Keep up with Ransomware

늘고 있는 Play 랜섬웨어 공격 위협

■ 개요

2024 년 3 월 랜섬웨어 공격으로 인한 피해 사례 발생 건수는 전월(418 건) 대비 약 3% 감소한 405 건으로 나타났다. LockBit 랜섬웨어 그룹은 인프라 압수 후 복귀해서 폭발적인 공격력을 드러냈으나 3 월에는 다소 주춤한 모습을 보이고 있다. 한편, BlackCat(Alphv) 랜섬웨어 그룹은 활동을 잠정 중단하고 엑시트 스캠(Exit scam)[1]으로 추측되는 여러 정황이 포착되기도 했다. 즉, 3 월 랜섬웨어 공격 피해 사례 발생 건수가 전월 대비 소폭 감소한 데에는 LockBit 랜섬웨어 그룹과 BlackCat(Alphv) 랜섬웨어 그룹의 활동이 줄어든 상황이 영향을 미친 것으로 풀이된다.

'notchy' 계열사로 추정되는 사용자가 BlackCat(Alphv)으로부터 수수료를 받지 못했다고 주장하는 글을 러시아 해킹 포럼 램프(RAMP)에 게시한 게 이슈가 되기도 했다. 헬스케어(Healthcare) 기업을 공격하고 약 350BTC(한화 약 352 억 원)를 받았으나 BlackCat(Alphv) 그룹의 운영진은 해당 가상 화폐를 모두 다른 주소로 옮기고 수수료를 계열사에 지불하지 않았다는 것이다. 게시글이 업로드 된 이튿날 다크웹 데이터 유출 사이트의 화면은 국제 수사기관에 의해 폐쇄된 것으로 변경됐다. 그러나 해당 웹 사이트는 수사기관이 아닌 BlackCat(Alphv) 그룹에 의해 변경된 것으로 확인됐다. 또, BlackCat(Alphv) 그룹은 연락 수단 중 하나인 Tox 메신저의 상태 메시지를 'GG', 'Selling source code 5kk'로 변경하는 등 수상한 움직임을 보였다. 이는 전형적인 엑시트 스캠의 정황으로, 이후 다크웹 사이트와 포럼 등에서도 종적을 감추며 사실상 운영을 중단한 것으로 추측된다.

반면 Play, Medusa, RansomHub 그룹은 지난 2 월 대비 피해를 게시하는 글을 늘리며, 타 랜섬웨어 그룹에 비해 왕성한 모습을 보였다. 먼저, Play 랜섬웨어 그룹은 IT 서비스 업체 Xplain 을 공격해 스위스 정부와 관련된 약 6 만 5 천 건의 문서를 탈취한 이력이 있다.

[1] 엑시트 스캠(Exit scam): 계열사에게 수수료를 지급하지 않거나 랜섬웨어 피해자에게 돈을 지불받고 파일 복구를 해주지 않은 채 사라지는 사기 행위

해당 사건은 지난해 5 월 발생했으나 관련 조사는 지난달 마무리되었으며, 약 10 개월이라는 상당한 시간과 자원이 소모되었다. 해당 사건은 랜섬웨어 공격으로 인한 피해가 단발성으로 끝나지 않는다는 교훈을 안고 있다.

또한, Play 랜섬웨어 그룹이 커넥트와이즈(ConnectWise)의 스크린커넥트(ScreenConnect) 취약점 CVE-2024-1708[2], CVE-2024-1709[3]를 악용한 공격을 시도한 정황이 확인되기도 했다. 해당 취약점은 LockBit, BlackCat(Alphv), BlackBasta, Bloody 그룹 등 최근 다양한 랜섬웨어 그룹에서도 활발하게 악용 중인 공격 방식이다. 구체적으로 1-day 취약점[4]을 악용한 랜섬웨어 공격을 수행한다. 이는 비교적 쉽게 공격 대상을 지정 후 침투하기 용이하다. 공격 대상은 Shodan, Censys 등 인터넷에서 액세스할 수 있는 장치를 검색, 모니터링 및 분석하는 데 도움이 되는 플랫폼을 악용해 취약점이 존재하는 서버를 선별해 정한다.

이외에도 젯브레인(JetBrains)의 팀시티(Teamcity)에서 발견된 CVE-2024-27198 인증 우회 취약점과 CVE-2024-27199 디렉토리 순회 취약점을 악용한 사례도 있었다. BianLian 그룹과 오픈소스로 제작된 Jasmin 랜섬웨어가 이를 악용해 데이터 탈취 및 파일 암호화를 수행한 것이다. 해당 취약점을 통해서 랜섬웨어 뿐만 아니라 암호화폐 채굴기 악성코드인 XMRig, 침투 테스트 도구인 Cobalt Strike, 백도어 악성코드 SparkRAT 등을 유포해 악의적인 작업을 수행할 수 있는 것으로 확인됐다.

앞서 언급된 ScreenConnect 와 Teamcity 취약점 모두 CVSS[5] 점수가 9.8(CVE-2024-27198), 7.3(CVE-2024-27199), 8.4(CVE-2024-1708), 10.0(CVE-2024-1709)으로 상당히 높은 위협을 나타내고 있다. 또한, 노출되어 있는 서버 대부분이 취약점이 패치되지 않은 채 운용되고 있어 여전히 해당 모듈과 서버를 운영하고 있을 경우 빠른 조치가 필요하다.

마지막으로, MS-SQL 데이터베이스 서버 취약점을 통해 유포되는 Mallox(Fargo) 랜섬웨어를 복호화 할 수 있는 툴이 공개됐다. 비록 최신버전을 제외한 2022 년 10 월부터 2024 년 2 월까지 유포된 Mallox 랜섬웨어 변종만 지원하나, 많은 버전을 지원하는 만큼 피해를 경감시킬 수 있을 것으로 보인다.

