Keep up with Ransomware

양날의 검 BitLocker

■ 개요

최근 랜섬웨어 그룹의 공격이 증가 추세를 보이고 있다. 2023 년 3 월 랜섬웨어 피해 건수는 464 건으로 지난 2 월 260 건에 비해 두 배 가까이 늘어난 것으로 나타났다. 3 월 피해 건수가 증가한 가장 큰 이유로는 Clop 그룹에 의한 공격 사례가 늘어난 영향으로 분석된다. Clop 그룹은 1 월 이후로 활동을 보이지 않다가, 2 월 GoAnywhere MFT(Managed File Transfer)[1] 취약점(CVE-2023-0669)을 이용하여 공격했다고 밝힌 뒤 3 월 공격 중 일부인 104 건을 게시했다. 지난 2 월 가장 많은 피해를 발생시킨 LockBit 그룹 역시 전월 대비 공격 사례가 다소 감소했으나 여전히 많은 수의 피해자를 발생시키고 있어 위협적인 모습을 보이고 있다.

랜섬웨어 그룹들이 사용하는 공격 전략 역시 다양화, 고도화되고 있다.

Bloody 랜섬웨어 그룹은 유출된 LockBit 소스코드를 사용한 랜섬웨어로 초기 침투를 돕는 브로커인 IAB(Initial Access Broker)를 구하고 있으며, Medusa 그룹은 미국의 공립학교와 가구 회사, 파키스탄의 우주 기술 연구소 등을 공격하여 탈취한 데이터를 공개하는 영상을 제작한 뒤 다크웹 유출 사이트에 게시했다.

또한 전 세계적으로 피해를 입히고 있는 BianLian 그룹은 피해자의 파일을 암호화하는 것에 그치지 않고, 데이터를 추출하여 강탈하는 방향으로 공격 전략을 다양화하고 있다. 최근 BianLian 그룹은 30 개 피해 조직에서 강탈한 정보를 다크웹 유출 사이트에 게시했다. 이 밖에도 과거 Babuk 그룹과 1 월 이후로 활동이 없다가 3 월에 재개하여 3 건의 희생자를 게시한 Karakurt 등 일부 랜섬웨어 그룹에서도 암호화를 하지 않고 데이터를 탈취하여 몸값을 요구하는 전략을 사용하고 있는 것으로 확인됐다.

이번 달 새로운 랜섬웨어 그룹으로는 DarkPower와 Abyss, MoneyMessage가 발견됐다. DarkPower 그룹은 유통, 교육, 건설 등 다양한 산업군을 공격하여 3 월 한 달간 총 10 건의 공격 사례를 게시했으며, Abyss 그룹은 제조, 의료 업계 등 7 건, MoneyMessage 그룹은 운송 업계 2 건의 공격 사례를 다크웹 유출 사이트에 게시하며 활동하고 있다. 이들은 신규 랜섬웨어 그룹임에도 불구하고 다수의 피해 사례를 남기고 있어 경각심을 가지고 지켜볼 필요가 있다.

[1] 소프트웨어로 안전하게 파일 전송 및 데이터 교환을 수행하는데 사용

한편 국내에서는 Mallox(Fargo), GlobeImposter, Nevada, LockBit 2.0 및 3.0, BitLocker 랜섬웨어 등이 확산되고 있다. Mallox 와 GlobeImposter 는 취약한 MS-SQL 서버를 타깃으로 하는 랜섬웨어이며, GlobeImposter 는 MedusaLocker 그룹이 공격에 이용하는 랜섬웨어로 RDP(Remote Desktop Protocol)[2]를 통해 확산되고 있다.

LockBit 2.0 은 이메일을 통해 첨부파일을 실행하도록 유도하는 공격 방법을 사용하고 있으며, 중소기업을 표적으로 한 공격이 지속적으로 발견되고 있다. 특히 최근 LockBit 2.0 은 실행 파일이 아닌 것처럼 이력서로 위장하여 교묘하게 유포되고 있는데, 실행 파일을 한글 이력서 문서처럼 보이기 위해 한글 프로그램의 아이콘을 사용하고 있으며 파일명과 확장자 사이에 많은 공백을 두고 있어 피해를 막기 위한 각별한 주의가 필요하다.

LockBit 3.0 은 서비스형 랜섬웨어로 주로 국내에서는 북한과 연관이 있다고 알려진 VenusLocker 그룹이 공격에 사용하는 랜섬웨어다. 이들은 3 월 29 일, 자신들의 다크웹 유출 사이트에 국세청을 해킹했다고 주장하며 4 월 1 일에 정보를 공개하겠다는 글을 게시한 바 있다. 이후 유출 데이터는 현재까지 공개되지 않고 있으며, 유출 사이트에 올라온 후 평균 1~2 주의 공개 예정 시간과 다르게 빠르게 공개를 예고한 점과 데이터 공개 시점이 4 월 1 일인 점 등의 근거로 만우절 장난으로 올렸을 가능성도 제기되고 있다. 하지만 데이터를 공개하지 않고 협상을 진행할 가능성과 협상이 제대로 성사되지 못했을 때 데이터를 공개할 가능성 등 여러 가지 조심스러운 추측이 나오고 있다.

BitLocker 랜섬웨어는 Windows 에서 제공하는 드라이브 암호화 기술인 BitLocker 를 이용하여 드라이브를 암호화시킨 후 금전을 갈취한다. 국내 의료기관 및 기업, 각종 중요 인프라 등에서 BitLocker 랜섬웨어로 인한 피해 사례가 지속적으로 확인되고 있다. BitLocker 는 MS Exchange[3] 서버의 취약점(CVE-2021-34473 [4], CVE-2021-34523 [5], CVE-2021-31207 [6])을 이용하여 침투하므로 해당 취약점이 패치 된 버전의 소프트웨어를 사용해 예방할 것을 권장한다.

[2] 원격으로 다른 컴퓨터에 연결하기 위해 Microsoft 에서 제공하는 프로토콜

[3] Microsoft 에서 개발한 메시징, 협업 소프트웨어 제품

[4] 원격 코드 실행 취약점으로 공격자가 인증되지 않은 원격 코드를 실행하여 Exchange Server 에 액세스 할 수 있다

[5] 권한 상승 취약점으로 원격 코드 실행 권한을 획득하여 시스템 권한 상승을 수행할 수 있다

[6] 보안 기능 우회 취약점으로 인증되지 않은 원격 코드를 실행하여 DNS 서버의 보안 기능을 우회할 수 있다

하지만 안타깝게도 지난달 대규모 랜섬웨어 공격 사례가 또다시 발생했다. 취약한 ESXi[7] 서버를 대상으로 공격이 이뤄졌으며, 이미 2 년전 발견된 CVE-2021-21974[8] 취약점을 사용한 것으로 분석됐다. 해당 취약점은 이미 패치가 완료되었으나 패치 되지 않은 취약한 서버를 검색해 엑시악스(ESXiArgs)[9]로 불리는 랜섬웨어(쉘 스크립트와 ELF 파일)를 통해 암호화를 시도했다.

