## Incident Forensic Analysis Report

# 침해사고 포렌식 보고서

Windows AD 침해사고 분석


**작 성 자** 신가현

**소 속** 시큐리티아카데미


**제 출 일** 2026-06-04

**문서 버전** v1.0

# 목 차

# 1. 사고 개요

본 보고서는 2026년 6월 1일 10:00~11:00 KST 구간의 ELK/Kibana alerts 로그, Timesketch 공격 태그 로그, 핵심 이벤트 star/comment를 근거로 Windows Server 3대 기반 AD 환경에서 발생한 침해 의심 행위를 분석한 결과이다. 핵심 공격 구간은 10:26:15~10:38:37 KST로 확인되며, PC01에서 employee1 계정 기반 실행/정찰 후 Kerberoasting, svc_file 계정 활용 FS01 원격 실행, LSASS 접근, 파일 업로드, DC01에 대한 관리자 계정 로그온 및 DCSync/Golden Ticket 정황으로 이어졌다.

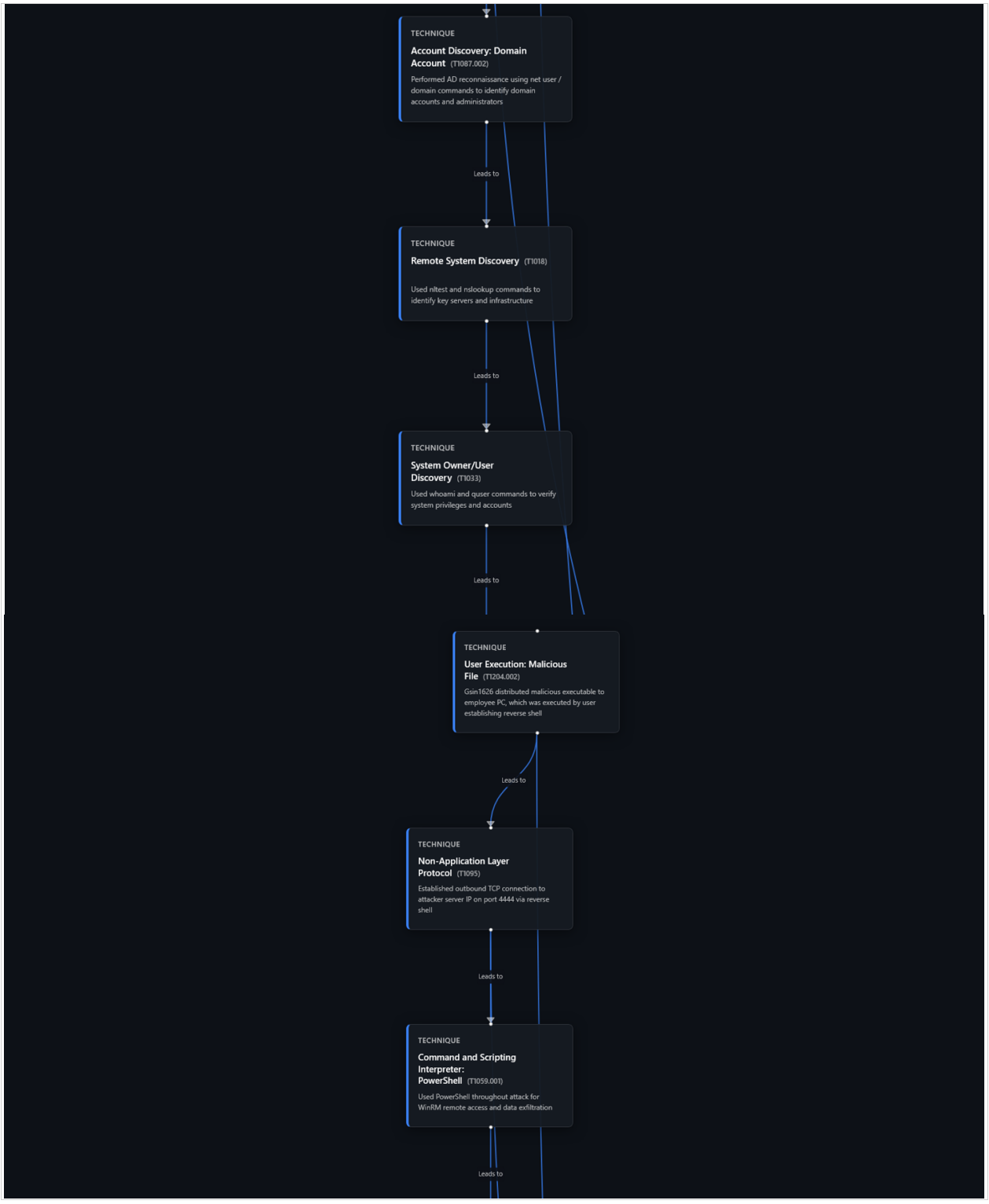
| | |
|---|---|
| **사고 명칭** | Windows AD 침해사고 분석 |
| **사고 유형** | AD 계정 침해, Kerberoasting, 원격 실행, 자격 증명 접근, DCSync, 파일 유출 의심 |
| **의뢰인 / 담당 부서** | KISIA 프로젝트 / DF 분석 |
| **사고 인지 일시** | 2026-06-01 10:26:15.667 KST |
| **사고 발생 추정 일시** | 2026-06-01 10:26:15.667 KST |
| **대응 착수 일시** | ELK Rule 탐지 이후 분석 착수 |
| **분석 기간** | 2026-06-01 10:00:00 ~ 2026-06-01 11:00:00 KST |
| **사고 심각도** | 심각: DC01 대상 DCSync 및 Golden Ticket 의심 정황, FS01 LSASS 접근, 외부 업로드 정황 확인 |
| **현재 처리 상태** | 분석 완료, 실제 격리/차단/복구 상태 확인 필요 |