---

[2] CVE-2024-1708: ConnectWise 의 ScreenConnect 에서 발생하는 디렉토리 순회 취약점

[3] CVE-2024-1709: ConnectWise 의 ScreenConnect 에서 발생하는 인증 우회 취약점

[4] 1-day 취약점: 발견된 취약점에 대하여 패치가 발표되었지만, 아직 적용되지 않은 취약점

[5] CVSS (Common Vulnerability Scoring System): 사이버 보안에 미치는 취약점의 위험성을 나타내는 수치

■ 랜섬웨어 뉴스

infosec

BlackCat(Alphv), Exit Scam 정황 포착

- 3월 3일, RAMP 포럼에 계열사 유저가 BlackCat(Alphv)으로 부터 수수료를 받지 못했다는 글 게시
- 2월 21일 발생한 HealthCare 기업 공격과 관련. 이를 통해 BlackCat(Alphv)이 받은 수익은 350BTC
- BlackCat(Alphv)은 수수료를 지불하지 않고 350BTC 모두 8개의 다른 주소로 전송
- BlackCat(Alphv) Tox 메신저 상태 메시지 변경 (GG → Selling source code 5kk)
- 다크웹 유출 사이트를 국제 수사 기관에 의해 폐쇄된 것처럼 FAKE 페이지 게시
- 다크웹 포럼에서도 모습을 감추며 사실상 운영 중단한 것으로 추정

JetBrains 社 TeamCity 취약점을 악용하는 랜섬웨어 그룹

- 인증 우회 취약점인 CVE-2024-27198과 디렉토리 순회 취약점인 CVE-2024-27199가 해당
- URL 조작을 통해서 TeamCity 엔드포인트에 접근이 가능하며, 이를 통해서 관리자 생성이 가능
- 3월 4일 취약점 완전 공개와 패치가 동시에 이루어 지면서 공격에 악용될 가능성 발생
- BianLian 그룹과 오픈소스로 제작된 Jasmin 랜섬웨어가 공격에 활용한 정황 포착
- 랜섬웨어 그룹 뿐만 아니라 채굴 악성코드와 백도어 등 다양한 악성코드 공격에 활용

Play, IT 서비스 업체 통해 스위스 연방 정부 데이터 유출

- 2023년 5월 발생한 공격으로, 같은 해 8월부터 행정 조사를 실시하여 2024년 3월까지 조사 진행
- 약 6만 5천건의 스위스 연방 정부 데이터가 유출되어 다크웹에 게시

aiohttp Python 라이브러리, 랜섬웨어 공격에 활용 의심

- aiohttp는 Python의 비동기 http 클라이언트/서버 프레임워크로, 디렉토리 순회 취약점인 CVE-2024-23334 발견
- 랜섬웨어 공격자 ShadowSyndicate가 2월부터 3월까지 해당 취약점에 취약한 서버를 스캔한 정황 발견
- 1월 28일 3.9.2 버전 출시로 패치 완료 및 2월 27일 GitHub*에 POC 익스플로잇 코드*공개

* GitHub : 웹 기반 소스코드 버전 관리 및 협업 플랫폼
* PoC (Proof of Concept) 익스플로잇 코드 : 취약점을 이용한 공격이 가능함을 보여주는 시현 소스코드

Mallox 랜섬웨어 복호화 도구 업데이트

- 키 생성을 통해서 복구하는 방식으로, 2022년 10월부터 2024년 2월까지의 변종 복호화 가능
- Mallox 그룹은 최신 변종에 대해서도 복호화 도구를 만들어보라는 포럼 글 게시

복호화 키를 포함한 CryptoWire 유포

- 2018년 유행하던 오픈 소스 기반 랜섬웨어로, 주로 피싱 메일을 통해 유포
- Autoit 스크립트로 제작되었으며, 스크립트에 복호화 키가 포함되어 있거나 복호화 키를 공격자 서버로 전송

Qillin, 영국 출판 및 사회적 기업 Big Issue 공격

- 인사 정보, 계약서 및 파트너 데이터, 재무제표 및 투자 정보 등 550GB의 데이터 탈취 주장
- Big Issue는 공격 인지 이후, 시스템 액세스를 제한하는 등 즉각적으로 조치 및 시스템 복구 진행
- 잡지 발행 및 배포에는 영향이 없다고 발표

Rust 버전 Qillin 랜섬웨어 변종 발견

- PowerShell Script를 활용하여 Rust 변종을 VMware vCenter* 및 ESXi 서버에 유포
- RMM 도구 및 Cobalt Strike, PsExec, SecureShell, SYS 드라이버 등 다양한 도구 및 시스템 활용

* VMware vCenter : 다수의 ESXi 및 가상 시스템을 중앙 집중 관리하여 모니터링 기능을 제공하는 서비스

KillSec 랜섬웨어 그룹 다크웹 유출 사이트 신규 개설

- 2023년 10월부터 텔레그램 채널 통해서 활동하던 랜섬웨어 그룹으로, 같은 해 11월 루마니아 경찰 공격 이력존재
- 2024년 3월, 다크웹 유출 사이트를 개설하여 피해자를 게시하기 시작

BlackByte와 RA Group 랜섬웨어 그룹 활동 재개

- BlackByte, 5개월 만에 다크웹 유물 사이트(DLS) 개편과 함께 신규 유출 1건 게시하며 활동 재개
- RA Group, RA World로 그룹명 변경 및 3개월 만에 유출 7건 게시하며 활동 재개

DarkRace 계열의 신규 랜섬웨어, Donex 등장

- DarkRace 랜섬웨어는 유출된 LockBit 빌더를 기반으로 개발
- 5월에 발견된 DarkRace 계열의 랜섬웨어를 사용하며, 신규 유출 5건 게시

Medusa, US #1364 Federal Credit Union 공격

- 미국의 금융 기관으로 대출, 투자, 저축, 카드 등 다양한 금융 서비스 제공
- 2월 21일 발생한 서비스 이용 장애와 연관된 것으로 추정
- 3월 7일 다크웹 유출 사이트에 게시

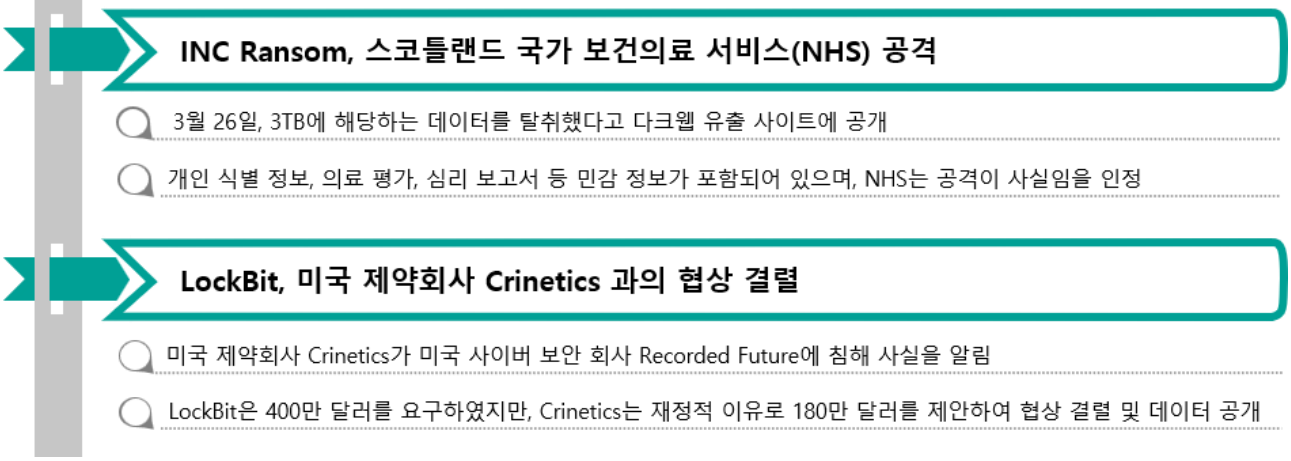

INC Ransom, 스코틀랜드 국가 보건의료 서비스(NHS) 공격
3월 26일, 3TB에 해당하는 데이터를 탈취했다고 다크웹 유출 사이트에 공개
개인 식별 정보, 의료 평가, 심리 보고서 등 민감 정보가 포함되어 있으며, NHS는 공격이 사실임을 인정
LockBit, 미국 제약회사 Crinetics 과의 협상 결렬
미국 제약회사 Crinetics가 미국 사이버 보안 회사 Recorded Future에 침해 사실을 알림
LockBit은 400만 달러를 요구하였지만, Crinetics는 재정적 이유로 180만 달러를 제안하여 협상 결렬 및 데이터 공개

