NHN Cloud
랜섬웨어 대응 가이드

NHN Cloud Ransomware Response Guide

NHN CLOUD

NHN Cloud 랜섬웨어 대응 가이드

저작권

문서 이력

버전	일자	이력 사항
1.0 버전	2024. 6.	NHN Cloud 랜섬웨어 대응 가이드 1.0 버전 출시
1.1 버전	2024. 8.	신규 CI 적용

목차

1 개요

최근 몇 년간 랜섬웨어가 사이버 공격의 주요 형태로 떠오르며, 기업과 개인 모두에게 심각한 피해를 입히고 있습니다. 이 악성 소프트웨어는 사용자의 파일을 암호화하고 원본 파일에 대한 접근을 차단하여 피해자로 하여금 금전적 보상을 요구합니다. 이로 인해 전 세계적으로 기업, 정부 기관, 은행, 병원 및 개인 사용자들에게 심각한 위협을 미치고 있으며, 그 피해는 재무적인 손실뿐만 아니라 신뢰와 안전까지 훼손시킬 수 있습니다. 이러한 배경 속에서 랜섬웨어로부터의 보호 및 대응은 현대 조직의 사이버 보안 전략에서 절대적으로 중요한 부분입니다.

본 가이드는 랜섬웨어에 대비하여 조직이 취할 수 있는 효과적인 대응 전략과 방안을 제시합니다. 또한 보안 전문가와 IT 관리자뿐만 아니라 모든 조직 구성원이 이해할 수 있는 방식으로 작성되었으며, 랜섬웨어에 대한 이해를 높이고 방어 전략을 강화하는 데 도움이 될 것입니다.

클라우드 환경에서도 적용 가능한 이 가이드는 NHN Cloud에서 제공하는 서비스와 함께 랜섬웨어로부터의 보호를 강화하는 데 필수적인 지침을 제공합니다. 클라우드 사용자들은 이 가이드를 활용하여 조직의 데이터 및 애플리케이션을 효과적으로 보호하고, 클라우드 환경에서의 랜섬웨어 공격에 대비할 수 있습니다. 랜섬웨어의 위협에 대응하고, 조직의 안전과 안정성을 유지하는 데 도움이 되기를 바랍니다.

1.1 랜섬웨어의 정의

1.1.1 랜섬웨어의 개념

랜섬웨어(ransomware)는 사용자의 컴퓨터 시스템을 장악하거나 데이터(시스템 파일, 문서, 이미지, 동영상 등)를 암호화하여 사용을 불가능하게 만든 후, 정상적인 작동을 위해 암호 키 또는 해제 방법을 알려주는 대가로 금전을 요구하는 악성코드입니다.

즉 몸값을 의미하는 ransom과 software의 합성어로, 사용자의 동의 없이 시스템에 설치되어 무단으로 파일을 암호화하고 금전을 요구하는 형태의 악성 프로그램입니다.

최초의 랜섬웨어는 1989년 조셉 팝(Joseph Popp)이 제작해 플로피 디스크를 이용하여 전파된 'AIDS.trojan'으로 일명, 'AIDS 플로피 사건'으로 알려져 있습니다. 이 사건은 전 세계 약 2만 명을 대상으로 악성코드가 심어진 플로피 디스크를 배송하여 당시 사회적 관심사인 후천성면역결핍증후군(AIDS)과 관련한 AIDS/HIV 감염의 위험도를 확인할 수 있는 프로그램의 설치를 유도하고, 해당 프로그램을 설치하면 PC 내 모든 파일을 암호화하여 몸값을 요구하는 전략으로 현재 랜섬웨어와 동일한 방법을 사용하였습니다.

악성코드와 랜섬웨어는 유포와 감염 방식이 유사하지만, 랜섬웨어에 감염된 파일은 복구가 매우 어렵습니다. 더구나 암호화된 파일에 대한 복호화를 빌미로 가상화폐(비트코인 등)를 요구함으로써 추적이 어려워지는 특징이 있습니다.

표 1 악성코드와 랜섬웨어 비교

구분	일반 악성코드	랜섬웨어
유포	이메일, 웹사이트, 네트워크 취약점 등 유포 방식 동일	
감염	소프트웨어 취약점 또는 피해자의 실행으로 악성코드 감염 동일	
동작	정보 및 파일 유출, DDoS 공격 등	문서, MBR, 사진 등 데이터 암호화
대응	악성코드 유포지 및 명령조정지(C&C) 서버 주소 차단	악성코드 유포지 및 명령조정지(C&C) 서버 주소 차단 ※ 복호화된 키가 저장된 서버(도메인/IP)와 통신 경로는 미차단
치료	백신 등을 통해 악성코드 치료	백신 등을 통해 악성코드 치료 암호화된 파일은 복구가 어려움
피해	개인, 금융 정보 유출 및 이를 이용한 2차 공격으로 피해 발생	암호화된 파일에 대한 복호화를 빌미로 가상화폐(비트코인 등)로 금전 요구, 협박

※ C&C: 해커가 악성코드에 감염된 PC에 원격으로 접속하기 위한 서버, PC로 악성코드 감염 시 C&C에 연결되어 해커의 명령을 수행

1.1.2 랜섬웨어 공격 단계

시간이 흐름에 따라 랜섬웨어 공격은 단순한 금전 요구에서 벗어나 더욱 광범위하고 파괴적인 형태로 진화했습니다. 이에 따라 이중 갈취 전술이 등장했으며, 공격자들은 도난 당한 데이터를 공개하겠다는 위협으로 피해자에게 더 큰 금액을 요구하고 있습니다. 이러한 랜섬웨어 공격은 기업에 경제적으로나 평판적으로 심각한 영향을 미칠 수 있습니다.
랜섬웨어 공격은 다양한 단계로 이뤄지며, 이를 간략히 설명하자면 다음과 같습니다.

❶ 초기 접속

공격자는 피해자의 시스템에 침투하기 전에 대상을 탐색하고 취약점을 찾아내어 초기 액세스를 얻습니다. 이를 위해 다양한 방법을 사용하는데, 대부분의 공격은 피싱 이메일이나 악의적인 링크를 통해 사용자를 속여 악성 소프트웨어에 감염시키는 방식이 있습니다.

❷ 감염

초기 액세스를 확보한 후, 공격자는 다양한 멀웨어와 도구를 활용하여 시스템을 감염시키고 데이터를 탐색합니다. 또한 네트워크를 모니터링하여 가능한 많은 시스템을 손상시키려고 합니다.

❸ 준비

공격자는 C&C(C2, command-and-control) 서버를 설정하여 대상 시스템에 암호화 키를 전송하고, 추가적인 멀웨어를 설치하여 랜섬웨어 공격을 더욱 용이하게 만듭니다.

❹ 스캐닝 및 암호화

이 단계에서 공격자는 네트워크 내의 중요한 데이터를 찾기 위해 시스템을 탐색하고 액세스 권한을 높이기 위한 작업을 수행합니다. 또한 데이터를 C&C 서버로 유출하여 이중으로 갈취하는 전략을 사용하기도 합니다. 이후 공격자는 C&C 서버에서 전송된 키를 활용하여 데이터와 시스템을 암호화합니다.

❺ 랜섬 노트

공격자는 랜섬을 요구하며, 피해자는 파일을 복구할 것인지 랜섬을 지불할 것인지 어려운 결정을 내려야 합니다.
랜섬웨어 공격은 기업 네트워크를 점점 더 성공적으로 침해하는 추세에 있습니다. 이는 공격자가 표적화된 감시 방법과 초기 액세스 확보를 위한 회피 기술을 사용하기 때문입니다. 공격자가 액세스 권한을 얻으면 영향을 극대화하기 위해 네트워크 전체로 확산하여 키 입력을 기록하거나 파일과 데이터를 유출하는 등의 방법으로 추가 데이터를 확보할 수 있습니다. 이러한 과정이 완료되면 파일이나 시스템을 잠그고 몸값을 요구합니다.

그림 1 랜섬웨어 공격 단계

1.2 랜섬웨어의 유형

랜섬웨어는 다양한 목적과 형태를 가지고 있습니다. 주로 금전 요구가 목적이지만, 목표와 방식에 따라 다양한 유형이 존재합니다. 아래는 랜섬웨어가 각기 다른 방식으로 시스템을 감염시키고 데이터를 암호화하는 유형을 설명합니다.

1.2.1 동작 방식에 따른 유형

파일 암호화 랜섬웨어(encrypting ransomware)

가장 흔하게 발생하는 랜섬웨어의 유형으로 사용자의 데이터를 암호화하여 복호화 키 없이는 접근을 불가능하게 만듭니다. 이러한 종류의 랜섬웨어는 사용자에게 금전을 요구하는 메시지를 표시하고, 복호화를 위한 키 또는 방법에 대한 정보를 얻기 위해 금전을 요구합니다. 일반적인 예로는 CryptoLocker, Locky, WannaCry, TeslaCrypt 등이 있습니다.

마스터 부트 레코드 랜섬웨어(MBR ransomware)

MBR(master boot record, 마스터 부트 레코드) 랜섬웨어는 시스템에서 부팅 방식과 관련된 정보를 저장하는 마스터 부트 레코드를 감염시켜 부팅 프로세스를 제어하여 시스템 자체를 사용 불가능한 상태로 만들 수 있습니다.
사용자가 시스템을 부팅하면 랜섬웨어 메시지나 화면이 나타나며, 사용자의 시스템에 접근할 수 없게 만듭니다. 일반적인 예시로는 Petya, NotPetya 등이 있습니다.

화면 잠금형 랜섬웨어(screen lockers ransomware)

화면 잠금형 랜섬웨어는 사용자의 시스템이나 기기 화면을 잠금 처리하는 랜섬웨어의 형태로 주로 Windows나 모바일 기기에서 발견되며 사용자가 해당 기기에 접근할 때 비밀번호나 암호를 요구하여 데이터에 대한 접근을 차단하는 형태의 랜섬웨어입니다. 이러한 유형의 랜섬웨어는 파일을 암호화하지는 않지만, 기기의 잠금 해제를 원할 경우 금전을 지불해야 합니다. 일반적인 예로는 Winlocker, Android.Lockdroid.E, FBI Ransomware 등이 있습니다.

1.2.2 목적에 따른 유형

금전 요구를 목적으로 하는 랜섬웨어

파일 또는 시스템을 암호화하여 암호 해제를 대가로 금전을 요구하는 랜섬웨어입니다. 대부분의 파일 암호화 랜섬웨어와 마스터 부트 레코드 랜섬웨어가 이러한 유형에 속하며, 대표적인 예로는 CryptoLocker, WannaCry 등이 있습니다.

시스템 마비를 목적으로 하는 랜섬웨어

사용자에게 금전을 요구하기 보다는 파일을 암호화하고, 시스템의 핵심 부분을 손상시켜 데이터를 파괴하거나 시스템을 사용 불가능하게 만드는 랜섬웨어가 있습니다. NotPetya, Bad Rabbit 랜섬웨어 등이 이러한 유형의 대표적인 예입니다.

기업 및 기관을 대상으로 하는 랜섬웨어

일반적으로 '비즈니스 랜섬웨어' 또는 '기업용 랜섬웨어'로 알려진 이 유형은 고도화된 기술과 전략을 사용하여 대규모 기업이나 정부 기관과 같은 조직을 대상으로 합니다. 이러한 랜섬웨어는 대규모 데이터의 피해와 더 많은 금전을 요구할 가능성이 높기 때문에 주목을 받고 있습니다. 공격자는 기업이나 기관에 대한 사전 조사를 통해 획득한 정보를 활용하여 고급 기술과 전략을 사용하여 네트워크 및 보안 취약점을 우회하고 랜섬웨어에 대한 탐지와 대응을 어렵게 만듭니다. 예를 들어 2018년 8월에 발견된 Ryuk 랜섬웨어는 러시아의 위자드 스파이더(wizard spider) 조직에서 배포한 Hermes 랜섬웨어의 변종입니다. Ryuk 랜섬웨어는 APT(advanced persistent threat, 지능형 지속 공격) 기법을 이용하여 기업과 기관을 대상으로 공격했으며, 주로 TrickBot 감염을 통해 네트워크에 침입합니다. Maze, Ragnar Locker 등의 기업용 랜섬웨어도 이와 유사한 형태로 나타납니다.

데이터 유출 협박을 목적으로 하는 랜섬웨어

독스웨어(doxware)나 리크웨어(leakware) 랜섬웨어는 대상 시스템의 파일이나 데이터를 암호화하는 것뿐만 아니라, 사용자의 중요한 데이터를 확보해 공개하겠다고 위협하는 형태의 랜섬웨어입니다. 기록, 사진, 개인 정보 및 기타 중요 데이터 등을 포함할 수 있습니다. 이러한 유형의 랜섬웨어는 사용자의 프라이버시를 침해하고 중요한 정보를 노출시킴으로써 피해를 입힙니다.

가짜 소프트웨어 판매를 목적으로 하는 랜섬웨어

스케어웨어(scareware)는 '겁을 주다(scare)'라는 영어 단어에서 유래한 것으로 공포를 이용하여 피해자를 속여 대가를 지불하거나 특정 행동을 유도하는 랜섬웨어를 말합니다. 주로 컴퓨터가 악성 바이러스에 감염되었다고 알림을 전송하고 결제를 유도하는 가짜 백신 소프트웨어가 스케어웨어의 대표적인 예시입니다. 이러한 스케어웨어는 사용자의 불안감과 불안전한 상태를 이용하여 사기를 치며, 피해자를 속여 금전을 요구하거나 비합리적인 행동을 하도록 유도합니다.

서비스형 랜섬웨어(ransomware as a service, RaaS)

서비스형 랜섬웨어는 랜섬웨어 그룹이나 조직이 랜섬웨어를 개발하고 운영하면서 다른 공격자에게 판매하는 사이버 범죄 비즈니스 모델을 말합니다. 서비스형 랜섬웨어는 공격자에게 랜섬웨어 키트를 제공하고 월간 구독, 일회성 수수료, 제휴 및 수익 공유 등의 방식으로 수익을 얻습니다. 이러한 서비스형 랜섬웨어는 사이버 범죄 활동의 상업화와 전문화를 부추기며, 사이버 범죄 생태계의 확산을 증가시키는 요인 중 하나입니다.

