KARA
Korea Anti Ransomware Alliance

2023.04.

KARA 랜섬웨어 동향 보고서

KARA 랜섬웨어 동향 보고서

■ 랜섬웨어 트렌드

✓ 랜섬웨어 트렌드 분석

최근 랜섬웨어 그룹들은 초기 침투부터 피해자 확보, 탐지 우회에 다양한 수단을 사용하며 전략적으로 공격을 수행하고 있다. 지난 2월 전 세계적으로 대규모 공격을 감행해 3,800대의 ESXi 서버를 감염시킨 ESXiArgs 랜섬웨어 공격자는 초기 침투를 위해 2년 전 발견된 취약점을 악용했으며 Play, Cuba 그룹은 MS Exchange 서버의 제로데이 취약점을 악용하는 등 공격자들은 다양한 경로를 모색해 초기 침투를 수행하고 있다.

한편 초기 침투를 전문적으로 수행하는 IAB(Initial Access Broker)를 찾는 그룹의 움직임이 확인되는 가운데 Medusa 그룹이 피해자로부터 탈취한 데이터에 접근하는 방법을 동영상으로 게시하고 BlackCat 그룹이 피해자의 사이트와 비슷한 도메인을 생성해 탈취한 데이터를 게시하는 등 피해자 협박, 데이터 유출 방식 또한 고도화되어가고 있는 것을 확인할 수 있으며 분석을 방해하고 탐지를 우회하기 위해 Go, Rust 언어로 랜섬웨어를 제작하는 시도 또한 지속적으로 확인되고 있다.

신규 랜섬웨어 및 그룹 활동

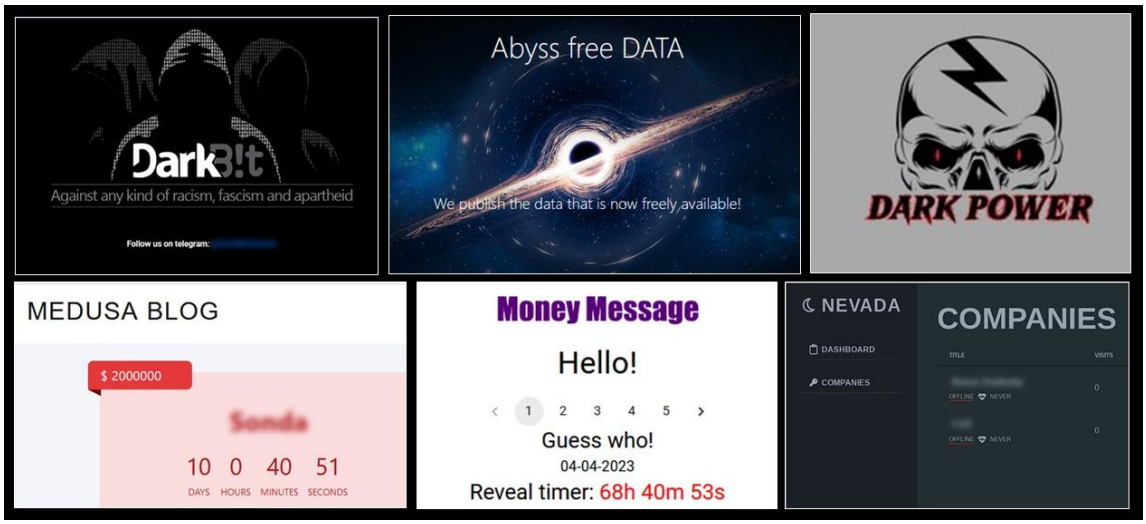


그림 1. 신규 랜섬웨어 및 그룹 활동

1분기에 발견된 Nevada, Medusa, DarkBit, Abyss, DarkPower, MoneyMessage 랜섬웨어 그룹 모두 다크웹을 운영하며 이중 협박 전략을 사용하고 있다. Nevada는 2월 중 발견된 그룹으로 Windows 및 VMware ESXi 시스템을 타깃으로 공격하고 있으며 Nokoyawa 랜섬웨어의 코드 및 암호화 알고리즘을 차용한 흔적이 발견되어 Nokoyawa 랜섬웨어의 변종으로 추측되고 있다. Medusa 그룹은 MedusaLocker 그룹과 비슷한 이름으로 인해 여러 추측이 나오고 있으나 2021년부터 활동을 시작한 그룹으로 2019년부터 활동을 하고 있는 MedusaLocker와는 별개의 그룹이다. 2021년 6월부터 활동을 시작한 Medusa 그룹은 활동이 부진하고 피해자가 거의 없었으나 올해 2월부터는 다크웹을 운영하고 다수의 기업 데이터를 유출하는 등 본격적으로 활동을 이어 나가고 있다.