그림 1. 랜섬웨어 동향

■ 랜섬웨어 위협

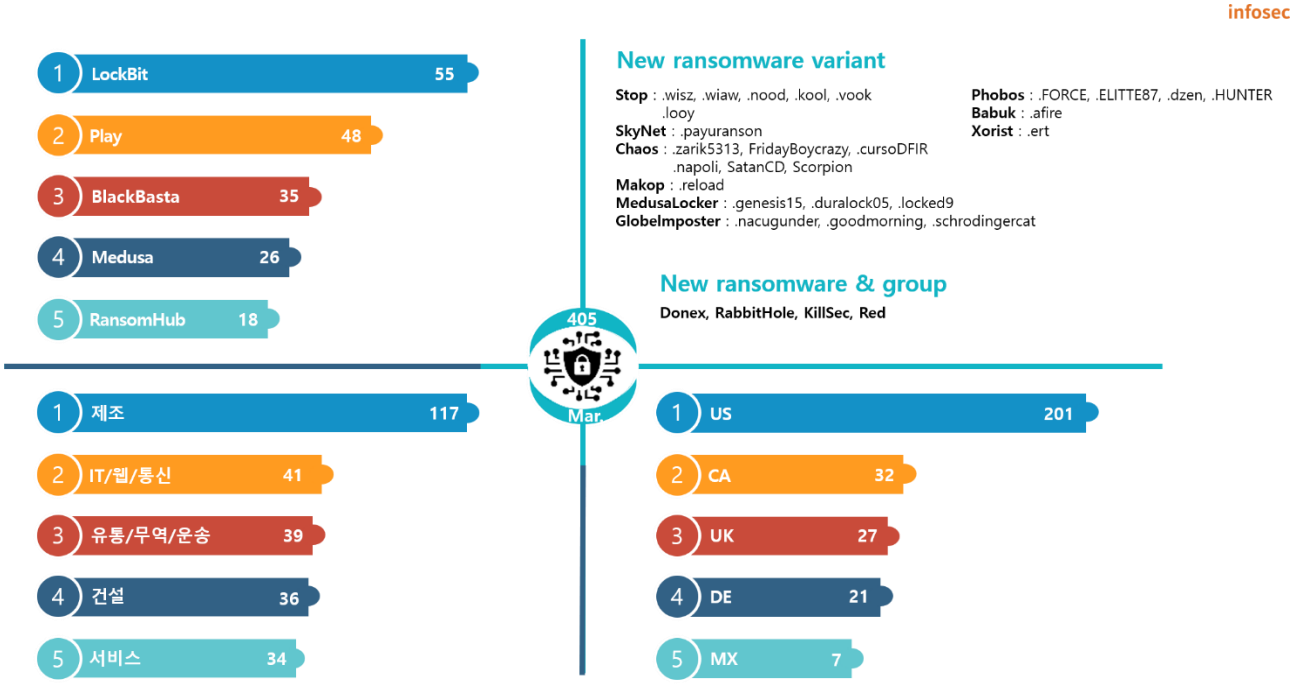


그림 2. 2024 년 3 월 랜섬웨어 위협 현황

새로운 위협

3 월에는 활동을 재개하는 그룹이 다수 발견됐다. 악명 높은 해킹 범죄 포럼인 브리치포럼(BreachForums)에서 활동하던 판매자 인텔브로커(IntelBroker)는 3 월에 계정을 복구하여 활동을 이어 나갔으며, BlackByte 랜섬웨어 그룹은 약 5 개월만에 데이터 유출 사이트를 개편하며 신규 유출 데이터를 게시했다. 마지막으로 라그룹(RA Group)은 2023 년 12 월 이후 3 개월만에 라월드(RA World)라는 이름으로 7 건의 데이터를 게시하며 활동을 재개했다.

Donex 그룹은 2023 년 5 월에 발견된 DarkRace 계열의 랜섬웨어를 사용하고 있으며, 현재까지 5 개의 조직에 대한 데이터를 유출시켰다. DarkRace 랜섬웨어는 유출된 LockBit 빌더의 코드를 기반으로 랜섬노트 형태, 파일 아이콘 변경, 변경되는 확장자 등 LockBit 랜섬웨어의 기술을 통합해 개발한 것으로 분석된다.

Rabbit Hole 그룹은 다크웹 데이터 유출 사이트가 발견됐다. 다만, 아직 어떠한 피해도 게시하지 않고 있어 인프라 구축 또는 공격을 준비하고 있는 것으로 보인다. KillSec 그룹은 2023 년 10 월부터 텔레그램을 통해 활동을 시작한 것으로 보이며, 최근 다크웹에 데이터 유출 사이트를 개설해 피해자를 게시하기 시작했다. 텔레그램의 유출 이력을 살펴보면 2023 년 11 월 루마니아 경찰 20 만 건의 데이터를 게시해 1,500 유로(한화 약 220 만 원)를 지불했다고 주장하고 있지만 사실 여부가 확인되지는 않은 상태다.

Red 그룹은 등장과 함께 총 12 건의 피해 유출을 게시했다. 발견 초기에는 유출 데이터의 모든 샘플 파일 다운로드 링크가 정상적으로 작동하지 않거나 일부 유출 대상이 이미 영업 정지된 곳을 나타내며 Scam 의혹이 존재했다. 하지만 4 월 1 일을 기준으로 모든 다운로드 링크가 정상적으로 작동하는 것이 확인되면서 이들이 Scam 그룹인지 여부는 더 지켜봐야 할 것으로 보인다.