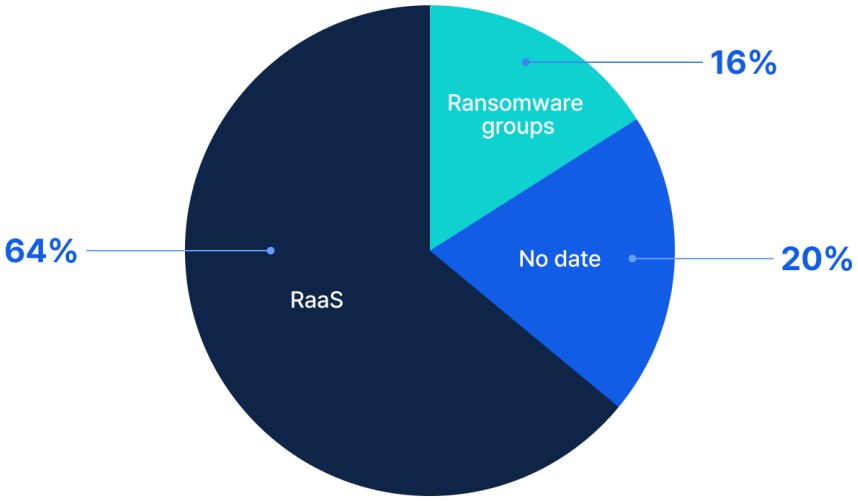

그림 2 2021년 전체 랜섬웨어 공격 중 서비스형 랜섬웨어 공격 비중[Group-IB]

[출처: 보안 뉴스]

1.3 랜섬웨어 피해

1.3.1 랜섬웨어 공격으로 인한 기업의 경제적 피해 및 기업 가치 손실

랜섬웨어 공격은 개인, 기업, 정부 기관 등 다양한 대상을 겨냥하며 막대한 경제적 피해를 초래합니다. 주로 비즈니스 손실, 공격자에게 지불한 금액, 보안 컨설팅 비용 등의 직접적인 비용 외에도 다른 손실 요소가 있습니다. 아래는 몇 가지 직접적인 금전적 손실 외에 나타나는 손실 요소입니다.

비즈니스 및 업무 중단

랜섬웨어 공격으로 인해 수일에서 수개월 동안 비즈니스 운영에 영향을 미칠 수 있습니다. 파일을 암호화하고 비즈니스 데이터를 손상시켜 직원들이 회사 계정에 로그인하지 못하거나 비즈니스를 위한 시스템과 네트워크를 사용할 수 없게 됩니다. 이로 인해 업무 중단이나 중요한 비즈니스를 위한 시스템과 데이터 사용이 불가능해져 기업에 큰 손해를 입힐 수 있습니다.

사이버 보험 및 복구 비용의 증가

많은 기업이 사이버 보안 공격에 대비하기 위해 보험을 활용하고 있습니다. 랜섬웨어로 인한 피해를 대비하여 보험을 가입하였지만, 피해로 인한 보험료가 상승하고, 보상 받는 보험금이 실제 피해보다 적을 수 있습니다. 뿐만 아니라, 보안 강화 및 피해 복구를 위해 보안 솔루션, 교육, 기타 복구를 위해 상당한 비용이 들어갑니다.

고객의 신뢰 상실과 회복

랜섬웨어 공격으로 인한 고객의 신뢰 하락은 심각한 문제로 여겨집니다. 서비스 이용이 불가능해지면서 영업 손실이 발생하고, 기업의 신뢰성과 안정성에 대한 의문이 생길 수 있습니다. 이로써 기존 고객과 잠재적 신규 고객뿐만 아니라 협력사나 투자자들까지도 영향을 받을 수 있습니다. 신뢰를 회복하기 위한 노력은 광고, 소셜 미디어 전략, 인터뷰 등의 마케팅 활동에 시간과 비용을 투입해야 하므로, 다른 생산적인 활동에 할애하는 시간과 비용이 줄어들 수 있습니다.

손해 배상 및 법적 조치

랜섬웨어 공격으로 인해 피해를 입은 고객에게 기업은 손해 배상을 해야 할 수 있습니다. 이는 직접적인 비즈니스 손실을 입은 고객뿐만 아니라 개인 정보 유출 등으로 인한 2차 피해에 대한 손해 배상도 고려해야 합니다. 뿐만 아니라, 산업군별 데이터 보호 및 사이버 보안 규정과 법적 요건을 확인하고 보완하는 것이 필요합니다.

1.3.2 주요 피해 랜섬웨어 종류

워너크립터(WannaCryptor) 랜섬웨어

워너크립터는 워너크라이(Wanna Cry) 또는 W크립트(Wcrypt) 등으로 알려진 랜섬웨어로 2017년 5월 12일부터 대규모 사이버 공격을 시작하여 미국, 영국, 스페인, 러시아 등을 시작으로 전 세계에 배포되었습니다.
Shadow Brokers 그룹이 2017년 4월에 NAS로부터 해킹하여 공개한 SMB(server message block) 취약점(MS17-010)인 이터널블루(EternalBlue)를 이용한 변형이 이 랜섬웨어의 제작에 사용되었습니다. 이 랜섬웨어는 은행, 헬스케어, 운송, 기업 등 다양한 부문에서 사용되는 Windows 운영체제를 실행하는 컴퓨터에 영향을 주었습니다.
Windows 운영체제의 취약점을 이용해 감염 후 컴퓨터 내의 파일을 암호화한 후 파일 복구 조건으로 비트코인 $300를 요구하는 메시지 창이 표시됩니다. 전 세계적으로 광범위하게 영향을 미치고 피해를 입힌 곳이 많았기 때문에 워너크립터는 랜섬웨어 공격 중에서도 특히 주목 받는 사례 중 하나입니다.

그림 3 워너크립터 랜섬웨어

Petya 랜섬웨어

2016년에 처음 발견된 Petya 랜섬웨어는 일반적인 파일 암호화와는 다르게 디스크 전체를 암호화하는 특징을 가지고 있습니다. 이 랜섬웨어는 주로 사용자의 이메일을 통해 감염되며, PDF나 SFX(SoundFX) 파일로 위장한 실행 파일이 첨부되어 있습니다. 사용자가 해당 파일을 다운로드하고 실행하면, 사용자 계정 컨트롤을 통해 블루스크린이 발생하고 강제로 재부팅이 이루어집니다. 재부팅 후에는 chkdsk 창이 나타나는데, 이는 디스크를 검사하는 것이 아니라 실제로는 디스크 전체를 암호화하는 과정입니다. 암호화가 완료된 후에는 번쩍이는 해골 화면과 Petya에 감염되었다는 랜섬 노트가 나타납니다.

Petya는 주로 Microsoft Windows 기반 시스템을 대상으로 MBR 영역을 변조하여 정상 부팅을 불가능하게 합니다. 이처럼 Petya 랜섬웨어는 디스크 전체를 암호화하는 특이한 특징과 감염된 시스템을 마비시키는 행위로 인해 악명을 떨친 랜섬웨어 중 하나입니다.

그림 4 Petya 랜섬 노트

NotPetya 랜섬웨어

2017년 6월에 발생한 대규모 사이버 공격에서 사용된 NotPetya는 Petya와 유사한 특징을 가졌지만, 몇 가지 중요한 차이점이 있어 카스퍼스키는 이 랜섬웨어를 'NotPetya'로 명명했습니다. Petya가 사용자의 악의적인 이메일 첨부 파일을 열어야만 감염이 시작되었다면, NotPetya는 사용자의 개입 없이도 빠르게 네트워크를 통해 확산할 수 있었으며, MFT(master file table)가 아닌 전체 하드 디스크 자체를 암호화하는 특징을 가지고 있었습니다.

NotPetya는 워너크라이 공격에서 사용된 것과 동일한 이터널블루 취약점(CVE-2017-0144)을 활용하여 네트워크 전파 기능을 추가했습니다. 이 공격은 악성 이메일에 노출이 없어도 전체 네트워크를 통해 빠르게 퍼져 나가며, 금전적 이익을 초월하여 기업과 국가 시설에 심각한 피해를 입히는 것으로 나타났습니다.

Ryuk 랜섬웨어

Ryuk 랜섬웨어는 2018년 8월에 발견된 랜섬웨어로, 주로 위자드 스파이더라는 조직에 의해 배포되며 Hermes 랜섬웨어의 변종으로 알려져 있습니다. 이 랜섬웨어는 APT 기법을 사용하여 정부 및 의료 기관을 대상으로 지능적이고 지속적인 공격을 수행한다는 점에서 심각한 사례입니다.

Ryuk 랜섬웨어는 파일을 암호화하기 위해 대칭 AES(256비트) 암호화와 비대칭 RSA(2,048비트 또는 4,096비트) 암호화를 함께 사용합니다. 대칭 키는 파일 내용을 암호화하는 데 사용되고, 비대칭 공개 키는 대칭 키를 암호화하는 데 사용합니다. 피해자가 랜섬머니를 지불하면 해당 비대칭 개인 키를 제공해 암호화된 파일을 해독할 수 있게 됩니다.

❶ CryptGenKey 함수를 사용하여 랜덤한 파일 암호 키 생성
❷ 생성한 키를 사용하여 AES-256-CBC로 파일 암호화
❸ 공격자의 공개 키를 사용하여 RSA-2048로 파일 암호화에 사용한 키 암호화

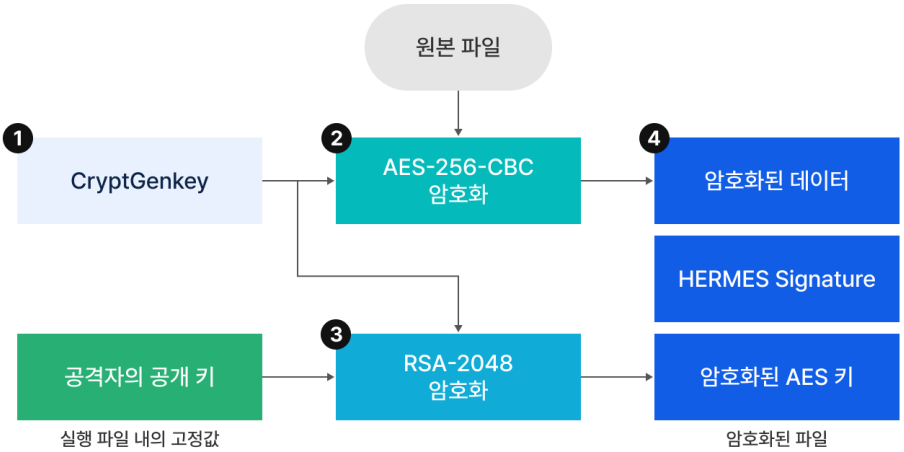

그림 5 파일 암호 키 생성 및 암호화 과정

Colonial Pipeline 랜섬웨어(DarkSide 랜섬웨어)

Colonial Pipeline 랜섬웨어 공격은 2021년 5월에 미국의 주요 연료 파이프라인 운영자인 Colonial Pipeline 컴퍼니에 DarkSide 랜섬웨어를 감염시켰습니다. 이 공격으로 미국 동부 지역의 연료 공급이 심각한 타격을 입었습니다. 미 연방 수사국(FBI)은 조사 결과 다크사이드(DarkSide) 그룹이 공격의 배후에 있었음을 확인하였습니다.

다크사이드 그룹은 동유럽 및 러시아 기반의 해킹 그룹으로 '서비스형 랜섬웨어' 형태로 활동하여 다양한 조직에 악성 소프트웨어를 제공하고 수익을 얻는 것을 목적으로 하였습니다.

Colonial Pipeline 사건은 고도로 조직적인 공격으로 국가의 중요 인프라에 대한 보안 필요성을 부각시켰습니다. 이 사건은 사이버 보안이 더 이상 기업 수준이 아닌 국가 차원에서 다루어져야 하는 문제임을 보여주었습니다. 특히 산업 현장과 사회 기반 시설에 대한 보안 강화가 시급하며, 긴급 대응 및 예방 계획의 수립이 반드시 이루어져야 함을 다시 한번 강조하고 있습니다.

1.3.3 랜섬웨어 피해 사례

피해 사례 1. 국내 제조 기업, 다크사이드 랜섬웨어 감염

2021년 1월 국내 제조업 분야의 유명 기업이 서비스형 랜섬웨어 유형의 다크사이드 랜섬웨어에 감염되어 내부의 다수 시스템이 피해를 입었습니다. 다크사이드는 이미 은퇴를 선언한 랜섬웨어 그룹이지만, 그들이 사용하던 다크사이드 랜섬웨어가 서비스형 랜섬웨어형태로 유통되어 공격에 악용된 사례입니다.

이전 스냅숏으로 복구된 웹 서버(web application server, WAS) WAS1과 WAS2 서버 분석 결과, 피해 기업의 경우 다크사이드 랜섬웨어와 웹 셸(webshell) 공격을 동시에 받은 것으로 알려졌습니다. 그러나 랜섬웨어 공격과 웹 셸 공격 간의 연관성은 확인되지 않아 다른 두 개의 그룹으로부터 공격을 받은 것으로 추정하고 있습니다.

피해 사례 2. 저작권 사칭 피싱 메일을 통한 록빗 랜섬웨어 유포

2022년 6월에는 저작권법 위반 내용으로 사칭한 피싱 메일을 통해 서비스형 랜섬웨어 유형의 록빗(LockBit) 랜섬웨어가 유포됐습니다. 해당 메일은 첨부된 파일명에 압축 파일의 비밀번호를 포함했습니다.

해당 랜섬웨어 공격을 분석한 결과, 첨부된 압축 파일을 풀면 PDF 파일 아이콘을 위장한 실행 파일이 존재한 것으로 드러났습니다. 해당 파일은 NSIS(nullsoft scriptable install system) 파일의 형태로 확인되었으며, 해당 스크립트 파일(.nsi) 내용을 보면 '162809383'의 데이터 파일을 디코딩하여 재귀 실행과 인젝션으로 악성 행위를 실행하게 됩니다.

해당 랜섬웨어는 복구를 막기 위해 볼륨 섀도 복사본을 삭제합니다. 또한, 랜섬웨어의 지속적인 실행을 위해 레지스트리 실행 키 등록과 LockBit_Ransomware.hta을 바탕화면에 드롭하여 배경화면 변경 및 재부팅 이후에도 유지될 수 있도록 레지스트리를 등록합니다. 그 이후 실행 중인 문서 파일 감염 행위 및 분석 회피를 위해 다수의 서비스와 프로세스를 종료합니다.

