

# Commonly Known Tools Used by Lazarus - JPCERT/CC Eyes

By 朝長 秀誠 (Shusei Tomonaga)

Published: 2021-01-19 · Archived: 2026-04-05 17:37:56 UTC

- [Lazarus](#)

It is widely known that attackers use Windows commands and tools that are commonly known and used after intruding their target network. Lazarus attack group, a.k.a. Hidden Cobra, also uses such tools to collect information and spread the infection. This blog post describes the tools they use.

## Lateral movement

These three tools are used for lateral movement. AdFind collects the information of clients and users from Active Directory. It has been observed that other attack groups also used the tool [\[1\]](#). SMBMap is used to have their malware infect other hosts. (Also check out our previous [blog post](#) on Lazarus.) It has also been observed that Responder-Windows was used to collect information in the network.

Name	Description	Reference
AdFind	Command line tool to collect information from Active Directory	<a href="http://www.joeware.net/freetools/tools/adfind/">http://www.joeware.net/freetools/tools/adfind/</a>
SMBMap	Tool to list accessible shared SMB resources and access those files	<a href="https://github.com/ShawnDEvans/smbmap">https://github.com/ShawnDEvans/smbmap</a>
Responder-Windows	Tool to lead clients with spoof LLMNR, NBT-NS, and WPAD	<a href="https://github.com/lgandx/Responder-Windows">https://github.com/lgandx/Responder-Windows</a>

## Stealing sensitive data

These three tools are used for information theft. Tools for such a purpose are used only in certain cases because malware itself usually has similar functions. Tools for collecting account information from browsers and email clients are particularly used. Attackers often archives collected files in RAR before exfiltration, and so does Lazarus attack group using WinRAR. As we mentioned in our previous blog post, the malware can archive files in zlib and send them. It means that files are not always sent in RAR.

Name	Description	Reference
XenArmor Email Password Recovery Pro	Tool to extract credentials from email clients and services	<a href="https://xenarmor.com/email-password-recovery-pro-software/">https://xenarmor.com/email-password-recovery-pro-software/</a>

XenArmor Browser Password Recovery Pro	Tool to extract credentials from web browsers	<a href="https://xenarmor.com/browser-password-recovery-pro-software/">https://xenarmor.com/browser-password-recovery-pro-software/</a>
WinRAR	RAR archiver	<a href="https://www.rarlab.com/">https://www.rarlab.com/</a>

### Other tools

These following tools are used for other purposes. Attackers sometimes create backdoors in the infected network using RDP, TeamViewer, VNC, and other applications. It is confirmed that Lazarus has used VNC and a common Microsoft tool ProcDump before. ProcDump is sometimes used when attackers attempt to extract user credentials from the LSASS process dump. Windows' counterpart of common Linux tools such as tcpdump and wget are also used.

Name	Description	Reference
TightVNC Viewer	VNC client	<a href="https://www.tightvnc.com/download.php">https://www.tightvnc.com/download.php</a>
ProcDump	Common Microsoft's tool to get process memory dump	<a href="https://docs.microsoft.com/en-us/sysinternals/downloads/procdump">https://docs.microsoft.com/en-us/sysinternals/downloads/procdump</a>
tcpdump	Packet capturing tool	<a href="https://www.tcpdump.org/">https://www.tcpdump.org/</a>
wget	Downloader	

### In closing

This blog post described tools used by Lazarus group. Although their malware contains many functions as we already covered in other blog posts, they still supplement it with tools which are widely available and commonly known. It should be noted that anti-virus software may not detect such tools.

The hash values of the tools covered in this blog post are listed in Appendix A.

Shusei Tomonaga

(Translated by Takumi Nakano)

### Reference

[1] Cybereason: Dropping Anchor: From a TrickBot Infection to the Discovery of the Anchor Malware  
<https://www.cybereason.com/blog/dropping-anchor-from-a-trickbot-infection-to-the-discovery-of-the-anchor-malware>

### Appendix A: Hash value

Be careful when using these hash values as IoC. The list contains tools that are commonly used for non-malicious purposes.

### AdFind

- CFD201EDE3EBC0DEB0031983B2BDA9FC54E24D244063ED323B0E421A535CFF92
- B1102ED4BCA6DAE6F2F498ADE2F73F76AF527FA803F0E0B46E100D4CF5150682
- CFD201EDE3EBC0DEB0031983B2BDA9FC54E24D244063ED323B0E421A535CFF92

### SMBMap

- 65DDF061178AD68E85A2426CAF9CB85DC9ACC2E00564B8BCB645C8B515200B67
- da4ad44e8185e561354d29c153c0804c11798f26915274f678db0a51c42fe656

### Responder-Windows

- 7DCCC776C464A593036C597706016B2C8355D09F9539B28E13A3C4FFCDA13DE3
- 47D121087C05568FE90A25EF921F9E35D40BC6BEC969E33E75337FC9B580F0E8

