TLP: GREEN

Anti-Forensic Techniques Used By Lazarus Group

V1.0

AhnLab Security Emergency Response Center (ASEC)

Feb. 23, 2023

AhnLab

Classification

Publications or provided content can only be used within the scope allowed for each classification as shown below.

Classification	Distribution Targets	Precautions
TLP: RED	Reports only provided for certain clients and tenants	**Documents that can only be accessed by the recipient or the recipient department** Cannot be copied or distributed except by the recipient
TLP: AMBER	Reports only provided for limited clients and tenants	**Can be copied and distributed within the recipient organization (company) of reports** Must seek permission from AhnLab to use the report outside the organization, such as for educational purposes
TLP: GREEN	Reports that can be used by anyone within the service	**Can be freely used within the industry and utilized as educational materials for internal training, occupational training, and security manager training** Strictly limited from being used as presentation materials for the public
TLP: WHITE	Reports that can be freely used	Cite source Available for commercial and non-commercial uses Can produce derivative works by changing the content

AhnLab

Remarks

The version information of this report is as follows:

Version	Date	Details
1.0	2023-02-23	First version

Contents

⚠️ CAUTION

This report contains a number of opinions given by the analysts based on the information that has been confirmed so far. Each analyst may have a different opinion and the content of this report may change without notice if new evidence is confirmed.

Overview

Since approximately a year ago, the Lazarus group's malware has been discovered in various Korean companies related to national defense, satellites, software, and media press. AhnLab has been continuously tracking the Lazarus threat group's activities and other related TTPs.

Among the recent cases, this post aims to share the anti-forensic traces and details found in the systems that were infiltrated by the Lazarus group.

Definition of Anti-Forensics

Currently, ransomware creators include individuals, cyber criminal gangs and state-supported groups. Out of these individuals and groups, cyber criminal gangs are the most proactive in ransomware development, while individuals and state-supported groups are less so. Privately developed ransomware is most often for research purposes with the intention of destroying data. Some state-sponsored threat groups also develop ransomware. The purpose of these cases is not for financial gain either but for data destruction, and Wipers, which do not allow recovery, are created disguised as ransomware.

Anti-forensics refers to the tampering of evidence in an attempt to mitigate the effectiveness of a forensics investigation at a crime scene. From a breaching point of view, anti-forensics generally have the following objectives.

- Detection evasion and obstruction of information collection
- Increase the analysis time of digital forensic analysts
- Disable or cause the malfunction of digital forensic tools
- Block, bypass or delete logs to hide traces of access or execution of tools

The Lazarus group carried out anti-forensics to conceal their malicious acts.

Anti-Forensic Techniques

While there are various standards on the classification of anti-forensic techniques, this post will use the most widely received anti-forensic classification proposed by Dr. Marcus Roger to distinguish and analyze concealment measures taken by the Lazarus group.

Dr. Marcus Roger classified anti-forensic techniques which hinder forensic analysis into 5 main categories: data hiding, artifact wiping, trail obfuscation, attacks against computer forensics, and physical.

Looking at the 5 categories above, the Lazarus group utilized data hiding, artifact wiping, and trail obfuscation, a total of 3 techniques.

1) Data Hiding

Data hiding refers to the method of data concealment that renders their detection difficult. Major examples include data obfuscation, encryption, steganography, and hiding data in non-allocated areas.

Encryption

The Lazarus group distinguished and used their malware in 3 parts. The loader, executable file, and configuration file. The major features of each file are as follows.

- Loader: Decrypts encrypted PE files and loads them onto the memory
- Encrypted PE: A malware that runs on the loader memory and decrypts encrypted configuration files to communicate with the C2 address.
- Encrypted Config: An encrypted configuration file that contains C2 information.

