Why Remediation Alone Is Not Enough When Infected by Malware - ASEC

By ATCP

Published: 2022-05-20 · Archived: 2026-04-05 16:49:09 UTC

In January 2022, a prominent Korean company in the manufacturing industry had many of its internal systems infected by the Darkside ransomware.

As the ransomware was found to be distributed using the AD group policy, AhnLab attempted to conduct a DC server forensic analysis. However, as the virtual environment operating system of the DC server operating in the virtual environment was damaged, the server could not be secured. Among the systems that were restored by the previous backup after the infection, the two WebLogic servers were found to be infected by WebShell during a similar period. AhnLab conducted the forensic analysis on the servers to check if WebShell was responsible for the Darkside infection.

The analysis result of WAS1 and WAS2 servers restored with previous snapshots showed that WebShell and Darkside were not related. However, there were Miner infections starting from April 2019, and there was a history of various malware infections and breach traces until February 2022 (the time of the analysis).

The company that uses the AhnLab product was aware of the infections, yet it seems the company did not identify how the infection happened in the first place. Apparently, the only action they took was remediating the system,

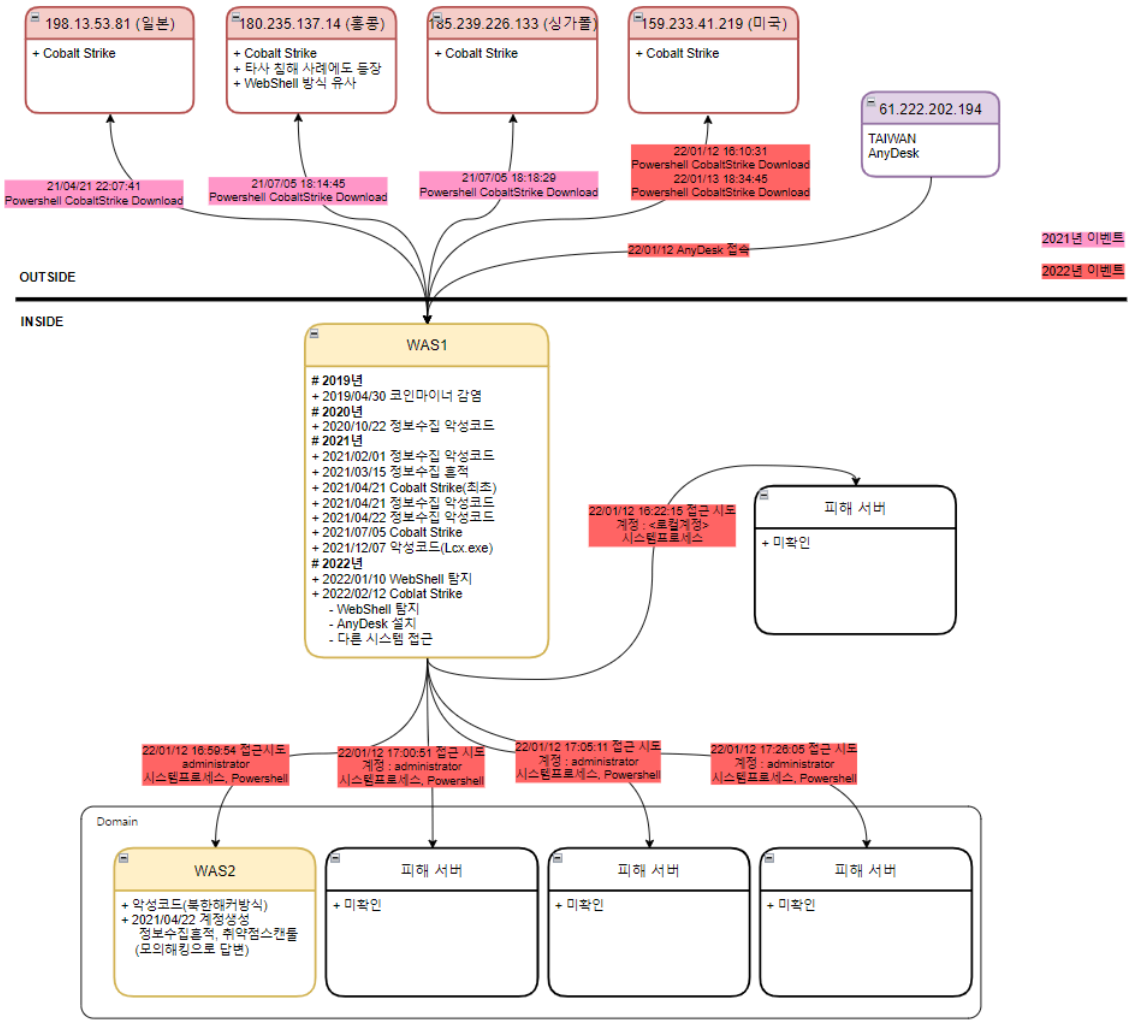
without identifying how the infection started.

