Special Report

Ransomware

KISA 한국인터넷진흥원

CONsortium of CERT CONCERT

4차 산업 혁명의 시대를 살아가는 지금 사이버 공간은 어디라고 특정할 것도 없이 모든 공간에서 랜섬웨어에 의한 위협으로 몸살을 앓고 있다. COVID-19의 펜데믹과 함께 IT 환경의 급격한 성장과 인터넷 사용 대상의 확대를 기반으로 랜섬웨어 공격에 의한 피해 범위와 규모 역시 급격하게 증가하고 있다. 랜섬웨어에 의한 피해 규모는 2015년 3천8백억에서 2021년 23.6조원으로 약 6,200%가 급증할 것으로 전망이 되며, 2031년에는 우리나라 2021년 예산 558조의 약 56%에 달하는 312조를 넘어설 것으로 전망되고 있다. 랜섬웨어 공격은 금전적 거래를 주 목적으로 하고 있으며, 공격 시 확보한 정보의 유출을 볼모로 한 협박 등 기존의 사이버 공격과는 다른 특징을 보이고 있다. 특히 금전적 거래는 비트코인 등 익명성을 가진 가상화폐를 이용함으로써 공격자에 대한 추적이 어려우며, 지역적 제약 없이 인터넷이 되는 곳이라면 어디든 공격의 대상으로 삼고 있다는 점에서 그 위협이 매우 심각하다고 하겠다.

이런 상황에서 한국인터넷진흥원(KISA)과 한국침해사고대응팀협의회(CONCERT)는 각급 기업/기관의 정보보호 담당자들이 랜섬웨어에 대한 효과적인 대응전략을 수립할 수 있도록 돕기 위한 방안을 고민했으며, 그 일환으로 Special Report: Ransomware 편을 준비했다. 본 리포트 작성을 위해 KISA의 전문가들과 10개 기업의 CONCERT 회원사 보안담당자가 참여했으며, 두 달 간 일곱 차례의 편집회의를 거쳐 리포트를 완성했다.

본 리포트에는 랜섬웨어의 활동 동향과 기술적 이해를 돕기 위한 정보들이 담겨 있으며, 기업 보안담당자들을 대상으로 한 랜섬웨어 설문을 실시해 기업들의 실제 대응상황과 인식수준을 파악해 볼 기회도 가질 수 있었다. 아울러 시중에 출시되어 있는 이른바 '랜섬웨어 전문 솔루션'에 대한 기업 정보보호 담당자 입장에서의 고찰도 담아 놓았다.

모쪼록 이번에 제공되는 리포트가 기업의 체계적인 랜섬웨어 대응전략 수립에 조금이나마 참고할만한 자료로 활용될 수 있기를 기대한다.

편집위원

김창오(야놀자)	윤우희(에스케어)	김형기(카카오)
장석은(엔씨소프트)	안소희(ENKI)	김형준(현대오토에버)
박제석(안랩)	최병훈(신세계디에프)	이익준(KGC인삼공사)
심상현(CONCERT)	이동근(KISA)	

목 차

1. 랜섬웨어의 최근 동향 4

1.1 랜섬웨어 동향 및 시사점	1.1.1 대규모 랜섬웨어 공격 타깃이 된 대기업들 1.1.2 치솟는 협상금액 1.1.3 새로운 랜섬웨어의 출현 1.1.4 상품형 해킹툴을 통한 대규모 랜섬웨어 공격 수행 1.1.5 RaaS를 통한 랜섬웨어 체인 사업화 1.1.6 국가 지원 해킹 그룹 출현	4
1.2 랜섬웨어의 확산		7
1.3 랜섬웨어의 공격 벡터	1.3.1 RDP 공격 1.3.2 이메일 공격 1.3.3 소프트웨어 취약점 공격	9
1.4 랜섬웨어 공격 사례	1.4.1 국내 기업 랜섬웨어 공격 사례 1.4.2 해외 기업 랜섬웨어 공격 사례	15

2. 랜섬웨어에 대한 이해 17

2.1 랜섬웨어의 종류별 특징	2.1.1 Clop Ransomware 2.1.2 Darkside Ransomware 2.1.3 Sodinokibi Ransomware	17
2.2 랜섬웨어의 공격 시나리오	2.2.1 RDP 브루트포스 2.2.2 (다양한 사칭을 이용하는) 피싱메일 2.2.3 AD 서버 탈취 2.2.4 알려진 취약점 공격	30
2.3 랜섬웨어의 기술적 대응과 한계	2.3.1 암호화 방식의 원초적 문제 2.3.2 검증된 암호 알고리즘을 사용하지 않는 랜섬웨어	31

3. 기업 담당자의 눈으로 바라본 랜섬웨어 35

3.1 설문조사 개요 및 요약		35
3.2 세부 조사결과	3.2.1 랜섬웨어에 대한 인식 조사 3.2.2 랜섬웨어 피해 영향도 조사 3.2.3 랜섬웨어 대응능력(탐지, 치료 및 복구) 3.2.4 랜섬웨어 전망 및 예방	37
3.3 설문조사 총평		43

4. 랜섬웨어 방어 및 대응 전략 44

4.1 랜섬웨어의 관리적 대응 방안	4.1.1 랜섬웨어 감염대응을 위한 비상조직체계 4.1.2 랜섬웨어 대응 비상조직의 역할 및 책임 4.1.3 랜섬웨어 감염 예방 대책 4.1.4 랜섬웨어 감염시 신고절차 4.1.5 랜섬웨어 관리적 대응 체크리스트	44
4.2 랜섬웨어의 기술적 대응 방안	4.2.1 이메일 보안 대응 4.2.2 악성 웹사이트와 악성 광고 대응 4.2.3 웜을 통한 전파의 대응 4.2.4 사용자 환경의 기술적 대응	55
4.3 랜섬웨어의 감염 분석	4.3.1 최초 감염경로 분석 4.3.2 내부 조사단계 분석 4.3.3 내부 감염(Lateral Movement) 분석 4.3.4 감염 파일 분석	60
4.4 랜섬웨어 대응을 위한 투자 전략	4.4.1 랜섬웨어의 피해 복구 방안 4.4.2 대기업의 대응 전략 4.4.3 중·소기업의 대응 전략	67
4.5 랜섬웨어 공격 피해 최소화를 위한 사후 대응 전략	4.5.1 백업관리 정책 및 방법 4.5.2. 기업규모별 대응전략 4.5.3 랜섬웨어 피해예방을 위한 복구전략	75

5. 랜섬웨어 전용 솔루션에 대한 고찰 86

5.1 랜섬웨어 기본 점검항목	5.1.1. 사용자 환경(End-point) 설치형 랜섬웨어 대응 솔루션 체크항목 5.1.2. 중앙처리형 랜섬웨어 대응 솔루션 체크항목	87
5.2 랜섬웨어 대응 솔루션들		89

■ 편집 후기 ----- 91

■ Appendix. 설문조사 항목 ----- 93

1. 랜섬웨어의 최근 동향

1989 년 12 월 Joseph L. Popp 를 통해 작성 배포된 첫 번째 랜섬웨어 공격을 시작으로 2021년 현재 랜섬웨어 공격은 점차 증가하고 있으며 그 피해규모 또한 날로 커지고 있다. 글로벌 랜섬웨어 감염 피해 금액은 2021년 말 23조6천억원에 이를 것으로 예상이 되며, 지금으로부터 10년 후인 2031년에는 약 312조7천억으로 피해금액이 천문학적 규모로 늘어날 것으로 예측된다.

년도	2015	2021	2026	2031
피해금액	3천8백억	23조6천억	84조3천억	312조7천억

표 1. 글로벌 랜섬웨어 피해금액 (출처 : Cyber Crime Magazine 2021)

국내 역시 랜섬웨어 공격에 의한 피해 신고 건수가 증가하고 있으며, 랜섬웨어 공격자에 의한 협상 요구 금액 및 실질적 기업의 피해 금액 또한 기하급수적으로 증가하고 있다.

년도	2018	2019	2020	2021
신고건수	22건	39건	127건	55건
랜섬웨어 평균 피해 협상 (건당)	$41,198	$84,116	$154,108	$220,298

표 2. 최근 3년간 랜섬웨어 침해사고 신고 현황 (출처 : 과학기술정보통신부/ COVEWARE 2021)

랜섬웨어는 금전적인 요구, 즉 몸값(Ransome)을 요구하는 악성 프로그램을 지칭한다. 초기 랜섬웨어는 피해자의 정보자산에 접근 후 암호화를 수행할 뿐, 피해자 정보를 직접 훔치지는 않았지만, 최근 랜섬웨어들은 기업 및 피해자와의 협상력을 높이기 위해 피해 대상의 개인정보나 중요 및 기밀정보를 유출하고 탈취한 정보를 볼모로 다크웹에 단계적으로 공개하는 등 더욱 악질적 협상 방법으로 진화하고 있다.

2021년 COVEWARE에서 조사한 바에 의하면 랜섬웨어의 평균 협상 금액은 2019 년 건당 84,116 달러, 2020년 154,108달러, 2021년 220,298달러로 매년 2배 이상씩 커지고 있다. 특히 2019년부터 2020년으로 넘어오면서 최다 협상 금액이 500만 달러에서 1,000만 달러로 두 배 이상 증가되었으며, 이는 랜섬웨어로 인한 금전적 피해 규모가 점점 더 커지고 있다는 것을 의미한다. 개인을 대상으로 하던 공격이 이제는 더 큰 대가를 얻어내기 위해 기업과 공공의 안전을 위협하는 방향으로 그 공격 범위를 확대하고 있다.

1.1 랜섬웨어 동향 및 시사점

최근 랜섬웨어 동향을 살펴보면 공격자들은 큰 돈을 목적으로 대기업을 목표로 APT 공격 등 다양한 해킹 기술을 이용한 공격을 수행하고 있다. 랜섬웨어 공격의 동향과 특징들을 살펴보고 어떠한 공격들이 우리의 생활을 위협하는지 알아보자.

1.1.1 대규모 랜섬웨어 공격 타깃이 된 대기업들

최근 랜섬웨어 공격자는 사업분야를 가리지 않고 피해 범위와 규모에 더 집중하며, 최근 대기업의 대규모 랜섬웨어 피해가 급증하고 있다. 공격자들은 규모가 큰 기업에 침투하기위해 노력하고 있고 최근 2년 동안 외국계 글로벌 기업인 Garmin, Canon, Campari, Capcom, Foxconn, Colonial Pipeline 및 AXA 와 같은 기업들이 큰 피해를 당했으며 많은 한국계 글로벌 기업들도 랜섬웨어의 타깃이 되었다. 공격자들은 앞으로도 큰 수익을 얻기 위해 대기업들을 지속적으로 표적화 할 가능성이 높다. 랜섬웨어 공격자는 일반 개인들보다 보상 가능성이 높은 기업을 선호한다. 뿐만 아니라, 최신 랜섬웨어 그룹은 암호화 전 주요 데이터를 유출한 후 다크웹 게시 위협을 미끼로 협상력을 확보한다. 피해 기업은 기업 평판 손상부터 주주 관계, 규제 기관의 벌금에 이르기까지 모든 종류의 리스크를 고려해야 하므로, 랜섬웨어 공격자와 불리한 조건에서 협상을 하게 되는 경우가 많다.

1.1.2. 치솟는 협상 금액

공격자가 대기업 공격에 성공했을 때 협상 금액의 수준을 새로운 차원으로 끌어 올리고 있다(표 2 참고). 랜섬웨어의 평균 복호화 협상 비용은 2019년 약 8만 달러에서 2020년 평균 약 15만 달러로 상향됐다. 특히 2020년 대형 글로벌 기업 랜섬웨어 침해시에는 협상금액이 수백만 달러로 올라간 정황이 매체를 통해 보도된 바 있다. 보안 전문가들은 특히 Maze, DoppelPaymer 및 RagnarLocker가 평균 1백만 달러에서 2백만 달러 사이의 협상금액을 요구하는 위험한 랜섬웨어 패밀리라는 사실을 경고하고 있다.

1.1.3 새로운 랜섬웨어의 출현

대기업들은 Windows, Linux 서버 시스템을 서비스 운영 목적으로 사용하므로 최근 랜섬웨어 공격자들은 Windows 뿐만 아니라 Linux 플랫폼을 대상으로 한 랜섬웨어 버전을 출시하고 있다. Defray777, Mespinoza, Babuk, Nephilim 및 Darkside는 이미 Linux 플랫폼 공격 랜섬웨어를 출시했고, Sodinokibi 랜섬웨어는 Unix 랜섬웨어 버전을 2021년 7월 출시했다.
Linux 플랫폼 공격은 VMware 및 클라우드 하이퍼바이저를 공격의 목표로 한다.
VMware의 vSphere 및 vSAN 제품 라인에서 문제를 진단하는 Skyline Health Diagnostics 기

능을 악용한 대형 공격이 보고된 바 있으며, 여기에 Linux 플랫폼 공격은 대규모 정보가 저장된 NAS 또는 대규모 Storage를 공격하는 랜섬웨어로 발전하고 있다.
최근 랜섬웨어 공격은 APT 공격과 결합된 공격자 주도의 정찰 후, 대규모 파괴 행위를 수행한다. 인증서버 공격을 통한 빠른 확산과 백업 시스템 공격을 통한 복구 불능의 상태로 피해자를 몰아넣고 있다. Microsoft Cybersecurity Field CTO였고 SeucirtyCurve의 설립자인 Diana Kelley는 CyberSecurity.News와의 인터뷰에서 “백업 시스템을 파괴하게 되면 기업은 비즈니스 데이터를 확보하기 위해 공격자와 협상을 할 수밖에 없는 상황에 놓이게 된다.”라고 최근 랜섬웨어 공격의 치밀함을 밝혔다.

1.1.4 상품형 해킹 툴을 통한 대규모 랜섬웨어 공격 수행

Trickbot, Qakbot 및 Dridex와 같은 상용 멀웨어를 활용하는 랜섬웨어 공격자는 네트워크에 대한 초기 액세스를 확보해 Big Game Hunting 캠페인을 수행한다. 공격자들은 조직적이며 다양한 해킹기술을 보유하고 있을 뿐만 아니라, 투입조직, 관찰조직, 전파조직과 협상조직 등으로 전문 조직을 구성해 오랜 기간 잠복해 대규모 피해를 양산한다. 기업으로 유포된 악성코드들을 지속적으로 업데이트해 보안 솔루션의 탐지를 회피하는 기술을 활용하고 있으며, 사용되는 해킹 툴 또한 트로이안목마, 크리덴셜스터핑, 보안솔루션 회피기술, 악성코드 난독화기술, 심층정찰기술, 악성코드 업데이트 기술, 봇 네트워크 관리 기술들이 총동원되고 있다.

1.1.5 RaaS를 통한 랜섬웨어 체인 사업화

랜섬웨어 개발자가 사용하는 비즈니스 모델로, 소프트웨어 개발자가 SaaS 제품을 임대하는 것과 동일한 방식으로 랜섬웨어를 임대한다. RaaS를 활용하면 배경지식이 많지 않은 사람도 서비스에 가입하는 것만으로 랜섬웨어 공격을 손쉽게 수행할 수 있다. RaaS 키트는 기술 지원, 추가 번들 제공, 사용자 리뷰, 포럼 및 일반적인 SaaS 공급자가 제공하는 것과 유사한 형태의 서비스를 제공하는데, 다크웹 마켓에서 월 40달러 정도의 가격으로 서비스를 제공함으로써 많은 초보 사용자들이 쉽게 랜섬웨어 키트를 활용해 공격을 시작할 수 있다. 공격 대상에 따라 RaaS 서비스와 같이 해커를 고용할 수도 있으며, 대규모 공격 감행 후 15% 정도의 수수료를 지불하는 서비스형 해킹 공격도 제공되고 있다.

1.1.6 국가 지원 해킹 그룹 출현

국가가 후원하는 해킹그룹들도 대규모 해킹에 관심을 보이고 참여하기 시작했다. Lazarus 및 APT27과 같은 그룹은 국가 후원 해킹단체로 추정되며, 대규모 자금을 투입해 알려지지 않은 취약점 공격 및 신규 해킹 기술을 통해 기업 및 국가단체를 공격하여 금전보상 및 주요정보를 취득하는 수단으로 랜섬웨어를 활용하고 있다.

Darkside는 러시아와 동유럽에 기반을 두고 활동했던 사이버범죄 조직으로, 2021년 5월 미국 대형 송유관 운영사인 콜로니얼 파이프라인을 공격했는데, 이 공격으로 콜로니얼의 운영이 중단되면서 미 남동부 일대 석유 공급에 큰 차질을 빚어 세계적으로도 큰 이슈가 됐다. 이 조직 또한 RaaS를 운영하고 있으며 5개의 계열조직화 된 각 클러스터를 통해 공격 활동을 벌이고 있다.

REvil 역시 Darkside와 마찬가지로 러시아 우호 조직을 표적으로 삼지 않기 때문에 러시아에 기반을 둔 것으로 추정된다. 이들은 과거 해커집단인 GandCrab과 관련이 있는 것으로 보이며 GandCrab의 코드와 유사성이 있는 것으로 파악되고 있다. 2021년 7월 단말관리 소프트웨어인 Kaseya를 해킹해 수천대의 시스템을 감염시킨 것도 3rd Party 취약점을 이용한 악성코드 배포였으며 그 배후에 대규모 해킹 조직이 존재함을 추정하고 있다.

1.2 랜섬웨어의 확산

최근에는 COVID-19 팬데믹으로 인한 재택근무 증가로 인해 랜섬웨어 감염률이 2배 이상 급증했다. 이러한 공격의 주된 이유는 재택 근무 과정에서 사이버 보안 조치가 부족해 감염률이 증가했기 때문으로 분석된다. 실제로 외부사용자를 위한 VPN G/W 장비의 취약점 공격 및 내부 접속 인증정보 유출이 발생하고 있고 안전하지 않은 재택 네트워크 환경에서 악성 URL접속을 통한 악성코드 감염 및 RDP 공격이 발생하고 있다. 해킹 조직은 이러한 경로로 감염된 단말을 통해 내부 주요 시스템에 접근하고 대규모 해킹을 발생시키고 있다.

2021년 순위	랜섬웨어 구분	점유율	2020년 순위
1	Sodinokibi	14.20%	-
2	Conti V2	10.20%	4
3	Lockbit	7.50%	6
4	Clop	7.10%	변종 신규진입
5	Egregor	5.30%	-3
6	Avaddon	4.40%	3
7	Ryuk	4.00%	-4
8	Darkside	3.50%	신규진입
9	Suncrypt	3.10%	-1
9	Netwalker	3.10%	-5
10	Phobos	2.70%	-1

표3. 랜섬웨어 종류 및 시장 점유율 (출처 : Cyber Crime Magazine 2021)

표 3은 2020년과 2021년에 전세계적으로 유행한 랜섬웨어들의 활동 지표를 나타내고 있다. 전세계적으로 최대 피해를 유발한 TOP 3 랜섬웨어로는 Sodinokibi, Conti, Lockbit 등이 있다. 최근의 랜섬웨어는 트로이목마와 같은 해킹 툴과 같이 접목되어 기존의 ATP 공격과 유사한 경향을 보이고 있다. 실제로 내부 정찰 및 공격 확산을 통해 기업 대상의 대규모 피해를 이끌어내는 해킹 그룹 주도의 공격이 늘어나고 있으며, 이들 그룹 모두 내부 정찰 및 랜섬웨어 공격 확산을 위해 트로이목마, 크리덴셜스터핑, 보안솔루션 회피기술, 악성코드 난독화기술, 심층정찰기술, 악성코드 업데이트기술, 봇 네트워크 관리기술 등을 복합적으로 사용하고 있다. 랜섬웨어와 관리 봇은 아래의 표4와 같은 상관 관계를 가지고 있다.

Bot	Ransomware
Trickbot	Ryuk, Conti, REvil, RansomExx
Quakbot	ProLock, Egregor, DoppelPaymer
Dridex	DoppelPaymer
IcedID	RansomExx, Maze, Egregor
Zloder	Ryuk, Egregor
SDBBot	Clop
Buer	Maze, Ryuk
Bazer	Ryuk

표4. 랜섬웨어 배포 및 관리에 사용되는 해킹 툴 (출처 : Proofpoint 2021)

랜섬웨어 공격 대상 OS 플랫폼은 Windows 플랫폼이 대부분이지만, 최근 랜섬웨어는 OS를 가리지 않고 대규모 침해사고를 유발하기 위해 MacOS, Androiod, iOS 및 Linux/Unix에 이르기까지 감염 범위를 넓혀가고 있는 상태다.

플랫폼 종류	Windows	MacOS	Android	iOS	Linux
피해분포	84%	7%	5%	3%	1%

표5. 랜섬웨어 플랫폼 별 공격현황 (출처 : PupleSec 2021)

공격자들이 기업을 랜섬웨어에 감염시키기 위해 사용한 공격벡터를 살펴보면 RDP 공격, 이메일을 통한 악성코드 전파, 소프트웨어 취약점 공격 등이 가장 주된 공격 벡터로 조사됐다.

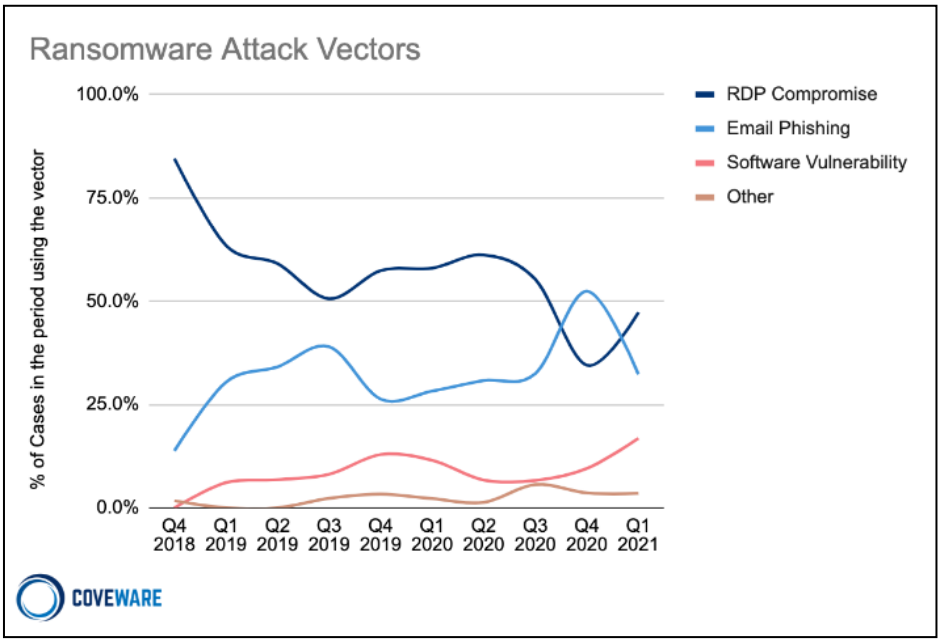


그림 1. 랜섬웨어 공격 벡터 현황 (출처 : Coveware 2021)

1.3 랜섬웨어의 공격 벡터

1.3.1. RDP 공격

RDP 공격은 Shodan과 같은 사이트를 이용해 외부에 공개되어 있는 RDP 서비스를 목표로 공격하는 것이다. 원격 접속으로 외부에 잘못 노출된 서버에 연결한 후, 내부의 Active Directory 서버 등을 통해 내부 전체 시스템을 대상으로 대규모 악성코드 전파를 수행하는 사례가 발생하고 있다.

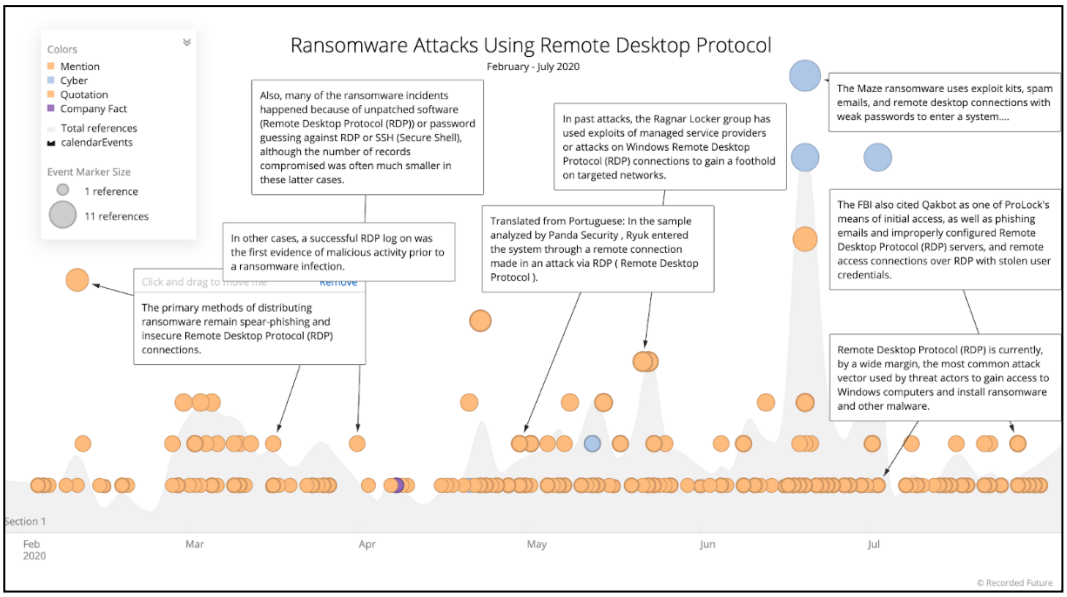


그림 2. 원격 데스크탑 공격 현황 및 주요 이슈 (출처 : Recorded Future 2020)

웹 서비스를 제공하기 위한 웹 서버 중 외부로 노출된 RDP 및 SSH 서비스는 Shodan과 같은 사이트를 통해 쉽게 확인이 가능해 내부 시스템의 침투를 통한 악성코드의 전파 통로로 활용되고 있다.

아래 그림 3의 Shodan 인텔리전스를 통해 나타난 정보를 보면, 전세계 3백만대 이상의 RDP 서비스가 대외적으로 노출되어 있으며, 해커들은 이런 시스템에 자격증명 대입 공격을 통해 시스템에 접속하게 된다.

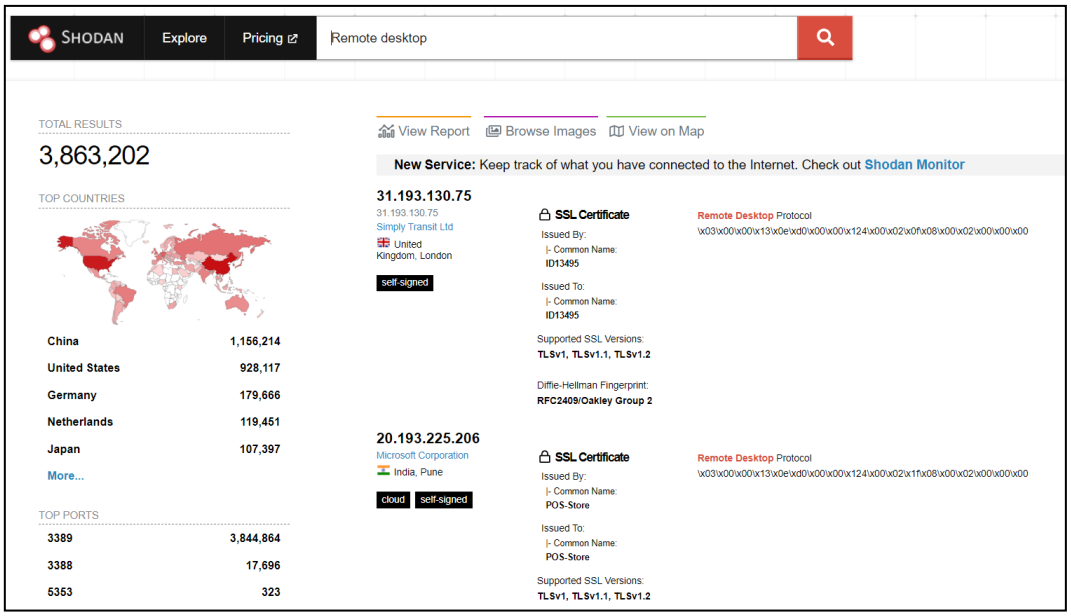


그림 3. 외부로 공개된 원격 데스크톱 서비스 현황 (출처 : Shodan 2021)

해커그룹들은 다크웹 마켓에서 최신 VPN 접속 정보 및 RDP 접속 정보를 판매하고 있으며, RaaS 이용자들은 구매한 정보를 이용해 기업 내부 네트워크에 침투하고 있다.

1.3.2. 이메일 공격

이메일 내 첨부문서 또는 악성링크를 통한 랜섬웨어 감염 또한 주요 공격벡터로 알려져있다. 해외 보안회사의 설문조사를 보면 랜섬웨어 감염의 가장 주요한 요인으로 이메일 공격을 꼽고 있으며, 다음으로는 직원의 보안 의식 부족과 악성 웹 사이트를 꼽았다.

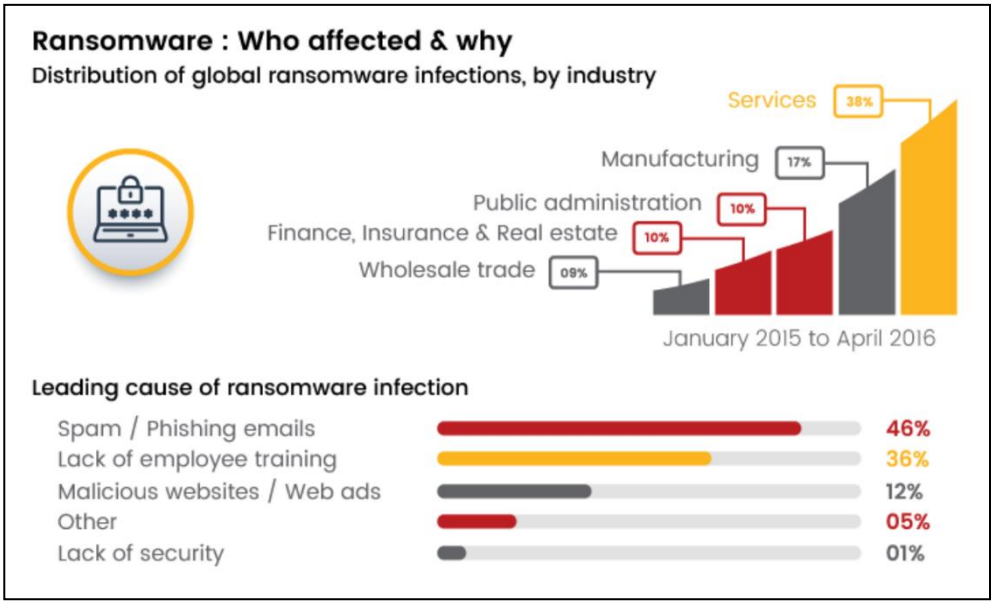


그림 4. 랜섬웨어의 공격 벡터

(출처 : https://www.briskinfosec.com/blogs/blogsdetail/Will-your-backups-protect-you-against-ransomware-)

해커들은 사용자를 기만하기 위해 국내에서는 한컴오피스의 취약점을 이용한 공격이 유행하고 있고, 해외에서는 Office 및 PDF를 통한 공격이 주로 발생하고 있다.

가. 관심형 문서를 통한 취약점 활용 사례

한컴오피스의 취약점을 통해 숨겨진 사용자 알림없이 자바스크립트를 호출하는 공격 유형.

그림 5. 한글파일 취약점 기반 자바스크립트 호출 (출처 : 안랩)

나. 관심 유도 문서를 통한 사용자 클릭 유도 사례

문서 내 숨겨진 객체를 사용자가 클릭하면 실행하게 만드는 공격 방법.

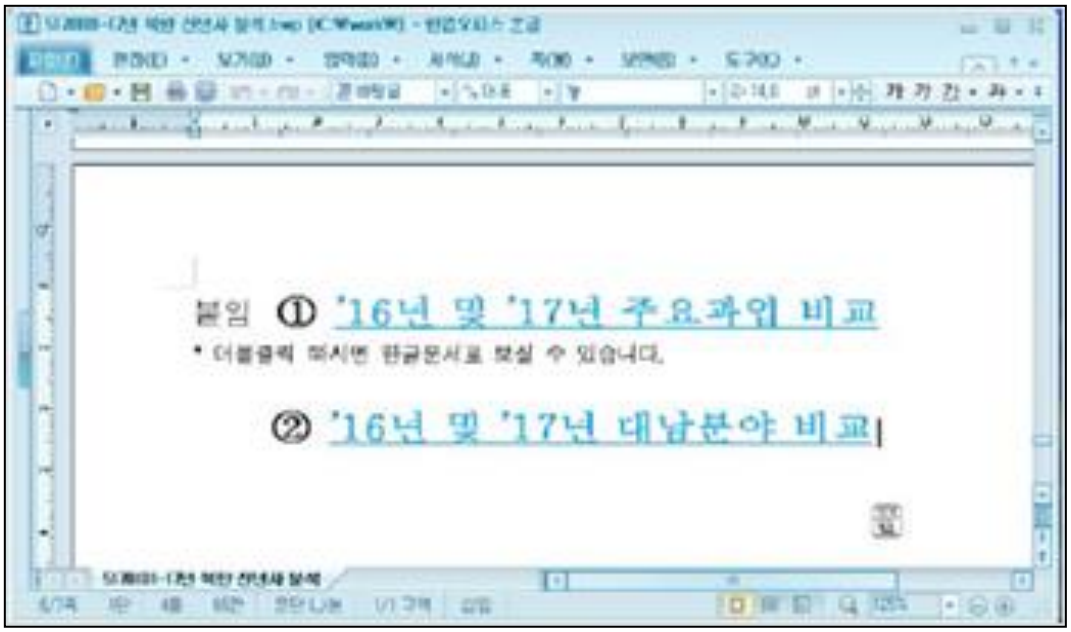


그림 6. 문서 링크를 통한 객체 호출 유도 (출처 : 안랩)

다. 관심 유도 문서를 통한 사용자 클릭 유도 사례

계약 서명 관리 클라우드 시스템 문서로 위장해 사용자 매크로 실행을 유도하는 공격 방법.
매크로 실행 시 PowerShell 기반의 공격이 발생함.

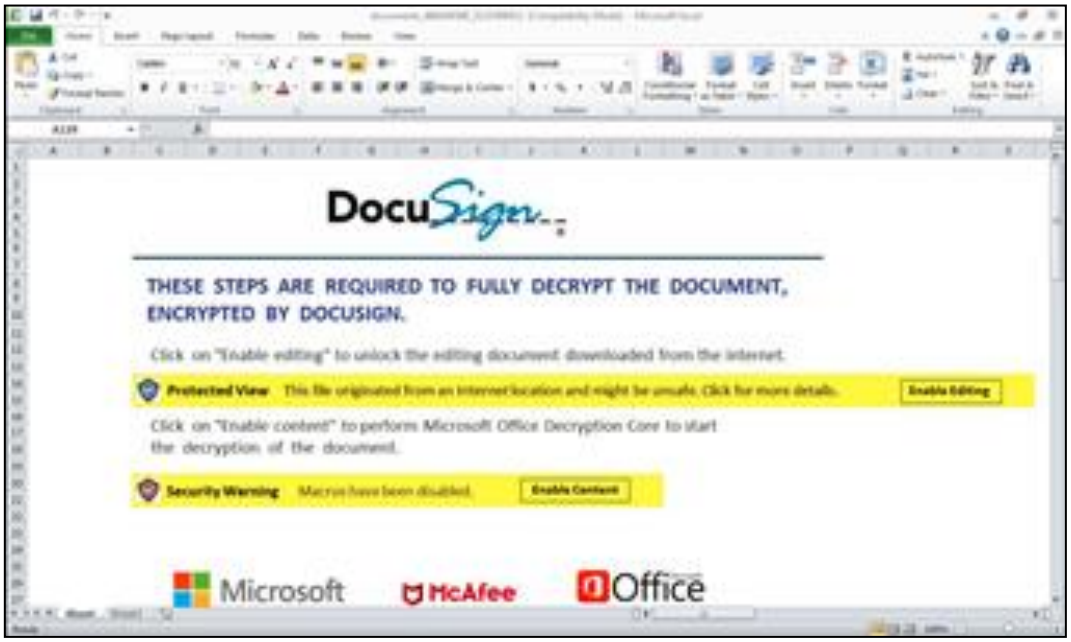


그림 7. Qakbot 미끼 문서 – 매크로 실행 유도 엑셀파일 (출처 : ProofPoint 2021)

라. 입사 지원서 위장 공격 사례

입사지원서 파일을 가장한 링크파일을 통해 파워쉘 또는 자바스크립트를 호출하는 공격 유형.