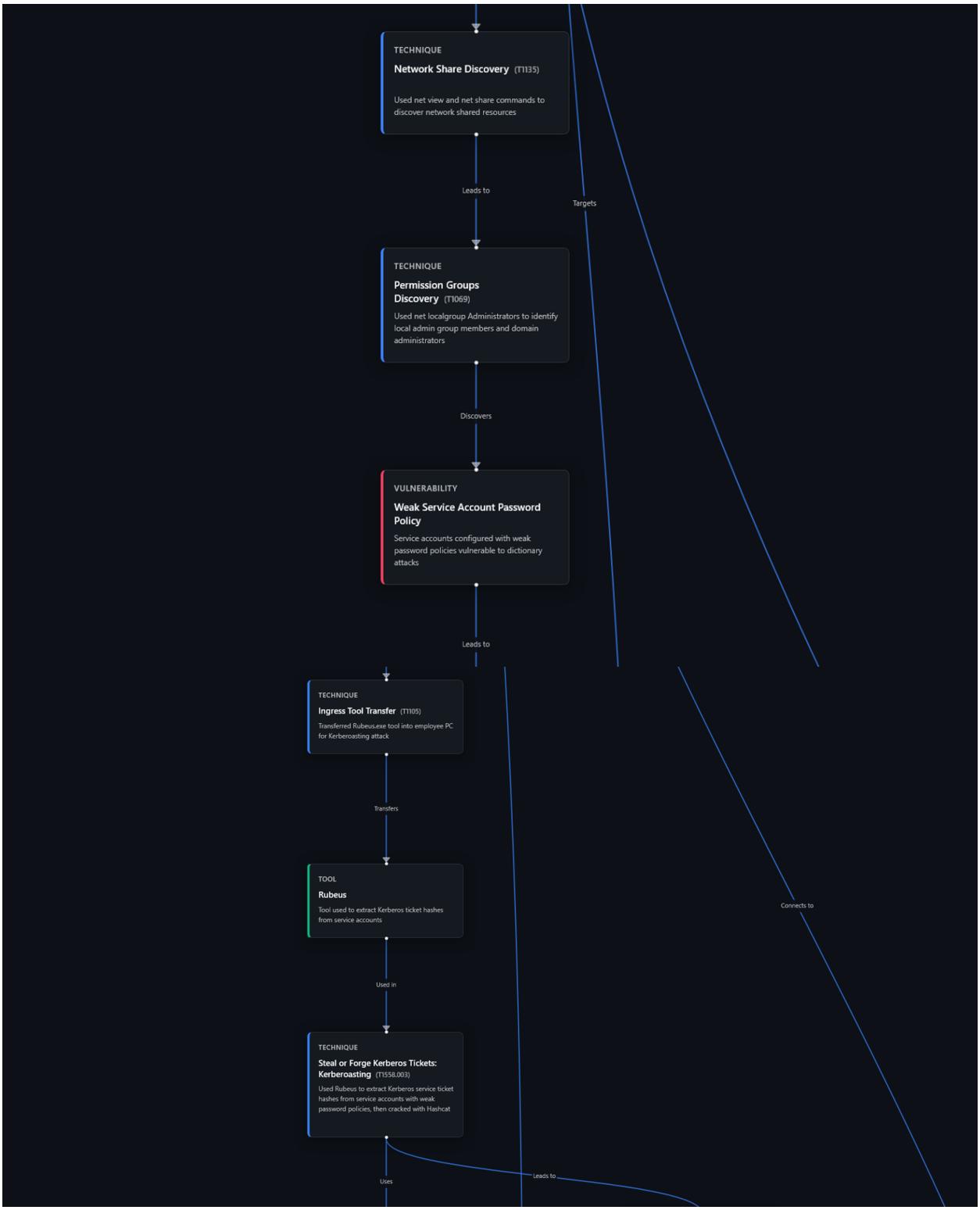
## 1.1. 사고 요약

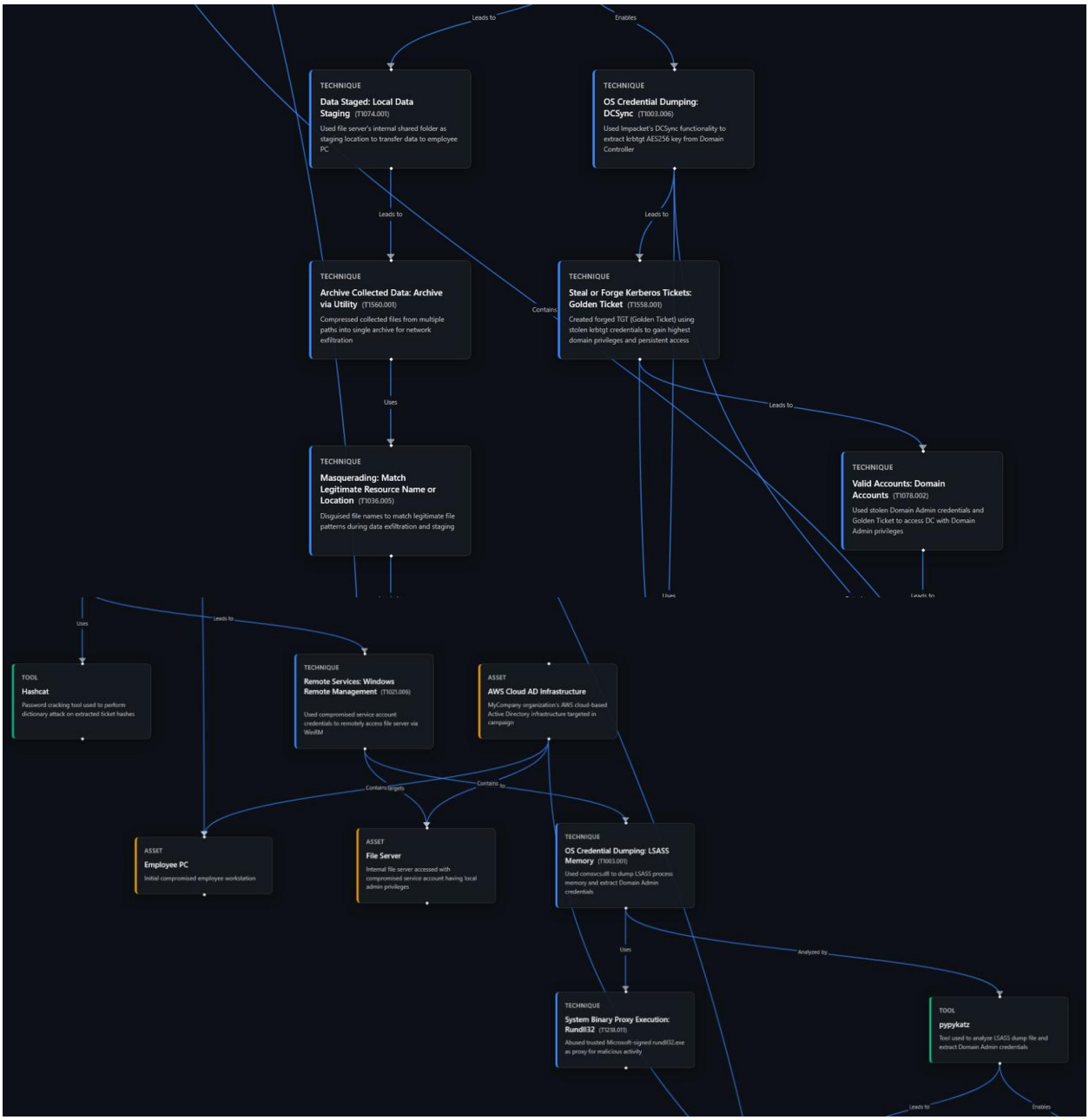
• PC01.mycompany.local 에서 MYCOMPANY₩employee1 권한으로 알 수 없는 실행 파일(SecurityUpdate.exe)의 자식 프로세스 cmd.exe 실행이 확인되었다.
• employee1 계정은 DC01 에서 svc_file 서비스 계정에 대한 Kerberoasting 의심 TGS 요청을 수행한 것으로 탐지되었다.