While the malware infecting the system may not inflict serious damage, leaked control and information of the internal systems may be traded between attackers and utilized in attacks that may cause serious issues in the future. As such, when the malware is detected, simply remedying the system and deleting the malware is not enough. To prevent further breaches and attacks of similar types, a detailed analysis of the infected system to identify the cause of the malware infections and breaches is needed, as well as resolving the identified issues.

Breach Details

The traces of the breach discovered on the targeted company's WAS1 and WAS2 servers are as follows:

WAS1 was infected with CoinMiner in 2019. It was later infected with various malware types such as Cobalt Strike, WebShell, and info-leaking malware. It appears that the breach had been progressing for the recent 2-3 years by the various attackers. WAS2 had a malware strain likely created by a North Korean hacker, meaning it was probably being targeted by an APT attack. There were also various breach traces discovered on April 22, 2021, but the targeted company stated that it received a penetration testing service on that day.



Initial Approach

WAS1 was infected with CoinMiner on April 30, 2019. The malware was downloaded from 146.196.83.217. According to the Tencent Security blog, the IP address is related to a miner named RunMiner. It was found to be distributed by using the WebLog Deserialization vulnerability CVE-2017-10271.

The initial breach trace of WAS2 happened on April 29, 2020. There was a trace of the attacker attempting to infiltrate WebShell. The WebLogic version of WAS1 and WAS2 was 12.1.3, which is a version existing in the CVE-2017-10271 vulnerability mentioned above. It is likely that the initial breach happened due to the WebLogic vulnerability of the two servers.

Obtaining Account

On October 22, 2020, a hacking tool included with the dictionary attack feature and lsass.dmp file (a dump file for the lsass.exe process) were found as a compressed file (1.rar) in the shared folder of the WAS1 system. It seems the attacker stole the password by the dictionary attack method and process dump for lsass.exe.

Through the lsass.dmp file secured by the attacker, one can obtain various information such as drmftp, plain password of the Administrator account, and NTLM hash as shown below.

