

Lazarus attack group attack case using public certificate software vulnerability widely used by public institutions and universities

 asec.ahnlab.com/ko/48416

nuno

Feb 2023, 2

Since last year (March 2021), the Lazarus attack group's malware has been found in a number of domestic companies such as defense, satellite, software, and media companies, and the AhnLab Security Emergency Response Center (ASEC) has been continuously tracking and analyzing the activities of the Lazarus attack group and related malware.

The affected customer in this case had already been breached once by the Lazarus attack group in May 2022, and the breach recurred due to a 5-day vulnerability in the same software. At the time of the May 0 breach, the customer was using a weak version of the certificate-related program widely used in public institutions and universities, and all the software was updated to the latest version after the accident. This time, however, it was breached by a 2022-day vulnerability in the software.

ASEC has reported the software to KISA, but the vulnerability has not been clearly identified, and the manufacturer and software are not disclosed in this article because no software patch has been released yet.

In addition to this incident, the Lazarus Group is continuously researching various software vulnerabilities to infiltrate domestic institutions and companies, and is continuously changing TTP by disabling security products, and using anti-forensic technologies to hinder and delay detection and analysis.

This report is based on the victim's forensic analysis report. The report was prepared in January, but after delaying disclosure due to software vulnerability patching issues, the company decided to release the software information after anonymizing it. When a software patch is released, we will redistribute a report of the version that released the information.

Outline of the incident

CATEGORY	DESCRIPTION
Duration of the incident	2022/10/21 ~ 2022/11/18
Customer Type	Financial Business
Damage System Type	Windows 10
Damage Status	Backdoor malware infection and C2 communication
Types of attacks	<ul style="list-style-type: none">• Lateral movement using 0-Day vulnerability of company A's certificate program ※ Since the patch has not yet been released, vulnerable software information is not disclosed• Disabling vaccines through BYOVD attacks• Anti-forensics<ul style="list-style-type: none">◦ Timestamp operation◦ Change the file name randomly and delete it◦ Delete execution artifacts◦ Use the same file name as the system file name
assailant	Lazarus

Summary of analysis results

After analyzing the two PCs received from the customer, it was confirmed that PC01 and PC02 were subjected to lateral movement attacks using vulnerabilities in the certificate software. PC02 was attacked from an unidentified internal system on October 10, and PC21 was attacked by PC01 on November 11. Given that PC18 and PC02 had the latest version of certificate software installed, it is believed that the attacker used a 01-Day vulnerability. In addition, PC02 and PC0 experienced Vo1 incapacitation on November 02, but a different method was used.

The system analyzed this time was subjected to a lateral movement attack and was not related to the initial influx of attackers. It is believed that the victim's Internet network was threatened by the Lazarus attack group, which successfully broke in in May.

SYSTEM	DATE	DESCRIPTION	
PC01	2022/11/18	Lateral movement attack due to certificate software vulnerability (PC02 → PC01)	
	2022/11/18	V3 Disabling Occurs	
PC02	2022/10/21	Lateral movement attack due to certificate software vulnerability (unknown internal system → PC02)	
	2022/11/18	V3 Disabling Occurs	

[Table] Major malicious actions by each system

PC01 Analysis

PC01 is believed to have been compromised by a 2022-Day vulnerability attack in certificate software on 11/18/10 00:35:0. Three network connection attempts were made from PC02 to the service TCP port of PC01's certificate software. In the previous two connections, there was no special response from PC01, but when PC02 accessed PC11 at 18:10 on 00/01 using skype.exe (unsecured) created using svchost.exe, PC01 encountered an error (AppCrash) in the certificate software, and malicious actions began thereafter. When AppCrash occurred, all error reports (WARs) and memory dump files stored in the system were deleted and could not be checked. It appears to have been intentionally deleted by the attackers.