비슷한 시기에 발견된 DarkBit 그룹은 다크웹, 트위터, 텔레그램 등의 SNS를 통해 이스라엘에 대한 반정부적인 메시지와 인종차별에 대한 반감을 표출하는 등 핵티비즘(Hacktivism)[1]의 성격을 보이고 있으며 특정 산업의 정리해고 문제를 트위터를 통해 여러 번 지적하고 랜섬노트를 통해서도 언급하는 등 정리해고에 의한 개인적인 보복으로 추측되었으나 이란 배후 해킹 조직 MuddyWater의 소행으로 드러났다.

3월에 발견된 그룹 중 DarkPower 그룹은 활동을 시작함과 동시에 다수의 피해 기업을 다크웹에 게시했으나 그 이후로 현재까지 추가적인 피해자는 발생하지 않고 있으며 Abyss, MoneyMessage 그룹은 기업들을 타깃으로 지속해서 공격을 수행하고 있다.

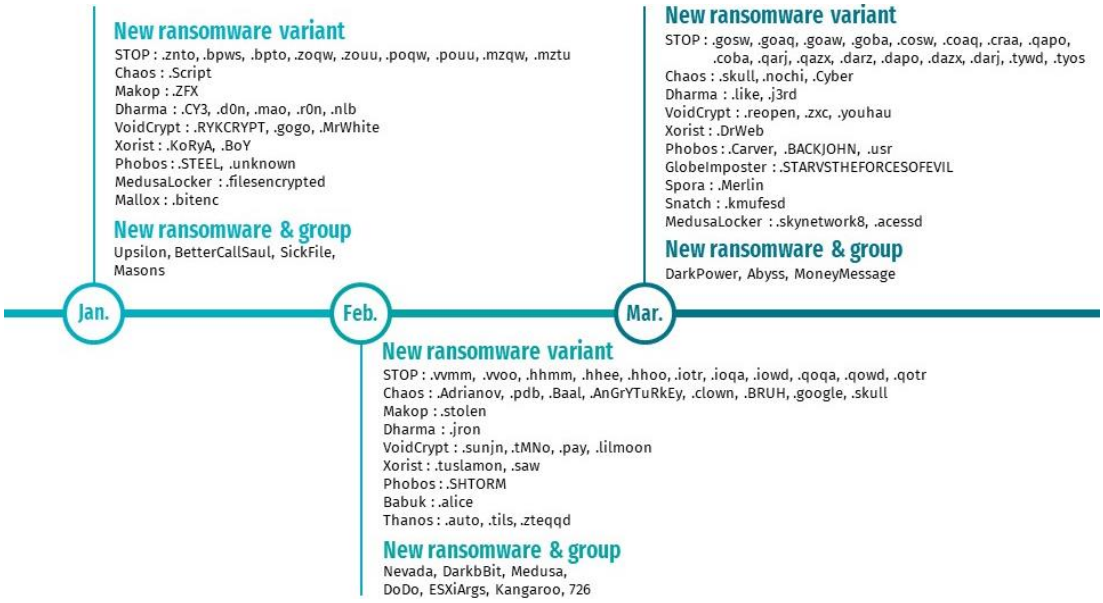


그림 2. 신규/변종 랜섬웨어 활동

[1] 핵티비즘(Hacktivism): 정치·사회적 목적을 달성하기 위해 시스템을 해킹하고 무력화하는 행위

신규 랜섬웨어와 변종 랜섬웨어도 지속적으로 발견되고 있다. 그중 Linux, ESXi 서버를 타깃으로 하는 Royal 랜섬웨어 변종과 Linux를 타깃으로 하는 Clop 랜섬웨어 변종이 발견됐다. 2월 초에는 BlackCat v3(버전 3)와 다형성이 적용된 v3 morph가 발견되었으며 같은 달 말에 v3 morph2가 발견되기도 했다. 한편 2022년 6월에 발견된 LockBit Red, BlackMatter 랜섬웨어의 소스코드를 사용한 LockBit Black에 이어 1분기에는 LockBit Green이 발견되었는데 LockBit Green은 작년 3월 유출된 Conti 랜섬웨어의 소스 코드를 차용한 것으로 확인됐으며 이는 LockBit 그룹이 계열사를 지속적으로 모집함과 동시에 본인들의 활동을 과시하기 위한 것으로 추측할 수 있다.

