블랙캣 랜섬웨어 침해사고 기술보고서

등록일	@June 19, 2023 2:37 PM
최종수정일	@June 22, 2023 10:23 AM
저자&감수	중소기업침해사고피해지원서비스(KISA & 플레인비트)

1. Introduction

랜섬웨어(Ransomware)란 몸값을 뜻하는 랜섬(ransom)과 악성코드(malware)의 합성어로 사용자의 컴퓨터가 랜섬웨어에 감염될 경우 중요 데이터가 암호화되며, 암호화된 데이터를 복구하기 위한 대가로 금전을 요구하는 악성코드를 말한다.

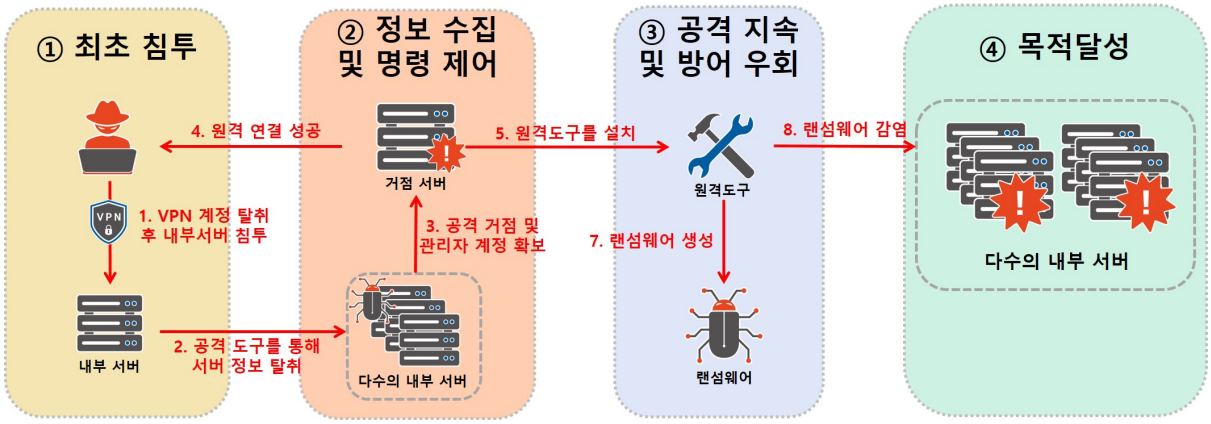
이번 기술 보고서의 주제인 블랙캣(BlackCat 또는 ALPHV) 랜섬웨어는 `21년 11월 전세계 처음으로 발견되었으며, RUST 프로그래밍 언어를 기반으로 한 최초의 랜섬웨어로 백신 탐지 확률이 낮으며 빠르게 암호화가 가능하고 다양한 운영체제 플랫폼에서 사용할 수 있는 특징이 있다.

특히 '22년 4월 美 FBI는 해당 랜섬웨어에 의한 피해 확산을 예방하기 위해 공격 IoC(Indicators of Compromise) 공개했으며, 국내에서도 `22년 7월 이후 현재까지 제조업체를 대상으로 총 5건의 피해가 확인되었다. 이에 한국인터넷진흥원과 플레인비트는 신고된 피해 기업의 분석을 통해 발견된 공격자들의 공격 방법과 전략에 따른 대응방안(ATT&CK 프레임워크)을 소개하여 유사 사고사례를 예방하고자 한다.

2. Summary

블랙캣 랜섬웨어 해킹그룹의 기업 침투단계는 아래와 같다.

- **(최초침투)** VPN 계정 탈취 후 내부 침투
- **(정보수집)** 공격도구를 통해 계정 및 서버 정보 수집
- **(내부이동)** 수집된 계정정보 및 서버정보를 통해 내부이동
- **(거점확보)** AD 관리자 계정을 탈취해 공격 거점 확보 및 원격 접근 프로그램 설치
- **(내부전파)** 공유 폴더 및 SMB를 통해 악성코드 설치 및 스크립트 실행
- **(목적달성)** 거점서버를 통해 다른 서버에 랜섬웨어 실행



3. ATT&CK Matrix

3.1 Initial Access: 최초 침투 - (개요도 ①)

가. External Remote Services

공격자는 다크웹* 및 무작위 대입 공격을 통해 기업의 VPN 계정을 탈취하여 내부 시스템에 접근한다. 아래 내용는 무작위 대입 공격을 통한 VPN 계정 탈취 로그이다.