특정 서비스 및 프로세스 종료 후에는 암호화가 진행되며, 드라이브 타입이 DRIVE_REMOVABLE, DRIVE_FIXED, DRIVE_RAMDISK인 경우 암호화가 진행됩니다. 암호화된 파일은 .lockbit의 확장자와 특정 아이콘을 가지며, Restore-My-Files.txt 파일명의 랜섬 노트가 해당 폴더에 생성됩니다.

피해 사례 3. 이력서 형태로 위장해 열람 유도하는 록빗 2.0 랜섬웨어

서비스형 랜섬웨어 형태의 공격 사례로 이력서로 위장해 유포되는 록빗 2.0(LockBit 2.0) 랜섬웨어 공격 시도가 있었습니다. 2022년 11월 사례에서는 피싱 이메일에 첨부된 압축 파일명이 '사람이름.zip' 형태로 존재하고, 내부에는 추가적인 압축 파일이 존재했습니다. 추가 압축 파일 내부에서는 사진 파일을 위장한 록빗 2.0 랜섬웨어와 정상 엑셀 파일을 확인할 수 있었습니다. 유포되고 있는 랜섬웨어 파일명은 '(특수문자)이력서_221112(빠릿하게 일하는 모습 보여드리겠습니다).exe' 형태인 것을 확인하였습니다.

해당 공격의 경우 .exe 실행 파일 아이콘으로 표현된 V3 Zip 화면과 다르게 실제 폴더에는 사진 파일로 위장한 형태의 실행 파일이 존재합니다. 랜섬웨어가 실행되면 '(기존 파일명).lockbit'의 파일명으로 암호화가 수행되며, Restore-My-Fils.txt의 랜섬 노트와 함께 감염 화면을 띄웁니다.

록빗 2.0보다 업그레이드 버전인 록빗 3.0 랜섬웨어의 유포 방식도 동일합니다. 수집된 랜섬웨어는 '(특수문자)이력서_201116(경력사항도 같이 기재하였습니다 잘 부탁드립니다).exe'라는 파일명 형태로 유포됐습니다. 록빗 3.0 랜섬웨어는 한글 파일로 위장한 형태로 유포되고 있으며, 대량 유포를 위해 파일명 일부를 변경한 것으로 추정됩니다. 해당 랜섬웨어가 실행되면 '(기존 파일명).YQ85HpV1'의 파일명으로 암호화가 진행됩니다.

2 랜섬웨어 감염 기술

2.1 암호화 기술 개요

2.1.1 랜섬웨어가 사용하는 주요 암호화 방식

랜섬웨어는 파일이나 시스템에 액세스를 차단하고 데이터를 암호화하기 위해 다양한 암호화 기술을 활용합니다. 랜섬웨어 공격에 사용되는 암호화 기술은 다양한 방식으로 점점 고도화되고 있으며, 주로 대칭 키 암호화와 비대칭 키 암호화 방식을 활용합니다.
다음은 랜섬웨어가 주로 사용하는 암호화 방식에 대한 간략한 설명입니다.

대칭 암호화(symmetric encryption)

대칭 암호화는 연산 알고리즘이 단순하여 암호화 속도가 빠르며, 대용량 데이터에 효과적으로 작동합니다. 그러나 동일한 키를 암호화와 복호화에 사용하기 때문에 사용된 키가 노출되면 데이터를 복구할 수 있으므로 키 관리가 매우 중요합니다.

비대칭 암호화(asymmetric encryption)

비대칭 암호화는 공개 키와 개인 키 두 개의 키를 사용합니다. 공개 키로 데이터를 암호화하면 해당 데이터는 개인 키로만 복호화할 수 있습니다. 공개 키를 알고 있더라도 개인 키를 모르면 복호화가 불가능하기 때문에 여러 대상을 암호화할 경우 유용하지만, 대칭 키에 비해 연산 알고리즘이 복잡하여 암호화 속도가 느린 단점이 있습니다.

하이브리드 암호화(hybrid encryption)

랜섬웨어의 종류에 따라 다양한 암호화 방식이 사용되지만, 하이브리드 암호화는 대칭 암호화의 빠른 처리 속도와 효율성을 유지하면서도, 비대칭 암호화의 안전성을 활용하여 키 교환 및 보안 측면의 어려움을 극복합니다. 이 과정에서, 공격자는 대칭 암호화를 사용하여 빠르게 파일을 암호화하고, 이를 위해 사용한 대칭 키를 공개 키로 암호화하여 안전하게 전송합니다. 이로써 키 교환의 어려움을 해결하며, 공격자의 개인 키가 없는 한 데이터를 복호화하는 것이 불가능하게 됩니다.

표 2 암호화 방식 비교

구분	대칭 키(비밀 키) 암호화	비대칭 키(공개 키, 개인 키) 암호화
개념	• 암호 키(비밀 키)=복호 키(비밀 키) • 대칭 구조	• 암호 키(공개 키)와 복호 키(개인 키)가 다름 • 복호화 키만 비밀로 간직 • 비대칭 구조
특징	• 대용량 데이터 암호화에 유리	• 전자서명, 공인인증서 등 다양한 이용
알고리즘	• AES, DES, SEED, HIGHT, IDEA, RC5, ARIA	• Diff-Hellman, RSA, DSA, ECC, Rabin, ElGamal
키 개수	• 암호를 공유하는 사용자의 순서쌍 개수 • n(n-1)/2	• 사람당 2개씩(공개 키, 비밀 키) • 2n
키 교환	• 키 관리가 어려움	• 키 분배, 키 관리가 용이 • 키 변화 빈도가 적음

암호화/복호화 속도	• 빠름	• 느림
암호화할 수 있는 평문의 길이	• 제한 없음	• 제한 있음
기밀성	• 가능	• 가능
인증	• 부분적 가능	• 가능
무결성	• 부분적 가능	• 가능
부인 방지	• 불가능	• 가능

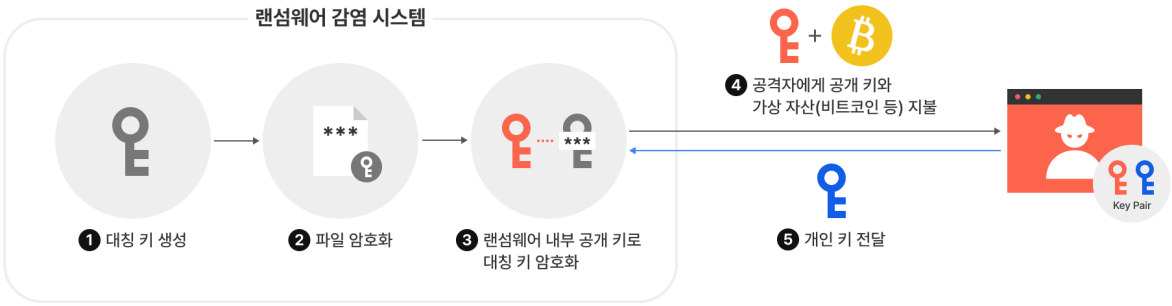

그림 6 랜섬웨어 파일 암호화 과정

❶ 감염 대상 시스템에 랜섬웨어가 실행되면 파일 암호화에 사용할 대칭 키(AES, RC4, Salsa20 등)를 생성합니다.

❷ 대칭 키는 파일 암호화에 사용합니다. 하나의 대칭 키로 PC의 모든 파일을 암호화시키기도 하지만, 최근에는 암호화시키는 각 파일마다 대칭 키를 새로 생성하는 방식도 사용됩니다. 이는 감염 PC 메모리에 남아있는 대칭 키를 확보하여 복구를 시도하는 것을 방지하기 위한 것으로 보입니다.

❸ 파일 암호화에 사용된 대칭 키는 랜섬웨어 내부에 존재하는 공개 키(RSA 등)로 암호화되어 파일 내부 또는 시스템 (레지스트리, 별개 파일 등)에 저장됩니다.

❹ 파일 암호화가 완료되면 랜섬 노트 등을 통해 가상 자산(비트코인 등)을 요구합니다. 랜섬 노트에는 보통 공개 키 정보나 감염 PC를 식별할 수 있는 정보가 포함되어 있으며, 공격자는 해당 정보도 함께 보낼 것을 요구합니다.

❺ 공격자는 공개 키와 한 쌍으로 된 개인 키를 보유하고 있으며, 비용 지불이 완료된 후 개인 키가 포함된 복구 프로그램을 제공합니다.

2.2 랜섬웨어 감염 주요 경로와 기술

랜섬웨어 공격의 주요 경로는 악성 이메일, 피싱 사이트, 악성 광고, 보안 설정이 미흡한 유 · 무선 네트워크, 소프트웨어 취약점 등을 통해 시스템에 침투합니다. 이러한 감염 경로를 파악하고 예방하기 위한 보안 조치를 마련하는 것이 매우 중요합니다. 또한, 감염이 발견되면 추가 확산을 막기 위해 신속하고 효과적인 대응이 필요합니다.

2.2.1 악성 이메일 및 첨부 파일

랜섬웨어 공격자들은 주로 악성 피싱 이메일을 통해 악성 파일이나 링크를 전파합니다. 이메일을 이용하여 공격자들은 불특정 다수 또는 특정한 대상에게 손쉽게 악성 첨부 파일이나 악성 링크를 전송할 수 있기 때문에 이 방법을 자주 사용합니다.
공격자들은 신뢰할 만한 기관, 회사, 또는 개인으로 위장해 긴급성 또는 흥미로운 주제를 사용하여 사람들의 호기심을 자극하고 악성 첨부 파일을 열거나 악성 링크를 클릭하게 유도하여 랜섬웨어에 감염되도록 합니다.

2.2.2 웹사이트 취약점을 통한 감염

사용자는 신뢰할 수 없는 웹사이트나 애플리케이션의 취약점을 악용하여 사용자의 동의나 명시적인 행동 없이 자동으로 악성 코드가 다운로드되고 실행되는 드라이브 바이 다운로드(drive by download) 공격에 의해 랜섬웨어에 감염될 수 있습니다. 즉 사용자가 보안에 취약한 웹사이트 또는 악성 웹사이트를 방문하는 것만으로도 사용자 시스템이 랜섬웨어에 감염될 수 있습니다.
그렇기 때문에 사용자는 신뢰할 수 없는 웹사이트는 방문하지 않고, 웹 브라우저 및 소프트웨어를 최신 상태로 유지하는 것이 중요합니다.

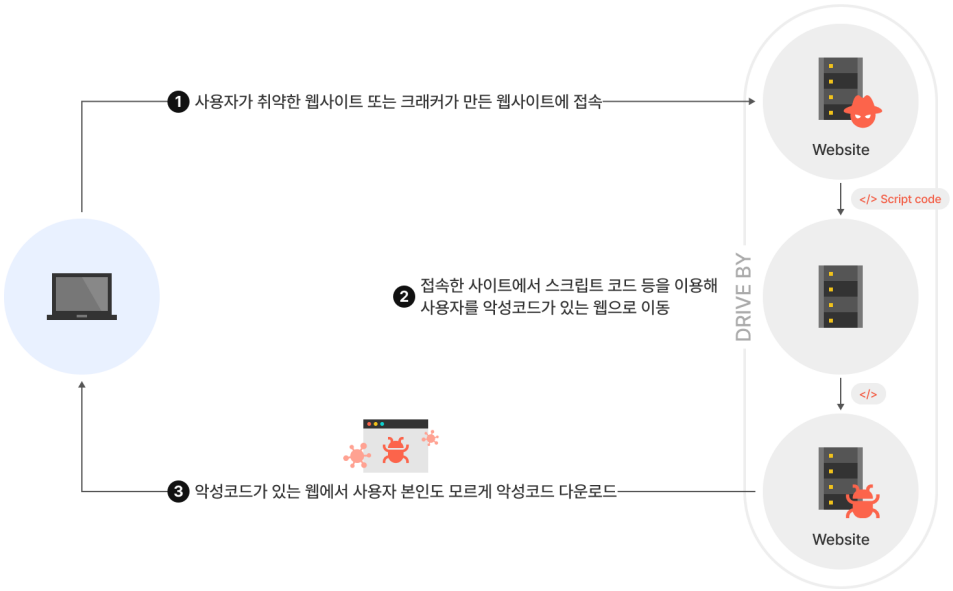

그림 7 드라이브 바이 다운로드 공격 방식

[출처: 한국인터넷진흥원(KISA)]

※ 드라이브 바이 다운로드: 취약한 웹사이트에 방문하였을 뿐인데 사용자 모르게 악성 스크립트가 동작하고 취약점을 유발시키는 코드를 실행하여 악성코드를 다운로드하고 실행하여 사용자의 PC를 감염시키는 기법입니다.

2.2.3 RDP를 통한 무차별 암호 대입 공격

RDP(remote desktop protocol, 리모트 데스크톱 프로토콜)는 원격으로 컴퓨터에 접속하기 위한 프로토콜이지만, 취약한 구성이나 사용자 인증 취약점을 이용하여 랜섬웨어 공격의 대상이 될 수 있습니다. 공격자는 주로 기본적으로 사용되는 RDP 포트(TCP 3389)를 스캔하여 취약한 시스템을 찾아냅니다. 그리고 대상이 확인되면 무차별 암호 대입을 통해 접근 권한을 획득하여 시스템을 완전히 제어한 후 파일을 전송하고 실행시키는 등의 방법으로 랜섬웨어를 배포하고 데이터를 암호화합니다.