랜섬웨어 공격 그룹 트렌드

분업을 준비하는 일부 랜섬웨어 그룹의 움직임이 확인되고 있다. 3월에는 Bl00dy 그룹이 텔레그램을 통해 IAB를 구인하는 글을 게시하기도 했는데, 이는 초기 침투를 보다 원활하게 수행하기 위한 목적도 있지만 그룹 내에서 각자의 역할을 분담하고 분업하기 위한 목적으로도 볼 수 있으며 일부 그룹이 규모를 확장하기 위해 분업을 준비하는 것으로 추측할 수 있다.

한편 Radar, Endurance 등 일부 랜섬웨어의 주 활동 장소였던 해커 커뮤니티 브리치 포럼(Breached forum)의 일부 운영자들이 FBI에 의해 체포된 후 사이트 운영을 중단함에 따라 일부 랜섬웨어 그룹들의 활동 영역에도 변화가 있을 것으로 추측된다.

비주류 언어를 사용해 랜섬웨어를 개발하는 그룹 또한 지속적으로 발견되고 있다. 작년에 발견된 Hive, BlackCat, BianLian 등의 랜섬웨어에 이어 1분기에는 Go 언어로 제작된 DarkBit, Rust 언어로 제작된 Nevada 랜섬웨어가 발견되는 등 Go, Rust 언어로 랜섬웨어를 개발하는 시도가 지속적으로 확인되고 있다. 공격자들은 안정성과 빠른 속도를 보장하는 Go, Rust 언어로 랜섬웨어를 개발해 정적 컴파일[2]과 메모리의 안정성을 보장하는 언어적 특성으로 생성되는 다수의 더미 코드 및 복잡한 구조로 기존의 주류 언어(C/C++/C#)로 개발된 랜섬웨어보다 분석을 지연시키고 탐지를 회피하고 있으며 크로스 컴파일[3] 기능을 통해 다양한 운영체제를 타깃으로 랜섬웨어를 개발하고 공격을 수행하고 있다.

[2] 정적 컴파일: 소스코드의 모든 부분을 기계어로 변환해 실행파일을 생성하는 과정

[3] 크로스 컴파일: 다른 CPU나 운영체제에서 실행 가능한 프로그램을 생성하는 과정

국내 동향

국내기업 및 불특정 다수를 타깃으로 한 랜섬웨어 공격이 여럿 발견됐으며 그중 Nevada, LockBit 2.0, Magniber 랜섬웨어가 불특정 다수를 대상으로 유포되고 있다. 2017년부터 우리나라를 타깃으로 유포되기 시작한 Magniber 랜섬웨어는 지난 분기에 코로나 관련 파일명을 위장해 유포된 데 이어 1분기에는 윈도우 인스톨러(MSI)를 위장해 유포되고 있으며 LockBit 2.0 랜섬웨어는 2021년부터 이력서 또는 저작권 사칭 메일을 통해 유포됐으며 1분기에도 지속적으로 발견되고 있다.

GlobeImposter, Mallox, Play, LockBit 등 일부 그룹들이 국내 기업들을 타깃으로 공격한 정황도 발견됐다. 2월에는 국내기업을 타깃으로 하는 GlobeImposter(tzw) 캠페인이 확인되고 국내 제조업체가 Monster 랜섬웨어에 감염된 사례가 확인되었으며 2월과 3월에는 Mallox, Play 그룹이 각각 반도체 기업과 법률회사로부터 탈취한 데이터를 유출하는 등 국내 기업의 피해가 꾸준히 발생하고 있다. 3월 말 LockBit 그룹은 국세청의 데이터를 탈취했다는 게시글과 유출 예정 일자를 다크웹에 게시했으나 예정 일자가 지난 현재까지 유출된 데이터가 게시되지 않고 있으며 해당 유출 예정 날짜가 만우절이었다는 점에서 이벤트성 게시글일 가능성도 존재하지만 실제 데이터가 탈취되어 협상 중일 가능성도 있어 예의 주시할 필요가 있다.

한편 불특정 공격자들이 일부 국내기업의 시스템에 침투한 뒤 Windows 운영체제에 기본으로 탑재되어 있는 BitLocker[4]를 악용해 드라이브를 암호화하고 금액을 요구하는 등 랜섬웨어 없는 랜섬웨어에 의한 피해도 1분기에 다수 발견되고 있다.