DATE TIME	DESCRIPTION	REMARKS
2022/11/15 16:18:52	svchost.exe network connection 10.20.XXX.125:XXXXX	Presumed to be an attack failure or connection test
2022/11/18 9:49:31	svchost.exe network connection 10.20.XXX.125:XXXXX	Presumed to be an attack failure or connection test
2022/11/18 10:00:27	network connection .exe skype.exe 10.20.XXX.125:XXXXX	Successful exploits

[Table] History of access from PC02 to certificate software service port of PC01 (V3 behavior log)

아티팩트 정보

파일 이름 AppCrash_██████████.exe_9474ee13fbc7651aabaf2f3c9b1fedc9e7489e51_bc343f60_cab_ddd4e0eb-714c-4cf4-ae23-43cd18c59603

일련 번호 업데이트 6029131104

타임스탬프 날짜/시간 2022-11-18 AM 10:00:35

이유 The file or directory is created for the first time.

MFT 레코드 수 42893

MFT 참조 번호 34339947158742925


상위 MFT 레코드 수 1997

부모 MFT 참조 번호 281474976712653

파일 특성 The handle that identifies a directory.
A file or directory that is compressed.

소스 정보 Normal Event

보안 ID 0

유형  UsnJrnl

항목 ID 282826

[Figure] Record of Crashdump File Generation in Certificate Software

Among the traces identified in PC01, the difference from the attack that occurred in May is that the process used after the vulnerability attack in the certificate software was svchost.exe rather than ftp.exe, and the vulnerable version of the software was installed at the time, but this time all the latest versions were installed, so there is no known vulnerability information.

TARGET	INSTALL DATE	SOFTWARE VERSION	COMPROMISED DATE
PC01	2022/07/01	Up-to-date	2022/11/18
PC02	2022/08/30	Up-to-date	2022/10/21

[table] Certificate software versions installed on PC01 and PC02

After accessing PC01, the attacker injected a malicious thread into a normal process (svchost.exe) and used it for C2 communication and backdoor. It then neutralized the V3 product installed on the system, and created and executed additional malicious files.

In addition, in this analysis, traces of manipulation of the timestamp of malicious files were confirmed, and anti-forensic behaviors such as randomly changing and deleting file names when deleting files were found, so it seems that attackers are actively interfering with the analysis.

TIMELINE (PC01)

The timeline of the infringement identified in PC01 is as follows:

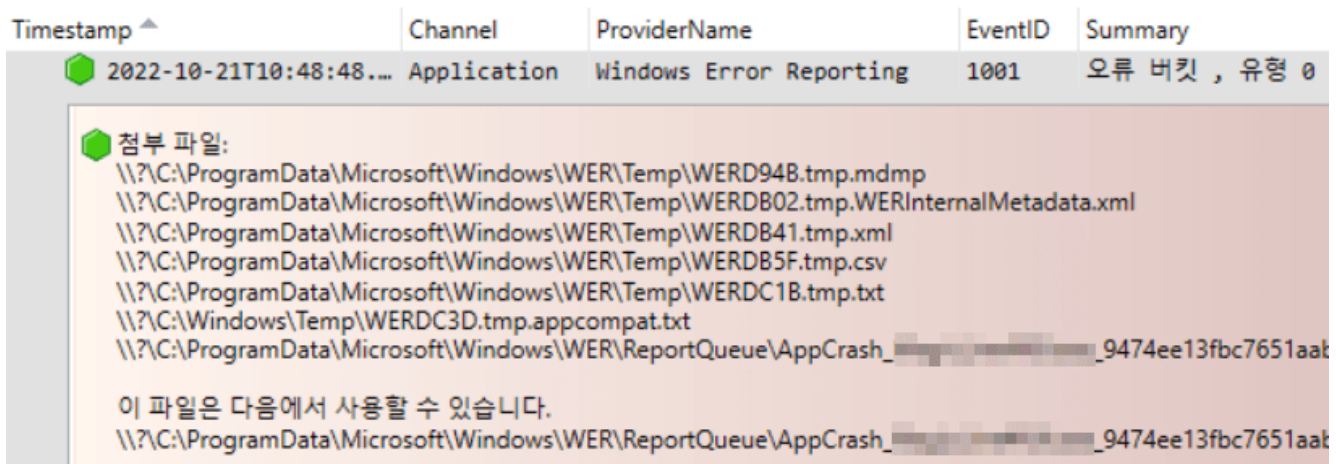
TIME (22/11/18)	CATEGORY	BEHAVIORS
10:00:37	injection	svchost.exe injects a malicious thread into a running process to start malicious activity