Top5 랜섬웨어

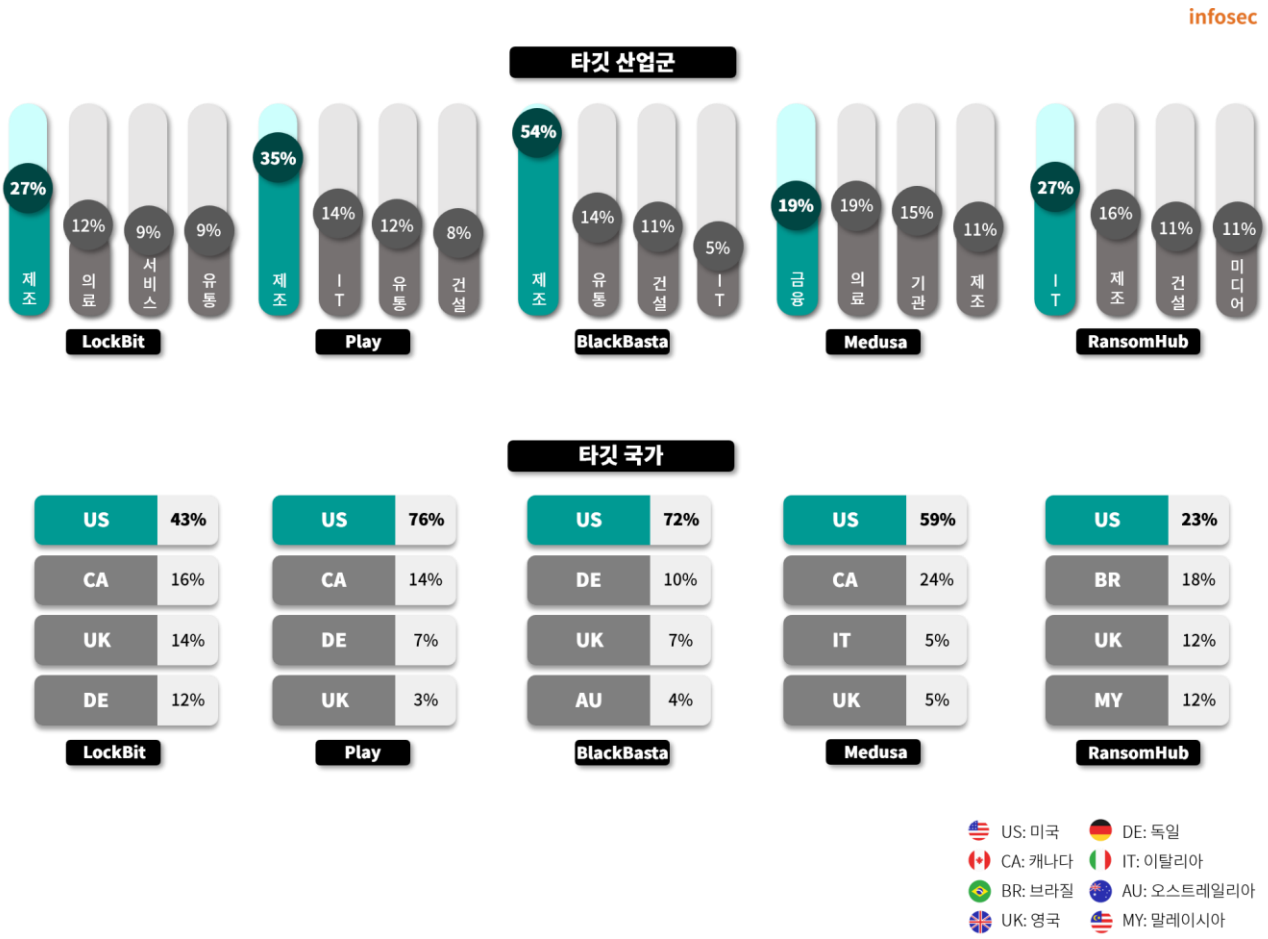


그림 3. 산업/국가별 주요 랜섬웨어 공격 현황

LockBit 랜섬웨어 그룹은 활동을 재개한 이후, 활발한 공격을 수행하며 가장 많은 피해자를 양산하고 있다. 이 가운데 '금전적인 부분을 타협하지 않는' 독특한 전략을 사용하고 있는 모습이 포착됐다.

지난 3 월 18 일 미국의 스타트업 제약 회사인 크리네틱스(Crinetics)를 다크웹 데이터 유출 사이트에 게시했다. 공개된 내용은 Crinetics 가 비밀 유지를 위반하고 미국 보안 회사인 레코디드 퓨쳐(Recorded Future)에 침해 사실을 공유했다는 것이다. 또한, LockBit 랜섬웨어 그룹은 Crinetics 에게 400 만 달러(한화 약 55 억 원)를 지불하지 않으면 데이터를 공개하겠다고 통보했으나, Crinetics 는 재정상황의 이유로 180 만 달러(한화 약 25 억 원)를 제시했다고 밝혔다. 결국 LockBit 은 이를 받아들이지 않고 데이터 공개를 통보하고 대화를 종료했다. 이러한 행보는 다른 기업들에게 협상 금액을 타협하지 않는다는 경고성 메시지를 보낸 것으로 풀이된다.

Play 랜섬웨어 그룹은 2022 년부터 꾸준하게 활동을 이어왔다. 올해 초 잠시 주춤하는 모습을 보였지만, 근래 다시 공격 사례가 증가하고 있다. 최근 랜섬웨어 트렌드와 일치하는 취약점을 악용한 공격을 수행하고 있지만, RaaS[6] 운영이 다수를 차지하는 다른 그룹과는 달리 서비스형 랜섬웨어 운영을 하지 않는 폐쇄적인 그룹으로 알려져 있다.

BlackCat(Alphv) 랜섬웨어 그룹의 활동 중단과 강세를 보였던 다른 랜섬웨어 그룹이 주춤하는 사이, Medusa, BlackBasta, RansomHub 그룹은 많은 랜섬웨어 공격을 수행하며 Top5 랜섬웨어로 급부상했다. BlackBasta 그룹은 지난 1 월 다크웹 유출 사이트가 약 10 일 동안 오프라인으로 변경되며 활동이 주춤한 모습을 보였지만, 최근 지속적으로 악용되고 있는 ScreenConnect 취약점 공격 수행 정황이 발견되면서 꾸준히 피해자를 게시하고 있는 것으로 파악된다.

Medusa 랜섬웨어 그룹은 최근 텍사스 정부 기관인 Tarrant Appraisal District(TAD)를 공격해 70 만 달러(한화 약 9 억 6000 만 원)의 몸값을 요구했지만 협상에 실패한 것으로 보인다. 또, 금융 기관인 US #1364 Federal Credit Union 을 공격해 서비스 장애를 일으킨 바 있다.

