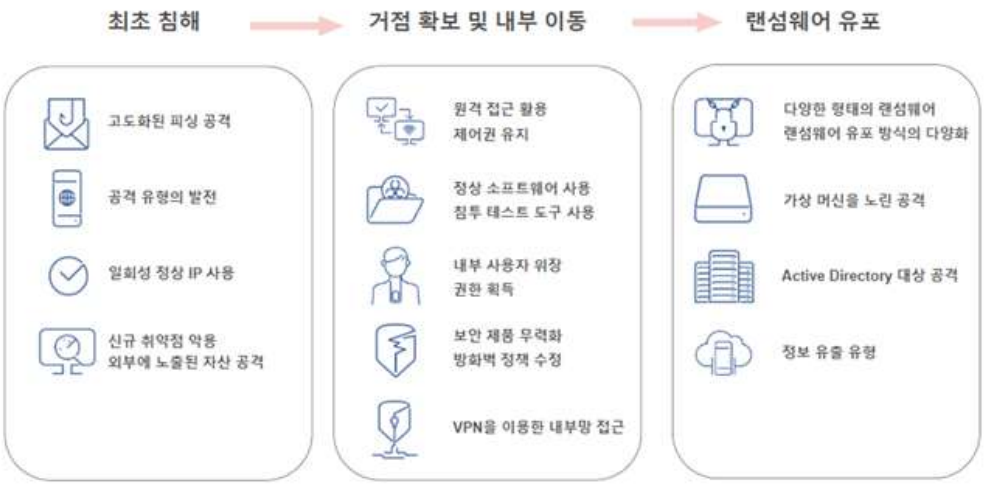
실제 사례로 보는 랜섬웨어 대응 방안

ASEC(AhnLab SEcurity intelligence Center)는 침해 사고 분석 후 AhnLab TIP(Threat Intelligence Platform)를 통해 침해사고 분석을 통해 얻은 인사이트를 포렌식 보고서로 제공하고 있다. 본 문서에서는 랜섬웨어 피해 확산을 줄이기 위해, 랜섬웨어 침해 사고들만 선별해 공격자들의 공격 기법과 랜섬웨어 침해 예방을 위한 점검 사항을 소개한다.

ASEC은 랜섬웨어 동향을 꾸준히 모니터링 하고 있으며, 매월 보고서를 발간하고 있다. AhnLab TIP 서비스 구독 시 보다 다양한 위협 분석 콘텐츠들을 확인할 수 있다.

랜섬웨어 침해 사례에서 확인된 공격 기법

그림 1]은 최초 침해부터 거점 확보 및 내부 이동과 랜섬웨어 유포까지 랜섬웨어 공격 흐름 별 주요 기법들을 구조화한 것이다.



[그림 1] 랜섬웨어 침해 공격 포인트와 공격 기법

다음 [표 1]은 최근 발생했던 랜섬웨어 침해 사례에서 공격자들이 활용한 공격 기법과 특징을 정리한 것이다.