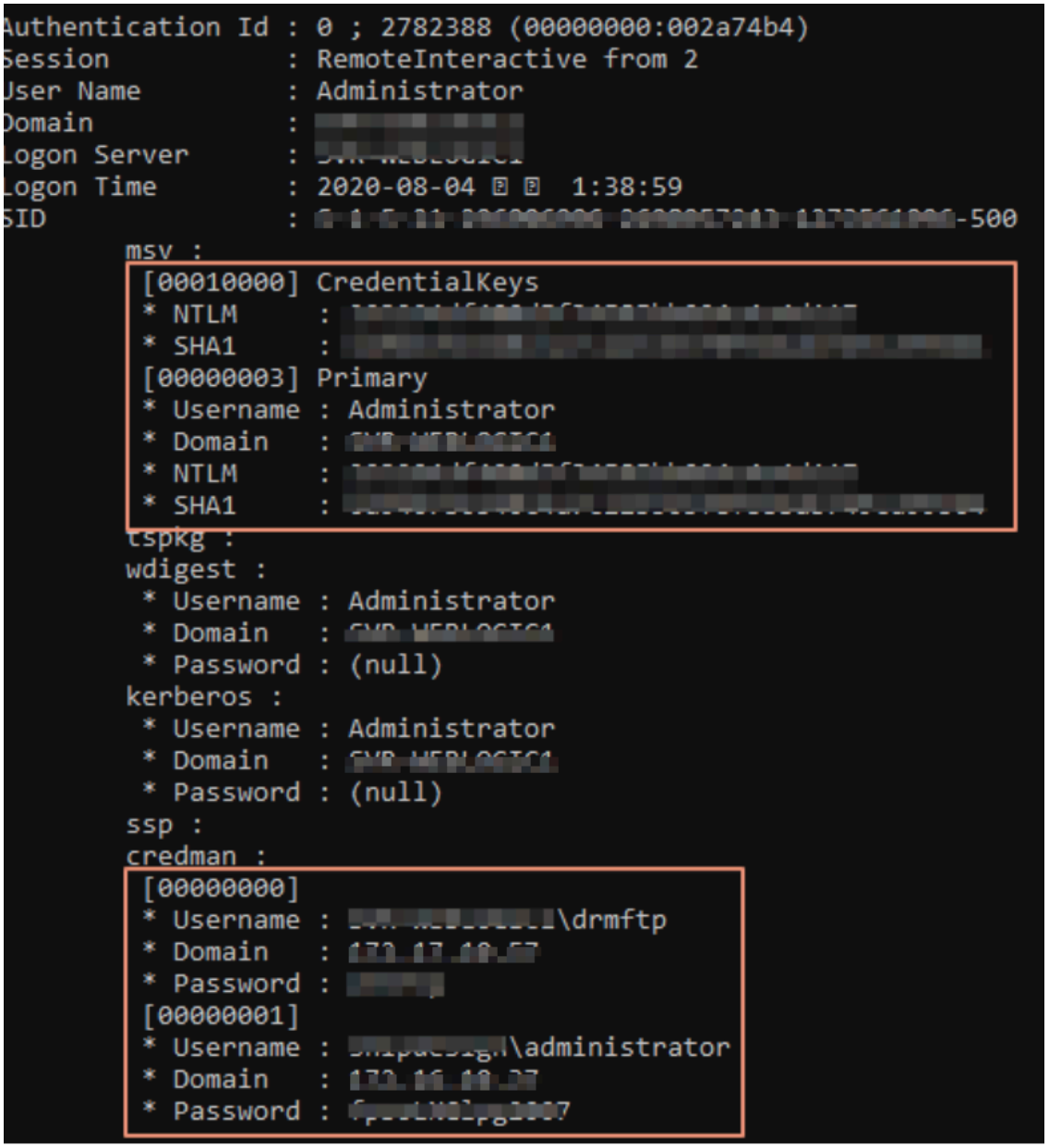


Figure 2. Account information (ID, plain password, and NTLM Hash) extracted from Isass.dmp stolen by the attacker

The targeted company's administrator account was in a vulnerable state:

- The password for the Administrator account did not change once since it was created.
- The account used a password that could be easily guessed.
- As the Administrator account's password for both WAS1 and WAS2 was the same, it is likely that most of the other servers used the same password for their administrator accounts.

Reverse RDP Access

After obtaining the account with the administrator privilege, the attacker sometimes had direct control of the system within the organization by accessing it with the Reverse RDP method using Lcx.exe.

Lcx.exe is an open-source tunneling tool that can be used to connect the external attacker with the internal system. The RDP communication process of Lcx.exe is as follows:

