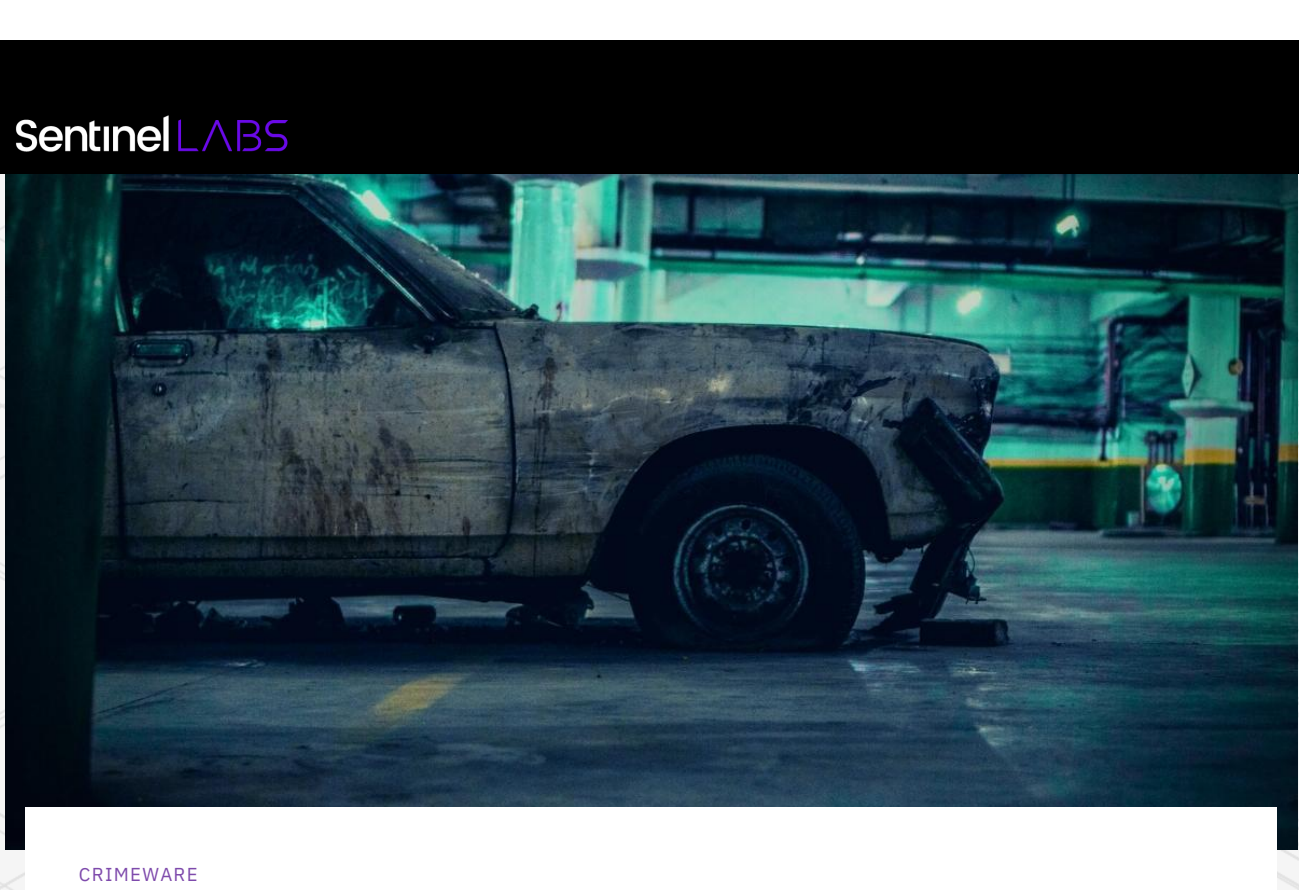
SentinelLABS



CRIMEWARE

LockBit 3.0 Update | Unpicking the Ransomware's Latest Anti-Analysis and Evasion Techniques

