

신뢰를 조정하는 공격자

# 중앙 관리 소프트웨어를 통한 공급망 공격 분석

#Supply Chain, #Zero Trust, #Attack Chaining, #SBOM

이글루코퍼레이션 보안분석팀, 김미희



# Contents.

- I. 중앙 관리형 SW를 이용한 공격사례 분석
- II. 중앙 관리형 SW를 이용한 사이버 공격의 대응전략

신뢰를 조정하는 공격자 : 중앙 관리 소프트웨어를 통한 공급망 공격 분석

# I . 중앙 관리형 SW를 이용한 공격사례 분석

## 중앙 관리 소프트웨어

*Centralized Management Software*

장치, 시스템, 네트워크, 사용자 등 다양한 자산에 대해  
설정, 모니터링, 제어, 배포, 보안 정책 적용을  
중앙 관리 콘솔을 통해 수행할 수 있도록 지원하는 소프트웨어







중앙 집중형 제어(Centralized Control), Client-Server(Agent-Manager)  
자동화된 배포 및 갱신, 정책기반 관리  
권한분리 및 접근제어 제공

중앙 관리 소프트웨어에서 발생하는 보안사고를 대응하기 어려운 이유는  
상당수의 상용 솔루션은 Agent-Manger구조이기 때문에 다양한 기술 스택이 존재  
**SPoF, 과도한 권한 집중, 이상탐지 및 취약점 한계로 사고 인지 및 분석 지연 발생**

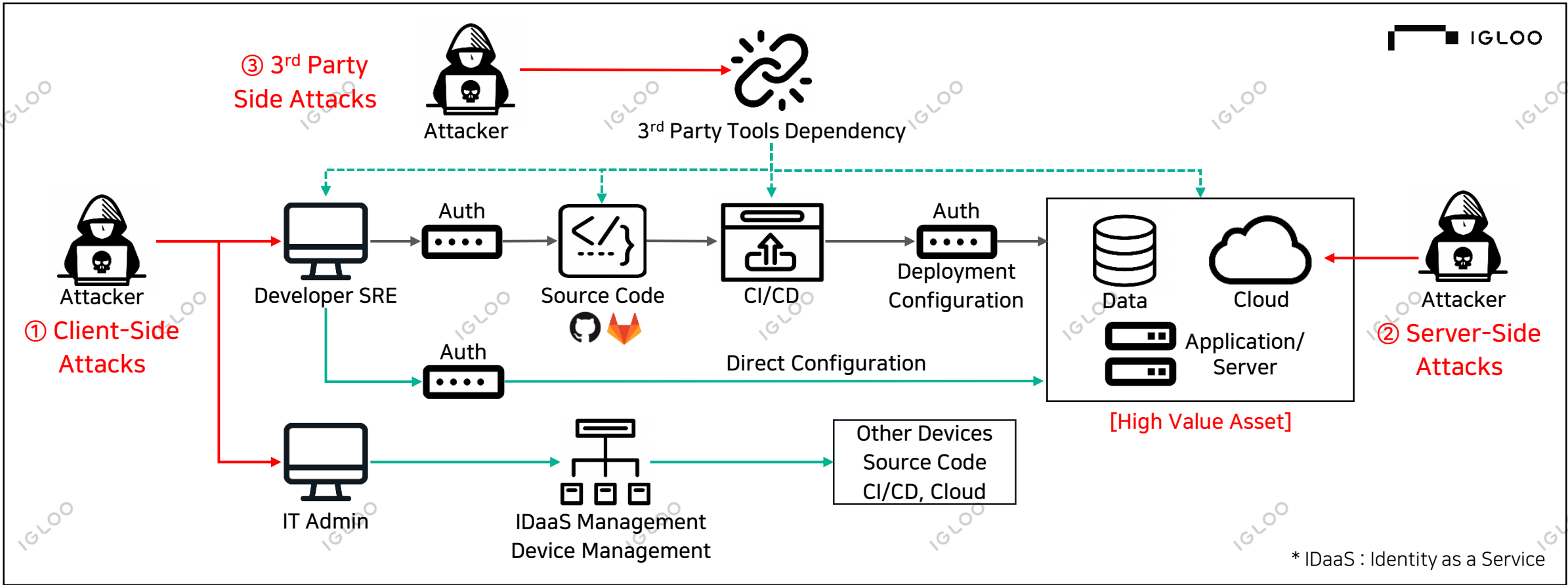
분류	설명	주요 소프트웨어 및 솔루션 설명
1. 시스템 관리	OS, 소프트웨어 배포, 패치, 전력/성능 설정 등 전반적인 IT 인프라 운영 관리	<ul style="list-style-type: none"> <li>Microsoft SCCM / MECM : Windows 시스템 업데이트, 앱 배포, 인벤토리 관리</li> <li>Red Hat Satellite : RHEL 서버 패치 및 설정 자동화</li> <li>Ansible Tower : 인프라 구성 및 상태 자동화</li> <li>PDQ Deploy/Inventory : 중소기업 환경에서 Windows 소프트웨어 배포</li> </ul>
2. 네트워크 관리	네트워크 장비 상태 모니터링, 구성 변경, 트래픽 분석	<ul style="list-style-type: none"> <li>SolarWinds Network Performance Monitor : SNMP 기반 네트워크 성능 모니터링</li> <li>PRTG Network Monitor : 장비 상태/성능 시각화</li> <li>Cisco DNA Center : SDN 기반 장비 제어, 트래픽 최적화</li> <li>Nagios + Nconf : 오픈소스 네트워크 상태 모니터링</li> </ul>
3. 보안 관리 (Endpoint/Network)	엔드포인트 보안, EDR, 악성코드 방지, 방화벽 설정 등	<ul style="list-style-type: none"> <li>CrowdStrike Falcon : 클라우드 기반 EDR, 위협 탐지</li> <li>Trellix ePO (이전 McAfee) : 중앙에서 엔드포인트 보안 설정 통합 관리</li> <li>Microsoft Defender for Endpoint : Windows 10/11 디바이스 통합 보안</li> <li>Symantec Endpoint Security : 위협 탐지 및 정책 배포</li> </ul>
4. 자산 및 구성 관리 (ITAM/CM DB)	하드웨어 및 소프트웨어 인벤토리, 구성 관계 시각화	<ul style="list-style-type: none"> <li>ServiceNow CMDB : ITIL 기반 구성 관리</li> <li>Lansweeper : 자동 자산 탐지 및 라이선스 모니터링</li> <li>GLPI : 오픈소스 IT 자산 및 티켓팅 시스템</li> <li>ManageEngine AssetExplorer : 라이선스 감사, 자동 자산 스캔</li> </ul>