10:00:37	C2 communication	svchost.exe connects to the attacker's C2 address 121.78.246.155(dalbinews.co.kr)
10:10:01	Malicious file creation	Malicious file creation C:\ProgramData\tszui.tmp (unsecured)
10:17:55	Anti-forensics	Rename and delete malicious files Rename: C:\ProgramData\tszui.tmp -> Delete phqghumeaFile : C:\ProgramData\phqghumea (unsecured)
10:18:47	C2 communication	svchost.exe connects to the attacker C2 address 121.78.158.46 (www.studyholic.com)
10:20:28	Neutralize security products	V3 detects security product incapacitation (Exploit/Win.Lazardoor.GEN)
10:20:24	C2 communication	Network connection to attacker C2 183.110.224.172 (ctmnews.kr)
10:27:58	Malicious file creation	Malicious file creation C:\ProgramData\perlcritic.exe (unsecured)
10:28:53	Generate vulnerable driver files	Malicious file execution C:\ProgramData\perlcritic.exe (unsecured)Driver file creation (not malicious) C:\Windows\System32\drivers\PROCEXP152.SYS (secured)
10:29:16	Malicious file creation	Malicious file creation C:\ProgramData\tds.tmp (unsecured)
10:29:36	Anti-forensics	Rename and delete malicious files Rename: C:\ProgramData\tds.tmp -> mxnsbqyDelete files: C:\ProgramData\mxnsbqy (unsecured)
10:41:33	Anti-forensics	Delete AppCrash File Delete File : C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_XXXXXXXXXXXX.exe_9474ee13fbc7651aabaj2f3c9b1fedc9e7489e51_bc343f60_ddd4e0eb-714c-4cf4-ae23-43cd18c59603 (unsecured)
10:42:19	Anti-forensics	Rename and delete malicious files Rename: C:\ProgramData\perlcritic.exe -> kxlmatoynktxlDelete files: C:\ProgramData\kxlmatoynktxl (unsecured)
10:44:31	Malicious file creation	Create (secure) backdoor loader (LegacyUserManager.dll) Loading target file: C:\ProgramData\Microsoft\Crypto\Keys\Keys.dat (secured) C:\ProgramData\Microsoft\Settings\Settings.vwx (secured)
10:44:47	Anti-forensics	Timestamp (Standard Information) operation of the backdoor loader (LegacyUserManager.dll) (Secure)
10:45:47	Malicious file creation	Creation (Secured) of backdoor program (Keys.dat) Creation of malware with C2 access and file download function
10:45:56	Anti-forensics	Timestamp (Standard Information) manipulation (Secured) of backdoor program (Keys.dat)
10:46:12	Malicious file creation	Creation of backdoor program (Settings.vwx) (secured) Creation of malware with C2 access and file download function
10:46:30	Anti-forensics	Timestamp (Standard Information) manipulation (Secured) of backdoor program (Keys.dat)

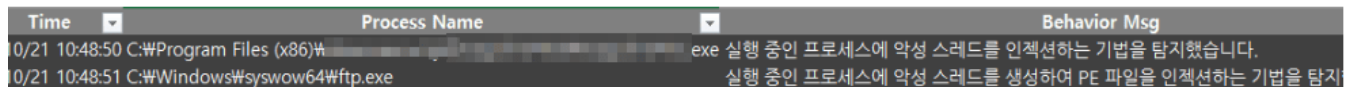
[table] Malicious behavior of attackers found on PC01

PC02 Analysis

The attacker was found to have accessed PC10 by exploiting a vulnerability in the certificate software on 21/10 48:48:02. AppCrash occurred during the attack of the vulnerability, after which the ftp.exe was executed and malicious behavior began. This is the same method that occurred in the affected customer in May. The IP of the system that accessed PC5 has not been determined.