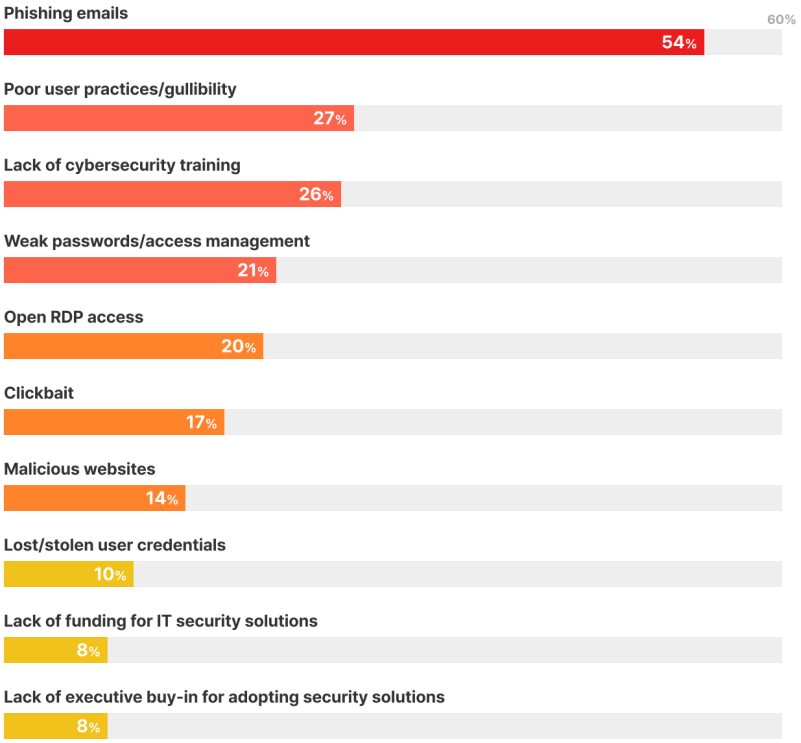

그림 8 랜섬웨어 공격의 주요 원인

[출처: Datto's Global State of the Channel Ransomware Report]

3 랜섬웨어 예방 및 탐지 방안

3.1 랜섬웨어 피해 예방 수칙

랜섬웨어는 악성 소프트웨어로, 컴퓨터나 파일을 암호화하여 사용자에게 금전적 보상을 요구합니다. 랜섬웨어 공격으로부터 피해를 최소화하고 예방하기 위해서는 몇 가지 중요한 예방 수칙을 준수하는 것이 필요합니다. 아래는 랜섬웨어 피해를 방지하기 위한 주요 권고 사항입니다.

모든 소프트웨어를 최신 버전으로 업데이트하여 사용합니다.

보안 업데이트가 제공되는 최신 버전의 운영체제를 사용하고 매달 또는 긴급 발표되는 보안 업데이트를 적용하도록 합니다. 또한 보안 지원이 중단된 운영체제는 최신 버전으로 교체해서 사용하는 것을 권장합니다.
그 외 인터넷 브라우저, Java, Adobe Acrobat Reader 등과 같은 소프트웨어를 항상 최신으로 유지하고 불필요한 소프트웨어는 삭제하는 것이 좋습니다.

백신 소프트웨어를 설치하고, 최신 버전으로 업데이트합니다.

신뢰할 수 있는 백신 소프트웨어를 사용하고 최신 업데이트를 유지하는 것이 중요합니다. 또한 실시간 감시 및 검사를 활성화하여 악성 파일을 항상 검사할 수 있도록 해야 합니다.

출처가 불명확한 이메일과 URL 링크는 실행하지 않습니다.

의심스러운 이메일이나 메시지를 통해 수신한 첨부 파일이나 링크는 송신자를 꼭 확인 후 실행합니다.
특히 매크로가 포함된 MS Office, 스크립트, 실행 파일 등은 각별한 주의를 기울여야 합니다.

신뢰할 수 없는 사이트 및 파일 공유 사이트 등에서의 파일 다운로드 및 실행에 주의합니다.

신뢰할 수 없는 사이트나 파일 공유 사이트는 악성파일을 위장한 파일을 유포하는 경우가 많아 가능한 신뢰 사이트를 통해 확인된 파일을 다운로드하는 것을 습관화해야 합니다.

중요 자료는 별도 매체에 정기적으로 백업합니다.

업무 및 중요 문서는 주기적으로 백업을 하고, 외부 저장 장치를 이용해 별도의 장소에 안전하게 보관하는 것이 좋습니다. 또한 PC 및 네트워크에서의 '공유 폴더' 사용을 주의해야 합니다. 하나의 PC가 랜섬웨어에 감염될 경우 공유 폴더를 통해 다른 PC로 확산될 수 있으므로 주의해야 합니다.

[출처: 랜섬웨어 피해 예방 5대 수칙(한국인터넷진흥원(KISA))]

3.2 랜섬웨어 예방 방안

3.2.1 보안 업데이트 및 패치

주기적인 업데이트와 패치의 중요성

보안 업데이트와 패치는 시스템의 보안을 강화하는 핵심적인 요소입니다. 랜섬웨어는 보안 취약점을 통해 시스템에 침투하기 때문에, 주기적으로 시스템과 소프트웨어를 최신 상태로 유지하는 것이 중요합니다. 이를 통해 최신 보안 조치를 적용하고 취약점을 최소화하여 공격을 방어할 수 있습니다.
또한 조직은 보안 업데이트 정책을 수립하여 모든 시스템이 정기적으로 업데이트되도록 해야 합니다. 자동 업데이트 기능을 활용하거나 PMS(patch management system, 패치 관리 시스템)를 이용하여 보안 업데이트를 우선적으로 진행하는 것이 좋습니다.

최신 보안 취약점에 대한 대응 전략

조직은 보안 취약점을 효과적으로 관리하고, 조기에 취약점을 감지하는 프로세스를 수립해야 합니다. 운영체제 및 소프트웨어의 취약점을 주기적으로 모니터링하고, 보안 업데이트 정보를 주기적으로 확인하여 최신 취약점에 대해 신속하게 대응해야 합니다.
업데이트를 배포하기 전에는 실제 업무 환경을 고려하여 테스트를 진행하여 문제가 발생하지 않도록 안정성을 확보하는 노력도 필요합니다.

3.2.2 클라우드(NHN Cloud) 환경 취약점 점검 및 위협 식별

랜섬웨어 감염을 효과적으로 예방하기 위해서는 클라우드 리소스를 정기적으로 점검하고 취약한 부분을 조치해야 합니다.
랜섬웨어의 여러 감염 경로 중 하나는 시스템이나 애플리케이션의 취약점을 악용하는 것입니다. 따라서 주기적으로 시스템 및 애플리케이션의 취약점을 점검하고 발견된 취약점을 제거함으로써 랜섬웨어의 공격 경로를 사전에 예방할 수 있습니다.
아래는 NHN Cloud에서 제공하는 클라우드 운영 자산 식별 및 취약점 점검 서비스입니다.

Resource Watcher

Resource Watcher는 조직 내 서비스에서 생성된 모든 리소스를 그룹 및 태그를 활용하여 생성, 변경, 삭제를 효율적으로 모니터링하고 관리할 수 있습니다.
또한, 알림 조건을 설정하여 리소스에서 발생하는 다양한 변경 사항을 신속하게 확인할 수 있습니다. 이를 통해 주요 자산을 식별하고 모니터링하여 랜섬웨어 감염을 예방하기 위한 체계적인 계획을 수립할 수 있습니다.

Security Advisor

Security Advisor는 NHN Cloud의 조직 및 프로젝트에 생성된 리소스의 보안 설정 상태를 점검하고 모범 사례와 이용 내역을 비교 분석하여 안전한 서비스를 이용할 수 있도록 권장 가이드를 제시하고 있습니다.
전체 또는 개별적으로 점검 항목을 선택할 수 있으며, 점검 주기는 일 또는 주 단위로 설정 가능합니다. 또한 등록된 이메일로 점검 결과를 발송할 수 있습니다. 이 서비스를 이용하여 주기적인 점검을 통해 클라우드 리소스의 보안성을 강화할 수 있습니다.

Server Security Check

NHN Cloud는 인스턴스의 운영체제에 대한 주요 보안 설정 값을 점검하여 시스템의 보안 수준을 최적화하고 잠재적인 취약점을 제거하여 취약점을 악용하는 랜섬웨어와 같은 위협으로부터 예방 할 수 있는 **Server Security Check**를 제공합니다.

이 서비스는 주요 정보통신 및 전자금융 기반 시설 보안 기준에 근거하여 NHN Cloud의 축적된 경험을 적용해 점검을 수행합니다.

App Security Check

App Security Check는 NHN Cloud의 실무 경험과 전문 기술을 기반으로 웹 및 모바일 애플리케이션의 보안 취약점을 점검하고 대응 방안을 제공하여 잠재적인 취약점을 사전에 조치할 수 있도록 합니다. 취약점을 식별하고 조치하는 과정을 통해 랜섬웨어 감염에 대비할 수 있습니다.

3.2.3 네트워크 아키텍처 보안 강화

랜섬웨어는 운영체제 및 애플리케이션의 취약점을 악용하여 네트워크를 통해 빠르게 전파되기도 합니다. 이를 방지하기 위해 허가되지 않은 트래픽 및 접근을 차단하고, 최소 권한의 원칙을 준수하며, 서비스 용도와 특성에 맞는 분리된 구성으로 네트워크 구성 보안을 강화하여 안전한 클라우드 환경을 구성해야 합니다.

네트워크 분리 구성

NHN Cloud의 VPC(virtual private cloud)는 터널링 기술을 기반으로 논리적으로 격리된 가상 네트워크 환경을 구축할 수 있습니다. 이를 통해 서비스, 개발, 테스트 등의 영역을 완전히 독립된 네트워크 영역으로 구성할 수 있으며, 필요에 따라 인터넷 접속이 가능한 영역과 인터넷 접근이 차단된 프라이빗한 영역으로 설정하여 높은 수준의 보안과 격리된 네트워크를 구성할 수 있습니다. 더 나아가 추가 리전을 활용하여 DR(disaster recovery, 재해 복구)을 구성할 수 있습니다.

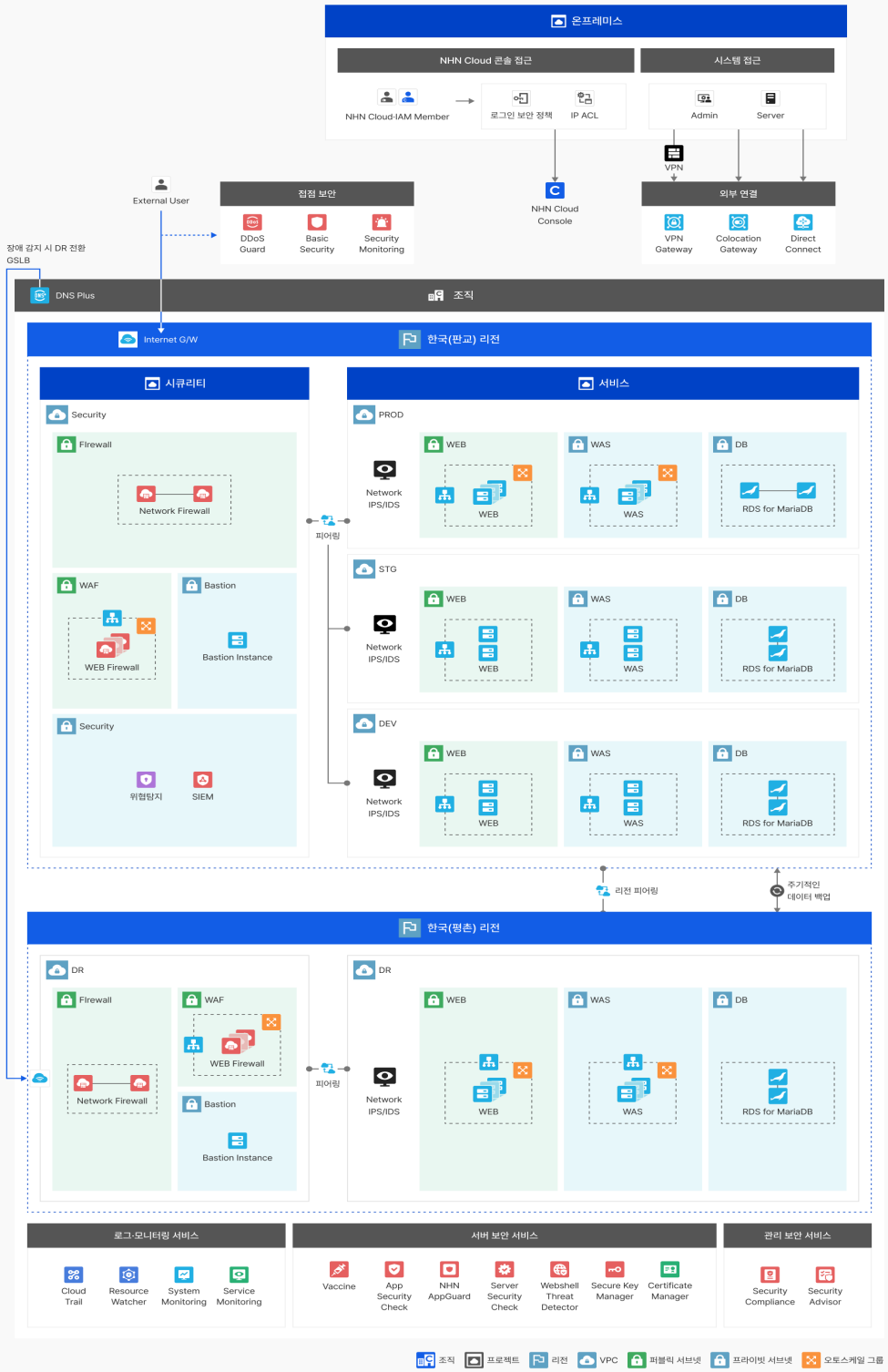

그림 9 NHN Cloud 네트워크 아키텍처(참고)

※ NHN Cloud 네트워크 아키텍처 보안 가이드를 활용하여 다양한 네트워크 보안 아키텍처를 경험할 수 있습니다.

네트워크 및 호스트 접근 통제

올바른 네트워크 및 호스트에 대한 접근 통제는 랜섬웨어와 같은 악성코드의 외부 침입을 방지하고, 내부 사용자나 기기에서 발생할 수 있는 비정상적인 행위나 전파를 방지하고 시스템을 보호합니다.
NHN Cloud의 주요 접근 통제 서비스 3가지는 다음과 같습니다.

- **Network Firewall**은 NHN Cloud 환경에서 별도의 방화벽 제품을 사용하지 않더라도 고객의 가상 자산을 효율적으로 관리하고 외부 및 내부 네트워크 통신 정책을 관리할 수 있는 특화된 방화벽 서비스를 제공합니다. 허브 앤 스포크 구조로 외부 공격을 차단하고 VPC 간 내부 트래픽을 제어하여 고객의 가상 환경을 안전하게 보호하고 고가용성을 보장합니다.