분류	설명	주요 소프트웨어 및 솔루션 설명
5. 정책 및 접근 통제 관리	사용자 인증, 접근 제어, MFA, 정책 일괄 적용	<ul style="list-style-type: none"> <li>Okta : SSO, MFA, 사용자 라이프사이클 관리</li> <li>Microsoft Entra ID (구 Azure AD) : 클라우드 ID 및 접근 정책</li> <li>Ping Identity : IAM + SSO 솔루션</li> <li>FreeIPA : 오픈소스 기반 인증 및 접근 제어 관리</li> </ul>
6. 로그 및 모니터링 관리 (SIEM)	로그 수집, 보안 이벤트 상관 분석, 알림	<ul style="list-style-type: none"> <li>SPiDER TM, SPiDER ExD, ELK Stack (Elasticsearch + Logstash + Kibana), IBM Qradar, Wazuh 등</li> </ul>
7. 취약점 및 패치 관리	시스템/앱의 취약점 스캔, 패치 배포 및 이력 관리	<ul style="list-style-type: none"> <li>Qualys VMDR : 클라우드 기반 자산 탐지 및 취약점 관리</li> <li>Tenable Nessus / Tenable.sc : 취약점 스캐닝 및 리포팅</li> <li>Ivanti Neurons Patch : Windows/Linux 시스템 패치 배포</li> <li>OpenVAS : 오픈소스 취약점 스캐너</li> </ul>
8. 원격 제어/지원 관리	IT 지원팀 원격 접속, 유지보수, 문제 해결	<ul style="list-style-type: none"> <li>TeamViewer / AnyDesk : 사용자 원격 지원</li> <li>BeyondTrust Remote Support : 보안 중심 원격 지원</li> <li>Chrome Remote Desktop, RemotePC</li> </ul>

최근 2년간(2023년-2025년) 국가 지원 위협 행위자(Threat Actor)로 인해 대규모 공급망 공격 증가  
RaaS와 같은 랜섬웨어 공격그룹까지 가세하면서 전세계적으로 SW공급망 공격 확산

Vendor	Date	Nation	Actor	Description
OT/NW Appliances	최근 5년간		Volt Typhoon	▪ AA24-038A에 따르면 Volt Typhoon(Dev-0391, UNC3236, Voltzite 등) PRC 지원을 받는 위협 행위자로 인해 Fortinet, Ivanti, Citrix, Cisco등 NW Appliance를 통해 접근 후 AD, NTDS.dit, LotL, FRP등으로 미국 중요 인프라 공격 수행
XZ Utils	2021 ~ 2024	-	Jia Tan (JiaT75)	▪ 2024.03.29 Linux의 데이터 압축 라이브러리인 XZ Utils 5.6.0과 5.6.1에서 SW공급망 공격으로 백도어 악성코드가 포함되는 CVE-2024-3094취약점으로 인해 공격자가 SSH인증을 우회해 운영체제에 대한 RCE공격 가능
Cyber-Link	2023.11		Lazarus, APT38	▪ 대만 멀티미디어 소프트웨어 CyberLink(Diamond Sleet)에서 탈취한 인증서로 인증한 다운로더 악성코드가 주입된 CyberLink 설치 프로그램(LambLoad) 배포하여 일본, 대만, 캐나다, 미국 등 국가에서 100개 이상의 장치에 영향
Okta	2023.10	-	-	▪ 3rd Party Identity Attack으로 1Password, BeyoundTrust, Cloudflare등 고객사 정보 탈취
JetBrains	2023.09 ~ 10		Cozy Bear, APT29	▪ SolarWinds 해커가 JetBrains TeamCity 서버의 RCE 취약점 악용(CVE 2023-42793)
Jump Cloud	2023.06 ~ 07		UNC4899, APT43	▪ 북한 정찰총국(RGB)은 상용 VPN 공급자와 함께 L2TP Ipsec 터널과 ORB를 활용해 Source Address를 숨기고 ExpressVPN 외에도 NordVPN, TorGuard등 사용 ▪ 다운스트림 고객(SW솔루션 엔터티) JumpCloud 에이전트로 실행되는 악성Ruby식별(2023.06.27 15:51:57 UTC)
MOVEit	2023.05		ClOp	• Progress의 기업용 파일 전송 프로그램 MOVEit 취약점으로 5월부터 약 2,620개 조직과 7,720만 명 피해 발생 • CVE-2023-34362, CVE-2023-35036(공격자들은 2021.07과 2022.04 취약점 테스트 후 2023.05 취약점 사용) • 2023.06 CVE-2023-36934, CVE-2023-36932, CVE-2023-36933 등 추가 취약점 발견
3CX	2023.03		Lazarus, UNC4736	▪ 채팅, 화상·음성 통화 등 사용자 커뮤니케이션 제공 엔터프라이즈 소프트웨어인 3CX DesktopApp 공급망 공격 ▪ 3CX직원이 트레이딩 테크놀로지스(Trading Technologies)의 엑스트레이더(X_TRADER)다운로드 과정에서 악성코드에 감염되어 베일드시그널(VEILED SIGNAL) 백도어를 통해 3CX빌드서버 침투 후 정보탈취
Applied Materials	2023.02	-	-	▪ 공급망 공격으로 랜섬웨어 피해가 발생되어 2023년 1분기에만 2억 5천만 달러 손실