CISA[10]는 대규모 랜섬웨어 공격이 발생함에 따라 피해를 경감시키기 위해 암호화 방식의 허점을 통해 감염된 ESXi 가상 머신 환경을 복구할 수 있는 툴을 배포했다. 하지만 공격자가 이를 인지하고 암호화 방식을 바꿔 다시 공격을 시도하고 있으며, 지금까지도 취약한 서버를 대상으로 랜섬웨어 공격을 이어가고 있다.

또한 리눅스 및 ESXi 서버를 대상으로 공격을 시도하는 또 다른 네바다(Nevada) 랜섬웨어도 발견됐다. 해당 랜섬웨어 역시 CVE-2021-21974 취약점을 사용하고 있으며, ESXiArgs 랜섬웨어와 마찬가지로 대규모 공격을 시도하고 있는 것으로 확인됐다. 이처럼 취약한 ESXi 서버의 대규모 감염 사례가 지속적으로 확인되고 있어 각별한 주의가 필요하다.

이러한 대규모 랜섬웨어 공격과 더불어 다크웹을 통한 이중 협박 전략을 사용하는 신규 랜섬웨어 그룹인 DarkBit, Medusa 가 발견되고 있다. 또한 V IS VENDETTA 그룹의 활동 정황도 다크웹에서 발견되고 있다. 기존 Cuba 랜섬웨어 그룹의 유출 사이트 URL 과 동일한 URL 을 포함하고 있으며, 'test.'가 추가된 URL 을 사용하여 Cuba 랜섬웨어 그룹의 서브 도메인으로 확인된다.

마지막으로 국내 제조 관련 중소기업 중 한 곳이 Mallox 랜섬웨어에 감염되어 유출된 데이터가 다크웹에 게시된 사실이 확인됐다. Mallox 랜섬웨어는 취약한 MS-SQL 을 대상으로 공격을 시도하는 랜섬웨어로 파일 암호화 및 데이터 유출을 통해 이중 협박 전략을 구사한다. MS-SQL 계정 관련 공격을 통해 서버에 접속 후 추가로 설치한 원격 프로그램으로 랜섬웨어 공격을 시도하거나, SQL 을 이용하여 스크립트 혹은 파워쉘 명령어를 통해 랜섬웨어 공격을 수행한다. 데이터베이스 서버는 감염될 경우 기업에서 제공하는 대부분의 서비스를 정상적으로 운용할 수 없어 암호화된 파일을 최우선으로 복호화를 해야 하는 중요한 시스템이다. 취약한 데이터베이스는 공격자 입장에서 손쉽게 침투할 수 있는 경로 중 하나로 MS-SQL 을 사용하는 국내 기업의 적절한 보안 조치가 필요하다.

---

[7] VMware 에서 개발한 가상화 OS

[8] VMware ESXi OpenSLP 에서 힙 오버플로우(heap overflow)로 인해 발생하는 원격코드실행 취약점

[9] 일종의 랜섬웨어로, 프랑스의 국가 침해 대응 센터(CERT)가 2 월 3 일 먼저 발견해 경고. VMWare 의 ESXi 라는 하이퍼바이저들을 노리는 랜섬웨어임을 발표

[10] CISA(Cybersecurity and Infrastructure Security Agency, 미국 사이버 보안 전담 기관)

■ 랜섬웨어 뉴스

LockBit 3.0 랜섬웨어 그룹, 국세청 홈페이지 공격 주장

- LockBit 3.0 이 국세청을 공격했다고 주장
- 이미지, 관련내용, 샘플 등을 게시하지 않은 상태
- 만우절 장난일 가능성 및 협상 진행 중 등 여러 가능성 존재

Breached forum, FBI 에게서 안전하지 않다는 우려로 사이트 폐쇄

- 악명 높은 포럼 중 하나인 Breached forum 관리자는 FBI 를 비롯한 법 집행 기관이 사이트 서버에 액세스 가능하다는 우려를 밝히고 사이트를 폐쇄
- 창립자인 Pompompurin 이 FBI 에 의해 체포되었다는 소식 이후로 관리자가 사이트를 폐쇄
- Telegram 채널은 당분간 운영되며, 잠재적으로 새로운 사이트를 구축하는데 도움을 줄 것이라고 언급

LockBit 랜섬웨어 그룹, SpaceX 의 관련 기술 기업 데이터 탈취 주장

- LockBit 랜섬웨어 그룹이 SpaceX 관련 기술 기업의 데이터를 탈취했다고 주장

GlobeImposter 랜섬웨어, RDP 통해 재확산 중, MedusaLocker 조직에서 유포

- RDP 활성화된 시스템 스캐닝 후 무차별 대입 또는 사전 공격 수행하여 침투
- GlobeImposter 랜섬노트에 기재된 이메일 주소와 onion 주소가 MedusaLocker 그룹이 사용하는 목록에 포함

Clop 랜섬웨어 그룹, GoAnywhere 제로데이 피해자 갈취 시작

- GoAnywhere MFT 의 제로데이 취약점을 사용하여 데이터를 탈취
- 데이터를 탈취한 기업에게 금전을 갈취

Microsoft SmartScreen 제로데이 취약점, Magniber 랜섬웨어 배포에 악용

- 1 월부터 SmartScreen 우회 기술을 악용할 수 있는 CVE-2023-24880 취약점을 이용하여 악성 파일 유포
- 해당 취약점은 CVE-2022-44698 의 새로운 변종