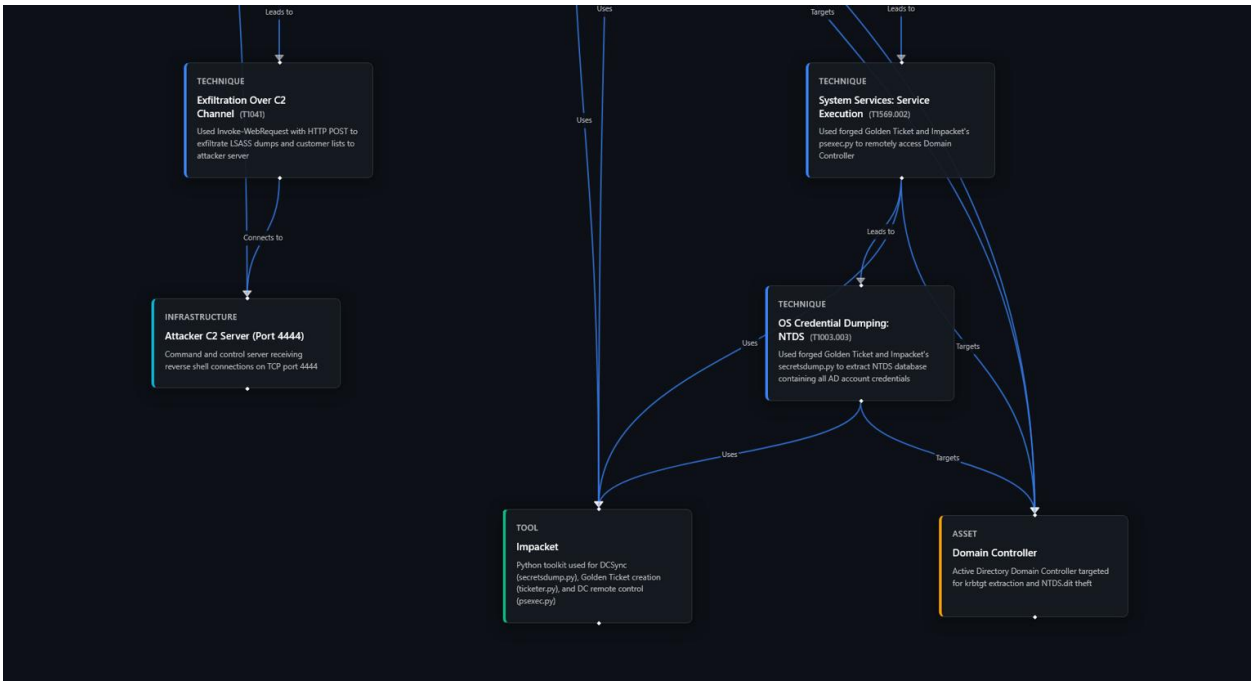
• PC01 및 FS01 에서 PowerShell 기반 HTTP 업로드 정황이 확인되었으며, hashes.txt 및 share_data.zip 이 54.180.55.229:8081 로 업로드된 것으로 분석된다.
• svc_file 계정은 FS01 에 WinRM 기반 원격 실행을 수행했고, 이후 rundll32.exe 가 lsass.exe 에 접근하여 LSASS 메모리 덤프가 의심된다.
• 비인가 IP 10.0.1.194 에서 DC01 에 admin_user 및 Administrator 계정으로 네트워크 로그온이 발생했고, 근소한 시차로 DCSync 의심 AD 복제 권한 접근이 탐지되었다.
• Administrator 계정 관련 TGT 요청 없이 TGS 요청이 발생한 Golden Ticket 의심 Kerberos 활동이 확인되어 도메인 권한 침해 가능성이 높다.
• 데이터 유출은 HTTP 업로드 정황으로 의심되나, 실제 업로드 파일 내용과 외부 서버 수신 여부는 추가 확인이 필요하다.

## [그림 1] 침해사고 관계도


TECHNIQUE
Account Discovery: Domain Account (T1087.002)
Performed AD reconnaissance using net user / domain commands to identify domain accounts and administrators
Leads to
TECHNIQUE
Remote System Discovery (T1018)
Used nltest and nslookup commands to identify key servers and infrastructure
Leads to
TECHNIQUE
System Owner/User Discovery (T1033)
Used whoami and quser commands to verify system privileges and accounts
Leads to
TECHNIQUE
User Execution: Malicious File (T1204.002)
Gsin1626 distributed malicious executable to employee PC, which was executed by user establishing reverse shell
Leads to
TECHNIQUE
Non-Application Layer Protocol (T1095)
Established outbound TCP connection to attacker server IP on port 4444 via reverse shell
Leads to
TECHNIQUE
Command and Scripting Interpreter: PowerShell (T1059.001)
Used PowerShell throughout attack for WinRM remote access and data exfiltration
Leads to