그림 8. 한글파일 위장 링크 파일 (출처 : 안랩)

마. 미리보기 유도 클릭 유도 사례

송장 유형으로 전송되어 사용자가 내용을 보기 위해 매크로를 실행하도록 유도하는 공격 방법.

그림 9. Trickbot 미끼 문서 – 매크로 실행 유도 엑셀파일 (출처 : ProofPoint 2021)

바. 미리보기 유도 클릭 유도 사례

송장 유형으로 전송된 엑셀파일, 문서 잠금 해제를 위해 매크로 실행을 유도하는 공격 방법.

그림 10. Dridex 미끼 문서 – 매크로 실행 유도 엑셀파일 (출처 : ProofPoint 2021)

사. 브라우저 업데이트 유도 사례

사용자에게 브라우저 및 웹 어플리케이션 업데이트를 요청하는 악성 URL을 통해 악성코드 다운로드 및 실행 유도

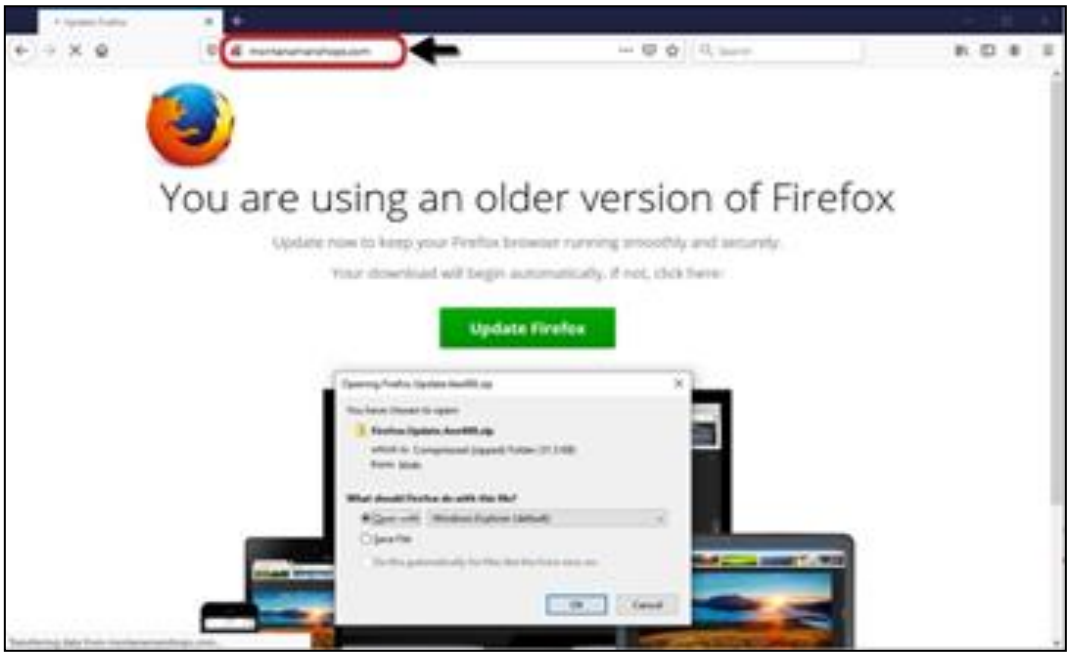


그림 11. Fake 업데이트 캠페인 사례 (출처 : ProofPoint 2021)

1.3.3. 소프트웨어 취약점 공격

2019년 말부터 COVID-19으로 인해 재택근무가 늘어나게 됐고, 이러한 환경의 변화에서 VPN 소프트웨어의 사용이 급격히 늘어났으며, 이로 인해 VPN 취약점을 이용한 대규모 랜섬웨어 공격이 늘어나게 됐다. 2019 년 여름 이후 Pulse Secure, Palo Alto Networks, Fortinet, Citrix, Secureworks 및 F5를 비롯한 글로벌 VPN 장비 들로부터 다양한 취약점이 공개됐다. 이러한 취약점은 재택근무를 지원하는 기업의 공격 벡터로 활발히 활용되고 있다.

해커들은 취약점을 보유하고 있는 VPN 접속 정보를 다크웹 마켓을 통해 구매하고 취약한 패스워드가 설정된 RDP 접속을 통해 내부 시스템을 침입하는 방법을 사용하고 있다.

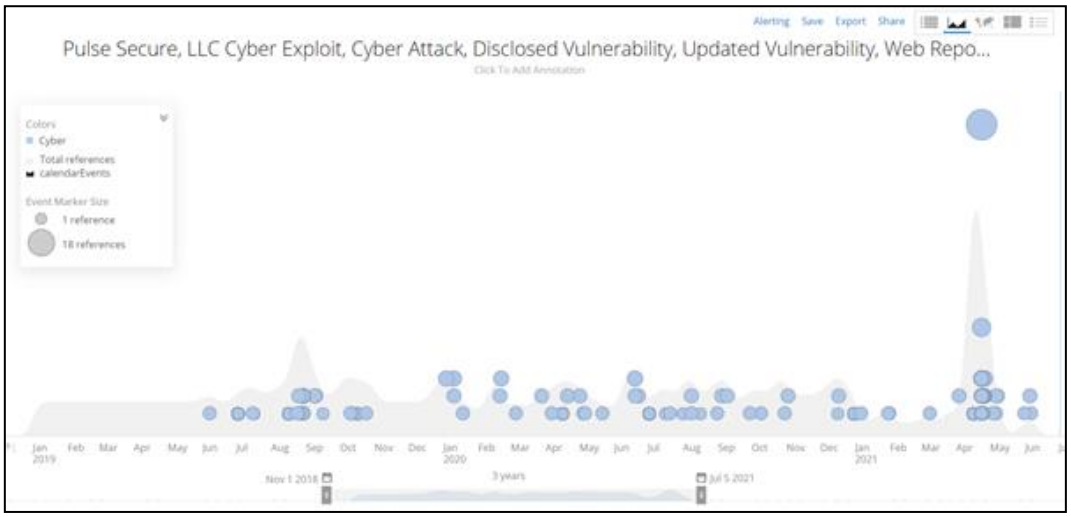


그림 12. Pulse Secure 취약점 관련 이벤트 현황 (출처 : Recorded Future 2021)

1.4 랜섬웨어 공격 사례

앞서 언급했듯이 2020년부터 랜섬웨어 공격은 규모가 큰 기업을 대상으로 발생되고 있으며, 협상금액 또한 천문학적으로 늘어나고 있다. 국내의 기업들도 피해 기업이 될 수 있다는 전제로 랜섬웨어 공격에 대비하기 위한 보안 조치의 수행이 필요하다.

1.4.1. 국내 기업 랜섬웨어 공격 사례

뉴스매체를 통해 알려진 국내 랜섬웨어 감염 사례를 살펴보면 2020년 이전은 보안수준이 낮은 중소 제조사나 서비스업 기업을 대상으로 랜섬웨어 공격이 이루어졌고 협상금액이 현재보다는 적은 금액을 요구했다. 2020년부터는 보안수준이 높은 대기업군이 공격대상에 포함되고 대형 피해사례들이 보고되고 있다. 대기업의 경우 보안 수준이 높은 본사 보다 보안 수준이 약한 해외 지점을 주로 겨냥하였다.

1.4.2. 해외 기업 랜섬웨어 공격 사례

해외 랜섬웨어 감염 사례를 살펴보면 2019년부터 소규모 공격이 아닌 APT형 공격이 늘어나고 있는 것을 알 수 있다. 상대적으로 보안 수준이 낮은 병원 또는 지자체를 대상으로 한 공격이 일어났고 2020년 부터 국내 사고와 비슷하게 대기업 또는 기간산업을 대상으로 한 공격이 발생하고 있다. 3rd Party 취약점을 이용해 다수의 기업을 동일한 공격 기법으로 공격하는 사례도 발생했다. 취약점이 패치 되지 않은 기업을 공격해 내부의 주요시스템을 점거하고 수많은 시스템을 한꺼번에 감염 시키는 APT형 공격과 함께 합의금으로 천문학적 금액을 요구하는 해킹그룹의 주도적인 랜섬웨어 공격 캠페인이 큰 사회적 문제로 대두되고 있다.

발생시기	피해기업	랜섬웨어 공격그룹	피해금액
2021년 3월	ACER	Revil	USD $50M
2021년 4월	QUANTA	Revil	USD $50M
2021년 4월	NBA	Babuk	Unknown
2021년 5월	AXA	Avaddon	Unknown
2021년 5월	COLONIAL PIPELINE	DarkSide	USD $5M
2021년 5월	BRENNTAG	DarkSide	USD $4.4M
2021년 6월	JBS FOODS	Revil	USD $11M

표6. 글로벌 랜섬웨어 공격 현황 (출처 : Touro College Illinois 2021)

2. 랜섬웨어에 대한 이해

랜섬웨어(Ransomware)란 운영체제가 설치되어 있는 자산에 존재하는 파일을 암호화 함으로써 사용할 수 없게 만드는 악성코드를 말한다. 랜섬웨어 종류별로 파일 암호화 방법, 감염 대상, 감염 자산에 미치는 영향 등이 다르며 공격자, 공격 그룹, 피해 대상에 따라 요구하는 금액도 모두 다르다.

2.1. 랜섬웨어의 종류와 특징

랜섬웨어의 종류에는 국내를 대상하는 Clop Ransomware를 포함하여 RaaS(Ransomware as a Service)형태로 제공되는 형태 등 다양한 종류의 랜섬웨어가 있다.

RaaS는 사용자가 원하는 악성코드를 맞춤 제작해 판매 및 제공 하는 서비스로, 악성코드를 통해 사용자가 금전적 이익을 취할 경우 악성코드 제작자와 이익을 공유하는 방식의 서비스를 의미한다. RaaS를 이용하는 대표적인 랜섬웨어는 케르베르(Cerber), 갠드크랩(GandCrab), 소디노키비(Sodinokibi) 등이 있다. 랜섬웨어 제작자 Darksupp는 공격 대상을 제한하는 특징을 가지고 있으며, 제휴자 및 병원, 학교, 대학, 비영리 단체, 공공 단체는 공격 대상에서 제외했다. 이는 추후 발생하게 될 법의 처벌을 고려한 것으로 추정된다.

2.1.1. Clop Ransomware

2019년부터 국내를 대상으로 유포되기 시작한 랜섬웨어로, 러시아 정부의 지원을 받는 것으로 추정되는 TA505 그룹이 배후로 알려졌으며, 국내의 다양한 기업을 공격 대상으로 한다. 주로 AD(Active Directory) Server를 사전 장악 후 랜섬웨어를 유포한다. 2020년 12월 이랜드 그룹이 Clop 랜섬웨어 감염되어 피해를 입었으며, Clop 랜섬웨어는 정상파일로 위장하기 위해 그림 13과 같이 디지털서명 정보를 가지고 있는 특징이 있다.

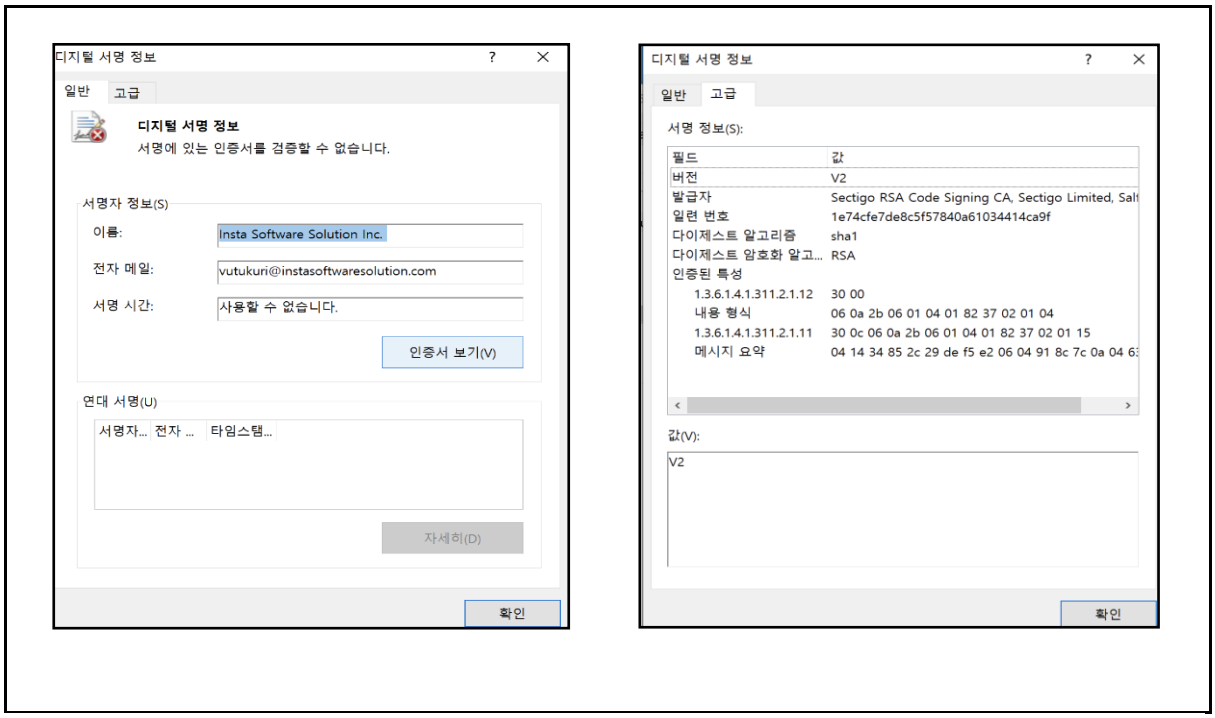


그림 13. Clop Ransomware의 디지털 서명 정보

Clop 랜섬웨어는 내부 암호화시 다중 스레드를 이용해 감염을 진행하며 그림 14에서 보는 것과 같이 감염에서 제외되는 확장자 정보를 가지고 있다. 감염된 파일의 재 감염을 막기위해 확장자에 CLLP도 포함되어 있다.

```
if ( sub_402B80(String1, CI0P) )
  return 1;
if ( sub_402B80(String1, OCX) )
  return 1;
if ( sub_402B80(String1, DLL) )
  return 1;
if ( sub_402B80(String1, EXE) )
  return 1;
if ( sub_402B80(String1, SYS) )
  return 1;
if ( sub_402B80(String1, LNK) )
  return 1;
if ( sub_402B80(String1, IOC) )
  return 1;
if ( sub_402B80(String1, INI) )
if ( sub_402B80(String1, MSI) )
  return 1;
if ( sub_402B80(String1, CHM) )
  return 1;
if ( sub_402B80(String1, HLF) )
  return 1;
if ( sub_402B80(String1, LNG) )
  return 1;
if ( sub_402B80(String1, TTF) )
  return 1;
if ( sub_402B80(String1, CMD) )
  return 1;
if ( sub_402B80(String1, BAT) )
  return 1;
result = sub_402B80(String1, CLLP);
if ( result )
```

그림 14. Clop Ransomware의 감염 제외 확장자(16종)

Clop 랜섬웨어에는 감염에서 제외되는 파일 및 디렉토리명을 다음의 코드값으로 저장하고 있다.

0x7A53F792 (AUTOEXEC.BAT)	0x45575934 (BOOT.INI)	0xFA12254F (Shphos)	0xFA747F45 (Recovery)	0xFA9269AE (BOOTMGR)
0xEA932256 (NTLDR)	0x917FE531 (BOOTSECT.BAK)	0xD6452416 (DESKTOP.INI)	0xE2C4812A (NTUSER.DAT.LOG)	0x6932F547 (PerfLogs)
0x58CAE791 (Application Data)	0x55B2AC88 (System Volume Information)	0x28B5FD61 (Tor Browser)	0xA932103 (-)	0x8916CC4 (AppData)
0xE892B59F (Windows)	0xB890E4CF (Packages)	0xB7E0EDC0 (Microsoft)	0x9663BE08 (recycle.bin)	0x8A53E4D9 (Chrome)
0x89D322CE (AhnLab)	0x71ADF2E1 (INetCache)	0x7933A751 (WINNT)		

표 7. 감염에서 제외되는 파일(23종)

Clop 랜섬웨어에는 암호화 대칭키를 감염된 파일의 하단에 포함하고 있으며, 내부 소스 코드에 하드코딩 되어있다.

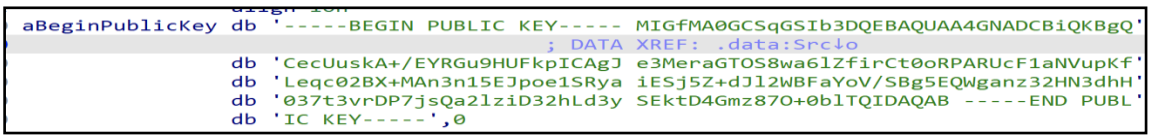


그림 15. 암호화 대칭키의 저장

Clop 랜섬웨어는 감염 시 다음과 같은 랜섬노트가 생성되며, 공격자들과 협상을 진행하지 않으면 공격자들은 탈취한 데이터를 업로드한다.

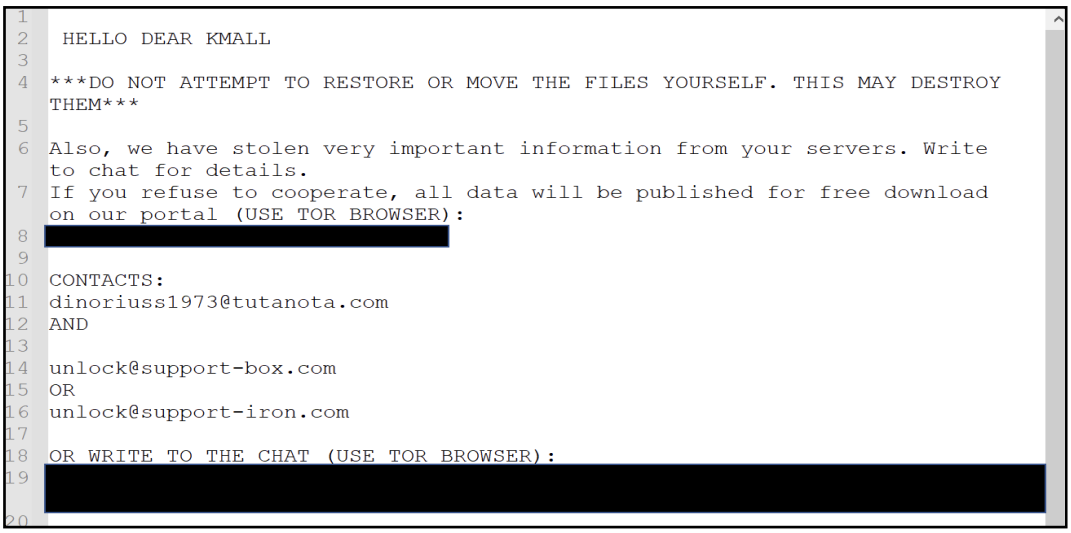


그림 16. 랜섬노트명 : README_README.txt

(CLOP 정보공개 이미지 출처 : https://therecord.media/ukrainian-police-arrest-clop-ransomware-members-seize-server-infrastructure/)

2.1.2. Darkside Ransomware

Darksupp(DarkSide Ransomware)는 2020년 8월부터 유포되었으며 RaaS(Ransomware as a Service)형태로 제공중에 있다. 해당 랜섬웨어의 특징은 다음과 같다.
Darkside 랜섬웨어 내부에는 안티바이러스 제품군 탐지 우회 및 분석 방해를 위해 중요 문자열 모두가 자체구현 암호 알고리즘을 통해 암호화되어 있으며, 중요 문자열 복호화는 2단계를 거쳐 진행된다.

STEP 1. 키 생성 단계

하드 코딩된 초기 테이블 값을 이용하여 키 테이블을 생성한다.

```
v3 = 240;
v4 = *key_table1;
v5 = key_table1[1];
v6 = key_table1[2];
v7 = key_table1[3];
do
{
  *&key_410ABE[v3 + 12] = v4;
  *&key_410ABE[v3 + 8] = v7;
  *&key_410ABE[v3 + 4] = v5;
  *&key_410ABE[v3] = v6;
  v4 -= 269488144;
  v7 -= 269488144;
  v5 -= 269488144;
  v6 -= 269488144;
  v3 -= 16;
}
while ( v3 >= 0 );
v8 = 0;
v9 = 0;
v10 = 0;
do
{
  while ( 1 )
  {
    LOBYTE(result) = key_410ABE[v9];
    LOBYTE(v8) = result + *(key_table2 + v10) + v8;
    HIBYTE(result) = key_410ABE[v8];
    ++v10;
    key_410ABE[v8] = result;
    key_410ABE[v9] = HIBYTE(result);
    if ( v10 >= size )
      break;
    LOBYTE(v9) = v9 + 1;
    if ( !v9 )
      return result;
  }
  v10 = 0;
  LOBYTE(v9) = v9 + 1;
}
while ( v9 );
return result;
```

그림 17. 키 생성 단계

STEP 2. 문자열 복호화

첫번째 단계에서 생성된 키 테이블을 이용해 아래 그림과 같은 알고리즘을 통해 문자열을 복원한다.

```
int idx_1; // edx
int idx_2; // ebx
_BYTE *v5; // edi
int num_1; // eax
char num_2; // ch
char result; // al

dword_410CCE = 0;
dword_410CD2 = 0;
qmemcpy(byte_410BBE, key_410ABE, 0x100u);
idx_1 = 0;
idx_2 = 0;
v5 = (a1 - 1);
num_1 = 0;
do
{
  LOBYTE(idx_2) = byte_410BBF[idx_1] + idx_2;
  LOBYTE(num_1) = byte_410BBF[idx_1];
  num_2 = byte_410BBE[idx_2];
  byte_410BBE[idx_2] = num_1;
  byte_410BBF[idx_1] = num_2;
  LOBYTE(num_1) = num_2 + num_1;
  ++v5;
  result = byte_410BBE[num_1];
  LOBYTE(idx_1) = idx_1 + 1;
  *v5 ^= result;
  --size;
}
while ( size );
dword_410CCE = idx_1;
dword_410CD2 = idx_2;
return result;
```

그림 18. 문자열 복호화 단계

아래 그림과 같이 시스템의 언어를 파악해 특정 국가를 제외하는 기능이 존재하며, 제외되는 국가는 아래 목록과 같다.

코드	국가 언어	코드	국가 언어
0x419	러시아	0x43F	카자흐어
0x422	우크라이나	0x440	키르기스스탄
0x423	벨로루스	0x442	투르크멘어
0x428	타지크	0x443	우즈베키스탄
0x42B	아르메니아	0x444	타타르어
0x82C	아제르바이잔어	0x818	루마니아어
0x437	조지아어	0x843	우즈베키스탄

표 8. 제외 국가 코드 표

Darksupp 랜섬웨어 내부에 존재하는 설정 값은 자체 구현 알고리즘으로 암호화된 상태로 저장되어 있으며, 구매자가 악성행위를 다양하게 결정해 배포할 수 있는 형태로 제작되어 있다. 아래 코드는 설정파일 내부에 존재하는 다양한 기능 구현을 처리하는 루틴이다.

```
if ( Emptying_Recycle_flag )
{
  if ( file_handle_41092C )
  {
    DeobfuscateString(xmmword_40B322, dword_40B31E);// Emptying Recycle Bin
    LogMessage(file_handle_41092C, &unk_40B20A, xmmword_40B322, 0, 0);
    sub_4013DA(xmmword_40B322, dword_40B31E);
  }
  EnumDrives();
}
if ( Delete_Shadow_flag )
{
  if ( file_handle_41092C )
  {
    DeobfuscateString(xmmword_40B380, dword_40B37C);// Deleting Shadow Copies
    LogMessage(file_handle_41092C, &unk_40B20A, xmmword_40B380, 0, 0);
    sub_4013DA(xmmword_40B380, dword_40B37C);
  }
  DeletingShadowCopies(a1);
}
if ( Unstalling_Services_flag )
{
  if ( file_handle_41092C )
  {
    DeobfuscateString(xmmword_40B350, dword_40B34C);// Uninstalling Services
    LogMessage(file_handle_41092C, &unk_40B20A, xmmword_40B350, 0, 0);
    sub_4013DA(xmmword_40B350, dword_40B34C);
  }
```

그림 19. 설정 파일 내의 기능 구현 처리 루틴

설정파일에 존재하는 기능 목록은 아래와 같다.

오프셋	설명	오프셋	설명
0x1	암호화 모드 설정 (1: FULL, 2: FAST, 이외에 값: AUTO)	0xB	로깅
0x3	로컬 디스크 암호화	0xD	특정 디렉토리 무시
0x4	네트워크 공유 파일 암호화	0xE	특정 파일 무시
0x5	감염 PC 운영체제 언어 정보 조회	0xF	특정 확장자 무시
0x6	볼륨 섀도우 백업 파일 삭제	0x12	프로세스 종료
0x7	휴지통 비우기	0x13	서비스 중지
0x8	자가 삭제	0x14	기능 사용되지 않음.
0x9	UAC 우회	0x15	랜섬노트 생성
0xA	토큰 권한 설정	0x16	뮤텍스 생성

표 9. 설정파일에 존재하는 기능 목록

Darksupp 랜섬웨어의 파일 암호화에는 Salsa20 및 RSA 암호화 알고리즘을 사용한다. Salsa20 알고리즘을 이용해 파일을 암호화 하고 암호화가 완료된 Salsa 키 값은 RSA 공개키를 통해 RSA 알고리즘으로 암호화 된다. Salsa20 암호화 키를 암호화 하기 위해 사용된 RSA 공개키는 위에서 언급된 자체 구현 암호 알고리즘을 통해 암호화된 상태로 하드코딩 되어 있다.

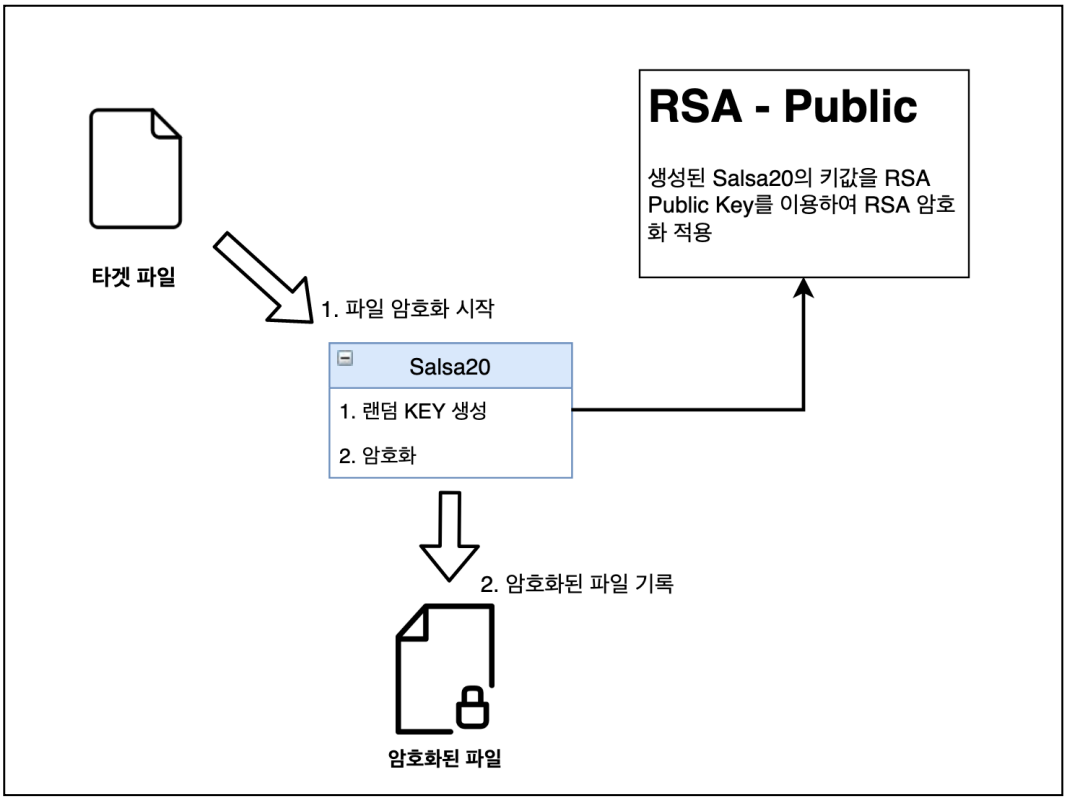


그림 20. 파일 암호화 과정

Darksupp 랜섬웨어는 18개의 암호화대상 제외 디렉토리 목록을 정의하고 있다.

Windows	appdata	application data	boot
google	mozilla	program files & program files (x86)	programdata
system volume information	tor browser	windows.old	intel
msocache	perflogs	x64dbg	public
all users	default		

표 10. 제외 디렉토리 목록(18개)

Darksupp 랜섬웨어의 암호화 대상에서 제외되는 50개의 확장자 목록은 아래와 같다.

386, adv, ani, bat, bin, cab, cmd, com, cpl, cur, deskthemepack, diagcab, diagpkg, dll, drv, exe, hlp, icl, icns, ico, ics, idx, ldf, lnk, mod, mpa, msc, msp, msstyles, msu, nls, nomedia, ocx, prf, ps1, rom, rtp, scr, shs, spl, sys, theme, themepack, lock, key, msi, hta, pdb, diagcfg, wpx

표 11. 제외 확장자 리스트(50개)

Darksupp 랜섬웨어는 파일 복원 방지를 위해 다음과 같은 추가 악성 행위를 수행하는 특징을 가지고 있다.

- 휴지통 비우기
- 볼륨 섀도 복사본 삭제
- 특정 서비스 및 프로세스 종료

종료되는 서비스 및 프로세스 목록은 31개로 다음과 같다.

종료 프로세스 목록	sql, oracle, ocssd, dbsnmp, synctime, agentsvc, isqlplussvc, xfssvccon, mydesktopservice, ocautoupds, encsvc, firefox, tbirdconfig, mydesktopqos, ocomm, dbeng50, sqbcoreservice, excel, infopath, msaccess, mspub, onenote, outlook, powerpnt, steam, thebat, thunderbird, visio, winword, wordpad, notepad
종료 서비스 목록	vss, sql, svc$, memtas, mepocs, sophos, veeam, backup

표 12. 종료 프로세스 목록(31개)과 종료 서비스 목록(8개)

Darksupp 랜섬웨어는 시스템에 대한 암호화가 공격자 의도대로 성공되면 아래 데이터를 C&C 서버로 전송한다.

```
{
  "bot":{
     "ver":"[악성코드 버전 정보]",
     "uid":"[{15}[a-z0-9] 복호화된 데이터에 존재함.]"
  },
  "os":{
     "lang":"[감염 피시 언어 정보]",
     "username":"[유저 이름]",
     "hostname":"[컴퓨터 이름]",
     "domain":"[도메인 이름]",
     "os_type":"windows",
     "os_version":"[운영체제 버전 정보]",
     "os_arch":"[운영 체제 비트 정보]",
     "disks":"[디스크 사용량]",
     "id":"[암호화된 감염 피시 하드웨어 아이디]"
  }
}
{
   "id":"[암호화된 감염 피시 하드웨어 아이디]",
   "uid":"[{15}[a-z0-9] 복호화된 데이터에 존재함.]",
   "enc-num":"[암호화 파일 개수]",
   "enc-size":"[전체 암호화 사이즈]",
   "skip-num":"[암호화가 안 된 파일 개수]",
   "elapsed-time":"%u.%u"
}
```

그림 21. 피해자 기초 데이터 및 암호화 결과 전송 코드

2.1.3. Sodinokibi Ransomware

Sodinokibi 랜섬웨어는 2019년 Gandcrab 제작자들이 서비스를 종료함과 동시에 등장한 랜섬웨어이다. 대표적인 공격벡터로는 다양한 대상을 사칭(경찰청, 은행, 헌법재판소, 입사지원서 등)한 내용의 피싱메일이 있다. 그러나 피싱메일 뿐만 아니라 다양한 공격벡터를 통해 랜섬웨어가 유포되기도 한다. 최근 미국 카세야(Kaseya)社의 VSA 제품 제로데이 취약점을 이용해 대규모 공급망 공격 진행 후 해당 랜섬웨어를 유포해 큰 피해를 입힌 사례가 있다. Sodinokibi Ransomware 악성코드는 감염 직후 아래 그림과 같이 'Your files are encrypted !!!'라는 메시지를 포함한 화면으로 피해자 바탕화면을 수정하는 특징을 가지고 있다.

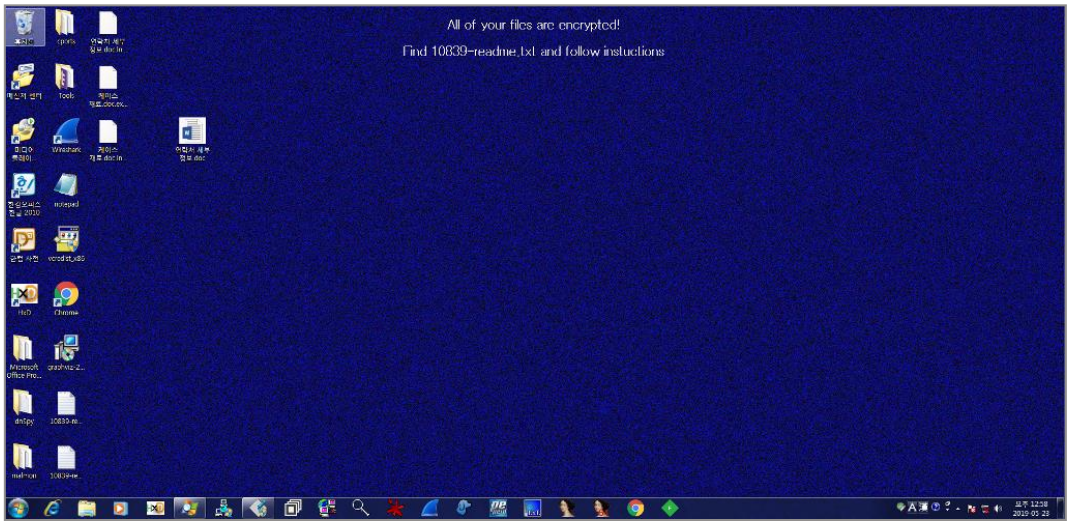


그림 22. Sodinokibi Ransomware 감염 화면

Sodinokibi 랜섬웨어는 주로 피싱 메일을 통해 유포된다. 한국 대상으로 배포된 메일 중에는 한국 증권사 농협을 사칭한 사례가 있다. 피싱 메일 제작 시 타깃 국가에 대한 고도의 조사 과정이 포함 되어 있는 것으로 추정되며, 아래 그림은 피싱 메일의 원문이다.