The Lazarus group transmits the configuration file that has the C2 information and the PE file that communicates with the C2 in encrypted forms to evade detection by security products. The encrypted files operate after being decrypted onto the memory by the loader file. They then receive additional files from the C2 and perform malicious acts.
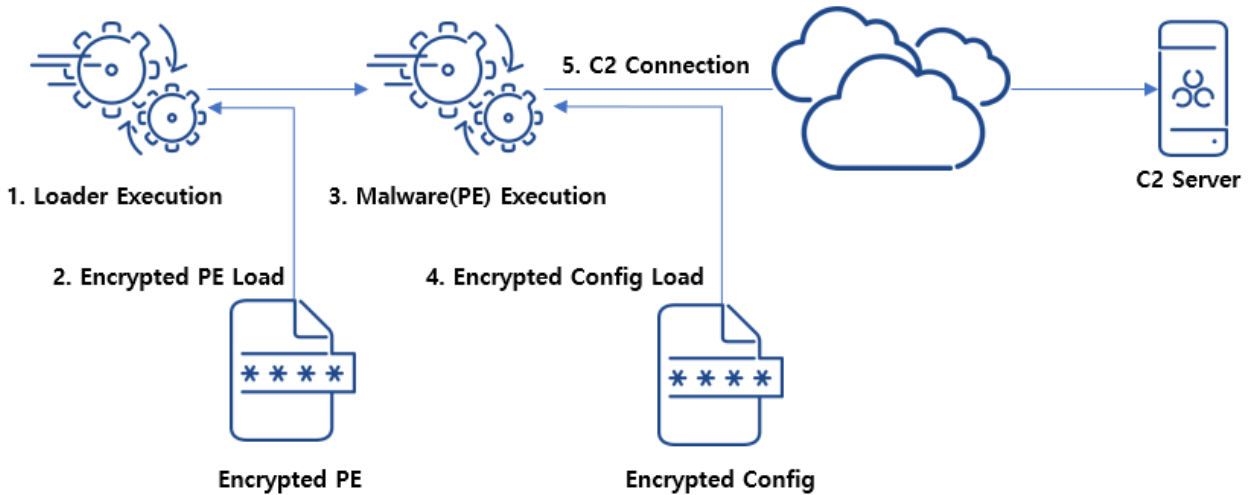
Figure. Backdoor operation process

Other Forms of Data Hiding

The Lazarus group either used a system folder as a hiding place or imitated the name of a normal file to hide their malware. The default system folders are where their malware hiding is mainly done. The malware is hidden by either creating a similar folder within the system or by disguising the malware as a normal file within a system file that's hidden by default.

- C:₩ProgramData₩
- C:₩ProgramData₩Microsoft₩
- C:₩Windows₩System32₩

The C:₩ProgramData folder is a default system folder which is hidden by default. A folder with a name similar to the default folder (MicrosoftPackages) is created inside this folder as a malware hiding place or the malware is disguised as a similar file inside the default folder.

Filename #1	Std Info Creation date	Std Info Modification d	Std Info Access date	Std Info Entry date
/ProgramData/MicrosoftPackages	2021/11/29 05:37:53.717	2021/12/14 04:44:58.236	2021/12/14 04:44:58.279	2021/12/14 04:44:58.236
/ProgramData/MicrosoftPackages/Nwsapagentc.dat	2021/11/29 05:39:45.396	2021/11/30 00:11:28.099	2021/11/30 00:11:28.099	2021/11/30 00:11:28.099
/ProgramData/MicrosoftPackages/Nwsapagentd.dat	2021/11/29 05:40:06.120	2021/11/29 05:40:12.515	2021/11/29 05:40:12.515	2021/11/29 05:40:12.515

Figure. Similar folder created to use as a malware hiding place

Filename #1	FN Info Creation date	Std Info Creation date	Std Info Modification d	Std Info Access date
/ProgramData/Microsoft/Crypto/Keys/Keys.dat	2022-11-18 01:45:47.782	2019-12-25 14:24:06.781	2019-12-25 14:24:06.784	2022-02-17 22:43:58.485
/ProgramData/Microsoft/Settings/Settings.vwx	2022-11-18 01:46:12.796	2022-05-13 07:09:19.310	2022-11-21 01:34:41.790	2022-11-21 01:34:41.790

Figure. Hiding malware by imitating default folder names

AhnLab

2) Artifact Wiping

Artifact wiping refers to the task of permanently deleting specific files or the whole file system. Not only does it involve file deletion, but expert tools can also be used to erase all traces of use. For example, the Disk Clean-up utility, file deletion, and disk demagnetization are all included in artifact wiping.

File Wiping

Excluding the backdoor malware, the Lazarus group deleted the malware and the artifacts that occurred while the malicious behavior was being performed. In the malware's case, its data was overwritten and its filename was changed before being deleted.

The original file content can no longer be seen if the data section is overwritten during file deletion since this makes data recovery through methods such as file restoration and data carving difficult.