JIM WALTER / JULY 21, 2022

By Jim Walter & Aleksandar Milenkoski

LockBit 3.0 ransomware (*aka* LockBit Black) is an evolution of the prolific LockBit ransomware-as-a-service (RaaS) family, which has roots that extend back to BlackMatter and related entities. After critical bugs were discovered in LockBit 2.0 in March 2022, the authors began work on updating their encryption routines and adding several new features designed to thwart researchers. In June 2022, LockBit 3 caught the interest of the media as the ransomware operators announced they were offering a 'bug bounty' to researchers. In this post, we provide an overview of the LockBit 3.0 ransomware update and offer a technical dive for researchers into LockBit 3.0's anti-analysis and evasion features.

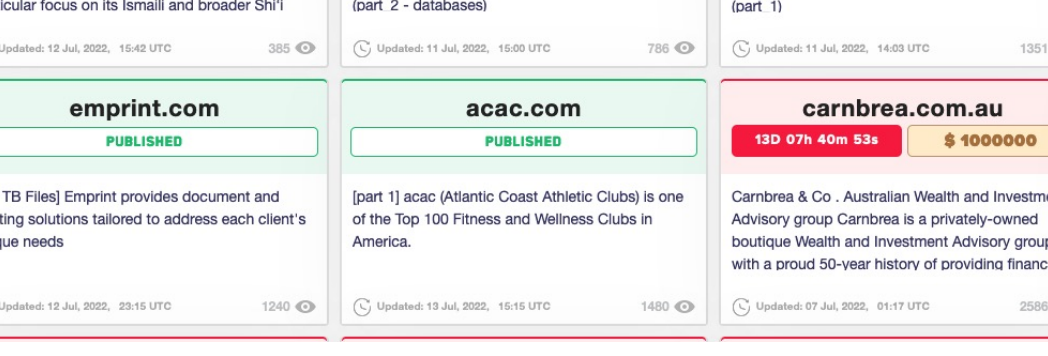
LockBit 3.0 Changes and New Features Since LockBit 2.0

Around June of 2022, operators and affiliates behind LockBit ransomware began the shift to LockBit 3.0. Adoption of LockBit 3.0 by affiliates has been rapid, and numerous victims have been identified on the new "Version 3.0" leak sites, a collection of public blogs naming non-compliant victims and leaking extracted data.

LockBit 3 ransomware leaks site

In order to improve resilience, the operators have been aggressive with regards to standing up multiple mirrors for their leaked data and publicizing the site URLs.

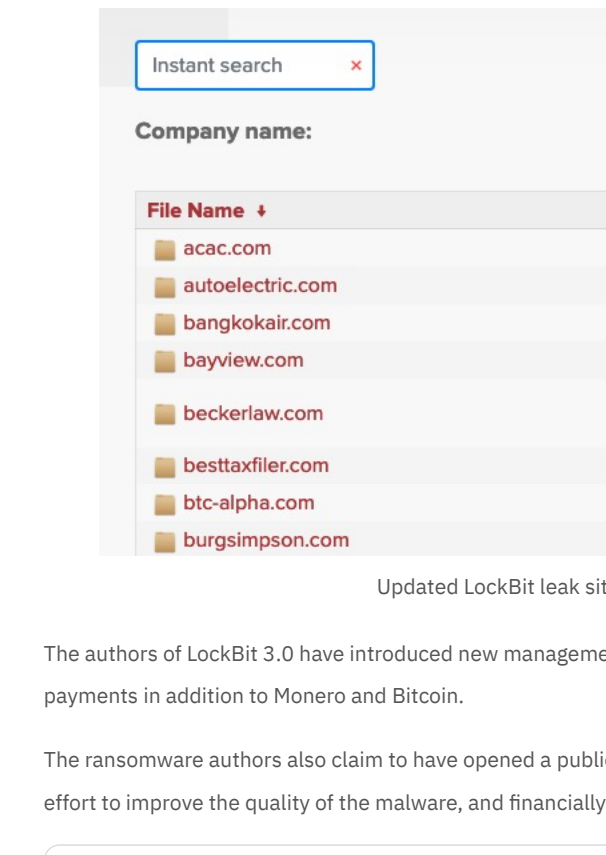
LockBit has also added an instant search tool to their leaks site.