새로운 DarkPower 랜섬웨어, 첫 달에 10 명의 피해자 주장

- DarkPower 랜섬웨어가 새롭게 등장
- 전 세계를 대상으로 10 건의 피해자 유발

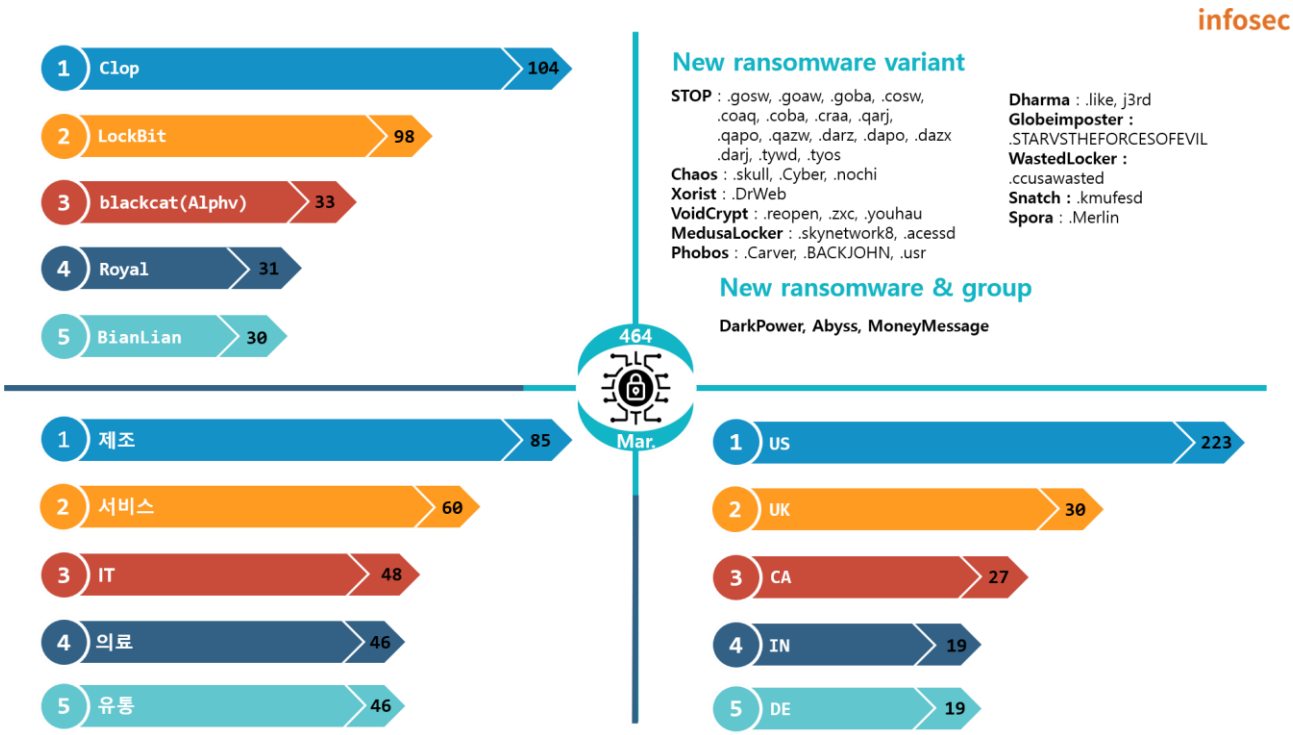
Medusa 랜섬웨어 그룹, 미니애폴리스 학교에서 유출된 데이터를 영상으로 게시

- Medusa 그룹은 미니애폴리스 학교에서 탈취한 데이터를 게시하겠다고 협박
- 탈취한 데이터에 접근하는 영상을 제작하여 공개
- 편집 방식을 자극적으로 하여 다크웹 외부로 공개되었을 경우 악영향을 미칠 수 있음

BianLian 랜섬웨어 그룹, 데이터 갈취로 공격 노선 변경

- 데이터를 암호화하는 랜섬웨어를 유포하던 BianLian 그룹이 암호화를 하지 않는 랜섬웨어 배포
- 데이터를 탈취하여 금전 갈취에 사용하는 것으로 공격 노선 변경

■ 랜섬웨어 위협



새로운 위협

BlackCat(Alphv) 랜섬웨어의 변종이 발견됐다. 기존 BlackCat 랜섬웨어 버전과 다른 점은 액세스 토큰을 대신하는 매개변수가 있어야 랜섬웨어 실행이 가능하다는 점과 복잡해진 난독화를 적용했다는 점, Config 데이터가 JSON 형식이 아니라는 점이다. 또한 해당 버전 업데이트 이후 다형성을 적용한 변종을 생성하여 유포하고 있는데, 이는 탐지를 회피하기 위한 전략의 일환으로 보인다. 이외에도 Stop 랜섬웨어의 변종 역시 다수 확인되고 있다.

*출처: 각 그룹별 사이트 이미지

3 월에도 신규 랜섬웨어 그룹의 출현은 지속적으로 발견되고 있다. DarkPower, Abyss, MoneyMessage 로 불리는 3 개의 그룹이 확인됐다. DarkPower 랜섬웨어 그룹은 미국, 프랑스, 이스라엘 등 여러 국가의 조직과 기업을 대상으로 공격 중이며, 현재까지 10 건의 희생자를 게시했다. 특히 DarkPower 은 새로 발견된 3 개의 그룹 중 가장 많은 피해를 입히고 있는 것으로 확인되고 있다.

이들의 주 공격 방식은 크로스 플랫폼[11]을 지원하는 Nim[12]언어로 작성되었으며 랜섬노트가 pdf 로 되어있다는 특징을 가지고 있다. Abyss는 건설, 화학, 유통업 등에서 7건의 희생자를 유출 사이트에 게시한 바 있으며, MoneyMessage 그룹은 방글라데시와 하와이의 기업을 공격해 유출된 자료의 일부를 캡처하여 다크웹에 게시하였다.