FileName	FullPath	Event	SourceInfo	FileAttr
필터	필터	필터	필터	필터
perlcritic.exe	₩ProgramData₩perlcritic.exe	Data_Overwritten / File_Closed	Normal	Archive
perlcritic.exe	₩ProgramData₩perlcritic.exe	File_Renamed_Old	Normal	Archive
kxlmatmoynktxl	₩ProgramData₩kxlmatmoynktxl	File_Renamed_New	Normal	Archive
kxlmatmoynktxl	₩ProgramData₩kxlmatmoynktxl	File_Renamed_New / File_Closed	Normal	Archive
kxlmatmoynktxl	₩ProgramData₩kxlmatmoynktxl	File_Closed / File_Deleted	Normal	Archive

Figure. Malware deletion log confirmed in USNJrnl

The Lazarus group also deleted artifacts related to their malware execution at the same time. For example, the prefetch files, which are artifacts related to application execution, were collectively deleted to remove traces of the malware being executed.

TimeStamp	FileName	FullPath	Event	SourceInfo	FileAttr
필터	필터	.pf ✕	delete ✕	필터	필터
2022-11-18 08:27:21	SVCHOST.EXE-364C46CF.pf	₩Windows₩prefetch₩SVCHOST.EXE-364C46CF.pf	File_Closed / File_Deleted	Normal	Archive…
2022-11-18 08:27:21	VSSVC.EXE-6C8F0C66.pf	₩Windows₩prefetch₩VSSVC.EXE-6C8F0C66.pf	File_Closed / File_Deleted	Normal	Archive…
2022-11-18 08:27:21	SVCHOST.EXE-D586BDCE.pf	₩Windows₩prefetch₩SVCHOST.EXE-D586BDCE.pf	File_Closed / File_Deleted	Normal	Archive…
2022-11-18 08:27:21	SAFEDIN.EXE-EBC27446.pf	₩Windows₩prefetch₩SAFEDIN.EXE-EBC27446.pf	File_Closed / File_Deleted	Normal	Archive…
2022-11-18 08:27:21	SCHTASKS.EXE-DC1676CD.pf	₩Windows₩prefetch₩SCHTASKS.EXE-DC1676CD.pf	File_Closed / File_Deleted	Normal	Archive…
2022-11-18 08:27:21	NGENTASK.EXE-0E6CEC17.pf	₩Windows₩prefetch₩NGENTASK.EXE-0E6CEC17.pf	File_Closed / File_Deleted	Normal	Archive…
2022-11-18 08:27:21	RUNTIMEBROKER.EXE-2B2BA…	₩Windows₩prefetch₩RUNTIMEBROKER.EXE-2B2BAB0E.pf	File_Closed / File_Deleted	Normal	Archive…
2022-11-18 08:27:21	CKSETUP64.EXE-7C5EA70E.pf	₩Windows₩prefetch₩CKSETUP64.EXE-7C5EA70E.pf	File_Closed / File_Deleted	Normal	Archive…
2022-11-18 08:27:21	CKSETUP32.EXE-255BDE4D.pf	₩Windows₩prefetch₩CKSETUP32.EXE-255BDE4D.pf	File_Closed / File_Deleted	Normal	Archive…
2022-11-18 08:27:21	SVCHOST.EXE-47D06EA1.pf	₩Windows₩prefetch₩SVCHOST.EXE-47D06EA1.pf	File_Closed / File_Deleted	Normal	Archive…
2022-11-18 08:27:21	CKAGENT.EXE-7813C036.pf	₩Windows₩prefetch₩CKAGENT.EXE-7813C036.pf	File_Closed / File_Deleted	Normal	Archive…
2022-11-18 08:27:21	V3RESTORE.EXE-F30F4B02.pf	₩Windows₩prefetch₩V3RESTORE.EXE-F30F4B02.pf	File_Closed / File_Deleted	Normal	Archive…
2022-11-18 08:27:21	SVCHOST.EXE-67EC2DA7.pf	₩Windows₩prefetch₩SVCHOST.EXE-67EC2DA7.pf	File_Closed / File_Deleted	Normal	Archive…

Figure. Log showing the collective deletion of prefetch files

3) Trail Obfuscation

Trail obfuscation refers to the task of confusing the forensic process to hide malicious behavior. Modification/Deletion of logs, spoofing, inserting incorrect information, and backbone hopping can be considered examples of ways to interfere with analysis or confuse analysts.

Timestamp Changes

During the artifact wiping process, the Lazarus group would delete almost all the files and logs they used; however, there is a single malware strain that they would leave behind in the system, the backdoor malware. Backdoors characteristically must persist for long periods of time on the target system without being detected, so the Lazarus group modifies the malware creation timestamp information to hide the backdoor.