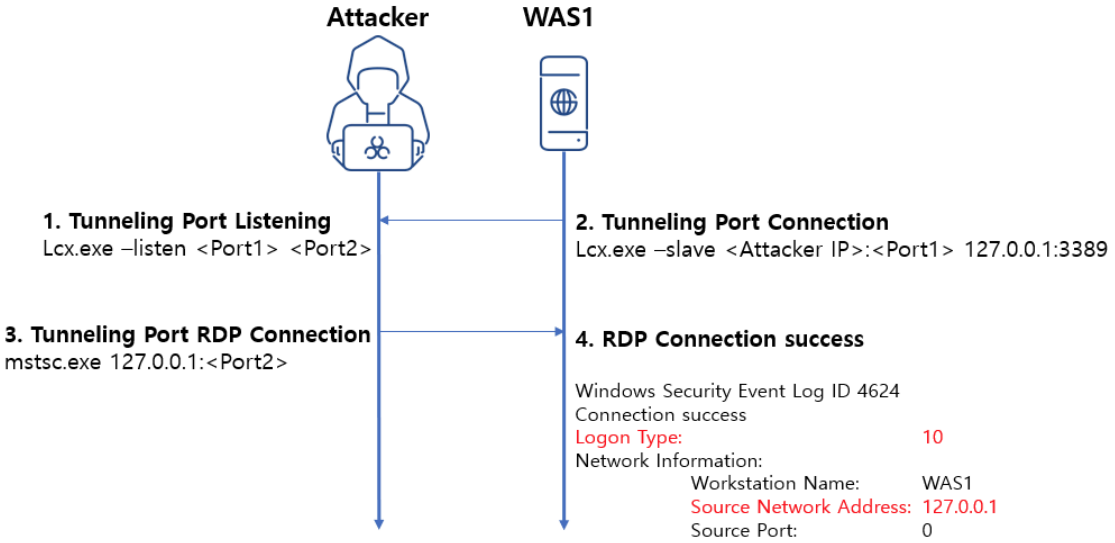


Figure 3. RDP communication process using Lcx.exe

The history of Lcx.exe being created and executed in WAS1 was confirmed, as well as the access IP of 127.0.0.1 recorded in the event log (Event ID: 4624). The accounts used for verifying tunneling were local Administrator and test, both of them being administrator accounts. The test account was created right before the event, most likely done by the attacker. Unfortunately, AhnLab could not check the IP that the external attacker used for remote access.

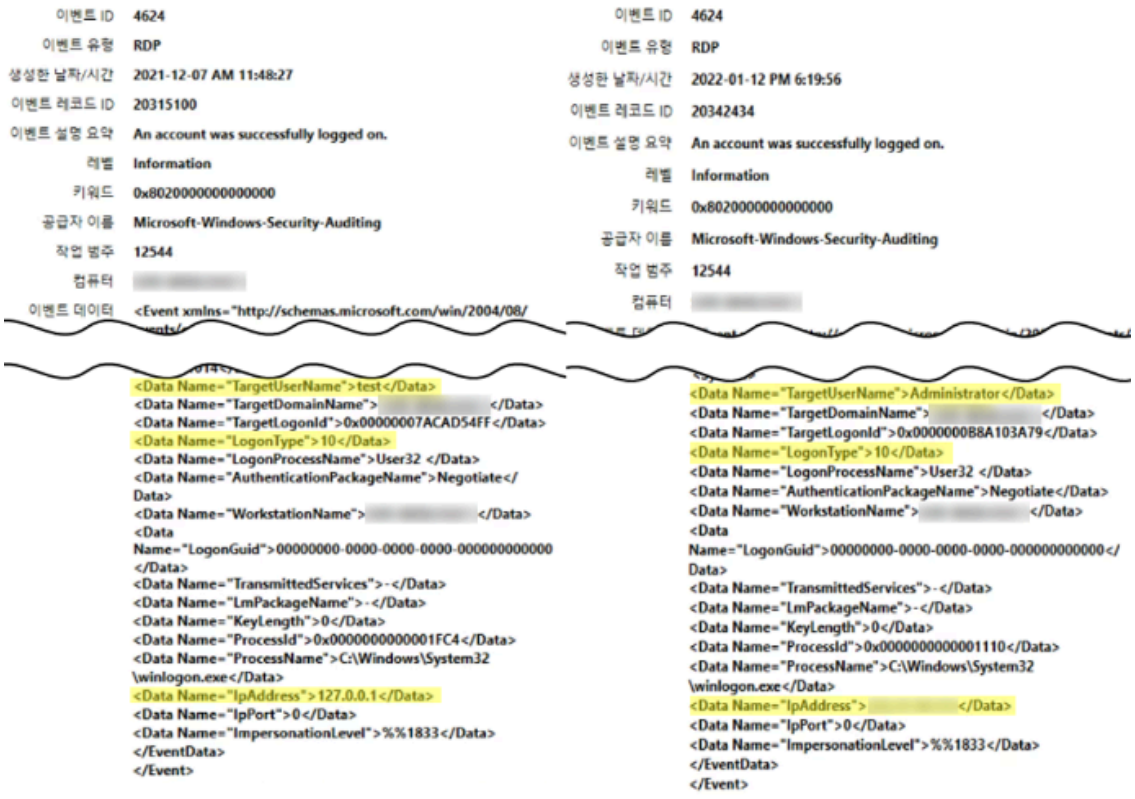


Figure 4. Tunneling RDP access event log – Event ID: 4624

Tools Used for Attack

The infected system had a scanning tool, proxy and port forwarding tool, WebShell, backdoor malware, etc.