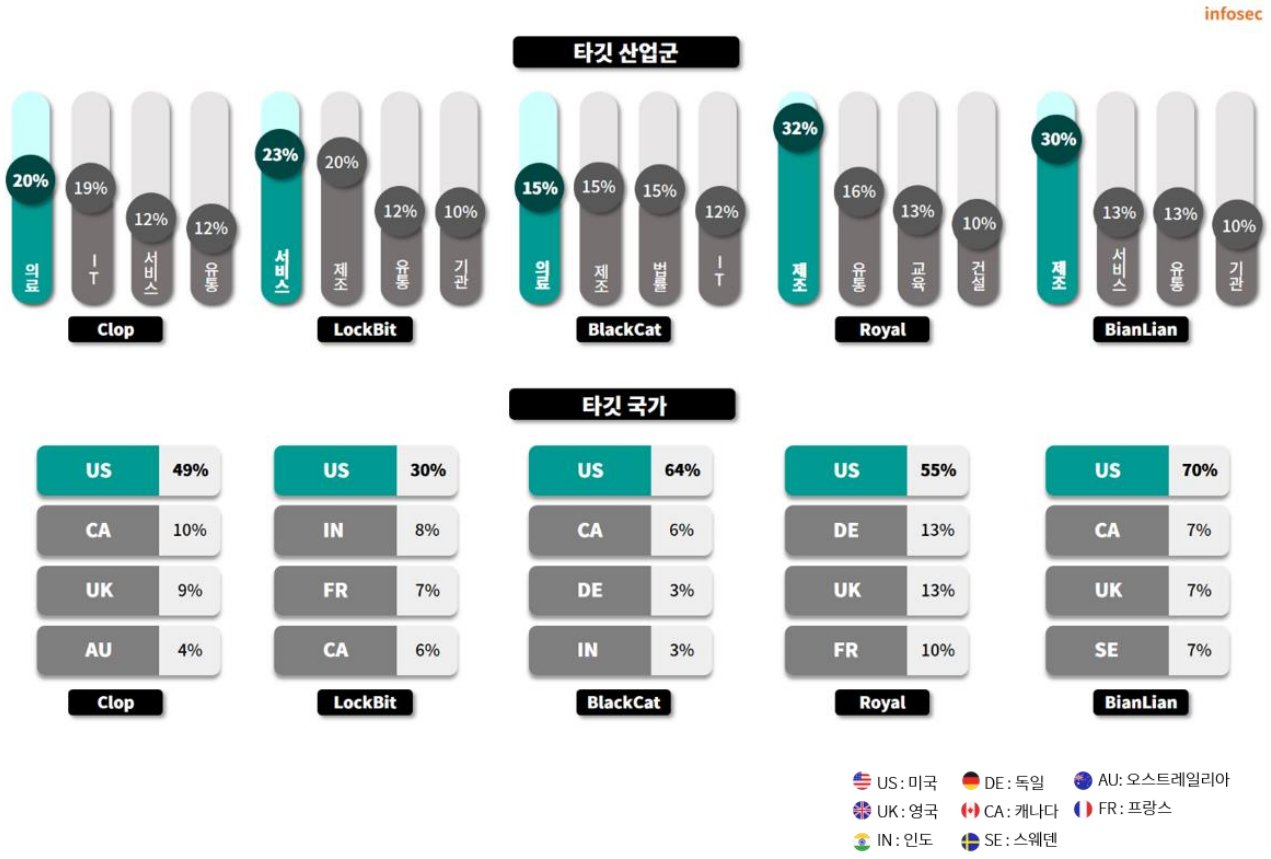
이처럼 랜섬웨어는 갈수록 분석하기 어려운 방향으로 진화하고 있으며, 다양한 국가와 기업을 대상으로 공격을 수행한 뒤 유출 사이트에 탈취한 정보 일부를 게시하여 협박을 시도하고 있다. 만약 금전을 지불하지 않을 경우 탈취한 정보를 공개하는 전략을 사용한다. 이러한 피해를 막기 위해서는 랜섬웨어로 인한 감염을 예방하는 것이 가장 중요하므로 조직에서는 수상한 메일이나 출처를 알 수 없는 파일을 조심해야 한다.

[11] 여러 종류의 환경에서 동작할 수 있는 언어

[12] 오픈 소스로 개발된 언어이며, 메모리 안정성과 비동기 및 병렬 프로그래밍을 지원하여 속도가 빠르다. 메모리 관리, 제네릭, 동시성 처리 등 여러 기능을 제공하기 때문에 C 언어에 비해 분석하기 어렵다는 특징이 있어 악성코드 제작에 이용하기도 한다

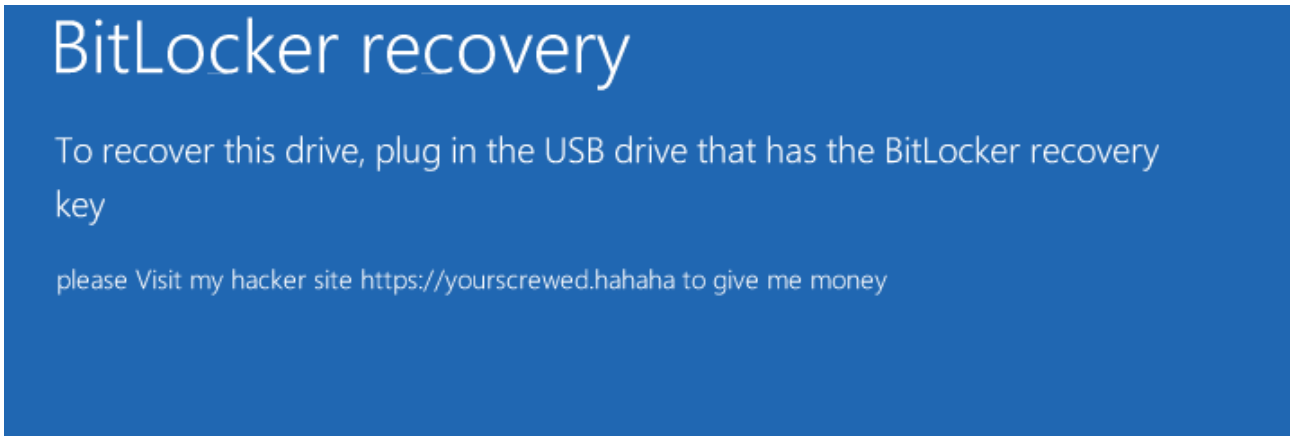
Top5 랜섬웨어

지난 3 월 Top5 랜섬웨어를 살펴보면 대부분 제조와 서비스 산업을 표적으로 공격이 이루어지고 있다. 전월 대비 피해 건수 급증한 원인으로는 Clop 랜섬웨어의 GoAnywhere MFT 취약점을 이용한 공격 사례 게시를 꼽을 수 있다. Clop 랜섬웨어 그룹은 1 월 이후로 활동 정황이 없다가, 2 월에 GoAnywhere MFT 의 취약점을 이용해 공격을 수행했다고 밝히며 피해자의 데이터를 유출 사이트에 게시했다. 실제 다수의 피해 사례가 확인되었고 다양한 산업 군에 걸친 공격을 수행하고 있다는 것이 밝혀졌다. BlackCat 역시 다양한 산업군을 대상으로 공격을 시도하고 있으며, Royal 과 BianLian 은 제조업에 공격을 집중하는 것으로 분석된다. 랜섬웨어의 타깃 국가로는 전 세계에서 미국이 가장 많이 지목되고 있다.



■ 랜섬웨어 집중 포커스

BitLocker 를 악용한 랜섬웨어



BitLocker 는 AES[13] 알고리즘과 디퓨저[14] 알고리즘을 사용하는 암호화 기능을 가지고 있다. 드라이브 암호화 기능은 원칙적으로는 허가 받지 않은 사람이 드라이브에 접근하는 것을 막아 데이터를 보호하는데 사용하는 기술이지만, BitLocker 를 악용한 랜섬웨어는 사용자의 드라이버를 암호화하여 금전적인 이득을 취하려는 공격이다. 특히 암호화 알고리즘을 직접 적용한 일반 랜섬웨어와 달리 Windows 시스템에 기본적으로 내장되어 있는 기능인 BitLocker 를 악용하여 암호화를 진행한다.