TECHNIQUE
Network Share Discovery (T1135)
Used net view and net share commands to discover network shared resources
Leads to
Targets
TECHNIQUE
Permission Groups Discovery (T1069)
Used net localgroup Administrators to identify local admin group members and domain administrators
Discovers
VULNERABILITY
Weak Service Account Password Policy
Service accounts configured with weak password policies vulnerable to dictionary attacks
Leads to
TECHNIQUE
Ingress Tool Transfer (T1105)
Transferred Rubeus.exe tool into employee PC for Kerberoasting attack
Transfers
TOOL
Rubeus
Tool used to extract Kerberos ticket hashes from service accounts
Used in
TECHNIQUE
Steal or Forge Kerberos Tickets: Kerberoasting (T1558.003)
Used Rubeus to extract Kerberos service ticket hashes from service accounts with weak password policies, then cracked with Hashcat
Uses
Leads to
Connects to


Leads to
Enables
TECHNIQUE
Data Staged: Local Data Staging (T1074.001)
Used file server's internal shared folder as staging location to transfer data to employee PC
TECHNIQUE
OS Credential Dumping: DCSync (T1003.006)
Used Impacket's DCSync functionality to extract krbtgt AES256 key from Domain Controller
Leads to
Leads to
TECHNIQUE
Archive Collected Data: Archive via Utility (T1560.001)
Compressed collected files from multiple paths into single archive for network exfiltration
Contains
TECHNIQUE
Steal or Forge Kerberos Tickets: Golden Ticket (T1558.001)
Created forged TGT (Golden Ticket) using stolen krbtgt credentials to gain highest domain privileges and persistent access
Uses
Leads to
TECHNIQUE
Masquerading: Match Legitimate Resource Name or Location (T1036.005)
Disguised file names to match legitimate file patterns during data exfiltration and staging
TECHNIQUE
Valid Accounts: Domain Accounts (T1078.002)
Used stolen Domain Admin credentials and Golden Ticket to access DC with Domain Admin privileges
Uses
Leads to
TOOL
Hashcat
Password cracking tool used to perform dictionary attack on extracted ticket hashes
TECHNIQUE
Remote Services: Windows Remote Management (T1021.006)
Used compromised service account credentials to remotely access file server via WinRM
ASSET
AWS Cloud AD Infrastructure
MyCompany organization's AWS cloud-based Active Directory infrastructure targeted in campaign
Contains targets
Contains
ASSET
Employee PC
Initial compromised employee workstation
ASSET
File Server
Internal file server accessed with compromised service account having local admin privileges
TECHNIQUE
OS Credential Dumping: LSASS Memory (T1003.001)
Used comsvcs.dll to dump LSASS process memory and extract Domain Admin credentials
Uses
Analyzed by
TECHNIQUE
System Binary Proxy Execution: Rundll32 (T1218.011)
Abused trusted Microsoft-signed rundll32.exe as proxy for malicious activity
TOOL
pypykatz
Tool used to analyze LSASS dump file and extract Domain Admin credentials
Leads to
Enables


Leads to
Uses
Targets
Leads to
TECHNIQUE
Exfiltration Over C2 Channel (T1041)
Used Invoke-WebRequest with HTTP POST to exfiltrate LSASS dumps and customer lists to attacker server
Uses
TECHNIQUE
System Services: Service Execution (T1569.002)
Used forged Golden Ticket and Impacket's psexec.py to remotely access Domain Controller
Connects to
Leads to
INFRASTRUCTURE
Attacker C2 Server (Port 4444)
Command and control server receiving reverse shell connections on TCP port 4444
TECHNIQUE
OS Credential Dumping: NTDS (T1003.003)
Used forged Golden Ticket and Impacket's secretsdump.py to extract NTDS database containing all AD account credentials
Uses
Targets
Uses
Targets
TOOL
Impacket
Python toolkit used for DCSync (secretsdump.py), Golden Ticket creation (ticketer.py), and DC remote control (psexec.py)
ASSET
Domain Controller
Active Directory Domain Controller targeted for krbtgt extraction and NTDS.dit theft

# 2. 분석 대상

[표] 증거 목록

| 번호 | 파일명 / 시스템명 | 수집 위치 | 파일 크기 | 해시값 (MD5 / SHA256) |
|---|---|---|---|---|
| 1 | timesketch_alerts.csv | ELK Kibana의 Alerts 로그를 수집하여 Timesketch 업로드용으로 가공 | 152KB | MD5 1d18e813431224dad102306af812a0e3<br>SHA256<br>8703c1751febeb8dc9ec3a130a9a40d874ca72637947f226bc86375403bd6e1a |
| 2 | tag_attack.zip | Timesketch 공격 태그 이벤트 | 29KB | MD5 ae2623af136b45eff5769418d9a0ff02<br>SHA256<br>6b08510bc50013a956b4b326672d277e0b254e383b2183f4033370d66e438480 |
| 3 | starred_comment.xlsx | Timesketch star 이벤트 및 comment | 21KB | MD5 82cc97f0a336a70d521b8046685b63a0<br>SHA256<br>60f720d7fb28f911a9cf77973f89ec6f7b6c82e539695d63165a3160ade6802e |
| 4 | alerts_logs.jsonl | ELK Kibana의 Alerts 로그 | 741KB | MD5 214edaad122b442f475da059abda6495<br>SHA256<br>f6245eda7644ad9041371745a94e17c890619347542e7d9b5fb28a536cff7175 |

## 2.1. 분석 환경 및 도구

| 구분 | 도구 / 환경 | 버전 | 용도 |
|---|---|---|---|
| 분석 대상 환경 | Windows Server 3대 (PC01, FS01, DC01) | Windows Server 2022 | Windows AD 환경 |

| 구분 | 도구 / 환경 | 버전 | 용도 |
|---|---|---|---|
| 로그 수집/검색 | ELK (ElasticSearch/Kibana) | 8.13.4 | alerts 로그 수집 및 탐지 룰 적용 |
| 타임라인 분석 | Timesketch | 20260326 | 공격 태그, star, comment 기반 핵심 이벤트 선별 및 타임라인 분석 |
| 보고서 작성 | Codex | 5.5 | 보고서 산출 |