RansomHub 그룹은 CIS[7], 쿠바, 북한, 중국, 루마니아 국가 및 비영리단체에 대한 공격을 시도하지 않겠다고 밝혔다. 다만, 다크웹 유출 사이트에 공개된 내용에 따르면 공격 제외 대상에서 루마니아가 빠져 있는 모습을 확인할 수 있다. 또한, 랜섬웨어에 재감염 되지 않도록 규칙을 설정했다. 이와 함께 RaaS 제휴 프로그램을 러시아 해킹 포럼인 RAMP 에 게시하며 홍보를 진행하고 있다. 해당 랜섬웨어는 x25519 알고리즘을 사용해 대칭키를 보호하고 하드웨어에 따라 AES256, chach20, xchacha20 대칭키 알고리즘으로 파일을 암호화하여 빠른 암호화 속도를 지원한다. Go 언어[8] 기반으로 작성되어 윈도우, 리눅스, ESXi[9], ARM/MIPS[10] 등 다양한 플랫폼을 지원하며, 계열사의 가상화폐 지갑을 협상에 사용해 지불이 확인되면 10%의 수수료만 제공하는 전략을 사용한다. 이는, BlackCat(Alphv) 그룹의 Exit scam 에 따라 금전적 손실을 입을 수 있는 상황을 방지하기 위한 전략으로 보인다.

---

[6] RaaS (Ransomware-as-a-Service): 랜섬웨어 그룹들이 계열사나 공격자에게 대가를 받고 랜섬웨어를 제공해주는 형태

[7] CIS (Commonwealth of Independent States): 소련의 해체로 독립한 국가들의 국제기구. 러시아, 몰도바, 벨라루스, 우즈베키스탄, 카자흐스탄 등이 포함됨

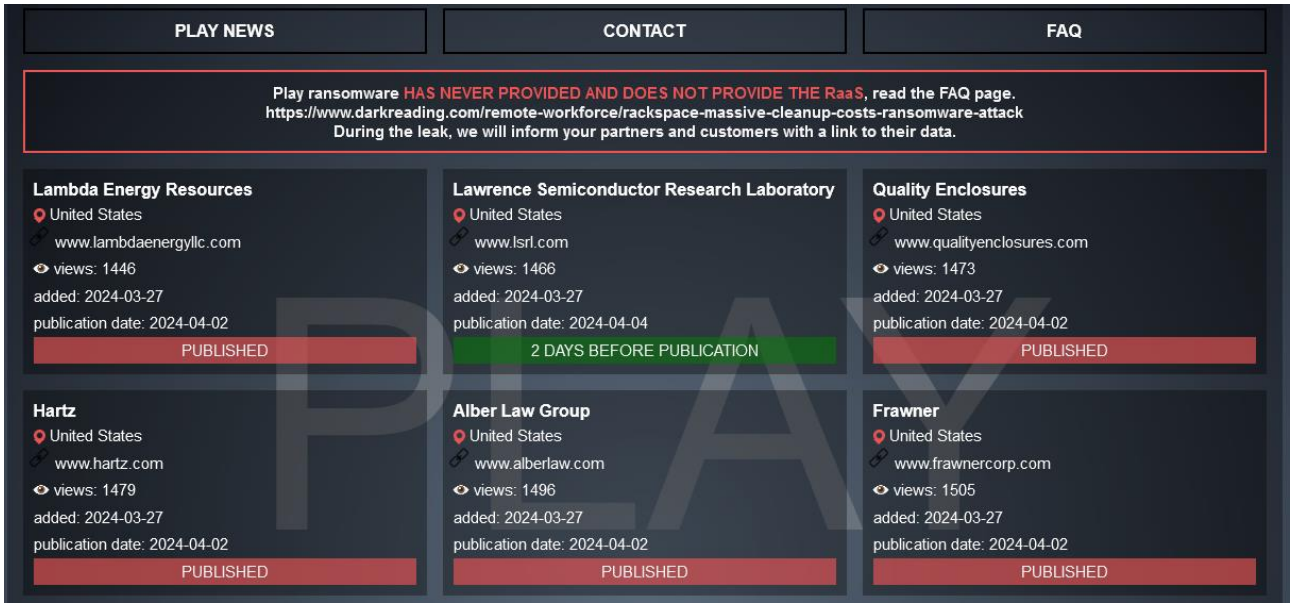
[8] Go 언어: Google 에서 생산성을 높이기 위해 개발한 오픈소스 프로그래밍 언어

[9] ESXi: VM 웨어에서 개발한 호스트 컴퓨터에서 다수의 운영체제를 동시에 실행시킬 수 있는 UNIX 기반 논리적 플랫폼

[10] ARM/MIPS: CPU 아키텍처의 한 종류. ARM 은 주로 Mac 이나 모바일에서 사용되며 MIPS 는 주로 임베디드 시스템에 사용됨

■ 랜섬웨어 집중 포커스

Play 랜섬웨어 개요



출처: Play 랜섬웨어 그룹 데이터 유출 사이트

Play 랜섬웨어 그룹은 2022 년 6 월부터 활동을 시작했으며 현재까지 약 410 여 건의 피해자를 다크웹 데이터 유출 사이트에 게시했다. 특히, Play 그룹은 일정 주기마다 다수의 피해자를 동시에 게시하는 특성을 보이고 있는데, 이번 3 월에만 48 건의 피해자를 게시했다. 다소 활동이 주춤했던 1 월 이후 꾸준히 공격 사례가 증가하고 있어 주의가 필요하다.

최근 다수의 랜섬웨어 공격에서 동일한 전략을 사용한 정황이 확인되며 Play 그룹이 RaaS 를 제공한다는 보고서가 공개됐다. 그러나 Play 그룹은 타 랜섬웨어 그룹들과 달리 RaaS 를 제공하지 않는다고 다크웹 유출 사이트에 밝혔다. Play 그룹의 발표를 100% 확신할 수는 없다. 이들이 RaaS 를 제공하지 않는다고 밝힌 이유는 실제로 서비스를 하고 있지 않거나 수사망을 좁히지 못하도록 하는 전략 등으로 볼 수 있다.

Play 랜섬웨어는 Hive, Nokoyawa 랜섬웨어와 상당히 유사한 전략을 구사한다. ▲권한 상승을 위한 Nekto, PriviCMD, WinPEAS ▲Cobalt Strike 를 통한 공격 도구 다운로드 ▲원격 제어가 가능한 Coroxy, SystemBC 악성코드 사용 ▲원격으로 프로그램을 실행할 수 있게 도와주는 도구인 PsExec 등을 사용해 이미 일부 연관성이 확인된 바 있다. 이외에도 독자적으로 개발한 Grixba 데이터 탈취 도구를 사용하거나 네트워크 상의 액티브 디렉터리 정보를 수집해 주는 도구인 AdFind 를 사용하는 등 차별화된 전략도 펼치고 있다.