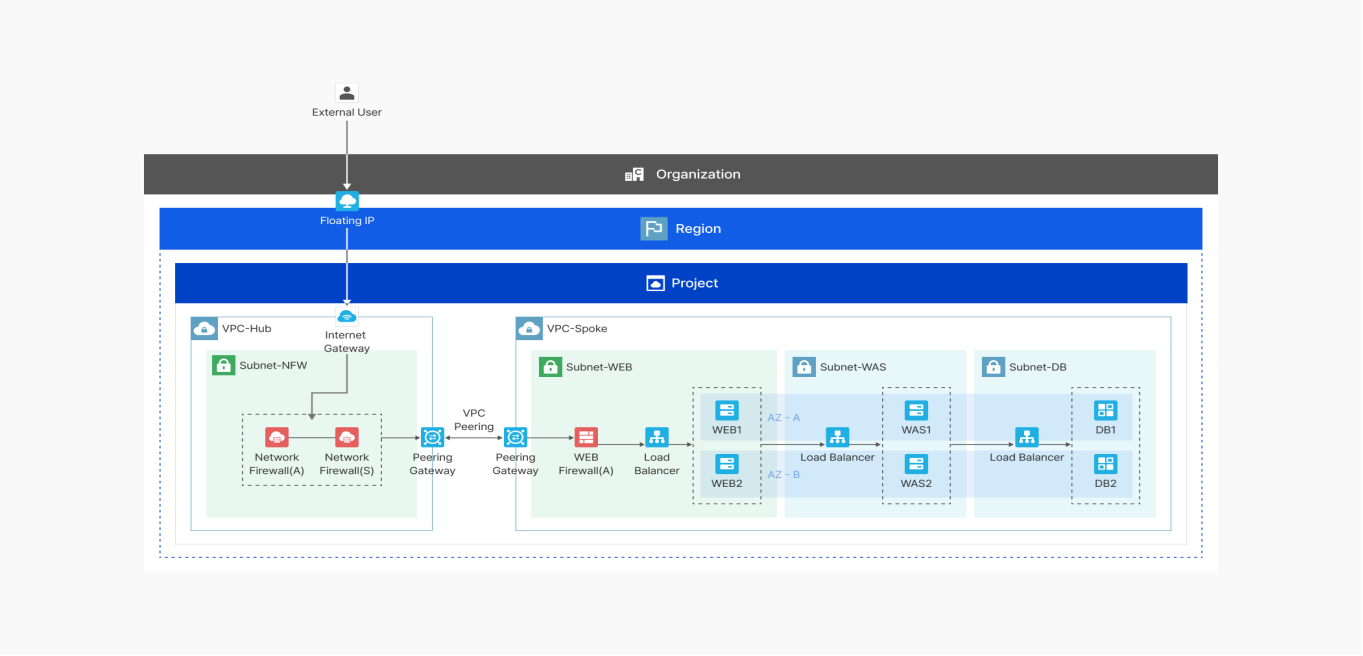

그림 10 NHN Cloud Network Firewall 서비스 구성도

- VPC에 적용되는 **Network ACL**은 VPC로 유입되는 트래픽을 제어하고 **Security Groups**은 인스턴스의 송·수신 트래픽을 제어해 불필요한 트래픽을 차단하여 Reverse Shell 등을 통한 랜섬웨어 위협을 예방할 수 있습니다.

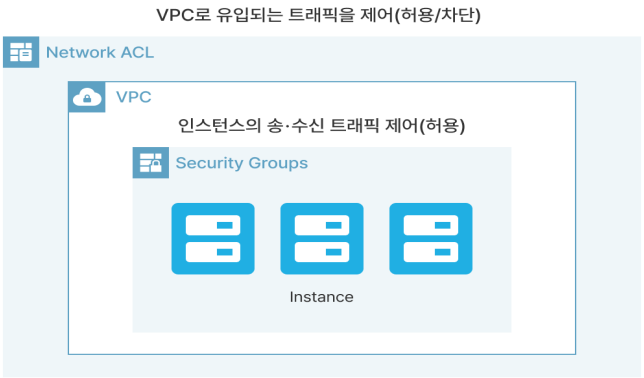

그림 11 Network ACL, Security Groups 트래픽 제어

3.2.4 가상 데스크톱 인프라(VDI)

VDI란 무엇인가?

VDI는 가상 데스크톱 인프라(virtual desktop infrastructure)로, 기업이나 조직에서 사용자에게 가상 데스크톱 환경을 제공하는 기술입니다. 이를 통해 사용자는 어디서나 안정적이고 일관된 작업 환경을 이용할 수 있으며, IT 관리자는 중앙에서 보안 관리와 리소스 할당을 효율적으로 수행할 수 있습니다.

NHN Cloud는 CC인증, GS인증, 클라우드 서비스 보안인증(CSAP)을 획득한 가상 데스크톱 서비스를 제공하여 원격 근무를 안전하고 효율적으로 지원하며, 다양한 하드웨어를 활용하여 맞춤형 스마트워크 환경을 제공합니다.

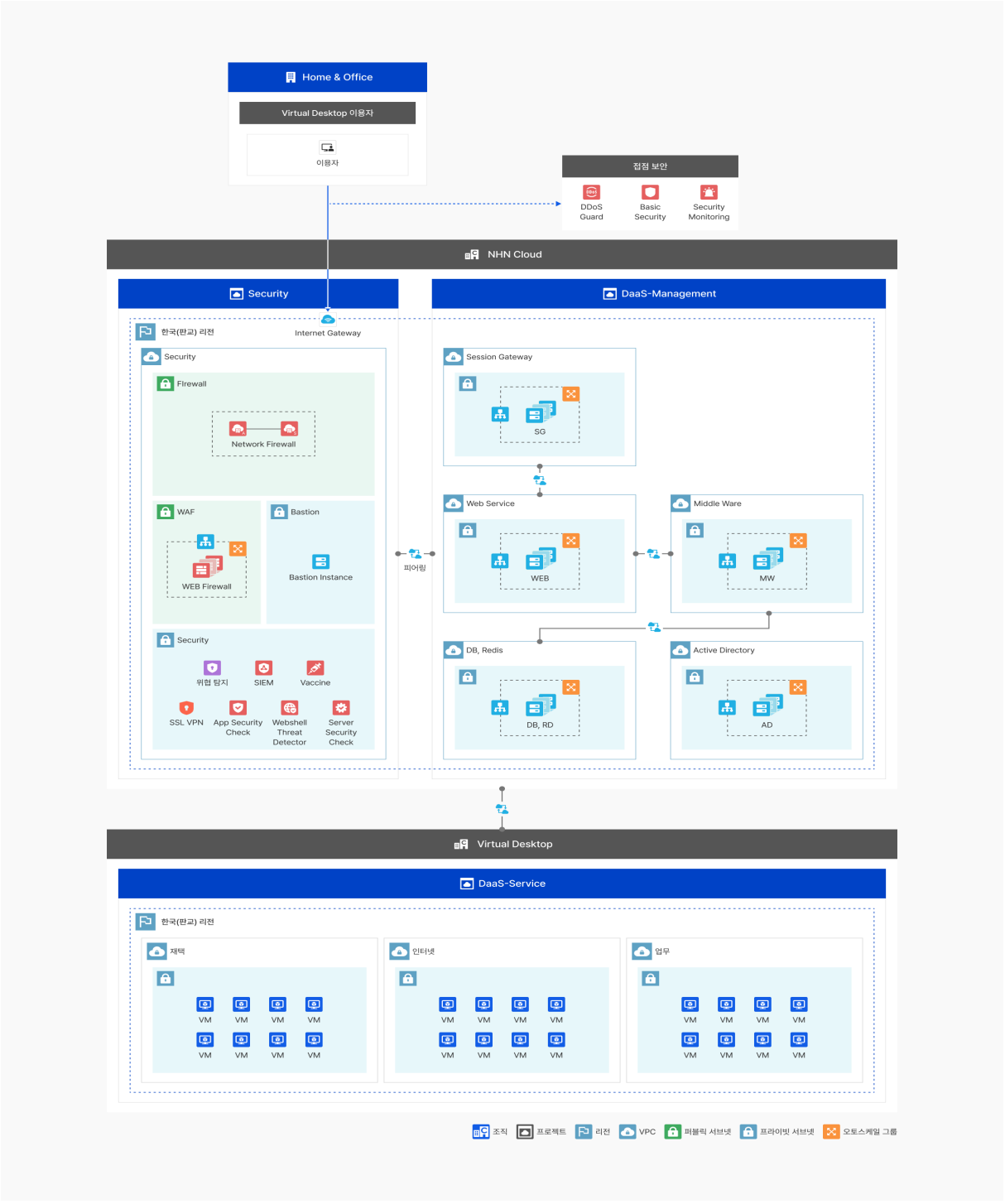

그림 12 NHN Cloud Virtual Desktop 구성도(예시)

VDI의 필요성

VDI를 사용하면 업무용 PC와 인터넷 PC를 구분하여 상호 격리된 환경을 조성할 수 있어 망 분리 조건을 충족시킬 수 있습니다. 또한, 재택 근무와 같은 업무 환경 변화로 인해 사용자의 단말이 외부 인터넷에 노출될 가능성이 높아지면서 외부 해킹, 악성코드, DDoS 공격 등 다양한 침해 위협이 증가하고 고도화되고 있습니다.
이러한 환경에서 VDI를 통해 중앙 집중화된 데이터 및 응용 프로그램 접근을 제공하여 보안 보호막을 형성할 수 있습니다. 사용자의 업무 환경은 가상화되어 중앙 집중화된 서버에서 실행되므로 사용자의 업무 환경에 대한 보안을 강화할 수 있습니다. 또한, 사용자 인증 및 액세스 제어 기능을 강화하여 민감한 정보의 유출을 방지할 수 있습니다. 이를 통해 외부 해킹 시도를 차단하고 중요한 데이터의 안전성을 보장할 수 있습니다.

랜섬웨어 감염 방지 효과

- **구성 특성에 의한 방어 효과**
  VDI는 실제 가동되는 가상 데스크톱과 사용자가 접속하는 단말이 원격 접속으로 구성됩니다. 이 경우 가상 데스크톱은 안전한 서버 팜(server farm)에 위치하여 사용자 노출로 인한 감염을 방지할 수 있습니다. 또한 가상 데스크톱과 사용자의 접속 단말기 간의 실제 데이터 유통이 통제되기 때문에 사용자 단말 감염에 따른 확산도 방지할 수 있습니다.
- **기능 적용에 따른 방어 효과**
  디스크 및 USB 제어, 키 입력 로깅 방지, 화면이나 동영상 캡처 방지, 암호화 전송 등을 통해 데이터 보호 및 악성코드 감염을 방지할 수 있습니다. 또한 감염된 VD를 삭제 후, 이전 백업된 데이터를 통해 VD가 재생성되어 신속하게 복구하고 피해를 최소화할 수 있습니다.

3.2.5 교육 및 인식 활성화

내부 사용자의 보안 인식은 조직의 전반적인 보안 방어 체계의 중요한 요소입니다. 랜섬웨어와 같은 악성코드가 내부 조직 및 시스템에 침투하는 경로 중 하나는 내부 사용자의 부주의나 부적절한 행동입니다. 따라서 랜섬웨어 감염을 최소화하고 보안 인식을 강화하기 위해서는 최신 보안 동향을 파악하고, 임직원 대상의 보안 교육 및 모의 훈련을 통해 보안 인식을 향상시키고 최상의 실천 방법을 전파하는 것이 중요합니다.

랜섬웨어 공격 사례 공유

랜섬웨어 공격 사례를 공유하여 공격 유형, 경로 및 피해 상황에 대한 이해를 높여 내부 사용자가 경각심을 가지고 주의하도록 합니다.

보안 조치 및 예방법

크리덴셜 스터핑(credential stuffing)이나 무차별 대입 공격과 같은 위협에 대비하기 위해 복잡한 암호를 사용하고, 동일한 암호를 여러 곳에 사용하지 않도록 하며, 2차 인증 등 보안 강화 수단을 활용합니다. 이메일 피싱 공격이나 파일 다운로드 및 링크 주의, 신뢰된 소스에서만 소프트웨어를 설치하는 등의 보안 조치 및 예방법을 공유합니다.

보고 및 대응 절차

랜섬웨어 대응 모의 훈련을 통해 조직의 보안 수준을 정량적으로 점검하고, 평상시 의심스러운 활동이나 이상 징후가 발견되면 보안 신고를 생활화하여, 보안 사고에 대한 대응 조직과 절차를 사전에 수립해야 합니다.

3.3 랜섬웨어 탐지 방안

랜섬웨어 공격으로 파일 및 데이터가 암호화되기 전, 조기에 증상을 발견하고 피해 확산 및 추가 공격에 대응하기 위해서는 랜섬웨어를 비롯한 악성코드 및 이상 행위와 같은 보안 위협이 발생할 때 실시간으로 모니터링하고 알림을 받아 조치할 수 있는 프로세스를 수립하는 것이 중요합니다.

3.3.1 시스템 모니터링을 통한 자원의 이상 징후 탐지

랜섬웨어 감염 시 파일을 빠르게 암호화하는 과정에서 CPU 및 메모리 등의 컴퓨팅 자원을 과도하게 사용합니다. NHN Cloud의 **System Monitoring**은 인스턴스를 구동할 때 자동으로 다양한 지표를 수집하며, 수집된 지표의 임계치를 설정하여 서버를 지속적으로 감시할 수 있습니다. 이상 징후를 감지하면 이를 신속히 파악하여 이용자에게 알림을 보내어 즉각 대응할 수 있도록 합니다. 이를 통해 시스템 자원의 과도한 사용으로 인한 이상 징후를 식별하고 신속한 조치를 취할 수 있습니다.

3.3.2 보안 관제(침해 위협 모니터링)를 통한 보안 위협 탐지

NHN Cloud는 외부 보안 위협을 실시간으로 감시하고 탐지된 위협을 효과적으로 대응할 수 있는 **Security Monitoring**을 제공합니다. 고도화된 보안 정책과 플랫폼을 통해 악의적인 보안 위협을 정확하게 탐지하여 이상 징후를 초기에 발견하고 고객에게 제공함으로써 외부 공격에 신속하게 대응하여 클라우드 자산을 안전하게 보호합니다.

3.3.3 보안 소프트웨어 및 안티바이러스 솔루션 활용

효과적인 안티바이러스 및 안티멀웨어 솔루션은 악성코드 및 랜섬웨어로부터 시스템과 개인 PC를 보호하는 데 중요한 역할을 합니다. 특히 시그니처 기반의 탐지 방식 외에도 행동 기반 탐지를 통해 알려지지 않은 변종에 대응할 수 있어야 합니다. 또한, 실시간으로 악성코드를 탐지하고 차단하며 필요 시 격리하고 치료하는 기능을 제공하며, 악성코드 탐지 정책을 긴급 또는 주기적으로 업데이트하여 최신 악성코드에 대응할 수 있어야 합니다. NHN Cloud는 클라우드 환경에서도 실시간 보안 위협과 악성코드를 탐지할 수 있는 서비스를 제공하고 있습니다.