### XenArmor Email Password Recovery Pro

- 85703EFD4BA5B691D6B052402C2E5DEC95F4CEC5E8EA31351AF8523864FFC096

### XenArmor Browser Password Recovery Pro

- 4B7DE800CCAEDDEE8A0EDD63D4273A20844B20A35969C32AD1AC645E7B0398220

### Winrar

- CF0121CD61990FD3F436BDA2B2AFF035A2621797D12FD02190EE0F9B2B52A75D
- EA139458B4E88736A3D48E81569178FD5C11156990B6A90E2D35F41B1AD9BAC1

### TightVNC Viewer

- A7AD23EE318852F76884B1B1F332AD5A8B592D0F55310C8F2CE1A97AD7C9DB15
- 30B234E74F9ABE72EEFDE585C39300C3FC745B7E6D0410B0B068C270C16C5C39

### Tcpdump

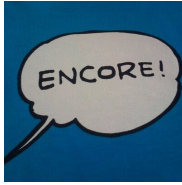
- 2CD844C7A4F3C51CB7216E9AD31D82569212F7EB3E077C9A448C1A0C28BE971B
- 1E0480E0E81D5AF360518DFF65923B31EA21621F5DA0ED82A7D80F50798B6059

### Procdump

- 5D1660A53AAF824739D82F703ED580004980D377BDC2834F1041D512E4305D07
- F4C8369E4DE1F12CC5A71EB5586B38FC78A9D8DB2B189B8C25EF17A572D4D6B7

### Wget

- C0E27B7F6698327FF63B03FCCC0E45EFF1DC69A571C1C3F6C934EF7273B1562F
- CF02B7614FEA863672CCBED7701E5B5A8FAD8ED1D0FAA2F9EA03B9CC9BA2A3BA



### [朝長 秀誠 \(Shusei Tomonaga\)](#)

Since December 2012, he has been engaged in malware analysis and forensics investigation, and is especially involved in analyzing incidents of targeted attacks. Prior to joining JPCERT/CC, he was engaged in security monitoring and analysis operations at a foreign-affiliated IT vendor. He presented at CODE BLUE, BsidesLV, BlackHat USA Arsenal, Botconf, PacSec and FIRST Conference. JSAC organizer.

### Related articles



### [Multiple Threat Actors Rapidly Exploit React2Shell: A Case Study of Active Compromise](#)

```
*key = 0x027c740d;
*key[4] = 0x21593c2;
*key[8] = 0x0e472034;
*key[12] = 0x00070000;
iv[0] = 0x12474d21;
iv[4] = 0x00000000;
iv[8] = 0x00700020;
iv[12] = 0x00700007;
v2 = m_ret_arg1offft0x350(a1 + 3);
if ( !((0->CryptAcquireContext)(a1, 0, "Microsoft Enhanced RSA and AES Cryptographic Provider", 0x10, 0x00000000) )
return 0;
v3 = m_ret_arg1offft0x350(a1 + 3);
hand1ehashubj = a1 + 1;
if ( !((0->CryptCreateHash)(*a1, 0x0000, 0, 0, a1 + 1) )
{
LABEL_0:
if ( !*a1 )
return 0;
v6 = m_ret_arg1offft0x350(a1 + 3);
(0->CryptSetHashContext)(*a1, 0);
return 0;
}
if ( !((CryptHashData)(hand1ehashubj, key, 100, 0)
|| (v8 = m_ret_arg1offft0x350(a1 + 3),
v8 = a1 + 2,
!(v8->CryptDeriveKey)(*a1, 0x0000, hand1ehashubj, 0x000000, a1 + 2) )// CALS_AES_128
{
if ( *hand1ehashubj )
{
v5 = m_ret_arg1offft0x350(a1 + 3);
(v5->CryptDestroyHash)(hand1ehashubj);
}
goto LABEL_0;
}
v10 = m_ret_arg1offft0x350(a1 + 3);
(v10->CryptSetKeyParam)(*v8, 3, 0x0000, 0); // SP_PADDING = PKCS7
v11 = m_ret_arg1offft0x350(a1 + 3);
(v11->CryptSetKeyParam)(*v8, 1, iv, 0); // iv = parameter
v12 = m_ret_arg1offft0x350(a1 + 3);
(v12->CryptSetKeyParam)(*v8, 4, 0x0000, 0); // SP_MODE = CBC
return *v8;
}
```