Play 그룹은 다크웹 유출 사이트에 유출된 자료를 게시할 때 '?' 문자를 사용해 이름을 숨겨 일정 기간 피해자를 특정하지 못하도록 보호하는 전략도 사용하고 있다. 이 경우 피해 사실을 알리지 않고 조용히 금전적 이득을 취할 수 있다. 다만, 이 전략은 모든 피해자가 아닌 협상의 여지가 있는 기업에 한해서만 사용하는 것으로 보인다.

분석결과, Play 랜섬웨어의 침투방식은 노출된 RDP[11] 서버, 탈취한 계정 사용, Fortinet VPN[12] 서버 취약점(CVE-2018-13379 [13] , CVE-2020-12812 [14]), MS Exchange Server [15] ProxyNotShell 취약점(CVE-2022-41040[16], CVE-2022-41082[17]), ConnectWise 의 ScreenConnect 취약점 CVE-2024-1708, CVE-2024-1709 등을 사용하는 것으로 밝혀졌다. 또한, 침투와 랜섬웨어 공격이 탐지되지 않도록 하는 회피 전략 중 하나인 RMM[18] 도구를 주로 악용하는 것으로 발견됐다. 해당 전략은 Play 뿐 아니라 다수의 랜섬웨어 그룹에서도 사용 중이다.

[11] RDP (Remote Desktop Protocol): 다른 컴퓨터를 원격으로 제어할 수 있도록 해주는 프로토콜

[12] VPN (Virtual Private Network): 인터넷 상에서 개인 정보를 보호하고 지역 제한을 우회하기 위해 사용하는 가상의 보안 네트워크

[13] CVE-2018-13379: FortiOS 시스템 파일을 다운로드할 수 있는 웹 경로 탐색 취약점

[14] CVE-2020-12812: 인증 요소인 FortiToken 입력 메시지가 표시되지 않고 로그인할 수 있는 부적절한 인증 취약점

[15] MS Exchange Server: 마이크로소프트에서 개발한 메시지, 협업 소프트웨어 제품

[16] CVE-2022-41040: 서버 측 요청 위조(SSRF, Server-Side Request Forgery) 공격 취약점

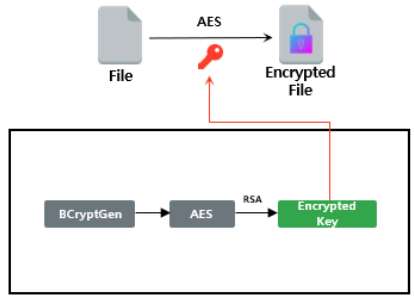
[17] CVE-2022-41082: 원격 코드 실행 취약점

[18] RMM (Remote Monitoring and Management): 원격 모니터링 및 관리를 제공하는 상용 프로그램

Play Ransomeware

암호화 키

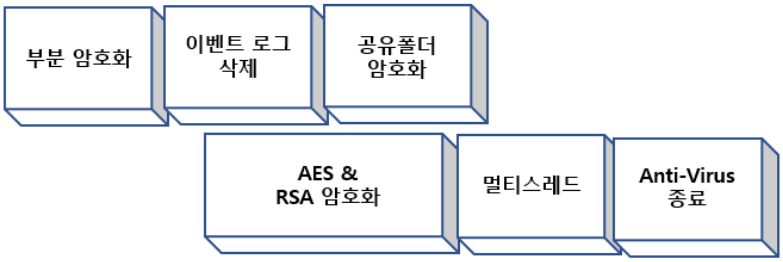
AES 알고리즘으로 파일 암호화를 하고, 해당 키를 RSA로 보호



암호화 방식

256MB 이하 : 전체 암호화
256MB 초과 4GB 이하 : 일정 비율마다 1MB씩 부분 암호화, 총 2MB만 암호화
4GB 초과 16GB 이하 : 일정 비율마다 1MB씩 부분 암호화, 총 3MB만 암호화
16GB 초과 : 일정 비율마다 1MB씩 부분 암호화, 총 4MB만 암호화

특징



랜섬노트

ReadMe.txt

변경 확장자

.PLAY

제작 언어

C/C++

그림 4. Play 랜섬웨어 개요

Play 랜섬웨어 전략

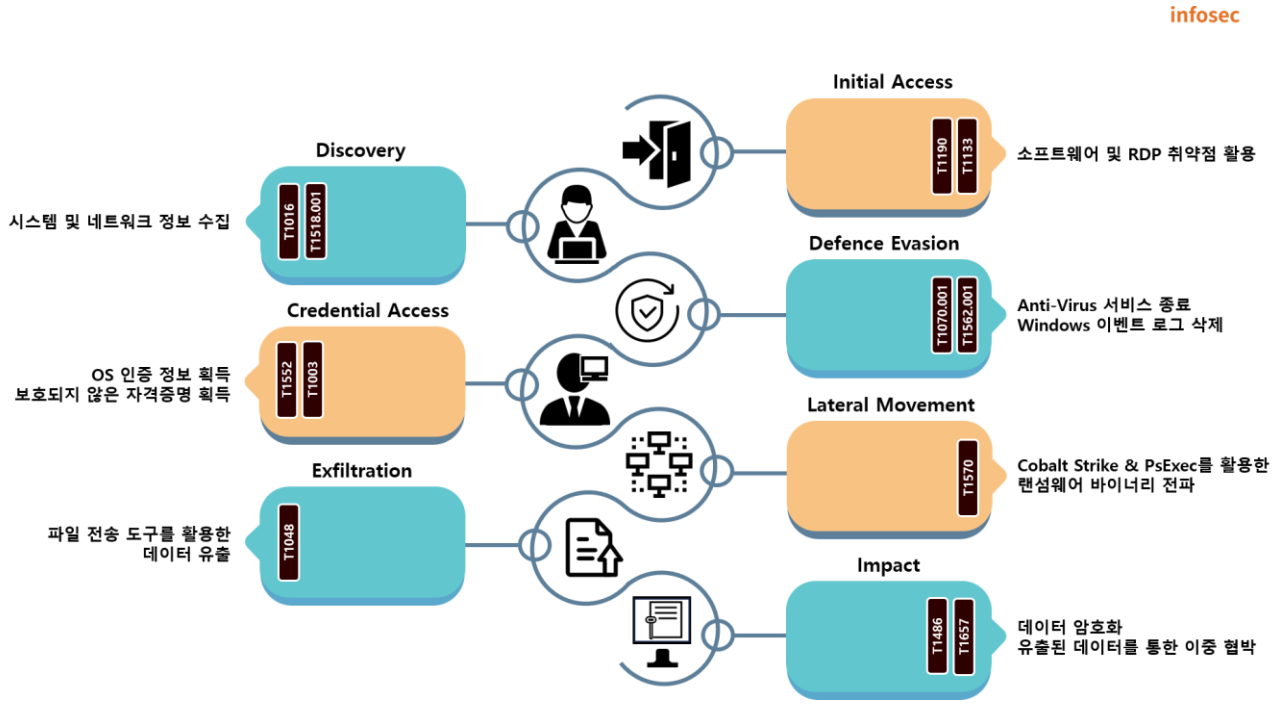


그림 5. Play 랜섬웨어 공격 전략

Play 랜섬웨어는 노출된 원격 데스크톱 프로토콜(RDP)이나 소프트웨어 취약점을 활용해 초기 침투를 시도한다. 포티넷(Fortinet) VPN 서버 취약점, MS Exchange Server ProxyNotShell 취약점, ConnectWise 의 ScreenConnect 취약점 등과 같은 RMM 취약점을 주로 활용했다. 이외에도 탈취한 계정 정보를 활용해 초기 침투를 시도한 이력도 존재한다.