[4] BitLocker: 하드디스크, USB와 같은 저장장치를 암호화 해 데이터를 보호하는 기능

1. 랜섬웨어 그룹 활동 및 통계

최근 3개월간 월 별 피해자 수가 늘어났으며 특히 2월과 3월 사이에 그 수가 급격하게 늘어난 것을 확인할 수 있다. 이는 Clop 랜섬웨어 그룹이 파일 전송 소프트웨어인 GoAnyWhere MFT의 제로데이 취약점(CVE-2023-0669)[5]을 악용해 다수의 기업에 피해를 입혔기 때문이며 현재까지는 100여 곳의 기업에서 피해가 확인되었으나 시간이 지나면서 추가적인 피해자가 발견될 것으로 추측된다. 2021년부터 활동을 시작하며 꾸준하게 피해자를 확보해오던 Hive 그룹은 1월에 FBI에 의해 다크웹이 폐쇄된 이후 추가적인 활동과 피해자가 발견되지 않고 있으며 작년 1분기 이후로 활동이 잠잠했던 Stormous 그룹이 3월 말부터 다수의 피해자를 확보하며 활동을 재개하기 시작하는 등 일부 그룹들의 활동에 변동이 확인된다. 이어서 LockBit, BlackCat, Royal, BianLian 그룹은 기업들을 타깃으로 지속적으로 피해를 입히고 있으며 피해국은 미국, 영국, 캐나다 순으로, 산업군에서는 제조, 서비스, 유통업 순으로 지난 분기와 비슷한 흐름으로 피해가 발생하고 있다.