[Picture] Certificate Software Error Log Verified on PC02 (Application.evtx)



[Picture] Certificate software found in Vo2 MDP log on PC3 and malicious thread injection code in ftp.exe

After first infiltrating PC10 on 21/02, the attacker created a malicious file that performed C2 server communication and backdoor functions through an injected ftp.exe.

On 10/27, unlike the attack on the 21st, instead of ftp.exe, it injected a malicious thread into the SVChost.exe process, after which it carried out malicious actions with control until 11/18.

On 11/15, it was confirmed that an FSWss file .exe was created to scan the internal network. After that, it was confirmed that he used svchost.exe to connect to the service port of PC01's certificate software twice.

On 11/18, a skype-server.exe file was created and the file was used to access PC01's TCP XXXXXX, and at this time, an AppCrash of the certificate software occurred on PC01, and then PC02 confirmed traces of disabling antivirus, creating and executing malicious files, etc., the same as PC01.

TIMELINE (PC02)

The timeline of the infringement identified in PC02 is as follows:

DATE	TIME	CATEGORY	BEHAVIORS
22/10/21	10:48:50	C2 communication	ftp.exe connects the attacker to the C2 address and the network 111.92.189.48 (www.scope.co.kr)
	10:48:51		ftp.exe connects the attacker C2 address and network 183.110.224.172 (ctmnews.kr)

	10:49:46		ftp.exe connects the attacker C2 address to the network 115.68.52.47 (www.artinsight.co.kr)
	10:51:35		ftp.exe connects the attacker to C2 address and network 114.108.129.89 (www.kfcjn.com)
	10:52:31		ftp.exe connects the attacker to C2 address and network 114.108.129.89 (www.kfcjn.com)
	10:59:33		ftp.exe connects the attacker to C2 address and network 114.108.129.89 (www.kfcjn.com)
	12:52:38		ftp.exe connects the attacker to C2 address and network 119.207.79.175 (lightingmart.co.kr)
	14:21:58	Malicious file creation	ftp.exe create file C:\Windows\System32\legacyusermanager.dll (secured)
	14:59:07		ftp.exe file created C:\Windows\System32\wptsextensions.dll (secured)
	15:34:47	Anti-forensics	Rename a malicious file Rename: C:\Windows\System32\legacyusermanager.dll -> C:\Windows\temp\lum.tmp (secured)
22/10/27	15:25:00	injection	Injecting malicious threads into normal processes (svchost.exe)
	15:26:05	C2 communication	svchost.exe connects the attacker with C2 address 115.68.52.47
	15:27:53	Malicious file creation	svchost.exe created malicious file C:\Windows\System32\wptsextensions.dll (secured)
22/11/15	11:32:36	Create a file	svchost.exe created malicious file C:\ProgramData\fsyss.exe (unsecured)
	11:32:48	File execution	Network scanning with fsyss.exe C:\ProgramData\fsyss.exe /scan /UseIPAddressesRange 1 /IPAddressFrom 10.20.XXX.1 /IPAddressTo 10.20.XXX.255 /stext C:\ProgramData\fsyss.log
	11:33:41	Anti-forensics	Rename malicious files Rename: C:\ProgramData\fsyss.exe -> xeudsgpfo (unsecured)
	12:50:13	Malicious file creation	svchost.exe creates file C:\ProgramData\fmssysn.exe (not secured)
	12:51:04	Execution of malicious files	svchost.exe runs other processes C:\ProgramData\fmSysN.exe 10.20.XXX.1 10.20.XXX.36 XXXXX 10 c:\programdata\fmSysN.log