Updated LockBit leak site with new Search feature

The authors of LockBit 3.0 have introduced new management features for affiliates and added Zcash for victim payments in addition to Monero and Bitcoin.

The ransomware authors also claim to have opened a public "bug bounty" program. Ostensibly, this appears to be an effort to improve the quality of the malware, and financially reward those that assist.



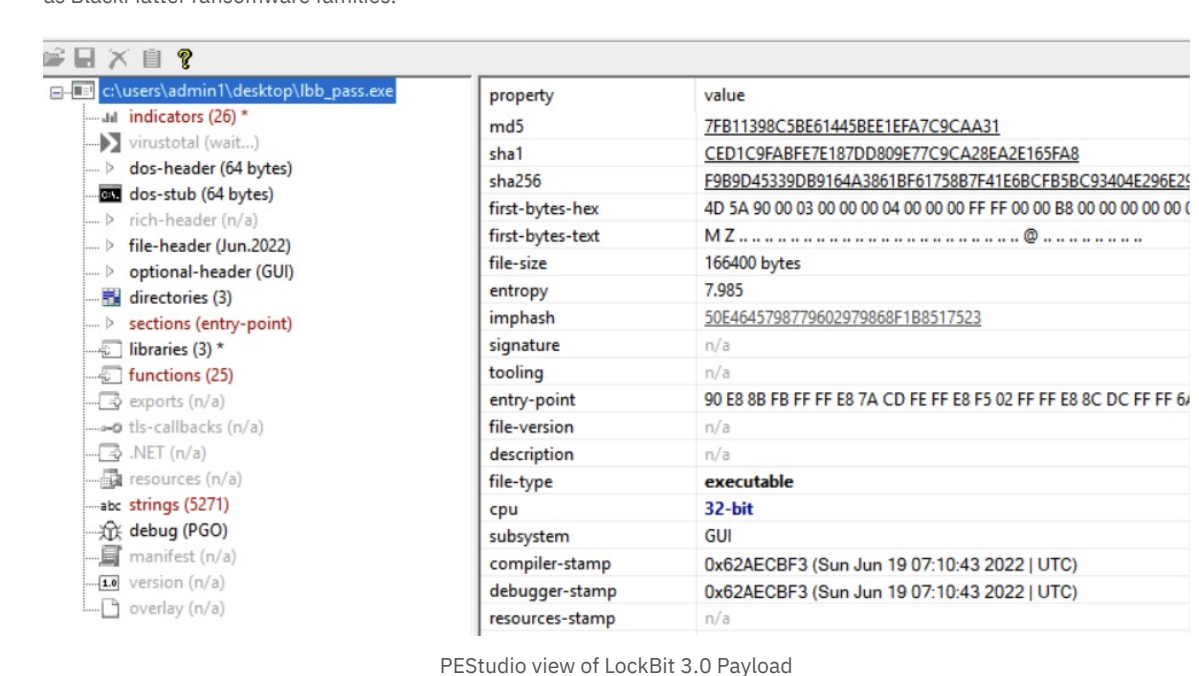
On top of that, there is a purported $1 million reward on offer to anyone who can uncover the identity of the program affiliate manager. Understandably, given the criminal nature of the operators, would-be researchers may find that reporting bugs to a crimeware outfit may not lead to the promised payout but could lead to criminal charges from law enforcement.

LockBit 3.0 Payloads and Encryption

The updated LockBit payloads retain all the prior functionality of LockBit 2.0.

Initial delivery of the LockBit ransomware payloads is typically handled via 3rd party frameworks such as Cobalt Strike. As with LockBit 2.0, we have seen infections occur down the chain from other malware components as well, such as a SocGholish infection dropping Cobalt Strike, which in turn delivers the LockBit 3 ransomware.