## 2.2. 분석 기준

| 항목 | 판단 기준 | 한계 / 비고 |
|---|---|---|
| 공격 이벤트 우선순위 | starred_comment.xlsx의 star/comment 이벤트를 최우선 분석 대상으로 판단 | 분석가가 핵심 이벤트로 선별한 로그이므로 신뢰도는 높지만, comment에 포함되지 않은 보조 이벤트는 누락될 수 있음 |
| 공격 행위 판단 | Timesketch에서 "공격" 태그가 부여된 로그를 공격 행위 판단의 주요 근거로 사용 | 태그는 분석가 판단 결과이므로 원본 로그와 함께 교차 확인 필요 |
| 전체 로그 맥락 | timesketch_alerts.csv 전체 alert를 기준으로 공격 전후 흐름, 반복 경보, 정상/비정상 맥락을 확인 | 전체 alert가 모두 공격을 의미하지는 않으므로 단순 경보 발생만으로 침해를 단정하지 않음 |
| AD 환경 기반 판단 | Windows Server 3대로 구성된 AD 환경에서 계정 인증, 권한 사용, 도메인 컨트롤러 접근, 서버 간 원격 실행 여부를 중심으로 판단 | AD 정상 관리 행위와 공격 행위가 유사할 수 있어 계정, 시간, 대상 호스트, 연속성을 함께 고려 |
| MITRE ATT&CK 매핑 | 탐지 룰에 매핑된 MITRE | 매핑은 탐지 룰 기반이므로 실제 |

| 항목 | 판단 기준 | 한계 / 비고 |
|---|---|---|
| | ATT&CK Technique을 기준으로 공격 전술과 기법을 분류 | 공격 성공 여부와는 구분 필요 |

# 3. 분석 결과 요약

전체 alerts 104건 중 Timesketch에서 공격 태그가 부여된 이벤트는 89건이며, 이 중 핵심 star/comment 이벤트는 12건이다. 공격 태그 구간은 2026-06-01 10:26:15.667~10:38:37.038 KST로 확인된다. 분석 결과 단순 경보가 아닌 AD 계정 기반 공격 흐름이 관찰되며, Kerberoasting, WinRM 원격 실행, LSASS 접근, HTTP 파일 업로드, DCSync, Golden Ticket 의심 활동이 연속적으로 발생했다.

## 3.1. 분석 관점

| 확인 항목 | 분석 관점 | 확인 근거 | 판단 결과 |
|---|---|---|---|
| 초기 침투 | 공격자가 최초로 내부 시스템에서 명령 실행 권한을 확보했는지 확인 | C01.mycompany.local에서 MYCOMPANY₩employee1 권한으로 cmd.exe 실행 탐지, 분석가 comment의 SecurityUpdate.exe 하위 프로세스 실행 내용 | 일반 사용자 계정 기반으로 의심 명령 실행이 발생하여 PC01이 초기 침투 또는 foothold 지점으로 판단됨 |
| 내부 정찰 | 공격자가 AD 환경의 계정, 시스템, 공유, 권한 그룹 정보를 수집했는지 확인 | Domain Account Discovery, Permission Group Discovery, Network Share Discovery, Remote System Discovery 관련 alert 및 PC01/FS01 탐색 로그 | 공격자가 내부 자산과 AD 구조를 파악하기 위한 정찰 행위를 수행한 것으로 판단됨 |
| 서비스 계정 탈취 시도 | 일반 계정이 서비스 계정의 Kerberos 티켓을 요청했는지 확인 | DC01에서 employee1@MYCOMPANY.LOCAL 계정이 svc_file 서비스 티켓을 요청한 로그, ServiceName=svc_file, Status=0x0 | 일반 계정이 관련 없는 서비스 계정 티켓을 요청하여 Kerberoasting 공격 정황으로 판단됨 |
| 내부 이동 | 탈취 또는 악 | FS01.mycompany.local에서 | Kerberoasting 이 |

| 확인 항목 | 분석 관점 | 확인 근거 | 판단 결과 |
|---|---|---|---|
| | 용된 계정을 이용해 다른 서버로 원격 접근했는지 확인 | MYCOMPANY₩svc_file 계정의 WinRM 기반 원격 실행 탐지 | 후 svc_file 계정을 이용해 파일 서버 FS01로 내부 이동한 정황으로 판단됨 |
| 자격 증명 접근 | 공격자가 추가 계정 정보를 확보하기 위해 LSASS 메모리에 접근했는지 확인 | FS01에서 C:₩Windows₩system32₩rundll32.exe가 C:₩Windows₩system32₩lsass.exe에 접근, GrantedAccess=0x1410 | LSASS 메모리 덤프를 통한 자격 증명 탈취 시도로 판단됨 |
| 관리자 계정 악용 | 비인가 IP에서 관리자 계정으로 도메인 컨트롤러에 접근했는지 확인 | DC01에서 10.0.1.194 출발지의 admin_user, Administrator 계정 LogonType 3 로그온 탐지 | 비인가 IP를 통한 관리자 계정 악용 정황으로 판단됨 |
| 도메인 자격 증명 탈취 | 도메인 컨트롤러의 복제 권한이 악용되었는지 확인 | DC01에서 admin_user, Administrator 계정의 DCSync 의심 AD 복제 권한 접근 탐지, AccessMask=0x100, 복제 권한 GUID 포함 | 도메인 계정 해시 탈취 목적의 DCSync 공격 정황으로 판단됨 |
| Kerberos 티켓 위조 | 정상 TGT 발급 없이 TGS 요청이 발생했는지 확인 | 10.0.1.194에서 4768=0, 4769>0 Kerberos 활동 탐지, ticket_hash 관찰 | Golden Ticket 또는 위조 Kerberos 티켓 사용 의심 정황으로 판단됨 |