중앙 관리 소프트웨어를 통해 공급망 공격으로 확산할 수 있는 공격벡터로 악용  
**Centralized Control 구조로 인해 공격 파괴력 극대화 가능**



< Hiroki SUEZAWA, Dangerous attack paths: Modern Development Environment Security - Devices and CI/CD pipelines, Reconstructed by IGLOO >

CWE Top 25를 통해 CVE와 공격 트렌드를 분석하여  
중앙 관리 소프트웨어를 포함한 소프트웨어의 공격 벡터의 유추가 가능

NO	CWE	취약점명	YoY
1	CWE-787	Out-of-bounds Write	
2	CWE-79	Cross-site Scripting	
3	CWE-89	SQL Injection	
4	CWE-416	Use After Free	up 3
5	CWE-78	OS Command Injection	up 1
6	CWE-20	Improper Input Validation	down 2
7	CWE-125	Out-of-bounds Read	down 2
8	CWE-22	Path Traversal	
9	CWE-352	CSRF	
10	CWE-434	Unrestricted Upload of File with Dangerous Type	
11	CWE-862	Missing Authorization	up 5
12	CWE-476	NULL Pointer Dereference	down 1
13	CWE-287	Improper Authentication	up 1
14	CWE-190	Integer Overflow or Wraparound	down 1
15	CWE-502	Deserialization of Untrusted Data	down 3
16	CWE-77	Command Injection	up 1
17	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	up 2
18	CWE-798	Use of Hard-coded Credentials	down 3
19	CWE-918	SSRF	up 2
20	CWE-306	Missing Authentication for Critical Function	down 2
21	CWE-362	Race Condition	up 1
22	CWE-269	Improper Privilege Management	up 7
23	CWE-94	Code Injection	up 2
24	CWE-863	Incorrect Authorization	up 4
25	CWE-276	Incorrect Default Permissions	down 5

[ 2023 CWE Top 25 ]

NO	CWE	취약점명	YoY	비고
1	CWE-79	Cross-site Scripting	up 1	0
2	CWE-787	Out-of-bounds Write	down 1	0
3	CWE-89	SQL Injection		0
4	CWE-352	CSRF	up 5	0
5	CWE-22	Path Traversal	up 3	0
6	CWE-125	Out-of-bounds Read	up 1	0
7	CWE-78	OS Command Injection	down 2	0
8	CWE-416	Use After Free	down 4	0
9	CWE-862	Missing Authorization	up 2	0
10	CWE-434	Unrestricted Upload of File with Dangerous Type		0
11	CWE-94	Code Injection	up 12	0
12	CWE-20	Improper Input Validation	down 6	0
13	CWE-77	Command Injection	up 3	0
14	CWE-287	Improper Authentication	down 1	0
15	CWE-269	Improper Privilege Management	up 7	0
16	CWE-502	Deserialization of Untrusted Data	down 1	0
17	CWE-200	Exposure of Sensitive Information to an Unauthorized Actor	up 13	NEW
18	CWE-863	Incorrect Authorization	up 6	0
19	CWE-918	SSRF		0
20	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	down 3	0
21	CWE-476	NULL Pointer Dereference	down 9	0
22	CWE-798	Use of Hard-coded Credentials	down 4	0
23	CWE-190	Integer Overflow or Wraparound	down 9	0
24	CWE-400	Uncontrolled Resource Consumption	up 13	NEW
25	CWE-306	Missing Authentication for Critical Function	down 5	0

[ 2024 CWE Top 25 ]