최근 BitLocker 를 악용한 랜섬웨어 공격으로 인해 국내 중소 규모의 의료기관과 기타 중요 인프라 조직에서 다수의 피해가 발생했다. 공격자들은 중소 의료기관에서 주로 사용하는 오픈소스 메신저 'X-Popup'으로 위장한 악성코드를 이용해 드라이브 암호화에 필요한 파일을 설치하고, 데이터 탈취 및 드라이브를 암호화했다. BitLocker 으로 인한 피해는 지금까지도 여러 국내 기업에서 지속적으로 발생하고 있어 주의가 필요하다.

BitLocker 를 악용한 랜섬웨어는 MS Exchange[15] 서버의 취약점(CVE-2021-34473, CVE-2021-34523, CVE-2021-31207)을 통해 초기 침투를 진행하므로 감염을 예방하기 위해서는 해당 취약점이 패치된 최신 버전으로의 업데이트가 필요하다. 특히 BitLocker 를 악용한 랜섬웨어는 감염되었을 경우 시스템에 큰 손실을 입힐 수 있으므로 조기 대처와 예방이 중요하다. 따라서 사용자들은 보안 관련 정보 및 최신 보안 솔루션에 대한 지속적인 업데이트를 유지하여 대응해야 한다.

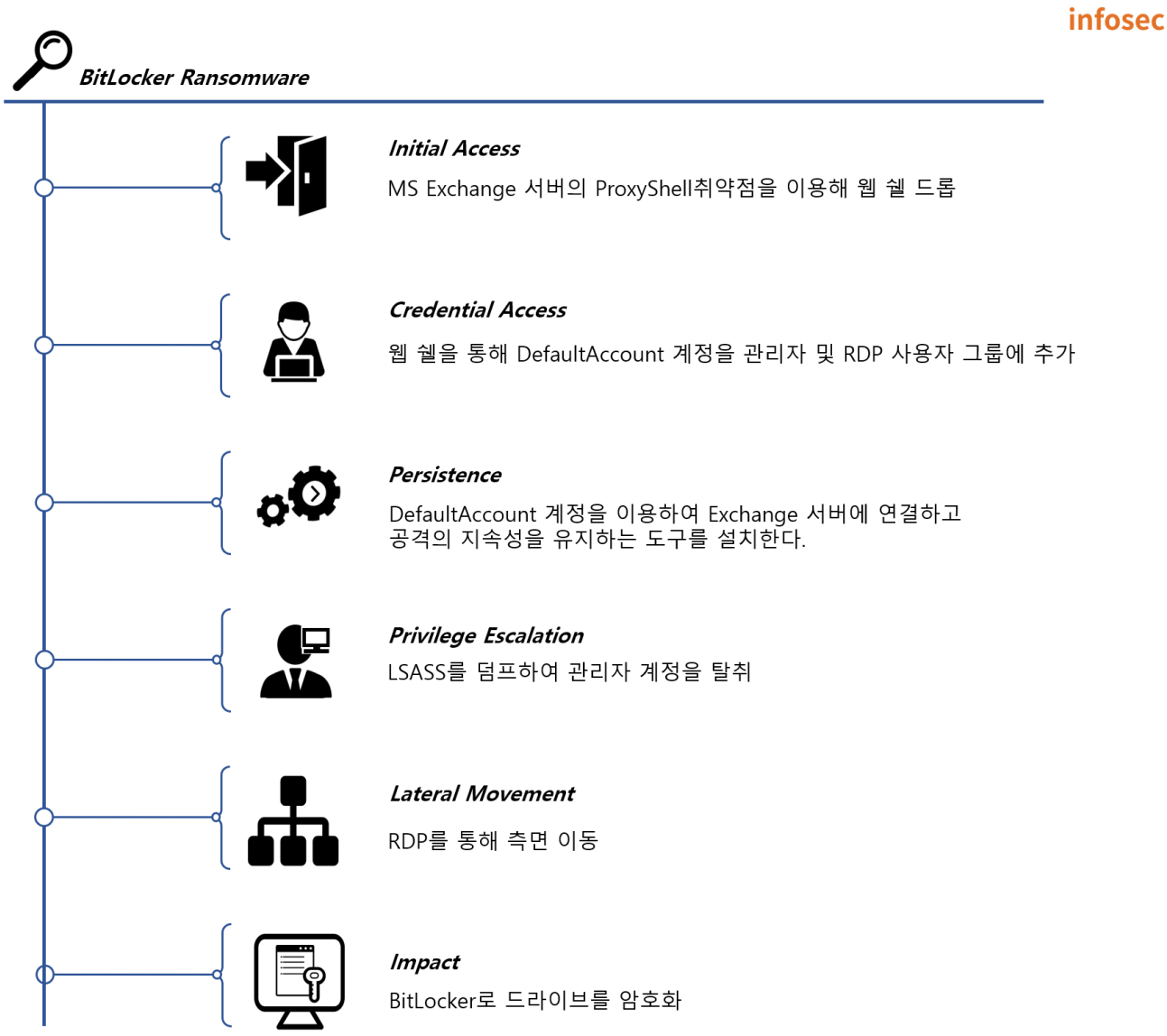
---

[13] 대칭키 암호화 알고리즘의 종류

[14] 암호문에 새로운 난수 값을 추가하는 알고리즘

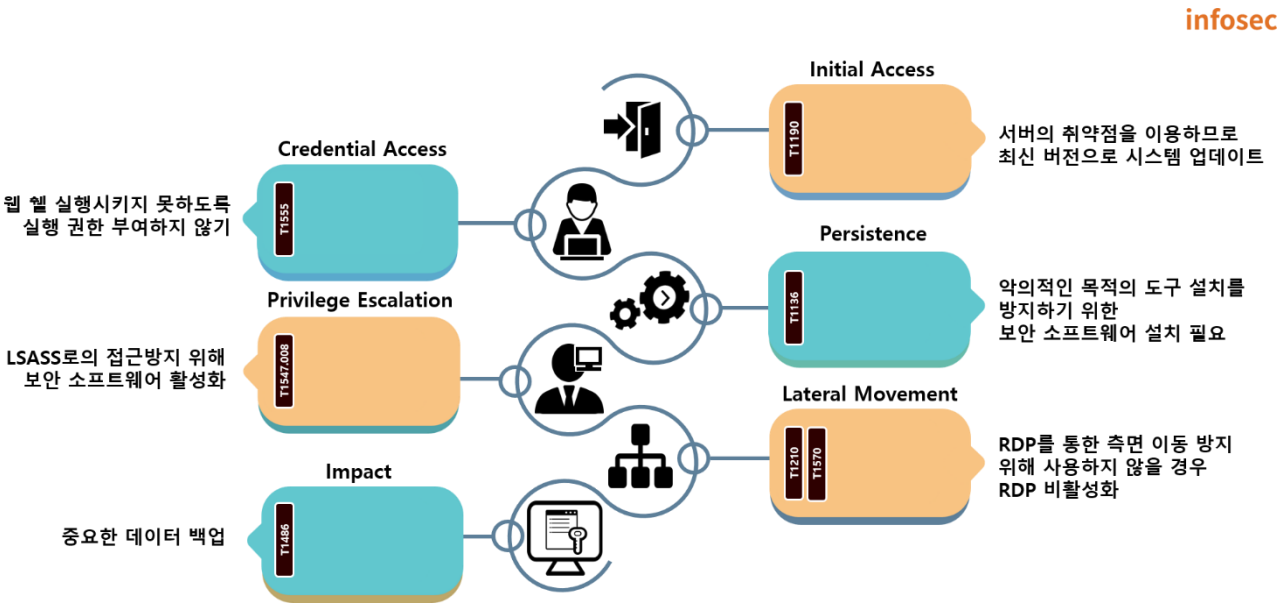
[15] 마이크로소프트 사에서 개발한 메시징, 협업 소프트웨어 제품

BitLocker를 악용한 랜섬웨어 감염 시나리오 1



- 초기 침투는 MS Exchange 서버의 ProxyShell 취약점을 이용하여 초기 액세스 권한을 얻어 웹 쉘을 드롭하여 이루어진다.
- 드롭한 웹 쉘을 이용하여 시스템에서 사용하는 계정인 DefaultAccount 계정을 관리자 그룹과 RDP 사용자 그룹에 추가하는 파워쉘 명령을 실행한다.
- 추가한 DefaultAccount 계정을 이용해서 Exchange 서버에 연결하고 공격의 지속성을 유지하는 배치파일을 실행시켜 악성 행위의 지속성을 유지시킨다.
- 그 후 프로세스 모니터링 도구로 LSASS(Local Security Authority Subsystem Service)를 덤프하여 관리자 계정에 대한 NTML(NT LAN Manager) 해시를 탈취하고 해독한다.
- 이렇게 탈취한 관리자 계정을 이용해서 RDP를 통해 측면으로 이동하여 BitLocker를 실행시켜 피해 시스템의 드라이브를 암호화시킨다.