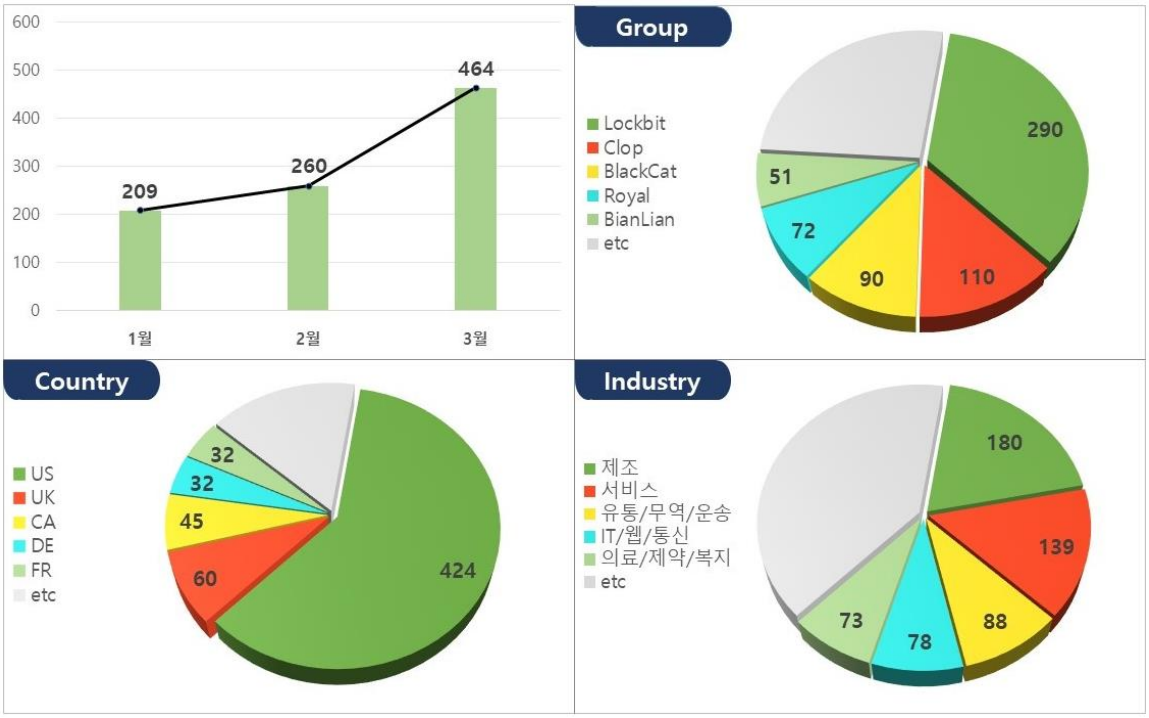


그림 3. 랜섬웨어 그룹 활동

[5] CVE-2023-0669: GoAnyWhere 소프트웨어에서 발생하는 원격 코드 실행 취약점

2. RDP를 노리는 GlobeImposter 랜섬웨어

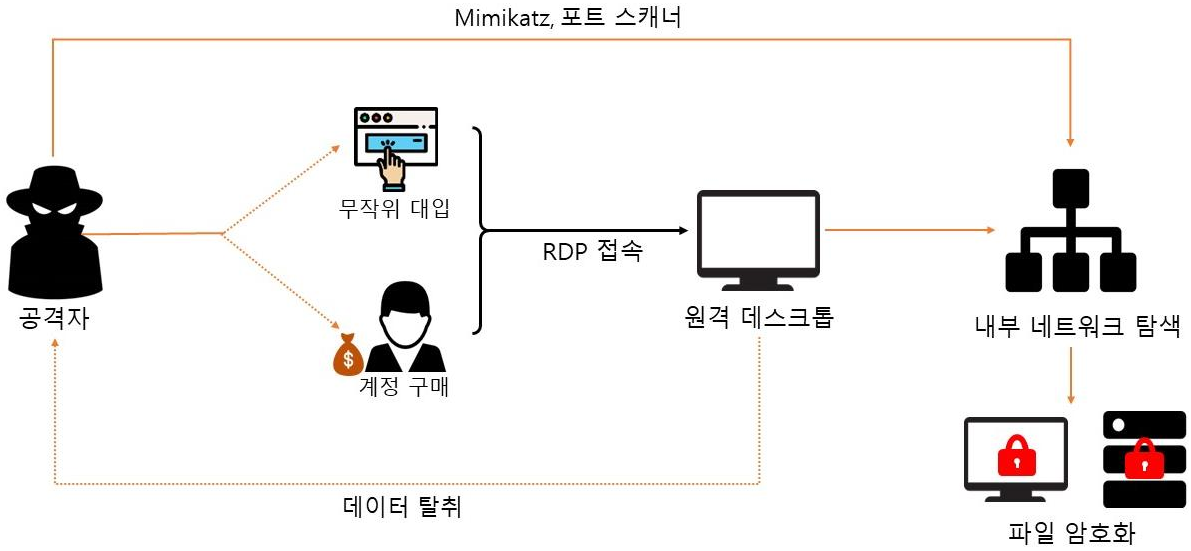


그림 4. RDP 침투 시나리오

지난 분기 GlobeImposter 랜섬웨어는 무작위 대입 공격, 디폴트 계정을 통해 취약한 MS-SQL 서버를 타깃으로 활발하게 공격을 수행해왔다. 한편 1 분기에는 RDP 를 통해 국내에 유포되는 정황이 확인되고 있으며 국내 기업들을 타깃으로 하는 GlobeImposter(tzw) 캠페인이 발견되는 등 국내를 타깃으로 한 공격에 사용되는 것을 확인할 수 있다.

GlobeImposter 랜섬웨어는 여러 그룹과의 연관성이 확인되고 있다. 지난 분기에는 Mallox 랜섬웨어에서 GlobeImposter 랜섬웨어 감염 시 확장자(.Globeimposter-Alpha865qqz)가 암호화 제외 대상으로 지정되어 있어 Mallox 그룹과의 일부 연관성이 확인되었다. 한편 1 분기에는 MedusaLocker 그룹과의 연관성이 제기되고 있는데 특히 두 그룹의 초기 침투 방식이 RDP 로 동일하다는 점과 과거 MedusaLocker 그룹이 사용하던 랜섬노트에 포함된 이메일이 최근 발견된 GlobeImposter 의 랜섬노트에 포함되어 있다는 점에서 연관성이 확인된다.

RDP 를 초기 침투 경로로 사용하는 랜섬웨어 그룹들은 공격을 수행하기 위해 다크웹, IAB 를 통해 RDP 계정을 구매하거나 무작위 대입 공격을 수행하여 초기 침투를 시도한다. 만약 침투에 성공할 경우 해당 서버의 파일을 암호화할 뿐만 아니라 Mimikatz[6], 포트 스캐너와 같은 도구를 다운로드 받아 내부 네트워크 시스템에 접근해 파일들을 암호화하는 방식으로 피해를 줄 수 있어 이를 예방하기 위한 적절한 보호 조치가 필요하다.