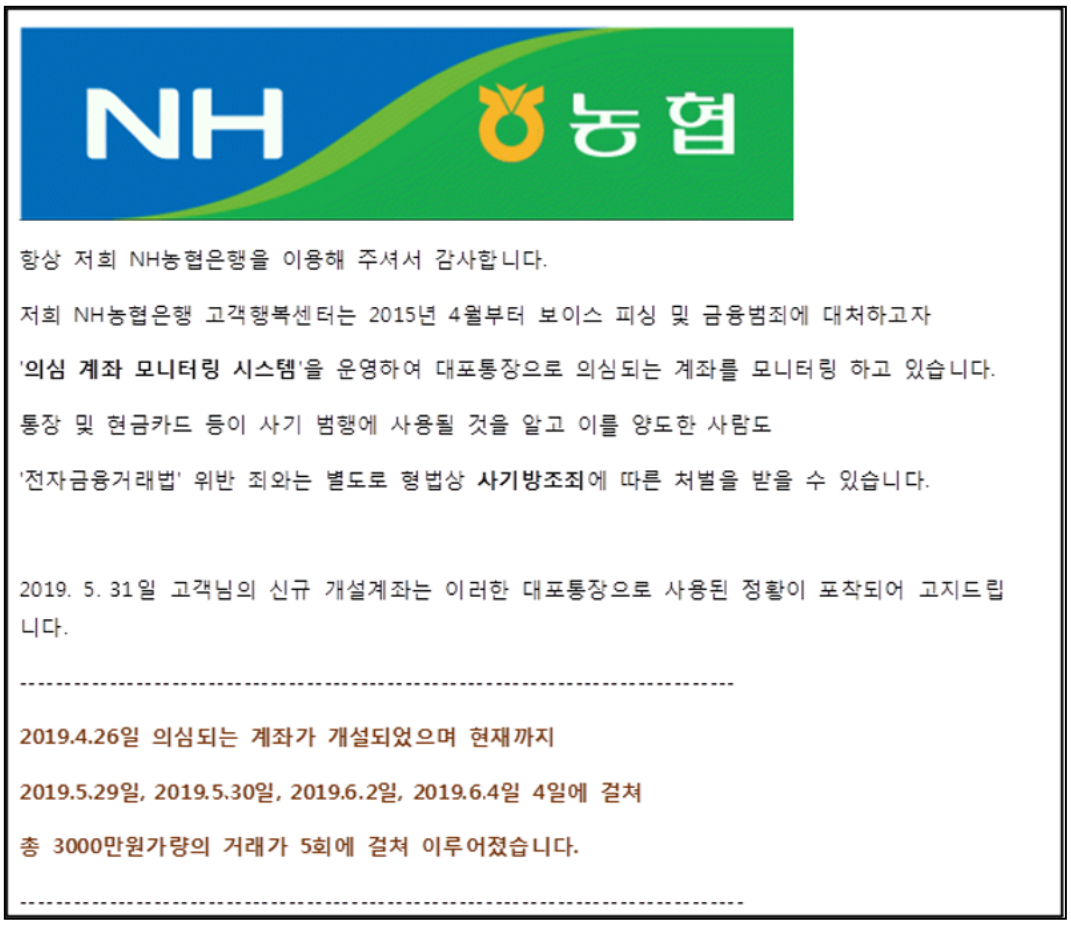


그림 23. Sodinokibi Ransomware 감염을 유도한 피싱 메일

아래 그림과 같이 본문의 마지막에는 '계좌 내용 확인' 버튼이 포함되어 있으며 버튼 클릭 시 유포지 서버에 접속해 추가 악성코드를 다운로드 받아오는 구조로 동작한다.

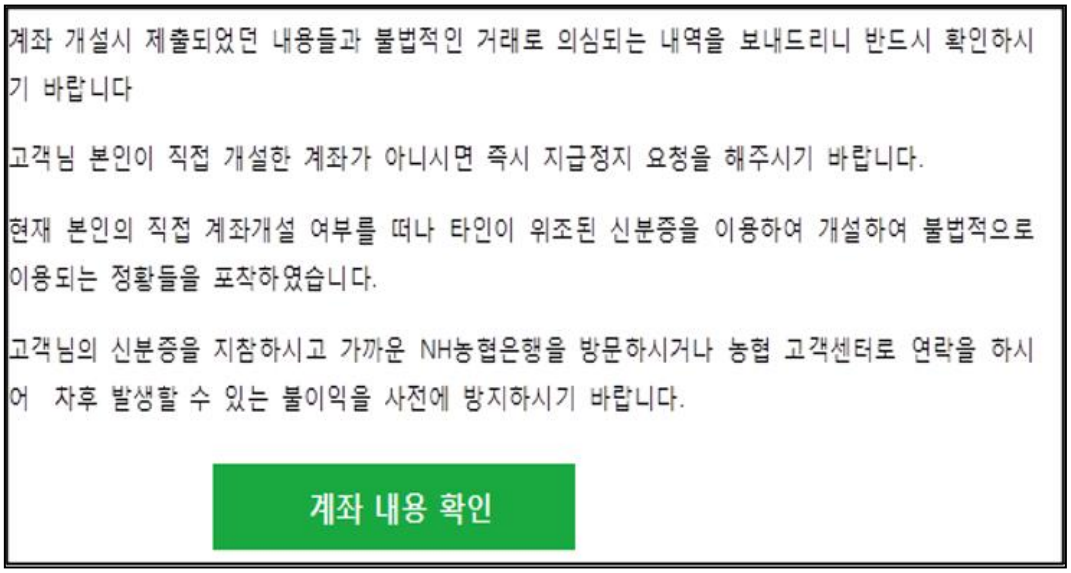
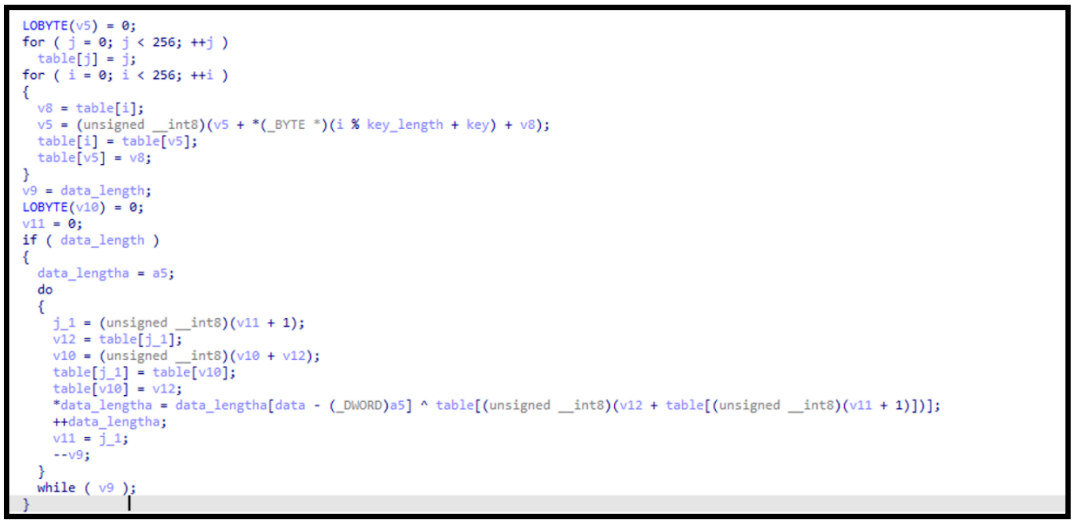


그림 24. Sodinokibi Ransomware 다운로드 요청 화면

메일은 불특정 다수에게 배포될 수 있는 형태로, 특정 기업을 타겟화한 공격 방식이 아닌 불특정 다수를 대상으로 제작된 악성코드임을 추정할 수 있다.
Sodinokibi Ransomware는 초기 동작 시 설정파일을 제작한다. 설정 파일은 RC4 암호 알고리즘을 통해 암호화 되어있으며 암호화에 사용되는 공개키 및 암호화에 사용된 키는 아래 레지스트리 경로에 생성된다.

- *HKLM₩SOFTWARE₩recfg₩pk_key*
- *HKLM₩SOFTWARE₩recfg₩sk_key*
- *HKLM₩SOFTWARE₩recfg₩0_key*

랜섬웨어의 설정파일은 아래와 같은 RC4 함수를 통해 복호화 되어 사용 된다.



```
LOBYTE(v5) = 0;
for ( j = 0; j < 256; ++j )
  table[j] = j;
for ( i = 0; i < 256; ++i )
{
  v8 = table[i];
  v5 = (unsigned __int8)(v5 + *(_BYTE *)(i % key_length + key) + v8);
  table[i] = table[v5];
  table[v5] = v8;
}
v9 = data_length;
LOBYTE(v10) = 0;
v11 = 0;
if ( data_length )
{
  data_lengtha = a5;
  do
  {
    j_1 = (unsigned __int8)(v11 + 1);
    v12 = table[j_1];
    v10 = (unsigned __int8)(v10 + v12);
    table[j_1] = table[v10];
    table[v10] = v12;
    *data_lengtha = data_lengtha[data - (_DWORD)a5] ^ table[(unsigned __int8)(v12 + table[(unsigned __int8)(v11 + 1)])];
    ++data_lengtha;
    v11 = j_1;
    --v9;
  }
  while ( v9 );
}
```

그림 25. Sodinokibi Ransomware 의 복호화 기능 구현

Sodinokibi 랜섬웨어 내부에는 암호화 대상에서 제외할 확장자 정보, 결제 정보, 랜섬노트, 공개키 등 악성 행위에 필요한 전반적인 데이터가 포함되어 있다.

제외 확장자	"idx","scr","ani","cur","nls","cpl","diagcab","mpa","hlp","rom","deskthemepack", "nomedia","cmd","com","386","lnk","icl","diagcfg","msp","sys","hta","icns", "msc","lock","msstyles","dll","ocx","prf","adv","wpx","drv","ps1","themepack", "msu","spl","mod","rtp","cab","msi","bin","ico","exe","key","ics","shs","bat","ldf", "diagpkg","theme"
제외 디렉토리	"windows", "application data", "perflogs", "$recycle.bin", "$windows.~bt", "program files (x86)", "google", "windows.old", "$windows.~ws", "programdata", "msocache", "boot", "intel", "tor browser", "program files", "appdata", "system volume information", "mozilla"
제외 파일	"thumbs.db", "ntuser.dat", "boot.ini", "ntldr", "ntuser.ini", "desktop.ini", "ntuser.dat.log", "bootsect.bak", "autorun.inf", "bootfont.bin", "iconcache.db"

표 13 Sodinokibi Ransomware의 암호화 제외 대상

랜섬웨어에서 사용한 암호화 알고리즘은 공격자의 비대칭키 중 개인키가 사용되며, 데이터를 암호화 하기 위해 사용하는 메커니즘은 아래 그림과 같다.

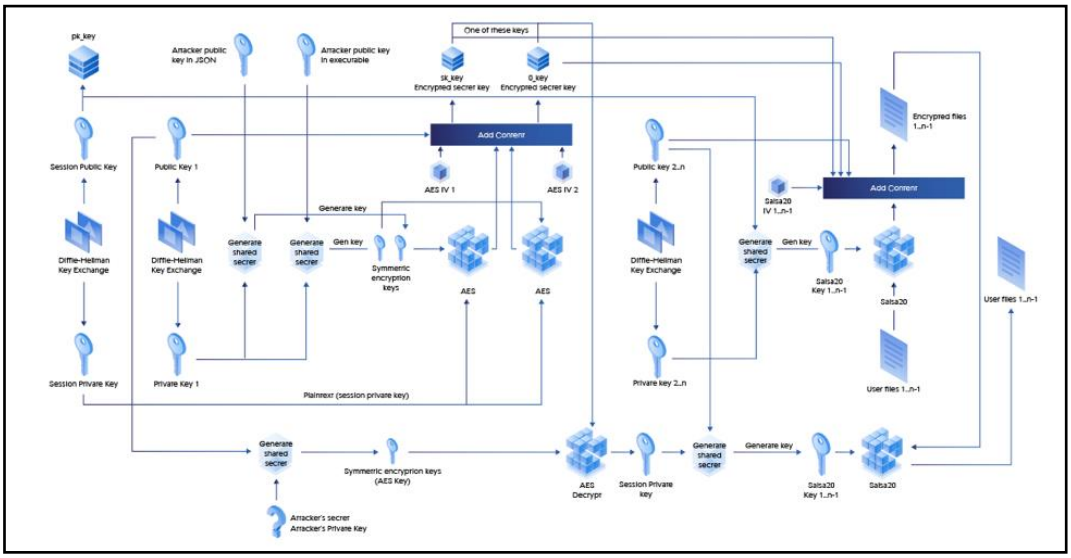


그림 26. 데이터 암호화 플로우

(출처: https://www.acronis.com/en-eu/articles/sodinokibi-ransomware/)

Sodinokibi 랜섬웨어에 의해 암호화를 끝마친 데이터 구조는 아래와 같다.

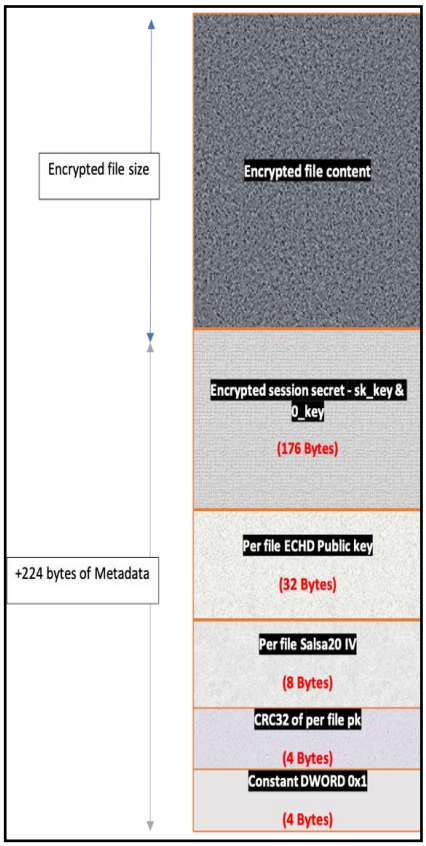


그림 27. Sodinokibi Ransomware 감염 후 데이터의 구조

(출처: https://www.acronis.com/en-eu/articles/sodinokibi-ransomware/)

Sodinokibi 랜섬웨어는 키를 공개키로 암호화 해 사용하는 보통의 랜섬웨어와 다르게 각 폴더마다 사용한 키가 다르게 구성되는 점, 랜섬웨어 페이지에서 폴더에 기록된 키를 공격자만 알 수 있는 키로 암호화 해 폴더 단위로 암호를 해제하는 방식을 취하고 있다는 점에서 차별화된다.

단계적으로 키 생성이 완료되면 아래 그림과 같이 랜섬웨어는 피해자 PC의 전반적인 정보를 C&C서버로 전송하며, C&C서버로 전송하는 데이터는 악성코드 초기 실행 시 한번에 수집된다.

```
CPU_Volume_Info_41D750 = (int)GetVolumeInformation_404165();// cpuid과, VolumeInfomation함수를 통해 데이터 수집후 커스텀 알고리즘으로 암호화후 전역변수에
if ( !CPU_Volume_Info_41D750 )
  CPU_Volume_Info_41D750 = (int)return_string_4050CE(v32);
sk_key_base_41D754 = (int)Get_reg_key_info_4021F5();// recfg에서 각종 키 정보를 가지고옴
rnd_ext_value_41D748 = (int)Get_rnd_ext_401B7B();// rngcnf레지에서 rnd_ext 값 가져옴 데이터 식별 불가
Username_41D758 = (int)GetIUsername_4042A2();// 유저이름
if ( !Username_41D758 )
  Username_41D758 = (int)return_string_4050CE(v32);
ComputerName_41D75C = (int)Get_Computer_name_403E14();// 컴퓨터 이름
if ( !ComputerName_41D75C )
  ComputerName_41D75C = (int)return_string_4050CE(v32);
Domain_Workgourp_info_41D760 = (int)Get_info_domain_403F7A();// 도메인 및 워크 그룹 정보
if ( !Domain_Workgourp_info_41D760 )
  Domain_Workgourp_info_41D760 = (int)return_string_4050CE(v32);
Locale_info_41D764 = (int)sub_404096();     // 운영체제 언어 정보
if ( !Locale_info_41D764 )
  Locale_info_41D764 = (int)return_string_4050CE(v32);
v6 = sub_4043B1();
v7 = v15;
if ( !v6 )
  v7 = v12;
dword_41D768 = (int)return_string_4050CE((__int16 *)v7);
OS_info_41D76C = (int)get_OS_name_40422C(); // 운영체제 버전 정보
if ( !OS_info_41D76C )
  OS_info_41D76C = (int)return_string_4050CE(v32);
v8 = check_drive_use_size_403E53(&v19);
Disk_size_41D770 = (int)base64_404C77((int)v8, 22 * v19, 0);
FREE_403B82(v8);
CPU_Version_x64_x86_41D7C0 = GetNativeSystemInfo_404481() ? 64 : 86;// CPU환경 확인
```

그림 28. C&C서버로 전송되는 데이터

Sodinokibi 랜섬웨어는 결제를 할 수 있는 페이지를 그림 29와 같이 제공한다.

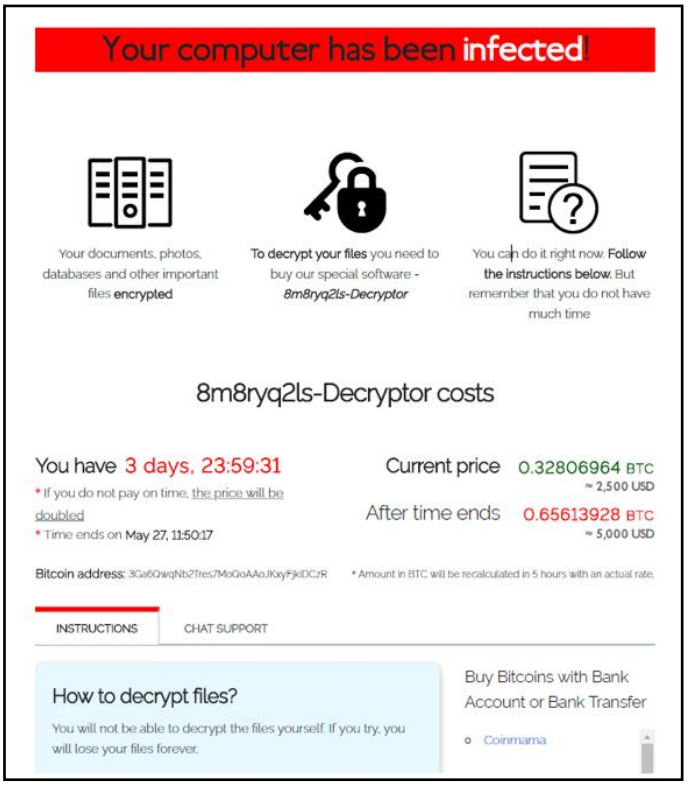


그림 29. Sodinokibi 랜섬웨어의 결제 페이지
(출처: https://www.acronis.com/en-eu/articles/sodinokibi-ransomware/)

2.2 랜섬웨어의 공격 시나리오

2.2.1. RDP 브루트포스

#1. 갑자기 먹통이된 사이트
특정 사이트를 관리하고 있는 담당자 C씨는 퇴근 후 한통의 전화를 받게 된다. C씨가 담당하고 있는 웹 사이트에 접속이 안된다는 전화였다. 부랴부랴 출근한 C씨는 웹 관련 서버가 동작하고 있는 PC에 랜섬웨어가 감염된 것을 발견했다. 해당 PC로는 아무것도 하지 않았던 C씨는 의아했다. 랜섬웨어는 어떻게 들어와 감염이 된 것일까.

공격자는 공개된 포트스캐닝 도구를 이용해 노출된 RDP를 스캔 후 브루트 포싱을 했다. 담당자 C씨는 보안에 대한 지식이 전무했기 때문에 이를 알리 없었다. RDP 접속 실패에 대한 제한이 걸려있지 않았고, 이는 결국 공격자의 침입으로 이어졌다. 공격자는 PC에 손쉽게 접속해 보안 제품을 모두 무력화하고 랜섬웨어를 실행한 후 유유히 사라졌다.

2.2.2. (다양한 사칭을 이용하는) 피싱메일

#2. 채용담당자와 포트폴리오
인사 담당자 B씨는 구직사이트에 신입 직원을 뽑기 위해 채용공고를 올렸다. 채용 관련 문의 사항을 접수하기 위한 회사 메일주소도 함께 올려 두었다. 해당 사이트에서 게시글을 보고 많은 이들이 최씨의 회사에 지원을 했다. 많은 문의사항들이 회사 메일로 접수됐고, 개중에는 이력서도 포함돼있었다. 인사 담당자 최씨는 아무런 의심없이 해당 메일을 클릭했다. 간단한 본인 소개와 포트폴리오 파일을 함께 첨부한다는 내용의 메일이었다. 메일에는 김OO.7z파일이 첨부돼 있었다. 담당자는 포트폴리오 확인을 위해 해당 파일의 압축을 풀었다. 폴더 내부에는 포트폴리오.doc 파일이 있었다. 아이콘도 분명 워드 아이콘이었다. 인사담당자 최씨는 포트폴리오를 확인하기 위해 의심없이 실행했고, 잠시 뒤 랜섬웨어에 감염됐다.
해당 파일은 문서 파일이 아닌 문서 아이콘으로 변경된 exe 파일이었으며, 파일명은 포트폴리오.doc(긴 공백).exe였다.

2.2.3. AD 서버의 탈취

#3. 서버 담당자에게 온 한통의 메일
서버 담당자 A씨는 업무 중 한통의 메일을 확인하게 된다. 엑셀 첨부파일이 포함되어 있는 별 내용이 없는 메일이었다. 시덥잖게 생각한 담당자 A씨는 해당 메일의 첨부파일을 실행했다. 매크로를 사용해야 본문의 내용을 확인할 수 있다는 엑셀 시트가 나왔다. 본문의 내용을 확인하기 위해 [콘텐츠 사용]을 눌러 매크로를 실행시켰고, 파일을 다운로드하는 듯한 로딩화면이 나오고는 이

후 별 반응이 없었다. 아무런 일도 일어나지 않자 담당자 A씨는 별 내용이 없는 것으로 판단하고는 해당 프로그램들을 모두 종료했다. 그로부터 며칠 후, A씨가 담당하고 있던 서버를 이용해 사내에 랜섬웨어가 유포되어 회사의 일부가 마비됐다.

A씨가 실행한 엑셀 파일의 매크로 영역에는 공격자가 심어둔 공격 코드가 포함되어 있었다. 해당 코드로 인해 공격자의 C&C서버로부터 추가 악성코드가 다운로드 됐으며, 해당 악성코드는 현재 실행중인 환경이 도메인 서버(AD)인지 확인 후 실행중인 환경의 정보를 C&C로 전달했다. 공격자들은 전달받은 내용들을 이용해 내부 데이터를 탈취 후 랜섬웨어를 유포했다.

2.2.4. 알려진 취약점 공격

#4. 웹서버와 랜섬웨어
웹서비스 개발자 B씨는 며칠 전 백엔드 서버 업데이트 과정에서 'puppy.png;.jsp'라는 파일을 발견했다. 수상한 파일을 발견한 B씨는 코드를 읽어 나가며 웹 서비스 상에서 동작하는 Webshell 형식의 악성코드임을 인지했다.

불안감을 느낀 B씨는 서둘러 파일을 삭제했다. 하지만 며칠 뒤 담당하고 있던 B씨가 담당하고 있던 웹 서버는 모두 마비됐다. 서버 담당자는 윈도우즈 복원 기능을 이용해 시스템을 복원했지만, 불과 몇 초 뒤 다른 유형의 랜섬웨어에 서버가 재감염 됐다.

B씨가 분석한 'puppy.png;.jsp' 파일은 웹셀형 악성코드이다. 그러나 웹 서비스 상 파일 업로드 취약점이 존재했고, 이를 악용해 공격자는 개발자의 행동을 보고 추적을 피하기 위해 랜섬웨어를 돌렸다. 공격자는 서비스가 정상적으로 동작하는 것을 보고 완벽하게 흔적을 제거하기 위해 쉐도우 볼륨을 삭제하는 유형의 랜섬웨어를 한번 더 동작시킨 것이다.

2.3 랜섬웨어의 기술적 대응과 한계

2.3.1. 암호화 방식의 원초적 문제

랜섬웨어 구현기술 에서 언급된 암호알고리즘 등을 이용해 암호화된 파일을 키(KEY) 없이 복원하는 방법은 현시점에서는 암호 알고리즘 자체를 무력화 시키는 방법밖에 없다. 이는 곧 수학적으로 검증된 정의에 대한 오류를 찾아야하는 문제로 이어지기 때문에 사실상 복원이 불가능하다고 볼 수 있다. 복호화 툴이 공개된 랜섬웨어의 경우는, 공격자들이 키를 직접 공개하거나 파일 내부에 하드코딩 되어있는 키값을 이용한다.

그 예로 Darkside 랜섬웨어 복구툴을 들 수 있다. 루마니아의 보안업체 비트디펜더 (Bitdefender)에서는 Darkdise 랜섬웨어에 대한 복구툴을 공개했다. 비트디펜더에서 공개한 자료를 역공학 분석 결과, 단순히 하드코딩된 RSA Private Key 정보를 통해 파일을 복원하는 것으로 확인됐다. 아래 그림은 비트디펜더의 Darkside 랜섬웨어 복구툴에 하드코딩 되어있는 키 값이다. 해당 공격 그룹은 미 송유관 해킹사건을 통해 세간의 주목을 받았으며 미 정부의 압박(해킹 서버 압류, 결제 블로그 마비 등)으로 인해 활동을 중단하고 비밀키를 공개한 바 있었다.

그림 30. Darkside 랜섬웨어 복구툴에 하드코딩되어 있는 키 값

Darkdise 랜섬웨어 사례처럼 공격자가 직접 공개한 키를 이용하지 않는 한 RSA 공개키를 이용한 파일 암호화 방법의 경우 정공법으로는 파일 복원이 어려우며, 일반 랜섬웨어에서는 두개 이상의 암호화 알고리즘을 이용해 파일을 암호화 하기때문에 사실상 알고리즘을 무력화하지 않는 이상 암호화된 파일을 복호화하기는 매우 어렵다.

2.3.2. 검증된 암호 알고리즘을 사용하지 않는 랜섬웨어

Petya 랜섬웨어는 일반적으로 파일을 암호화하는 랜섬웨어와는 거리가 멀지만, 시스템을 암호화하고 금전을 요구하는 수법이 랜섬웨어와 비슷해 랜섬웨어로 불리는 악성코드이다. 2016년에 처음 공개되어 국내에도 감염된 사례가 존재하는 악성코드인 Peyta 랜섬웨어는 MBR 파티션에 새로운 코드를 추가하고 원본 데이터를 0x37과 단순 Xor를 하는 방식을 가지고 있다.

그림 31. Petya 랜섬웨어에 감염된 PC의 모습

Petya 랜섬웨어는 다른 랜섬웨어와는 달리 수학적으로 검증된 암호 알고리즘을 사용하지 않기 때문에 비교적 손쉽게 데이터를 복원할 수 있다. 아래 그림은 Petya 랜섬웨어로 손상된 MBR 파티션의 데이터이다.

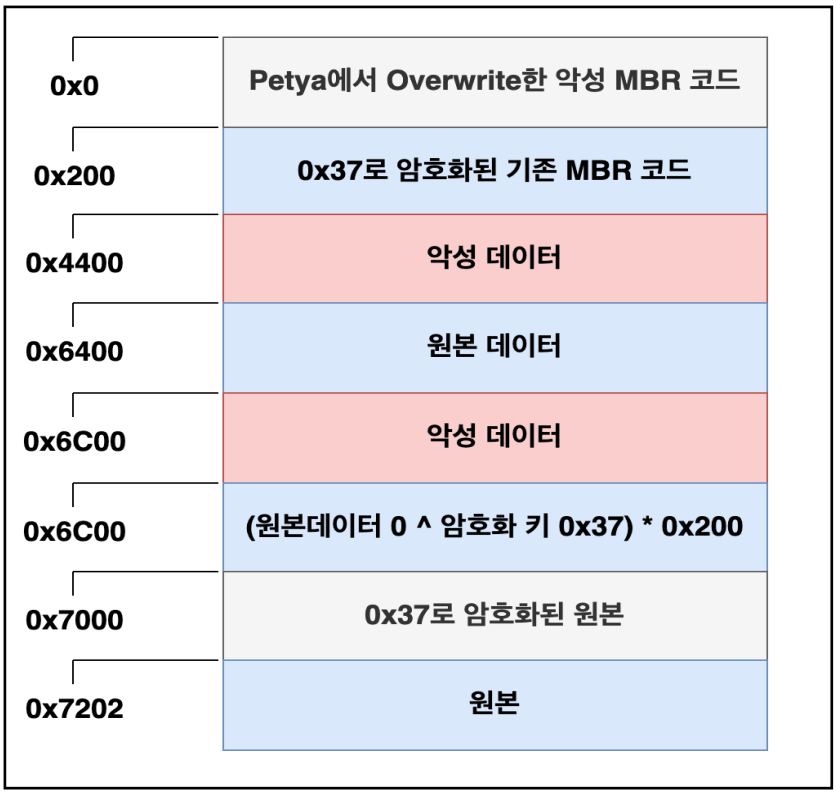


그림 32. Petya 랜섬웨어로 손상된 MBR 파티션

Petya 랜섬웨어는 컴파일된 시간에 따라 암호화 키가 달라지는데, 0x6c00~0x7000 원본 데이터가 0인 부분에서 키가 노출되는 취약점을 가지고 있다. 또한 해당 부분은 비대칭키 기반의 암호화가 아니기에 악성코드 샘플 내에서 MBR을 암호화 하는 코드 구조를 분석한다면 손쉽게 복호화 키를 추출할 수 있다. 따라서, 해당 케이스 또한 검증된 구조를 가지고 있지 않다는 점에서 복원 가능한 랜섬웨어로 분류되고 있다.

그러나 이와 반대로 검증된 암호 알고리즘을 사용하지 않기 때문에 정확한 알고리즘 분석이 불가능해 복호화를 할 수 없는 경우도 발생한다. 파괴형 랜섬웨어의 경우가 이에 해당하며, 이경우 금전을 목적으로 하는 것 보다는 데이터를 파괴하고 시스템을 사용할 수 없게 하는게 목적이기때문에 복호화가 불가능하다.

3. 기업 담당자의 눈으로 바라본 랜섬웨어

3.1 설문조사 개요 및 요약

본 리포트에서는 기업의 보안담당자의 입장에서 랜섬웨어에 대한 이해도와 대응현황을 알아보기 위해 CONCERT 회원사와 국내 과학기술정보통신부에 등록되어 있는 CISO를 대상으로 설문조사를 실시했고, 682개의 기업 CISO 및 보안담당자가 응답을 했다. 응답기업의 50%는 100명 미만의 중소기업이며, 100명 이상 ~ 500명 미만 기업이 33.28%, 500명 ~ 1,000명 미만이 6.05%, 11%가 1,000명 이상의 직원으로 구성된 기업이다. 응답자는 많은 산업 부문을 대표하고 있지만, 응답비율은 제조 및 소비재, IT와 인터넷 및 게임, 서비스, 유통과 커머스 순으로 높은 것으로 나타났다.

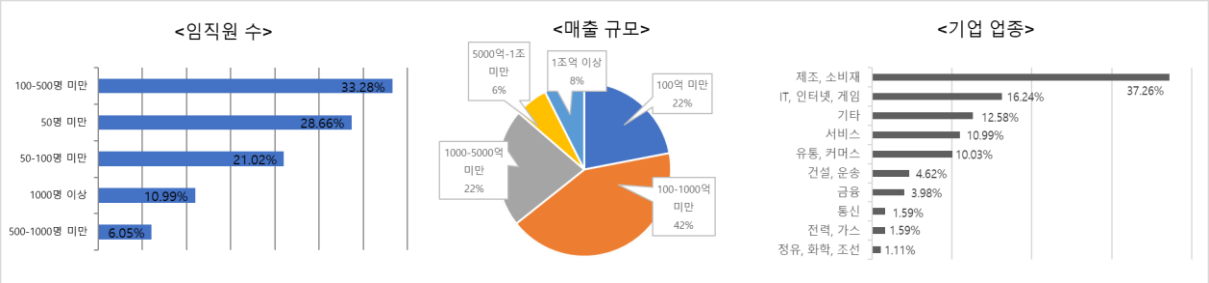


그림 33. 설문 응답기업의 분포현황

이번 설문은 랜섬웨어에 대한 인식조사, 랜섬웨어 피해 영향도 조사, 랜섬웨어의 대응능력(탐지, 치료 및 복구)과 전망 및 예방을 위한 기업의 대응관점에서 총 30개의 문항으로 구성됐다.

설문 결과에 따르면 응답자 전체의 95%가 랜섬웨어가 기업의 비즈니스에 위협이 되고 있다고 응답했고, 약 40%의 기업이 랜섬웨어로 인한 피해경험이 있는 것으로 조사됐다. 또한 피해경험이 있는 기업의 7.4%는 공격자에게 비용을 지불한 경험이 있는 것으로 확인됐고, 피해가 없는 기업의 43%는 랜섬웨어 피해가 생긴다면 공격자에게 비용을 지불하거나 모르겠다고 응답해 눈길을 끌었다. 또한 전세계적으로 랜섬웨어 피해가 급증하고 있는데 아직까지 44%의 기업은 랜섬웨어에 대한 대응계획을 수립하지 못하고 있다는 설문결과도 주목된다.

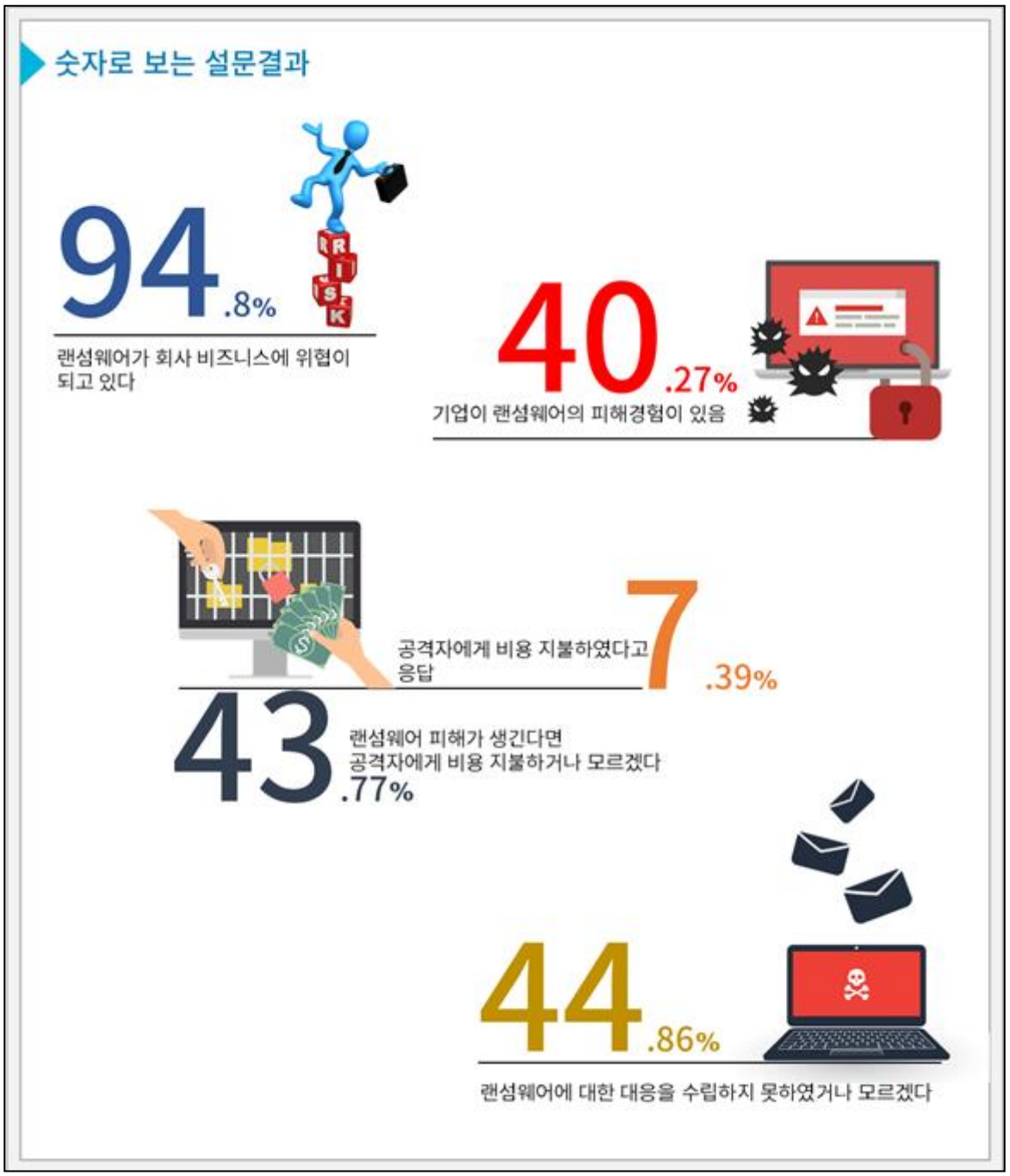


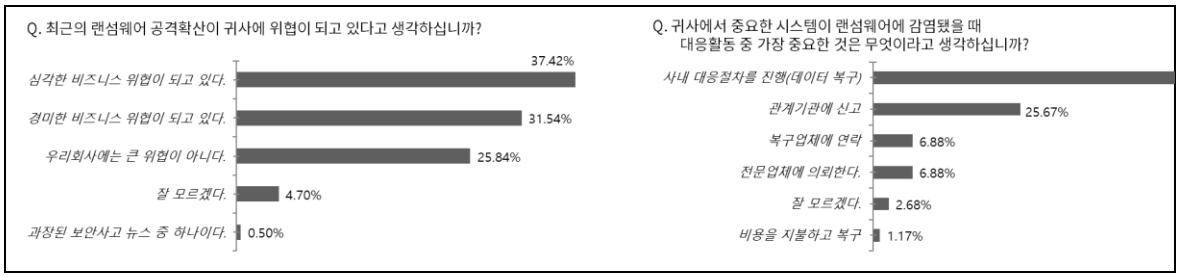
그림 34. 숫자로 보는 설문 결과

3.2 세부 조사결과

3.2.1 랜섬웨어에 대한 인식 조사

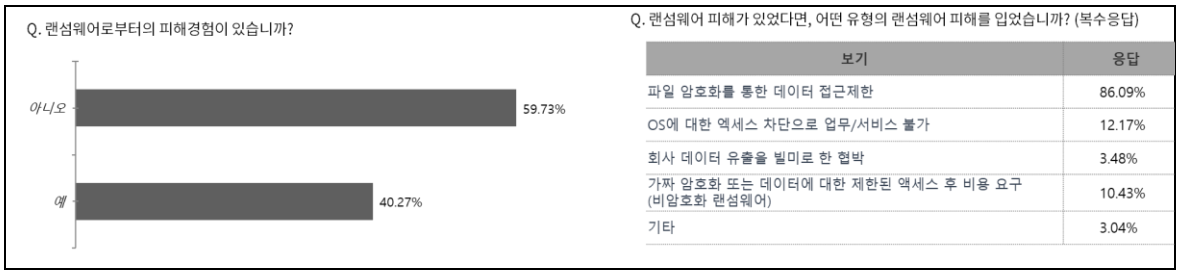
첫번째 섹션의 설문조사 결과는 기업의 보안담당자들이 현재 랜섬웨어에 대한 위협을 어떻게 인식, 대응하고 있는지를 조사하는 결과로서, 각 문항별 응답결과를 참고해 몇 가지 중요한 통계를 살펴보았다.