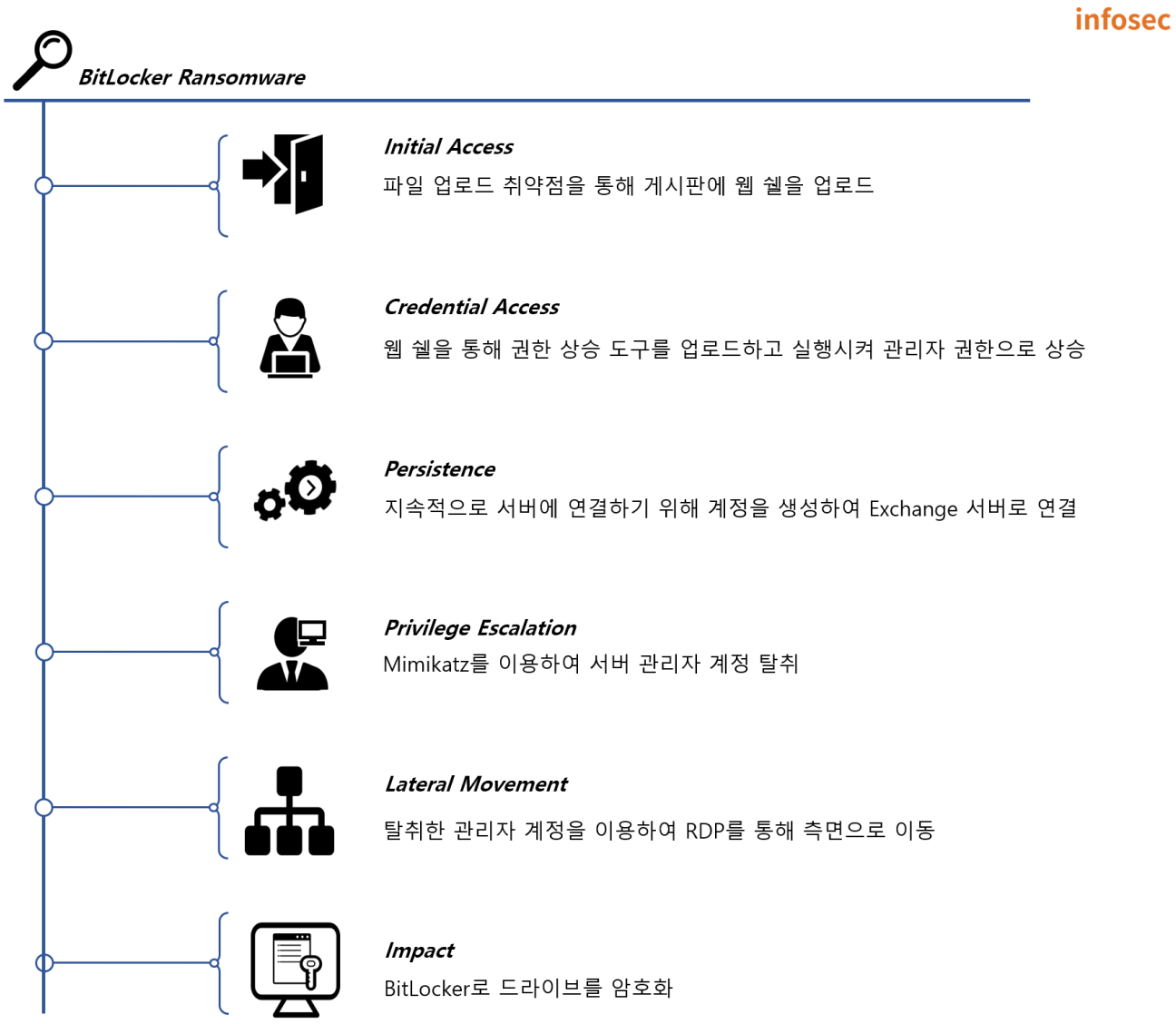
시나리오 1 - 단계별 대응방안



- 서버의 취약점을 이용하므로 해당 취약점이 패치된 버전으로 시스템 업데이트를 진행해야 한다. Microsoft의 카탈로그 페이지(https://www.catalog.update.microsoft.com)에 접속하여 사용 중인 버전을 검색하면 업데이트 목록을 확인할 수 있으며, 취약점이 패치 된 버전을 다운로드해 적용시켜야 한다.
- 업로드한 웹 쉘을 실행시킬 수 없게 업로드 경로에 실행 권한을 부여하지 않아야 하며, 파일 확장자 필터링 등의 조치가 필요하다.
- 또한 악의적인 목적의 도구 설치를 방지하기 위하여 보안 소프트웨어 설치가 필요하고 LSASS 덤프를 예방하기 위하여 LSASS로의 접근을 막아주는 ASR(Attack Surface Reduction)[16] 규칙 혹은 해당 접근을 차단할 수 있는 행위 기반 규칙이 적용된 보안 소프트웨어를 활성화하는 것을 권장한다.
- 마지막으로 파일이 암호화되었을 경우를 대비해 중요한 데이터는 보안 백업을 통해 데이터를 보호해야 한다. 백업 데이터 보호를 위해 원본과 다른 형식으로 백업 데이터를 보호하고 데이터 사본 간 격리, 백업 데이터 암호화 등을 갖춰야 하며, 이러한 백업 파일은 허용된 사용자만 접근할 수 있도록 제한해야 한다.

[16] 악성코드의 공격 경로를 차단하는 기술

BitLocker를 악용한 랜섬웨어 감염 시나리오 2



- 부적절한 확장자 검증 등과 같은 파일 업로드 취약점을 통해 게시판에 웹 쉘을 업로드한다.
- 이렇게 업로드 된 웹 쉘을 통해 Sweet Potato, Juicy Potato 와 같은 권한 상승 도구를 업로드하고 실행하여 관리자 권한으로 상승한다.