---

[6] Mimikatz: Windows 운영체제 계정 및 암호 탈취 도구

GlobeImposter 랜섬웨어

1) Background

- GlobeImposter는 2017년 초에 발견된 랜섬웨어로 Globe 랜섬웨어의 작동 방식과 랜섬노트가 유사하다는 점에서 FakeGlobe 랜섬웨어로 불려왔다. 주로 피싱 메일, RDP를 초기 침투 방식으로 사용하며 미국, 유럽, 아시아 등의 지역을 대상으로 공격을 시도해왔다.
- 2017년 9월에는 Locky 랜섬웨어의 기능과 GlobeImposter 랜섬웨어의 기능이 함께 포함되어있는 변종이 발견되었으며 해당 랜섬웨어를 실행할 경우 Locky 랜섬웨어에 먼저 감염되고 추가로 GlobeImposter 랜섬웨어에 감염되어 파일을 복구하기 위해서 두 번의 비용 지불 및 복호화 과정을 수행해야 한다.
- 지난 4분기에 발견된 Mallox 랜섬웨어의 암호화 제외 대상에 GlobeImposter 랜섬웨어 감염 시 확장자(.Globeimposter-Alpha865qqz)가 포함되어 있어 두 그룹 사이에 일부 연관성이 확인되었으나 1분기에는 GlobeImposter 랜섬웨어의 초기 침투 방식과 MedusaLocker 그룹의 초기 침투 방식이 RDP로 같다는 점과 MedusaLocker 그룹이 사용하던 랜섬노트에 포함된 이메일이 최근 발견된 GlobeImposter의 랜섬노트에 포함되어 있다는 점에서 MedusaLocker 그룹과의 연관성이 확인된다
- 2월부터 국내 기업들을 타깃으로 하는 GlobeImposter(tzw) 캠페인이 발견되었으며 해당 랜섬웨어에 감염될 경우 파일의 확장자가 .tzw 로 변경된다.
- GlobeImposter 랜섬웨어는 RDP를 통해 유포되고 있으며 공격자들은 초기 침투를 위해 RDP의 기본 포트(3389)를 스캐닝해 RDP가 활성화되어 있는 시스템들을 공격 대상으로 선정한다.
- 공격 대상을 선정한 후 무작위 대입 공격 또는 IAB, 다크웹에서 구한 유출된 계정을 통해 접속을 시도하고 접속에 성공할 경우 랜섬웨어를 통해 파일을 암호화한 후 추가로 Mimikatz, 포트 스캐너와 같은 툴을 사용해 내부 네트워크 시스템에 접근해 암호화를 시도한다.