It appears that the biggest reason they are altering the time information is to evade timeline analysis. Timeline analysis refers to the analyzing technique that track the files that were created/modified/deleted/accessed around the time of an incident. When the timestamp information is altered, logs involving the malware are omitted from the analysis process, confusing the analysis direction, or leading to incorrect conclusions.

The timestamp of the malware that was found in a system was found to perfectly match the timestamp of some other file on the same system.
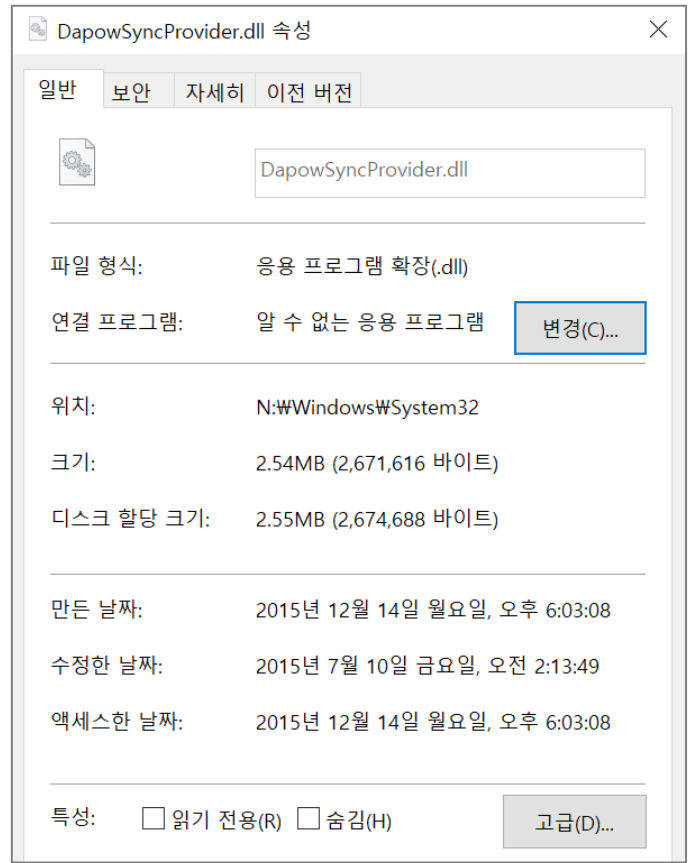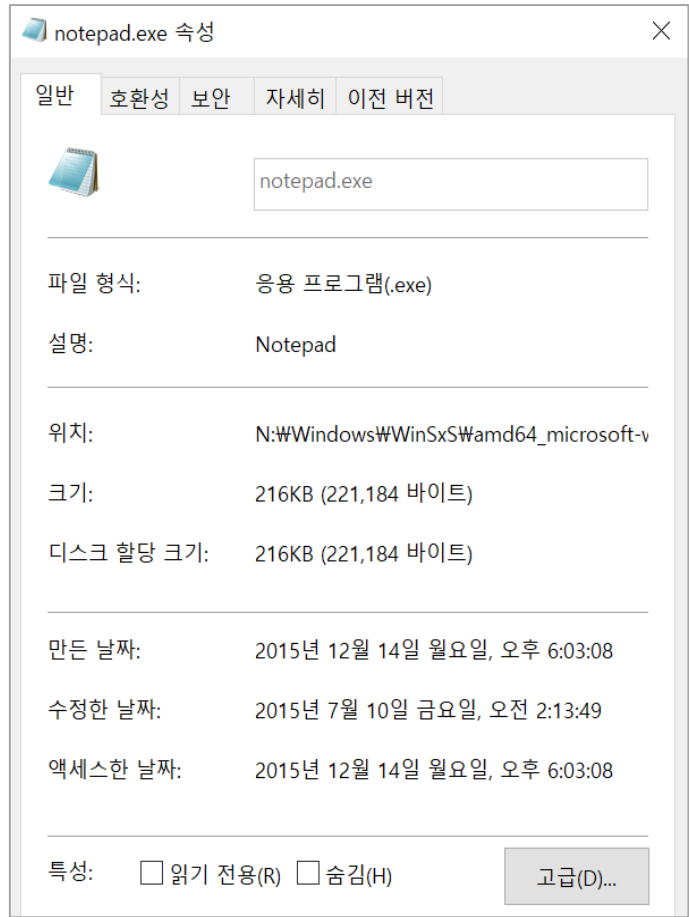
Figure. Timestamp comparison of a default system file (notepad.exe) and malware
(DapowSyncProvider.dll)

The $STANDARD_INFORMATION property and the $FILE_NAME property respectively have 4 timestamps in the Windows file system (NTFS): the file creation, modification, access, and entry modification timestamps. The timestamps displayed on the Windows file properties tab is the data from $STANDARD_INFORMATION.