- 지속적으로 서버에 연결하기 위해 계정을 생성하고 해당 계정으로 Exchange 서버에 연결하는 작업을 한다.
- Mimikatz[17]를 이용하여 서버 관리자 계정의 NTML 해시를 탈취하여 해독한 다음 해당 계정을 이용해 RDP 로 측면 이동을 진행하여 이동한 시스템에서 BitLocker 를 실행시켜 드라이브를 암호화한다.

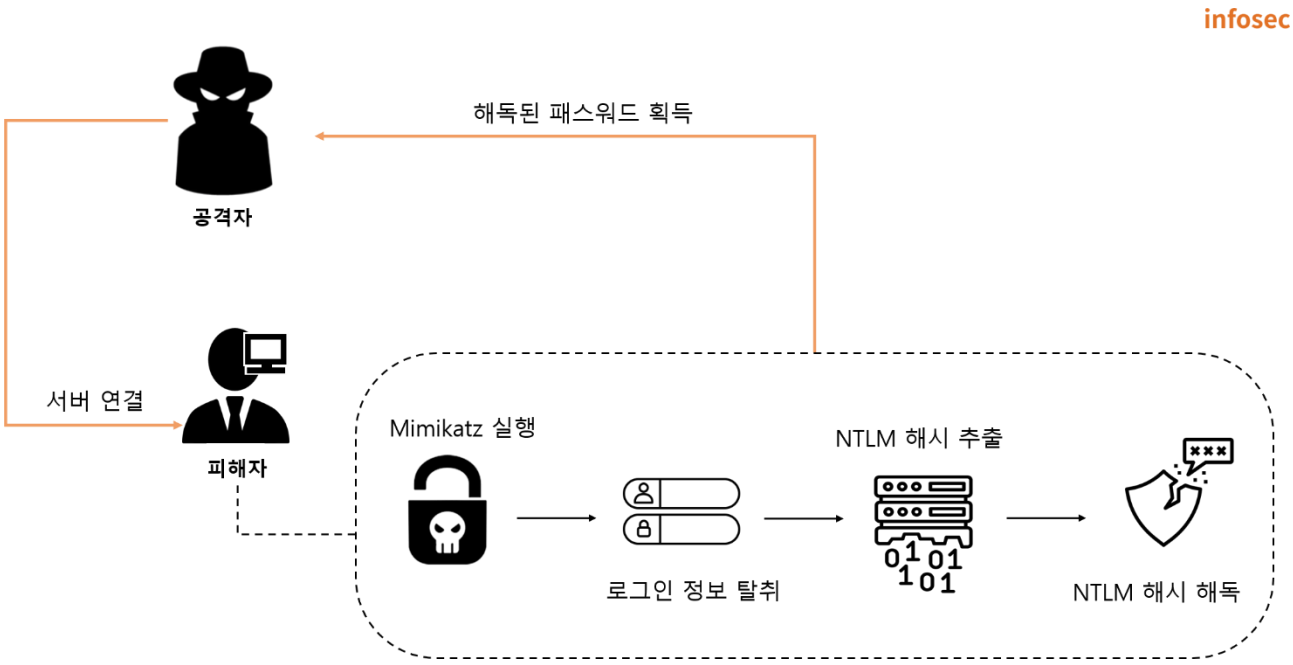
[17] Windows 인증 정보를 탈취하고 관리자 권한을 획득하는데 사용하는 도구

시나리오 2 – Mimikatz 살펴보기

Mimikatz 는 Windows 시스템에서 자격증명(NTLM 해시, Kerberos[18] 티켓 등) 정보를 수집하는 도구이다. Mimikatz 는 로컬 시스템 계정 정보와 암호 해시를 추출하는 lsadump, 로그인 정보와 Kerberos 티켓을 탈취하는 sekurlsa, 프로세스 토큰을 복제하거나 다른 계정으로 변경하는 token 등 다양한 기능을 제공한다. 악성코드에서 많이 사용하는 기능은 lsadump, sekurlsa, Kerberos 기능 등이 있다.

lsadump	로그인 정보를 암호화된 형태로 저장하는 LSASS 의 메모리 내용을 복제한다. 악성코드는 해당 기능을 통해 로그인 정보를 탈취한다.
sekurlsa	암호화되지 않은 형태의 사용자 인증 정보를 탈취한다. 악성코드는 해당 기능을 통해 현재 로그인한 사용자의 개인정보를 탈취한다.
Kerberos	악성코드는 해당 기능을 통해 Kerberos 프로토콜의 인증 정보를 탈취한다.

시나리오 2 에서 사용한 Mimikatz 의 기능은 NTML 해시 탈취 기능이다. 해당 시나리오에서 서버 관리자 계정의 NTML 해시를 탈취한 과정은 다음과 같다.