이번 설문조사에서는 응답기업의 94.8%가 랜섬웨어를 비즈니스의 위협으로 인식을 하고 있으며, 그중 기업의 심각한 위협이 되고 있다고 응답한 결과도 37.43%로 나타났다. 응답한 기업의 75%는 랜섬웨어 공격의 위협수준에 대해 위협수준이 보통이거나 매우 높은 것으로 응답했다. 특히 기업에서 랜섬웨어에 감염됐을 때 대응활동 중 가장 중요한 활동으로는 백업된 데이터를 이용한 사내 대응절차 진행을 꼽았으며, 그 뒤로 관계기관에 신고, 복구업체 및 전문업체에 의뢰 등을 꼽았다.



3.2.2 랜섬웨어 피해 영향도 조사

이전 섹션에서 랜섬웨어가 기업의 비즈니스를 위협하는 중대한 공격으로 간주됐지만, 과연 기업에서 실제 얼마나 많은 피해가 있었는지, 피해가 없었다면 어떤 피해가 예상되는지 설문을 통해 확인해 보았다.
먼저 피해경험 여부에 대한 질문에 응답기업의 40.27%가 랜섬웨어로부터 피해 경험이 있는 것으로 확인됐으며, 이중 7%넘는 기업이 공격자에게 비용을 지불한 것으로 확인됐다. 보안사고 또는 피해경험을 묻는 질문에 대한 응답이 일반적으로 매우 보수적이거나 회피 경향을 보인다는 점을 감안하면, 40%가 넘는 피해경험 응답은 다소 충격적 이기까지 하다.



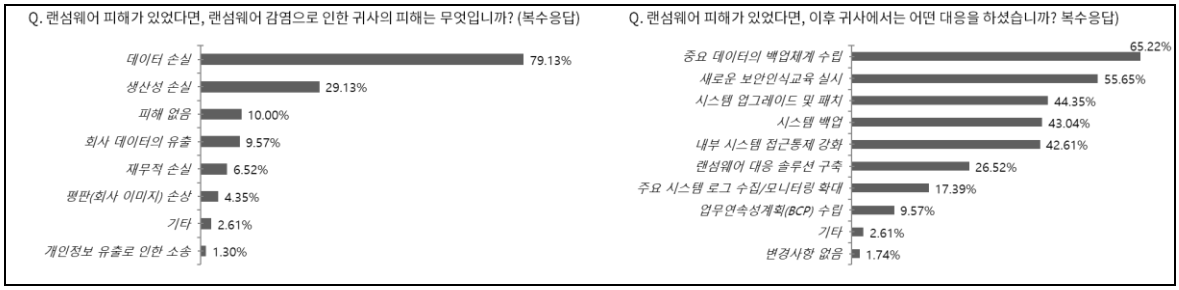
Q. 랜섬웨어 피해가 있었다면, 어떤 유형의 랜섬웨어 피해를 입었습니까? (복수응답)

보기	응답
파일 암호화를 통한 데이터 접근제한	86.09%
OS에 대한 엑세스 차단으로 업무/서비스 불가	12.17%
회사 데이터 유출을 빌미로 한 협박	3.48%
가짜 암호화 또는 데이터에 대한 제한된 액세스 후 비용 요구 (비암호화 랜섬웨어)	10.43%
기타	3.04%

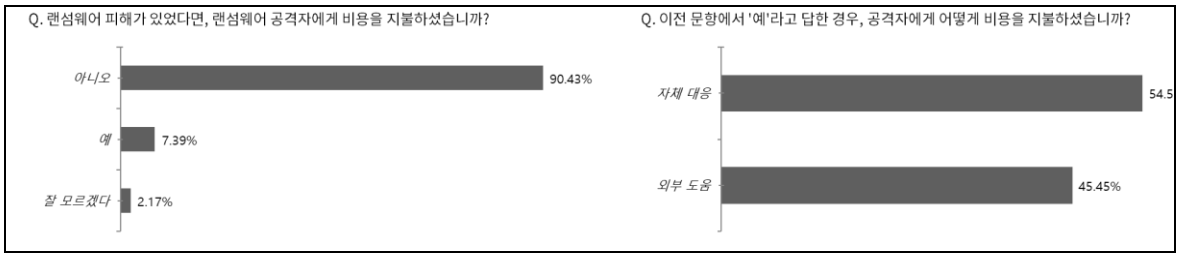
랜섬웨어 피해를 입은 기업에서 기타의견을 포함하여 89%는 파일을 암호화해 액세스 할 수 없게 만드는 랜섬웨어 공격을 받은 것으로 나타났으며, OS영역에 대한 액세스를 차단해 업무 및 서비스를 불가하게 만드는 공격비율도 12.17%에 달했다. 특히 회사 데이터 유출을 빌미로 한 협박 공격도 3.48%에 이르는 것으로 나타났다.

이러한 랜섬웨어 공격으로 인한 기업의 피해는 무엇일까? 랜섬웨어 피해경험이 있는 기업의 실제 피해사례를 설문으로 확인한 결과, 데이터의 손실, 생산성 손실이 가장 크게 나타났다. 이어서 9.57%의 기업은 회사 데이터의 유출로 인한 피해를 보았고, 개인정보 유출로 인한 소송도 피해기업 전체의 1.3%에서 발생한 것으로 나타났다.

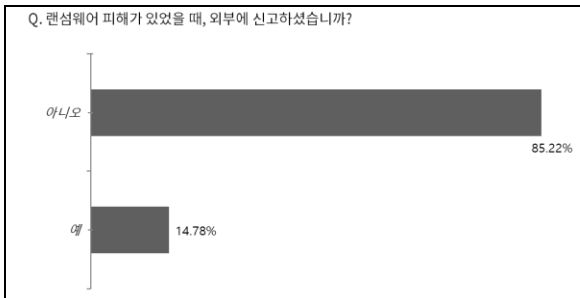
이러한 랜섬웨어의 피해이후 응답기업의 65.2%는 중요 데이터의 백업체계를 수립했고, 새로운 보안인식교육, 시스템 업그레이드 및 패치, 시스템 백업 등의 대응활동을 수행한 것으로 조사됐으며, 이어 내부 시스템에 대한 접근통제를 강화하고 랜섬웨어 대응 솔루션을 구축하고 주요 시스템에 대한 로그수집과 모니터링을 강화했다.



그렇다면, 랜섬웨어의 피해가 있었을 때 기업은 중요한 파일을 복구하기 위해 비용을 지불했을까? 응답자의 7.39%는 비용을 지불한 것으로 나타났고, 잘 모르겠다는 응답을 긍정으로 판단할 경우 약 10%의 기업에서 랜섬웨어 피해복구를 위해 공격자에게 비용을 지불한 것으로 추정된다. 비용지불방법은 공격자에게 자체적으로 지불하는 형태가 약 54%를 차지했고, 외부의 도움을 받아 지불한 경우도 45%를 넘었다. '랜섬웨어 복구전문'이라는 타이틀을 써놓고 있는 업체들은 대부분 기술적으로 복구를 지원하는 것이 아니라 공격자와의 협상, 비트코인 지불 등을 대행해주는 경우가 대부분인데, 이번 설문응답은 이 업체들의 비즈니스 영역이 엄연히 존재함을 입증하고 있다.



마지막으로, 피해기업은 과연 피해사실을 관계 기관에 신고했을까? 피해기업의 85.22%는 별도로 신고를 하지 않은 것으로 나타났으며, 반대로 신고한 경우는 14.78%에 불과한 것으로 확인됐다. 신고를 한 경우, KISA나 경찰 사이버수사대에 신고한 비율이 71%수준으로 나타났고, 25%는 외부 랜섬웨어 대응업체, 복구업체 등 민간기업에 복구를 단순의뢰 했지만 이를 '신고'로 간주하고 있었다. 피해를 신고하지 않은 기업의 경우, 경미한 피해로 신고할 수준이 아닌 것으로 판단한 것이 전체 응답의 51%를 차지했고, 자체 대응이 가능했다는 응답이 21.65%로서, 72%는 기업 내에서 대응이 가능했던 수준으로 나타났다. 다만, 어디에 신고해야 하는지 등의 신고절차를 몰라 신고를 하지 못한 비율도 11.46%를 차지했으며, 7%는 신고해도 피해복구를 기대할 수 없어 신고의 의미가 없는 것으로 판단했다는 응답을 보였다. 기타 의견으로는 신고절차의 복잡성, 신고 이후 조사 등의 부담, 기업의 이미지 손상 등이 신고를 꺼리는 요인으로 나타났다.



Q. 이전 문항에서 '예'라고 답한 경우, 어느 기관에 신고하셨나요?

응답	응답율
KISA	45.16%
경찰, 사이버수사대	25.80%
외부 랜섬웨어 대응업체	16.12%
기타	9.67%

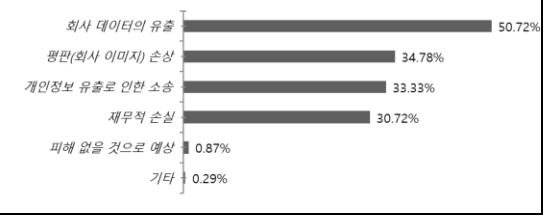
Q. 이전 문항에서 '아니오'라고 답한 경우, 신고하지 않은 이유는 무엇입니까?

응답	응답율
경미한 피해로 신고할 수준이 아님	50.95%
백업, PC초기화 등으로 자체 대응이 가능해서	21.65%
어디에 신고해야 하는지 등의 신고절차 등 모름	11.46%
신고해도 피해복구는 되지 않기에 의미 없음	7%
보안시스템 협력업체를 통한 유지보수 진행	3.82%
피해 당시 상황에 데이터 복구에만 집중	3.18%
기타	5.09%

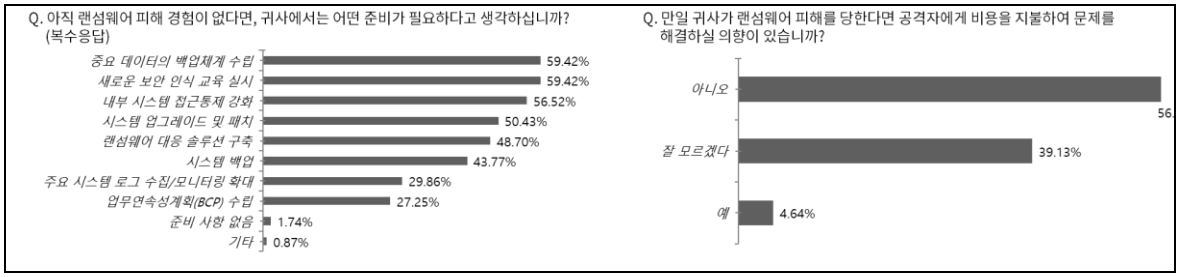
랜섬웨어의 피해경험이 없다고 응답한 기업 약 60%를 대상으로도 랜섬웨어로 인해 예상할 수 있는 피해가 무엇인지 확인했으며, 피해기업과 유사하게 파일 암호화를 통한 데이터의 접근제한과 OS에 대한 액세스 차단으로 업무 및 서비스가 불가능한 것을 가장 많은 비율로 꼽았다. 응답기업의 31%는 회사의 데이터 유출에 이은 협박을 우려하고 있으며, 기타 의견으로 개인정보 유출 및 가상자산에 대한 암호화로 출금을 제한하는 협박에 대한 우려도 있다.

Q. 아직 랜섬웨어 피해 경험이 없다면, 어떤 유형의 랜섬웨어 피해를 당할 수 있다고 생각하십니까 ? (복수응답)

보기	응답
파일 암호화를 통한 데이터 접근제한	67.25%
OS에 대한 액세스를 차단하여 업무/서비스 불가	43.48%
회사의 데이터를 유출하여 협박	31.30%
가짜 암호화 또는 데이터에 대한 제한된 액세스 후 비용 요구 (비암호화 랜섬웨어)	27.54%
기타	0.87%



랜섬웨어의 피해가 없었던 기업들은 예방대책으로 중요 데이터의 백업체계 수립, 임직원의 보안 인식교육, 내부 시스템의 접근 통제 강화, 시스템 업그레이드 및 패치, 랜섬웨어 대응 솔루션 구축, 시스템 백업 순으로 중요성을 인식하고 있었다. 특히 랜섬웨어 대응 솔루션 구축이 필요하다는 응답이 48.70%로 눈에 띄었으며, 전반적으로 전체 선택항목에서 높은 응답율을 보이고 있어 랜섬웨어에 대한 대응을 위해서는 단위보안이 아닌 종합적인 대책이 필요함을 역설적으로 보여주고 있다.

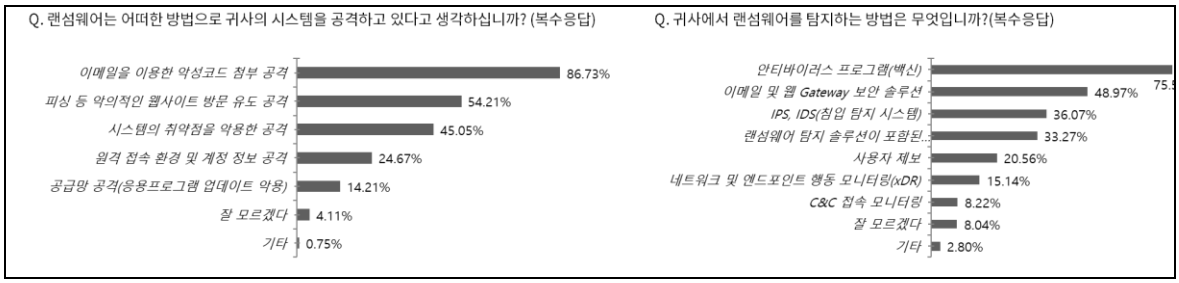


마지막 질문항목으로 피해경험이 없는 기업에서 랜섬웨어 피해를 당한다면 공격자에게 과연 비용을 지불해 문제를 해결할 의향이 있는지를 확인했는데, 56.23%의 응답 기업에서는 비용을 지불하지 않을 것으로 응답했으나, 39.13%의 기업은 잘 모르겠다고 응답했으며, 4.64%의 기업은 비용을 지불할 의향이 있는 것으로 나타났다. 잘 모르겠다는 응답이 상황에 따라 할 수도, 안 할 수도 있다는 응답임을 감안한다면, 데이터 및 시스템의 중요도에 따라 약 45%의 기업은 랜섬웨어 피해를 복구하기 위해 몸값을 지불할 용의가 있는 것으로 판단해 볼 수 있다.

3.2.3 랜섬웨어 대응능력(탐지, 치료 및 복구)

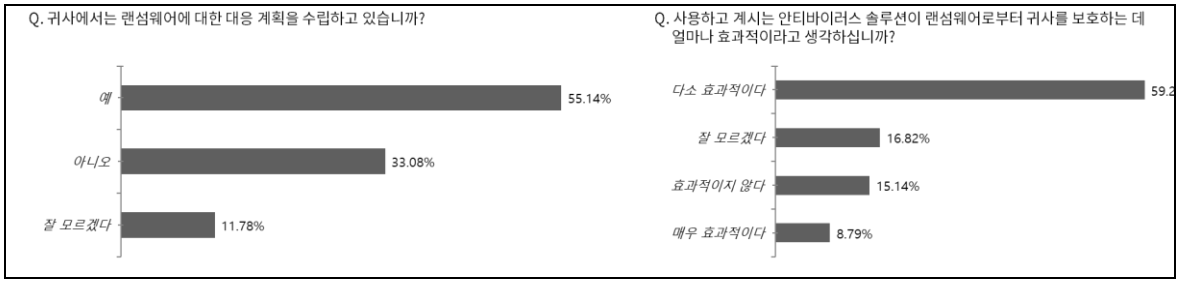
이번 섹션은 랜섬웨어 공격을 탐지하고 피해발생시 치료 및 복구를 위해 기업에서 어떤 대응체계를 갖추고 있는지를 묻는 설문으로 구성되었으며, 랜섬웨어가 일반적으로 기업에 어떻게 유입이 되고 얼마나 효과적으로 탐지할 수 있는지, 어떤 시스템이 랜섬웨어에 효과적으로 대응하는지를 알아보았다.

응답기업의 86.73%는 이메일을 이용한 악성코드 첨부를 통해 랜섬웨어가 감염되는 것으로 응답했고 피싱 등 악의적인 웹사이트 방문(54%), 시스템 취약점을 악용한 공격(45%), 원격 접속 환경 및 계정 정보를 이용한 공격과 공급망 공격 등의 순서로 기업에 공격을 시도하고 있는 것으로 나타났다.



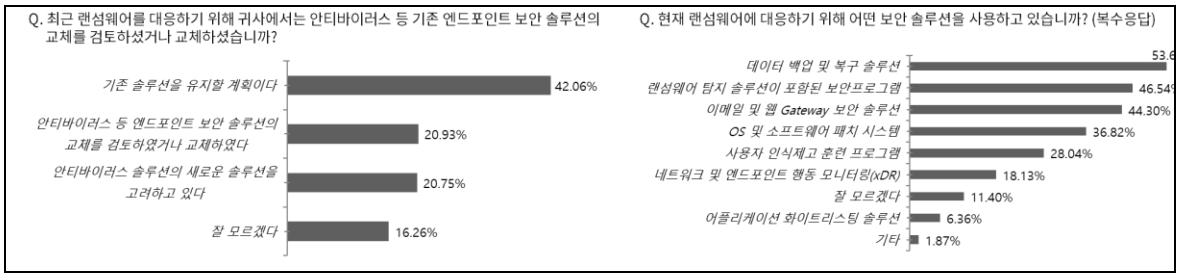
랜섬웨어를 탐지하는 방법으로 75.51%가 안티바이러스 프로그램(백신)에서 랜섬웨어를 탐지하고 있으며, 이메일 및 웹 게이트웨이 보안솔루션이 48.97%, IPS 및 IDC를 통한 탐지가 36%로 나타났다. 랜섬웨어 탐지 솔루션이 포함된 보안프로그램을 이용한 탐지의 경우도 33.27%로 응답됐으며, 뒤를 이어 사용자 제보(20.56%), 네트워크 및 엔드포인트 행동 모니터링(xDR) 시스템을 이용한 탐지(15.14%), C&C 접속 모니터링을 이용한 탐지(8.22%) 등의 순으로 나타났다. 기타 의견으로 자체 대응이 아닌 외부업체를 이용한 대응이라는 답변도 있다.

응답기업의 55.14%는 랜섬웨어에 대한 대응계획을 수립하고 있었으며, 준비하고 있지 못한 기업이 33.08%, 잘 모르겠다고 응답한 기업이 11.78%로서 약 45%의 기업에서는 랜섬웨어에 대한 대응을 제대로 수립하지 못하고 있는 것으로 나타났으며, 기존에 사용하고 있는 안티바이러스 솔루션(백신)이 랜섬웨어로부터 공격을 얼마나 효과적으로 방어하고 있는지에 대한 응답으로는 68%의 기업이 매우 효과적이거나 다소 효과적이라고 응답했다.



마지막으로 랜섬웨어를 대응하기 위해 기업에서는 안티바이러스 등 기존의 엔드포인트 보안솔루션의 교체를 검토한 적이 있거나 교체를 했는지에 대한 질문으로, 응답기업의 42%는 기존 솔루션을 유지할 계획이며, 20%의 기업은 보안솔루션 교체를 검토했거나 교체한 것으로 나타났다. 또한 추가로 새로운 솔루션을 고려하고 있다는 응답도 20%를 차지했다.

또한 현재 랜섬웨어에 대응하기 위해 사용하고 있는 보안솔루션으로는 데이터 백업 및 복구 솔루션이 가장 높은 53%의 비중을 보였으며, 랜섬웨어 탐지 솔루션이 포함된 보안프로그램이 46%, 이메일 및 웹 게이트웨이 솔루션이 44% 순으로 각각 확인됐다.

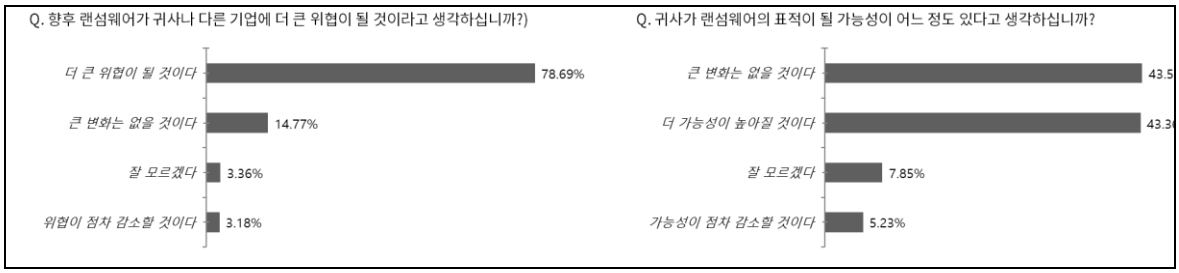


3.2.4 랜섬웨어 전망 및 예방

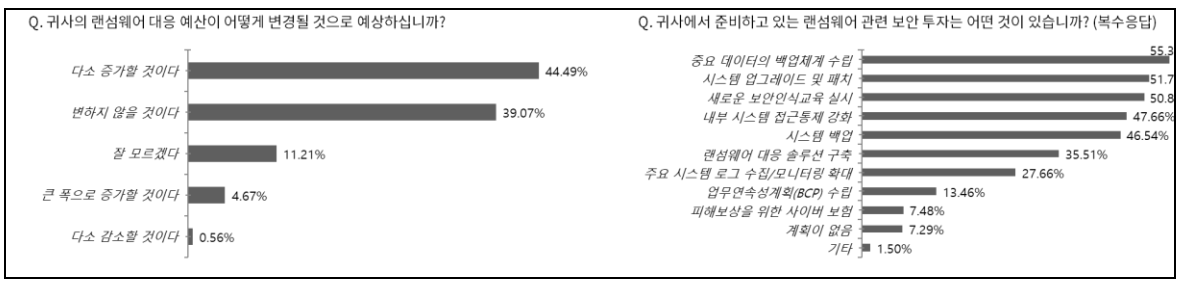
이번 설문의 마지막 섹션에서는 기업에서 판단하는 랜섬웨어의 전망과 이를 대비하는 전반적인 예산 및 투자의 증감여부 등을 알아보았다. 응답자의 93%는 랜섬웨어가 더 큰 위협이 될 것으로 걱정하고 있었으며, 44%는 랜섬웨어의 예산이 다소 증가할 것으로 예상했다.

먼저 향후 랜섬웨어가 기업에 더 큰 위협이 될 것이라고 생각하는지에 대한 설문결과 응답기업의 78%기 더 큰 위협이 될 것으로 생각하고 있었고, 14%는 큰 변화는 없을 것으로 응답했다. 반면 랜섬웨어의 위협이 점차 감소할 것으로 생각하는 비율도 3% 정도로 나타났다.

이러한 랜섬웨어의 위협속에서 응답기업이 앞으로 그 표적이 될 가능성이 있는지를 알아보는 설문에서 응답기업의 43%는 큰 변화가 없을 것으로 보는 반면, 같은 비율(43%)의 기업에서는 랜섬웨어 표적공격의 대상이 될 가능성이 더 높아질 것으로 생각했다. 가능성이 점차 감소할 것이라는 응답도 있다(5%).



그렇다면 기업에서 랜섬웨어에 대한 예산은 어떻게 변화할까? 응답기업의 4%가 랜섬웨어 대응 예산이 큰 폭으로 증가할 것으로 응답했고, 44%는 랜섬웨어 대응예산이 다소 증가할 것으로 생각했으나, 변화가 없을 것이라는 응답도 39%로 나타났다. 이는 앞선 설문응답에서 나타났던 대응계획을 수립하지 못하고 있는 비율(44%)과도 크게 다르지 않다.



마지막 설문은 응답 기업에서 준비하고 있는 랜섬웨어와 관련한 보안투자는 어떤 것이 있는지에 대한 설문으로, 중요 데이터의 백업체계 수립, 시스템 업그레이드 및 패치, 새로운 보안인식교육 실시, 내부접근통제 강화, 시스템 백업 순으로 응답했다. 또한 랜섬웨어 대응솔루션을 구축하고 주요 시스템 로그수집 및 모니터링 확대, BCP 계획 수립 및 피해보상을 위한 사이버 보험을 준비하는 계획들도 확인됐다.

3.3 설문조사 총평

이번 설문조사의 응답기업의 85%는 중견 및 중소형 기업으로 상대적으로 보안비용투자가 큰 대기업을 대상으로 한 결과가 아니였으며, 실제 현실에서 산업규모, 업종 별로 다양한 기업의 CISO 및 보안담당자의 입장에서 바라본 랜섬웨어에 대한 현황을 조사했다는 점에서 큰 의미를 가지며, 설문조사를 통해 나타난 결론을 아래와 같이 다시 한번 요약해 볼 수 있다.

- 94.8%의 기업이 랜섬웨어가 회사 비즈니스에 위협이 될 것으로 우려하고 있다.
- 절반 가까운 기업들이 랜섬웨어 피해경험이 있으며, 이중 7%의 기업은 실제 공격자에게 비용을 지불한 경험이 있다.
- 실제 피해가 발생한다면 기업의 50%는 비용을 지불해서라도 복구를 시도할 것으로 보인다.
- 절반 가까운 기업들이 랜섬웨어에 대한 대응계획을 아직 수립하지 못하고 있다.

이번 리포트 전반에서 다루어 지겠지만, 랜섬웨어는 새로운 변종이 계속해서 나타나고 있고, 공격을 실행하는 방법의 진화와 비례해 피해 또한 더욱더 커지고 있다. 설문조사에서도 많은 기업에서 랜섬웨어를 큰 위협으로 인식하고 있었으며, 앞으로도 더욱 위협이 커질 것으로 인식하는 것으로 나타났지만, 아직까지 대응체계를 갖추지 못한 기업도 상당수에 이르는 것으로 조사됐다.

새로운 랜섬웨어의 공격이 향후 지속적인 위협이라면, 기업의 입장에서도 취약한 부분을 점검하고 본 리포트에서 제시되는 랜섬웨어 대응방안을 충분히 숙지하고 검토하는 것이 필요할 것이다.

4. 랜섬웨어 방어 및 대응 전략

4.1 랜섬웨어의 관리적 대응 방안

핵심업무를 지원하는 IT 시스템이 랜섬웨어에 감염되면 해당 시스템을 사용할 수 없게 되고 기업의 업무가 마비된다. 무엇보다도 랜섬웨어에 공격당하지 않도록 관리적·기술적·인적 보안조치를 통하여 예방에 최선을 다해야 하겠지만 최악의 경우 랜섬웨어에 감염되어 핵심업무가 마비되는 시나리오에 대비하지 않을 수 없다. 그러므로, 랜섬웨어 감염 발생으로 업무중단 시 기업이 치명적인 피해를 당하지 않고 목표한 시간내에 업무를 재개하기 위해 기업은 랜섬웨어 대응을 위한 업무연속성계획(BCP, Business Continuity Planning)을 사전에 준비할 필요가 있다.

랜섬웨어 대응 업무연속성계획은 기업이 랜섬웨어에 감염되어 업무가 중단된 상황에서 미리 준비된 절차를 통해 기업의 핵심적인 업무가 지속될 수 있도록 사전에 준비된 비상대응 절차다. 랜섬웨어 대응 업무연속성계획은 감염예방을 위한 노력과 주요 정보가 암호화 되었을 때를 대비해 복구하기 위한 사전준비가 포함되며 랜섬웨어 감염 후 비상대응조치와 업무복구 및 재개를 위한 절차로 구성된다.

랜섬웨어 대응 업무연속성계획(BCP)을 통해 기업은 업무 중단시간을 최소화하여 재무적 손실을 최소화하고 체계적이고 투명한 대응을 통해 오히려 기업의 신뢰도를 높이는 기회로 만들 수 있다. 랜섬웨어 감염대응을 위한 업무연속성계획의 주요내용은 아래 표와 같다.

비상조직체계 구성 및 역할정의	랜섬웨어 감염으로 핵심업무가 중단 상황에서 체계적인 대응을 위해 비상조직체계를 사전에 구성하고 조직별, 개인별 역할을 명확히 규정한다.
기업의 핵심업무 및 이를 지원하는 IT시스템 식별	랜섬웨어 감염 상황에서도 반드시 운영하거나 복구 되어야 하는 핵심업무의 종류 및 범위를 선정하고 이를 지원하는 IT시스템을 식별한다.
업무연속성을 유지하기 위한 필요 자원 파악 및 준비계획 수립	핵심업무를 지원하는 IT시스템을 운영하는데 필요한 핵심인력과 필수 자원의 종류와 양을 파악하고 해당 시스템이 랜섬웨어에 감염되어 시스템이 정지되고 주요 정보가 암호화되는 시나리오를 상정하여 시스템 재개 및 정보복구 계획을 마련한다.
의사소통계획 수립	임직원, 고객, 협력업체, 정부부처 등 내·외부 비상 연락망을 구축하고 비상시 임직원들의 행동지침을 마련하여 교육한다.
랜섬웨어 감염 발생 상황에서의 대응방법 숙지	IT시스템 운영자는 핵심업무를 지원하는 시스템의 중요 정보가 암호화되어 서비스 운영이 중단된 상황에서도 업무재개에 필요한 정보를 복구하고 시스템을 재개하는 절차에 익숙해야 한다.

표 14. 랜섬웨어 감염대응을 위한 업무연속성계획의 주요내용

4.1.1. 랜섬웨어 감염대응을 위한 비상조직체계

평상시에 기업은 랜섬웨어 감염예방을 위한 활동을 수행함과 동시에 랜섬웨어에 언제 어떤 방법으로 공격당할지 모르기 때문에 랜섬웨어 감염 상황으로부터 체계적으로 회복하기 위한 비상조직체계를 구성해야 한다. 랜섬웨어 대응 비상조직은 랜섬웨어 감염되어 업무가 중단된 상황에서 사전에 준비된 복구계획에 따라 비상대응 및 업무복구를 수행한다.

랜섬웨어에 감염되어 기업의 정보가 암호화되면 해당 정보를 복호화 키없이 복구하는 것은 계산적으로 불가능하기에 기업은 주요 데이터를 안전하게 백업하고 보호하는데 우선적인 노력을 기울여야 한다. 그러므로 기업은 평상시 핵심업무를 지원하는 IT시스템을 식별하고 해당 시스템을 복구하는데 필요한 하드웨어 및 응용 소프트웨어를 파악하고, 자체 개발한 소스, 데이베이스, 자료, 설정 파일 등을 식별하여 이들을 주기적으로 백업하고 복구하는 절차를 모의훈련을 통하여 개선하는데 중점을 두어야 한다.

랜섬웨어 감염대응을 위한 비상조직체계는 최고 의사결정 기구인 비상대책위원회와 비상대응과 복구조직을 총괄하는 비상대책팀을 중심으로 구성된다. 비상대책팀은 비상대응팀, 업무복구팀, 커뮤니케이션팀과 경영지원팀 사이의 업무 협업 및 업무조율을 통해 IT시스템을 복구하고 핵심업무를 재개하는 역할을 수행한다. 기업의 규모 및 조직의 특성에 따라 기업은 각기 다른 형태의 비상대응조직을 구성할 수 있다. 물리적으로 해당 팀이 존재할 수도 있고 가상조직으로 구성될 수도 있으며 한 사람이 여러가지 역할을 담당할 수도 있다. 그렇지만 각 팀의 역할과 책임이 한 사람 이상으로 지정되어 업무재개시 병목이 생기지 않고 위기시에 비상대응이 병렬적으로 수행 될 수 있도록 해야한다. 비상대응시에는 관련 정부부처와의 협업 및 기술적·법률적 자문 등도 고려해야 한다.