`* 다크웹에 공개되어 있거나 판매되고 있는 VPN계정 구매`

📎 **무작위 대입 공격을 통한 VPN 계정 탈취 로그(VPN로그)**

date=2023-03-13 time=15:52:26 logid="0101039949" type="event" subtype="vpn" level="information" vd="root" eventtime=1678690346495768584 tz="+0900" logdesc="SSL VPN statistics" action="tunnel-stats" tunneltype="ssl-tunnel" tunnelid=860146678 remip=42.116.XX.XX tunnelip=20.20.20.3 user="son" group="SSLVPN" dst_host="N/A" nextstat=600 duration=17443 sentbyte=180445045 rcvdbyte=22665554 msg="SSL tunnel statistics"

(중간생략)

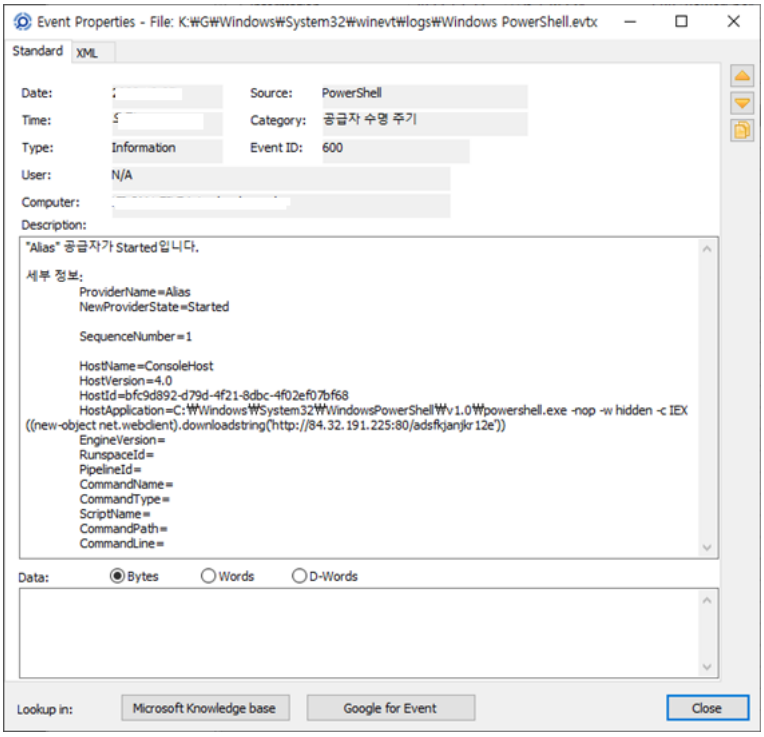
date=2023-03-13 time=15:44:30 logid="0101039949" type="event" subtype="vpn" level="information" vd="root" eventtime=1678689871043048253 tz="+0900" logdesc="SSL VPN statistics" action="tunnel-stats" tunneltype="ssl-tunnel" tunnelid=860146687 remip=42.116.XX.XX tunnelip=20.20.20.1 user="long" group="SSLVPN" dst_host="N/A" nextstat=600 duration=1203 sentbyte=16083894 rcvdbyte=2583989 msg="SSL tunnel statistics"

3.2 Execution: 실행 - (개요도 ② ③)

가. Command and Scripting Interpreter: PowerShell

파워셸을 이용하여 Coblat Strike 스크립트 다운로드 및 실행

📌 **파워셸을 통해 Cobalt Strike 실행 이력(이벤트로그)**



📌 **파워셸을 통해 추가 파일 다운로드(이벤트로그)**

```
Type :    Information
Date :
Time :
Event :   600
Source :    PowerShell
Category :  공급자 수명 주기
User :    N/A
Computer :  []
Description:
"Alias" 공급자가 Started입니다.

세부 정보:
ProviderName=Alias
NewProviderState=Started

SequenceNumber=1

HostName=ConsoleHost
HostVersion=4.0
HostId=f97081ad-4cf3-4a8d-82c9-f2154a9975e1
HostApplication=powershell.exe -executionpolicy remotesigned -File .\\Get-DataInfo.ps1 method
EngineVersion=
RunspaceId=
PipelineId=
CommandName=
CommandType=
ScriptName=
CommandPath=
CommandLine=
```

3.3 Persistence: 지속 - (개요도 ② ③)

가. External Remote Services

원격 접근 프로그램을 설치하여 VPN 통한 접근 외 외부에서 접근할 수 있는 추가적인 방법을 구성한다.

🚧 **공격자가 사용하는 원격 액세스 공격 도구**

도구명	도구 설명
ScreenConnect.exe	원격 접근 프로그램
Socks.exe / Socks2.exe	원격 접속 악성코드
winscp.exe	원격 접근 프로그램

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

공격자는 세션 정보 및 SSH HOST KEY 등 접속과 관련된 레지스트리를 변경하는 파일을 생성한다.

🚧 **공격자가 사용하는 세션 정보 도구**

도구명	도구 설명
putty.reg	접속 관련 registry 변경 파일
WinSCP.ini	ssh host key 및 세션 정보 존재

다. Scheduled Task/Job:Scheduled Task

공격자는 원격에서 접근하기 위해 악성 프로그램(원격제어 악성코드 등) 작업스케줄러에 등록한다.