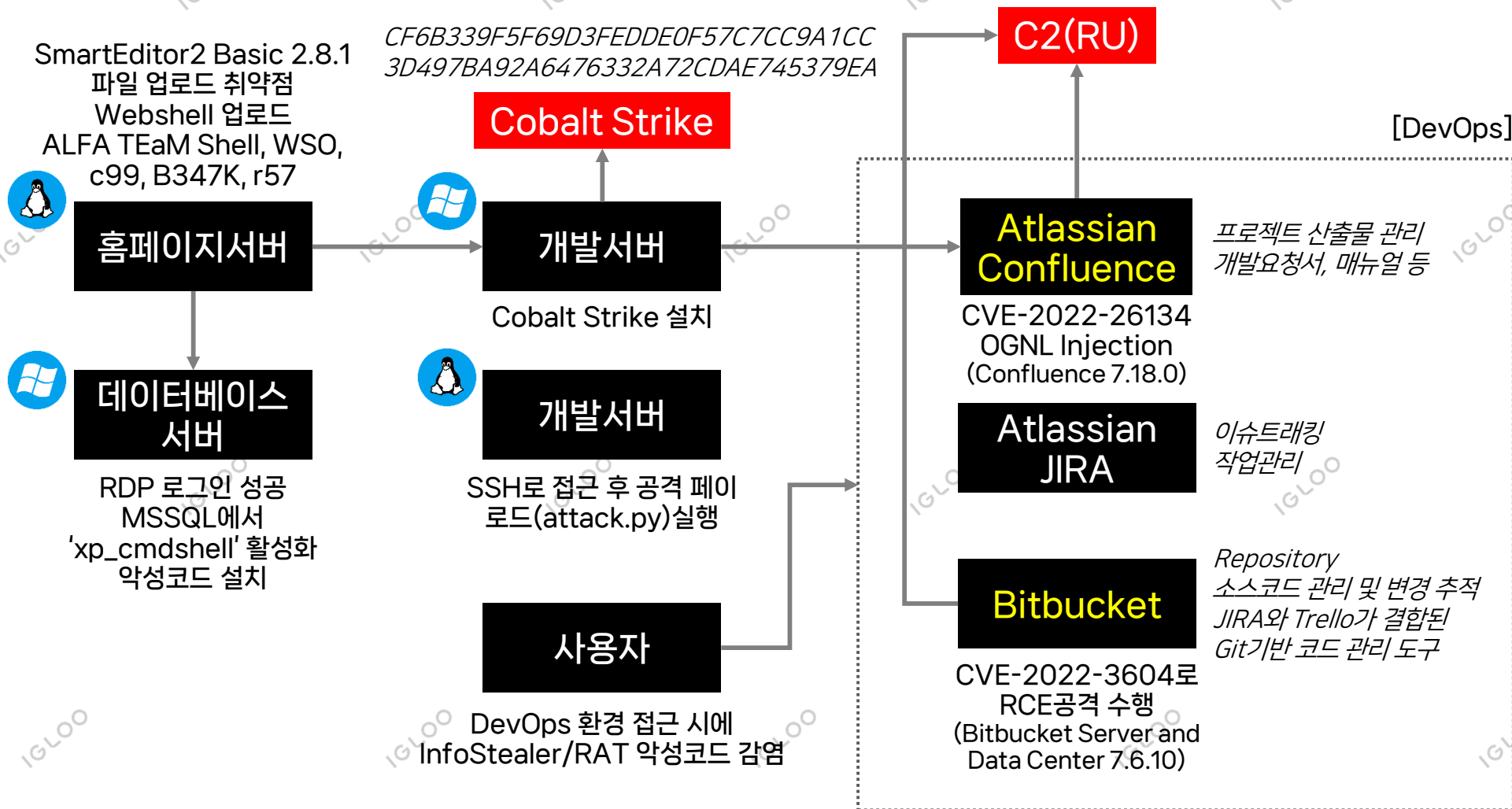
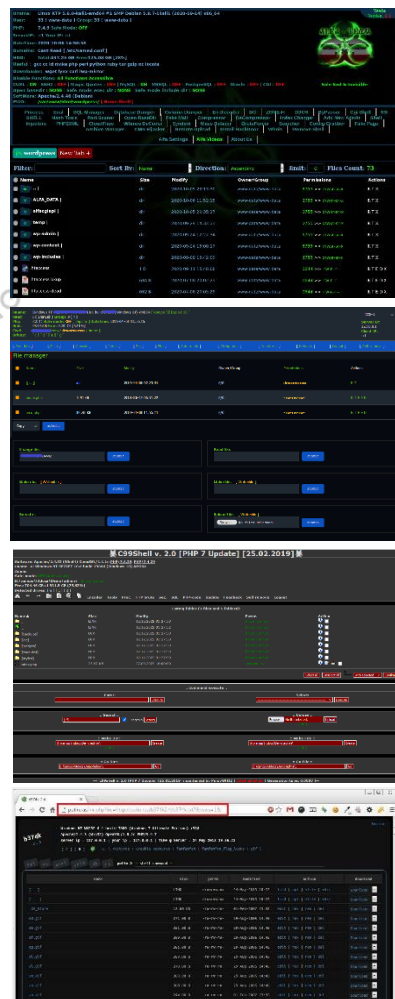


Code/Command/OS/SQL/XSS 등 입력값 검증 및 표현 취약점은 스테디셀러  
CWE-287, CWE-269, CWE-306 등 인증 우회 또는 권한 상승 → 관리자 권한 탈취로 귀결  
SSRF, Path Traversal, Unrestricted Upload 등 경로 우회 공격 증가  
KEV에 포함된 CWE-787, CWE-416, CWE-78 등 2023년 대비 3~5배 이상 증가됨에 따라  
실제 공격시도 및 위협 수준의 증가된 것을 알 수 있음