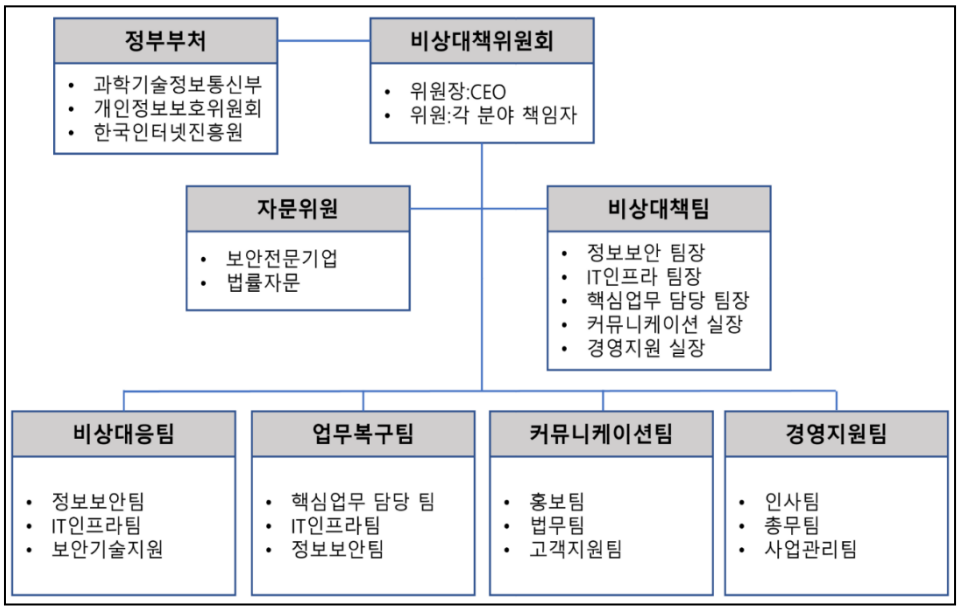


그림35. 랜섬웨어 대응 비상조직 사례

4.1.2. 랜섬웨어 대응 비상조직의 역할 및 책임

기업의 핵심업무를 지원하는 IT시스템이 랜섬웨어에 감염된다면 전사적으로 업무가 중단되고 모두들 어떻게 할지 몰라 극도의 혼란에 빠지게 된다. 그리고, 사내 및 사외 관련 이해관계자들로부터 기업의 현재 상황을 파악하기 위해 엄청난 양의 문의전화가 쏟아질 것이다. 이 때 랜섬웨어 대응 비상대응 조직은 위기상황을 통제하고 준비된 절차에 따라 업무를 재개하는 역할을 수행한다. 이를 위해서 비상대응 조직은 평상시에 랜섬웨어를 예방하고 탐지하여 처리하는 역할을 수행하고 랜섬웨어 감염 상황을 가정한 복구절차를 만들고 검증 및 개선하는 역할을 수행해야 한다.

비상대응조직은 랜섬웨어에 감염되어 업무가 중단된 위기상황에서도 기업의 피해를 최소화하고 목표한 시간내에 업무를 재개하기 위해 아래와 같은 역할과 책임에 따라 대응을 해야 한다.

■ **비상대책위원회**

비상대책위원회는 CEO가 위원장 역할을 하고 각 분야별 책임자(CFO, CIO, CISO, CPO 등)로 구성된다. 비상대책위원회의는 평상시에는 정보보안관리체계 및 업무연속성관리체계를 수립하여 최선의 정보보안 수준이 유지되고, 업무연속성계획을 준비 할 수 있도록 리더십을 발휘해야 한다. 비상시에는 현재의 피해상황을 신속하게 파악하고 상황을 통제하여 랜섬웨어 대응 및 업무재개를 위한 지휘센터로서의 역할을 수행해야 한다.

■ **정부부처**

랜섬웨어가 기업 내부에 전반적으로 감염이 일어나게 되면 과학기술정보통신부에 침해사고 신고를 해야한다. 또한, 개인정보가 유출된 정황이 파악된다면 개인정보보호 위원회에 개인정보 유출 신고를 해야 한다. 한국인터넷진흥원은 두 기관을 대신하여 해킹신고 및 개인정보유출 신고를 접수 받을 뿐만 아니라 해킹사고 및 개인정보유출에 대한 원인파악을 하는데 기술적 지원을 제공 할 수 있다.

■ **자문위원**

랜섬웨어 감염에 의한 비상대응 시 랜섬웨어 감염 경로 등을 찾아내고 대응하는데 자체적인 기술력이 부족할 수 있으므로 이런 상황을 대비하여 보안전문기업과 기술자문 계약을 검토할 필요가 있다. 그리고, 정부부처에 신고하거나 고객응대를 하는 과정에서도 컴플라이언스에 위배되는지 체크하고 법정소송에 대비하여 법률적 자문을 검토할 수 있다.

■ **비상대책팀**

비상대책팀은 평상시 랜섬웨어에 감염에 대비한 업무연속성계획을 마련하고 주기적인 모의훈련을 통해 지속적으로 업무연속성계획을 개선해야 한다. 이를 위해 핵심업무를 식별하고 이를 지원하는 IT시스템을 파악하여 해당 시스템이 랜섬웨어에 감염되는 리스크 시나리오를 작성하여 복구전략 및 복구계획을 수립한다. 해당 복구계획이 정상적으로 동작하는지 확인할 수 있도

록 주기적인 모의훈련을 통하여 효과성을 측정하여 지속적인 개선을 할 수 있도록 한다. 위기시에는 각 팀으로부터 수집되는 피해상황을 정리하여 비상대책위원회에 보고하고 의사 결정된 사항을 각 대응팀을 통해 수행하게 하고 관리하는 역할을 한다.

■ 비상대응팀

비상대응팀은 평상시 랜섬웨어 감염을 사전에 예방하고 신속하게 탐지하기 위한 업무를 수행한다. 이를 위해 정기적으로 시스템의 취약점을 파악하여 제거해야 하고 이상 징후를 탐지하여 조치해야 한다. 임직원의 실수로 랜섬웨어에 감염되는 것을 예방하기 위해 수시로 APT 메일 모의훈련을 하고 보안캠페인 및 보안교육을 통해 임직원의 보안의식을 높여야 한다. 비상대응팀은 비상시에는 랜섬웨어 감염을 탐지하거나 신고를 받고 랜섬웨어의 감염경로를 파악하여 제거하는 역할을 한다. 이때 좀비가 된 IT장비를 모두 찾아서 악성코드를 제거하지 않으면 시스템을 복구 했다고 하더라도 다시 랜섬웨어에 재감염 될 수 있으므로 주의해야 한다.

■ 업무복구팀

핵심업무를 지원하는 IT시스템의 복구조직은 IT인프라팀 및 개발 운영팀 등으로 구성되며 이들은 비상시 랜섬웨어 감염에 대비한 업무연속성계획에 따라서 백업 데이터를 획득하여 핵심업무 시스템을 복구하여 정상화 해야 한다. 그러므로 평상시에는 핵심 IT시스템별 복구계획서를 작성하고 지속적인 개선을 해야한다. 특히, 업무복구팀은 주요 정보의 백업 및 복구하는 책임을 가진다. 파악된 핵심 IT시스템을 복구하는데 필요한 정보에 대하여 복구목표시간과 복구목표시점을 고려하여 백업주기와 백업방법 선정한다. 그리고, 백업계획에 따라 주기적으로 백업을 수행하고 점검한다. 복구 필요시 백업본을 이용하여 신속하게 IT시스템을 복구할 수 있도록 지원해야 한다. 주의할 점은 백업을 하는데 필요한 총시간과 효율성을 고려하는 것도 필요하지만 복구시간이 중요한 경우에는 얼마나 빠른 시간 내에 복구 가능한지를 고려하여 백업방법을 선정해야 한다.

■ 커뮤니케이션팀

홍보부서는 사내·외 의사소통을 위한 주요 메시지를 작성하고 전파하기 위한 역할을 수행한다. 랜섬웨어에 감염되어 업무가 마비 된다면 기업을 둘러싸고 있는 많은 이해관계자와 긴밀하고 적절한 수준의 일관된 의사소통이 무엇보다 중요하다. 대외 커뮤니케이션은 주로 홍보부서에서 담당을 하고 내부 이해관계자로부터 수집된 정보를 정리하여 비상대응위원회의 검토를 거쳐 외부에 제공될 필요가 있다. 홍보부서에서는 랜섬웨어 감염을 상정한 모의훈련을 통해 대내외 의사소통 스크립트를 미리 작성하고 미비점을 보완해야 한다.

■ 경영지원팀

경영지원팀은 평상시에는 위기대응에 필요한 인력 및 비용, 시설 등을 식별하여 미리 준비했다가 비상시 위기대응조직에게 필요한 자원을 제공하고 이들의 업무를 지원하는 역할을 수행한다.

4.1.3 랜섬웨어 감염 예방대책

랜섬웨어의 공격이 기존의 보안 위협과 다른 점은 기업이 보유하고 있는 개인정보 등 중요 정보 자산에 대해 암호화를 통해 이용권을 박탈하고 탈취한 정보의 유통을 빌미로 금전적 거래를 요구하고 있어 그 피해의 영향도가 해당 기업 뿐만 아니라 사회 전반에 미칠 수 있다는 점이다. 따라서, 랜섬웨어 공격에 노출되지 않도록 사전 대응 체계를 마련 하는 것은 매우 중요하다.
랜섬웨어의 감염은 주로 다음과 같은 경로를 통해 이루어 진다.

- 메일의 첨부파일이나 URL의 접근을 유도함으로써 사용자 PC 감염
- 취약점이 존재하거나 조작된 웹페이지에 사용자의 접근을 유도하여 사용자
- PC감염
- 외부매체나 네트워크를 이용한 파일 동기화를 통한 감염
- 네트워크에 노출된 시스템의 취약점 을 이용한 감염

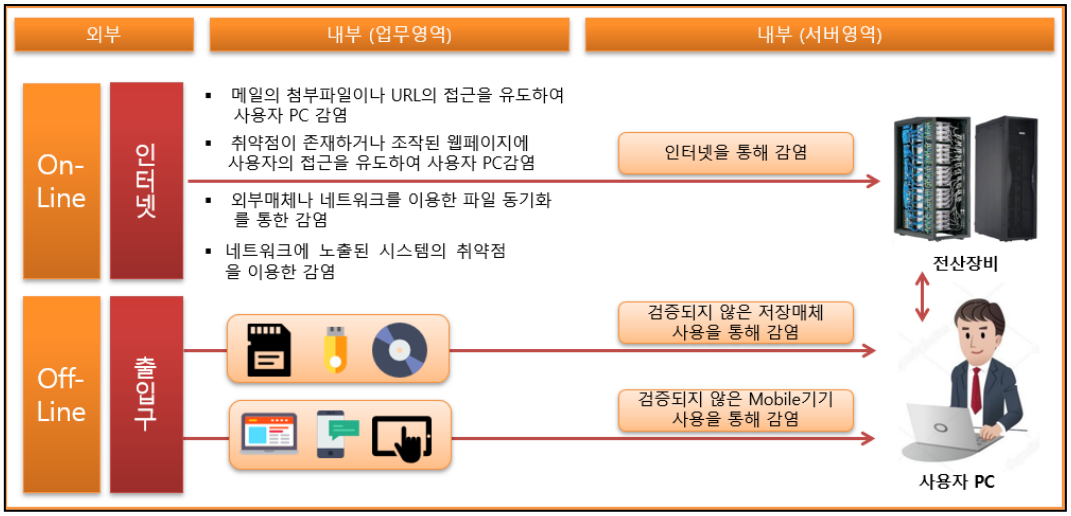


그림 36. 랜섬웨어 감염 예상경로

우리는 랜섬웨어의 감염 경로에 대해 대응 방안을 강구함으로써 공격의 피해로부터 사전 예방이 가능하다. 다만, 모든 전략을 구현하기에는 시간과 비용 등 많은 자원의 투자가 필요한 만큼 기업의 사정과 환경을 고려하여 효과적이며 효율적인 대응전략의 수립이 필요하다.

구분	예방 대책	사고 대응체계
주요활동	. 지속적 피싱메일 대응 모의훈련/교육 . SW 최신 업데이트/통합관리 . 백업/복구체계 구축/훈련 . 악성코드 탐지/차단 (24x365)	. 보안사고 신고/ 공동 비상대응 . 감염경로추적 및 확산방지 조치 . 백업데이터 복구 수행 . 재발방지대책 수립/조치

보호대책 (보안솔루션)	. URL Filter, Firewall, IPS/IDS, 복호화 . SPAM Mail Filter . Malware Sand Box . Network Forensic Tool . SIEM (Security Info. Event Mgt.) . EDR (Endpoint Detection & Response)	. C&C(악성코드 유포지) 접속차단 . 피싱메일 차단(발송자,첨부,컨텐츠) . 악성코드 분석/탐지 . 감염확산 경로추적 . 보안 이벤트 통합 로그분석/관제 . 단말의 상세 로그분석/대응

표 15. 예방 대책과 사고 대응 체계

랜섬웨어 감염사례 대다수가 피싱메일을 통해서 이루어지는 만큼 피싱메일에 대한 모든 사용자의 효과적인 대응이 가능하다면 이보다 더 좋은 랜섬웨어 예방대책은 없을 것이며, 이를 위한 피싱메일 대응훈련과 교육을 진행하는 기업 및 단체가 점차 증가하고 있다.

1단계	훈련 내용 과 방식 선정 (훈련 서비스 이용 or 훈련 시스템 구축)		준비
2단계	훈련용 피싱메일 발송 (훈련은 불시에 시행이 효과적)		모의훈련
3단계	피싱메일 신고 → 접수(보안팀)	피싱메일 링크 클릭시→ 감염	
4단계	훈련결과 공유 (감염자/감염부서 순위 공개)		경영층 보고
5단계	감염자 및 상위 감염부서 대상 재교육/훈련		감염자 교육

표 16. 피싱메일 대응훈련 시나리오 및 훈련시 감염률 변화추이

피싱메일 대응훈련이 입사시 또는 1~2년에 한번 하는 형식적인 절차에 그친다면 기대할 수 있는 효과는 크지 않을 것이며, 매월 또는 매 분기마다 시행하고 최고 경영층을 포함한 전 직원이 지속적으로 참여한다면 랜섬웨어 예방효과는 그 어떤 보안시스템보다 효과적일 것이다.

이러한 랜섬웨어의 감염예방 및 대응체계를 주요 활동 과 보안솔루션의 측면에서 아래와 같이 “랜섬웨어 감염예방 및 대응체계”를 운영중인 사례를 참조 할 수 있다. 물론 각 조직의 환경과 여건에 따른 보다 효과적인 대책과 대응체계는 각 조직의 보안조직과 더불어 모든 구성원의 공동 노력이 필수적일 것이다.

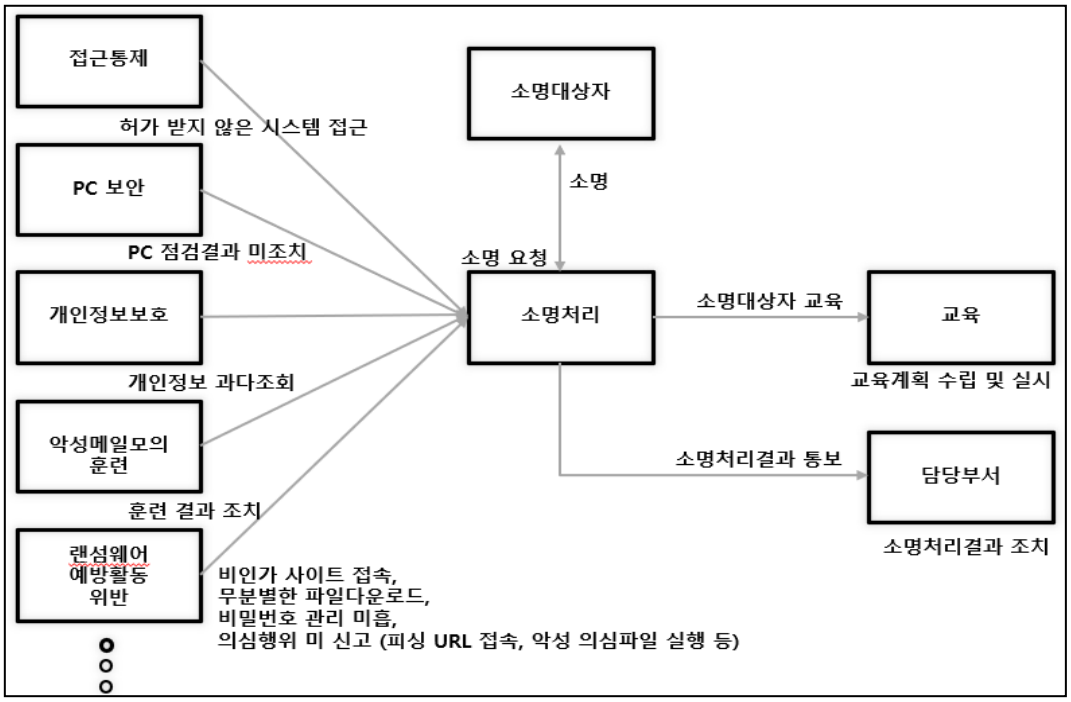


그림37. 보안인식 강화를 위한 소명처리 프로세스

이러한 피싱메일 보안 훈련이 신입사원 교육 또는 1년에 한번 하는 형식적인 훈련에 그친다면 효과는 크게 나타나지 못할 수 있다. 보안 교육/훈련이 정말로 효과가 있으려면 훈련횟수를 늘리고 CEO가 참여해야 한다. 최고경영자를 포함한 전 임직원이 참여하여 회사의 의사결정권자가 보안훈련을 중시한다는 것을 전 직원이 인식 할 경우, 보안교육/훈련은 그 효과는 극대화 될 것이다.

4.1.4 랜섬웨어 감염시 신고절차

기업의 주요 시스템에 랜섬웨어가 감염되었다면 이미 상당기간 APT 공격이 진행되어 사내의 주요 자료 및 개인정보가 암호화 됨과 동시에 외부로 유출되었을 가능성이 있으므로 침해사고 신고와 함께 개인정보 유출사고 신고를 검토해야 한다. 침해사고시에는 과학기술정보통신부 또는 KISA에 즉시 신고해야 하고 개인정보가 유출된 경우에는 신고대상 및 신고기준에 따라 신고기한 내에 개인정보보호위원회 또는 KISA에 신고해야 한다.

랜섬웨어 감염으로 인한 침해사고는 '보호나라 홈페이지 (https://boho.or.kr) > 상담 및 신고 > 해킹 사고' 또는 사이버민원센터 '국번없이 118'로 신고 할 수 있다. 이에 더하여 개인정보가 유출된 정황이 파악되면 '개인정보보호 포털(https://privacy.go.kr) > 민원마당 > 개인정보 유출· 침해신고'에 개인정보 유출신고를 할 수 있다.

구분	침해사고 신고	개인정보 유출 신고		
		개인정보처리자	정보통신서비스제공자	상거래 기업 및 법인
근거법령	정보통신망법 제48조의3	개인정보보호법 제34조	개인정보보호법 제39조의4	신용정보의 이용 및 보호에 관한 법률 제39조의4
신고대상	정보통신서비스제공자 집적정보통신시설 사업자	공공기관 및 민간기업 (정보통신서비스제공자 제외)	정보통신서비스제공자	상거래 기업 및 법인 (금융위 감독을 받는 곳은 제외)
신고기관	과기정통부 및 KISA	개인정보보호위원회 및 KISA		
신고기한	즉시	지체없이(5일이내)	지체없이(24시간이내)	지체없이
신고기준	-	1천명 이상 정보주체의 개인정보 유출 시	1건이라도 정보주체의 개인정보 유출 시	1만명 이상 이용자의 개인신용정보가 업무목적외로 누설되었음을 알게된 때
과태료	1천만원 이하	3천만원 이하		

표17. 개인정보·정보보호 침해사고 신고 바로알기, 출처 : KISA

랜섬웨어 감염으로 인한 해킹 사고 신고의 경우 랜섬웨어 감염이 확인되는 즉시 신고해야 하므로 우선적으로 기업의 랜섬웨어 감염상황을 정리하여 신고한다. 랜섬웨어 감염으로 인한 개인정보 유출 신고의 경우 신고기한 내에 유출된 개인정보의 항목 및 규모, 유출된 시점과 그 경위를 정확하게 파악하기 어려울 수 있으므로 우선 파악된 내용을 기준으로 신고하고 추후 내용이 파악되는 대로 보완 한다.

침해사고 신고 및 개인정보 유출 신고를 할 때는 랜섬웨어 감염으로 기업의 업무가 마비된 극도로 혼란한 상황이기 때문에 사전에 모의훈련을 통해 신고양식 중 고정된 부분을 미리 채워 두고 변경된 내용만 추가하여 신고할 수 있도록 사전에 준비하는 것이 좋다. 그리고, 외부 기관에 신고할 때에는 실무부서에서 개별적으로 진행하기 보다 비상대응팀에서 책임을 가지고 진행하며 법률자문을 받아 비상대책위원회에서 최종 검토하고 신고하는 것이 안전하다.

그림38. 홈페이지 신고 : 보호나라 홈페이지 (https://boho.or.kr) 〉 상담 및 신고 〉 해킹사고

4.1.5 랜섬웨어 관리적 대응 체크리스트

기업이 랜섬웨어 감염에 대비하여 사전에 준비해야 할 관리적 주요 목록을 아래와 같이 체크리스트로 정리하였다. 기업이 랜섬웨어 감염에 어느정도 대비하고 있는지 스스로 체크리스트를 따라 점검하고 미흡한 부분에 대해서는 경영진의 지원을 받아 개선할 필요가 있다.

■ **비상 조직체계 정비**

주요 내용	완료	진행중	미수행
랜섬웨어 감염 시 즉시 가동할 수 있는 비상조직체계를 구성하였는가?			
랜섬웨어 대응 비상조직을 구성하는 대응팀과 구성원의 역할과 임무가 명확히 규정되어 있는가?			

■ **핵심업무 및 IT시스템 식별**

주요 내용	완료	진행중	미수행
기업의 핵심업무를 파악하고 우선순위를 도출하였는가?			
핵심업무를 지원하는 IT시스템을 식별하였는가?			
해당 IT시스템이 랜섬웨어에 감염되어 업무가 중단될 경우 해당 시스템을 복구하기 위해 필요한 자원을 도출하였는가?			
해당 IT시스템의 업무를 재개하는데 필요한 주요 정보를 복구목표시점(RPO)에 따라 주기적으로 백업하고 있는가?			
해당 IT시스템의 취약점을 주기적으로 점검하고 발견된 취약점을 조치하고 있는가?			

■ **비상 연락망 구축 및 내·외부 커뮤니케이션**

주요 내용	완료	진행중	미수행
임직원, 협력업체, 주요고객 등 비상연락처 목록을 정기적으로 업데이트하고 있는가?			
랜섬웨어 감염 신고 등 악성코드 감염 시 의사소통이 원활하게 이루어지고 있는가?			
랜섬웨어 감염 예방 및 대응, 신고를 위한 교육이 실시되고 있는가?			

■ 랜섬웨어 감염으로 인한 위기상황 대응

주요 내용	완료	진행중	미수행
랜섬웨어 감염 발생시 조직내 신고 및 대응책을 마련하고 모든 구성원에게 전파하였는가?			
랜섬웨어를 포함한 악성코드의 감염경로를 파악하고 제거하는데 필요한 기술적·인적 자원을 준비하였는가?			
정부부처에 해킹사고 신고 및 개인정보유출 신고 절차를 마련하였는가?			

■ 복구 및 사후조치

주요 내용	완료	진행중	미수행
업무 중단 후 시간의 흐름에 따라 예상되는 피해정도(금전적 영향, 고객관계 등)와 복구 소요시간을 파악하였는가?			
핵심업무를 지원하는 IT시스템에 대하여 가용할 수 있는 자원상황을 고려하여 우선순위에 따른 복구진행계획이 수립되어 있는가?			
랜섬웨어 감염되어 주요 정보가 암호화되고 서비스가 중단 된 상황으로부터 정상화되는 계획이 마련되어 있는가?			
랜섬웨어 감염 발생 시나리오에 대응하여 백업복구 모의훈련을 수행하고 있는가?			

4.2 랜섬웨어의 기술적 대응 방안

기술적으로 랜섬웨어 대응을 위한 최적의 방안은 두말 할 필요도 없이 랜섬웨어에 걸리지 않도록 하는 사전 차단을 통한 예방을 하는 것이다. 이제 랜섬웨어의 감염/전파에 대한 기술적인 대응 방안에 대해서 알아보자.

랜섬웨어 기술적 차단 대응 방안과 관련해 NIST에서는 랜섬웨어 의 차단과 완화를 위해 조직에서 자신의 준비상태를 점검하기 위한 NIST IR 8374, Preliminary Draft를 공개하고 있으며 랜섬웨어의 대응을 위해서 식별, 보호, 탐지, 대응, 복구 등 5가지 단계에 대한 Profile을 제공하고 있다. 해당 내용을 참고해 4.2절의 대응 방안을 적용할 수 있다.

분류	하부 분류	랜섬웨어 어플리케이션
자산 관리 (ID.AM)	ID.AM-2: SW 플렛폼과 어플리케이션	현재 설치된 SW 이름, 버전, 장비들에 대한 정보를 모두 식별 하고 취약점이 있는 경우 패치가 되었는지 확인해야 함
	ID.AM-3: 조직의 통신 및 데이터 흐름	공격자에 의한 내부망 공격시 어떠한 정보의 흐름이 위험한지를 식별해야 함
	ID.AM-4: 외부 정보 시스템	랜섬웨어 이벤트 발생시 일시적인 통신 단절에 대비한 외부 파트너와의 대응 연락 체계를 갖추기 위해 외부와의 연결을 모두 식별하고 위험 요소를 컨트롤 할 수 있게 해야 한다.
위험 평가 (ID, RA)	ID.RA-1 : 자산 취약점 식별 및 문서화	조직 자산의 취약점을 식별하고 문서화 하고 지속적으로 취약점에 대해서 완화 혹은 제거해 나간다면 향후 랜섬웨어 발생 가능성이 줄어든다.
공급망 위험 관리 (ID, SC)	ID.SC-5 : 대응 및 회복 계획 및 테스트는 공급업체 및 타사 공급업체와 함께 수행	랜섬웨어 비상 계획은 공급업체와 타사 공급업체와 함께 조정하며 계획에는 활동을 테스트 하기 위한 조항이 포함돼야 한다. 계획에는 공급업체와 타사 공급업체가 영향을 받는 부분이 포함돼야 한다.
신원 관리, 인증 및 접근 제어 (PR.AC)	PR.AC-1 : 승인된 장치, 사용자 및 프로세스에 대해 신원 및 자격 증명이 발급, 관리, 확인, 취소 및 감시된다.	대부분의 랜섬웨어 공격은 네트워크 연결을 통해 수행되며 랜섬웨어 공격이 자격증명손상으로 시작되므로 적절한 자격증명 관리는 필수 사항은 아니지만 필요한 완화 방법이다.
	PR.AC-3 : 원격 접속 관리	대부분의 랜섬웨어 공격은 원격으로 수행된다. 원격 접속과 관련된 권한을 관리하면 시스템의 악성 코드 삽입 및 데이터 유출로부터 보호할 수 있다. 다중 토큰 기반 인증은 계정 손상을 감소시킬 수 있다.
	PR.AC-4 : 최소 권한 및 직무 분리 원칙을 통합해 접근 권한과 인증이 관리 된다.	대부분의 랜섬웨어 침입은 사용자 자격 증명의 손상을 통해 발생하거나 권한이 부여되지 않아야 하는 프로세스를 호출 함으로 발생한다.

표18. NIST IR 8374 Profile의 기술적 부분 발취

랜섬웨어 감염 예상 경로를 이용한 공격을 탐지하고 차단하기 위해 일반적으로 기업에서 수행할 수 있는 대응방법은 다음과 같다.

구분	대응방법	
	정책/절차	수단
이메일을 통한 랜섬웨어 감염 예방을 위한 대응 상태를 확인한다.	악성코드 탐지/차단	안티바이러스
	이메일 문서첨부에 삽입된 악성 매크로 및 스크립트 탐지/차단	CDR (Content Disarm and Reconstruction)
	랜섬웨어 공격메일에 대한 필터링	메일필터링
이메일의 첨부 파일들에 대해서 동적 분석이나 패턴 기반으로 랜섬웨어 파일의 유무를 검사한다	랜섬웨어 통제절차	Attach File SandBox
원격 접속과 관련된 권한관리 및 다중 토큰 기반 인증을 사용하는지 확인한다.	원격접속관리 절차	mOTP, OTP토큰, 지문 등
최소 권한 및 직무 분리 원칙을 통합하여 접근 권한과 인증이 관리 되고 있는지 확인한다.	접근통제 절차	접근통제관리 시스템 (계정 신청,승인 등)
네트워크를 통한 랜섬웨어 Code의 발견 및 예방 통제와 방법이 구현 되어있는지 확인 한다	침해사고 대응절차	IPS, APT솔루션
랜섬웨어 Code의 이상행위 발견 및 추적 방법이 구현되었는지 확인 한다	침해사고 대응절차 (이상행위 탐지)	xDR솔루션, 포렌식 솔루션
랜섬웨어 예방통제와 이를 사용자 가 적절하게 인지할 수 있는 절차가 구현되었는지 확인한다	보안인식 교육 및 보안 위반 시 소명처리 절차	보안포털 (교육/소명 프로세스 등)
반입되는 모바일 기기/저장매체에 대한 랜섬웨어 감염 예방 수단이 존재 하고 시행 되는지 확인한다.	매체 삽입 시 자동으로 랜섬웨어 감염 파일검사	안티바이러스, 반출입통제 시스템

표19. 랜섬웨어 대응 방법

4.2.1 이메일 보안 대응

이메일은 공격자가 다양한 통제를 거치지 않고 개개인의 직원들에게 접근할 수 있는 가장 효과적인 수단이다. 이러한 점 때문에 악성코드나 계정 탈취 등의 공격들에 이메일이 사용되고 있으며, 먼저 이메일에 대한 보안을 강화하는 것만으로도 랜섬웨어의 감염 원인을 대폭 제거할 수 있다. 이는 물론 다른 악성코드나 피싱에도 함께 적용될 것이다.

강화 방안	설명	효과성
메일 필터링	메일의 수신 서버 단에서 특정 이메일 송신자에 대해서 송신자 주소, IP, 메일 제목 등에 대해서 차단을 하는 기술로서 평판 DB와 연계해 서버 단에서 랜섬웨어 공격 메일에 대한 차단이 가능한 기술이다.	랜섬웨어 공격자의 메일 송신 정보를 통한 기본적인 방어 방법이다.
CDR (Content Disarm and Reconstruction)	이메일 문서 첨부파일 (ppt, hwp, pdf etc)에 삽입된 악성 매크로나 스크립트를 제거하는 기술로 탐지/차단의 개념이 아닌 무효화 개념의 기술이다. 무효화 된 문서 파일은 원본 형식을 유지한채 스크립트나 매크로가 완전히 제거된다.	이메일 문서 첨부파일등에 스크립트나 매크로를 이용해 랜섬웨어를 유포하는 공격을 대부분 무력화 시킬 수 있다.
SPF (Sender Policy Framework)	메일 발송 서버의 정보를 DNS에 등록해 이메일의 전송자 주소와 실제 메일 서버의 IP 정보가 일치하는지를 확인하는 기술이다. Ex. 도메인에 등록된 SPF 샘플 v=spf1 ip4:35.190.247.0/24 ip4:64.233.160.0/19 ip4:66.102.0.0/20 ip4:66.249.80.0/20 ip4:72.14.192.0/18 ip4:74.125.0.0/16 ip4:108.177.8.0/21 ip4:173.194.0.0/16 ip4:209.85.128.0/17 ip4:216.58.192.0/19 ip4:216.239.32.0/19 ~all	수신자는 메일 수신 시 발송된 메일의 송신 IP와 도메인의 SPF를 비교해 이상이 있을 경우 차단 하거나 경고를 띄울 수 있다.
DKIM (Domain Keys Identified Mail)	메일을 송신하고자 하는 서버는 하나 이상의 공개키 쌍을 생성하고 DNS에 공개키를 TXT 레코드로 등록하고 송신 메일의 헤더에 서명을 추가한다. 수신 측에서는 도메인의 공개키로 수신된 메일헤더의 서명을 복호화 하고 서명을 확인하는 기술이다. Ex. 메일 헤더내의 DKIM 샘플 DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=icloud.com; s=04042017; t=1507961490; bh=gxfNbx7oBPAJBKZ0sGgbmmstq1veVnVVqv2GpmQta4A=;	디지털 서명 기술을 이용해 메일의 유효성을 검증하고 송수신자에 대해 검증하므로 출처와 전송 중 위조 등에 대한 검증이 가능하다.

DMARC (Domain-based Message Authentication, Report & Conformance)	표준 이메일 인증 방법으로 SPF, DKIM과 함께 사용되며 메일의 실제 송신자와 헤더상의 From의 도메인을 정렬 방식에 따라서 3가지 정책으로 허용, 격리, 거부로 지정해 메일에 대한 처리를 수행함으로써 인증을 강화하는 기술이다.
	
	Ex.
	v=DMARC1; p=none;
	rua=mailto:dmarc_reports@sample.com;
	ruf=mailto:dmarc_reports@sample.com
		SPF, DKIM과 함께 사용되므로 실질적인 해킹 메일이 주로 스푸핑된 것을 고려하면 스푸핑 메일에 대한 효과적인 검증이 가능하다.

Attach File Sandbox & Mail 서버 안티 바이러스	이메일의 첨부 파일들에 대해서 동적 분석이나 패턴 기반으로 악성 파일의 유무를 검사하는 기술들이다. 메일 서버에 백신을 적용하는 경우 클라이언트의 한 개 백신 대비 다수 백신의 적용이 가능하므로 효과적임	직접 첨부파일에 랜섬웨어가 첨부되어 전송될 경우 이에 대한 차단이 가능하다.

표 20. 기업에서 적용할 수 있는 메일 차단 보안 기술들

위의 방법은 일반적으로 기업에서 직접 메일 서버를 구축해 운영할 경우 적용할 수 있는 메일 공격의 방어 방법에 대해서 서술했지만, 만약 Google Gsuite의 Gmail과 같은 클라우드 환경의 메일 서비스를 사용한다면 위의 리스트에서 SPF, DKIM, DMARC에 대한 적용은 가능하므로 클라우드 환경을 사용하는 경우에도 반드시 적용하는 것이 필요하다. (참고 KISA 클라우드 서비스 보안인증제 운영 변경관리서)

위의 방안 전체를 적용한다면 당장에 랜섬웨어를 통한 감염은 많은 부분 차단이 가능할 것이라고 생각한다. 1차적으로 메일 필터링, SPF, DKIM, DMARC가 신뢰된 메일만을 필터링 하고 여기서 통과된 랜섬웨어들은 CDR과 SandBox가 추가로 차단을 수행할 수 있으므로 공격자가 이를 우회하는 데에는 어려움이 따를 것으로 보인다.

4.2.2 악성 웹 사이트와 악성 광고 대응

랜섬웨어의 유포를 위해서 웹사이트를 해킹해 조작하거나 정상적인 광고에 악성 링크를 심어 두는 경우가 다음으로 많은 전달 방법으로 나타났다. 여기서 한 가지 주의할 점은 이메일을 통한 피싱 공격에서 직접적으로 랜섬웨어 파일을 첨부해 보내는 경우는 드물며 파일을 유포하기 위해 특정 웹 사이트에 업로드하고 이메일로 링크를 보내는 경우가 많으므로 악성 웹 사이트와 이메일은 같이 운영되는 감염 방법으로 봐도 무방하다. 즉 피싱 이메일 공격의 악성 링크를 효과적으로 막는 것이 가장 중요하다.

강화 방안	설명	효과성
싱크홀 (SinkHole)	랜섬웨어 유포 사이트에 대한 IP 차단 시 HTTPS로 된 도메인 기반의 경우 공격자가 IP를 변경하면 재 접속될 위험이 있으므로 자체적으로 DNS SinkHole을 구축하여 도메인 자체의 질의를 차단해 접속을 제한하는 기술 자체 DNS 서버를 사용하는 경우 서버에서 차단하면 되며 그렇지 않을 경우 개인 PC에 설정해 사용할 수 있다.	도메인 기반으로 접근하는 암호화된 접속에 대해서 완벽히 차단이 가능하다.
인터넷 격리	인터넷을 사용하는 애플리케이션이 가상화 OS를 통해서 실행되도록 하고 사용자는 실행된 결과를 받아보는 기술로, 대표적으로 웹 브라우저의 실행은 가상 OS에서 하고 렌더링 된 결과만 사용자에게 보여주는 기술	웹을 통해 전파되는 랜섬웨어에 대해서 감염의 위험을 최소화 시킬 수 있다.

표 21. 악성 사이트와 악성 광고를 차단하기 위해 기업에서 적용할 수 있는 인프라 방안

4.2.3 웜을 통한 전파의 대응

기업의 사무 환경과 서비스 환경은 규모가 커질수록 그 복잡도가 증가하게 된다. 이로 인해 전체 망에 대한 가시성이 떨어지게 되고 적절한 접근통제 방안의 미흡으로 웜의 형태를 띄는 랜섬웨어를 통해서 외부에서의 감염 혹은 내부에 감염된 이후 다량 감염이 발생할 수 있다. 이러한 감염을 막기 위해서는 아래의 방안의 적용을 고려해 보아야 한다.