📌 **작업스케줄러에 악성코드 등록(이벤트로그)**

```
Type :    Information
Date :
Time :
Event :   106
Source :    Microsoft-Windows-TaskScheduler
Category :  등록된 작업
User :    \SYSTEM
Computer :
Description:
"NT AUTHORITY\System" 사용자가 작업 스케줄러 작업 "\wow64"을(를) 등록했습니다.
```

```
작업 스케줄러 설정파일(wow64)

<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.1" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo>
    <Author>GOOD\administrator</Author>
  </RegistrationInfo>
  <Triggers>
    <TimeTrigger>
      <Enabled>true</Enabled>
      <Repetition>
        <Interval>PT2M</Interval>
        <Duration>P365D</Duration>
        <StopAtDurationEnd>false</StopAtDurationEnd>
      </Repetition>
      <StartBoundary>                </StartBoundary>
    </TimeTrigger>
  </Triggers>
                          (중간 생략)
<Actions Context="Author">
    <Exec>
      <Command>C:\Program Files\socks.exe</Command>
      <Arguments>start</Arguments>
    </Exec>
  </Actions>
</Task>
```

3.4 Privilege Escalation: 권한 상승 - (개요도 ②)

가. Valid Accounts: Domain Accounts

공격자는 지속성, 권한 상승, 방어 회피를 얻기 위한 수단으로 도메인 계정의 자격 증명을 획득한다. 도메인 계정 자격 증명을 얻기 위해 Credential Dump를 하거나 도메인 컨트롤러를 손상시키기도 한다.

3.5 Defense Evasion: 방어 회피 - (개요도 ③)

가. Impair Defenses : Disable or Modify Tools

공격자는 랜섬웨어 등 악성코드 탐지를 막기 위해 윈도우 디펜더 등 백신을 강제 종료한다.

🚧 공격자가 사용하는 백신 제거 및 종료 도구

도구명	도구 설명
del.bat	백신 셧다운 스크립트
ProcessHacker.exe	시스템 프로세스를 관리하기 위한 유틸리티 도구
psexec64.exe	시스템 프로세스를 관리하기 위한 유틸리티 도구
file64.exe	특정 프로세스(백신 포함) 강제 종료
ComKJ.sys	특정 프로세스(백신 포함) 강제 종료
Backstab.exe	백신 강제 종료 도구

3.6 Credential Access: 자격 증명 - (개요도 ②)

가. OS Credential Dumping : Security Account Manager

공격자는 계정정보를 획득하기 위해 계정탈취 도구(mimikatz)를 사용하여 계정정보를 수집한다.

공격자가 사용하는 계정탈취 도구

도구명	도구 설명
mimikatz.exe	계정 정보 수집 도구

계정 정보 수집 도구(mimikatz.exe) 실행 이력 (UserAssist)

Program Name	Run Counter	Focus Count	Focus Time	Last Executed
Kaspersky Lab.KAV.Toasts	0	1	0d, 0h, 00m, 04s	
C:₩Users₩Administrator₩Downloads₩WPR (old)₩WPR (old)₩wpr.exe	1	3	0d, 0h, 00m, 41s	2022-06-13 12:25:40
C:₩Users₩Administrator₩Downloads₩jknvekgt.exe	3	4	0d, 0h, 03m, 01s	2022-06-13 12:34:10
C:₩Users₩Administrator₩Downloads₩x64₩mimikatz.exe	1	1	0d, 0h, 00m, 12s	2022-06-13 12:35:24
C:₩Users₩Administrator₩Downloads₩1₩net64.exe	2	32	0d, 0h, 44m, 52s	2022-06-13 12:50:07
Microsoft.Windows.RemoteDesktop	5	46	0d, 1h, 28m, 14s	2022-06-15 18:11:34

3.7 Discovery: 탐색 - (개요도 ②)

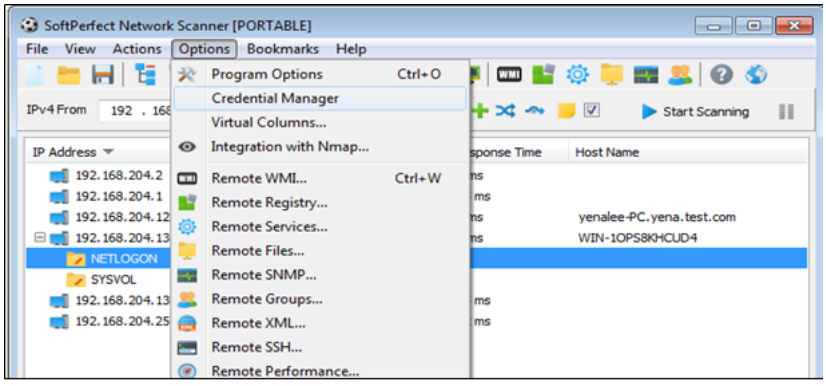
가. Network Service Discovery

공격자는 내부 이동을 위해 네트워크 스캔 도구를 사용하여 피해 시스템 네트워크 정보를 수집한다.