The attacker used various tools for different purposes: collecting information for infiltration, port forwarding for establishing an external connection, installing backdoor for persistence, etc. The tools discovered in the system are shown below.

분류	파일명	주요 기능
Scanning	systems.exe	• 취약점 스캐닝, 내부 네트워크 포트 스캐닝 및 서비스 취약점 확인 • 패스워드 Dictionary Attack 기능 존재 • 취약점 공격 성공 시 시스템 명령어 실행
	chrome.exe	• 인자로 입력 받은 IP 네트워크 스캔 도구 • 대상 시스템의 NetBIOS 이름, IP 주소, 컴퓨터 이름, 사용자 이름, MAC 주소 수집
	AliveScan.exe	• 네트워크 대역 내 존재하는 시스템 IP 주소 수집
	Ladon64.exe	• SMB를 포함한 다수 취약점 확인 • 패스워드 Dictionary Attack 기능 존재
Proxy	Lcx.exe	• 포트 포워딩 툴 • 공격자는 내부망 시스템에 RDP 기능을 수행할 수 있음
	frpc.exe	• 역방향 프록시 툴 • 공격자는 내부망 시스템에 원격 접속 기능을 수행할 수 있음
Backdoor	agent.exe	• 침투 테스트 툴로 네트워크 프록시 기능, 파일 업로드 및 다운로드, 리모트 쉘기능 존재
	npc.exe	• 웹을 통해 관리되는 인트라넷 침투 테스트 프록시 툴 • 클라이언트/서버 제어 및 정보 확인 기능
Remote Desktop	anydesk.exe	• GmbH사의 원격 데스크톱 애플리케이션으로 원격 제어, 파일 전송, VPN 기능을 제공. • 공격에 사용됐을 것으로 추정되나, 고객사 내부에서 관리용으로 사용하는 도구라고 답변

Table 1. Tools Used for Attack

To bypass anti-malware products, the attacker used open-source programs that are relatively difficult to detect as attack tools. AhnLab detects and blocks malware and attack tools discovered in the infected system using the aliases below.

[File Detection]

- Unwanted/Win32.NSSM
- Unwanted/Win32.BitCoinMiner
- Unwanted/Win32.BitCoinMiner
- Dropper/Win.Agent
- Dropper/Win32.Agent
- Dropper/Win.Agent
- HackTool/Win.Fscan
- HackTool/Win.Fscan
- HackTool/Win.Fscan
- HackTool/Win.NbtScan
- Malware/Gen.Reputation
- HackTool/Win.AliveScan
- Exploit/Win.Scanner
- HackTool/Win.LCX
- HackTool/Win.Stowaway
- HackTool/Win.NPS
- HackTool/Win.Frp
- HackTool/Win.Frp
- Malware/Win64.Generic
- Patched/Win.Loader
- HackTool/Win.ExploitScanner

[File MD5]

- 1136efb1a46d1f2d508162387f30dc4d
- ae00198dfa0ef3a7e5fea8dd06a8d8b8
- f2f94708cef791d9664d2e4fa20ff520
- 0dabd600cea6dcf3c049a667b67b4482
- 99b0638f134a0d607edb8dbab01d3f95
- 763f2cae2072647d61d11047c8aaaf09
- e636a07bb8d8fbfb1cab5557fdc217aa
- 0f7baf15408a49895439aa273ee7f867
- 7650484a85247bc922de760a6a335a76
- 62eada472d6d2d7606ba322c8b7f9153
- f01a9a2d1e31332ed36c1a4d2839f412
- f4a992b87d70c622eef107a09d712e9e
- d221d51f4599ae051709b5cf5c45af10
- fb6bf74c6c1f2482e914816d6e97ce09
- 4b8fbfc68b9969549f050c0e8366a10d
- 716979a28125fa65903e77dc5b399383
- 88a5ebccf60464764d0fe015d71bf330
- d862186f24e644b02aa97d98695c73d8
- 114f26e7b46d0f4c4a202353c41ce366

- 0b877ea03db28b275dd535f16dd78239
- fe12b5008334ad718008307e1a0750f7

[IP/URL]

- 198.13.53.81
- 180.235.137.14
- 185.239.226.133
- 159.233.41.219

Subscribe to AhnLab's next-generation threat intelligence platform 'AhnLab TIP' to check related IOC and detailed analysis information.