상세 항목	공격에 활용된 사례

고도화된 피싱 공격	**더욱 정교해진 피싱 메일 콘텐츠** - 정상 사용자 사칭 - AI를 이용한 정교한 콘텐츠 제**작**
일회성 정상 IP 사용	**공격자로 특정하기 어려운 정상 IP 사용** - 해외 인터넷 서비스 업체(ISP) IP - 익명의 VPN IP - 클라우드 IP **공격에 활용된 IP는 재활용하지 않음**
VPN을 이용한 내부망 접근	**다중 인증(MFA)이 적용되지 않은 VPN 장비를 이용한 내부망 접근**
신규 취약점 악용	**0-Day, 1-Day 취약점을 적극적으로 활용** - 보안 패치가 되지 않은 취약한 자산을 식별해 공격 수행 **서비스 취약점을 이용한 시스템 접근** - MS Exchange Server 취약점을 이용한 시스템 접근 - Atlassian Confluence 취약점을 이용한 시스템 접근
외부에 노출된 자산 공격	**외부 노출된 원격 데스크탑 프로토콜(RDP) 포트로 'Brute Force' 공격** - 윈도우 관리자 계정(Administrator)
원격 접근 활용	**공격자들은 GUI 제어권 선호** - Reverse RDP - Google Chrome Desktop - Team Viewer
제어권 유지	**백도어 파일을 자동 실행에 등록** **원격 제어 프로그램(TeamViewer)** **터널링 도구(LCX, Plink)** **웹셸**
침투 테스트 도구 사용	**침투 테스트 도구를 공격 목적으로 사용** - BloodHoundAD - 코발트 스트라이크(Cobalt Strike) - AveMaria RAT을 이용한 시스템 제어
정상 소프트웨어 사용	**공격 시 정상 소프트웨어 악용** - NirSoft 프로그램 - Netscan - PsExec - Plink - Lcx - Team Viewer - MEGA Cloud - Rclone - ADfind - TreeSizeFree - ProcessHacker - dControl
AD 환경 대상	**액티브 디렉토리(AD) 인프라 정보 수집** - ADfind **AD 관리자 계정 정보가 있는 시스템 탐색** 메모리 내 AD 관리자 계정 정보 수집
권한 획득	**로컬/도메인 관리자 자격증명 수집** - 미미카츠(Mimikatz)를 이용한 메모리 내 자격증명 정보 탈취 - NirSoft의 유틸리티를 이용한 자격증명 정보 탈취 - 상용 키로거(refog)를 이용한 키로깅
보안 제품 무력화	**시스템에 설치된 보안 제품 식별 시도** **GUI 제어를 이용해 보안 제품 서비스 중지 및 삭제** - 설치된 백신 제품 삭제(uninstall) - dControl을 이용한 Windows Defender 비활성화
방화벽 정책 수정	**로컬 방화벽 정책 수정** - 특정 서비스 포트(445, 3389) 정책 허용
다양한 형태의 랜섬웨어	**랜섬웨어 실행 파일 유형의 다양화**

	- EXE, DLL, PS1, MSI 같은 파일 유형의 랜섬웨어
내부 사용자로 위장	**내부 사용자와 공격자를 구분하기 어려운 행위** - RDP - SSH - SMB - WMIC
가상 머신을 노린 공격	**일반 파일 대신 가상머신을 노린 랜섬웨어 공격 증가** - 가상디스크 파일(VMDK)을 노린 랜섬웨어 공격 - ESXi 서버를 노린 랜섬웨어 공격
랜섬웨어 유포 방식 다양화	**공유 드라이브로 거점 시스템에 연결해 다수 시스템 파일 일괄 암호화** - sshfs를 이용 리눅스(Linux) 시스템 볼륨을 윈도우(Windows) 시스템에 마운트해 랜섬웨어로 암호화 - net share를 이용해 다른 시스템의 볼륨 마운트 및 파일 암호화 **랜섬웨어 원격 명령 실행** - 공유 드라이브로 랜섬웨어 다운로드 및 실행 - wmic를 이용해 랜섬웨어 파일을 다운로드 및 실행 - bat 파일로 다수 시스템에 일괄 명령 전달 **AD 서버의 IIS 서비스를 이용한 랜섬웨어 유포** - IIS 서비스 활성화 및 웹 서비스를 이용한 랜섬웨어 유포 **AD 그룹 정책을 이용한 랜섬웨어 유포**
정보 수집	**데이터 유출을 위해 중요 데이터 정보 수집** - TreeSizeFree
정보 유출 유형	**외부 데이터 클라우드 서비스로 데이터 유출** - Mega **공격자 서버(C2)로 데이터 유출**

[표 1] 랜섬웨어 공격 기법 및 활용 사례

랜섬웨어 침해 사례에서 확인된 공격 기법

다음으로, 안랩의 디지털 포렌식 전문 조직 'A-FIRST(AhnLab Forensic Intelligence ReSearch Team)의 랜섬웨어 관련 침해사고 포렌식 분석 사례 중 의미 있는 사례들을 선별해 간단히 살펴본다.

마찬가지로, 각 사례에 대한 상세한 내용은 AhnLab TIP 구독 서비스를 통해 확인할 수 있다.