공격자가 사용하는 네트워크 스캔 도구

도구명	도구 설명
net64.exe	네트워크 주소, 숨겨진 공유폴더 확인, 원격 접근 기능 제공
ADfind.exe	AD 정보 수집(도메인 계정, 권한 그룹, 네트워크 구성)
netscan.exe	네트워크 스캔 도구
NetworkShare_pre2.exe	네트워크 스캔 도구

- **net64.exe**



3.8 Lateral Movement: 내부 이동 - (개요도 ②)

가. Remote Services Remote Desktop Protocol

공격자는 수집한 정보를 이용하여 Active Directory 내의 다른 서버로 원격 접속하여 내부이동한다. 내부이동 시 위에서 사용한 RDP 정보 수집 도구 및 네트워크 스캔 도구를 통해 추가 서버를 찾으며, 가장 많은 정보를 가지고 있는 서버를 거점으로 삼아 랜섬웨어 공격 준비를 한다.

나. Remote Services VNC

공격자는 원격 접근 프로그램(ScreenConnect.exe)을 설치하여 VPN을 통한 접근 외 외부에서 접근할 수 있는 방법을 추가한다.

📌 원격 접근 프로그램(ScreenConnect.exe) 설치 이벤트로그 (System.evtx)

시스템에 서비스가 설치되었습니다.

서비스 이름: **ScreenConnect Client (64b809f03e7ee623)**
서비스 파일 이름: "C:\Program Files (x86)\ScreenConnect Client (64b809f03e7ee623)\ScreenConnect.ClientService.exe"?e=Access&y=Guest&h=instance-cirigy-relay.screenconnect.com&p=443&s=520d306d-0107-4f9c-ade2-ebd80d745274&k=BgIAAACkAABSU0ExAAgAAAEAAQCpUxcBgpXCfG142Ltj1%2fyzENtvFB2woXWjZHqVXgzEqk7K6

서비스 유형: user mode service
서비스 시작 유형: auto start
서비스 계정: LocalSystem

📌 원격 접근 프로그램(ScreenConnect.exe) 실행 이벤트로그 (System.evtx)

ScreenConnect Client (3eaca1af958d8405) 서비스가 running 상태로 들어갔습니다.

📌 네트워크 스캔 도구(AdFind.exe) 사용하여 원격 접근 시도 이벤트로그 (Security.evtx)

명시적 자격 증명을 사용하여 로그온을 시도했습니다.
주체:
- 보안 ID: S-1-5-21-2805692261-3615434627-2978759279-500
- 계정 이름: Administrator
- 계정 도메인: [계정 도메인]
- 로그온 ID: 0x9EF76EAD9
- 로그온 GUID: {00000000-0000-0000-0000-000000000000}

자격 증명이 사용된 계정:
- 계정 이름: administrator
- 계정 도메인: [계정 도메인]
- 로그온 GUID: {76b3720e-8929-970e-a97f-8b308a137cba}

대상 서버:
- 대상 서버 이름: [대상 서버 이름]
- 추가 정보: ldap/[sever name]/[domain]

프로세스 정보:
- 프로세스 ID: 0x103c
- **프로세스 이름: C:\Users\Administrator\Downloads\1\AdFind.exe**

네트워크 정보:
- 네트워크 주소: -
- 포트: -

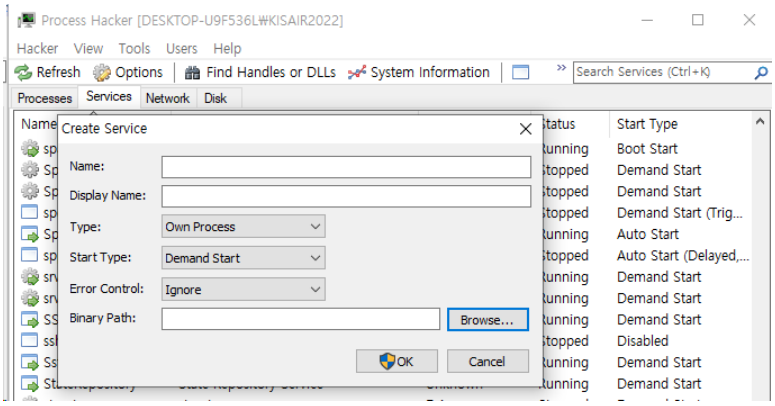
다. Lateral Tool Transfer

악성 파일을 사용하여 공유 폴더를 통해 다른 서버에 존재하는 파일을 실행한다.

🚧 공격자가 사용하는 악성 도구

도구명	도구 설명
ProcessHacker.exe	시스템 프로세스를 관리하기 위한 유틸리티 도구
del.bat	보안 소프트웨어를 무력화시키기 위한 배치 파일

- ProcessHacker.exe



3.9 Command and Control: 명령 및 제어 - (개요도 ② ③)

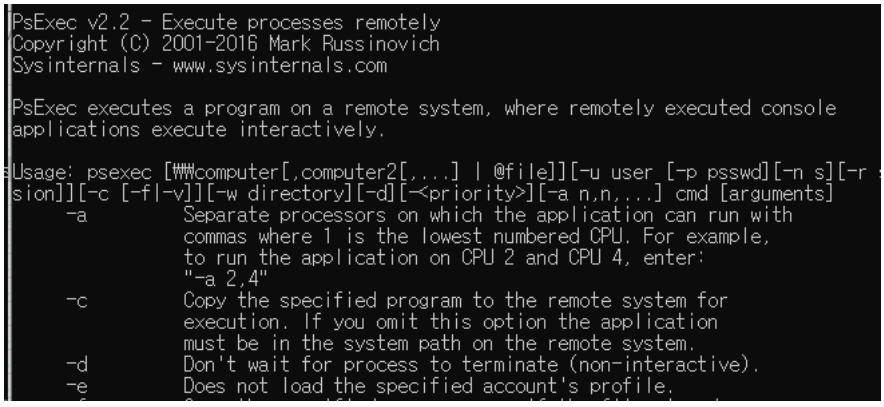
가. Remote Access Software

공격자는 다른 시스템에 대한 원격 액세스를 활용하기 위해 공격 도구를 사용한다.