Vaccine은 클라우드 환경에서 악성코드 및 랜섬웨어를 탐지하고 방어하기 위한 서비스입니다. 백신 매니저와 에이전트를 별도로 구매하지 않아도 Vaccine 서비스를 통해 클라우드 시스템을 안전하게 보호할 수 있습니다. 실시간 검사 및 수동 스캔 기능, 악성코드 탐지 및 격리 기능을 제공하며, 악성 웹사이트 접근 차단 기능을 이용하여 악성 웹사이트에 의한 랜섬웨어 위협에 대응할 수 있습니다. 또한 탐지 현황은 클라우드 콘솔과 이메일을 통해 확인할 수 있습니다.

NHN AppGuard는 안전한 모바일 애플리케이션 실행 환경을 위해 다양한 보안 위협으로부터 소스 코드 보호, 메모리 변조, 위·변조 방지 및 해킹 툴 차단 등 다양한 기능을 제공합니다. 이를 통해 신속한 보안 침해 시도에 대응하고 안정적인 서비스를 제공할 수 있습니다.

그 외 APT 대응 솔루션, EDR(endpoint detection and response), 문서 보안, 오피스 시큐리티 등 다양한 보안 솔루션을 활용하여 다층적인 보안 강화 접근 방식이 필요합니다.

4 랜섬웨어 대응 방안

4.1 업무 연속성 계획 수립(business continuity plan, BCP)

랜섬웨어로 인한 피해를 최소화하기 위해서는 관리적, 기술적 보안 조치를 통해 예방하고, 랜섬웨어를 탐지할 수 있는 체계를 마련해야 합니다. 또한 랜섬웨어에 감염되었을 때 핵심 업무는 유지하고 빠르게 대응하여 복구할 수 있는 체계를 준비해야 합니다.

랜섬웨어 공격은 비즈니스를 중단시키고 심각한 재정적 손실을 초래할 수 있기 때문에 BCP(business continuity plan, 업무 연속성 계획)는 랜섬웨어 및 기타 사이버 위협에 대비하여 준비되어야 합니다.

4.1.1 업무 연속성 계획 절차

1. 프로젝트 계획: 목표 및 범위 설정

2. 위험 평가 및 업무 영향 분석(business impact analysis, BIA)

a. 잠재적인 위험을 식별하고, 재난이나 비상사태가 발생했을 때 업무에 미치는 영향을 평가합니다.
b. 핵심 업무 프로세스 및 시스템의 우선순위를 정하고 대응 전략을 결정합니다.
c. 복구시간목표(RTO), 복구시점목표(RPO), 복구 우선순위 결정

3. 업무 연속성 전략 선정

a. BIA를 기반으로 업무 연속성을 유지하기 위한 전략을 개발합니다.
b. 필요한 리소스와 절차를 결정하고, 재난 대응 및 회복에 필요한 계획을 마련합니다.
c. 전략별 비용 분석, 전략 도출

4. 업무 연속성 계획 개발

a. 전략을 바탕으로 실제 대응 사항과 프로세스를 문서화하여 업무 연속성 계획을 개발합니다.
b. 위기 대응 팀의 역할과 책임, 통신 계획, 비상 연락망 등을 포함합니다.
c. 업무 연속성 계획 조직 구성 및 조직별 계획 수립

5. 계획의 시행 및 실행

a. 개발된 업무 연속성 계획을 실행 가능한 형태로 구현합니다.
b. 위기 대응 팀을 구성하고, 교육 및 훈련을 실시하여 계획을 효과적으로 시행할 수 있도록 합니다.

6. 테스트 및 평가

a. 업무 연속성 계획의 효과성을 확인하기 위해 정기적으로 테스트를 수행합니다.
b. 시나리오 기반 테스트나 시뮬레이션을 통해 계획의 강점과 약점을 식별하고, 개선할 수 있는지를 평가합니다.

7. 유지 및 개선

a. 업무 환경의 변화 및 새로운 위협에 대응해 업무 연속성 계획을 정기적으로 검토하고 업데이트해야 합니다.
b. 발생한 문제를 분석하고 개선점을 도출하여 계획의 효율성을 높입니다.

4.1.2 업무 연속성 계획 구성 요소

표 4 업무 연속성 계획 구성 요소

구성	세부 내용
재해 예방 (disaster prevention)	• 업무 영향 분석(BIA) • 재해 및 재난 분류, 취약성 발견, 발생 빈도와 예상 손실액 추정 • 내·외부 및 사회적 요인에 따른 원인 분류 • 리스크로 인한 업무비즈니스 영향력 평가 및 우선순위 선정 • 주요 프로세스의 복구 시간 설정 • 위험을 최소화할 수 있는 전략 대안 시스템 선정
대응 및 복구 (response & recovery)	• 재해 또는 재난으로 인한 인적 및 물적 자원에 대한 긴급 조치 및 업무 프로세스 복구 • 대응 및 복구 시나리오 작성 • 대응 계획: 비상시 행동 요령, 연락처, 설비, 조직 구성 및 분류, 체계 구성 • 복구 계획: 피해 집계 체계, 구제 계획, 복구 업무 우선순위, 표준 절차, 보고 체계 구축, 대외 협력 체계 구축 등
유지 보수(maintenance)	• 재난 발생에 따른 유형 분석 및 계획 수립을 위한 평가, 분석, 보완 활동 • 재해 계획의 지속적인 업데이트 및 유지 관리
모의 훈련(simulation)	• 비상 대응 계획에 따른 훈련 및 학습 내용을 평가하고 피드백 제공 • 시나리오 기반 훈련 실시, 긴급 상황에 대한 숙련된 대응력 확보

4.1.3 업무 연속성 대비책

랜섬웨어 공격은 업무 연속성을 위협할 수 있는 잠재적인 위험 요소 중 하나입니다. 이에 대응하여 조직은 다음과 같은 대비책을 마련해야 합니다.

- 위험 평가 및 취약점 분석: 시스템과 네트워크의 취약점을 식별하고 관리합니다.
- 백업 및 데이터 복원 계획: 주기적이고 완전한 데이터 백업을 수행하고, 복원 절차를 마련하여 긴급 상황에 신속하게 대응합니다.
- 사용자 교육과 보안 정책 강화: 직원들에 대한 보안 교육을 강화하고, 엄격한 보안 정책을 시행하여 안전한 업무 환경을 조성합니다.
- 위기 대응 계획 및 테스트: 랜섬웨어에 대비한 위기 대응 계획을 수립하고 주기적으로 테스트하여 대비력을 향상시킵니다.
- 보안 솔루션 및 업데이트 관리: 최신 보안 솔루션을 도입하고, 시스템 및 소프트웨어의 업데이트를 정기적으로 관리하여 보안을 강화합니다.

이러한 조치들을 통해 조직은 랜섬웨어 및 기타 사이버 위협으로부터의 보안을 강화하고 업무 연속성을 유지할 수 있습니다.

4.2 백업 전략 수립

4.2.1 효과적인 백업 전략의 중요성과 구축 방법

랜섬웨어에 대비한 효과적인 백업 전략은 조직의 데이터를 안전하게 보호하고, 재해나 사이버 공격으로부터 빠르게 복구할 수 있도록 하는 것입니다. 이를 위해 조직은 백업 관리 및 대응 전략을 수립해야 합니다.

백업 정책 결정을 위한 고려 사항

백업 정책은 조직의 운영 환경과 비용 등 다양한 요소를 고려하여 백업 대상, 데이터의 중요도, 복구 정책, 백업 방식 등을 결정해야 합니다. 백업 정책을 세우기 위해 필요한 고려 사항은 다음과 같습니다.

1. 백업 대상 식별

a. 데이터 종류 및 중요도에 따른 비즈니스 핵심 데이터의 우선순위를 정합니다.
b. 시스템 및 데이터의 중요도 기준으로 OS 및 데이터 백업 필요 대상을 선별합니다.

2. 복구시간목표(RTO), 복구시점목표(RPO) 설정

a. 데이터를 복구하는 데 걸리는 시간과 데이터 손실을 허용할 수 있는 한도를 정의합니다.
b. 백업 대상 시스템 및 데이터의 중요도에 맞는 RTO, RPO를 설정합니다.

3. 백업 주기 및 방식 결정

a. 운영체제, 애플리케이션, 데이터, 데이터베이스 등 대상에 따른 중요성과 변경 빈도에 따른 백업 주기를 결정합니다.
b. 시스템 및 서비스 특성을 고려하여 백업 가능 시간(야간, 주말 등), 백업 주기(일일, 주간, 월간 등), 백업 방식(전체, 증분, 차등 백업 등)을 선정합니다.

4. 백업 보관 주기 설정

a. 법적 요구사항이나 시스템 및 데이터의 중요도에 따라 일, 주, 월, 분기, 반기, 연간, 영구 보관 주기를 설정합니다.
b. 중요 시스템 및 데이터의 경우 2벌 이상의 백업 복제본 구성 여부를 확인합니다.

5. 백업 저장소의 구분

a. 1차 저장소는 온라인 디스크 형태로 구성하고, 중요 및 장기 보관을 할 경우 소산 및 별도 오프라인으로 보관합니다.
b. 온프레미스 저장소, 클라우드 저장소, 외부 백업 제공 업체 등 다양한 옵션이 있습니다.

6. 보안 및 암호화

a. 백업된 데이터의 보안을 고려하여 데이터 암호화 및 접근 제어 등의 보안 조치를 적용합니다.

7. 백업 복원 테스트 및 관리

a. 백업 전략 수립 후 실제 백업 후 복원 테스트를 통해 정상적으로 작동하며 데이터를 성공적으로 복구할 수 있는지 확인합니다.
b. 백업 및 복구 전략을 문서화하여 관련 정보와 절차를 기록합니다.
c. 시스템 및 비즈니스 현황을 고려하여 지속적인 검토와 개선을 합니다.

4.4.2 다양한 백업 방식 비교 및 선택

각각의 백업 방식은 목적 및 장단점이 다르기 때문에 백업 대상인 시스템과 데이터의 중요도, 그리고 백업 조건 등을 고려하여 기업의 환경에 맞는 선택을 하는 것이 중요합니다.

전체 백업(full backup)

변경된 데이터나 고유한 데이터를 구분하지 않고 전체 데이터를 백업하는 방식입니다.

- 장점: 복구 시에는 일부 백업 방법보다 간편하며, 상대적으로 증분 백업에 비해 복구 시간도 짧습니다.
- 단점: 백업 수행 시에는 많은 양의 저장 매체가 필요하며, 백업에 소요되는 시간과 비용이 상당히 많이 들어갑니다.

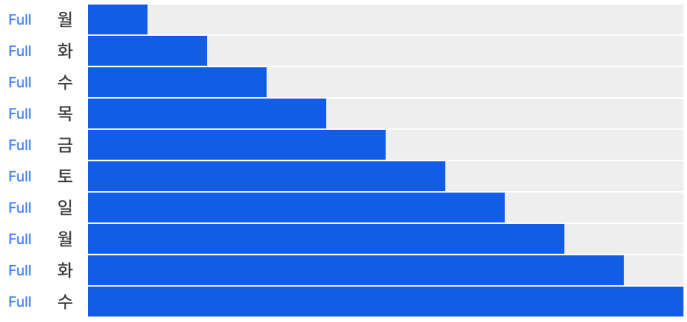

그림 13 전체 백업

증분 백업(incremental backup)

최종 전체 백업 또는 최종 증분 백업 이후에 변경된 데이터만 백업합니다.

- 장점: 변경된 데이터만 백업하므로 데이터의 양이 적어 백업 시간이 단축됩니다.
- 단점: 복구 과정에서 최종 백업된 전체 및 모든 후속 증분 백업본까지 복구해야 하기 때문에 복구 작업이 번거롭고 경우에 따라 시간이 오래 걸릴 수 있습니다.

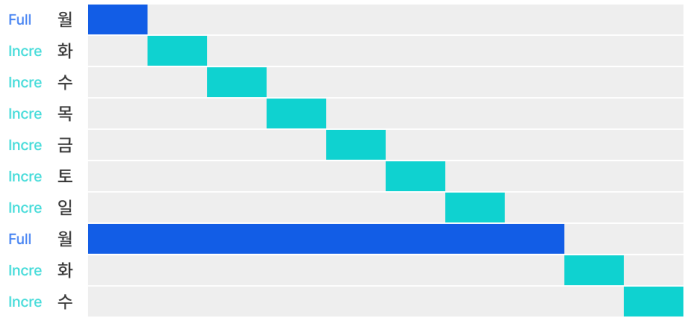

그림 14 증분 백업

차등 백업(differential backup)

마지막 전체 백업 이후 변경된 모든 데이터를 백업합니다.

- 장점: 전체 백업 이미지와 가장 최근의 차등 이미지만 복구하면 되기 때문에 복구 시점에 따라 다르지만 대개 증분 백업보다 복구 속도가 빠릅니다.
- 단점: 파일이 변경 되면 예정된 다음 전체 백업까지 매일 백업합니다. 따라서 파일이 변경될 때마다 파일 크기가 증가하게 되며, 다음 전체 백업 때까지 파일 크기가 점점 커지게 됩니다.

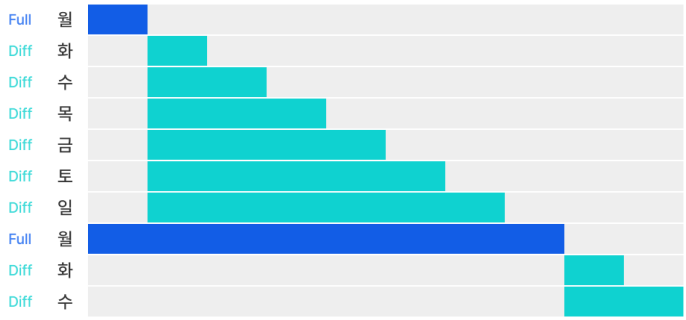

그림 15 차등 백업

신세틱 백업(synthetic backup)

선택된 폴더의 전체 백업 이후 변경, 추가된 데이터를 증분 백업 형식으로 저장 후 두번째 전체 백업 작업 시 중간에 모아 둔 증분 백업을 이용하여 전체 백업으로 재생성하는 방식입니다.

- 장점: 신세틱 백업을 이용하면 백업 서버에서 이미 저장되어 있는 증분 데이터를 이용해 전체 백업을 새로 만들기 때문에 네트워크 사용량을 줄일 수 있습니다.
- 단점: 기능이 다양하고 복잡한 인터페이스를 가지고 있기 때문에 초기 설정 및 구성이 다소 복잡할 수 있습니다.

