Commonly Known Tools Used by Lazarus

blogs.jpcert.or.jp/en/2021/01/Lazarus_tools.html

朝長 秀誠 (Shusei Tomonaga)

January 20, 2021

Email

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	http://www.joeware.net/freetools/tools/adfind/
SMBMap	Tool to list accessible shared SMB resources and access those files	https://github.com/ShawnDEvans/smbmap
Responder-Windows	Tool to lead clients with spoof LLMNR, NBT-NS, and WPAD	https://github.com/lgandx/Responder-Windows

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

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	https://www.tightvnc.com/download.php
ProcDump	Common Microsoft's tool to get process memory dump	https://docs.microsoft.com/en-us/sysinternals/downloads/procdump
tcpdump	Packet capturing tool	https://www.tcpdump.org/
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

4B7DE800CCAEDEE8A0EDD63D4273A20844B20A35969C32AD1AC645E7B0398220

Winrar

- CF0121CD61990FD3F436BDA2B2AFF035A2621797D12FD02190EE0F9B2B52A75D
- EA139458B4E88736A3D48E81569178FD5C11156990B6A90E2D35F41B1AD9BAC1

TightVNC Viewer

- A7AD23EE318852F76884B1B1F332AD5A8B592D0F55310C8F2CE1A97AD7C9DB15
- 30B234E74F9ABE72EEFDE585C39300C3FC745B7E6D0410B0B068C270C16C5C39

Tcpdump

- 2CD844C7A4F3C51CB7216E9AD31D82569212F7EB3E077C9A448C1A0C28BE971B
- 1E0480E0E81D5AF360518DFF65923B31EA21621F5DA0ED82A7D80F50798B6059

Procdump

- 5D1660A53AAF824739D82F703ED58000498OD377BDC2834F1041D512E4305D07
- F4C8369E4DE1F12CC5A71EB5586B38FC78A9D8DB2B189B8C25EF17A572D4D6B7

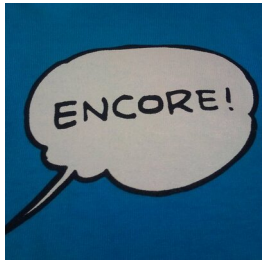
Wget

- C0E27B7F6698327FF63B03FCCC0E45EFF1DC69A571C1C3F6C934EF7273B1562F
- CF02B7614FEA863672CCBED7701E5B5A8FAD8ED1D0FAA2F9EA03B9CC9BA2A3BA

Email

Author

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.