초기 침투에 성공하면 자격 증명 탈취, 시스템 데이터 수집, 내부 전파, 원격 접속, 데이터 유출을 위한 도구들을 다운로드 받아 사용한다. 권한 상승을 위해 ▲Nekto ▲PriviCMD ▲WinPEAS 를 사용하며, 내부 전파를 위해 Cobalt Strike 와 PsExec 를 다운로드 한다. 또한 데이터 유출을 위해 자체 개발한 데이터 탈취 도구 Grixba 를 사용하거나, 압축 도구 WinRAR 과 파일 전송 프로그램 WinSCP 등 다양한 도구를 활용한다.

이처럼 Play 랜섬웨어는 다양한 도구를 활용하기 때문에 랜섬웨어 파일 자체에는 파일 암호화와 랜섬노트 생성 기능만 존재한다. 대신 랜섬웨어 파일의 분석을 어렵게 하기 위해 문자열을 난독화해 저장하고 프로그램 실행 흐름과 전혀 상관없는 가비지 코드를 사용하는 방식을 보이고 있다. 또한 프로그램 실행에 필요한 API 를 동적으로 불러오며, 해시 알고리즘 중 하나인 xxHash32 를 통해서 API 의 주소를 확인하는 방식도 사용한다.

파일 암호화는 대상 PC 의 드라이브뿐만 아니라 공유 폴더도 암호화한다. 파일마다 랜덤하게 생성된 AES 키를 통해서 파일을 암호화하며, 암호화에 사용된 키는 RSA 를 통해서 보호해 파일의 끝에 추가한다. Play 랜섬웨어는 빠른 암호화를 위해서 멀티스레드 방식과 부분 암호화 방식을 사용한다. 파일의 크기가 256MB 이하인 경우 파일 전체를 암호화하지만, 256MB 를 초과하면 파일의 일정 비율마다 1MB 씩만 암호화한다.

그림 6. Play 랜섬웨어 부분 암호화 방식

Play 랜섬웨어는 암호화를 위해서 파일을 1MB 크기의 Chunk 로 구분하며, 크기가 큰 파일의 경우 파일의 전체 Chunk 중에서 극히 일부 Chunk 만 암호화한다.

256MB 초과 4GB 이하의 파일은 첫번째와 마지막 Chunk 만 암호화하며, 4GB 초과 16GB 이하의 파일은 첫번째와 마지막 Chunk 뿐만 아니라 전체 Chunk 중 1/2 지점에 위치한 Chunk 까지 암호화한다. 마지막으로 16GB 보다 큰 파일은 첫번째와 마지막 Chunk 를 암호화하며, 1/3 지점과 2/3 지점에 위치한 Chunk 도 암호화한다. 만약 6,000 개의 Chunk 로 이루어진 파일이라면 첫번째와 마지막 Chunk 를 암호화하며, 1/2 지점인 3,000 번째 Chunk 또한 암호화한다.

Play 랜섬웨어 대응방안

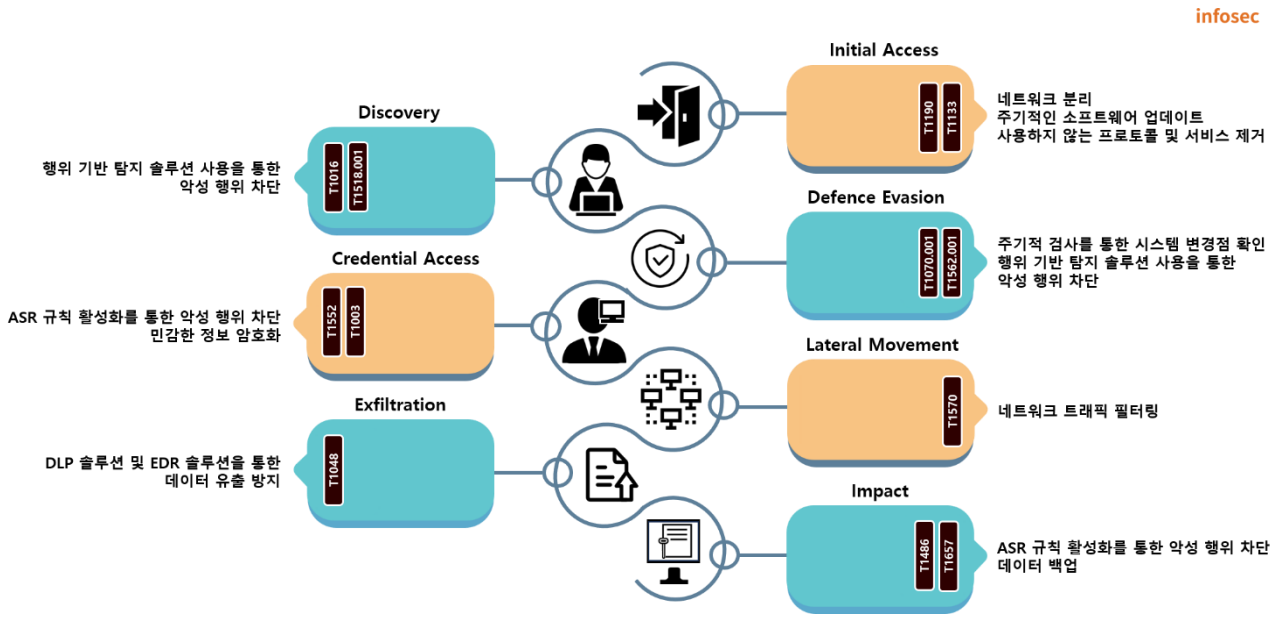


그림 7. Play 랜섬웨어 대응방안

Play 는 주로 소프트웨어의 취약점이나 프로토콜 취약점을 이용해 직접적으로 배포하기 때문에 소프트웨어나 운영체제를 취약하지 않은 버전으로 주기적으로 업데이트 하는 것이 중요하다. 또한, 사용하지 않는 프로토콜과 서비스는 비활성화 하거나 제거해 악용을 방지해야 한다. 이와 함께 네트워크를 세분화하여 분할하거나 가상 사설망을 사용하는 등 네트워크 분리를 통해 피해를 최소화할 수 있다.