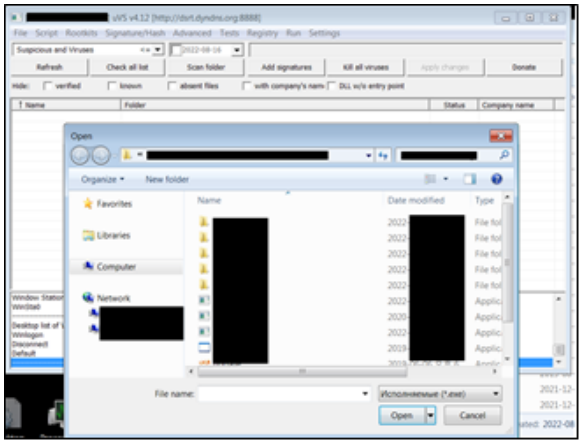
공격자가 사용하는 원격 액세스 공격 도구

도구명	도구 설명
psexec.exe	공유 폴더와 SMB를 사용하여 원격 접근, 명령어/파일 실행 등 기능 제공
PsExec64.exe	psexec.exe 64bit
zagent.exe	원격 프로세스 조작, 파일 실행 기능 제공

- **PsExec.exe**



- **zagent.exe**



3.10 Impact: 영향 - (개요도 ④)

가. Data Encrypted for Impact

공격자는 거점서버를 통해 다른 서버에 접속하여 랜섬웨어를 실행한다. 랜섬웨어명의 경우 회사명 혹은 무작위 값으로 되어 있고 해당 랜섬웨어를 실행시켜 파일을 암호화시킨다.

랜섬웨어

도구명	기타
[회사명].exe	windows 환경에서의 실행파일
[회사명].elf	linux 환경에서의 실행파일

랜섬웨어 실행 흔적 (Appcompatcache)

Cache Entry Position	Program Name	Modified Time
=	[redacted]	=
22	C:₩Users₩Administrator₩Downloads₩win₩[redacted].exe	2022-07-08 07:58:26

랜섬웨어에 감염된 후, 각 폴더에는 아래와 같은 랜섬노트(RECOVER-v*****n-FILES.txt)가 생성된다.

📎 **RansomNote**

> What happened?

Important files on your network was ENCRYPTED and now they have "v*****n" extension.
In order to recover your files you need to follow instructions below.

> Sensitive Data

Sensitive data on your network was DOWNLOADED.
If you DON'T WANT your sensitive data to be PUBLISHED you have to act quickly.
Data includes:

- Employees personal data, CVs, DL, SSN.
- Complete network map including credentials for local and remote services.
- Private financial information including: clients data, bills, budgets, annual reports, bank statements.
- Manufacturing documents including: datagrams, schemas, drawings in solidworks format
- And more...

Samples are available on your personal web page linked below.

> CAUTION

DO NOT MODIFY ENCRYPTED FILES YOURSELF.
DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.
YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.

> What should I do next?

1. Download and install Tor Browser from: https://torproject.org/
2. Navigate to: http://cfyk7s43hnxheiyyd4affb46mjcilyf5mzycjcoeotydqbgr2jcluwyd.onion/?access-key=r6R7nUjb6uCBC…(중간생략)…i6Zv%2BCzf9Zmjbf4HtDKPonZ1Q4vwR2Q%3D%3D

나. Shutdown / Reboot

랜섬웨어 감염을 위해 가상서버 일괄 종료한다. 추가적으로 랜섬웨어 감염 시키고 서버를 재부팅한다.

ATT&CK Matrix

Tatic	ID	Sub-techniques	Description
Initial Access	`T1133`	External Remote Services	외부 장비(VPN)를 통한 접근
Execution	`T1059.001`	Command and Scripting Interpreter: PowerShell	파워셸을 이용한 Cobalt Strike 스크립트 다운로드 및 실행
Persistence	`T1133`	External Remote Services	외부 장비 외 추가 접근 환경 구성
Persistence	`T1547.001`	Boot or Logon Autostart Execution : Registry Run Keys / Startup Folder	접속 관련 레지스트리 변경
Persistence	`T1053.005`	Scheduled Task/Job:Scheduled Task	작업스케줄러에 악성코드 등록
Privilege Escalation	`T1078.002`	Valid Accounts: Domain Accounts	도메인 계정 사용
Defense Evasion	`T1562.001`	Impair Defenses : Disable or Modify Tools	백신 강제 종료
Credential Access	`T1003.002`	OS Credential Dumping : Security Account Manager	계정 탈취 도구 사용
Discovery	`T1046`	Network Service Discovery	네트워크 스캔 도구 사용
Lateral Movement	`T1021.001`	Remote Services : Remote Desktop Protocol	원격 데스크톱(RDP)을 통해 원격 접속