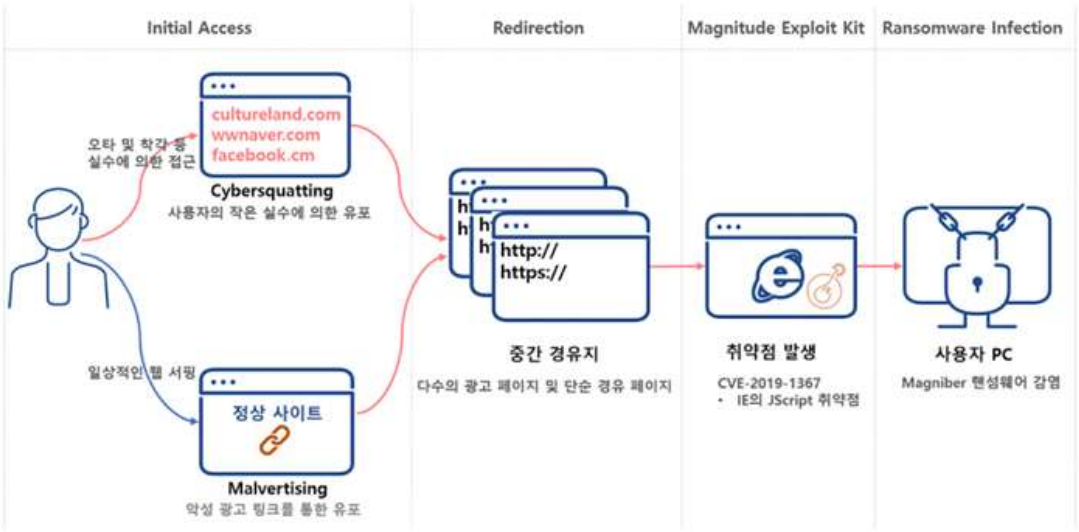
Case 1: 코발트 스트라이크를 이용한 AD 환경 공격 사례

지난 2019년, TA505 공격 그룹이 국세청 세금계산서를 사칭한 스피어 피싱 이메일을 대량 유포했다. 공격자는 윈도우 AD를 사용하는 기업을 대상으로 공격을 수행했으며, 코발트 스트라이크를 이용해 기업 내 시스템을 장악하고 도메인 관리자 권한을 확보했다. 다행히 랜섬웨어 유포까지는 진행되지 않았지만, 공격을 시도하는 과정을 확인할 수 있었던 사례다.

**참고: 코발트 스트라이크는 모의 침투 테스팅 도구지만 공격자들이 선호하는 공격 도구이기도 하다.*

Case 2: 사이버 스쿼팅 사이트 직접 접근에 의한 매그니베르 랜섬웨어 감염 사례

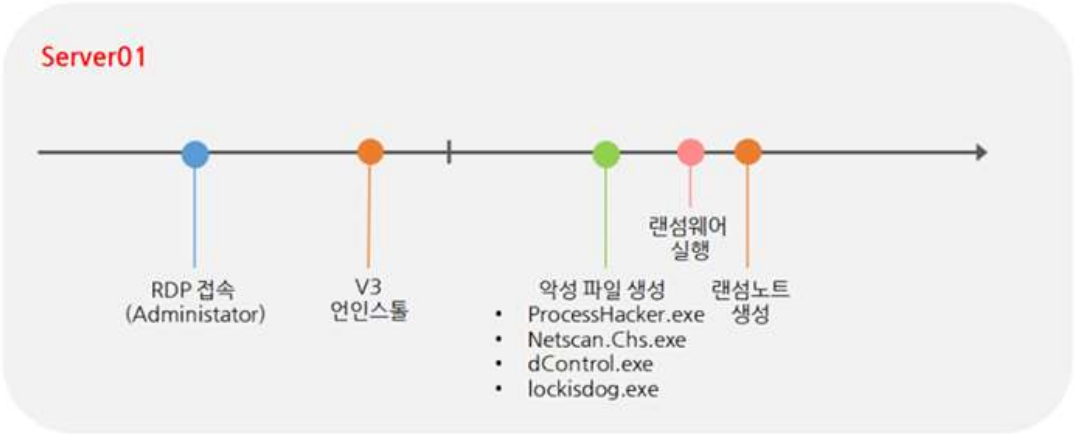
사이버 스쿼팅(Cyber Squatting)은 인터넷 도메인을 선점해두고 각종 이득을 취하는 행위를 뜻한다. 공격자는 오타가 빈번하게 발생하는 도메인명을 미리 선점하고, 피해자가 악성 페이지로 리디렉션(redirect) 되도록 준비한다. 사용자가 URL을 입력하는 과정에서 오타가 발생하게 되면 공격자의 악성 웹 사이트로 접속하게 된다.