다음은 Play 랜섬웨어 그룹에서 악용한 것으로 확인된 취약점이며 영향을 받는 서버 혹은 솔루션을 사용하고 있다면 취약점이 패치된 버전으로 업데이트가 필요하다.

CVE	설명	영향 버전	패치 버전
CVE-2018-13379	Fortinet 의 보안 OS FortiOS 에서 SSL VPN 을 사용하는 경우, 시스템 파일을 다운로드 받을 수 있는 파일 경로 탐색 취약점	5.4.6 ~ 5.4.12 5.6.3 ~ 5.6.7 6.0.0 ~ 6.0.4	5.6.8 이상 6.0.5 이상
CVE-2020-12812	Fortinet 의 보안 OS FortiOS 에서 SSL VPN 을 사용하는 경우, 이중 인증(2FA)이 제대로 수행되지 않는 부적절한 인증 취약점	6.0.9 이하 6.2.0 ~ 6.2.3 6.4.0	6.0.10 이상 6.2.4 이상 6.4.1 이상
CVE-2022-41040	MS Exchange Server 에서 발생하는 서버 측 요청 위조(SSRF) 공격 취약점	업데이트 이전의 Exchange Server 2013, 2016,	KB5019758 업데이트
CVE-2022-41082	MS Exchange Server 에서 발생하는 원격 코드 실행 취약점	업데이트 이전의 Exchange Server 2013, 2016,	KB5019758 업데이트
CVE-2024-1708	원격 데스크톱 솔루션 ScreenConnect 취약점으로, 임의의 파일이나 디렉토리에 접근할 수 있는 경로 탐색 취약점	23.9.7 이하	23.9.8 이상
CVE-2024-1709	원격 데스크톱 솔루션 ScreenConnect 취약점으로, 원격 데스크톱에 시스템 관리자 계정을 생성할 수 있는 인증 우회 취약점	23.9.7 이하	23.9.8 이상

표 1. Play 랜섬웨어가 악용한 소프트웨어 취약점

초기 침투 이후 데이터 수집, 랜섬웨어 배포 등 악성행위를 위해서 Anti-Virus 서비스를 종료시킨다. 또한 OS 인증 정보와 보호되지 않은 각종 자격 증명을 획득하여 공격에 추가적으로 활용한다. 따라서, ASR 규칙 활성화를 통해 악성 행위를 차단하거나 계정 정보와 같이 민감한 정보는 암호화하여 안전하게 보관해야 한다.

코발트 스트라이크(Cobalt Strike)와 PsExec 를 사용해 원격지에 랜섬웨어를 전파하고 실행한다. 따라서 이를 방지하기 위해 네트워크 모니터링 도구를 통해 지속적으로 트래픽 흐름과 액세스를 제어하고, 알 수 없거나 신뢰할 수 없는 출처가 내부 시스템에 접근하는 것을 막는 네트워크 트래픽 필터링을 해야 한다.

데이터 탈취와 파일 암호화에 대해서도 대비가 필요하다. 이는, DLP[19] 솔루션이나 EDR[20] 솔루션을 활용해 데이터 유출을 방지할 수 있다. 데이터 유출 과정에서 정상 도구들을 사용하는 경우도 있어 사전에 인지할 수 있도록 조치가 필요하다.

특히, 대용량 파일일 경우 더욱 주의가 필요하다. 이외에도 파일 복구를 위해 정기적으로 백업을 생성해 관리해야 하며, NAS[21]와 백업 저장소의 데이터를 삭제하는 경우도 존재하므로 별도의 네트워크나 저장소에 데이터를 소산 백업[22]해 관리하는 것을 권장한다. Play 랜섬웨어의 경우, 백업 복사본을 삭제하는 기능이 확인되지 않았기 때문에, 별도의 복원 지점을 생성해 일부 파일을 복구할 수 있다.

[19] DLP (Data Loss Prevention): 데이터의 흐름을 감시하여 중요 정보 유출을 감시/차단하는 데이터 유출 방지 솔루션

[20] EDR (Endpoint Detection and Response): 컴퓨터와 모바일, 서버 등 단말기에서 발생하는 악성 행위를 실시간으로 감지하고 분석 및 대응하여 피해 확산을 막는 솔루션

[21] NAS (Network Attached Storage): 네트워크에 연결되어 여러 사용자가 데이터를 공유하고 접근할 수 있는 저장 장치

[22] 소산 백업: 백업된 데이터를 일정거리 떨어진 장소에 분리 보관하는 방식

Indicator Of Compromise

Play : SHA256

5a0a4e5379e1f0bc9bdd42f5c638c601a0068da4b19b063e5276a01494ae116e
2d01ddc075b48db3ba69b036f9f5977f3607edba5dec6799e4fae7ccd4f1ba75
50d72707eb0a9b7f4ecaa8e0242675e3349b9d67901ac020635ae2ec0eb328e4
64087027f0c727a807c8b6ccf602398adc9d346fe518cbd3b589348702dc39ed

File Name

LkToXG.exe
Thimble pulverization
P137.exe

■ 참고 사이트

• Symantec 공식 홈페이지(https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/play-ransomware-volume-shadow-copy)

• BleepingComputer 공식 홈페이지(https://www.bleepingcomputer.com/news/security/play-ransomware-gang-uses-custom-shadow-volume-copy-data-theft-tool/#google_vignette)

• CISA 보안 권고문(https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a)

• The Register 뉴스레터(https://www.theregister.com/2024/03/08/swiss_government_files_ransomware/)

• SOCRadar 공식 홈페이지(https://socradar.io/dark-web-profile-play-ransomware/)

• Trend Micro 공식 홈페이지(https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-play)

• Malwarebytes 공식 홈페이지(https://www.malwarebytes.com/blog/news/2023/12/fbi-issues-advisory-over-play-ransomware)

• CISA 합동 권고문(https://www.cisa.gov/news-events/alerts/2023/12/18/fbi-cisa-and-asds-acsc-release-advisory-play-ransomware)

• DarkReading 뉴스레터(https://www.darkreading.com/cloud-security/-play-ransomware-group-targeting-msps-worldwide-in-new-campaign)

• MS 보안 대응 센터(https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41082)

• MS 보안 대응 센터 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41040)

• NIST 국가 취약점 데이터베이스(https://nvd.nist.gov/vuln/detail/CVE-2018-13379)

• NIST 국가 취약점 데이터베이스(https://nvd.nist.gov/vuln/detail/CVE-2024-12812)

• NIST 국가 취약점 데이터베이스(https://nvd.nist.gov/vuln/detail/CVE-2024-1708)

• NIST 국가 취약점 데이터베이스(https://nvd.nist.gov/vuln/detail/CVE-2024-1709)