SUCCESS
Path:        C:\Users\Public\Microsoft System Manager.exe
Duration:    0.0000000

PID:            6212
Command line:   "C:\Users\Public\Microsoft System Manager.exe"
```

Figure 12 - View of Procmon window showing the process creation of the wiper.



```
INCD-SecurityUpdate-FEB24.exe    7024  RegEnumValue  HKCU\Keyboard Layout\Preload    SUCCESS
INCD-SecurityUpdate-FEB24.exe    7024  RegEnumValue  HKCU\Keyboard Layout\Preload    SUCCESS
```

```
Thread:      1680
Class:       Registry
Operation:   RegEnumValue
Result:      SUCCESS
Path:        HKCU\Keyboard Layout\Preload
Duration:    0.0000026

Index:     1
Name:      2
Type:      REG_SZ
Length:    18
Data:      0000040d
```

Figure13 - View of Procmon window showing the "RegEnumValue" operation.

Conclusion

In conclusion, the analysis of the malware targeting Israeli entities in the context of the "Haravot Barzel" war reveals a sophisticated and deceptive campaign aimed at infiltrating Windows systems. The malware spreads through deceptive emails, masked as a "Software Update".

Using basic tools like IDA, CFF Explorer and strings, we delved into the malware's code structure and behavior. Further investigation uncovered intricate functionalities designed to evade detection and escalate privileges. The malware checks for specific keyboard language settings before executing its payload, indicating a targeted approach towards Israeli citizens.

The analysis also revealed the presence of anti-Netanyahu propaganda embedded in the malware, along with additional malicious payloads within the loader. The first dropped malware, posing as "Windows Defender Agent", suggests a focus on targeting Windows PCs within active directory environments, while the second dropped malware, labeled as "Microsoft System Manager", serves as a wiper, corrupting files on infected systems.