[그림 2] 사이버 스쿼팅 사이트 접근에 의한 매그니베르 랜섬웨어 감염 과정

피해자는 몇 차례 리디렉션을 거친 후 인터넷 익스플로러(Internet Explorer)의 JScript 취약점을 통해 랜섬웨어에 감염된다. 일반적으로 불특정 다수를 노린 공격이지만, 특정 조직의 도메인과 유사한 도메인을 선점하는 방식으로 특정 조직을 대상으로도 공격이 가능함을 확인할 수 있었던 사례다.

Case 3: 기업 백신 관리 정책 미흡으로 인한 로키스 랜섬웨어 감염 사례



[그림 3] 로키스 랜섬웨어 감염 과정

공격자는 AD 관리자 권한을 확보한 뒤, RDP를 통해 내부 이동을 수행했다. GUI 권한을 가진 공격자는 피해 시스템에 설치된 백신 프로그램을 직접 삭제하고 로키스(Lockis) 랜섬웨어 파일을 실행했다. 공격에 사용된 랜섬웨어 파일은 백신이 탐지 가능한 악성 파일이므로, 백신 프로그램이 제거되지 않았다면 침해를 예방할 수 있었다. 백신 프로그램이 임의로 삭제되지 않도록 하는 관리 정책의 중요성을 알 수 있었던 사례다.

Case 4: 다크사이드 랜섬웨어 감염 사례 - 악성코드 감염 시 단순 치료에 그쳐서는 안되는 이유

공격자는 AD 관리자 권한을 획득한 뒤 도메인 컨트롤(DC) 서버에서 AD 그룹 정책을 이용해 다크사이드(Darkside) 랜섬웨어를 배포했다. 이는 지난 2~3년 동안 여러 공격자에 의해 침해 정황이 다수 확인된 사례로, 오랜 기간 내부 시스템이 취약한 상태로 노출되어 있었다. 보안 점검 등을 통해 침해 사실을 빠르게 인지했더라면 피해 규모를 줄일 수 있었던 사례다.

Case 5: Windows Defender를 무력화하는 하이브 랜섬웨어 감염 사례

공격자는 AD 관리자 권한을 획득 후, 공유 폴더를 이용해 DC 서버로 하이브(Hive) 랜섬웨어 유포를 시도했다. 하지만 Windows Defender에 의해 랜섬웨어 파일이 탐지되자, RDP로 직접 접속하여 Windows Defender를 OFF한 후 랜섬웨어를 실행했다.