강화 방안	설명	효과성
네트워크 가시성 강화 및 접근 통제의 강화	내부와 외부에서 발생하는 트래픽에 대한 가시성 (어떠한 프로토콜의 트래픽이 어떤 방향으로 흘러가는지 등)에 대한 강화를 통해서 외부에서 랜섬웨어가 들어올 수 있는 포트가 열려 있는지를 감시하고, 내부에서 웜 성격의 랜섬웨어가 전파될 수 있는 인프라가 존재하고 포트가 열려 있는지를 파악하며, 불필요한 경우에는 내/외부의 모든 요소(접근 포트, 애플리케이션 등)를 차단한다.	SMB 웜 성격의 웜의 경우 공인 IP가 할당된 Windows 서버를 통해서 외부에서 내부 혹은 내부에서 감염되고 전파될 수 있다. 이러한 진입 지점 자체를 차단한다.
Active Directory 강화	Windows 관리를 위한 AD의 관리자 권한 탈취를 통한 다량의 랜섬웨어 감염이 발생하고 있고 백업 서버가 AD에 연결된 경우 백업 서버도 감염되므로, AD의 관리자 계정에 대한 철저한 관리와 꼭 필요한 시스템만 연결하는 등의 관리 방안을 수립해 관리해야 한다.	내부로 랜섬웨어가 침투 되었을 때 AD를 통한 다량의 전파나 전체 시스템의 장악을 힘들게 만든다.

표 22. 웜을 통한 전파 대응방안

4.2.4 사용자 환경의 기술적 대응

사용자 환경에서 랜섬웨어의 감염을 탐지, 차단 할 수 있는 방안은 다음과 같다.

강화 방안	설명	효과성
안티 바이러스	악성코드(랜섬웨어)의 감염을 차단하는 기본적인 End-Point 보호 솔루션	기 공개된 악성코드(랜섬웨어)가 실행되는 것을 차단한다.
OS 패치 (PMS)	OS 상에 존재하는 취약점 등을 통해서 랜섬웨어가 감염/전파 될수 있으므로 항상 최신의 패치를 OS에 적용한다. 다수의 사용자에게 패치를 항상 최신으로 유지하기 위해서 PMS (Patch Management System)의 도입을 검토한다.	알려진 취약점을 통해서 랜섬웨어가 감염/전파 되는 것을 최소화 할 수 있다.
EDR	End-Point 단에 설치되어 행위 기반으로 악성코드(랜섬웨어)의 감염과 전파를 탐지하고 차단하도록 하는 기술	알려지지 않은 일부 악성코드(랜섬웨어)에 대해서 탐지/차단이 가능하다.

표 23. 사용자 환경에서의 랜섬웨어 대응방안

4.3 랜섬웨어의 감염 분석

랜섬웨어는 파일을 암호화 시키고 이를 볼모로 돈을 요구한다는 점이 기존 악성코드의 성격과는 다른 점이라고 할 수 있다. 물론 랜섬웨어에 데이터 유출이나 명령을 받는 기능을 하는 유형도 있으나 목적 자체가 정보를 볼모로 하기 때문에 최종 목적이 다르다고 할 수 있으며 목적이 다르기 때문에 랜섬웨어의 내부 악성코드 패키징도 다르다고 할 수 있다.

따라서, 랜섬웨어를 탐지/차단하거나 감염되었을 때의 복구 방안에 대한 계획을 세우고자 한다면 랜섬웨어에 대한 기본적인 분석 방법에 대해서 살펴보는 것이 순서일 것이다.

4.3.1. 최초 감염 경로 분석

먼저 랜섬웨어 분석의 첫 번째는 감염 및 전파 경로의 분석이다. 랜섬웨어가 실질적으로 감염되었다면 최우선으로는 복구가 최우선이나 완료된 이후에는 반드시 감염의 전파 경로 분석을 수행해 차후 동일한 사고가 일어나지 않도록 대응해야 한다.

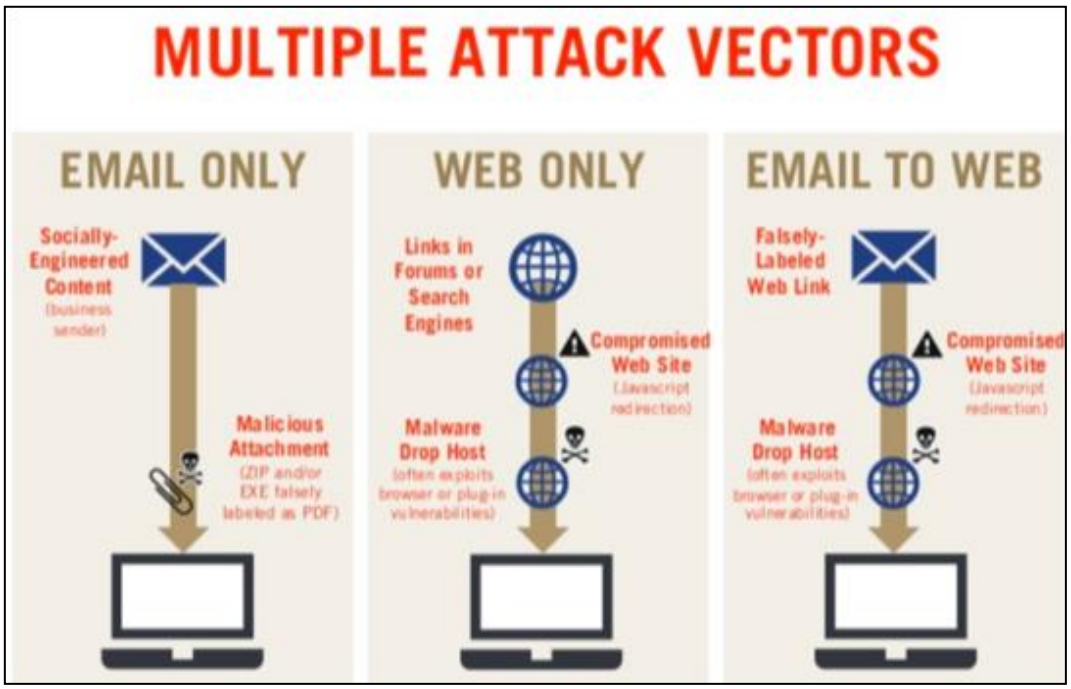


그림39. Multiple Attack Vectors

https://www.trustedsec.com/blog/incident-response-ransomware-series-part-2/

일반적으로 이메일에 파일을 첨부하는 형태, 그리고 웹상에 랜섬웨어 감염이 가능한 사이트를 개설하거나 이러한 웹 사이트를 메일로 전송하는 방법이 가장 일반적이라고 할 수 있다. 대응 방법의 경우 4.2장에서 설명했으므로 해당 장을 참고해 효과적인 전략을 수립하기 바란다.

4.3.2 내부 조사 단계 분석

기존의 악성 코드가 시스템을 장악한 이후 이를 통해서 공격자가 접속한 다음 시스템 내부에 원하는 서버까지 도달하는 등의 행위를 위한 침투였다면, 랜섬웨어는 다수의 서버를 감염 시켜 볼모로 삼기 위한 공격이 대부분이다. 그러므로 랜섬웨어 공격 코드는 한 대의 서버에 감염된 이후 대부분 내부망에 대한 추가 감염을 위해서 내부망에 대한 조사를 수행하게 된다.

내부망에 대한 조사는 먼저 내부망 혹은 외부망에 대한 네트워크 식별을 수행한 이후 본인이 찾고자 하는 대상 네트워크에서 SMB, SAMBA와 같은 기본적인 네트워크 공유와 Active Directory 서비스나 WMI , SSH와 같은 원격 관리 툴에 대한 조사 등을 수행한다.

내부조사 단계는 랜섬웨어가 목표으로 하는 OS의 유형에 따라 일부 상이할 수 있고 내부 조사 방향과 내용도 틀려지므로 이에 대해 고려한 후 분석을 수행해야 한다.

4.3.3 내부 감염(Lateral Movement) 분석

랜섬웨어는 내부감염을 위한 조사를 마무리 했다면 실제 주변 시스템에 감염을 전파해 볼모를 늘리려고 할 것이며, 실제로 내부 조사 단계에서 조사된 정보를 기반으로 공격을 수행한다.

내부 감염 요소	설명
공유 파일 (SMB, SAMBA etc)	OS에 무관하게 공유된 저장소가 존재하는지를 스캔한다. 만약 공유 저장소가 발견되면 PSExec 등을 이용한 전파나 공유된 파일들에 대해서 암호화를 하고 랜섬노트를 남겨 둔다.
WMI	Windows에서 PowerShell을 이용한 WMI 의 사용은 관리에 강력함을 제공하지만 랜섬웨어의 전파의 주요 경로 중 하나로 사용된다.
Active Directory	Windows의 AD가 존재하는지 확인하고 AD의 관리자 권한을 획득하고자 한다. 만약 AD의 관리자 권한이 획득되면 이하의 모든 시스템이 감염될 것이다.
SSH	최근 발견된 DarkRadation와 몇가지 랜섬웨어에서 SSH를 통한 전파를 시도하는 웜 코드가 함께 발견됐고, 해당 코드는 SSH의 Brute-Force 나 SSH키를 이용해 주위 시스템에 전파를 시도한다.
RDP (Remote Desktop)	Windows 원격 데스크탑이 열려 있을 경우 이를 통한 전파를 시도한다.

표 24. 내부 감염요소 분석

각 내부 전파 감염 요소에는 계정이 유출되거나 쉽게 추측이 가능한 경우 혹은 최초 감염된 PC 혹은 서버를 통해서 덤프 된 인증 값으로 인해서 전파된다.

위에서 언급한 내부 감염 요소들은 지금까지 알려진 요소들 일뿐이다. 기존의 웜들이 FTP, Telnet 등의 기본적인 리눅스 서비스 뿐 아닌 Hadoop, Docker 등의 인프라 구성요소들을 이용해 전파에 악용되고 있으므로 이러한 부분을 이용해 랜섬웨어가 감염을 전파하는 수단으로 사용될 수 있으므로 주의를 기울여야 한다.

4.3.4 감염 파일 분석

실제로 초기 진입 단계에서 모든 것이 차단되었다면 기업 담당자는 랜섬웨어가 들어온 것도 인지하지 못할 것이다. 하지만 최초 감염 이후에는 실제로 랜섬웨어에 감염이 한대라도 된 상태일 것이며 이런 경우 기업 보안 담당자는 해당 웜이 어떤 형태의 웜인지 그리고 어떤 방식으로 전파 감염 되었는지 분석을 진행해야 하는 경우가 있다. 아래는 sophos에서 작성한 랜섬웨어의 기술적 특징을 나열한다.

	WANNACRY	GANDCRAB	SAMSAM	DHARMA	BITPAYMER
Type	Cryptoworm	Ransomware-as-a-Service (Raas)	Automated Active Adversary	Automated Active Adversary	Automated Active Adversary
Code-signed	-	-	-	-	-
Privilege escalation	Exploit	Credentials	Credentials	Credentials	Exploit
Network first	-	-	-	Yes	Yes
Multi-threaded	-	-	-	Yes	-
File encryption	Copy, In-place	In-place	Copy	Copy	In-place
Rename	After	After	After	After	After
Key blob	Header	End of file	Header	End of file	Ransom note
Wallpaper	Yes	Yes	-	-	-
Vssadmin	After	After	Before	Before, After	Before
BCDEdit	After	-	-	-	-
Cipher	-	-	-	-	-
0 allocation	-	-	-	Yes	-
Flush buffers	Yes	Write Through	-	-	Yes
Encryption by proxy	-	Yes	-	-	-

	RYUK	LOCKERGOGA	MEGACORTEX	ROBBINHOOD	SODINOKIBI
Type	Automated Active Adversary	Automated Active Adversary	Automated Active Adversary	Automated Active Adversary	Ransomware-as-a-Service (Raas)
Code-signed	-	Yes	Yes	-	-
Privilege escalation	Credentials	Credentials	Credentials	Credentials	Exploit
Network first	-	-	-	-	-
Multi-threaded	Yes	-	-	-	Yes
File encryption	In-place	In-place	In-place	Copy	In-place
Rename	After	Before	Before	After	After
Key blob	End of file	End of file	Separate file	New	End of file
Wallpaper	-	-	-	-	Yes
Vssadmin	After	-	After	Before	Before
BCDEdit	-	-	-	Before	After
Cipher	-	After	After	-	-
0 allocation	-	-	-	-	-
Flush buffers	-	-	-	-	-
Encryption by proxy	Yes	-	Yes	-	-

그림 40. Sophos 연구소의 2019년 랜섬웨어 동작 연구 자료

위의 각 항목은 아래와 같은 뜻을 가진다.

파일 분석시 확인 요소	설명
코드 서명 (Code Signing)	랜섬웨어 파일에 신뢰된 코드 서명을 추가해 탐지를 어렵게 만든다.
권한 상승 (Privilege Escalation)	인증을 위한 계정이나 Exploit을 통해 시스템과 파일에 접근하기 위한 충분한 권한을 획득한다.
원격 드라이브 우선 공격 (Network First)	로컬 시스템의 파일보다 네트워크상에 공유되어 있는 저장소를 우선적으로 찾아내 암호화 한다.
다중 스레드 (Multi-threaded)	암호화 속도를 높이기 위해 다중 스레드 기술을 사용한다.

파일 암호화 (File Encryption)	파일 암호화 시에 랜섬웨어가 사용하는 방식으로 덮어쓰기(In-Place)와 복사(Copy) 두가지 방식으로 나누어진다. 덮어쓰기의 경우 원본파일을 덮어쓰므로 복구가 불가능하나, 복사 방식의 경우 별도로 다른 원본 파일의 삭제가 없다면 복구가 가능한 경우가 있다.
이름 바꾸기 (Rename)	랜섬웨어가 암호화를 수행하면서 파일의 이름을 바꾸는 시점을 말한다. 암호화 되기 이전과 이후로 나누어 진다.
키 저장 영역 (Key Blob)	랜섬웨어가 암호화된 문서의 복구를 위해서 키를 저장하는 위치를 지정한다.
암호화 공고 (WallPaper)	해당 시스템이 볼모가 되었음을 알리는 경고문을 띄우거나 띄우지 않을수 있다.
윈도우 복구 기능 무력화 (VssAdmin)	Windows에서 제공하는 복구기능을 무력화 시키고자 복구를 위한 Windows의 Volume Shadow Service(VSS)상의 백업을 삭제한다.
Windows 복구 기능 (BCDEdit)	Windows의 진단 복구 기능을 사용하지 못하게 한다.
CIPHER.EXE	Windows에서 제공하는 기본 암호화 기능을 이용해 기존 원본 파일을 완전 삭제한다.
0 할당 (0 Allocation)	원본 파일을 일반적으로 삭제하면 파일 복구 툴로 복구가 가능하다. 이것을 막기 위해서 파일 삭제시에 파일 크기를 0으로 설정해 복구를 방해한다.
쓰기 캐시 (Flush Buffers)	Windows에서는 성능 향상을 위해서 디스크에 데이터를 쓰는 경우 메모리에 버퍼를 두고 저장한다. 이럴 경우 랜섬웨어가 데이터를 저장할때 버퍼를 거치게 되어 암호화된 파일로 교체가 안되고 남아 있을수 있으므로 FlushFileBuffers를 이용하거나 직접 쓰는 방식으로 쓰기 버퍼를 사용하지 않게 한다.
신뢰된 프로세스를 통한 암호화 (Encryption by Proxy)	Windows의 보호 시스템을 우회 하기 위해서 랜섬웨어는 powershell.exe나 svchost.exe와 같은 프로세스에 악성코드를 삽입해 파일을 암호화 하기도 한다.

표 25. 파일 분석시 확인요소

현재의 피해 현황과 복구 현황을 정확하게 파악하기 위해서는 위와 같이 감염된 랜섬웨어에 대한 정보를 정확하게 파악하는 것이 가장 좋다. 예를 들어 랜섬웨어 이지만 충분한 원본 파일 삭제나 Windows의 복구 기능을 무력화 하지 못한 랜섬웨어의 경우 디스크 복구 툴을 이용하는 방법으로도 복구가 가능할 수도 있기 때문이다. 다만 최신 랜섬웨어의 경우에는 이러한 부분이 많이 보완된 경우가 많으므로 주의 깊게 살펴보아야 한다.

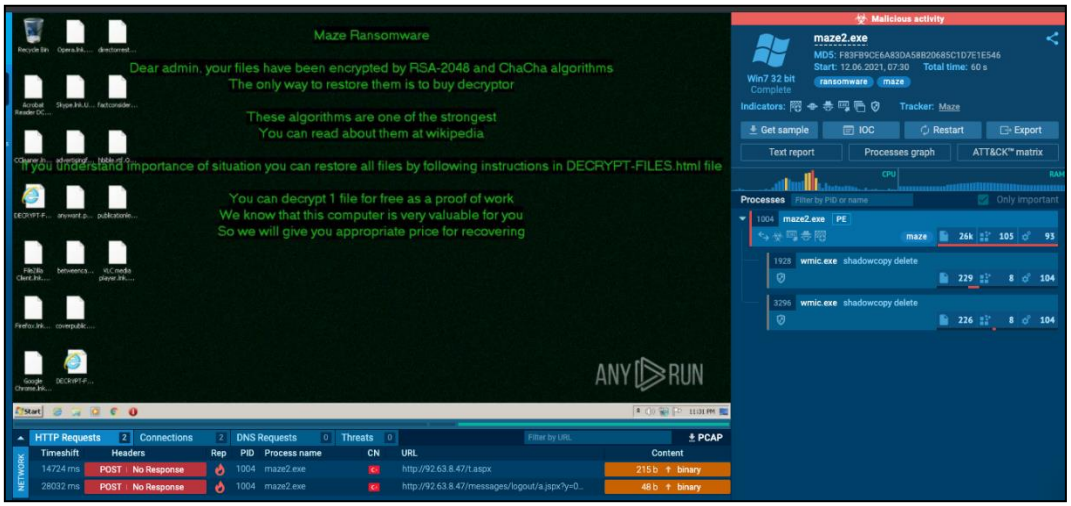


그림 41. any.run 에서 제공하는 maze 랜섬웨어 분석 샘플

다만 실제 분석에 있어서 보안분석팀에 악성코드 분석가를 보유한 경우에는 정확하게 해당 랜섬웨어의 동작 방식을 알아내도록 리버스 엔지니어링을 하거나 정적/동적 분석을 하는 것이 가장 좋지만, 별도로 악성코드를 분석할 수 있는 인력이 없거나 현재 감염되어 정보가 유출되는 경우에는 동적 분석 기능을 제공해 주는 any.run 과 같은 온라인 분석 도구를 통해서 해당 랜섬웨어에 대한 동적 분석을 수행할 수 있고, 그 결과를 통해서 빠르게 공격자가 통신하는 도메인과 IP를 수집해 차단한다면 정보 유출과 감염의 전파를 차단하는 데 큰 도움이 된다.

	정적분석	동적분석	하이브리드 분석
개념	악성코드를 실행하지 않고 그 외형을 분석하여 소프트웨어의 구조파악과 기능을 찾아내는 분석기법으로 악성코드의 지문(Finger Print) 확인, 실행파일이 사용하는 문자열 검색, 소스코드 분석(코드리뷰, 3자분석), 리버스엔지니어링을 통한 구조분석을 한다.	악성코드를 분석가능한 환경(샌드박스) 에서 실행시킨 후 실행과정에서의 다양한 입/출력 데이터의 변화 및 사용자 상호 작용에 따른 변화를 점검하여 분석하는 기법으로 디버깅(논리적인 오류를 찾아내는 테스트 과정), 스트레스테스트 (한계치까지 테스트를 반복하여 취약점 발견), 모의해킹(실제 해커가 사용하는 도구와 기법을 이용하여 해당 시스템으로 침투가능성을 진단), 리버스 엔지니어링(동적 역공학 분석툴을 이용한 구조분석) 등의 방법을 이용한다.	정적 분석의 결과와 동적 분석의 결과를 서로 상관시켜 보안 취약점을 탐지하는 방법으로 동적분석의 취약점 발견 항목에 대한 구조적인 코드 확인이 어렵다는 문제점을 개선하여 동적분석 결과의 취약점을 제시하며 스택정보 및 소스코드 위치를 제공하고 개선방법을 제시하여 효율성과 안정성을 높일 수 있는 방법이다.
특징	- 분석할 소스를 실행할 필요가 없이 실행 과정이나 결과 보다는 실행 전 구현에 초점 - 컴포넌트 간 발생할 수 있는 통합된 보안 취약점 발견은 제한적 - 설계, 구조 관점의 보안 취약점은 발견할 수 없으며, 오탐의 위험이 있음 - 동적 분석기법 과 상호 보완적 기능 수행 - (단점) 입력 값의 유효성 측면에서 점검하므로 유효성 검증을 통과한 값들을 이용한 공격에는 미탐(False Negative), 오탐(False Positive) 가능성 존재함	- 소프트웨어를 실행하여 분석 실행 과정/결과가 중요 - 정적분석에서 발견되지 않는 사용상의 문제점 발견으로 인한 수정비용 절감 - 설계 및 구조적 보안 취약점 발견가능 - 정적 분석기법 과 상호 보완적 기능 수행	- 상세 연계분석 (시스템파일, 문서파일, 텍스트, 키워드) - 보안탐지로그의 문자열 패턴분석 (webshell , SQL Injection ,Editor, Attacking System, URI, XSS, Tools) - 장기추이/연계분석 , 이상행위 IP추적 (C&C IP 통신 추적) - 내부 정보자산 유형별 위협 분석 - 임계치 이상의 트래픽 , 특정유형의 네트웍 행위 분석

표 26. 랜섬웨어 분석기법 비교

랜섬웨어 등 악성코드들은 점차 진화하여 각종 보안솔루션에 탐지되지 않기 위하여 기능적으로는 동일하나, 다른 형태의 파일로 변화한 난독화(Obfuscation)를 사용하여 각종 보안시스템의 탐지 및 분석기법을 피하고 있다. 난독화 기술은 원래 디지털 저작권 목적으로 사용되었으나, 이를 악성코드 은닉에 활용하고 있는 상황이다. 정적분석결과를 동적분석에서 활용하여 오탐 과 미탐을 효과적으로 줄일 수 있는 하이브리드 방안은 현재 가장 효과적인 랜섬웨어 탐지방안이다.

악성코드는 암호화 통신을 통하여 유입될 경우 기존 보안장비에서 탐지가 불가능하므로, 트래픽의 복호화 이후 탐지될 수 있는 체계를 고려해야 하며, 특히 대규모 IDC의 경우 개별 보안장비별 복호화 수행 보다는 한번의 복호화 후 여러 보안장비에 동시에 적용될 수 있는 구성이 각 다양한 보안장비 성능의 활용에 효율적일 것이다.

4.4 랜섬웨어 대응을 위한 투자 전략

위험은 증가하고 있고 공격기법은 점점 지능화되고 경제적 피해가 커지고 있다. 이에따라 특정 제품이나 일부 조직에 의존하는 정보보호활동 만으로는 기업의 랜섬웨어 공격과 같은 고도화된 위험에 대응하기에는 한계가 있으며, 부분적 보안이 아닌 전사 보안을 위한 지속적이고 체계적인 보안관리활동이 가능하여야 한다.

그러나, 기업에서의 정보보호 활동은 한정된 예산과 자원으로 인해 지속적이고 체계적인 활동에 제약을 받고 있으며, 이로 인해 정보보호 요소들 가운데 우선순위를 정하고 선택과 집중을 통해 효과적인 기업의 정보보호 투자를 수행하기 위한 노력이 필요하다.

IDG조사(2019년)에 따르면 기업의 보안지출의 우선 요소는 모범사례(74%), 규정준수 (69%), 조직에 발생한 보안사고에 대한 조치(35%), 이사회의 지시(33%), 다른 조직에서 발생한 보안사고에 대한 사전 조치(29%) 등 이었다.

또한, 기업의 체계적인 정보보호 활동을 돕는 정보보호관리체계(ISMS) 항목의 중요도 인식과 투자의 우선순위 비교 연구에 따르면 기술적 물리적 통제요소인 접근통제, 물리적 보안, 시스템 개발 보안, 운영보안을 중요하게 생각하고 있고, 실제 투자도 접근통제, 물리적 보안, 운영보안을 중심으로 많이 이루어 지고 있는 것으로 나타났다.

사전 관리적 통제 분야에서는 인적보안과 정보보호 교육에 대한 중요도가 높은 것으로 조사 되었으며 외부자 보안, 인적보안, 정보자산 관리 분야를 중심으로 투자가 이루어 지고 있는 것으로 나타났다.

사후 관리적 통제 분야에서 침해사고 관리과 IT 재해복구에 대한 중요도가 높은 것으로 조사되었으며 침해사고 관리보다는 IT 재해복구를 중심으로 투자가 이루어 지고 있는 것으로 나타났다.
이러한 현상은 기업 경영진 관점에서 비즈니스 가치가 비대면 온라인 디지털 영역으로 급격하게 전환되고 있는 만큼 정보시스템의 장애(서비스 중단 등)로 인한 경영 리스크 우려로 인해 IT재해복구에 대한 투자 우선순위 가 높아지고 있는 것으로 판단된다.

상대적 중요도			상대적 투자 정도		
항목	중요도	순위	항목	투자정도	순위
침해사고 관리	0.177	1	IT 재해복구	0.144	1
접근통제	0.105	2	접근통제	0.138	2
인적보안	0.099	3	물리적 보안	0.135	3
IT 재해복구	0.099	4	침해사고 관리	0.116	4
정보보호 교육	0.09	5	운영보안	0.089	5

표 27. 상대적 중요도와 상대적 투자정도의 TOP5평가항목 비교
(출처 :정보보호관리체계항목의 중요도 인식과 투자의 우선순위 비교, 이중정)

현재 대부분 기업들이 수행하고 있는 기술적 대응으로 랜섬웨어 공격을 100% 방어하기에 한계가 있다. 맨디언트사의 '보안효과성 보고서(2020발표)'에 따르면 침투테스트 공격의 절반이상(53%)은 탐지되지 않고 기업내 환경에 성공적으로 침투 했으며,했다. 침투 후 보안 툴에 의해 탐지된 공격은 26%, 완전히 차단된 공격은 33%정도였다. 또한 경보를 발생시킨 공격은 단 9%에 지나지 않았다.

이처럼 다양한 이메일, 웹 사이트 등 이용자 기만을 통한 공격에서부터 제로데이 취약점을 이용하는 등 다양한 경로와 고도화된 공격 기술을 이용하는 랜섬웨어 공격으로부터 완전히 자유로워 지기 어렵다. 또한, 랜섬웨어 피해 발생 시 복구가 불가하여 주요 정보자산이 소멸된다면 기업의 존폐를 좌우할 수도 있다. 따라서, 랜섬웨어 공격에 대해서는 피해 예방을 위한 활동과 사후 복구를 위한 대응 방안에 대한 고려가 함께 필요하며, 공격의 타겟이 되었을 때 그 피해를 최소화 하고 기업 활동을 빠르게 복구 할 수 있는 전략이 필요하다. 이를 위해서는 비즈니스 연속성 계획(BCP : Business Continuity Plan)수립과 체계적인 백업과 복구 전략을 통해 효과적인 대응이 가능할 것이다.

또한, 랜섬웨어 피해예방 측면에서 다른 기업들 의 랜섬웨어 사고 대응에 대한 모범사례를 보면 랜섬웨어 피해로부터 문제를 해결하는 최선의 방법은 체계적인 백업을 통해 사건이 발생되면 빠르게 데이터를 복구하는 것이 재난수준으로 피해가 커지는 것을 최소화하는 효과적인 방법으로 인식하고 있다.

4.4.1 랜섬웨어의 피해 복구 방안

본 장에서는 랜섬웨어에 감염되었을 때 유형과 긴급도에 따라 피해 복구 방안을 설명하며 본 방안은 기업의 상황과 감염된 망의 구조, 자료의 중요도에 따라 다를 수 있다. 복구를 한다는 것은 이미 랜섬웨어에 최소한 한대 이상의 시스템이 감염된 상황일 것이다. 그렇다면 감염된 상황과 감염된 형태에 따라 피해를 복구하는 수준이 상이할 수 있다.

복구를 위한 단계		설명
1	감염된 랜섬웨어 파악	어떠한 랜섬웨어에 감염되었는지 기술적 특성은 무엇인지, 현재 감염되어 전파를 위해서 시도하고 있는 방법이나 외부 통신이 있는지 등에 대한 전반적인 내용에 대해서 파악한다. 이에 따라 어떠한 방식으로 대응하는지 방법이 결정된다. PS. 상세한 분석은 아래의 6번 이후에 수행해도 무방하다. 지금 시점에서는 외부 통신과 감염, 전파 경로 파악이 최우선 이다.
2	랜섬웨어 외부 통신 채널 차단	공격자와의 통신 채널을 열수 있는 Trojan 계열 랜섬웨어의 경우 공격자와 통신하고 있는 외부 통신 채널을 빠르게 차단해야 한다. 공격자는 명령어를 통해 랜섬웨어를 추가적으로 전파하거나 데이터를 유출해 가지고 나갈 수 있다.
3	감염 전파 경로의 차단	외부 요소에 의한 재감염을 피하기 위해 외부에 열린 감염 요소를 빠르게 파악해 제거한다. 이메일의 경우에는 관련된 메일을 모두 격리해야 한다. 그리고 파악된 랜섬웨어가 Worm의 형태를 가질 경우 전파 하는 상황을 파악해 빠르게 차단한다.
4	감염 현황 파악	랜섬웨어가 더 이상 확산 되지 않는 것을 확인하고 전체적으로 감염된 현황(대수)을 파악한다.
5	백업 데이터 정상 존재 여부 확인	백업 데이터가 존재하는지, 피해가 없었는지 확인한다.
6	시스템 및 데이터 복구	감염된 시스템들을 대상으로 백업 데이터가 존재하는 시스템들에 대해서 복구를 수행한다. 백업 데이터가 존재하지 않는 경우에는 파악된 랜섬웨어의 유형에 따라서 복구를 시도해 볼 수 있다. Ex. 잠금 랜섬웨어의 경우 Windows 복구 모드로 진입이 가능한지 외부에서 접속이 가능한지 등을 확인해봐야 한다. 그리고 잠금과 암호화 두가지 모두 타 시스템에서 해당 디스크에 접근해 파일을 읽을 수 있는지 확인해봐야 한다. 만약 일반적인 방법으로 파일의 접근이 불가능 하다면 파일 복구 솔루션을 사용해 볼 수 있다. 지워진 파일을 복구하는 것과 동일한 방법으로도 복구가 가능한 지 등을 체크해 본다.
7	정보 유출 현황 신고	랜섬웨어 감염으로 인해 정보 유출이 실제로 발생했거나 공격자로 데이터가 전송된 부분이 확인될 경우 4.1의 관리적 방안에서의 랜섬웨어 신고 절차에 따라 빠르게 신고하고 대응한다.
8	복구 불가 상황 대응	6번 항목의 복구 방안을 검토해 보았으나 복구할 수 없는 경우 외부 기관이나 보안 회사와의 협업을 통해서 해결 방안을 모색 할 수 있다. 다만 공격자에게 금전적인 지급을 통해서 랜섬웨어를 해결하는 것은 최악의 마지막 경우로 모색 한다.

표 28. 랜섬웨어의 복구 단계

랜섬웨어 외부 통신 차단에서 최근의 랜섬웨어나 악성코드가 Tor를 사용하는 경우가 발생하고 있다. 이럴 경우 DNS나 트래픽을 이용한 탐지는 불가능하며 Tor Exist Node와의 통신을 모두 탐지하고 있다고 하더라도 신규로 생성된 Tor 노드라면 해당 목록에 없을 수 있다. 이럴 경우를 대비해 네트워크와 시스템 단에 충분한 보안 대책을 수립하고 IDS에 Tor 접속 패턴을 입력하고 테스트 해보고, 만약 최근의 Tor 탐지가 가능한 AI 계열 등의 보안 제품을 보유했다면 적극 활용하기 바란다.

백업 계획을 구축하면서 NAS나 SAN을 이용해 직접 시스템에 지속적으로 인증 없이 연결해둔 상태에서 파일 복사를 이용해 백업을 하는 것은 공격자에게 데이터를 헌납하는 경우로 절대적으로 피해야 한다.

이상에서 알아본 랜섬웨어 대응 단계는 아래의 랜섬웨어 유형에 따라서 그 단계가 달라지게 되므로 아래의 유형들에 대해서 참고하기 바란다.

랜섬웨어의 유형	설명	기본 복구 방향
암호화 랜섬웨어	파일에 대한 암호화를 수행하며 대상은 로컬의 문서 파일 혹은 원격 저장소의 문서 파일을 대상으로 암호화를 수행하는 랜섬웨어	단순 암호화와 잠금 랜섬웨어의 경우 외부와의 통신이나 감염의 전파를 위한 방안이 없을 경우가 있다. 이런 경우 수십 대나 수백 대의 피해가 아닌 1-2대의 피해로 끝나는 경우가 있으므로 대응 단계 1단계에서 파악한 랜섬웨어 유형에 따라서 시간을 두고 복구를 진행할 수도 있다.
시스템 잠금 랜섬웨어	시스템을 사용하지 못하게 잠그는 형태의 랜섬웨어로 OS영역에서의 잠금과 하드웨어 형태의 잠금 두가지 형태로 구성된다.	

표 29. 랜섬웨어의 유형

위 두 가지 유형의 랜섬웨어에 추가적인 Worm이나 Trojan의 기능을 수행하는 랜섬웨어의 대응은 아래와 같다. (아래의 랜섬웨어들은 암호화와 잠금 랜섬웨어 두 가지 중 어느 것이라도 기능이 추가될 수 있다.)

추가 기능 유형	설명	기본 복구 방향
Worm 기능형 랜섬웨어	Worm과 결합, 랜섬웨어를 스스로 확산시키기 위해서 다양한 시도를 수행하며 전파 가능 부분이 확인되면 이를 통해서 Worm과 같이 전파된다.	내부 감염 시 랜섬웨어 확산을 위해서 다양한 내부망 공격을 발생시키며 Worm의 유형을 띄므로 내부 네트워크에 장애를 발생시킬 수준으로 스캔과 취약점 공격이 발생할 수 있다. 서비스 안정화를 위해서 긴급으로 대응해야 하며 전파에 이용되는 취약점과, 외부 저장소를 통해서 랜섬웨어가 다운로드 되는 경우라면 다운로드 경로 두 가지를 빠르게 차단해야 한다.

Trojan 기능형 랜섬웨어	감염될 경우 공격자가 직접 시스템을 장악, 다양한 공격 행위를 수행한다. 암호화 및 정보 유출 등 다양한 형태로 동작한다.	가장 위험한 경우로 Trojan 기능을 가진 암호화나 잠금 랜섬웨어에 감염될 경우 공격자가 내부의 모든 자료를 외부로 반출해 갈 수 있다. 랜섬웨어 유형 중 가장 빠르게 대응해야 하며 공격자의 통신 채널을 차단하는 것이 가장 좋으나 만약 불가능하다면 감염된 PC나 서버를 빠르게 내/외부 네트워크와 격리해야 한다.

표 30. 랜섬웨어 유형별 복구방향

4.4.2 대기업의 대응 전략

대규모 인력/조직/예산을 보유한 대기업군에서 적절한 랜섬웨어 대응전략을 다음과 같이 유형별로 수립할 수 있다.