## 3.2. 사고 타임라인

| 일시 | 출발지 / 대상 | 행위 | 근거 (로그·아티팩트) |
|---|---|---|---|
| 2026-06-01 10:26:15.667 KST | PC01.mycompany.local(employee1) | PC01.mycompany.local에서 employee1 권한으로 Windows 명령 셸 실행이 탐지됨 | 알 수 없는 실행 파일 (SecurityUpdate.exe)의 자식 프로세스로 cmd.exe가 실행됨. |
| 2026-06-01 10:29:19.125 KST | DC01.mycompany.local / ::ffff:10.0.4.216(employee1) | 10.0.4.216(PC01)에서 employee1 계정의 Kerberoasting 의심 | 일반계정 (employee1)이 관련 없는 서비스계정(svc_file)에 대한 티켓을 요청함. 커버로스팅 공격 의심. |
| 2026-06-01 10:29:43.136 KST | PC01.mycompany.local(employee1) / 54.180.55.229:8081 | PC01.mycompany.local에서 PowerShell 기반 HTTP 파일 업로드 또는 유출 의심 행위가 탐지됨 | 일반계정 (employee1)이 Powershell 기반 HTTP 파일 업로드를 통해 PC01의 hashes.txt 파일을 54.180.55.229:8081에 업로드함 |
| 2026-06-01 10:31:09.567 KST | FS01.mycompany.local(svc_fil)e | FS01.mycompany.local에서 svc_file 계정의 WinRM 기반 원격 실행 정황이 탐지됨 | 일반계정 (employee1)이 서비스 계정(svc_file)에 대한 티켓 요청 성공 이후 svc_file 계정이 파일서버 (FS01)로 원격 접 |

| 일시 | 출발지 / 대상 | 행위 | 근거 (로그·아티팩트) |
|---|---|---|---|
| | | | 속함. |
| 2026-06-01 10:32:07.072 KST | FS01.mycompany.local / (SYSTEM) | FS01.mycompany.local에서 C:₩Windows₩system32₩rundll32.exe가 C:₩Windows₩system32₩lsass.exe에 접근한 LSASS 메모리 덤프 의심 행위가 탐지됨 | svc_file의 FS01 원격 접속 이후, lsass.exe에 접근함. LSASS 메모리 덤프 행위 의심. (GrantedAccess=0x1410) |
| 2026-06-01 10:34:31.111 KST | FS01.mycompany.local (svc_file) | FS01.mycompany.local에서 PowerShell 기반 HTTP 파일 업로드 또는 유출 의심 행위가 탐지됨 | svc_file의 FS01 원격 접속 이후, svc_file이 FS01에서 Powershell의 HTTP 파일 업로드를 통해 share_data.zip 파일을 54.180.55.229:8081로 전송함. |
| 2026-06-01 10:36:48.851 KST | 10.0.1.194(admin_user) / DC01.mycompany.local | DC01.mycompany.local에서 관리자 또는 도메인 계정의 의심스러운 네트워크 로그온이 탐지됨 | svc_file의 lsass.exe 접근 및 파일 유출 이후, 비인가 IP(10.0.1.194)로부터 관리자 계정(admin_user)으로 도메인 컨트롤러(DC01)에 로그온함. |
| 2026-06- | DC01.mycompany.local(ad | DC01.mycompany.local에서 | 비인가 |

| 일시 | 출발지 / 대상 | 행위 | 근거 (로그·아티팩트) |
|---|---|---|---|
| 01 10:36:48.872 KST | min_user) | admin_user 계정의 DCSync 의심 AD 복제 권한 접근이 탐지됨 | IP(10.0.1.194)의 도메인 컨트롤러(DC01) 로그온 발생 후 근소한 시차로 DCSync 의심 AD 복제 권한 접근이 탐지됨. |
| 2026-06-01 10:38:18.848 KST | DC01.mycompany.local(Administrator) | DC01.mycompany.local에서 의심스러운 서비스(LjYLAjAi.exe) 설치 또는 실행 행위가 탐지됨 | 비인가 IP(10.0.1.194)의 도메인 컨트롤러(DC01) 로그온 이후, 알 수 없는 서비스(LjYLAjAi.exe)가 systemroot 경로에서 설치 또는 실행됨. |
| 2026-06-01 10:38:19.095 KST | ::ffff:10.0.1.194(Administrator) | 알 수 없는 호스트(10.0.1.194)에서 Administrator 계정 관련 Golden Ticket 의심 Kerberos 활동이 탐지됨 | 비인가 IP(10.0.1.194)에서 TGT 요청(4768) 없이 TGS 요청(4769)이 탐지됨. |
| 2026-06-01 10:38:36.873 KST | 10.0.1.194(Administrator) / DC01.mycompany.local | DC01.mycompany.local에서 관리자 또는 도메인 계정의 의심스러운 네트워크 로그온이 탐지됨 | Administrator 관련 Golden Ticket 의심 Kerberos 활동이 탐지된 이후, 비인가 IP(10.0.1.194)에서 Administrator으로 도메인 컨트롤러 |

| 일시 | 출발지 / 대상 | 행위 | 근거 (로그·아티팩트) |
|---|---|---|---|
| | | | (DC01) 로그온 |
| 2026-06-01 10:38:36.955 KST | DC01.mycompany.local(Administrator) | 핵심 탐지: DC01.mycompany.local에서 Administrator 계정의 DCSync 의심 AD 복제 권한 접근이 탐지됨 | Administrator 관련 Golden Ticket 의심 Kerberos 활동이 탐지된 이후, Administrator계정으로 DCSync 의심 AD 복제 권한 접근이 탐지됨 |

## 3.3. MITRE ATT&CK 매트릭스

| Initial Access | Execution | Credential Access | Discovery | Lateral Movement | Exfiltration |
|---|---|---|---|---|---|
| T1078.002 Valid Accounts: Domain Accounts | T1059.003 Command and Scripting Interpreter: Windows Command Shell | T1003.001 OS Credential Dumping: LSASS Memory | T1018 - Remote System Discovery | T1021.006 Remote Services: Windows Remote Management | T1041 - Exfiltration Over C2 Channel |
| | T1059.001 Command and Scripting Interpreter: PowerShell | T1003.006 OS Credential Dumping: DCSync | T1033 - System Owner/User Discovery | | |
| | T1569.002 System Services: Service Execution | T1558.001 Steal or Forge Kerberos Tickets: Golden Ticket | T1069 - Permission Groups Discovery | | |
| | | T1558.003 Steal or Forge Kerberos Tickets: Kerberoasting | T1087.002 Account Discovery: Domain Account | | |
| | | | T1135 - Network Share Discovery | | |