The payloads themselves are standard Windows PE files with strong similarities to prior generations of LockBit as well as BlackMatter ransomware families.



PEStudio view of LockBit 3.0 Payload

LockBit ransomware payloads are designed to execute with administrative privileges. In the event that the malware does not have the necessary privileges, a UAC bypass will be attempted (CMSTP).

LockBit 3.0 achieves persistence via installation of System Services. Each execution of the payload will install multiple services. We have observed the following service names in conjunction with LockBit 3.0 ransomware payloads.

```
SecurityHealthService
Sense
sppsvc
WdBoot
WdFilter
WdNisDrv
WdNisSvc
WinDefend
wscsvc
vmicvss
vmvss
VSS
EventLog
```

As with previous versions, LockBit 3.0 will attempt to identify and terminate specific services if found. The following service names are targeted for termination in analyzed LockBit 3.0 samples:

```
backup
GxBlr
GxCIMgr
GxCVD
GxFWD
GxVss
memtas
mepocs
msexchange
sophos
sql
svc$
veeam
vss
```

In addition, the following processes are targeted for termination:

```
agntsvc
dbeng50
dbsnmp
encsvc
excel
firefox
infopath
isqlplussvc
msaccess
mspub
mydesktopqos
mydesktopservice
notepad
ocautoupds
ocomm
ocssd
onenote
oracle
outlook
powerpnt
registry
sqbcoreservice
steam
synctime
tbirdconfig
thebat
thunderbird
visio
winword
wordpad
xfssvccon
```

LockBit 3.0 writes a copy of itself to the `%programdata%` directory, and subsequently launches from this process.

The encryption phase is extremely rapid, even when spreading to adjacent hosts. The ransomware payloads were able to fully encrypt our test host in well under a minute.

On execution, the LockBit 3.0 ransomware will drop newly-formatted ransom notes along with a change to the desktop background. Interestingly, notepad and wordpad are included in the list of prescribed processes as noted above. Therefore, if a victim attempts to open the ransom note immediately after it is dropped, it will promptly close since the process is blocked until the ransomware completes its execution.

The new LockBit 3.0 ransomware desktop wallpaper is a simple text message on a black background.

LockBit 3.0 Desktop Wallpaper

The extension appended to newly encrypted files will also differ per campaign or sample. For example, we have seen "HLJkNskOq" and "futRjC7nx". Both encrypted files and the ransom notes will be prepended with the campaign-specific string.

```
futRjC7nx.README
HLJkNskOq.README
```

During our analysis, we observed infected machines shutting down ungracefully approximately 10 minutes after the ransomware payload was launched. This behavior may vary per sample, but it is worth noting.

Post-infection, LockBit 3.0 victims are instructed to make contact with their attacker via their TOR-based "support" portal.

```
~~~ LockBit 3.0 the world's fastest and most stable ransomware from 2019~~~

>>>>> Your data is stolen and encrypted.
If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind that once your data appears on our leak site, it could be bought by your competitors at any second, so don't hesitate for a long time. The sooner you pay the ransom, the sooner your company will be safe.

Tor Browser Links:
http://lockbitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion
http://lockbitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd.onion
http://lockbitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd.onion
http://lockbitapt5x4zkjbcqmz6frdhecqqgadevyiwqxukksspnlidyvd7qd.onion
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion
http://lockbitapt72iw55njgnqpymggskg5yp75ry7rirtdg4m7i42artsbqd.onion
http://lockbitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqgpjpid.onion
http://lockbitaptbdiajqtplcrigzgdjprwugkkut63nbvy2d5r4w2agyekqd.onion
http://lockbitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kgtzjqd.onion

Links for normal browser:
http://lockbitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion.ly
http://lockbitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd.onion.ly
http://lockbitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd.onion.ly
http://lockbitapt5x4zkjbcqmz6frdhecqqgadevyiwqxukksspnlidyvd7qd.onion.ly
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion.ly
http://lockbitapt72iw55njgnqpymggskg5yp75ry7rirtdg4m7i42artsbqd.onion.ly
http://lockbitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqgpjpid.onion.ly
http://lockbitaptbdiajqtplcrigzgdjprwugkkut63nbvy2d5r4w2agyekqd.onion.ly
http://lockbitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kgtzjqd.onion.ly