	13:06:49	Anti-forensics	Rename malicious files: C:\ProgramData\fmsysn.exe -> yfvepuvxbi (not secured)
	16:18:52	Network Access	svchost.exe attempts to access certificate software port on PC01 10.20.XXX.125:XXXXX(PC01)
	16:33:06	Malicious file creation	svchost.exe creates file C:\ProgramData\skypeserver.exe (unsecured)
22/11/18	9:49:31	Network Access	svchost.exe attempts to access certificate software port on PC01 10.20.XXX.125:XXXXX(PC01)
	9:51:07	악성파일 생성	svchost.exe created malicious file C:\ProgramData\skypeserver.exe (unsecured)
	9:56:31		svchost.exe가 악성파일 생성 C:\ProgramData\sfbappsdk.dll (미확보)
	10:00:08	C2 통신	skypeserver.exe가 공격자 C2주소와 네트워크 연 결 121.78.246.155(dalbinews.co.kr)
	10:00:27	네트워크 접근	skypeserver.exe가 인증서 소프트웨어 포트에 접근 성공 10.20.XXX.125:XXXXX(PC01)
	10:06:14	안티 포렌식	악성파일 이름 변경 이름 변경: C:\ProgramData\sfbappsdk.dll -> bxikemvqhcz (미확보)
	10:06:42		악성파일 이름 변경 변경 전: C:\ProgramData\skypeserver.exe -> kqcfqbxbgfbmwem (미확보)
	11:04:32	인젝션 C2 연결	정상 프로세스(svchost.exe)에 악성 스레드 인젝션 svchost.exe가 공격자 C2주소와 네트워크 연결 121.78.158.46(studyholico.co.kr)
	11:05:45	보안 제품 무력화	V3가 보안 제품 무력화 행위 탐지 (Exploit/Win.Lazardoor.GEN)
	11:06:56	취약한 드라이버 파일 생성	악성코드 생성 C:\ProgramData\perlcratic.exe (미확보)
	11:07:02		악성코드 실행 C:\ProgramData\perlcratic.exe (미확보)취약한 드라 이버 파일 생성 C:\Windows\System32\drivers\PROCEXP152.SYS (확보)
	11:12:18		악성코드 생성 및 실행 C:\ProgramData\perlcratic64.exe (미확보)

[표] PC02에서 발견된 공격자의 악성 행위

Major malicious acts

Disabling V3 by BYOVD

In the PC01 and PC02 systems, an attempt to disable V11 was detected (Exploit/Win.Lazardoor.GEN) at 18/10 20:28:11 and 05:45:3, respectively, and the period after which V3 was disabled is as follows:

- PC01: 11/18 10:20:28 ~ 11/18 11:25:00 (about 1 hour)
- PC02: 11/18 11:05:45 ~ 11/21 14:07:08 (about 75 hours)

During this period, V3-related processes are running, but normal behavior detection is not possible. However, after the system reboots, V3 returns to normal.



[Picture] Vo1 Neutralization Detection Log Seen on PC3

Attackers need access to kernel memory to manipulate kernel memory on Windows systems to disrupt the operation of security products, and in May, Taiwanese component manufacturer ENE Technology's ene.sys was used in a BYOVD attack.

At the time of detection of Vo1 incapacitation of PC02 and PC3, no trace of the attack method was found. Rather, a vulnerable driver file was created on the system after the V3 outbreak, which is the driver file of Procexp152 of ProcessExplorer, a process management utility provided .SYS free of charge by Microsoft, and is a vulnerable driver that can be used for BYOVD attacks. However, this driver file was created after Vo1 defeat on both PC02 and PC3, and was used by the perlcritic.exe (unsecured) file generated by the attacker.

In other words, the order of V3 defeat occurrence time and driver file creation time does not match, so it is a BYOVD attack, PROCXP152. It is not yet possible to say whether SYS was used to neutralize V3.

The method that occurred in May and the method that occurred in November have the following differences.