## 3.4. MITRE ATT&CK 기법 상세

| 기법 ID | 사용 기술 | 설명 |
|---|---|---|
| T1059.003 | Windows Command Shell | PC01에서 employee1 권한 cmd.exe 실행. SecurityUpdate.exe 하위 프로세스로 실행되어 정상 관리 행위가 아닌 공격 실행 정황으로 판단. |
| T1087.002 / T1069 / T1018 / T1135 / T1033 | Discovery | PC01 및 FS01에서 계정, 그룹, 시스템, 공유, 원격 시스템 탐색 경보가 반복 발생. 공격자의 환경 파악 단계로 판단. |
| T1558.003 | Kerberoasting | employee1@MYCOMPANY.LOCAL이 svc_file 서비스 티켓을 요청하고 Status=0x0으로 성공. 일반 계정이 관련 없는 서비스 계정 티켓을 요청한 점이 핵심 근거. |
| T1021.006 | WinRM Remote Execution | svc_file 계정이 FS01에 WinRM 기반 원격 실행을 수행. Kerberoasting 이후 서비스 계정 악용 가능성. |
| T1003.001 | LSASS Dump | FS01에서 rundll32.exe가 lsass.exe에 GrantedAccess=0x1410으로 접근. LSASS 메모리 덤프 의심. |
| T1041 | Exfiltration Over C2 Channel | PC01/FS01에서 PowerShell HTTP 업로드가 탐지되었고, comment 기준 hashes.txt 및 share_data.zip이 54.180.55.229:8081로 업로드됨. |
| T1003.006 | DCSync | DC01에서 admin_user 및 Administrator 계정의 AD 복제 권한 접근이 다수 탐지됨. 비인가 IP 로그온 직후 발생한 점이 중요. |
| T1558.001 | Golden Ticket | 10.0.1.194에서 TGT 요청 없이 TGS 요청이 관찰되어 위조 Kerberos 티켓 사용 의심. |
| T1569.002 | Service Execution | DC01에서 LYJH 서비스 |

| 기법 ID | 사용 기술 | 설명 |
| --- | --- | --- |
| | | 및 %systemroot%₩LjYLAjAi.exe 설치/실행 정황이 확인됨. |

# 4. 공격 흐름 분석

| 공격 단계 | 통제 실패 지점 | 사용 기법(TTPs) | 공격 인과 분석 |
|---|---|---|---|
| 1. 초기 침투 | employee1 계정 또는 PC01 실행 경로의 신뢰성 검증 미흡 가능성 | T1059.003 | SecurityUpdate.exe 하위 cmd.exe 실행 이후 정찰 경보가 이어져 PC01 foothold 확보 정황으로 판단. |
| 2. 권한 상승 및 거점 확보 | 서비스 계정 티켓 요청과 자격 증명 보호 미흡 가능성 | T1558.003, T1021.006, T1003.001 | employee1의 Kerberoasting 이후 svc_file로 FS01 원격 실행 및 LSASS 접근이 발생해 자격 증명 탈취/확대 가능성이 높음. |
| 3. 내부 이동 | AD 계정 기반 원격 접근 통제 및 이상 행위 탐지 미흡 가능성 | T1021.006, T1078.002 | svc_file이 FS01에 접근하고 이후 10.0.1.194에서 DC01 관리자 계정 로그온이 발생해 내부 이동 및 권한 확장 흐름으로 판단. |
| 4. 데이터 접근 및 유출 시도 | 외부 HTTP 업로드 통제 및 민감 파일 반출 탐지 미흡 가능성 | T1041 | PC01의 hashes.txt, FS01의 share_data.zip 외부 업로드 정황이 확인됨. 실제 파일 내용과 수신 여부는 추가 확인 필요. |
| 5. 도메인 장악 시도 | 관리자 계정/도메인 복제 권한 보호 미흡 가능성 | T1003.006, T1558.001, T1569.002 | admin_user/Administrator 로그온 직후 DCSync 및 Golden Ticket 의심 활동, 의심 서비스 실행이 관찰되어 도메인 권한 침해 가능성이 큼. |

# 5. 침해지표

| 유형 | 지표 값 | 설명 |
|---|---|---|
| 외부 IP | 10.0.1.194, 54.180.55.229 | DC01 관리자 계정 로그온 및 Golden Ticket 의심 Kerberos 활동 출발지 |
| 파일 | SecurityUpdate.exe | 리버스 쉘 연결을 통한 초기 침투에 사용된 도구로 탐지된 파일 |
| 파일 | hashes.txt, share_data.zip | 외부 업로드 의심 파일명. 실제 내용 확인 필요 |
| 계정 | MYCOMPANY₩employee1 | 리버스 쉘을 통한 PC01 명령 실행, Kerberoasting 의심 서비스 티켓 요청 계정 |
| 계정 | MYCOMPANY₩svc_file | FS01 WinRM 원격 실행 및 LSASS 접근 이후 활동 관련 계정 |

| 유형 | 지표 값 | 설명 |
|---|---|---|
| 파일 | %systemroot%₩LjYLAjAi.exe | DC01 의심 서비스 설치 또는 실행 |
| Kerberos | ticket_hash=ewiqn88sNnnHZpuzTl+tNdxtOvqZ9p4+wXbN9s1XV0Q= | Golden Ticket 의심 활동에 반복 관찰된 티켓 해시 |

# 6. 피해 범위 및 영향

| 구분 | 영향 받은 자산 | 피해 내용 | 영향 수준 |
|---|---|---|---|
| 계정 | employee1 | 초기 실행 및 Kerberoasting 의심 행위에 사용됨. 계정 탈취 또는 악용 가능성. | 높음 |
| 계정 | svc_file | FS01 원격 실행 및 LSASS 접근 흐름에 사용됨. 서비스 계정 자격 증명 노출 가능성. | 높음 |
| 계정 | admin_user, Administrator | DC01 로그온 및 DCSync/Golden Ticket 정황과 연계됨. | 심각 |
| 시스템 | PC01 | 명령 실행, 정찰, hashes.txt 업로드 정황. | 높음 |
| 시스템 | FS01 | WinRM 원격 실행, LSASS 접근, share_data.zip 업로드 정황. | 높음 |
| 시스템 | DC01 | DCSync 및 Golden Ticket 의심 활동으로 도메인 전체 영향 가능성. | 심각 |
| 데이터 | hashes.txt, share_data.zip | 외부 업로드 의심. 실제 파일 내용 및 유출 성공 여부 확인 필요. | 확인 필요 |

## 6.1. 영향 평가

• 기밀성: hashes.txt, share_data.zip 외부 업로드 정황과 LSASS 접근, DCSync 의심으로 계정/데

이터 기밀성 침해 가능성이 높다.

• 무결성: DC01에서 의심 서비스 LYJH 및 LjYLAjAi.exe 설치/실행 정황이 있어 시스템 설정 변경 가능성이 있다.