- $STANDARD_INFORMATION: property that exists by default in all files that contains the basic information of files such as their timestamps, characteristics, owner ID, and security ID.
- $FILE_NAME: property that exists by default in all files that contains the filename and various other additional data of files as its purpose is to save the name of files.

$MFT was extracted and the timestamps were compared for a detailed timestamp analysis. As a result, the team discovered that the timestamp in the $STANDARD_INFORMATION property of a default system file (notepad.exe) and the malware (DapowSyncProvider.dll) matched perfectly.

FileName	$STANDARD_INFORMATION			$FILE_NAME		
	Creation	Modification	Access	Creation	Modification	Access
notepad.exe	15/12/14 09:03:08.63	15/07/09 17:13:49.37	15/12/14 09:03:08.63	15/12/14 09:03:08.63	15/07/09 17:13:49.37	15/12/14 09:03:08.63
DapowSync Provider.dll	15/12/14 09:03:08.63	15/07/09 17:13:49.37	15/12/14 09:03:08.63	22/11/09 13:58:54.40	22/11/09 13:58:54.40	22/11/09 13:58:54.40

Table. Timestamp comparison between malware and a default system file

The Lazarus group changed the malware's timestamp so that it matched and appeared like a default system file in order to evade timeline analysis.

The timestamp modification details of malware found in systems that have recently been infiltrated by the Lazarus group are as follows.

AhnLab

Systemfile	A사 PC01	B사 PC01	B사 PC02	B사 SERVER	C사 PC01	C사 PC02	D사 PC01	D사 PC02
변경 없음	Nwsapagents.dll Nwsapagentd.dat Nwsapagentc.dat			Nlas.dll imaadp64.acm				
파일 명과 유사한 시스템 파일		configmanager.tlb C_77706e.NLS wpnsvc.dll						
cmd.exe			configmanager.tlb C_68656c.NLS		Keys.dat			
notepad.exe			helpsvcs.dll		Settings.vwx		srmxlib.dll	dapowsyncprovider.dll
system.ini					legacyusermanager.dll	wptsextensions.dll Keys.dat Settings.vwx		
ntdll.dll							winsuspend.efi	winsuspend.efi
nslookup							srms-apr-w.dat	corpomofo.uce

범례

Loader
Encrypted PE
Encrypted Config

Figure. Modification of malware timestamps

With the organized information above, the characteristics of the Lazarus group's malware timestamp modification method can be summarized in the following ways.

- Not all malware have their timestamps modified.
- The timestamps are not set to arbitrary values, but rather copied over from default system files.
- Considering that there are systems with modified and unmodified timestamps within the same incident, it can be assumed that timestamp modification is optional.
- It appears that the copy target is selectable as the same malware would have the timestamps of different system files.

The team has confirmed that the timestamp modification technique done by the Lazarus group is also being used by other APT groups to hide their malware.

APT Group	Description
APT28	APT28 has performed timestomping on victim files.
APT29	APT29 modified timestamps of backdoors to match legitimate Windows files.
APT32	APT32 has used scheduled task raw XML with a backdated timestamp of June 2, 2016. The group has also set the creation time of the files dropped by the second stage of the exploit to match the creation time of kernel32.dll. Additionally,

APT Group	Description
	APT32 has used a random value to modify the timestamp of the file storing the clientID.
Chimera	Chimera has used a Windows version of the Linux touch command to modify the date and timestamp on DLLs.
Kimsuky	Kimsuky has manipulated timestamps for creation or compilation dates to defeat anti-forensics.
Lazarus	APT38 has modified data timestamps to mimic files that are in the same folder on a compromised host.Several Lazarus Group malware families use timestomping, including modifying the last write timestamp of a specified Registry key to a random date, as well as copying the timestamp for legitimate .exe files (such as calc.exe or mspaint.exe) to its dropped files.
Rocke	Rocke has changed the timestamp of certain files.
TEMP.Veles	TEMP.Veles used timestomping to modify the $STANDARD_INFORMATION attribute on tools

Table. Groups using the timestamp modification technique (MITRE ATT&CK)

AhnLab

Conclusion

During the Lazarus group's attack process, they would either encrypt their malware or disguise them with system file names to evade detection by security products. They also modified the timestamps of files to hinder analysis. Moreover, they displayed their meticulousness by overwriting their data before deleting their execution traces to obstruct data recovery.