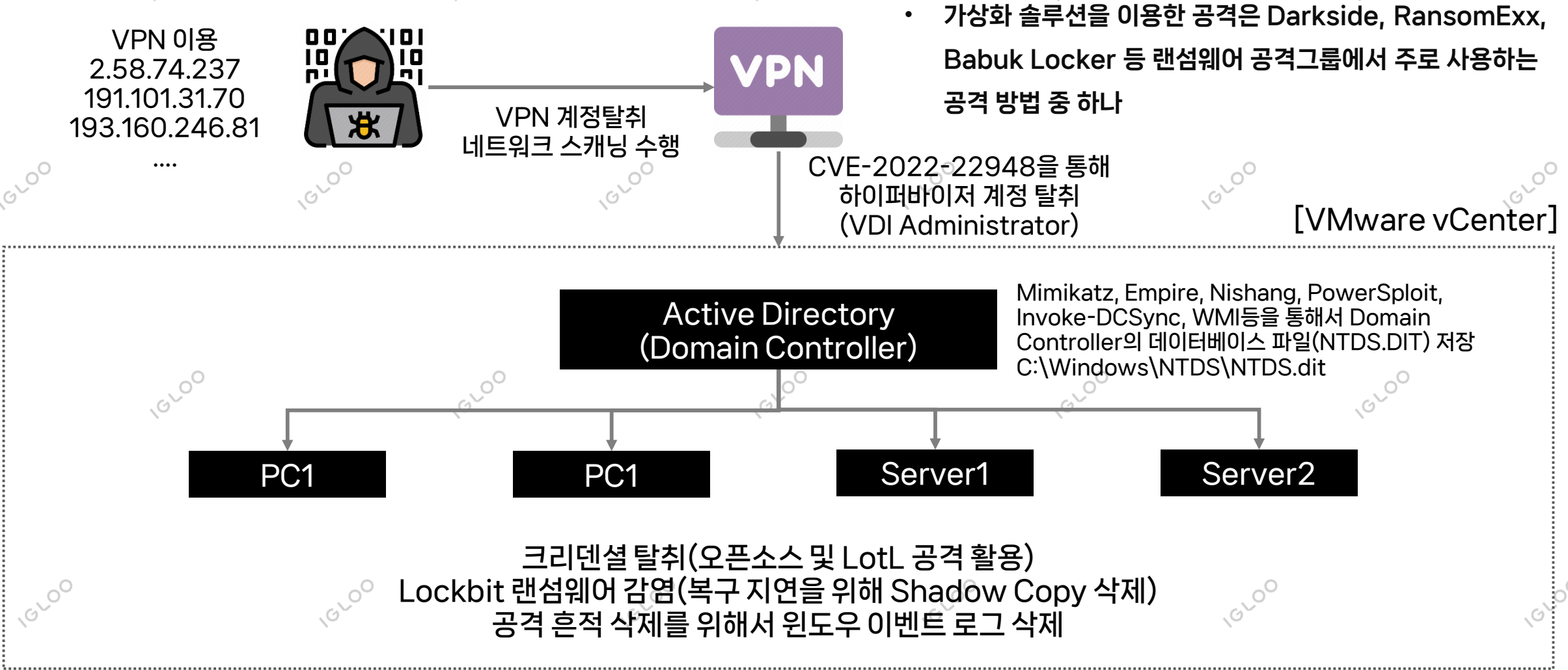
공격 유형	CWE	취약점 명	KEV CVE건수		증감 추세
			`23	`24	
입력 검증 및 표현 부재	CWE-79	Cross-site Scripting (XSS)	3	4	증가
	CWE-89	SQL Injection	4	6	증가
	CWE-78	OS Command Injection	5	23	크게 증가
	CWE-77	Command Injection	4	4	유지
	CWE-94	Code Injection	7	6	소폭 감소
	CWE-20	Improper Input Validation	1	35	급증
	CWE-22	Path Traversal	4	16	증가
웹 보안 미비 (Web UI/세션 관련)	CWE-502	Deserialization of Untrusted Data	5	14	증가
	CWE-352	Cross-Site Request Forgery (CSRF)	0	0	지속적 위험
인증 및 권한 관리 미흡	CWE-434	Unrestricted Upload of File with Dangerous Type	0	5	증가
	CWE-287	Improper Authentication	4	10	증가
	CWE-862	Missing Authorization	0	0	유지 (탐지 어려움)
	CWE-863	Incorrect Authorization	2	0	감소
	CWE-269	Improper Privilege Management	0	5	증가
	CWE-306	Missing Authentication for Critical Function	5	8	증가
	CWE-798	Use of Hard-coded Credentials	2	2	유지

공격 유형	CWE	취약점 명	KEV CVE건수		증감 추세
			`23	`24	
시스템 리소스 및 메모리 공격	CWE-787	Out-of-bounds Write	18	70	급증
	CWE-125	Out-of-bounds Read	3	2	감소
	CWE-416	Use After Free	5	44	급증
	CWE-476	NULL Pointer Dereference	0	0	유지
	CWE-119	Improper Restriction of Operations within Buffer	2	7	증가
	CWE-190	Integer Overflow/Wraparound	3	4	유지
	CWE-400	Uncontrolled Resource Consumption	0	-	-
	CWE-362	Race Condition	-	8	새로 부상
	CWE-918	Server-Side Request Forgery (SSRF)	2	16	증가
기타 보안 관련	CWE-276	Incorrect Default Permissions	-	0	유지
	CWE-200	Exposure of Sensitive Info to Unauthorized Actor	0	-	-