Tatic	ID	Sub-techniques	Description
Lateral Movement	T1021.005	Remote Services : VNC	원격 접근 프로그램 사용
Lateral Movement	T1570	Lateral Tool Transfer	악성 파일 사용하여 공유 폴더통한 원격 접근
Command and Control	T1219	Remote Access Software	원격 액세스 활용하기 위한 공격 도구 사용
Impact	T1486	Data Encrypted for Impact	랜섬웨어 감염
Impact	T1529	System Shutdown / Reboot	랜섬웨어 감염 후 재부팅

4. Defense

4.1 VPN 보안강화

VPN 계정 보안

VPN 계정의 패스워드는 주기적 변경과 복잡성(영/대소문자, 숫자, 특수문자 혼합 10자리 이상 권장)을 만족하도록 정책적 설정이 필요하다. 또한 VPN 접속시, 소유(또는 생체 기반 2차 인증(문자메시지, 모바일 앱 등)을 적용하는 것을 권장한다. 추가적으로 퇴사자 및 미사용 계정은 바로 삭제하여 관리해야한다.

VPN 접근제어 강화

비허가된 외부 접근 차단을 위해 VPN 접속 허용 IP를 화이트리스트 방식으로 접근 제어 설정하고 해외 접속이 필요한 계정 외의 계정에서 VPN 사용이 불가하도록 설정하는 것을 권장한다.

4.2 랜섬웨어 대응

랜섬웨어 차단 기능 활성화

각종 백신 프로그램은 랜섬웨어 방지 기능을 제공한다. '제어된 폴더 액세스', '파일 위변조 탐지', '랜섬웨어 데이터 복구' 등 일부 유/무료 서비스들을 활성화하여 랜섬웨어로부터 보호할 수 있다.

랜섬웨어 대응 가이드 라인 확인

한국인터넷진흥원은 랜섬웨어 감염 시 이에 대응하기 위한 목적으로 랜섬웨어 대응 가이드라인을 제공하고 있다. 가이드라인에서는 랜섬웨어 예방을 위한 보안 수칙이나 랜섬웨어 대응과 관련된 요청 등의 내용이 포함되어있다.

💡 **다운로드 방법**
www.boho.or.kr → 자료실 → 가이드 및 매뉴얼
'랜섬웨어 대응 가이드', '안전한 정보시스템 백업 가이드'

💡 **랜섬웨어 대응 가이드**
https://www.boho.or.kr/kr/bbs/view.do?searchCnd=1&bbsId=B0000127&menuNo=205021&pageIndex=2&categoryCode=&nttId=27048

💡 **안전한 정보시스템 백업 가이드**
https://www.boho.or.kr/kr/bbs/view.do?searchCnd=1&bbsId=B0000127&menuNo=205021&pageIndex=1&categoryCode=&nttId=36327

중요 자료 정기 백업

시스템 내 중요 파일이 백업되어 있지 않을 경우 피해 규모가 커질 수 있다. 중요 파일을 네트워크로 연결된 다른 서버로 백업할 경우 랜섬웨어 감염 시 백업 서버 또한 감염될 수 있다.

때문에, 중요 파일은 주기적으로 외부 저장장치나 인터넷이 연결되어 있지 않은 오프라인 환경의 PC 또는 서버 등에 백업을 수행하는 것을 권고한다. 또한, 백업 파일이 저장되는 시스템은 2차 인증을 적용하여 인가자만 접근할 수 있도록 설정하는 것을 권고한다.

4.3 시스템 및 인프라 관리

사용하지 않는 서비스 비활성화

가장 대표적인 서비스로는 SSH, TELNET, 원격 데스크톱, VPN 등 사용하지 않는 서비스들이 외부에서 접근 가능할 경우 초기 공격 대상이 될 수 있으며, 이미 공격자가 서버에 침투하였을 경우에는 내부 확산으로 이어질 가능성이 매우 높다. 때문에, 사용하지 않는 서비스는 비활성화 및 제거하는 것을 권고한다.

Active Directory 환경 보안 정책 점검

다수의 전산 자원 관리를 위해 사용되는 AD(Active Directry)는 도메인에 가입되어 있는 단말기나 서버의 일률적 제어가 가능하기 때문에 침해사고 발생 시 피해 규모가 커질 수 있다. AD 환경에서의 기본 보안 강화는 아래와 같다.