대응전략 (규모, 예산, 인력)		대기업군		
정책/절차	**수단**	**유형 1**	**유형 2**	**유형3**
이메일 문서첨부에 삽입 된 악성 매크로 및 스크립트 탐지/차단	CDR (Content Disarm and Reconstruction)	O	O	O
랜섬웨어 공격메일에 대한 필터링	메일필터링	O	O	O
랜섬웨어 파일 통제절차	Attach File SandBox	O	O	X
악성 파일 통제 절차	안티바이러스, PMS	O	O	O
원격접속관리 절차	mOTP, OTP토큰, 지문 등	O	O	O
접근통제절차	접근통제관리 시스템, (계정 신청,승인 등)	O	O	O
침해사고 대응절차 (네트워크 기반)	IPS, APT솔루션	O	O	O
이상행위 식별 및 조사	xDR솔루션, 포렌식 솔루션	O	O	X
매체 삽입 시 자동으로 랜섬웨어 감염 파일검사	안티바이러스,반출입통제 시스템	O	O	O
보안인식 교육 및 보안 위반 시 소명처리 절차	보안포털 (교육/소명 프로세스 등)	O	X	X

표 31. 대기업군 랜섬웨어 대응전략

■ **유형 1**

- 보안관제전문업체를 이용한 24시간 실시간 보안관제 서비스 수행 시 (내부 유입 악성파일 통제절차 포함)
- 랜섬웨어 의심파일에 대한 전담 포렌직(xDR 등) 수행인력 보유 시
- 보안인식 교육 및 정기적인 점검을 통한 소명처리 절차 수행 시

⇨ 지속적인 보안관리 활동

- 정기적인 시스템 취약점 점검(VPN, 원격제어 시스템 등)
- 패치관리 철저

■ **유형 2**

- 보안관제전문업체를 이용한 24시간 실시간 보안관제 서비스 수행 시 (내부 유입 악성파일 통제절차 포함)
- 랜섬웨어 의심파일에 대한 전담 포렌직(xDR 등) 수행인력 보유 시
- 보안인식 교육 및 정기적인 점검을 통한 소명처리 절차 미 수행 시

⇨ 지속적인 보안관리 활동

- 정기적인 시스템 취약점 점검(VPN, 원격제어 시스템 등)
- 패치관리 철저
- 보안인식교육 및 소명처리 절차 수행

■ **유형 3**

- 보안관제전문업체를 이용한 24시간 실시간 보안관제 서비스 수행 시 (내부 유입 악성파일 통제절차 제외)
- 랜섬웨어 의심파일에 대한 전담 포렌직(xDR 등) 수행인력 미 보유 시
- 보안인식 교육 및 정기적인 점검을 통한 소명처리 절차 미 수행 시

⇨ 지속적인 보안관리 활동

- 정기적인 시스템 취약점 점검(VPN, 원격제어 시스템 등)
- 패치관리 철저
- 보안인식교육 및 소명처리 절차 수행 (특히, 악성파일 감염 시 유입경로에 대해 집중적인 조사 및 소명처리 필요)

4.4.3 중·소기업의 대응 전략

대기업에 비해 소규모 인력/직/예산을 보유한 중소기업 군에서는 적절한 랜섬웨어 대응전략을 다음과 같이 유형별로 수립할 수 있다

대응전략 (규모, 예산, 인력)		중소기업 군		
정책/	수단	유형 1	유형 2	유형3
악성코드 탐지/차단	안티바이러스	O	O	O
이메일 문서첨부에 삽입 된 악성 매크로 및 스크립트 탐지/차 단	CDR (Content Disarm and Reconstruction)	O	O	X
랜섬웨어 공격메일에 대한 필터링	메일필터링	O	X	X
랜섬웨어 통제절차	Attach File SandBox	O	X	X
원격접속관리 절차	mOTP, OTP토큰, 지문 등	O	O	X
접근통제절차	접근통제관리 시스템, (계정 신청,승인 등)	O	X	X
침해사고 대응절차 (네트워크 기반)	IPS, APT솔루션	O	O	X
이상행위 식별 및 조사	xDR솔루션, 포렌식 솔루션	X	X	X
매체 삽입 시 자동으로 랜섬웨어 감염 파일검사	안티바이러스, 반출입통제 시스템	O	X	X
보안인식 교육 및 보안 위반 시 소명 처리 절차	보안포털(교육/소명 프로세스 등)	X	X	X

표 32. 중소기업군 랜섬웨어 대응전략

■ **유형 1**

- 보안관제전문업체를 이용한 24시간 실시간 보안관제 서비스 수행 시
  (내부 유입 악성파일 통제절차 제외)
- 랜섬웨어 의심파일에 대한 전담 포렌직(xDR 등) 수행인력 미 보유 시
- 보안인식 교육 및 정기적인 점검을 통한 소명처리 절차 미 수행 시

⇨ 지속적인 보안관리 활동

- 정기적인 시스템 취약점 점검(VPN, 원격제어 시스템 등)
- 패치관리 철저
- 보안인식교육 및 소명처리 절차 수행
  (특히, 악성파일 감염 시 유입경로에 대해 집중적인 조사 및 소명처리 필요)

■ **유형 2 / 유형 3**

- 최소한의 침해대응 보안관제 서비스(방화벽, IPS 탐지/차단) 수행 또는 미수행 시
  (관제대상이 DMZ 구간 웹서버로 한정 등)
- 최소 권한 및 직무 분리 원칙을 통합한 접근권한과 인증관리 절차 미수행 시
- 안티바이러스 솔루션을 이용한 악성코드 탐지 및 차단 대응이 주요 대책인 경우

⇨ 지속적인 보안관리 활동

- 패치관리 철저
- 보안인식교육 및 소명처리 절차 수행
  (특히, 악성파일 감염 시 유입경로에 대해 집중적인 조사 및 소명처리 필요)
- 랜섬웨어 백업 및 복구전략 수립 및 시행 필요 (즉시)

4.5 랜섬웨어 공격 피해 최소화를 위한 사후 대응 전략

기존의 보안 공격이 주로 기밀성(Confidentiality)에 대한 위협을 중심으로 이루어졌다면, 랜섬웨어 공격은 가용성(Availability)에 대한 위협을 기반으로 이루어지고 있다. 가용성에 대한 위협은 기업의 경제적 생산활동에 직접적인 영향을 미치게 되는 만큼 매우 심각한 보안 위협으로 인식되고 있다.

정보시스템의 가용성을 유지하기 위해 백업대상, 주기, 방법, 보관장소, 보관기간, 소산 등의 절차를 수립하고 이행해야 하며 아울러 사고발생 시 적시에 복구할 수 있게 관리하여야 한다.

그리고, 정보시스템 재해복구지침(TTA)에서는 '재해'는 정보기술 외부로부터 기인하여 예방 및 통제 불가능한 사건으로 인해 정보기술 서비스가 중단되거나, 정보시스템의 장애로 부터 예상 복구 소요시간이 허용 가능한 범위를 초과하여 정상적인 업무수행에 지장을 초래하는 피해라고 정의한다.

즉, 랜섬웨어 피해예방을 위한 백업관리는 정보시스템의 데이터 원본을 백업을 통해 원래대로 되돌릴 수 있는 상태로 지속적으로 관리하고, 정보시스템의 손실 발생 시 예상 복구 소요시간 범위를 초과하지 않고 다운타임을 최소화하여 이전의 상태로 회복시켜 서비스를 재개하는 것이라고 정의할 수 있다. 이러한 랜섬웨어 공격으로부터 피해에 대해 기업은 재해에 준한 장애로 인식하여 관리하여야 한다.

따라서, 기업 경영진과 실무자들은 이러한 인식하에 랜섬웨어 피해 사고를 당한 경우를 대비해 체계적인 백업 및 복구 관리절차와 재해복구 절차에 준한 운영 매뉴얼을 통해 지속적인 개선활동을 수행하여야 한다.

구분	2018	2019	2020	2021
비용	$46,800	$141,000	$274,000	$380,000

표 33. 랜섬웨어로부터 발생되는 다운타임으로 미치는 평균피해비용 (출처: Safely Detectives)

4.5.1 백업관리 정책 및 방법

가. 백업관리 정책

랜섬웨어 피해 사고 발생 시 다운타임을 최소화하여 신속하게 복구를 하기 위해 선행해야 하는 작업이 백업이다. 이러한 백업과 복구를 위해 기업에 중요한 백업 자료가 서버나 PC, 노트북, 기타 물리적 장치, 클라우드 플랫폼, 가상머신 등 어느 환경의 어느 장비에서 사용되고 있는 지를 조사해야 한다.

또한, 백업 대상에 따라 시스템 백업, 데이터 백업, 변경 로그 백업 등 다양한 방식이 있으며, 외부의 영향으로부터 백업 데이터의 안전성 확보를 위해 다중 백업을 실시하고 있다.

더불어 비용을 수반하는 저장매체의 용량(백업용량 * 보관주기)을 확보하기 위해 백업해야 할 장치 수량도 정확히 파악해야 한다

- 대상 선정 : Server/PC/노트북 등
- 대상 구분 : System Image(설정파일 등), Data File, 로그파일, 업무용 프로그램 등
- 백업 기간 : 주기적인 원본백업, 원본구간별 일일 증분 또는 차등백업
- 예상백업 볼륨 선정 : File/DB 설치용량 등 (백업 횟수가 많아지면 비용이 증가됨)
- 백업본의 유효성 테스트
- 백업 담당자/관리자

다음으로, 데이터의 중요도를 검토한다. 기업 내 유지 관리에 사용할 서비스를 비롯해, 운영 서비스 중요도에 맞는 RTO(Recovery Time Objective, 복구목표시간)와 RPO(Recovery Point Objective, 복구목표시점)를 세워야 한다.

또한, 체계적인 백업관리를 위해 담당자/관리자를 지정하여 물리적, 가상 및 클라우드 등의 여러 플랫폼에 대한 백업 작업을 고려해서 지속적으로 백업 및 복구 관리와 재해복구업무를 수행할 수 있도록 하여야 한다.

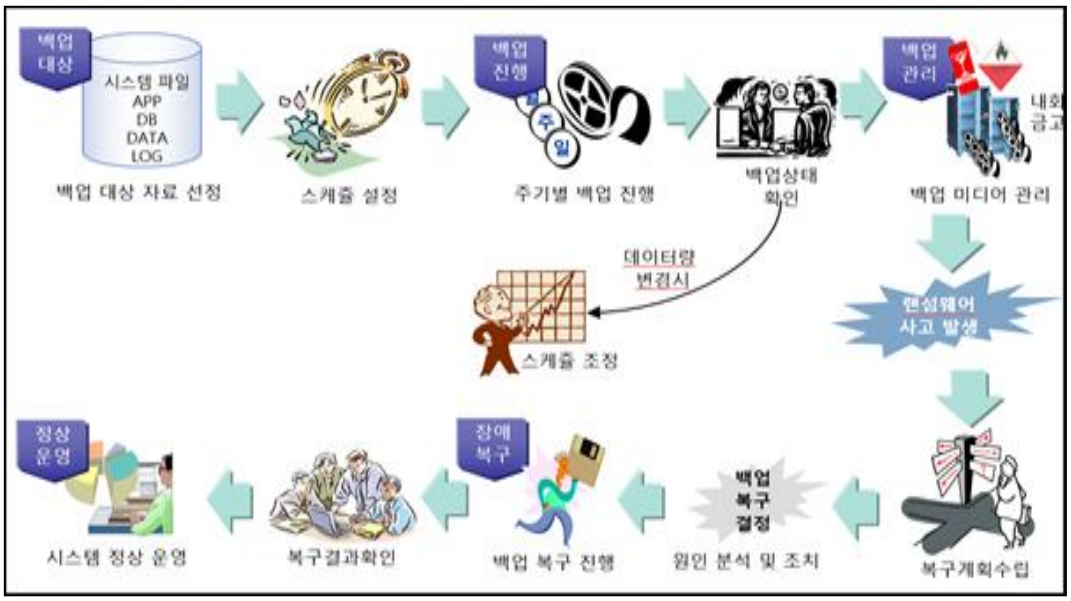


그림 42. 백업 및 복구 흐름

특히, 랜섬웨어 피해예방을 위한 백업 시 유의해야 할 점은 오프라인 백업도 유지해야 한다. 악성 행위를 보면 접근 가능한 파일은 물론, 백업 데이터까지 삭제하려 시도하고 있다. 일부 악성프로그램은 백업 파일을 다시 암호화하기도 한다. 따라서 중요 데이터를 안전하게 보호하기 위해서는 소산백업 이후 네트워크에 연결되지 않은 오프라인 상태로 데이터를 보유해야 한다.

만약, 이러한 구성을 위한 비용과 관리가 부담스러운 기업에서는 IDC센터나 클라우드 서비스업체를 통해 백업 및 복구관리를 위탁하는 방법도 있다. 이 또한 클라우드 기반 백업을 사용할 경우에도 오프사이트 백업도 고려하여야 한다.

나. 정보시스템 백업방법

일반적으로 기업들은 월간 백업은 전체백업(FULL BACKUP)으로 수행하고 일 또는 주간 백업은 증분백업(Incremental backup)을 수행하고 있다. 그리고, 백업 시스템과 관리체계를 갖추지 못한 기업에서는 정보시스템 장애에 대비해 자동화 백업(CDP:Continuous Data Protection)을 수행하는 경우도 있다.

하지만, 자체적으로 백업관리 체계를 구축하였거나 전문업체를 통한 서비스를 제공받지 않고 일부 중요파일에 대해 자동화백업(예: 매일 오전 10시, 오후 10시에 각각 이미지백업(스냅샷 복제) 예약)을 수행한 경우, 만약 오후 1시 즈음 랜섬웨어 바이러스가 발견된다 하더라도 오전 10시에 백업한 정상 버전으로 복원하면 된다. 그러나, 랜섬웨어를 당일 발견하지 못하고 2일 후 발견한 경우 피해를 막을 수 없는 문제점이 있다.

구분	내용	특징
전체 백업 (Full backup)	지정한 디렉토리 아래의 모든 파일과 디렉터리를 저장소로 복사하는 백업방법	복구 시에 일부 다른 백업 방식보다 간편하고 시간이 증분 백업에 비해 상대적으로 덜 걸린다는 장점이 있다.
증분백업 (Incremental backup)	'전체백업'과는 달리 최종 전체 백업 혹은 최종 증분 백업 이후에 변경된 파일만을 복사 (예: 전체 백업은 월별로 실시)	전체 백업과 비교할 때 증분 백업은 매일 백업해야 하는 파일의 양이 적어 빠른 백업이 가능하다는 점이 장점이다. 그러나 복구 과정에서는 최종 백업된 전체 및 모든 후속 증분 이미지나 복사본까지 복구해야 하기 때문에 복구 작업이 번거로워지고 경우에 따라서는 시간이 훨씬 더 걸릴 수 있다.
자동화 백업 CDP (Continuous Data Protection)	일반적인 파일단위 백업 서비스와는 달리 이미지백업 (Volume Snapshots 방식)이면서 분 단위까지 백업을 받고 필요시 특정 백업 시점으로 복원 할 수 있는 백업 서비스	전반적으로 비용과 시간이 많이 필요한 백업 관리 체계를 구축하지 못한 기업에서 빠른 복구를 위해 디스크의 일부를 복구용 저장소로 사용할 수 있다. 그러나, 랜섬웨어 감염을 바로 인지하지 못하면 감염된 파일이 이미지 백업되는 위험이 존재한다.

표 34. 백업방법별 특징 (출처: KISA)

4.5.2. 기업규모별 대응전략

가. 대기업을 위한 정보시스템 백업 방식

랜섬웨어 대응을 위한 안전한 정보시스템 백업을 구성하는 방식은 데이터와 해당 데이터가 백업이 되는 테이프 장치와의 연결 방식에 따라 직접(Direct) 백업, 네트워크(Network) 백업, SAN 백업의 세 가지로 크게 나누고 있다

1) 직접 백업

데이터 장치와 테이프 장치 간의 연결이 SCSI나 직접 연결된 형태를 의미한다. 대개 서버에 DAT와 같은 장치가 직접 연결돼 사용하는 전통적인 방식으로 현재도 TAPE 이용한 소산 방식으로 꾸준한 사용을 하고 있으며, 백업 시 별도 TAPE에 보관되기 때문에 최근 랜섬웨어 감염으로 인한 피해를 최소화할 수 있는 방안으로 제시되고 있다.

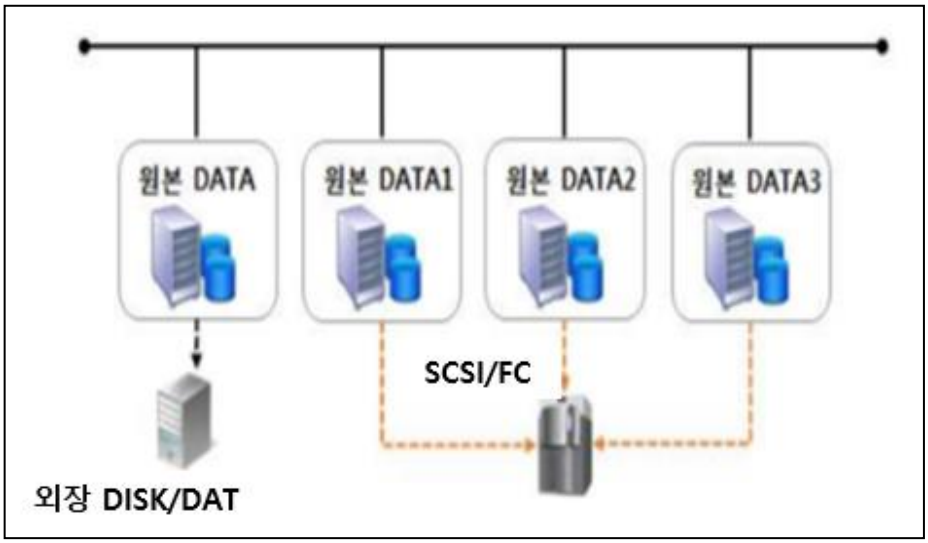


그림 43. 직접 백업 구성

2) 네트워크 백업(Network Backup)

현재는 사용이 크게 줄어든 백업 방법으로 데이터 장치와 테이프 장치 간의 연결 이 TCP/IP 네트워크로 연결된 형태를 말한다. 백업 전용 서버에 백업장비를 모두 연결하고 나머지 서버는 이 백업 전용 서버를 통해 백업을 수행한다.

네트워크 백업은 백업 장치를 공유하므로 직접 백업에 비해 백업 장치에 대한 중복 투자를 줄일 수 있다는 장점이 있으나 백업 데이터가 네트워크를 통해 전달되므로 백업 성능이 저하될 수 있다는 점은 단점이 있다. 또한, 공격자가 네트워크에 연결된 백업 시스템에 침투하여 백업 데이터를 암호화하거나 삭제할 수 있어 백업 스케줄이 없는 시간에는 오프라인으로 설정하는 것이 중요 하다.

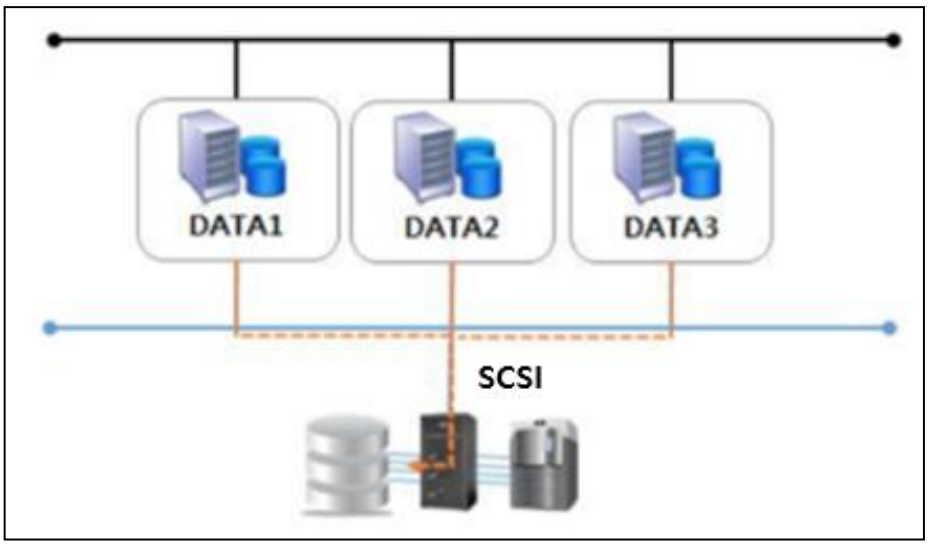


그림 44. 네트워크 백업 구성

3) SAN 백업

직접 백업과 네트워크 백업의 장점만을 이용해 구성한 최적의 백업 구성 방식으로 백업 장치 공유 및 관리 측면에서 매우 뛰어난 성능 및 유연성이 있는 백업 방식이다. 다양한 백업방식(전체 백업, 증분백업 등) 적용할 수 있어 현재도 대기업 등에서 많이 사용 중인 백업 기술이다.

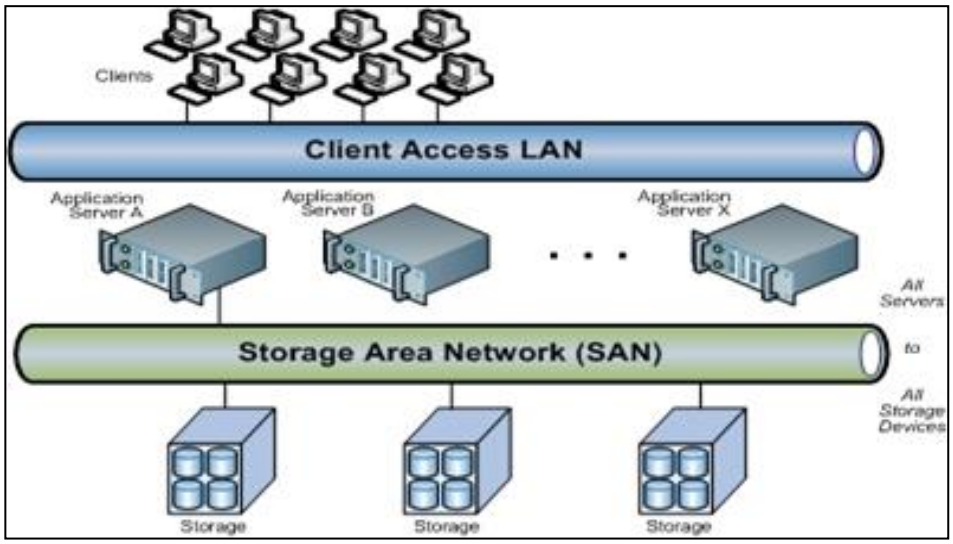


그림 45. SAN 백업 구성 (출처: SNIA)

4) 디스크 복제

디스크 복제는 주로 중요하거나 빠른 시간에 백업이 필요한 경우 디스크에서 디스크로 직접 복제하는 백업 방식이다. 백업 완료 후 시간이 흘러 데이터의 변경이 있을 경우 변경된 데이터만을 다시 백업 함으로 백업 시간이 타 백업방식에 비해 짧은 장점을 보유한다. 장애 혹은 잘못된 작업으로 데이터 손실 및 변경 시 백업 본을 기준으로 변경된 부분만을 리스토어(restore)함으로 복구 시간이 빠르다는 장점이 있으나 구성에 따른 비용이 많이 소요된다.

그림 46. 디스크 백업

5) Cloud 백업

Cloud 백업은 최근 도입된 물리적으로 떨어진 외부영역에 백업하는 방식이다. 일반적으로 로컬 네트워크 내에서 1차 백업 후 외부에 2차 백업으로 소산 개념으로 백업하는 방식으로 비용을 최소화할 수 있는 방식 중 하나이다. 기술적/물리적 통제요소인 접근통제, 물리적 보안 등으로부터 보호 및 모니터링 되어 개인 및 국내 중소기업에 랜섬웨어 등으로 데이터를 보호하기 위한 방안으로 적합하나 다소 비용이 소요된다.

특히, 외부 Cloud 사용 시 이용자(개인)의 경우 웹 계정을 사용하여 백업할 수 있으며, 기업의 경우 Gateway 방식구성으로 Gateway 간 VPN 또는 API연동으로 SSL통신 구성방식으로 구성된다.

그리고, 해당 서비스 제공은 국내 통신사와 해외 IT기업이 서비스를 제공하고 있으며. 클라우드 서버에 백업데이터가 보관되기 때문에 안전한 클라우드 계정 관리가 중요하다. OTP 등 멀티 인증을 사용하도록 권고한다.

그림 47. Cloud 백업 구성

나. 중·소기업을 위한 정보시스템 백업 방식

대기업을 제외한 비교적 규모가 작은 중소기업의 경우 랜섬웨어 예방을 위한 백업 구축 방식은 내부 네트워크에 NAS 또는 외장 디스크를 구축하여 백업하는 환경이며 외부에 소산 백업으로 데이터 안정성 확보하는 방법은 비용부담의 요소가 있다.

따라서, 백업 방법 선택 시 고려 사항 중소기업에서는 예산, 백업용량의 크기, 백업의 편의성, 백업 매체의 보관 공간 확보를 고려하여 백업 매체 및 방법을 선택해야 한다.

- 예산이 부족할 경우, 백업 매체가 저렴한 테이프 백업이나 초기 구축 비용이 적게 소요되는 클라우드 백업을 권할 수 있다.
- 백업용량의 크기 대용량(1TB 이상)을 주기적으로 백업해야 할 시 테이프 백업이 적당하다
- 편의성 백업 및 소산을 위한 다양한 기능을 제공하고 있는 클라우드 백업 및 NAS 백업을 추천한다. PC 등의 소규모 자료를 수시로 백업하고 보관할 시에는 외장 디스크 백업을 사용할 수 있다.

그리고, 랜섬웨어로부터 안전하게 데이터를 보존하기 위해 원격장소에 보관하거나 오프라인으로 백업 데이터를 보관 할 수 있도록 TAPE, 외장디스크, 외부의 다른 NAS, 혹은 클라우드 서비스를 이용하는 방식이 있다.

1) TAPE 백업

저렴한 가격 대비 성능, 이동성, 용량 관리의 용이성 등의 특징을 가지고 있다. 최근 랜섬웨어 등으로부터 기업의 중요 데이터를 보호하기 위한 방법 중 하나로 TAPE백업 방식을 채택을 권고하고 있으며, 대부분 저비용으로 구성할 수 있는 장점 때문에 비교적 규모가 작은 기업에 사용하는 것이 유리하다.

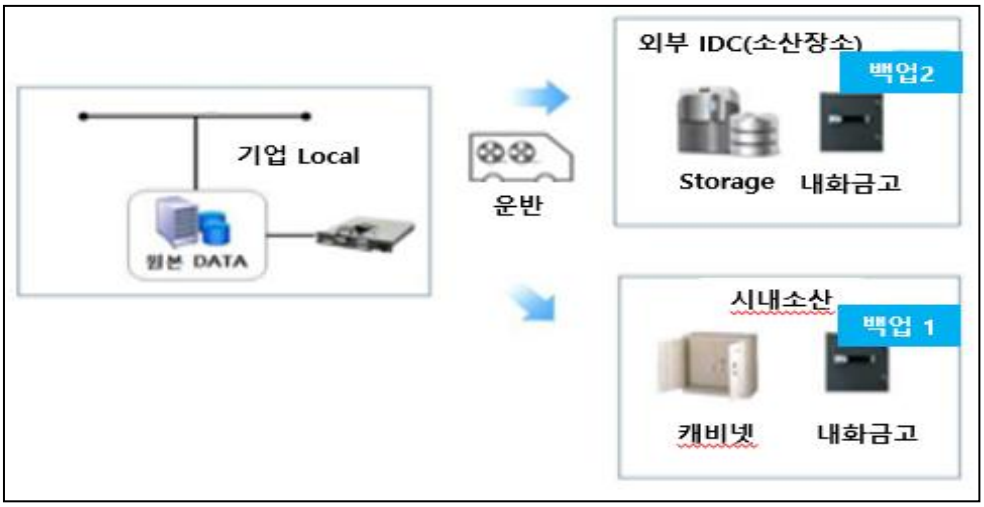


그림 48. Tape 소산 백업 구성

2) Cloud 백업

Cloud 백업은 외부 저장소에 백업을 수행하는 것으로 최근 개인, 중소기업 등 다 양한 이용자 계층에서 많이 사용하고 있다. Cloud 서비스 이용 시 구성 방식에 따라 Gateway 구성 방식과 SSL 통신 방식, 웹 접근방식으로 제공된다.

랜섬웨어 등 외부 침해 시 데이터 무결성 유지를 위해 반드시 백업 설정에서 “덮어쓰기” 방지 설정을 하여 이미 감염된 데이터가 Cloud 백업 저장소 내의 데이터에 덮어쓰기 되지 않도록 방지해야 한다. 또한 클라우드 백업 서비스 사용시 인증 정보가 탈취되거나 통신구간 암호화 미 적용으로 주요 정보가 외부에 노출되지 않도록 주의해야 한다.

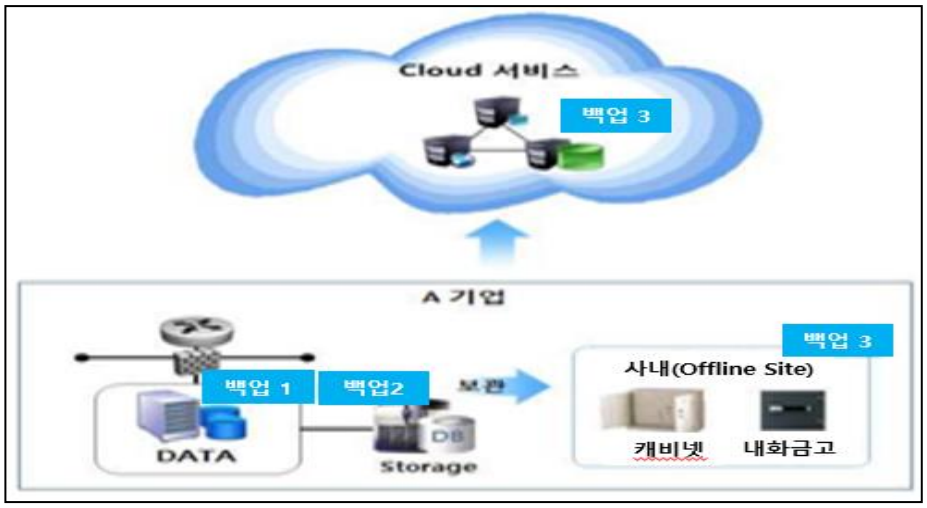


그림 49. Cloud 소산 구성

3) NAS 백업

데이터 복구를 중시하는 일부 소비자와 중소기업은 백업을 위해 전용 NAS(Network Attached Storage) 기기의 사용을 고려할 수 있다. 랜섬웨어 감염 예방을 위해 백업 이후 네트워크를 반드시 분리하여 기존 백업 데이터에 덮어쓰기가 되지 못하도록 NAS정책에 반영 또는 원본데이터를 단계적으로 복제해야 한다. NAS는 자체 백업 애플리케이션을 보유하고 있어 PC백업, 파일 공유, 원격지 백업에 대하여 백업 정책을 이행할 수 있다. 그러나, 전용 백업 소프트웨어가 없는 경우 백업 데이터를 백업 시 모두 '읽기 전용으로 설정'하여 추후 데이터 망실이 발생한 경우 복구될 수 있도록 무결성을 유지해야 한다.

또한, 백업 완료 후 백업 매체관리는 별도의 접근통제 절차를 수립하여 운영하며, 네트워크를 통해 백업된 NAS디스크 1본을 사내 네트워크가 분리된 장소 (Off-Site)에 분리 보관하고 소산백업이 어려운 환경인 동일장소 백업 시 백업 후 네트워크 분리 보관하여 별도의 시건된 장소에 보관하거나, 백업된 데이터를 원격지 NAS 스토리지 또는 외부 백업센터(IDC) 스토리지에 백업하는 방법이 있다.

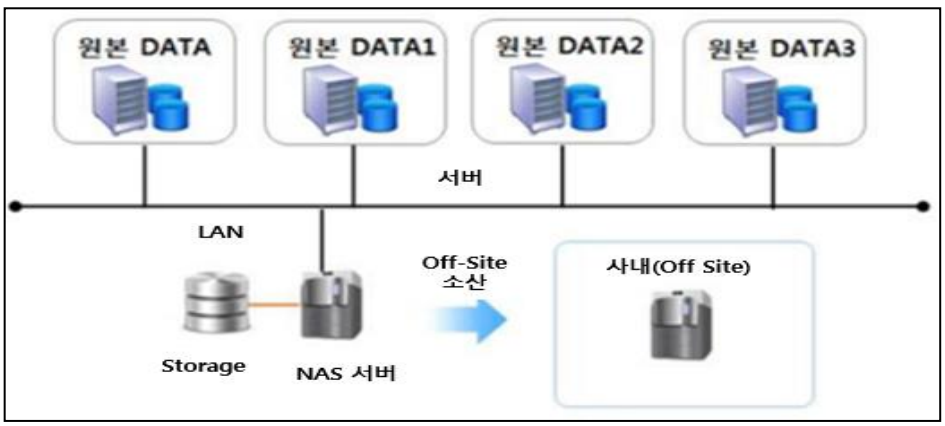


그림 50. NAS 백업 소산 구성

4) 외장 디스크 백업(USB/DVD 등)

외장 디스크(USB/DVD 등) 백업방식은 시스템 운영체제 내 작업 스케쥴 기능(Window 스케쥴 관리, Linux/Unix Crontab)을 배치 프로세스로 구성하고 정기적(주간, 월간) 백업 스케줄을 설정하여 개발 소스 및 기업의 중요 파일에 대하여 직접 백업을 받아 별도로 시건 장치가 있는 캐비넷 또는 별도 장소에 보관한다.

본 백업은 주로 사용자 PC 데이터를 백업하는 방식으로 랜섬웨어로부터 데이터를 보호하는 적절한 방법 중 하나이며 동일 장소 백업 시 효과적이며, 백업 후 백업매체 관리 절차를 수립해야 한다.

백업절차는 외장 디스크(USB/DVD 등)이 직접백업과 동일하므로 향후 랜섬웨어 감염에 대비하기 위해서 여러 개의 백업 매체를 사용하여 백업을 수행해야 안전 하다. 또한, 백업 담당자는 백업이 완료된 경우 반드시 백업된 데이터를 검증해야 하며, 백업 이력(백업 날짜, 백업데이터 종류, 백업 수행자 등)을 관리해야 한다.

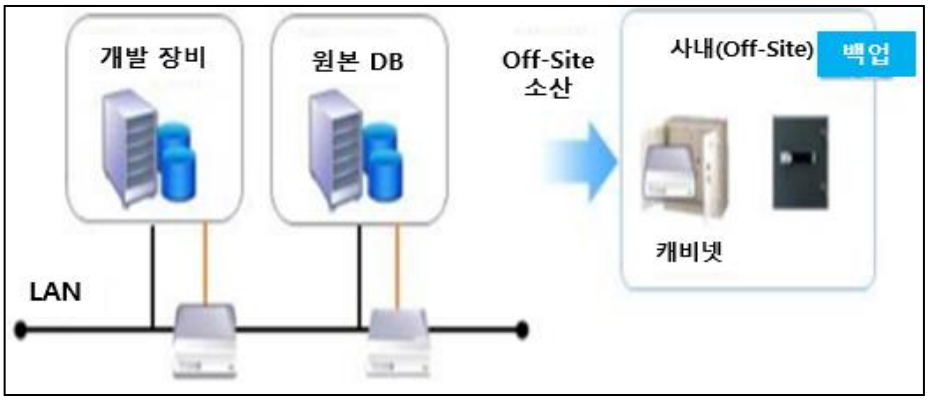


그림 51. 외장 디스크 소산 백업 구성

4.5.3 랜섬웨어 피해예방을 위한 복구전략

기업의 비즈니스 활동에 직접적인 영향을 주는 업무 연속성을 보장할 수 있도록 수립한 재해복구전략에 기반하여 랜섬웨어 피해 발생 시 예상 복구 소요시간 범위를 초과하지 않고 다운타임을 최소화하여 이전의 상태로 회복시켜 서비스를 신속하게 재개할 수 있도록 복구절차를 숙지하고 주기적으로 훈련을 실시하여야 한다.

가. 백업 수행 점검 및 복구훈련

1) 백업대상 시스템에 대해 적절한 소프트웨어 모듈이 설치되었는지 확인하고 백업대상 파일들이 모두 포함되어 있는지 확인한다.