CATEGORY	ATTACK IN MAY, 2022	ATTACK IN NOVEMBER, 2022
Attack Techniques	BYOVD Technique	Not verified
Vulnerable drivers	Drivers from ENE Technology ene.sys	Microsoft's ProcessExplorer driver was created after V3 disabled PROCEXP152.sys
loader	sb_smbus_sdk.dll	<ul style="list-style-type: none"> perlcratic.exe (not secured) perlcratic64.exe (unsecured)
Service registration	Service registered	No sign of service registration

[Table] Comparison of traces related to V5 incapacitation in May and November

Antiforensics

PC01 and PC02 were found to have performed antiforensic actions to erase the traces of the attack.

CATEGORY	SYSTEM	DESCRIPTION
Manipulating timestamps on files	PC01, PC02	<p>[PC01]</p> <ul style="list-style-type: none"> C:\Windows\System32\LegacyUserManager.dll Manipulated creation time : 2019-03-19 13:49:35 C:\ProgramData\Microsoft\Crypto\Keys\Keys.dat <ul style="list-style-type: none"> Manipulated creation time : 2019-03-19 13:49:35 Manipulated/created time : 2019-12-25 23:24:06 C:\ProgramData\Microsoft\Settings\Settings.vwx Manipulated creation time : 2022-05-13 16:09:19 <p>[PC02]</p> <p>C:\Windows\system32\wptsextensions.dll Manipulated creation time : 2019-03-19 13:49:35</p>
Delete a file after renaming a file	PC01, PC02	<p>[PC01]</p> <ul style="list-style-type: none"> C:\ProgramData\tszui.tmp -> phqghumea C:\ProgramData\perlcratic.exe -> kxlmamoynktxl C:\ProgramData\tds.tmp -> mxnsbqy <p>[PC02]</p> <ul style="list-style-type: none"> C:\ProgramData\fsyss.exe -> xeudsgpfo C:\ProgramData\fmssysn.exe -> yfvepuvxbi C:\ProgramData\sfbappsdk.dll -> bxikemvqhcsz C:\ProgramData\skypeserver.exe -> kqcfqbxbgfbmwem
Delete Prefetch	PC01	MSIEXEC.EXE-8FFB1633.pf, PERLCRATIC.EXE-2EB3AC0F.pf and many more

Malware used by attackers

List of malware

CATEGORY	FILENAME	SYSTEM	DESCRIPTION
loader	wptsextensions.dll	PC02	<ul style="list-style-type: none"> Path: C:\Windows\System32\wptsextensions.dll Load Backdoor File Keys.dat
	legacyusermanager.dll	PC01 PC02	<ul style="list-style-type: none"> Path: C:\Windows\System32\legacyusermanager.dll Load Backdoor File Keys.dat
	lum.tmp	PC02	<ul style="list-style-type: none"> Path: C:\Windows\Temp\lum.tmp Load the backdoor file configmanager.tlb
backdoor	Keys.dat	PC01 PC02	<ul style="list-style-type: none"> Path: C:\ProgramData\Microsoft\Crypto\Keys\Keys.dat loaded by wptsextensions.dll 2022/11/18 14:56:54 GMT Designed to run after +9, additional commands can be performed via cmd.exe Downloads additional binaries from the C2 server and runs them in fileless form
	Settings.vwx	PC02	<ul style="list-style-type: none"> Loaded in wptsextensions.dll Randomly access from the following 3 C2s <ul style="list-style-type: none"> hxxps://www.artinsight[.]co.kr/data/admin/list.php hxxps://www.kfcjn[.]com/member/process/sms.php hxxps://ctmnews[.]kr/member/process/success.php
	Settings.vwx	PC01	<ul style="list-style-type: none"> Loaded in legacyusermanager.dll Randomly access from the following 3 C2s <ul style="list-style-type: none"> hxxps://www.artinsight[.]co.kr/data/admin/list.php hxxps://www.kfcjn[.]com/member/process/sms.php hxxps://ctmnews[.]kr/member/process/success.php
Exploited legitimate files	ProcEXP152.sys	PC01 PC02	<ul style="list-style-type: none"> Path: C:\Windows\System32\drivers\PROCEXP152.SYS Drivers in ProcessExplorer Vulnerable driver module enables antivirus neutralization through BYOVD attacks
	fswss.exe	PC02	<ul style="list-style-type: none"> Path: C:\ProgramData\fswss.exe NirSoft utility with the ability to scan the network or turn on a remote computer WakeMeOnLan: https://www.nirsoft.net/utils/wake_on_lan.html