① 불필요한 관리자 계정 비활성화

② 관리자 계정 최소한 사용

③ 그룹 정책 템플릿(GPT) 변경 사항 모니터링

④ AD 정책 배포와 관련 SMB 포트 사용 이벤트 모니터링

⑤ 서버 계정 간 적절한 액세스 제어 구현

망 분리 인프라 환경 구성 권고

공격자는 취약한 호스트 PC, 서버를 감염시키며, 감염된 호스트들은 다른 호스트 PC들을 찾아서 공격한다. 악성코드에 감염된 서버와 동일한 네트워크 대역에 속해 있는 서버는 2차 공격 및 감염에 취약할 수 있다. 때문에, 사내 시스템 업무 유형들을 파악하여 업무에 맞는 네트워크 망을 구성하여 체계적으로 관리 및 운영해야 한다.

원격 데스크톱 접근 보안 강화

공격자는 원격 데스크톱 프로토콜을 이용하여 피해 시스템에 접근할 수 있다. 공격자가 원격으로 서버에 접근할 경우 일반 사용자처럼 작업을 수행할 수 있다. 따라서 인가된 사용자만 접근이 가능하도록 화이트리스트 정책을 권고한다. 또한, 원격 데스크톱 접근 시 OTP와 같은 다중 인증 방식(MFA, Multi-Factor Authentication)을 통해 서버에 접속할 수 있도록 제한하는 것을 권고한다.

로컬 관리자 계정 정보 변경

피해 시스템에 지속적인 접근 유지를 위해 백도어 계정을 생성한다. 윈도우 서버의 경우 ‘Administrator’가 기본 관리자 계정으로 생성된다. 관리가 계정 이름을 변경하거나 비활성화하여 공격자로부터 관리자 계정 접근을 제한해야 한다. 또한, 비밀번호 정책은 공격자가 유추하기 어려운 특수문자, 대/소문자, 숫자 조합으로 10자리 이상을 권고한다.

4.4 잠재적 위협 요소 제거

악성 파일 삭제 또는 운영체제 재설치 후 사용

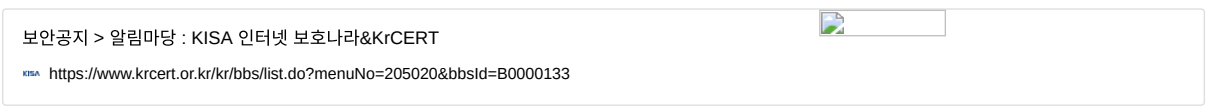
공격자가 사용한 공격 도구가 서버 내에 존재할 경우, 동일한 공격자에 의해 추가 공격이 수행될 가능성이 높다. 공격자가 추후 공격을 위해 남겨둔 파일, 프로세스, 서비스 등 위협 요소를 제거하여 공격자의 추가 공격을 차단한다. 혹은 운영체제를 재설치 하는 것도 위협을 제거하는 하나의 방법이 될 수 있으므로 최신 운영체제 설치하여 취약점에 대비하는 것을 권고한다.

4.5 한국인터넷진흥원 정보보호 서비스 활용

한국인터넷진흥원은 개인/기업 보안에 도움이 될 수 있다. 중소기업 대상으로 현재 ‘중소기업 침해사고 피해지원 서비스’를 제공 중이다. 더불어 각종 보안 보고서, 대응 가이드를 제공하고 있으며 보안 관련 중요한 이슈 발생시 홈페이지 내 보안공지를 통해서 공유하고 있다. 자세한 내용은 아래 한국인터넷진흥원 인터넷 보호나라에서 확인할 수 있다.

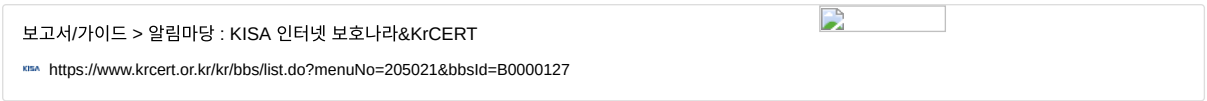
한국인터넷진흥원 보안공지

보안 관련 주요 이슈 발생시 한국인터넷진흥원에서 관련 내용을 공지하고 있다.



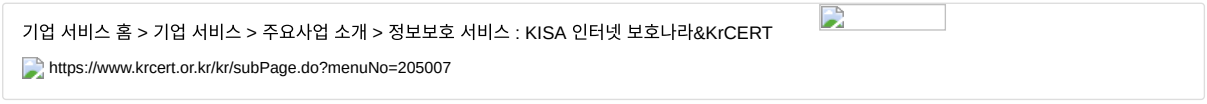
한국인터넷진흥원 배포 가이드/보고서

한국인터넷진흥원에서 발간하는 각종 보안 가이드와 공격그룹 분석 보고서를 제공하고 있다



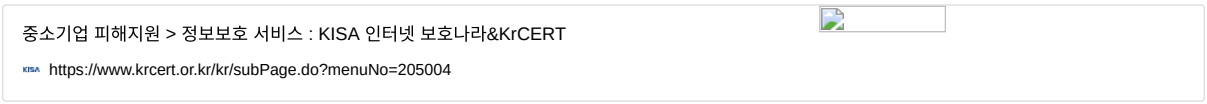
중소기업 대상 보안서비스

중소기업을 대상으로 한국인터넷진흥원에서 제공하는 보안서비스이며, 이번 샤오치잉 공격 관련으로는 내 서버 돌보미, 중소기업 홈페이지 보안강화 보안서비스를 권장한다.