• 가용성: 제공 로그에서 서비스 중단이나 장애 정황은 명확히 확인되지 않는다.

• 개인정보 유출 여부: 제공 로그만으로는 확인되지 않으며, 업로드 파일 내용 확인이 필요하다.

• 법적/규제 영향: 도메인 관리자 권한 및 파일 유출 가능성이 있어 조직 내부 기준에 따른 사고 등급 및 신고 의무 검토가 필요하다.

# 7. 대응 및 개선 방안

## 7.1 의사결정 요약

| 판단 항목 | 현재 판단 | 의사결정 사항 | 근거 |
|---|---|---|---|
| 사고 심각도 | 심각 | AD 도메인 침해 가능성이 있는 중대 사고로 분류 | DC01에서 DCSync 및 Golden Ticket 의심 활동 확인 |
| 공격 성공 여부 | 일부 성공 정황 확인 | 단순 시도가 아닌 내부 이동 및 권한 확장 사고로 대응 | FS01 WinRM 실행, LSASS 접근, DC01 관리자 계정 로그온 확인 |
| 영향 범위 | PC01, FS01, DC01 | 3개 서버를 동일 사고 범위로 조사 및 격리 검토 | PC01 실행/정찰, FS01 원격 실행, DC01 DCSync 정황 |
| 영향 계정 | employee1, svc_file, admin_user, Administrator | 계정 잠금, 비밀번호 초기화, Kerberos 티켓 무효화 | Kerberoasting, 원격 실행, 관리자 로그온, DCSync 로그 |
| 데이터 유출 | 유출 의심, 추가 확인 필요 | 외부 IP 차단 및 업로드 파일 내용 확인 | hashes.txt, share_data.zip 외부 업로드 comment |

## 7.2. 근본 원인

• 확인된 원인: 일반 계정 기반 서비스 티켓 요청, 서비스 계정 기반 FS01 원격 실행, DC01 관리자 계정 로그온 및 DCSync 의심 접근이 연속적으로 발생했다.

• 추정 가능한 원인: employee1 또는 svc_file 계정의 자격 증명 탈취, 서비스 계정 권한 과다, 관리자 계정 보호 미흡, 외부 업로드 통제 미흡 가능성이 있다.

• 추가 확인 필요: 최초 침투 경로, SecurityUpdate.exe 원본/해시, 업로드 파일 내용, 10.0.1.194의 소유 주체, 실제 DCSync 성공 여부, 의심 서비스 파일 확보 여부.

## 7.3. 개선 권고 사항

| 구분 | 번호 | 권고 사항 | 우선순위 | 목표 및 기대 효과 | 담당 / 기한 |
|---|---|---|---|---|---|
| 침해 복원력 | 1 | PC01, FS01, DC01 즉시 격리 및 메모리/디스크 증거 보존 | 즉시 | 추가 확산 방지 및 포렌식 증거 보존 | 보안 운영팀 / 즉시 |
| | 2 | employee1, svc_file, admin_user, Administrator 비밀번호 변경 및 세션/티켓 무효화 | 즉시 | 탈취 계정 재사용 차단 | AD 운영팀 / 즉시 |
| | 3 | 10.0.1.194 및 54.180.55.229:8081 관련 통신 차단 및 이력 조사 | 즉시 | 외부 유출 및 C2 가능성 차단 | 네트워크 운영팀 / 즉시 |
| 탐지 개선 | 4 | Kerberoasting, DCSync, Golden Ticket, LSASS 접근 탐지 룰 상관분석 강화 | 단기 | 단일 경보가 아닌 공격 흐름 기반 탐지 | 보안 운영팀 / 1개월 |
| 재발 방지 | 5 | 서비스 계정 권한 최소화, SPN/암호 정책 점검 | 단기 | 서비스 계정 악용 위험 감소 | AD 운영팀 / 1~3개월 |
| | 6 | 관리자 계정 MFA 및 Tiered Administration 적용 | 중기 | DC01 관리자 권한 오남용 방지 | 보안전략팀 / 3개월 |

| 구분 | 번호 | 권고 사항 | 우선순위 | 목표 및 기대 효과 | 담당 / 기한 |
|---|---|---|---|---|---|
| 로그 개선 | 7 | PowerShell Script Block, WinRM, Sysmon, Kerberos 로그 보존 기간 및 필드 정합성 강화 | 단기 | 추가 분석 및 재발 탐지 능력 향상 | 보안 운영팀 / 1개월 |

# 8. 결론

## 8.1. 종합 결론

제공된 로그와 Timesketch 분석 결과를 종합하면, 본 사고는 단순 경보가 아니라 AD 환경에서 계정 기반 공격 흐름이 연속적으로 관찰된 침해 의심 사고로 판단된다. 핵심 근거는 employee1 계정의 의심 실행 및 Kerberoasting, svc_file 계정의 FS01 WinRM 원격 실행, LSASS 접근, 외부 HTTP 업로드, 10.0.1.194에서의 DC01 관리자 계정 로그온, DCSync 및 Golden Ticket 의심 활동이다. 특히 DC01에서 DCSync 및 Golden Ticket 정황이 확인되어 도메인 권한 침해 가능성이 높으므로 심각도는 '심각'으로 평가한다.

# 9. 부록

## 9.1. 첨부 자료 목록

- timesketch_alerts.csv : 전체 ELK alerts 로그 맥락 및 탐지 룰 분포 확인

- tag_attack.zip : Timesketch 공격 태그 이벤트 89 건 확인

- starred_comment.xlsx : 핵심 star/comment 이벤트 12 건 확인

- forensic_report_prompt_with_analysis_points.md : 보고서 산출 프롬프트 및 분석 포인트 기준

## 9.2. 수록  파일 목록

-

## 9.3. 용어 정의

- ELK : Elasticsearch, Logstash, Kibana 기반 로그 수집/검색/시각화 환경

- Timesketch : 시간순 이벤트 분석, 태깅, 코멘트 기반 포렌식 타임라인 분석 도구

- IOC : 탐지와 차단에 활용 가능한 침해지표

- MITRE ATT&CK : 공격자의 전술, 기법, 절차를 체계화한 지식 베이스

## 9.4. 참고 문헌

- SB-03 (Operation MyCompany Dominance) Campaign : https://spacebar-mitre-attack-campaigns.vercel.app/campaigns/SB-03/