Unsecured files	configmanager.tlb	PC02	<ul style="list-style-type: none"> Path: C:\Windows\System32\configmanager.tlb Backdoor estimation loaded by lum.tmp
	perlcrlic.exe perlcrlic64.exe	PC01 PC02	<ul style="list-style-type: none"> Path: C:\ProgramData\perlcrlic.exe Executed by cmd.exe and loads PROCEXP152.SYS
	sfbappsdk.dll	PC02	<ul style="list-style-type: none"> Path: C:\ProgramData\sfbappsdk.dll Injected svchost.exe created
	fmSysN.exe	PC02	<ul style="list-style-type: none"> Path: C:\ProgramData\fmSysN.exe Injected svchost.exe created The following traces of execution have been identified: fmSysN.exe 10.20.XXX.1 10.20.XXX.36 XXXXX 10 c:\programdata\fmSysN.log
	skypeserver.exe	PC02	<ul style="list-style-type: none"> Path: C:\ProgramData\skypeserver.exe Injected svchost.exe created C2 Connection
	tds.tmp	PC01	<ul style="list-style-type: none"> Path: C:\ProgramData\tds.tmp Deleted after being changed to a random file name
	tszui.tmp	PC01	<ul style="list-style-type: none"> Path: C:\ProgramData\tszui.tmp Deleted after being changed to a random file name

[table] List of malware

C2 used by attackers

CATEGORY	IP	DOMAIN	REMARKS
ftp.exe 최초 접근	111.92.189.48	www[.]scope.co.kr	
무력화 관련 C2 추정	121.78.158.46	www[.]studyholic.com	
	121.78.246.155	dalbinews[.]co.kr	
백도어 C2	119.207.79.175	—	5월 공격에도 사용됨
	183.110.224.172	ctmnews[.]kr	
	211.249.220.83	ctmnews[.]kr	
	1.254.179.18	www[.]artinsight.co.kr	
	103.6.182.57	www[.]artinsight.co.kr	
	104.109.245.186	www[.]artinsight.co.kr	
	112.106.58.23	www[.]artinsight.co.kr	
	115.68.52.47	www[.]artinsight.co.kr	

125.209.218.167	www[.]artinsight.co.kr	
3.39.49.255	www[.]artinsight.co.kr	
34.199.186.157	www[.]artinsight.co.kr	
52.148.148.114	www[.]artinsight.co.kr	
104.21.64.83	www[.]kfcjn.com	
112.106.58.23	www[.]kfcjn.com	
114.108.129.89	www[.]kfcjn.com	
117.52.137.138	www[.]kfcjn.com	
13.107.21.200	www[.]kfcjn.com	
162.247.241.2	www[.] kfcjn.com	
23.50.0.140	www[.] kfcjn.com	
52.79.120.37	www[.] kfcjn.com	

[table] List of C2s used by attackers

MITRE ATT&CK MAPPING

Tactics	TID	DESCRIPTION
Reconnaissance	–	–
Resource Development	T1587.001 Develop Capabilities: Malware	Backdoor and loader fabrication
	T1587.004 Develop Capabilities: Exploits	Prepare for certificate software vulnerabilities
	T1588.002 Obtain Capabilities: Tool	fswss.exe (wakemeonlan by Nirsoft.exe)
Initial Access	N/A	
Execution	T1059.003 Command and Scripting Interpreter: Windows Command Shell	Run perlcritic.exe
	T1203 Exploitation for Client Execution	Certificate Software Exploits
Persistence	N/A	–