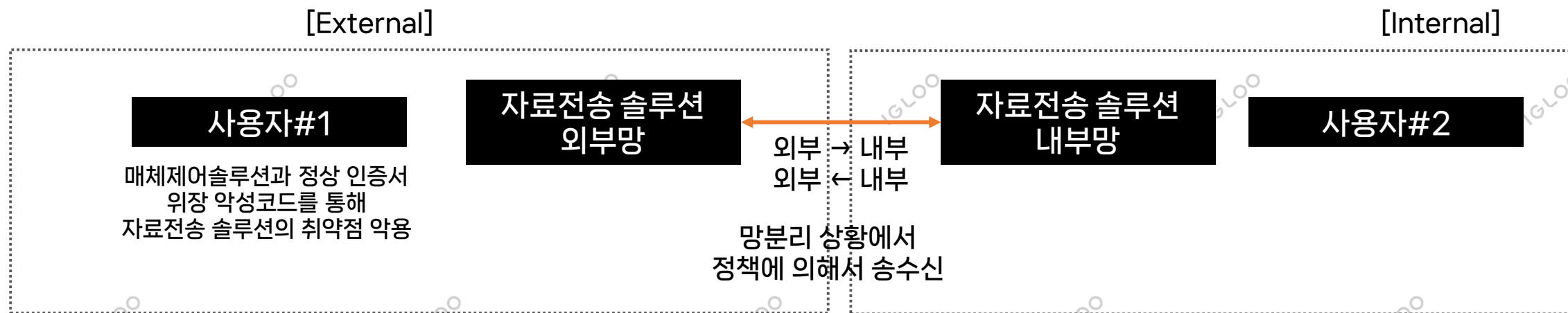
## 1. DevOps를 이용한 중앙 관리 소프트웨어 악용 사례



2. 가상화 솔루션을 이용한 중앙 관리 소프트웨어 악용 사례



### 3. 자료전송 솔루션을 이용한 중앙 관리 소프트웨어 악용 사례



File Name	Function	Command

3. 자료전송 솔루션을 이용한 중앙 관리 소프트웨어 악용 사례

- DPRK 국가 지원 공격 그룹인 Andariel(Onyx Sleet, Silent Chollima 등)은 파일 다운로드 및 실행 취약점이 있는 자료전송 솔루션을 이용해 C/C++또는 .NET으로 작성된 악성코드 유포
- 2023년 발견된 공격은 2017년 발견된 Lazarus(Hidden Cobra)의 Volgmer악성코드의 XOR키값과 동일하게 74615104773254458995125212023273를 사용

Description

This artifact is the service DLL embedded in the dropper malware's (1ECD83EE) resource named "MYRES" and during runtime it is decompressed and executed. This application has been identified as a fully functioning Remote Access Tool (RAT) designed to provide stealthy and persistent access to a compromised system.

To execute this DLL, it must be called from by its ServiceMain export. When called, the DLL will immediately attempt to unpack 1298 bytes of string data that is used during runtime. The algorithm displayed in Screenshot\_1 will be utilized to decode these strings. This algorithm, a simple XOR cipher, will also be utilized to decode and encoded traffic sent and received by this implant. The following hard-coded 16-byte key is utilized to decode the 1298 bytes of string data: 74615104773254458995125212023273 (hex encoded). Displayed below are the implant's decoded strings:

CVE	소프트웨어	취약점명
CVE-2023-42793	TeamCity	인증 우회 및 RCE
CVE-2023-3519	Citrix NetScaler	원격 코드 실행 (RCE)
CVE-2023-35078	Ivanti EPMM	인증 우회 및 RCE
CVE-2023-34362	MOVEit Transfer	SQL Injection 통한 RCE
CVE-2023-33246	RocketMQ	인증 우회 및 RCE
CVE-2023-32315	Openfire	인증 우회
CVE-2023-28771, CVE-2023-33010	Zyxel	RCE 및 명령 주입
CVE-2023-2868	Barracuda ESG	악성 이메일 통한 RCE
CVE-2023-27997	FortiGate SSL VPN	Pre-auth RCE
CVE-2023-0669	GoAnywhere MFT	명령 주입 취약점
CVE-2022-47966	ManageEngine	RCE (SAML 취약점)
CVE-2022-41352, CVE-2022-27925	Zimbra Collaboration Suite	RCE 및 인증 우회
CVE-2022-24990, CVE-2021-45837	TerraMaster NAS	명령 주입
CVE-2021-40684	Talend ESB Runtime	인증 우회
CVE-2021-3018	IPeakCMS	SQL 인젝션
CVE-2021-20038	SonicWall SMA100	Apache httpd기반 취약점
CVE-2021-20028	SonicWall SRA	인증 우회
CVE-2019-15637	Tableau	인증 우회
CVE-2019-0708	Microsoft RDP(BlueKeep)	원격 코드 실행
CVE-2017-4946	VMware V4H/V4PA	인증 우회

< CISA, MAR-10135536-D\_WHITE\_S508C / North Korea Cyber Group Conducts Global Espionage Campaign to Advance Regime's Military and Nuclear Programs, AA24-207A >

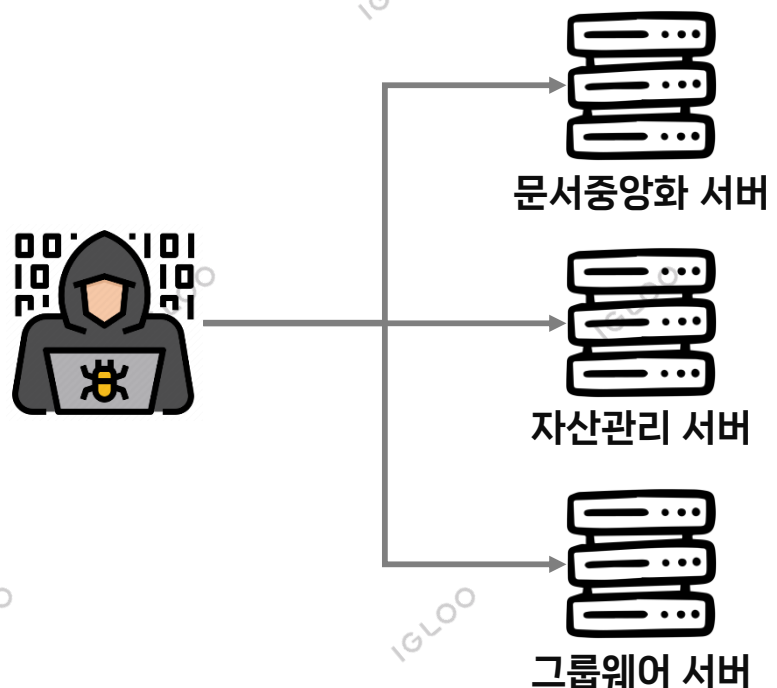
4. 자산관리/서버관리 솔루션을 통한 중앙 관리 소프트웨어 악용 사례

- Andariel에서 국내 자산관리 솔루션을 이용해 공격을 수행한 이후에는
- 1) Post-exploitation : AndarLoader, Andardoor, ModeLoader(Javascript 악성코드) 등
- 2) Remote Control : MeshAgent, MeshCentral