2) 특징

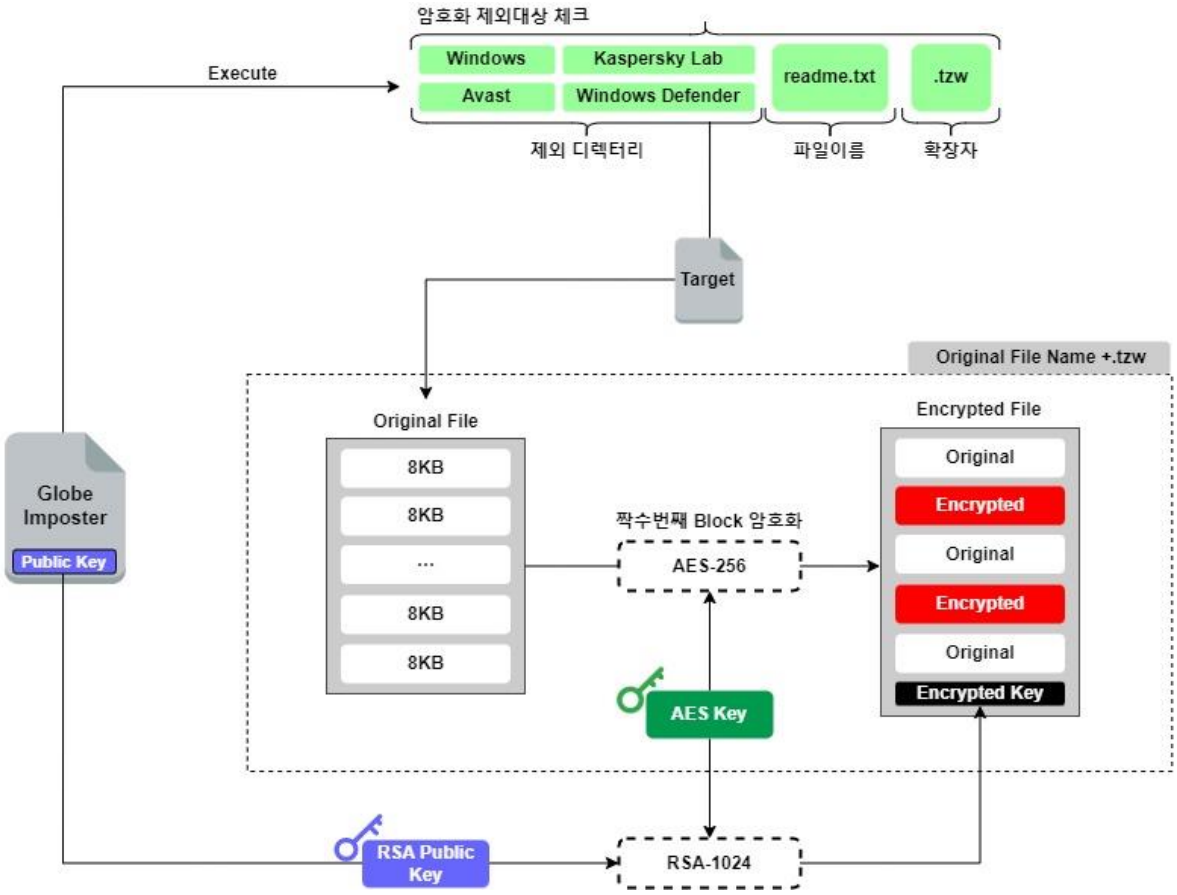


그림 5. GlobeImposter 암호화 로직

- 랜섬웨어 파일 내부에 난독화 되어있는 데이터를 복호화 하기위해 AES-256 알고리즘을 사용하며 이때 복호화 되는 데이터에는 암호화 제외 경로, 암호화 제외 파일 이름, 확장자가 포함되어 있다.
- 암호화 제외 디렉터리 중에 백신 제품과 관련된 디렉터리(Windows Defender, Kaspersky Lab, Avast)가 다수 포함되어있으며 이는 백신 관련 데이터를 변조할 경우 탐지되는 것을 우회하기 위함으로 추측된다.
- 각 파일을 8KB 크기의 블록으로 나눈 뒤 홀수 번째 블록만 AES-256 알고리즘을 사용해 암호화하며 사용한 키값은 RSA-1024 알고리즘으로 보호한 뒤 파일의 마지막 부분에 저장한다.

- 암호화 작업이 끝나면 Volume Shadow Copy[7]를 삭제해 데이터를 복구할 수 없게 하며 추가로 윈도우 이벤트 로그, RDP 접속 기록을 삭제하고 RDP 기능을 비활성화해 탐지 및 분석을 방해한다.

```
// @echo off
// vssadmin.exe Delete Shadows /All /Quiet
// reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" /va /f
// reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" /f
// reg add "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers"
// cd %userprofile%\documents\
// attrib Default.rdp -s -h
// del Default.rdp
// for /F "tokens=*" %1 in ('wevtutil.exe el') DO wevtutil.exe cl "%1"
```

그림 6. 이벤트 로그 삭제 및 RDP 비활성화

[7] Volume Shadow Copy: 스냅샷 또는 특정 시점의 복사본

3) IoC

SHA256	eab81d32180ddac56ed5d63e50ec4e20c0f1ceaab7e7e5f90d74883f5ae1bddc 6d3312e3992dc1244be5518718bb42558057f7ec59a50009892846acf58481d9 98e4a7b1d986cf70410dc14933dc2b3924056cb4cac52f0193cd3a93f58d6b07
File name	70.exe Tzw_1.exe DZ86eEu.exe

3. 랜섬웨어, 비주류 언어에 눈뜨다

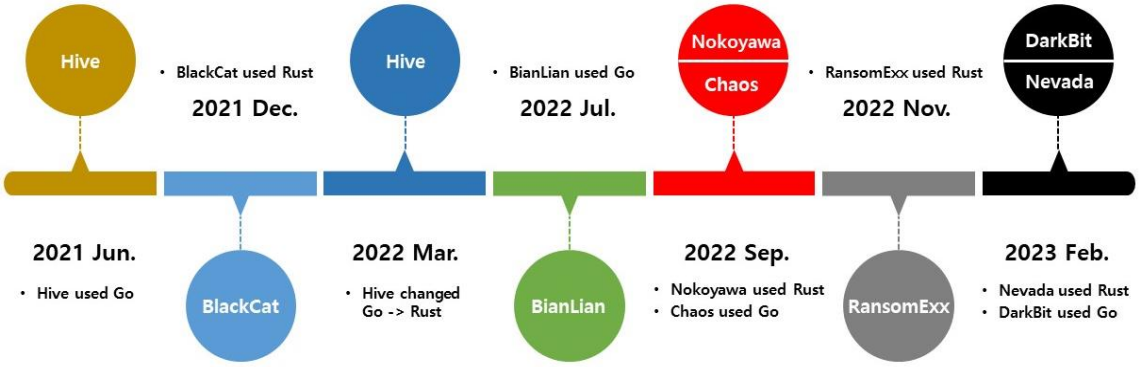


그림 7. 그룹별 Go, Rust 언어 사용 시기

최근 랜섬웨어 그룹들 사이에서 새로운 흐름이 발견되고 있다. 특히 작년과 올해에 Go, Rust 등의 언어로 제작된 랜섬웨어가 지속적으로 발견됨으로써 공격자들이 비주류 언어로 시선을 돌리는 것을 확인할 수 있다. 랜섬웨어 그룹 중에서는 Hive, BlackCat 그룹이 가장 먼저 Go, Rust 언어를 사용해 랜섬웨어를 개발하기 시작했으며 그 이후에도 BianLian, Nokyawa, Chaos 등 여러 랜섬웨어 그룹들이 Go, Rust 언어로 개발한 랜섬웨어를 사용하며 활동하기 시작했다. 이처럼 Go, Rust 언어로 개발하는 시도가 지속해서 발견되는 가운데 그 이유에 대해서 생각해볼 필요가 있다.