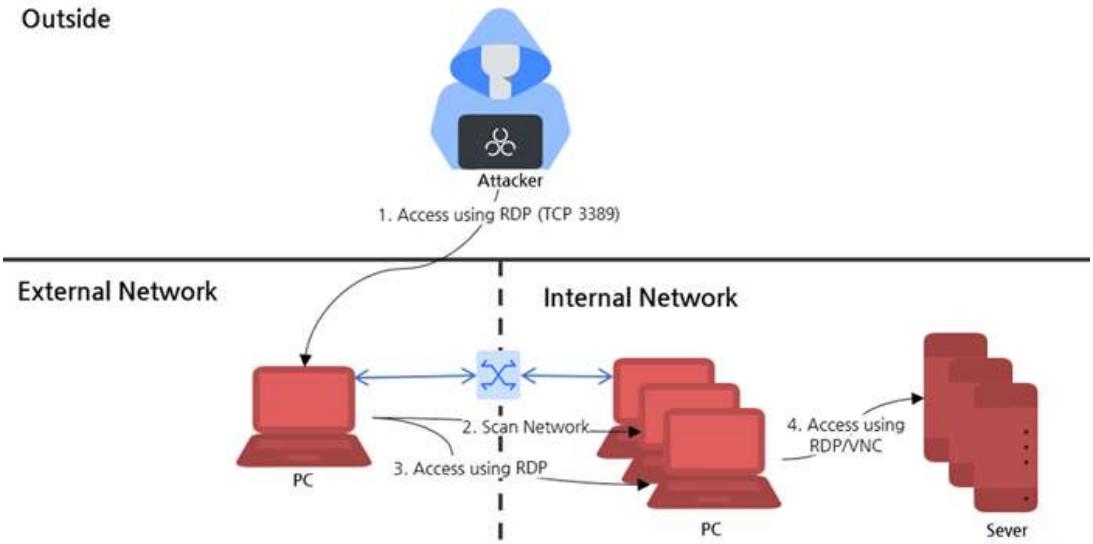
Case 6: 국내 기업을 타깃으로 공격한 귀신 랜섬웨어 감염 사례

공격자는 DMZ 존에 위치한 서버에 웹쉘(WebShell)을 삽입했다. 이후, AD 크리덴셜을 탈취하여 AD 서버로 접근했으며, AD 서버에 IIS 서버를 설치한 뒤 AD에 가입된 시스템에 랜섬웨어를 배포했다.

Case 7: RDP를 통해 침투한 후 ESXi 서버를 감염시킨 크라이시스 랜섬웨어 감염 사례

공격자는 Brute-Force 공격을 통해 기업 내 서버에 접근한 뒤, 윈도우 시스템에서 SSHFS(Secure SHell FileSystem)를 이용해 VMware ESXi 서버를 마운트한 후 크라이시스(Crysis) 랜섬웨어를 실행했다. 공격자는 암호화 대상으로, VMware의 가상 디스크 파일이 포함된 가상 디스크를 노렸다. 리눅스 서버들의 파일 시스템을 윈도우 시스템에 연결하고 윈도우용 랜섬웨어로 암호화 시킨 사례다.

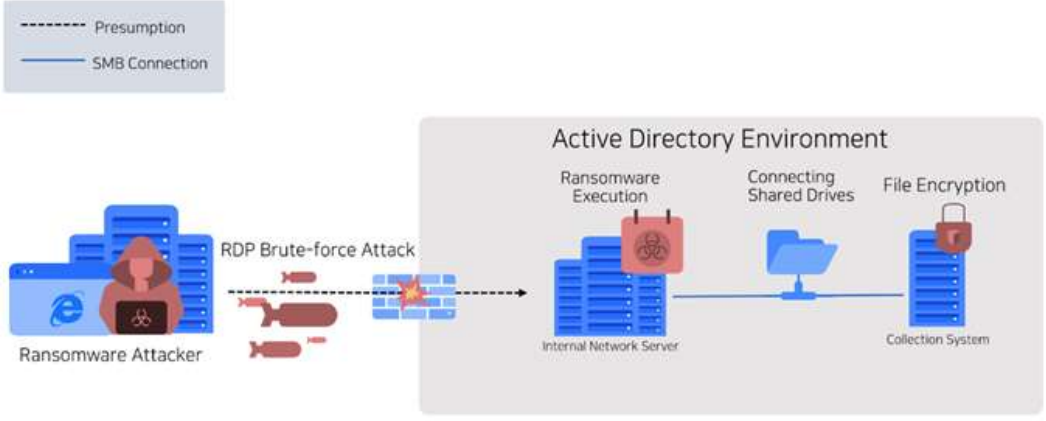
Case 8: RDP 노출과 쉬운 패스워드의 조합은 랜섬웨어를 부른다



[그림 4] 공격자의 내부 접근 흐름도

공격자는 외부 인터넷 환경에 RDP가 노출된 대상을 확인하고 Brute Force 공격으로 접근에 성공한 후, 내부 정찰을 통해 RDP로 내부망 시스템에 추가로 접근했다. 동일한 패스워드로 설정된 관리자 계정을 이용해 내부 주요 네트워크로 피해가 확산된 사례다.

Case 9: 공유 드라이브를 통한 랜섬웨어 감염 사례



[그림 5] 공유 드라이브를 통한 랜섬웨어 공격

공격자가 모든 시스템에 랜섬웨어를 배포하는 방식 대신, 소수 거점 시스템에서 다수의 시스템을 공유 드라이브로 연결해 랜섬웨어를 배포한 사례다.