>>>>> What guarantee is there that we won't cheat you?
We are the oldest ransomware affiliate program on the planet, nothing is more important than our reputation. We are not a politically motivated group and we want nothing more than money. If you pay, we will provide you with decryption software and destroy the stolen data. After you pay the ransom, you will quickly make even more money. Treat this situation simply as a paid training for your system administrators, because it is due to your corporate network not being properly configured that we were able to attack you. Our pentest services should be paid just like you pay the salaries of your system administrators. Get over it and pay for it. If we don't give you a decryptor or delete your data after you pay, no one will pay us in the future. You can get more information about us on Ilon Musk's Twitter https://twitter.com/hashtag/lockbit?f=live

>>>>> You need to contact us and decrypt one file for free on TOR darknet sites with your personal ID
```

LockBit 3.0 Ransom Note Excerpt

LockBit 3 Anti-Analysis & Evasion

The LockBit 3.0 ransomware uses a variety of anti-analysis techniques to hinder static and dynamic analysis, and exhibits similarities to the BlackMatter ransomware in this regard. These techniques include code packing, obfuscation and dynamic resolution of function addresses, function trampolines, and anti-debugging techniques. In this section, we cover some of the anti-analysis techniques that LockBit 3.0 uses.

LockBit 3.0 payloads require a specific passphrase to execute. The passphrase is unique to each sample or campaign and serves to hinder dynamic and sandbox analysis if the passphrase has not been recovered along with the sample. A similar technique has been used by Egregor and BlackCat ransomware. The passphrase is provided upon execution via the `-pass` parameter. For example,

```
lockbit.exe -pass XX66023ab2zyxb9957fb01de50cdfb6
```

Encrypted content located in the LockBit 3.0 payload is decrypted at runtime using an XOR mask. The images below show the content of the ransomware's `.text` executable segment before (label 1) and after (label 2) the ransomware has decrypted the segment content. The `.text` segment starts at the virtual address **0x401000**.

```
[...]
lb+0x1b095:
0:000> u 00401000 L0x40
lb+0x1000:
00401000 b87af2c029      mov     eax,29C0F27Ah
00401005 21a22ead2855    and     dword ptr [edx+5528AD2Eh],esp
0040100b 6bc1ae          imul    eax,ecx,0FFFFFFAEh
[...]
00401015 7895            js      lb+0xfac (00400fac)
00401017 c071eeb4        sal     byte ptr [ecx-12h],0B4h
0040101b 83ddff          sbb     ebp,0FFFFFFFFh
[...]
                                                  [1]

[...]
lb+0x1b09a:
0041b09a 83c628          add     esi,28h
0:000> u 00401000 L0x40
lb+0x1000:
00401000 cc              int     3
00401001 cc              int     3
00401002 cc              int     3
00401003 cc              int     3
[...]
00401010 cadf06          retf    6DFh
00401013 44              inc     esp
00401014 55              push    ebp
00401015 8bec            mov     ebp,esp
00401017 51              push    ecx
00401018 53              push    ebx
[...]
                                                  [2]
```

The content of the ransomware's *.text* executable segment

LockBit 3.0 also first stores in heap memory and then uses trampolines for executing functions, for example, the Windows system calls `NtSetInformationThread` and `ZwProtectVirtualMemory`. The ransomware obfuscates the function addresses that the trampolines execute using the XOR and/or bit rotation obfuscation technique.