While analyzing the anti-forensic techniques used by the Lazarus group, it was revealed that various other APT groups have also been using the same techniques to erase their attack traces.

When investigating and analyzing incidents, users must consider the possibility of the threat actor using anti-forensic techniques. Continuous research on tracking methods is required to ensure that malware can be traced even when anti-forensic techniques are applied.

[File Detection]

- Trojan/Win.LazarShell (2021.11.30)
- Trojan/BIN.Encoded (2021.12.15)
- Trojan/BIN.Encoded (2021.12.15)
- Trojan/Win.LazarLoader (2022.09.06)
- Data/BIN.EncPe (2022.09.06)
- Data/BIN.Encoded (2022.10.04)
- Backdoor/Win.Lazardoor (2022.09.06)
- Data/BIN.EncPe (2022.09.06)
- Data/BIN.Encoded (2022.10.04)
- Trojan/Win.LazarLoader (2022.09.06)
- Data/BIN.EncodedPE (2022.09.06)
- Trojan/Win.Lazardoor (2022.12.09)
- Data/BIN.Lazarus (2022.12.09)
- Trojan/Win.Lazardoor (2022.12.09)
- Data/BIN.Lazarus (2022.12.09)
- Data/BIN.Lazarus (2022.12.10)
- Trojan/Win.Lazardoor (2023.01.11)
- Data/BIN.EncodedPE (2023.01.12)

AhnLab

- Data/BIN.Encoded (2023.01.12)
- Trojan/Win.Lazardoor (2023.01.11)
- Data/BIN.EncodedPE (2023.01.12)
- Data/BIN.Encoded (2023.01.11)

[File MD5]

- B3E03A41CED8C8BAA56B8B78F1D55C22
- 1E7D604FADD7D481DFADB66B9313865D
- 7870DECBC7578DA1656D1D1FF992313C
- B457E8E9D92A1B31A4E2197037711783
- 1F1A3FE0A31BD0B17BC63967DE0CCC29
- C16A6178A4910C6F3263A01929F306B9
- 202A7EEC39951E1C0B1C9D0A2E24A4C4
- 1F1A3FE0A31BD0B17BC63967DE0CCC29
- 8543667917A318001D0E331AEAE3FB9B
- CA9B6B3BCE52D7F14BABDBA82345F5B1
- 97BC894205D696023395CBD844FA4E37
- C7256A0FBAB0F437C3AD4334AA5CDE06
- FC8B6C05963FD5285BCE6ED51862F125
- 27DB56964E7583E19643BF5C98FFFD52
- 61B3C9878B84706DB5F871B4808E739A
- 6EA4E4AB925A09E4C7A1E80BAE5B9584
- BD47942E9B6AD87EB5525040DB620756
- 67D306C163B38A06E98DA5711E14C5A7
- C09B062841E2C4D46C2E5270182D4272
- 747177AAD5AEF020B82C6AEABE5B174F
- E73EAB80B75887D4E8DD6DF33718E3A5
- BA741FA4C7B4BB97165644C799E29C99
- 064D696A93A3790BD3A1B8B76BAAEEF3

More security, More freedom

AhnLab, Inc.

220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, Korea

Tel : +82 31 722 8000 | Fax : +82 31 722 8901

https://www.ahnlab.com

https://asec.ahnlab.com/en

About ASEC

AhnLab Security Emergency Response Center (ASEC), through our team of highly skilled cyber threat analysts and incident responders, delivers timely and accurate threat intelligence and state-of-the-art response on a global scale. ASEC provides the most contextual and relevant threat intelligence backed by our groundbreaking research on malware, vulnerabilities, and threat actors to help the global community stay ahead of evolving cyber-attacks.

About AhnLab

AhnLab is a leading cybersecurity company with a reliable reputation for delivering advanced cyber threat intelligence and threat detection and response (TDR) capabilities with cutting-edge technology. We offer a cybersecurity platform comprised of purpose-built products securing endpoint, network, and cloud, which ensures extended threat visibility, actionable insight, and optimal response. Our best-in-class researchers and development professionals are always fully committed to bringing our security offerings to the next level and future-proofing our customers' business innovation against cyber risks.

AhnLab