Case 10: Atlassian Confluence 취약점을 악용한 1-Day 공격

공격자는 Atlassian Confluence 취약점(CVE-2023-22515, CVE-2023-22518)을 이용한 공격 시도하고, C3RB3R 랜섬웨어를 유포했다. 최근 Atlassian Confluence 제품에 대한 취약점이 연달아 공개되면서, Atlassian Confluence 취약점 패치가 적용되지 않거나, 최신 패치 관리에 미흡한 서버들을 대상으로 1-Day 공격이 수행된 사례다.

랜섬웨어 침해 예방을 위한 점검 항목

랜섬웨어 침해 관련 사례들에서 공격자들이 활용한 공격 기법을 분석하여 랜섬웨어 침해를 예방하기 위한 점검 항목을 선정했다. 해당 항목들을 점검해 공격자의 침투 난이도를 높여 침해 가능성을 낮추고, 공격 과정에서 탐지될 확률을 높여 침해가 발생하기 전에 차단할 수 있을 것으로 기대한다.

분류	점검 항목	세부 내용
정책 관리	관리자 계정 권한 관리	**불필요한 관리자 계정 삭제** **관리자 권한 계정은 최소한의 인원에게만 부여**
	패스워드 관리	**기본/공용 패스워드 사용 금지** **웹 브라우저 내 계정/패스워드 자동 입력 사용 금지** **패스워드 힌트에 패스워드 명시 금지** **AD 관리자 계정을 인증한 PC에서는 작업 후, 시스템 재시작** - 메모리 내 인증 정보 제거)
	외부에 노출된 영역 관리	**불필요한 노출 영역 제거 및 최소화** - 서비스 용도 외 외부 노출을 최소화 **접근 제한이 필요할 경우 최소 권한으로 설정** - 최소 권한으로 정해진 기간 내 허용 - 주기적인 접근 제한 목록 관리가 필요
	공유 드라이브 설정 관리	**기본 공유 비활성화**
	원격 데스크톱 설정 관리	**원격 데스크톱 서비스 비활성화** **원격 관리가 필요한 서버 자산은 별도 관리, 접근 가능 시스템 제한**
	방화벽 정책 관리	**공격 활용 가능한 프로토콜 통신 비활성화하는 방향으로 정책 관리** - RPC(135), SMB(445), RDP(3389) 등

		통신이 필요한 경우에 한해서만 별도 허용 및 네트워크 모니터링 **내부 서버 간 접근 제어 정책 설정** **-** 서버 간 통신이 필요한 경우 필요한 서비스에 한해서만 허용
자산 관리	EoS 자산 관리	**서비스 지원 종료된 운영체제, 애플리케이션, 서비스 업데이트 권고** **업데이트가 불가피할 경우 별도 모니터링 필요**
	취약점 모니터링 및 관리	**보안 권고 및 신규 취약점 모니터링 실시** **신규 취약점 공개 시 취약 자산 식별 및 조치** **-** 패치 관리 솔루션(PMS) 도입 **기존 취약점도 취약 자산이 새로 발생하는지 모니터링 방안 마련**
보안 제품	VPN 제품 설정	**외부에서 내부망 접근 시 사용되는 VPN 제품 설정 점검** **-** MFA를 필수로 사용하도록 설정
	백신 제품 사용	**랜섬웨어 탐지** - 알려진 랜섬웨어 파일 탐지 - V3 '행위 기반 진단 사용' 정책 사용 시 볼륨 섀도우 카피가 삭제될 때 랜섬웨어 행위 차단 가능 - 디코이 파일 변조 시 랜섬웨어 행위 차단 가능
	제품 보호 기능 사용	**보안 제품 서비스 중지/삭제 보호 기능을 사용하도록 설정** **-** V3의 경우 '잠금 설정 사용' 기능을 통해 설정 변경 차단, 프로그램 삭제 방지 기능 제공
	보안 사각지대 최소화	**망/Zone 내부에서 발생하는 행위 모니터링 방안 필요** **-** 망/Zone 외부, 내부 간 통신과 행위는 기존 보안 제품으로 대부분 모니터링 가능 - 하지만, 내부/내부간 통신 모니터링 사각지대 존재 **EDR/XDR 유형 보안 제품으로 보안 사각지대 최소화**
모니터링	원격 접근 이벤트 모니터링	**시스템 접근 모니터링 강화** **-** 관리 콘솔 외에서 발생하는 원격 접근 이벤트 모니터링 강화 **비정상 행위 모니터링 필요** **-** 관리자 시스템, AD 서버 등 네트워크 접근이 비교적 자유로운 시스템은 내부 거점으로 사용될 수 있음
	Outbound 트래픽	**Outbound 트래픽 모니터링 필요** **-** Reverse Shell 또는 포트 포워딩 탐지
	Windows Defender 이벤트 모니터링	**Windows Defender 활성화 이벤트 모니터링** **-** 백신 무력화 시도 탐지 - 윈도우 환경에서 백신 제품 설치 시 Windows Defender 비활성화 - 이후 백신 제품이 종료되거나 제거될 경우 Windows Defender 다시 활성화됨