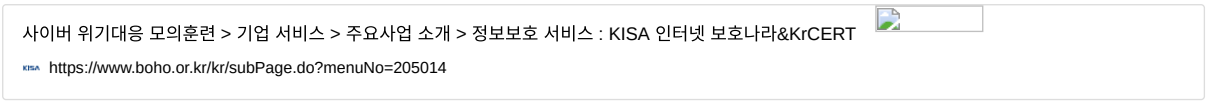
중소기업 침해사고 피해지원 서비스

중소기업에서 침해사고가 발생하는 경우 한국인터넷진흥원에서 원인분석 및 재발방지를 위한 원인제거, 예방컨설팅, 보안교육을 지원하고 있다.



사이버 위기대응 모의훈련

중소기업에 해당되지 않더라도 중견, 대기업 등 참여대상 제한이 없는 서비스도 제공하고 있다. 사이버 공격 예방 및 피해 최소화를 위해 기업의 보안수준 강화와 임직원 인식을 제고하고자 실전형 모의훈련을 실시하고 있다.



5. Conclusion

지금까지 블랙캣 랜섬웨어 해킹그룹의 공격 방법과 전략에 대해 살펴 보았다. 지금 이 순간에도 공격자들은 기업 전산 시스템에 침투하기 위해 새로운 원데이 취약점과 전략으로 공격을 시도하고 있으며 랜섬웨어 침해사고는 그 동안 쌓은 기업의 대외 이미지와 신뢰를 한 순간에 무너 질 수 있다는 사실을 잊지 말아야 한다.

이를 위해 기업 보안·전산 담당자는 주요 자산과 백업 체계를 다시 한 번 재점검하여 보안을 강화하고 한국인터넷진흥원에서 공개한 침해사고 기술보고서와 보호나라의 보안공지, 다양한 사이버 보안 매체 등에 관심을 기울여 공격자들의 전략을 예측하여 대비한다면 최소한 공격자가 목표를 달성을 하기 전 차단·예방 할 수 있을 것이다.

※ 기업 침해사고 발생 시, KISA-보호나라 홈페이지를 통해 신고

→ 랜섬웨어, 디도스, 일반 해킹사고 신고(https://www.boho.or.kr/kr/subPage.do?menuNo=205004)

IoC

악성코드

파일명	SHA1 **Hash**	**기능**
file64.exe	f5df10a3d5b3d0b511f8645d1c24260c449ef7b7	백신 등 특정 프로세스 종료
ComKJ.sys	b2f955b3e6107f831ebe67997f8586d4fe9f3e98	백신 등 특정 프로세스 종료
Backstab.exe	22a3eabf1f54476915448019ffff20aa74a2a2cd	백신 강제 종료 도구
socks.exe	c182f85d6315170d605cd87c11a6eb1404dd5fe3	원격제어형 악성코드
socks2.exe	35e56be708429e730c8c8165581eb168ea46e0f5	원격제어형 악성코드
processhacker.exe	c953d525c2d0bdf321ec98ab1a8cf69c2425102c	프로세스 실행 및 종료 도구
ADfind.exe	2cb6ff75b38a3f24f3b60a2742b6f4d6027f0f2a	AD Query 도구
winscp.exe	b0b063768ccdd5fead2052624d57454501ff7639	원격 접근 프로그램
psexec64.exe	fb0a150601470195c47b4e8d87fcb3f50292beb2	시스템 프로세스를 관리하기 위한 유틸리티 도구
netscan.exe	efe8b9ff7ff93780c9162959a4c1e5ecf6e840a4	네트워크 스캔 도구
NetworkShare_pre2.exe	629c9649ced38fd815124221b80c9d9c59a85e74	네트워크 스캔 도구
[무작위].exe	24c13d46de755cb22f904b3d601bc47ec8e4b53e	블랙캣 랜섬웨어

파일명	SHA1 **Hash**	**기능**
[회사명].exe	58964b055faf9b7f72d1725786f8112f56c187bd	블랙캣 랜섬웨어

공격자 IP

IP/domain	**국가코드(국가명)**	**행위**
91.208.52.149	NL(네덜란드)	VPN 접근
195.123.241.196	US(미국)	VPN 접근
185.220.101.36	DE(독일)	VPN 접근
5.135.174.210	FR(프랑스)	VPN 접근
147.135.36.162	US(미국)	VPN 접근
147.135.11.223	US(미국)	VPN 접근
5.181.234.58	US(미국)	VPN 접근
185.225.17.198	RO(루마니아)	원격접속
198.12.113.138	US(미국)	원격접속
84.32.191.225	LT(리투아니아)	Cobalt Strike C2
179.60.146.11	RU(러시아)	Cobalt Strike C2
195.189.96.174	LT(리투아니아)	C2
146.70.53.169	BG(불가리아)	C2