```
0:000> u 023b05b8  L0x18
023b05b8 b82a91a132      mov     eax,32A1912Ah
023b05bd 35cadf0645      xor     eax,4506DFCAh
023b05c2 ffe0            jmp     eax
[...]
023b05d5 c1c802          ror     eax,2
023b05d8 35cadf0645      xor     eax,4506DFCAh
023b05dd ffe0            jmp     eax
[...]
023b05ed c1c801          ror     eax,1
023b05f0 35cadf0645      xor     eax,4506DFCAh
023b05f5 ffe0            jmp     eax
[...]
023b0605 35cadf0645      xor     eax,4506DFCAh
023b060a ffe0            jmp     eax
[...]
```

Some of the function trampolines LockBit 3.0 implements

Several techniques are implemented for detecting the presence of a debugger and hindering dynamic analysis. For example, the ransomware evaluates whether heap memory parameters that indicate the presence of a debugger are set. Such flags are HEAP_TAIL_CHECKING_ENABLED (**0x20**) and HEAP_VALIDATE_PARAMETERS_ENABLED (**0x40000000**).

LockBit 3.0 examines the `ForceFlags` value in its PEB (Process Environment Block) to evaluate whether HEAP_VALIDATE_PARAMETERS_ENABLED is set.

```
v1 = *(_DWORD *)(getPEB() + 0x18);

if ( *(_DWORD *)(v1 + 0x44) & 0x40000000 )
  v1 = __ROR4__(v1, 1);
return dword_427414(v1, 8, a1);
```

LockBit 3.0 evaluates whether HEAP_VALIDATE_PARAMETERS_ENABLED is set

The ransomware also evaluates whether the `0xABABABAB` byte signature is present at the end of heap memory blocks that it has previously allocated. The presence of this byte signature means that HEAP_TAIL_CHECKING_ENABLED is set.

```
[...]
v8 = RtlAllocateHeapPtr(heapHandle, 0, 0x10);
if ( *(_DWORD *)(v8 + 0x10) != 0xABABABAB )
{
  *v6 = v8;
  ++v6;
}
[...]
```

LockBit 3.0 evaluates whether HEAP_TAIL_CHECKING_ENABLED is set

The LockBit 3.0 ransomware executes the NtSetInformationThread function through a trampoline, such that the `ThreadHandle` and `ThreadInformationClass` function parameters have the values of **0xFFFFFFFE** and **0x11** (`ThreadHideFromDebugger`). This stops the flow of events from the current ransomware's thread to an attached debugger, which effectively hides the thread from the debugger and hinders dynamic analysis.

```
[...]
005a36a8 b8ed57194d      mov     eax,4D1957EDh
005a36ad c1c009          rol     eax,9
005a36b0 35cadf0645      xor     eax,4506DFCAh
005a36b5 ffe0            jmp     eax {ntdll!NtSetInformationThread (77a90550)}
[...]
0:000> dps @esp L5
0019ff48  0040d2db lb+0xd2db
0019ff4c  fffffffe
0019ff50  00000011
0019ff54  00000000
0019ff58  00000000
[...]
```

LockBit 3.0 executes *NtSetInformationThread*

In addition, LockBit scrambles the implementation of the `DbgUiRemoteBreakin` function to disable debuggers trying to attach to the ransomware process. When it executes, LockBit 3.0 ransomware:

- Resolves the address of `DbgUiRemoteBreakin`.
- Executes the `ZwProtectVirtualMemory` function through a trampoline to apply the PAGE_EXECUTE_READWRITE (0x40) protection to the first 32 bytes of the memory region where the implementation of `DbgUiRemoteBreakin` resides. This makes the bytes writable.
- Executes the `SystemFunction040` (RtlEncryptMemory) function through a trampoline to encrypt the bytes that the ransomware has previously made writable. This scrambles the implementation of the `DbgUiRemoteBreakin` function and disables debuggers to attach to the ransomware process.