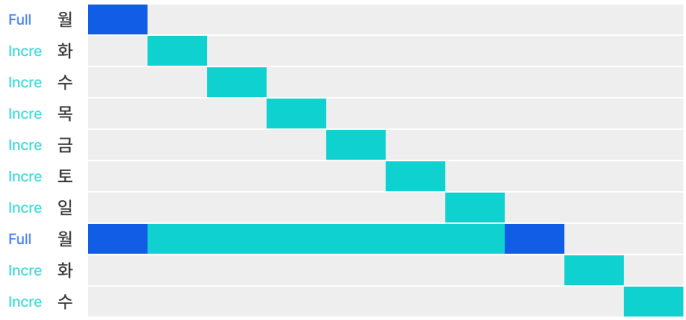

그림 16 신세틱 백업

중복 제거 백업(deduplication backup)

백업되는 데이터 중에서 중복되는 부분을 식별하고 제거하여 저장 공간을 절약하는 백업 방법입니다.

- 장점: 동일한 데이터가 여러 번 백업되는 것을 방지하고, 저장 매체의 용량을 효율적으로 활용할 수 있도록 도와줍니다.
- 단점: 중복 제거를 위한 처리 과정이 추가되어 백업 프로세스의 처리 속도가 느려질 수 있습니다.

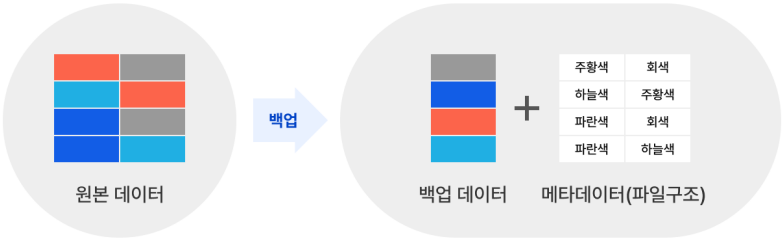

그림 17 중복 제거 백업

4.2.3 데이터 저장 및 백업을 위한 NHN Cloud 서비스

NHN Cloud의 백업 및 스냅숏 서비스를 이용하여 데이터를 정기적으로 백업하고 필요할 때 복구할 수 있습니다.
클라우드 콘솔을 통해 간편하게 백업 정책을 등록하고, 백업 이력을 확인하며, 필요한 경우 복구 요청을 할 수 있습니다. 또한, 백업 결과는 매일 이용자의 이메일로 전송됩니다.

Backup

보안 위험, 사용자의 조작 실수, 저장 장치의 고장, 자연재해 등으로 인한 데이터 손실에 대비해 복제본을 만들고 안전하게 보관하는 서비스입니다.
전체 및 증분 백업 방식을 함께 사용하고 있으며, 가변 길이 중복 제거(variable-length deduplication) 기술을 이용하여 전체 백업 이후에 발생하는 데이터 중복을 제거하고 백업 데이터를 최소화합니다. 이로써 백업 시간이 단축되고 네트워크 사용량도 줄어듭니다. 또한, 데이터는 암호화 과정을 거쳐 백업 스토리지로 안전하게 전송됩니다.
사용자가 백업 주기, 시간, 보관 주기 등을 자유롭게 설정할 수 있도록 하여 사용자의 다양한 요구에 부합합니다. 더 나아가 재해 상황에서 데이터를 더 안전하게 보관할 수 있는 소산 백업도 제공하고 있습니다.

Snapshot

Block Storage의 스냅숏 기능을 이용하면 이용자가 직접 Block Storage의 데이터를 복사하는 것보다 빠르게 데이터를 백업할 수 있습니다. 스냅숏을 활용하여 Block Storage를 복원 후 기존 인스턴스나 다른 인스턴스에 연결하여 데이터를 복구할 수 있습니다.

Image

Image는 운영체제 및 애플리케이션을 담고 있으며, 기본 보안 점검을 완료한 상태로 제공됩니다. 또한 각 기업의 운영 환경에 맞게 설정된 Image를 수정하여 사용할 수 있습니다. 특정 시점의 Image를 생성하여 랜섬웨어 감염 시 시스템과 데이터를 복원할 수 있습니다.

NAS

NAS 서비스를 사용하여 인스턴스에 공유 스토리지를 연결하여 데이터를 공유할 수 있습니다. 프로젝트의 네트워크를 통해서 NAS 스토리지에 접근하기 때문에 다른 프로젝트의 네트워크와 격리되어 있다면 접근 제어(ACL)를 통해 더 상세한 제어가 가능합니다. 또한 XTS-AES-256 알고리즘으로 암호화하여 데이터를 안전하게 보관할 수 있습니다.

데이터베이스 백업

NHN Cloud는 **RDS for MySQL**, **RDS for MariaDB**, **RDS for MS-SQL** 데이터베이스를 제공합니다. 자동 백업은 최대 730일까지 보관 가능하며, 특정 시점의 데이터베이스를 영구 저장하기 위해 수동으로 백업을 수행할 수 있습니다. 수동 백업은 명시적으로 삭제하지 않는 이상 DB 인스턴스가 삭제될 때까지 보존됩니다. 이러한 데이터베이스 백업 기능을 활용하여 장애 상황이나 랜섬웨어 감염과 같은 위험 상황에서 데이터베이스를 복구할 수 있습니다.

4.3 침해 사고 분석

4.3.1 침해 사고 분석

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제2조 제1항 제7호에 의하면 침해 사고는 해킹, 컴퓨터 바이러스, 논리 폭탄, 메일 폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보 시스템을 공격하는 행위로 인하여 발생한 사태를 의미합니다. 또한, 정보통신망의 정상적인 보호·인증 절차를 우회하여 정보통신망에 접근할 수 있도록 하는 프로그램이나 기술적 장치 등을 정보통신망 또는 이와 관련된 정보 시스템에 설치하는 행위도 침해 사고에 해당합니다. 즉, 침해 사고는 정보 유출, 시스템 파괴, 서비스 장애, 권한 상승 등의 공격 행위로, 이를 통해 안정적인 서비스 운영이 방해되는 것을 의미합니다.

침해 사고 분석은 조직 또는 시스템에 대한 사이버 공격 및 악의적인 행위가 발생했을 때, 그 원인, 피해 범위, 영향 등을 분석하는 과정입니다. 이를 통해 조직은 공격에 대한 이해를 높이고 보안 대응책을 마련하며, 향후 유사한 공격을 예방하는 데 도움을 얻을 수 있습니다.

본 가이드에서는 침해 사고 시 사고 분석자가 취해야 할 단계별 침해 사고 분석 절차를 한국정보보호진흥원(KISA)의 침해 사고 분석 절차 안내서를 참조하여 7가지 대응 요소에 대해 설명하였습니다.

침해 사고 분석 절차

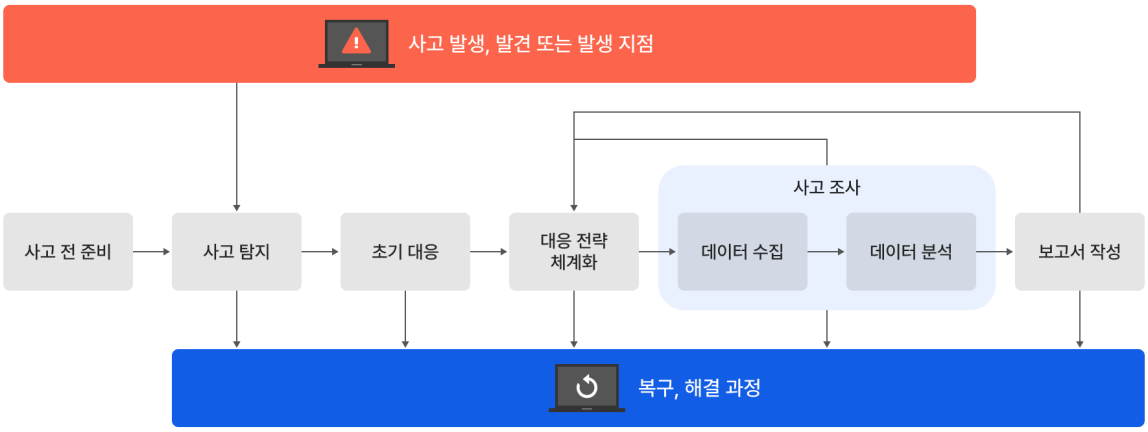

그림 18 침해 사고 대응 7단계

1. 사고 대응 전 준비 과정

- 사고가 발생하기 전 침해 사고 대응팀과 조직적인 대응을 준비합니다.
- 사고 대응 체제의 준비
  - 효율적인 사고 대응을 위해 준비 단계에서는 범조직적인 전략과 대처 방안을 개발해야 합니다.
  - 호스트 및 네트워크 기반 보안 측정 수행
  - 사용자 교육 훈련
  - 침입 탐지 시스템 설치
  - 강력한 접근 통제 실시
  - 취약점 평가 실시
  - 규칙적인 백업 수행
  - 침해 사고 대응팀과의 비상 연락망 구축

- 침해 사고 대응팀의 준비
  - 침해 사고 대응팀은 전문가 조직을 구성하고 시스템 네트워크 관리자와 긴밀한 협조 관계를 구성해야 합니다.
  - 사고 조사를 위한 도구(하드웨어, 소프트웨어) 구비
  - 사고 조사를 위한 문서 양식 정형화
  - 대응 전략 수행을 위한 적절한 정책과 운용 과정 수립
  - 직원들의 교육 훈련

2. 사고 탐지

- 정보 보호 및 네트워크 장비를 통해 이상 징후를 탐지하고 관리자가 침해 사고를 식별합니다.
- 초기 대응 점검표
  - 최초 탐지하게 된 경위와 인지된 상황을 정확하게 기록하고 보고하는 것이 좋습니다.
  - 현재 시간과 날짜
  - 사고 보고 내용과 출처
  - 사건이 일어난 일시
  - 관련된 하드웨어, 소프트웨어의 목록
  - 사고 탐지 및 사고 발생 관련자의 네트워크 연결 지점

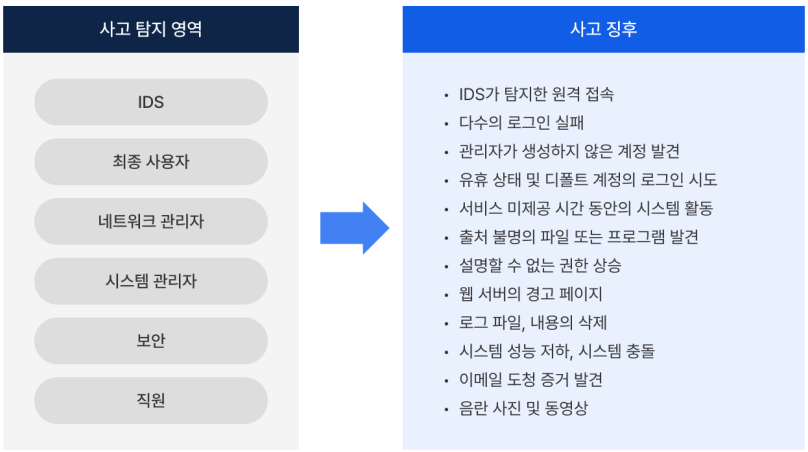

그림 19 사고 탐지 및 사고 징후

3. 초기 대응

- 조사의 초기 단계로 충분한 정보를 확보하여 사건의 유형 식별과 영향 평가를 통해 대응 전략을 세우는 것이 목적입니다.
- 침해 사고 대응팀을 소집하고, 네트워크와 시스템의 정보를 수집하여 업무 및 서비스에 영향도 검증을 확인합니다.
- 실제 사고 유무와 적절한 대응이 되었는지, 사건의 유형 식별, 잠재적 영향은 무엇인지 등을 파악해 사고를 어떻게 처리할 것인지 대응 전략을 수립합니다.

4. 대응 전략 수립

- 주어진 사건의 환경에서 가장 적절한 대응 전략을 결정하도록 합니다.
- 환경의 전체적인 고려
  - 사고의 세부 항목과 요인에 대한 재조사가 필요합니다.
  - 대응 능력, 기술 자원, 정책적 고려, 법적 제한, 업무 목적에 의해 결정합니다.
- 적절한 대응 고려
  - 공격 환경과 대응 능력을 고려하여 다양한 대응 전략을 수립해야 합니다.

- 대응 전략은 조직의 업무 목표를 고려하여 상위 관리자가 승인해야 합니다.
- 운영의 영향도, 대외 이미지, 경제적 영향 등을 고려해야 합니다.

5. 사고 조사

- 데이터 수집과 분석을 통하여 사고가 언제, 누구에 의해, 어떻게 발생했는지를 파악하고 피해 확산 및 재발 방지 방안을 고려합니다.
- 데이터 수집
  - 접근 가능한 데이터를 모두 수집합니다.
  - 호스트 기반 정보와 네트워크 기반 증거로 나누어서 수집 분석합니다.
- 데이터 분석
  - 수집된 모든 정보의 전체 조사를 의미합니다.

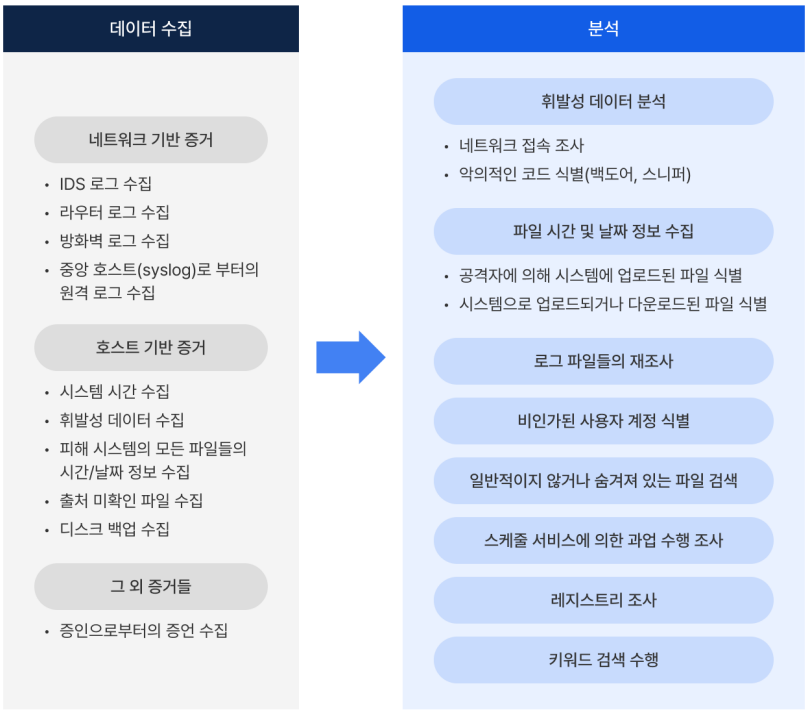

그림 20 데이터 수집 및 분석 예

6. 보고서 작성

- 사고 보고서를 작성할 때에는 데이터 획득, 보관, 분석 등의 과정을 명확하고 객관적으로 서술해야 합니다. 사건의 세부사항을 정확하게 기술하고 의사 결정자가 이해하기 쉬운 형식으로 보고서를 작성해야 합니다.