[18] 컴퓨터 네트워크에서 사용자가 신원을 확인하고 인증을 받을 때 보안을 유지하기 위한 프로토콜

Step 1) 로그인 정보 탈취

Mimikatz 를 실행하여 “sekurlsa::logonpasswords” 명령을 입력하여 현재 시스템에 로그인 되어 있는 사용자의 로그인 정보를 탈취한다.

Step 2) NTLM 해시 추출

위에서 실행한 명령의 결과로 출력된 내용 중 관리자 계정에 해당하는 NTLM 해시를 가져온다.

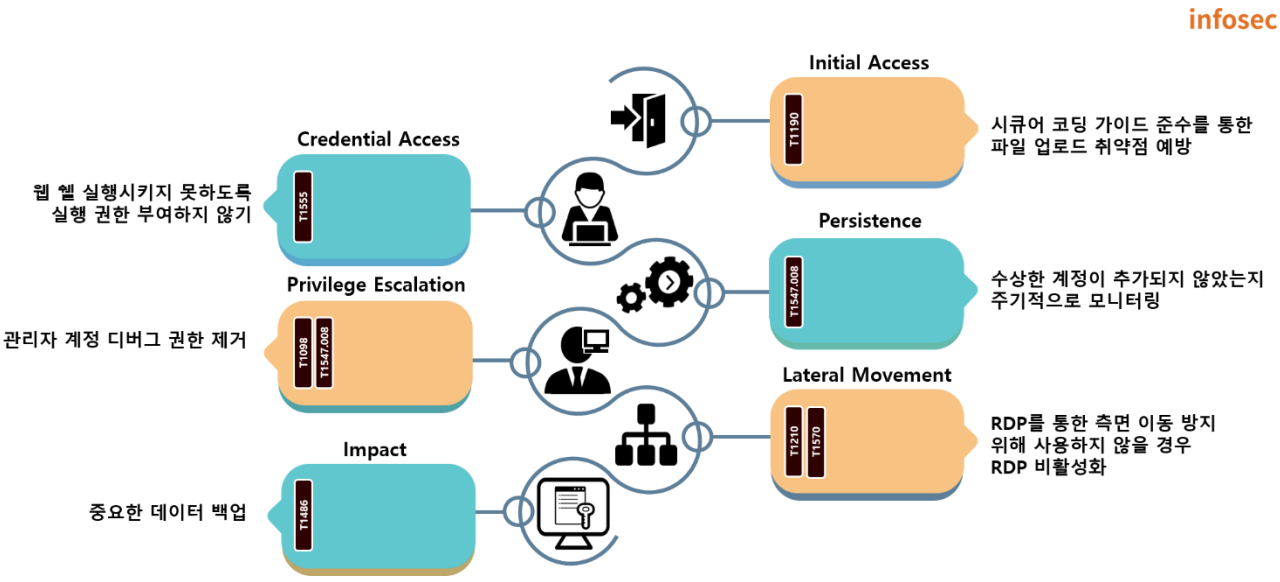
Step 3) NTLM 해시 해독

추출한 NTML 해시를 John the Ripper, Cain & Abel, Hashcat 등의 도구를 사용하여 해독한다. 이러한 도구들은 브루트 포스[19]나 레인보우 테이블[20] 등의 방법을 사용하여 해시 값을 해독한다.

[19] 가능한 모든 경우의 수를 시도하여 비밀번호나 암호화된 데이터를 찾아내는 공격 기법

[20] 해시 함수를 사용하여 저장된 비밀번호를 미리 계산하여 테이블로 만들고, 이를 이용하여 해시된 값을 빠르게 역산하여 비밀번호를 찾아내는 공격 기법

시나리오 2 - 단계별 대응방안



- 파일 업로드 취약점 악용을 예방하기 위하여 화이트 리스트를 기반으로 확장자 검사를 진행하고 만약 업로드 되었을 경우 실행되는 것을 막기 위하여 파일이 저장되는 경로의 실행 권한을 제거한다.
- 그리고 권한 상승 도구와 Mimikatz 가 설치되는 것을 예방하기 위해서 상위 디렉터리 접근을 제한하는 정책을 설정해야 하며, 이러한 도구를 탐지하는 보안 소프트웨어를 설치해야 한다.
- 만약 Mimikatz 가 설치되었을 경우 NTLM 해시가 탈취될 수 있으므로, Mimikatz 가 디버그 권한을 획득하지 못하게 관리자 계정의 디버그 권한을 제거하고 사용하지 않을 경우 RDP 를 비활성화하여 측면 이동을 예방한다. 또한 수상한 파일이나 계정이 추가되지는 않았는지 주기적으로 모니터링을 진행해야 한다.
- 마지막으로 파일이 암호화되었을 경우를 대비해 중요한 데이터는 보안 백업을 통해 데이터를 보호해야 한다. 백업 데이터 보호를 위해 원본과 다른 형식으로 백업 데이터를 보호하고 데이터 사본 간 격리, 백업 데이터 암호화 등을 갖춰 허용된 사용자만 접근할 수 있도록 제한해야 한다.

■ 참고 사이트

URL : https://www.swascan.com/bitlocker-ransomware-malware-analysis/

URL :http://idchowto.com/%EC%9C%88%EB%8F%84%EC%9A%B0-%EB%B9%84%ED%8A%B8%EB%9D%BC%EC%BB%A4-bitlocker-%EB%9E%9C%EC%84%AC%EC%9B%A8%EC%96%B4-%EC%82%AC%EA%B3%A0%EC%82%AC%EB%A1%80-%EB%B6%84%EC%84%9D/

URL : https://thestack.technology/ransomware-attack-bitlocker/

URL : https://iboysoft.com/wiki/bitlocker-virus.html

URL : https://www.bleepingcomputer.com/news/security/clop-ransomware-gang-begins-extorting-goanywhere-zero-day-victims/

URL : https://www.securityweek.com/microsoft-smartscreen-zero-day-exploited-to-deliver-magniber-ransomware/

URL : https://www.bleepingcomputer.com/news/security/ransomware-gang-posts-video-of-data-stolen-from-minneapolis-schools/

URL : https://www.boannews.com/media/view.asp?idx=114832

URL : https://www.bleepingcomputer.com/news/security/BianLian-ransomware-gang-shifts-focus-to-pure-data-extortion/

URL : https://www.securityweek.com/ransomware-group-claims-theft-of-valuable-spacex-data-from-contractor/

URL : https://www.scmagazine.com/analysis/ransomware/north-korea-using-healthcare-ransomware-attacks-to-fund-further-cybercrime-feds-say

URL : http://www.datanet.co.kr/news/articleView.html?idxno=154612

URL : https://www.boannews.com/media/view.asp?idx=116717

URL : https://thehackernews.com/2023/02/north-korean-hackers-targeting.html