재해복구	데이터 백업 방안	**데이터 백업/복구 전략 수립** - 서비스 유형에 따라 데일리 백업, 패치 버전에 따른 데이터 백업 등 서비스 복구 전략을 설정 **가상 디스크/하이퍼바이저 자산 보호** - 해당 자산을 노린 공격에 대비한 백업 수준과 침해 시 복구 전략을 설정
	서비스 복구 방안	**재해복구(DR) 방안 마련** - 랜섬웨어로 침해 발생 시 서비스 대체
모의 훈련	보안 인식 제고 캠페인	**사용자 대상 공격으로 침해가 시작되는 경우 다수** - 피싱 메일 모의 훈련 - 보안 인식 교육 진행
	사고 대응 모의 훈련	**침해 발생 시 빠른 대응을 위한 훈련을 진행 및 절차 검토** - APT 사고 대응 모의 훈련 - 재해복구 모의 훈련

[표 2] 랜섬웨어 침해 예방을 위한 점검 항목

랜섬웨어 침해 원인 분석을 위한 점검 항목

마지막으로, 랜섬웨어 침해 발생 시 침해 원인 분석을 위해 점검해야 할 항목들을 선정했다. 랜섬웨어 침해 발생 후, 원인 분석 없이 복구가 진행되면 동일한 원인으로 인해 랜섬웨어에 재감염될 수 있다.

따라서 랜섬웨어 침해 발생 시 원인 분석을 통해 시스템 내 잔존하는 악성 파일을 식별하고 침해 과정 및 원인 분석을 통해 재발을 방지하고 시스템 복구를 위한 준비가 필요하다

점검 항목	세부 내용
피해 시스템 보존 절차 점검	**네트워크 절체 및 시스템 전원 유지 상태로 격리 가능 여부 점검** - 전원을 끄면, 라이브 시스템에서 획득 가능한 정보가 유실되기 때문에 가급적 전원을 유지한 채 격리
보안 장비 로그 저장 기간 확인	**보안 장비 로그는 최소 6개월 이상 보관** - 최초 침해부터 랜섬웨어 침해까지 수 시간, 수 개월, 심지어 수 년이 걸리는 경우도 있음. - 사후 분석을 위해 가능한 장기간의 로그 보관 **VPN 사용 시 VPN 사용 로그로 실제 사용자 식별 가능 여부 점검** - 사용자 식별 불가 시, VPN IP 할당 방식을 사용자 별 정적 할당 방식으로 고려
사고 발생 시 보안 장비 로그 수집	**침해 인지 시점 기준으로 수집 가능한 보안 장비 로그 수집** - 보안 장비 로그 저장 기간이 짧을 경우, 침해 인지 시점에 수집 가능한 정보를 미리 수집.

[표 3] 랜섬웨어 침해 원인 분석을 위한 점검 항목

보다 다양한 랜섬웨어 분석 정보와 위협 인텔리전스 콘텐츠는 자사 위협 인텔리전스 플랫폼 'AhnLab TIP' 구독 서비스를 통해 확인할 수 있다.

►TIP 포털 바로가기

AhnLab

A-FIRST팀 이권왕 선임연구원