```
[...]
0040d300 e8a3a6ffff      call    lb+0x79a8 (004079a8)
0:000> p
[...]
lb+0xd305:
0040d305 8945fc          mov     dword ptr [ebp-4],eax ss:002b:0019ff5c=00000000
0:000> ln @eax
[...]
(77acb370)   ntdll!DbgUiRemoteBreakin   |  (77acb3d0)   ntdll!DbgUiSetThreadDebugObject
Exact matches:
    ntdll!DbgUiRemoteBreakin (<no parameter info>)
[...]
00583df0 b8d4ac5f65      mov     eax,655FACD4h
00583df5 c1c801          ror     eax,1
00583df8 35cadf0645      xor     eax,4506DFCAh
00583dfd ffe0            jmp     eax {ntdll!ZwProtectVirtualMemory (77a909a0)}
[...]
022f4798 b82015843a      mov     eax,3A841520h
022f479d c1c001          rol     eax,1
022f47a0 ffe0            jmp     eax {CRYPTBASE!SystemFunction040 (75082a40)}
[...]
```

LockBit 3.0 modifies the implementation of the *DbgUiRemoteBreakin* function

The images below depict the implementation of the `DbgUiRemoteBreakin` function before (label 1) and after (label 2) the LockBit 3.0 ransomware has modified the implementation of the function.

```
0:000> u ntdll!DbgUiRemoteBreakin L0x20
ntdll!DbgUiRemoteBreakin:
77cfb370 6a08            push    8
77cfb372 683895d577      push    offset ntdll!PssNtWalkSnapshot+0x5638 (77d59538)
77cfb377 e8d88ffdff      call    ntdll!wcstok_s+0x6084 (77cd4354)
77cfb37c 64a130000000    mov     eax,dword ptr fs:[00000030h]
77cfb382 80780200        cmp     byte ptr [eax+2],0
77cfb386 7509            jne     ntdll!DbgUiRemoteBreakin+0x21 (77cfb391)
77cfb388 f605d402fe7f02  test    byte ptr [SharedUserData+0x2d4 (7ffe02d4)],2
77cfb38f 7428            je      ntdll!DbgUiRemoteBreakin+0x49 (77cfb3b9)
77cfb391 64a118000000    mov     eax,dword ptr fs:[00000018h]
77cfb397 f680ca0f000020  test    byte ptr [eax+0FCAh],20h
77cfb39e 7519            jne     ntdll!DbgUiRemoteBreakin+0x49 (77cfb3b9)
77cfb3a0 8365fc00        and     dword ptr [ebp-4],0
77cfb3a4 e8d773fcff      call    ntdll!DbgBreakPoint (77cc2780)
77cfb3a9 eb07            jmp     ntdll!DbgUiRemoteBreakin+0x42 (77cfb3b2)
77cfb3ab 33c0            xor     eax,eax
77cfb3ad 40              inc     eax
77cfb3ae c3              ret
77cfb3af 8b65e8          mov     esp,dword ptr [ebp-18h]
77cfb3b2 c745fcfeffffff  mov     dword ptr [ebp-4],0FFFFFFFEh
77cfb3b9 6a00            push    0
77cfb3bb e870dffbff      call    ntdll!RtlExitUserThread (77cb9330)
77cfb3c0 cc              int     3
77cfb3c1 cc              int     3
[...]
                                                  [1]