2) 비상시 복구 훈련은 정기적으로 실시하여 데이터의 무결성 및 가용성을 확인해야한다. 또한 복구 훈련을 통해 복구시간을 산정하여야 하는데 일반 파일의 경우에는 복구시간이 리 스토어 시간과 동일하지만, 데이터베이스의 경우 리스토어 시간과 리커버리시간을 합친 시간 이 복구시간이 된다.

- 리스토어 시간은 테이프로 백업 받은 데이터를 다시 디스크로 복사하는 시간으로서 백업 장비의 성능과 디스크 성능에 따라 좌우된다.

- 리커버리 시간은 리스토어 이후에 정보시스템에 장애가 난 시점으로 복구하는 시간으로서, 데이터 베이스가 변경로그 모드인 경우 백업 후 장애시점까지 발생한 변경로그를 데이터베이스에 적용하는 시간이다

복구 = 리스토어 시간 + 리커버리 시간

나. 유의 사항

1) 백업 저장 매체에 대한 물리적 접근통제와 물리적인 백업 테이프 접근은 원본 파일시스템이 이 또는 데이터베이스가 있는 디스크에 루트 권한으로 접근하는 것과 동일하다. 테이프를 무방비로 노출시킨다면 어느 곳에서나 테이프를 읽을 수 있다. 따라서 별도의 접근통제 절차를 수립해야 한다.

2) 백업 테스트를 통한 백업 및 복원의 정기적 적정성 확인 및 다양한 환경에서 테스트를 연 1회 이상 실시하여 데이터의 무결성과 시스템의 가용성을 유지해야 한다.

- 실제 환경을 반영해 하드웨어, 소프트웨어, 서비스 장애 상황 테스트 (랜섬웨어 등 악성코드 삽입 여부 포함)
- 사용할 수 있는 모든 복원 옵션을 테스트
- 테이프 같은 기존 백업 미디어가 새로운 백업 하드웨어 및 소프트웨어에서 정상작동 하는지 여부 확인

3) 백업 담당자 및 운영자 PC 보안강화
- 기업의 백업 담당자들의 업무용 PC에 대해 비인가자의 접근을 통제 해야 한다.
- 최신 패치 및 백신 업데이트를 실시간 으로 설정해야 하고 외부 인터넷을 차단 또는 망을 분리 해야 한다.
- 백업 담당자 및 운영자 PC를 대상으로 악성코드 감염, 백신 업데이트, 패치, 공유폴더 사용, 외부 인터넷 사용 여부 등에 대한 보안성을 주기적으로 점검해야 한다.

5. 랜섬웨어 전용 솔루션에 대한 고찰

최근 발생하고 있는 랜섬웨어 공격의 경우 앞서 1.1.3에서 언급한바와 같이 APT 공격과 결합된 공격자 주도의 정찰 후, 대규모 파괴, 유출 행위도 수행한다

이러한 공격행위에 대해 각 보안담당자가 랜섬웨어 공격과 APT 공격을 이해하고 대응에 맞는 솔루션을 도입하는게 매우 중요하기 때문에, 여기에서는 랜섬웨어 공격과 APT 공격 등에 대한 차이를 살펴본 후 랜섬웨어 솔루션 도입 시 검토해야 할 항목들에 대해 살펴보고자 한다.

APT 공격 목적은 해당 기업의 시스템에 정보를 획득하고자 침투와 정보유출을 목적으로 하고 있다.

공격방식으로는 무작위로 대량 배포되는 일반 악성코드와는 달리 치밀하게 계획돼 소량 배포하면서 침투를 시도하고, 잠복하는 동안 여러 번의 공격을 지속적으로 시도한다. 침투 시 보통 타깃이 되는 기업이나 단체, 기관, 사람에 대해 치밀하게 조사를 진행하는 사회공학적 기법을 사용하고 있다. 침투 후에는 오랜 시간 동안 잠복을 통해 원하는 정보에 접근하거나 다량의 정보를 유출하기도 한다.

또, 공격 유형도 집단을 타깃으로 정하고 공격하므로 개인보다는 집단에서 타깃을 정하고 공격하는 경우가 많다는 특징이 있다. 이때 조사조, 공격조, 협박조 등 과정을 세분화해 분업하기도 하며, 일부 외국의 사례를 보면 불법적인 범죄집단이나 목적으로 가지고 정보를 유출 하고자 하는 기관으로부터 스폰서십을 받기도 한다.

이에 비해 랜섬웨어 공격의 최종목적은 댓가(돈 또는 가상화폐 등)를 요구하는 것이 뚜렷하다.

최근 공격방식으로는 앞선 1.2에서 언급한 바와 같이 AD서버 및 VPN 등과 같은 장비의 취약점을 통한 내부침투, 사회공학적 기법 등의 이메일, URL 유도 등과 같은 취약점을 통한 내부침투 후 문서, 사진, MBR, DB정보 등 데이터를 암호화 하며 유출도 한다.

다만 랜섬웨어 공격의 기술적 기량은 공격자의 기술과 정교함의 정도에 따라 암호화된 파일의 해독키가 없으면 물리칠 수 없는 공격이 있는가 하면, 일부는 공격자에게 몸값을 주지 않고도 리버스 엔지니어링을 통해 해결 가능한 경우도 있다.

APT 공격과 랜섬웨어 공격은 과정상의 차이보다는 행위에 대한 차이 및 목적에 대한 차이가 있다고 보며 APT 공격대응과 랜섬웨어 공격대응에 대한 가장 큰 차이는 사전탐지, 복구 및 예방활동의 차이로 본다

즉. 공격행위에 대한 선제대응 방법이 차단에 집중화 되어 있는지 차단 및 예방에 집중화 되어 있는지가 가장 크다고 판단한다. 이에 랜섬웨어 대응 솔루션 도입 전 검토해야 할 사항과 도입 시 검토해야 할 사항에 대해서 정리해보고자 한다

먼저 랜섬웨어 대응 솔루션 도입 전에는 안티 스팸 솔루션의 형식과 같은 중앙 집중식으로 도입을 할 것인지 EDR과 같이 PC영역에서 대응하는 솔루션을 도입할 것인지 검토를 해야 한다.

5.1 랜섬웨어 기본 점검항목

5.1.1. 사용자 환경(End-point) 설치형 랜섬웨어 대응 솔루션 체크항목

PC의 경우 다양한 사용자환경에 따라 동작여부를 측정해야 한다. 이중 지원이 가능한 OS 영역, 사전방어 및 행위차단, 대피소 및 SMB 서버보호, 탐지 및 진단방법, 백업 등의 다양한 기능들이 제공돼야 한다. 또한 각 PC의 정책을 동일하게 적용함으로써 랜섬웨어 감염을 최소화 해야 한다. 자세한 측정항목 중 기본기능은 다음과 같다.

가. 적용 또는 지원 가능한 OS 영역
사용자 PC의 경우 랜섬웨어 대응 솔루션이 지원되는 OS 버전을 확인해야 한다. MAC OS인지 WIndow 기반 OS인지 확인 후 버전별 OS에 맞게 제공이 되는지 확인해야 한다.

나. 랜섬웨어 사전방어 및 파괴행위 차단여부 확인
랜섬웨에 대응에 대한 전용 엔진의 보유여부 및 이를 기반으로 여러 종류의 랜섬웨어 행위에 대한 실시간차단 및 행위 탐지, 롤백이 가능한지 확인해야 한다.

다. 랜섬웨어 대피소 기능
PC 내 파일의 훼손시 원본 파일을 백업 폴더로 실시간 백업 및 보호할 수 있어야 한다.

라. SMB 서버보호 기능
원격지 PC 또는 가상화 영역에 대한 폴더, 드라이브 변조 시 알람 및 보호가 가능해야 한다.

마. 탐지 및 진단방법
랜섬웨어에 대해 시그니처 기반의 탐지인지 행위기반의 탐지인지 가상화검증 및 실행방법인지 등 탐지 및 진단방법에 대해 확인돼야 한다. 이중 시그니처 기반과 행위기반의 탐지가 동시에 적용되거나 여러 방식의 탐지방식으로 적용되는 지 확인하면 된다

바. 행위기반(상황인지)기반의 탐지 여부

상황인식 기반 랜섬웨어 탐지 기술은 파일의 변조 시점에 정상적 변경과 악의적 변경을 판단해 별도의 업데이트 없이 신종 랜섬웨어의 사전 탐지가 가능한지 확인이 필요하다. 상황인식 기반(CARB) 기술은 파일이 변경될 때 확인되는 정보가 매우 다양하므로, 이를 추적하고 관리해 정상적인 파일의 변경과 비정상적 변경의 구분이 가능해야 한다.

사. OS 및 중요 데이터의 백업기능

최근 랜섬웨어는 대부분 Microsoft VSS공격을 수행하므로 제공되는 백업 기술이 VSS를 쓰지 않는 독립적 기술인지 확인해야 한다. OS 복원과 별개로 사용자 데이터는 실시간 백업/복원이 지원돼야 한다. 또한 복원 과정에 복원된 파일의 재 암호화를 방어하기 위해 복원 파일의 보호 기능을 같이 제공해야 한다.

5.1.2. 중앙처리형 랜섬웨어 대응 솔루션 체크항목

중앙처리형 랜섬웨어 대응 솔루션들의 경우 이메일 및 망연계 시스템, 내부망에서의 전파감염 등에 효율적인 탐지와 차단이 가능해야 한다. 특히 네트워크 구간에서의 이상 트래픽을 감지하는 경우와 첨부파일 및 URL 등을 기반으로 탐지해 랜섬웨어 파일을 격리, 차단하는 경우로 나누어 볼 수 있다.

탐지에 대한 행위, 고도화된 탐지기술 및 차단여부, 파일 전문분석 엔진의 여부 등을 체크해야 하는데, 특히 진단시간의 경우 매우 빠른 시간을 요구하고 있으며 초기침입을 차단할 수 있어야 한다.

가. 행위기반 악성코드 탐지

내장되어있는 엔진을 통한 알려진 악성코드에 대한 빠른 탐지/차단 기능 유무를 확인한다. 실 환경과 동일한 환경을 가상분석 환경에 적용함으로써 탐지의 정확성을 높이고 오탐으로 인한 피해가 최소화 돼야 한다.

나. 폐쇄 환경에서의 악성코드 탐지

가상 분석 시스템을 통해 폐쇄 환경에서도 분석 기능을 제공하며, 정적 분석 시스템 및 동적 분석 시스템을 이용해 악성코드를 행위기반 분석기법을 통해 탐지하는 기능이 구현되는지 확인돼야 한다.

다. 장비 증가에 대비한 유연한 확장성

사용자의 환경 등의 증가 및 연계되어 있는 시스템의 확대를 대비하기 위한 장비의 환경유연성이 확보돼야 한다.

라. 통합 관리를 위한 가시성 확보

대시보드, 통합리포트를 통해 관리대상 보안수준, 악성 파일 분석현황, 주요 이벤트, 현황정보 등의 파악이 가능해야 하며, 주요 보안 이벤트 발생 시 알림(E-mail, SMS 등) 및 타 시스템과의 연계 기능 (Syslog, SNMP)을 통한 담당자의 빠른 상황인지가 매우 중요하다.

마. 알려지지않은 악성코드의 탐지

행위기반 탐지 우회공격, 알려지지 않은 Zero-Day 공격적 악성행위가 없는 악성코드의 탐지, 진단, 차단이 가능해야 한다.

5.2 랜섬웨어 대응 솔루션들

현재 기업들이 사용하고 있는 랜섬웨어대응 솔루션들은 행위기반의 탐지 및 분석을 기본으로 하고 있으며 행위기반 + AI 기술과 접목하는 경우 / 행위기반 + 센서 / 행위기반 + 백업 / 인증 + 행위기반 + 백업등과 같이 다양한 방식을 혼합한 탐지 및 대응기술 등도 제공하고 있다.

탐지의 경우 문서를 암호화 시키는 것은 압축 프로그램이 압축하는 행위와 같은데 학습된 AI 기능이 압축행위에 대한 정상적행위와 악의적인 행위의 차이를 구별해 랜섬웨어 행위를 차단하는 경우도 있다,

방어의 경우 중요한 파일에 대해서 PC 내 특정폴더에 주기적으로 저장, 백업하고 해당 폴더를 보호하여, 감염이 되더라도 피해를 최소화 하도록 하는 기능의 솔루션들도 존재한다. 최근에는 PC 내 실시간으로 백업을 하는 것과 동시에 클라우드백업(정책에 따른 설정)을 실시하여 랜섬웨어를 방어하기도 한다.

위 기능을 제공하는 솔루션들의 공통적인 특징으로는 예전 솔루션의 경우 탐지 및 방어에 집중되었다면 백업 및 복구 등과 같은 복구 프로세스를 함께 적용해 기업의 리스크를 최소화 하는 방안이 함께 적용되고 있다는 점을 들 수 있다.

이에 현재 시장에 출시돼있는 주요 솔루션들의 특징을 소개하고자 한다.

- N사의 랜섬웨어 대응 솔루션의 경우 행위기반으로, AI를 접목시켜 랜섬웨어 진단력을 강화시켰다. 특히 랜섬웨어가 문서를 암호화 시키는 것은 압축 프로그램이 압축하는 행위와 같은데 랜섬웨어의 악성코드가 압축을 하는 행위에 대해 AI가 이러한 차이를 구별해 탐지하는 방식이다.

- A사의 랜섬웨어 솔루션의 경우 백업 및 복원, 가상화영역의 실행 및 검증방식을 사용하고있다. 중요한 파일에 대해 PC의 특정 폴더에 주기적인 백업을 통해 관리하는 프로그램으로 자체보호기술을 이용해 항상 특정 폴더를 보호함으로써 랜섬웨어에 감염이 되더라도 피해가 발생하지 않도록 하는 것이 특징인 솔루션이다.

- E사의 경우 행위기반 및 백업방식으로 구성되어 있다. 랜섬웨어 방식(사전차단 및 파일복구 제공), PC백업(파일생성 및 수정 시 PC에 실시간 백업과 필요시 사용자가 일괄복원), 클라우드 백업 등의 단계별 대응을 통해 랜섬웨어를 방어한다.

- B사의 랜섬웨어 솔루션은 행위기반 + 센서방식으로 운영 중이다. 1차 알려진 랜섬웨어 블랙리스트 차단, 2차 신/변종 랜섬웨어 유사도 차단, 3차 랜섬웨어 암호화 행위 센서 차단, 4차 화이트리스트 기반 폴더 보호로 단계별로 보호하고 있다.

- C사의 경우 행위기반 + 백업형태로 구성되어 운영 중이다. 자체 개발한 엔진을 통해 랜섬웨어를 특정할 수 있는 시그니처나 패턴 없이 파일 변조 시점에서의 상황을 판단하는 핵심 기술로, 파일의 변화를 실시간으로 감지해서 알려지지 않은 훼손 행위에 대해서도 정확히 탐지, 원상복구가 가능하도록 되어있는 것이 특징이다.

- S사의 경우 중앙집중식으로 이메일 구간, 파일구간에서 어셈블로 레벨의 악성코드 분석을 수행함으로써 탐지 및 차단을 하고 있다. 또한 AI 및 자동화 기술을 바탕으로 대규모의 악성코드 공격을 자동으로 탐지를 하고 있는 것이 특징이다.

- Q사의 경우 네트워크 감지 및 응답(NDR) 어플라이언스가 선택적으로 네트워크 트래픽을 차단하고 멀웨어의 레터럴 무브먼트를 탐지해 데이터 누출 및 암호화가 발생하기 전에 적대적 활동을 중지하는 것이 특징이다.

물론 제품가격이 비싸고 AI 등과 같은 기술을 적용한 랜섬웨어 대응 솔루션을 도입한다고 해서 랜섬웨어 방어가 완벽히 보장되는 것은 아니다. 보안담당자로서 우리기업에 맞는 규모 및 업무의 형태, 조직 구성원간의 커뮤니케이션 방식 등에 따라 알맞는 솔루션을 검토하는 것이 매우 중요하다. 또한 우리기업이 보호해야 할 데이터 및 자산에 대해서 우선순위를 정하고 보호정책에 맞는 솔루션을 고려해야 할 것이다.

편집 후기

카카오 김형기

몇 해 전 국내 호스팅 업체의 랜섬웨어 감염 사고로 인해서 이름을 알리기 시작한 랜섬웨어가 이제는 국내외에서 심각한 사업 위기를 초래할 수준으로 위협이 되어 가고 점차 웜 등과 결합하여 고도화 되어 가고 있습니다. 이러한 시기에 랜섬웨어에 대한 기업의 대응에 도움이 될 수 있는 문서의 작성에 참여 할 수 있게 되어 기쁘게 생각합니다. 랜섬웨어에 대한 모든 걸 다 넣지는 못하였지만, KISA/CONCERT 관계자 여러분과 위원장님, 그리고 다른 편집위원님들의 큰 노력으로 꼭 필요한 부분은 들어가 있다고 할 수 있는 본 보고서가 기업 담당자님의 랜섬웨어 대응에 도움이 되었으면 좋겠습니다. 감사합니다.

엔씨소프트 장석은

이번 랜섬웨어 리포트의 편집위원으로 참여하면서, 수년전부터 많은 이슈가 되고 있었던 랜섬웨어의 확산이 실제 기업에게 얼마나 많은 피해를 주고 있는지, 기업은 랜섬웨어를 어떻게 대응하고 있을까에 대한 궁금함을 갖고 설문조사를 준비하고 결과를 정리했습니다. 기업을 대상으로 한 대규모 설문조사를 했고, 피해경험에 대한 보수적인 답변을 감안했을 때 조사대상의 절반의 기업이 크고 작은 랜섬웨어의 피해를 당했던 것을 확인했고, 좀더 적극적인 정보공유와 방어체계대한 종합적인 지원이 필요하다는 것을 깨닫는 소중한 경험이었습니다. 절정의 무더위에 리포트를 작성에 고생하신 다른 편집위원분들께도 감사의 말씀을 드립니다.

신세계디에프 최병훈

공격을 하는 방법은 다양해 지고 피해는 지속적으로 커져가고 있는 이 시대에 최근 화두가 되고 있는 랜섬웨어에 대한 정의 및 각 기업에서의 준비항목, 솔루션 도입의 체크포인트 등에 대해 정리하는 뜻깊은 시간이었습니다. 특히 소수의 정보보안담당자들이 있는 기업 또는 많지 않은 정보보안 예산으로 운영을 하는 정보보호 담당자 분들께서 이번 랜섬웨어 레포트를 통해 보다 효율적인 랜섬웨어 방어대책을 세우는데 도움이 되었으면 좋겠습니다. 금번 레포트를 작성하신 모든 집필위원님들과 랜섬웨어 리포트를 기획하신 KISA/CONCERT 관계자 모든 분들 수고 많으셨습니다

안랩 박제석

보안담당자로서 랜섬웨어는 정말 피하고 싶은 악성코드입니다. 랜섬웨어에 공격을 당하게 되면 철저한 사전준비 외에는 대안이 없는게 현실입니다. 보안담당자로서의 경험과 기업내 관리자로서의 지식을 기반으로 랜섬웨어 감염 대응을 위한 업무연속성계획을 기술하였습니다. 부족하지만 여러분의 회사에서 랜섬웨어를 대응하기 위한 사전준비에 도움이 되기를 희망합니다. 무더운 더위속에서도 함께 리포트를 작성하신 편집위원님들과 리포트를 기획하고 편집하신 관계자 분들께도 감사드립니다.

KGC인삼공사 이익준

금융회사, IDC, 중소기업의 IT 및 정보보호 담당자들과 소통하면서 실무차원에서 필요한 백업 및 복구 방법에 대해 정리하는 의미 있는 시간이었습니다. 다양한 랜섬웨어 공격 피해가 산불, 지진과 같이 기업의 생존을 위협하는 심각한 재해와 동일하다는 인식변화 와 IT 부서 및 정보보호 부서가 서로 공동체로서 적극 협력하여 랜섬웨어 위협을 사전에 예방 하고 피해 발생 시 신속하게 복구하는데 본 리포트가 도움이 되기를 희망합니다..

ENKI 안소희

랜섬웨어는 악성코드 분석가로서 분석할 때마다 힘들고 고통스러운 악성코드입니다. 감염 시 너무 많은 자산에 미치는 피해를 코드단에서부터 생생하게 확인하기 때문에 더욱더 그리 느껴집니다. 이번에 리포트를 작성하면서 여러 규모의 기업 보안 담당자분들의 이야기를 들으며, 랜섬웨어의 대응 방안에 대한 다양한 관점에 대해 많이 배워갑니다. 이 리포트를 통해 많은 기업의 보안 담당자분들이 랜섬웨어의 위협으로부터 보다 자유로워지길 희망합니다. 랜섬웨어 사전 예방부터 사후 대응까지 많은 분야에서 이 리포트가 많은 사람들에게 도움이 되었으면 좋겠습니다. 멋진 기회 주셔서 감사합니다.

에스케어 윤우희

최근 랜섬웨어 공격이 전문가 집단을 통한 APT 공격을 통한 대규모 피해를 발생시키고 있습니다. 미국의 경우 송유관 기업을 대상으로 한 사보타주 공격이 발생하였습니다. 갈수록 공격은 고도화되고 진보하고 있습니다. 보안관계자 분들께서 방어란 어렵지만 기업 생존을 위해 반드시 필요한 영역이라는 자부심과 긍지를 가지고 근무하셨으면 합니다. 보안업계 종사자로서 금번 보고서 작성이 랜섬웨어의 위험성과 공격동향을 심층적으로 분석하는 계기가 되었고 작성된 내용이 보안관리자분들께 작게나마 도움이 되었으면 합니다. 보고서 작성에 참여해주신 CISO님, 보안전문가님들과 함께 많은 것을 배우고 나눌 수 있는 좋은 기회를 주심에 감사의 마음 전합니다.

CONCERT 심상현

랜섬웨어에 대한 대책들을 보면 늘 갑갑한 마음입니다. 대부분의 보안대책에는 사전/사후대책을 논할 수 있는 반면, 랜섬웨어는 특이하게도 사후대책이라 할만한 것이 여간 군색한 게 아니기 때문입니다. 그럼에도 불구하고 본 리포트에 최대한 많은 것을 포함시키려 노력했습니다. 모든 사고를 완벽하게 예방할 수 없고, 사고대응을 위한 투자여력도 기업마다 다른 환경에서도 우리 보안담당자들은 늘 '선량한 관리자의 주의 의무'를 다해야 하기 때문입니다. 때론 즐겁고 때론 지난한 협업이라는 과정을 즐거운 기억들로 채워주신 모든 편집위원 분들께 진심으로 감사드립니다.

Appendix. 설문조사 항목

안녕하십니까?
한국인터넷진흥원(KISA)과 (사)한국침해사고대응팀협의회(CONCERT)에서는 각급 기업/기관의 보안담당자 여러분들을 대상으로 **랜섬웨어에 대한 이해도와 대응현황**을 알아보기 위한 설문조사를 실시하고 있습니다.
본 설문 결과는 **'Special Report - Ransomware 대응'을** 통해 공개할 예정이며, 응답하신 내용들은 순수 연구목적으로만 활용됩니다. 현실적인 정보 공유가 될 수 있도록 회원여러분의 적극적인 응답을 요청드립니다.

※ **주관기관 : (사)한국침해사고대응팀협의회(CONCERT) / Tel. 02-3474-2490**

모집단 참조를 위한 기초조사

<table>
<tr><td>기업규모
( )</td><td>① 50명 미만
② 50~100명 미만
③ 100~500명 미만
④ 500~1,000명 미만
⑤ 1,000명 이상</td><td rowspan="2">업종
( )</td><td rowspan="2">① IT, 인터넷, 게임
② 금융
③ 제조, 소비재
④ 유통, 커머스
⑤ 전력, 가스
⑥ 건설, 운송
⑦ 통신
⑧ 정유, 화학, 조선
⑨ 서비스
⑩ 직접입력( )</td></tr>
<tr><td>매출규모
( )</td><td>① 100억 미만 미만
② 100~1000억 미만
③ 1000~5000억 미만
④ 5000억~1조 미만
⑤ 1조억 이상</td></tr>
</table>

Ⅰ. 랜섬웨어에 대한 인식 조사

1. 최근의 랜섬웨어 공격확산이_'귀사'에 위협이 되고 있다고 생각하십니까? ( )

① 우리회사에 심각한 비즈니스 위협이 되고 있다
② 우리회사에 경미한 비즈니스 위협이 되고 있다
③ 비즈니스 위협이 맞으나 우리회사에는 큰 위협이 아니다
④ 비즈니스 위협이 아니라, 다소 과장된 보안사고 뉴스 중 하나이다
⑤ 잘 모르겠다.

2. 랜섬웨어의 급증과 피해확산으로부터의 가장 큰 교훈은 무엇이라고 생각하십니까? ( )

① 우리회사도 언젠가는 랜섬웨어의 피해자가 될 수 있어 대응이 필요하다
② 랜섬웨어는 새로운 방식으로 더욱 위협적으로 진화하고 있어 대응이 어렵다
③ 랜섬웨어에 대한 임직원들의 보안인식에 대한 교육과 대응이 중요하다
④ 다른 악성코드보다 더 위험한 공격이다
⑤ 랜섬웨어를 완벽하게 대응하기는 너무 어려운 과제이다
⑥ 뉴스기사들 보다 더 큰 위협이 되고 있다
⑦ 잘 모르겠다

3. '귀사'에서 중요한 시스템이 랜섬웨어에 감염됐을 대응활동 중 가장 중요한 것은 무엇이라고 생각하십니까? ( )

① 공격자들에게 비용을 지불하고 복구한다
② 관계기관(KISA, 경찰 등)에 신고한다
③ 침해사고대응을 위한 전문업체에 의뢰한다
④ 복구업체에 연락하여 복구방안을 찾는다
⑤ 백업된 데이터로 복구하는 사내 대응절차를 진행한다
⑥ 잘 모르겠다

4. 귀사에 대한 랜섬웨어 공격의 위협 수준은 어느정도라고 생각하십니까?( )

(매우 낮다) 1 2 3 4 5 6 7 8 9 10 (매우 높다)

Ⅱ. 랜섬웨어 피해 영향도 조사

5. 랜섬웨어로부터의 피해경험이 있습니까? ( )

※본 질문은 답변에 따른 다른 문항을 확인해 주십시오.

① 예(6번 문항으로 이동)

② 아니오(7번 문항으로 이동)

6. 랜섬웨어의 피해 경험이 있는 회사에 소속된 분만 6-1 ~ 6-4문항에 답변을 부탁드립니다.

6-1. 랜섬웨어 피해가 있었다면, 어떤 유형의 랜섬웨어 피해를 입었습니까?

[해당되는 모든 것 선택] ( )

① 파일 암호화를 통한 데이터 접근제한

② OS에 대한 액세스 차단으로 업무/서비스 불가

③ 회사 데이터 유출을 빌미로 한 협박

④ 가짜 암호화 또는 데이터에 대한 제한된 액세스 후 비용 요구(비 암호화 랜섬웨어)

6-2. 랜섬웨어 피해가 있었다면, 랜섬웨어 감염으로 인해 '회사'의 피해는 무엇입니까?

[해당되는 모든 것 선택] ( )

① 생산성 손실(서비스 장애, 시스템 다운 등)

② 데이터 손실

③ 회사 데이터의 유출

④ 평판(회사 이미지) 손상

⑤ 재무적 손실

⑥ 개인정보 유출로 인한 소송

⑦ 피해 없음

6-3. 랜섬웨어 피해가 있었다면, 이후 회사에서는 어떤 대응을 하였습니까?

[해당되는 모든 것 선택] ( )

① 새로운 보안인식교육 실시

② 시스템 업그레이드 및 패치

③ 내부 시스템 접근통제 강화

④ 주요 시스템 로그 수집/모니터링 확대

⑤ 랜섬웨어 대응 솔루션 구축

⑥ 중요 데이터의 백업체계 수립

⑦ 시스템 백업

⑧ 업무연속성계획(Business Continuity Planning) 수립

⑨ 변경사항 없음

⑩ 기타( )

6-4. 랜섬웨어 피해가 있었다면, 랜섬웨어 공격자에게 비용을 지불하였습니까? ( )

① 예

② 아니오

③ 잘 모르겠다

7. 랜섬웨어의 피해 경험이 없는 회사에 소속된 분들께서만 7-1 ~ 7-4문항에 답변을 부탁드립니다.

7-1. 아직 랜섬웨어 피해 경험이 없다면, 어떤 유형의 랜섬웨어 피해를 당할 수 있다고 생각하십니까? [해당되는 모든 것 선택] ( )

① 파일 암호화를 통한 데이터 접근제한

② OS에 대한 액세스를 차단하여 업무/서비스 불가

③ 회사의 데이터를 유출하여 협박

④ 가짜 암호화 또는 데이터에 대한 제한된 액세스 후 비용 요구(비 암호화 랜섬웨어)

7-2. 아직 랜섬웨어 피해 경험이 없다면, 랜섬웨어 감염으로 인해 '회사'가 입을 수 있는 피해는 무엇이라고 생각하십니까? [해당되는 모든 것 선택] ( )

① 생산성 손실(서비스 장애, 시스템 다운 등)

② 데이터 손실

③ 회사 데이터의 유출

④ 평판(회사 이미지) 손상

⑤ 재무적 손실

⑥ 개인정보 유출로 인한 소송

⑦ 피해 없을 것으로 예상

7-3. 아직 랜섬웨어 피해 경험이 없다면, 회사에서는 어떤 준비가 필요하다고 생각하십니까? [해당되는 모든 것 선택] ( )

① 새로운 보안인식교육 실시

② 시스템 업그레이드 및 패치

③ 내부 시스템 접근통제 강화

④ 주요 시스템 로그 수집/모니터링 확대

⑤ 랜섬웨어 대응 솔루션 구축

⑥ 중요 데이터의 백업체계 수립

⑦ 시스템 백업

⑧ 업무연속성계획(Business Continuity Planning) 수립

⑨ 준비 사항 없음

⑩ 기타( )

7-4. 만일 '회사'가 랜섬웨어의 피해를 당한다면 공격자에게 비용을 지불하여 문제를 해결 하실 의향이 있습니까? ( )

① 예

② 아니오

③ 잘 모르겠다

III. 랜섬웨어의 탐지

8. 랜섬웨어는 어떠한 방법으로 '귀사'의 시스템을 공격하고 있다고 생각하십니까?
[해당되는 모든 것 선택] ( )

① 이메일을 이용한 악성코드 첨부 공격

② 피싱 등 악의적인 웹 사이트 방문 유도 공격

③ 원격 접속 환경 및 계정 정보 공격

④ 시스템의 취약점을 악용한 공격

⑤ 공급망 공격(응용프로그램 업데이트 악용)

⑥ 잘 모르겠다

⑦ 기타 ( )

9. 귀사에서 랜섬웨어를 탐지하는 방법은 무엇입니까? [해당되는 모든 것 선택] ( )

① 이메일 및 웹 Gateway 보안 솔루션

② 안티바이러스 프로그램(백신)

③ 랜섬웨어 탐지 솔루션이 포함된 보안프로그램

④ IPS, IDS(침입 탐지 시스템)

⑤ 네트워크 및 엔드포인트 행동 모니터링(xDR)

⑥ C&C 접속 모니터링

⑦ 사용자 제보

⑧ 공격을 받은 적이 없다

⑨ 잘 모르겠다

⑧ 기타 ( )

10. 귀사의 렌섬웨어 공격에 대한 탐지 대응 수준은 어느정도라고 생각하십니까? ( )

(매우 낮다) 1 2 3 4 5 6 7 8 9 10 (매우 높다)

Ⅳ. 랜섬웨어의 치료 및 복구

11. 귀사에서 랜섬웨어의 대응 계획을 수립하고 있습니까? ( )

① 예
② 아니오
③ 잘 모르겠다

12. 사용하고 계시는 안티바이러스 솔루션이 랜섬웨어로부터 '회사'를 보호하는 데 얼마나 효과적이라고 생각하십니까? ( )

① 매우 효과적이다
② 다소 효과적이다
③ 효과적이지 않다
④ 잘 모르겠다

13. 최근 랜섬웨어를 대응하기 위해 귀사가 안티바이러스 등 기존의 엔드포인트 보안 솔루션의 교체를 검토하셨거나 교체하였습니까? ( )

① 안티바이러스 등 엔드 포인트 보안솔루션의 교체를 검토하였거나 교체하였다
② 안티바이러스 솔루션의 새로운 솔루션을 고려하고 있다
③ 기존 솔루션을 유지할 계획이다
④ 잘 모르겠다

14. 현재 랜섬웨어에 대응하기 위해 어떤 보안 솔루션을 사용하고 있습니까?
[해당되는 모든 것 선택] ( )

① 이메일 및 웹 Gateway 보안 솔루션
② 데이터 백업 및 복구 솔루션
③ 랜섬웨어 탐지 솔루션이 포함된 보안프로그램
④ 네트워크 및 엔드포인트 행동 모니터링(xDR)
⑤ 사용자 인식제고 훈련 프로그램
⑥ OS 및 소프트웨어 패치 시스템
⑦ 어플리케이션 화이트리스팅 솔루션
⑧ 잘 모르겠다
⑨ 기타 ( )

15. 랜섬웨어 공격에 대해 회사의 치료및복구 대응수준은 어느정도라고 생각하십니까? ( )

(매우 낮다) 1 2 3 4 5 6 7 8 9 10 (매우 높다)

V. 랜섬웨어 예방

16. 향후 랜섬웨어가 귀사나 다른 기업에 더 큰 위협이 될 것이라고 생각하십니까? ( )

① 더 큰 위협이 될 것이다
② 큰 변화는 없을 것이다
③ 위협이 점차 감소할 것이다
④ 잘 모르겠다

17. 귀사가 랜섬웨어의 표적이 될 가능성이 어느 정도 있다고 생각하십니까? ( )

① 더 가능성이 높아질 것이다
② 큰 변화는 없을 것이다
③ 가능성이 점차 감소할 것이다
④ 잘 모르겠다

18. 귀사에서 랜섬웨어 대응에 필요한 예산이 어떻게 변경될 것으로 예상하십니까? ( )

① 큰 폭으로 증가할 것이다
② 다소 증가할 것이다
③ 변하지 않을 것이다
④ 다소 감소할 것이다
⑤ 잘 모르겠다

19. 귀사에서 준비하고있는 랜섬웨어 관련 보안 투자는 어떤것이 있나요?
[해당되는 모든 것 선택] ( )

① 새로운 보안인식교육 실시
② 시스템 업그레이드 및 패치
③ 내부 시스템 접근통제 강화
④ 주요 시스템 로그 수집/모니터링 확대
⑤ 랜섬웨어 대응 솔루션 구축
⑥ 중요 데이터의 백업체계 수립
⑦ 시스템 백업
⑧ 업무연속성계획(BCP) 수립
⑨ 피해보상을 위한 사이버 보험
⑩ 계획이 없음
⑪ 기타 ( )

20. 귀사의 랜섬웨어 공격에 대한 예방 대응 수준은 어느정도라고 생각하십니까? ( )

(매우 낮다) 1 2 3 4 5 6 7 8 9 10 (매우 높다).

바쁘신 일정 속에서도 본 설문에 참여해 주셔서 감사합니다!

(사)한국침해사고대응팀협의회 | CONCERT

CONsortium of CERT

현명한 사용자들의 Security Power User Group

CONCERT 사용설명서 보기

세미나&워크샵

- FORECAST
- 정회원워크샵
- 해킹방지워크샵
- Round Up
- OnTact-x

보안핵심인사이트(교육)

- 개인정보보호 컴플라이언스 전문가 양성 교육
- 개인정보 유출사고 대응훈련
- 개인정보보호 필수문서 교육
- 좋은 보고서 작성의 이론과 실습 교육
- ISMS-P 인증심사원 자격 검정 대비

정보제공

- 사무국리포트
- Consumer Report
- 기업정보보호 이슈 전망 보고서
- 뉴스레터

한국침해사고대응팀협의회

CONsortium of CERT CONCERT | Tel. 02-3474-2490
https://concert.or.kr