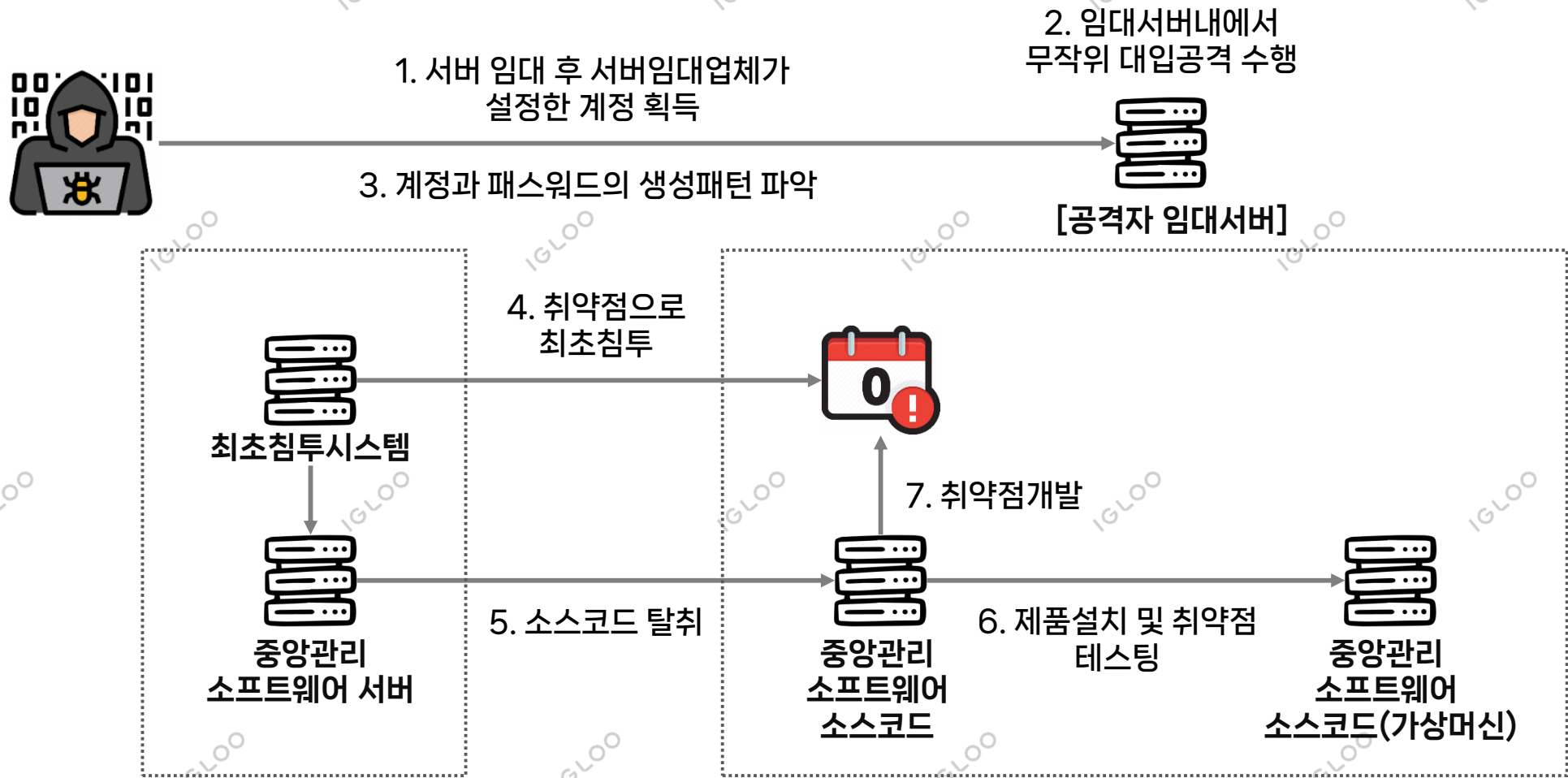
제품군	공개일자	취약점명
	2024.01.04	RCE로 악성코드 감염 등의 피해 유발
	2024.06.28	/blazeds/api/account/login 기능을 통해 사용자 인증 우회 서버 디렉토리 내 보안 취약파일 : /blazeds/jsp/api/imonMobile/*, /blazeds/jsp/imonMobile/*
	2024.08.28	임의 명령어 실행 및 임의파일생성 취약점
	2024.05.13	원격 코드 실행(RCE) 및 권한 상승(Local Privilege Escalation) 취약점