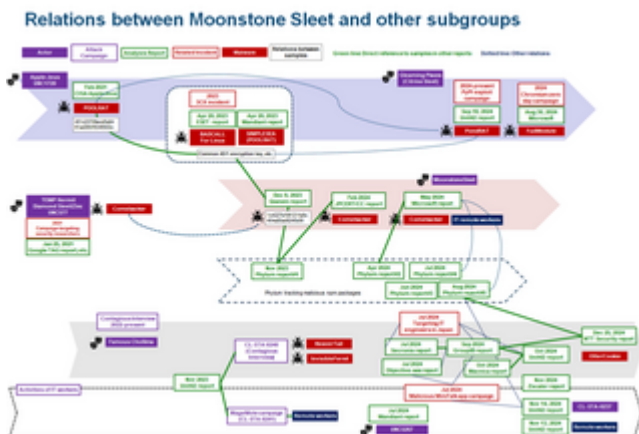
### [Update on Attacks by Threat Group APT-C-60](#)

```
python parse_crossc2beacon_config.py beacon.bin
[+] Decoded Config Data
Offset 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Encode to ASCII
000000 29 01 00 00 7F 00 00 01 B3 15 00 00 09 00 00 00 ).....
000010 31 32 37 2E 30 2E 30 2E 31 00 00 00 0C 01 00 127.0.0.1.....
000020 00 2D 2D 2D 2D 2D 42 45 47 49 4E 20 50 55 42 4C -----BEGIN.PUBL
000030 49 43 20 4B 45 59 2D 2D 2D 2D 2D 2D 0A 4D 49 47 66 I.C.KEY-----,MIGF
000040 4D 41 30 47 43 53 71 47 53 49 62 33 44 51 45 42 MA0GCSqGS1b3DQEB
000050 41 51 55 41 41 34 47 4E 41 44 43 42 69 51 4B 42 AQUAA4GNADCB1QKB
000060 67 51 43 4E 53 33 38 6C 48 50 32 56 33 4A 44 34 gQCNS381HP2V3JD4
000070 47 54 39 55 63 61 4C 68 41 6B 70 4D 64 51 41 47 GT9UcaLhAkPmDQAG
000080 52 6E 36 4E 77 36 52 48 6E 56 35 54 2F 69 48 4A Rn6Nw6RHnVST/1HJ
000090 2B 7A 48 4C 48 38 32 71 37 58 4B 6D 6F 2B 72 55 +zHLH82q7Xkmo+rU
0000A0 2B 49 7A 59 70 58 6E 57 55 37 70 4D 73 69 53 64 +IzYpXmU7pMs1Sd
0000B0 71 2B 63 52 78 4D 6F 54 4C 6D 68 4E 6F 71 32 55 q+cRxMoTmLmNoq2U
0000C0 54 57 4B 39 6F 39 52 6F 64 63 5A 7A 5A 58 73 6B TWK9o9RodcZtZXsk
0000D0 62 4D 37 54 7A 4B 37 55 5A 6A 79 61 70 54 49 4A bM7TzK7UZjyapTIj
0000E0 66 63 71 36 42 57 4D 64 73 4D 78 36 67 48 34 4F fcq6BwMdsMx6gH4O
0000F0 73 6C 42 2F 35 77 6E 63 33 77 51 78 55 62 4F 61 s1B/Swnc3wXubOa
000100 71 45 6F 6B 4B 6F 72 5A 77 6D 68 55 33 77 49 44 qEokKorZumHU3wID
000110 41 51 41 42 0A 2D 2D 2D 2D 2D 45 4E 44 20 50 55 AQAB-----END.PU
000120 42 4C 49 43 20 4B 45 59 2D 2D 2D 2D 2D 41 41 41 BLIC.KEY-----AAA
000130 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 .....
[+] Config Data
C2: 127.0.0.1:5555
PUBLICKEY: -----BEGIN PUBLIC KEY-----
MIGFMA0GCSqGS1b3DQEBQUAA4GNADCB1QKBgQCNS381HP2V3JD4GT9UcaLhAkPmDQAGRn6Nw6
RHnVST/1HJ+zHLH82q7Xkmo+rU+IzYpXmU7pMs1Sdq+cRxMoTmLmNoq2UTWK9o9RodcZtZXsk
bM7TzK7UZjyapTIjfcq6BwMdsMx6gH4Os1B/Swnc3wXubOaqEokKorZumHU3wIDAQAAB
-----END PUBLIC KEY-----
```

### [CrossC2 Expanding Cobalt Strike Beacon to Cross-Platform Attacks](#)

```
movsx ecx, cs:num7
movd xmm1, eax
cvtqdqpd xmm1, xmm1
movsx ecx, cs:num3
movd xmm0, eax
cvtqdqpd xmm0, xmm0
addsd xmm0, xmm0
subsd xmm1, xmm0
mulsd xmm1, xmm2
movsd [rbp+1410+ph0Prev], xmm1
call ret2
movsx r9d, al
call ret0
movsx ecx, al
imul r9d, ecx
call ret7
movsx eax, al
add eax, r9d
movsx ecx, cs:num9
add ecx, ecx
movsx ecx, cs:num8
xor edx, edx
div ecx
movsx ecx, cs:num1
cmp eax, ecx
jz short loc_7FF85B1895C0
call ret1
movsx edx, al
movsx eax, cs:num0
imul edx, eax
lee r8d, [rdx+rdx*2]
add r8d, r8d
call ret9
movsx ecx, al
sub r8d, ecx
call ret6
movsx ecx, al
add r8d, ecx
movsx ecx, cs:num3
add ecx, r8d
```

### [Malware Identified in Attacks Exploiting Ivanti Connect Secure Vulnerabilities](#)



### [Tempted to Classifying APT Actors: Practical Challenges of Attribution in the Case of Lazarus's Subgroup](#)

Source: [https://blogs.jpccert.or.jp/en/2021/01/Lazarus\\_tools.html](https://blogs.jpccert.or.jp/en/2021/01/Lazarus_tools.html)