Privilege Escalation	<u>T1068 Exploitation for Privilege Escalation</u>	PROCEXP152.sys
Defense Evasion	<u>T1562.001 Impair Defenses: Disable or Modify Tools</u>	V3 Incapacitation
	<u>T1070 Indicator Removal</u>	Delete Prefetch files
	<u>T1070.004 Indicator Removal: File Deletion</u>	Delete malicious files – sfbappsdk.dll, fswss.exe, fmSysN.exe, skypeserver.exe, perlcritic.exe, perlcritic64.exe Delete crashdump files
	<u>T1070.006 Indicator Removal: Timestomp</u>	Change malicious file time information
Credential Access	N/A	–
Discovery	<u>T1046 Network Service Discovery</u>	fswss.exe, fmSysN.exe
Lateral Movement	<u>T1210 Exploitation of Remote Services</u>	Internal movement using certificate software vulnerabilities
Collection	N/A	–
Command and Control	<u>T1071.001 Application Layer Protocol: Web Protocols</u>	C2Server Communication
	<u>T1102 Web Service</u>	Exploiting legitimate domains as C2 servers
Exfiltration	N/A	–
Impact	N/A	–

IoC

Malicious files

No	MD5 Hash	File Name	AhnLab Detection Name
1	61B3C9878B84706DB5F871B4808E739A	wptsextensions.dll	Trojan/Win.Lazardoor.C5327680
2	C7256A0FBAB0F437C3AD4334AA5CDE06	legacyusermanager.dll	Trojan/Win.Lazardoor.C5327680
3	A6602EF2F6DC790EA103FF453EB21024	lum.tmp	Trojan/Win.Lazardoor.C5327681
4	FC8B6C05963FD5285BCE6ED51862F125	Keys.dat (PC01)	Data/BIN. Lazarus
5	6EA4E4AB925A09E4C7A1E80BAE5B9584	Keys.dat (PC02)	Data/BIN. Lazarus
6	27DB56964E7583E19643BF5C98FFFD52	Settings.vwx (PC01)	Data/BIN. Lazarus
7	BD47942E9B6AD87EB5525040DB620756	Settings.vwx (PC02)	Data/BIN. Lazarus

Malicious IP/URL

No	IP	URL	Country
1	111.92.189.48	www[.]scope.co.kr	KR
2	121.78.158.46	www[.]studyholic.com	KR
3	121.78.246.155	dalbinews[.]co.kr	KR
4	119.207.79.175	–	KR
5	183.110.224.172	ctmnews[.]kr	KR
6	211.249.220.83	ctmnews[.]kr	KR
7	1.254.179.18	www[.]artinsight.co.kr	KR
8	103.6.182.57	www[.]artinsight.co.kr	KR
9	104.109.245.186	www[.]artinsight.co.kr	US
10	112.106.58.23	www[.]artinsight.co.kr	KR
11	115.68.52.47	www[.]artinsight.co.kr	KR
12	125.209.218.167	www[.]artinsight.co.kr	KR
13	3.39.49.255	www[.]artinsight.co.kr	US
14	34.199.186.157	www[.]artinsight.co.kr	US
15	52.148.148.114	www[.]artinsight.co.kr	US
16	104.21.64.83	www[.]kfcjn.com	US
17	112.106.58.23	www[.]kfcjn.com	KR
18	114.108.129.89	www[.]kfcjn.com	KR
19	117.52.137.138	www[.]kfcjn.com	KR
20	13.107.21.200	www[.]kfcjn.com	US
21	162.247.241.2	www[.]kfcjn.com	US
22	23.50.0.140	www[.]kfcjn.com	US
23	52.79.120.37	www[.]kfcjn.com	US

Detailed analysis information on related IOCs can be accessed through the subscription service of AhnLab's next-generation threat intelligence platform 'AhnLab TIP'.

Categories:Malware Information

Tagged as:A-FIRST,BYOVD,DFIR,Infringement Case,Lazarus