## 5. 문서중앙화 솔루션을 통한 중앙 관리 소프트웨어 악용 사례

- 북한발 위협행위자에 의해 `25.1 바이오의약업체(`25.3.4, NIS 공개) 문서 중앙화 솔루션(내부문서 통합관리 및 유통)을 침투 시도하여 연구자료유출을 시도하였으나 차단
- 해당 사건을 포함하여 `25.3.4 '국정원, S/W 공급망 관련 北해킹 확산 경고'를 통해 △IT용역업체 해킹을 통한 기관·기업 우회 침투 △IT솔루션·S/W 취약점을 악용한 침투 △보안관리 허점을 노린 해킹 등 3가지 공격유형을 활용해 자료 탈취로 인한 주의를 당부



6. 중앙 관리 소프트웨어 악용 사례



< TTPs #11: Operation An Octopus - 중앙 집중형 관리 솔루션을 노리는 공격전략 분석, KrCERT >



신뢰를 조정하는 공격자 : 중앙 관리 소프트웨어를 통한 공급망 공격 분석

## II. 중앙 관리형 SW를 이용한 사이버 공격의 대응전략

조직 규모와 IT구성에 따라 중앙 관리 소프트웨어 공격벡터의 차이가 발생  
오픈소스를 활용한 소프트웨어 개발이 증가하면서  
중앙 관리 소프트웨어를 이용한 공급망 공격 벡터로 악용되기 때문에 조직 규모에 따른 대응필요

항목	대기업	중소기업 및 기관	클라우드/Ops 기반 조직
주요 사용 도구	통합형 엔터프라이즈 플랫폼 (Microsoft Intune, ServiceNow, CrowdStrike 등)	모듈형 또는 오픈소스 관리 도구 (ManageEngine, Zabbix, phpMyAdmin 등)	클라우드 기반 네이티브 도구 (AWS Systems Manager, Okta, GitHub Actions 등)
공격자 목표	전사 시스템 장악 및 공급망 전파	보안이 약한 거점 확보 후 확산	API, 토큰 탈취 통한 클라우드 리소스 통제
대표 공격 사례	SolarWinds Orion (2020) Ivanti EPMM, CVE-2025-4427/4428 MOVEit Transfer (2023)	Kaseya VSA (2021) 3CX DesktopApp (2023) ManageEngine 취약점 연쇄 악용(CVE-2022-47966)	CodeCov (2021) CircleCI (2023) GitHub Actions 악용 사례
공격 벡터 특징	AD SSO 통합 권한 탈취 자동 배포 기능 악용해 악성코드 전파 정상 이미지 위장해 탐지 어려움	인증 미흡 기본 설정 그대로 사용 웹 UI 취약점 XSS RCE 등 패치 지연 다양성으로 공격 지속 가능	CI CD 환경에서 자격증명 유출 IAM 정책 오용 IaC 컨테이너에 악성코드 삽입
탐지 및 대응의 한계	대규모 통합 구조로 로그 분석 복잡 정상 트래픽과 공격 트래픽 구분 어려움	로그 미수집 자동화 미흡 전문 인력 부족으로 대응 지연	로그 분산 서버리스 특성으로 포렌식 어려움 외부 SaaS 연동으로 추적 복잡
보안 권고	핵심 관리 플랫폼은 별도 보안망 구성 이상행위 탐지 시스템 연동 자동화 정책 최소 권한 적용	관리 도구 접근 제어 IP MFA 오픈소스 보안 검증 및 업데이트 체계화 감사 로그 필수 설정	IAM 정책 최소화 및 RBAC 적용 클라우드 보안 플랫폼 CSPM CWPP 도입 CI CD 보안 검토 주기화

중앙 관리형 소프트웨어는 공급망 공격의 가장 취약한 공격 벡터로  
중앙 통제 구조에 특화된 보안 아키텍처 설계와 Red Teaming 기반 대응 시나리오를 통해  
Trust Boundary 집중 점검이 필요

구분	상세 대응전략
공격 표면 최소화	<ul style="list-style-type: none"><li>• 중앙 관리 시스템은 별도 네트워크(관리망)에서만 운영하고, 외부 인터넷 또는 사용자망에서 직접 접근 불가하도록 설계(예: 내부 방화벽 + ZTNA 게이트웨이 이중 통제)</li><li>• API 서버 접근은 mTLS 기반 인증과 IP Allow List 적용, 그리고 Swagger UI 등의 공개 테스트 콘솔은 운영 환경에서 제거관리 UI/콘솔에 접근하는 모든 관리자 계정은 Just-in-Time 권한 요청 시스템을 통해 임시 부여되도록 구성(예: BeyondTrust, CyberArk 등의 PAM 연계)</li><li>• 오케스트레이션 또는 패치 배포 모듈은 개별 분리하여 마이크로서비스 구조로 설계하고, 배포 기능은 업무망에서 분리된 전용 노드에서만 허용</li><li>• 에이전트-서버 간 통신은 일방향(pull 방식) 구조로 제한하고, push 방식 또는 명령 송신은 요청 인증 토큰 및 TTL기반으로 제한</li></ul>
공격자 시점의 위협 시나리오 탐지 적용	<ul style="list-style-type: none"><li>• MITRE ATT&amp;CK TTP기반의 모니터링 강화 : T1021(Remote Services): 중앙서버에서 SSH/RDP 연결이 비정상적으로 증가할 경우, T1059(Command Execution): 중앙 관리 UI를 통해 script 실행이 빈번하게 발생</li></ul>
Security Orchestration & Behavioral Monitoring	<ul style="list-style-type: none"><li>• SOAR를 통해 비인가 접근 시 즉시 사용자 세션 종료 및 관리자 알림, 계정 비활성화 등을 Playbook 구성</li><li>• Auditd, TTY Recording, API Request Logging을 병행 적용하여 추적 강화</li></ul>

# THANK YOU