7. 복구 및 해결 과정

- 향후 유사한 공격을 식별하고 예방하기 위해 보안 정책을 수립하고 절차를 변경합니다. 또한 사건 기록과 장기적인 보안 정책 수립에 대한 수정 계획을 결정하고 관리적, 기술적 조치를 조정합니다.

악성코드 은닉 사이트 분석 사례

악성코드가 숨겨진 해킹 피해 시 종종 해당 악성코드를 삭제하고도 여러 차례에 걸쳐 악성코드가 재삽입되는 현상을 발견할 수 있습니다. 이는 체계적인 사고 분석과 대응 절차를 거치지 않고 홈페이지의 악성코드만을 단순히 삭제했기 때문입니다.
악성코드가 삽입된 사이트의 경우 웹 페이지에 포함된 악성코드를 삭제하는 것뿐만 아니라 서버에 존재하는 웹 셸과 같은 백도어 프로그램을 찾아내고, 이를 통해 침해된 서버의 취약점을 확인하여 근본적인 침해 원인을 제거하는 것이 중요합니다.
웹 페이지의 악성코드 은닉 사고에 대한 대응 절차는 다음과 같습니다. 이러한 절차는 일반적으로 해킹 피해 기업이나 기관에서 자체적으로 사고 처리를 위해 채택하는 기본적인 절차이며, 시스템의 무결성을 보장하기 위해 법적 증거로 활용해야 하는 경우에는 체계적인 포렌식 절차를 따라야 합니다.

1. 악성코드 삽입 사실 인지 및 삭제

웹사이트에 은밀하게 삽입된 악성코드는 방문자를 감염시킬 수 있으므로 신속하게 제거해야 합니다. 이는 웹 페이지에 iframe또는 object 코드를 삽입하거나, 인코딩된 코드를 삽입하거나, 오류 정보 표시 페이지에 코드를 삽입하는 등 다양한 방법으로 이루어질 수 있습니다. 따라서 악성 링크와 코드를 즉각 제거하는 것이 중요합니다.

2. 웹 로그 및 이벤트 로그 분석

웹 로그 및 이벤트 로그를 분석하여 공격에 이용된 취약점과 피해 규모를 조사합니다. 웹 로그가 방대한 경우 공격 로그를 찾기 어려울 수 있으므로 특정 키워드를 중심으로 탐색하는 것이 효과적일 수 있습니다. 일반적인 웹 공격에서 나타나는 몇 가지 문자열은 다음과 같습니다. 하지만 이러한 문자열이 모두 공격임을 단정할 수는 없으므로 분석 효율성을 위한 용도로 사용해야 합니다.

※ 참고 키워드: ODBC, 80040e07, and, select, delete, create, cmd.exe, xp_cmdshell, POST

3. 백도어 등 해킹 프로그램 제거

로그 분석 및 파일 시스템 분석을 통해 백도어 및 기타 해킹 프로그램을 발견하고 이를 제거합니다. 악성코드 은닉 사고에서 흔히 발견되는 해킹 프로그램 중 하나는 웹 셸입니다. 웹 셸은 일반적으로 ASP 또는 PHP로 제작되며 파일 추가, 삭제, 변경 및 원격 명령 실행과 같은 기능을 통해 시스템을 완전히 제어할 수 있습니다. 공격자가 웹 셸을 통해 시스템에 침입하고 악의적인 행위를 할 경우, 해당 행위는 웹 로그에 기록됩니다. 따라서 웹 로그 분석 과정에서 웹 셸의 사용 여부를 주의 깊게 살펴봐야 합니다.

4. 주변 시스템 분석

한 대의 서버가 해킹되면 이를 통해 내부망의 다른 서버까지 침투하려고 시도할 수 있습니다. 예를 들어, 웹 서버가 해킹된 경우에는 DB 서버 등 인접한 서버도 이미 침투되었을 수 있습니다. 웹 취약점으로부터의 SQL Injection 공격은 실제로 DB 서버에서 명령이 실행될 수 있으므로, 웹 서버와 연결된 DB 서버의 해킹 가능성을 특히 염두에 두어야 합니다.

5. 취약점 제거 및 보안 강화

해킹에 악용된 취약점을 포함한 전반적인 보안 취약점을 점검하고 제거함으로써 해킹 재발을 방지해야 합니다. 더불어 안티바이러스나 웹 방화벽과 같은 추가적인 보안 도구를 도입하여 안전한 서비스 운영을 고려해야 합니다.

6. 서비스 재개 및 모니터링

조치를 모두 마치고 난 이후에도 일정 기간 동안 공격 모니터링을 강화해야 합니다. 대부분의 해커들은 한 번 침투한 사이트를 다시 공격하기 위해 시도합니다. 따라서 웹 로그 및 트래픽 분석을 통해 이러한 공격 시도를 탐지할 필요가 있습니다.

4.4 랜섬웨어 감염 신고 절차

랜섬웨어에 감염되면 시스템 파괴와 암호화뿐만 아니라 개인정보나 기밀 데이터의 유출이 발생할 수 있습니다. 이러한 침해 사고와 개인정보 유출이 발생할 경우, 해당 상황에 따라 사고를 즉시 신고해야 합니다.

4.4.1 법적 의무

대부분의 국가 및 지역에서는 데이터 보호 및 사이버 보안과 관련된 법률이 존재합니다. 이러한 법률은 기업이나 조직이 랜섬웨어 공격을 당한 경우에 대한 의무를 명시하고 있습니다.
일반적으로 이러한 법률은 랜섬웨어 공격 사건이 발생했을 때 즉시 관련 당국에 신고할 것을 요구하거나 규정합니다.

4.4.2 신고 절차

랜섬웨어 감염 사건이 발생하면 해당 국가 또는 지역의 법률 및 규정에 따라 관련 당국에 신고해야 합니다.
신고 절차는 주로 온라인 양식, 전화, 이메일 또는 직접 방문 등 다양한 방법을 통해 이루어질 수 있습니다. 또한 일부 국가에서는 랜섬웨어 공격 사건을 신고할 때 특정한 양식이나 절차를 따를 것을 요구할 수 있습니다.

표 5 침해 사고 신고 절차

구분	세부 내용
신고 대상	• 정보통신서비스 제공자 • 집적정보통신시설 사업자
근거 법령	• '정보통신망 이용촉진 및 정보보호 등에 관한 법률' 제48조의3
신고 기관	• 과학기술정보통신부 • 한국인터넷진흥원(KISA)
신고 기한	• 즉시
신고 기준	-
과태료	• 1천만 원 이하
신고 방법	• KISA 보호나라&KrCERT 홈페이지(**https://www.boho.or.kr** 또는 **https://www.krcert.or.kr**) > 침해사고 신고 > 신고하기 > 랜섬웨어 • 사이버민원센터 국번 없이 118

개인정보 유출 신고 절차

개인정보처리자가 개인정보를 유출한 경우에는 「개인정보 보호법」 제34조가 적용됩니다. 다만, 정보통신서비스 제공자 등은 「개인정보 보호법」 제39조의4가, 신용정보회사 등(상거래 기업 및 법인)은 「신용정보법」 제39조의4가 우선 적용됩니다.

※ 신용정보회사 등(상거래기업 및 법인): 개인정보보호위원회 등에 신고
※ 신용정보회사 등(상거래기업 및 법인을 제외한 전체): 금융위원회 등에 신고

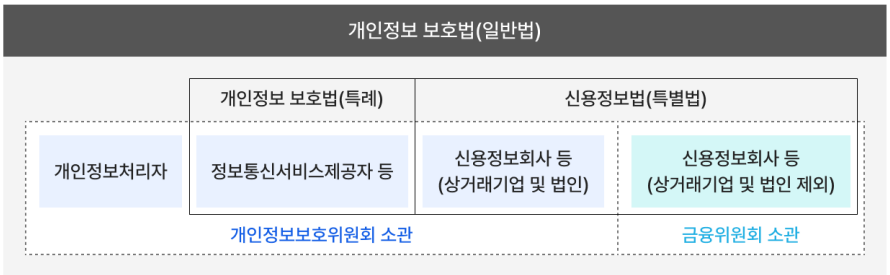

그림 21 개인정보 유출 관련 법 체계

표 6 개인정보 유출 신고 절차

신고 대상	• 개인정보처리자	• 상거래 기업 및 법인
근거 법령	• 「개인정보 보호법」 제34조	• 「신용정보의 이용 및 보호에 관한 법률」 제39조의4
신고 기관	• 개인정보보호위원회 • 한국인터넷진흥원(KISA)	• 개인정보보호위원회 • 한국인터넷진흥원(KISA)
신고 기한	• 72시간 이내	• 5일 이내
신고 기준	• 1천 명 이상의 정보 주체에 관한 개인정보가 유출 등이 된 경우 • 민감정보 또는 고유식별정보가 유출 등이 된 경우 • 개인정보처리시스템 또는 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대한 외부로부터의 불법적인 접근에 의해 개인정보가 유출 등이 된 경우 ※ 위 내용 중 어느 하나라도 해당하는 경우 신고하여야 함	• 1만 명 이상 신용 정보 주체의 개인신용정보가 유출(누설)된 경우
신고 내용	1. 정보 주체에의 통지 여부 2. 유출 등이 된 개인정보의 항목 및 규모 3. 유출 등이 된 시점과 그 경위 4. 유출 등에 따른 피해 최소화 대책 · 조치 및 결과 5. 정보 주체가 할 수 있는 피해 최소화 방법 및 구제 절차 6. 담당 부서 · 담당자 및 연락처	1. 신용정보주체에의 통지 여부 2. 유출(누설)된 개인신용정보의 항목 및 규모 3. 유출(누설)된 시점과 그 경위 4. 유출(누설) 피해 최소화 대책 · 조치 및 결과 5. 신용정보주체가 할 수 있는 피해 최소화 방법 및 구제 절차 6. 담당부서 · 담당자 및 연락처
과태료	• 3천만 원 이하	• 3천만 원 이하
신고 방법	• 인터넷 개인정보침해신고센터(**https://privacy.kisa.or.kr**) > 기업 · 공공 서비스 > 개인정보 유출 신고 > 유출신고 > 신고하기 • 사이버민원센터 국번 없이 118	

5 마무리

랜섬웨어 공격은 기업 및 다양한 조직과 개인에게 심각한 위협으로 작용합니다. 최근에는 고급 암호화 기술과 은닉 기술을 활용하여 탐지를 어렵게 만들고 있으며, 초기 랜섬웨어는 금전 요구에 그쳤지만 이제는 시스템 파괴와 데이터 갈취로 인해 사회적 안전까지 위협하고 있습니다.

그러나 보안 인식이 높아지고 인공지능과 기계 학습을 활용한 대응 기술도 발전하고 있습니다. 정부와 보안 기업은 랜섬웨어 및 사이버 침해 사고에 대응하기 위한 방안을 계속해서 개발하고 있습니다.

랜섬웨어로부터 우리의 소중한 정보자산을 보호하기 위해서는 기술적 이해와 사례를 분석하고, 종합적인 탐지, 예방, 대응책을 마련하는 것이 중요합니다.

NHN Cloud 보안 서비스

네트워크 보안
사용 권한이 없는 사용자의 네트워크 접속을 차단

DDoS Guard
외부로부터 DDoS 공격을 신속하게 탐지하고 차단

WEB Firewall
고객 클라우드 영역에 웹 방화벽이 구성되어 독립적인 운영 환경을 제공

Network Firewall
NHN Cloud 인프라의 안전한 보호를 위해 최적화된 네트워크 방화벽

취약점 점검
OS, 웹, 앱, 소스 코드 취약점 점검 및 가이드

App Security Check
애플리케이션에 대한 보안 취약점 검검 및 발견된 취약점에 대한 대응 방법 제공

Server Security Check
시스템에 대한 보안 취약점 점검 및 발견된 취약점에 대한 대응 방법을 제공

Security Advisor 무료
NHN Cloud 조직 및 프로젝트 자원의 보안 설정 상태 점검 및 권장 가이드 제공

위협 대응
외부 침입시도에 대해 클라우드 플랫폼 및 서비스 보호

Basic Security 무료
한국 리전을 이용하는 고객에게 제공하는 무료 보안 서비스

Security Monitoring
전문인력에 의한 외부 침입시도의 24시간 365일 보안 관제 서비스 제공

시스템 보안
시스템 및 데이터의 변조 및 유출 방지

Webshell Threat Detector 무료
시스템에 존재하는 웹 셸을 점검하고 발견된 웹 셸에 대한 대응 방법 제공

Vaccine
Trend Micro Deep Security 제품을 통해 악성코드로부터 이용자의 서버를 보호

애플리케이션 보안
안전한 API, 앱 보호

NHN AppGuard
모바일 애플리케이션의 코드 조작 방지

보안 컴플라이언스
보안 인증서 및 상세 가이드 제공

Security Compliance 무료
정보 보호 인증과 컴플라이언스에 대응할 수 있도록 보안 인증서와 상세 가이드를 제공

암호화
개인정보, 중요 데이터 암호화, 암호화 키 관리

Secure Key Manager
기밀 데이터를 중앙 집중적으로 관리하고, 인증을 통과한 클라이언트만 접근할 수 있도록 제어

통합 로그 관리
로그 보관, 이벤트 통합 모니터링, 위협 분석

SIEM
모든 보안 로그 수집 및 이벤트에 대한 종합적인 분석과 보안 위협 식별

엔에이치엔클라우드

13487 경기도 성남시 분당구 대왕판교로645번길 16 NHN 플레이뮤지엄

고객 센터: 1588-7967 I 이메일: support@nhncloud.com