0:000> uf ntdll!DbgUiRemoteBreakin
Flow analysis was incomplete, some code may be missing
ntdll!DbgUiRemoteBreakin:
77cfb370 ab              stos    dword ptr es:[edi]
77cfb371 6ad9            push    0FFFFFFD9h
77cfb373 a8e7            test    al,0E7h
77cfb375 2dc52ff6ed      sub     eax,0EDF62FC5h
77cfb37a 0cdc            or      al,0DCh
77cfb37c fa              cli
[...]
                                                  [2]
```

The implementation of the *DbgUiRemoteBreakin* function

Conclusion

LockBit has fast become one of the more prolific ransomware-as-a-service operators out there, taking over from Conti after the latter's fractious fallout in the wake of the Russian invasion of Ukraine.

LockBit's developers have shown that they are quick to respond to problems in the product they are offering and that they have the technical know-how to keep evolving. The recent claim to be offering a 'bug bounty', whatever its true merits, displays a savvy understanding of their own audience and the media landscape that surrounds the present tide of crimeware and enterprise breaches.

Short of intervention by law enforcement, we expect to see LockBit around for the forseeable future and further iterations of what is undoubtedly a very successful RaaS operation. As with all ransomware, prevention is better than cure, and defenders are encouraged to ensure that they have comprehensive ransomware protection in place. SentinelLabs will continue to offer updates and reports on LockBit activity as it develops.

Indicators of Compromise

SHA256

f9b9d45339db9164a3861bf61758b7f41e6bcfb5bc93404e296e2918e52ccc10
a56b41a6023f828cccaaef470874571d169fdb8f683a75edd430fbd31a2c3f6e
d61af007f6c792b8fb6c677143b7d0e2533394e28c50737588e40da475c040ee

SHA1

ced1c9fabfe7e187dd809e77c9ca28ea2e165fa8
371353e9564c58ae4722a03205ac84ab34383d8c
c2a321b6078acfab582a195c3eaf3fe05e095ce0

.ONION domains

lockbitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead[.]onion
lockbitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd[.]onion
lockbitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd[.]onion
lockbitapt5x4zkjbcqmz6frdhecqqgadevyiwqxukksspnlidyvd7qd[.]onion
lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd[.]onion
lockbitapt72iw55njgnqpymggskg5yp75ry7rirtdg4m7i42artsbqd[.]onion
lockbitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqgpjpid[.]onion
lockbitaptbdiajqtplcrigzgdjprwugkkut63nbvy2d5r4w2agyekqd[.]onion
lockbitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kgtzjqd[.]onion
lockbit7z2jwcskxpbokpemdxmltipntwlkmidcll2qirbu7ykg46eyd[.]onion
lockbitsupa7e3b4pkn4mgkgojrl5iqgx24clbzc4xm7i6jeetsia3qd[.]onion
lockbitsupdwon76nzykzblcplixwts4n4zoecugz2bxabtapqvmzqqd[.]onion
lockbitsupn2h6be2cnqpvncyhj4rgmnwn44633hnzzmtxdvjoqlp7yd[.]onion
lockbitsupo7vv5vcl3jxpsdviopwvasljqcstym6efhh6oze7c6xjad[.]onion
lockbitsupq3g62dni2f36snrdb4n5qzqvovbtkt5xffw3draxk6gwqd[.]onion
lockbitsupqfyacidr6upt6nhhyipujvaablubuevxj6xy3frthvr3yd[.]onion
lockbitsupt7nr3fa6e7xyb73lk6bw6rcneqhoyblniiabj4uwvzapqd[.]onion
lockbitsupuhswh4izvoucoxsbnotkmgq6durg7kficg6u33zfvq3oyd[.]onion
lockbitsupxcjntihbmat4rrh7ktowips2qzywh6zer5r3xafhviyhqd[.]onion

MITRE ATT&CK

T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
T1543.003 – Create or Modify System Process: Windows Service
T1055 – Process Injection
T1070.001 – Indicator Removal on Host: Clear Windows Event Logs
T1622 – Debugger Evasion
T1548.002 – Abuse Elevation Control Mechanism: Bypass User Account Control
T1485 – Data Destruction
T1489 – Service Stop
T1490 – Inhibit System Recovery
T1003.001 – OS Credential Dumping: LSASS Memory
T1078.002 – Valid Accounts: Domain Accounts
T1078.001 – Valid Accounts: Default Accounts
T1406.002 – Obfuscated Files or Information: Software Packing
T1218.003 – System Binary Proxy Execution: CMSTP
T1047 – Windows Management Instrumentation
T1119 – Automated Collection

RAAS

JIM WALTER

Jim Walter is a Senior Threat Researcher at SentinelOne focusing on evolving trends, actors, and tactics within the thriving ecosystem of cybercrime and crimeware. He specializes in the discovery and analysis of emerging cybercrime "services" and evolving communication channels leveraged by mid-level criminal organizations. Jim joined SentinelOne following ~4 years at a security start-up, also focused on malware research and organized crime. Previously, he spent over 17 years at McAfee/Intel running their Threat Intelligence and Advanced Threat Research teams.