Go는 Google 사에서 2012년에 정식으로 발표한 오픈소스 프로그래밍 언어이며 기존 주류 언어들과 유사한 코드 작성 방법으로 인한 쉬운 접근성, 싱글 코어에서 멀티스레드의 기능을 구현할 수 있는 Goroutine 제공, 빠른 실행 속도 등 다양한 특징을 가지고 있다. 그중에서 특히 눈여겨봐야 할 특징은 Go 언어가 정적 컴파일 언어라는 점이다. 정적 컴파일은 프로그램 제작 시 사용된 라이브러리 정보를 바이너리에 포함하는 것을 뜻하며 이를 통해 제작된 프로그램 내부에는 개발자가 작성한 공격 코드 이외의 문자열과 더미 코드들이 포함되게 된다. 랜섬웨어 공격자는 더미 코드들로 생성된 복잡한 구조와 난독화를 통해 분석을 지연시켜 탐지 회피의 가능성을 높이고 공격의 성공률을 높이고자 한다.

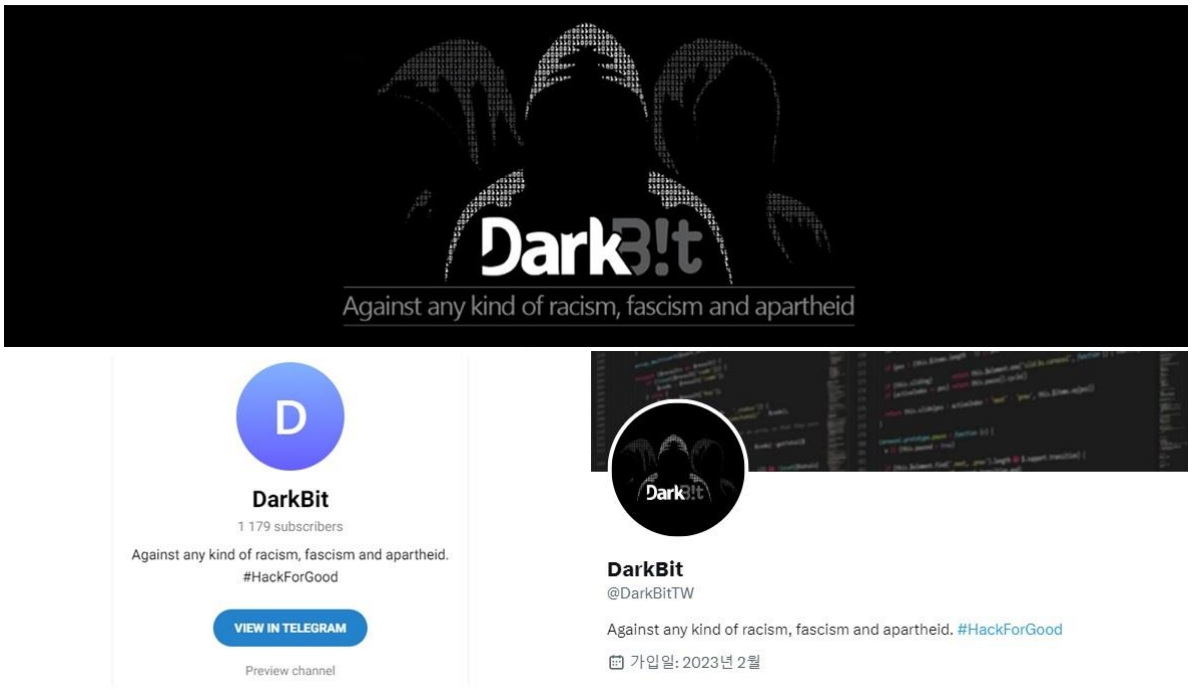
공격자들이 Rust 언어를 사용하는 이유도 이와 비슷하다. Rust 언어는 메모리의 안정성을 보장하는 언어로 C/C++ 언어와 다르게 사용자가 수동적으로 메모리를 관리하지 않아도 컴파일 시 컴파일러에서 메모리의 안정성을 보장해주는데 이때 컴파일러는 메모리 안정성을 보장하기 위해 여러 가지 런타임 코드와 보조 함수를 코드에 포함하게 되며 공격자들은 이 점을 이용해 분석을 방해하고 탐지 회피의 가능성을 높일 뿐만 아니라 메모리 충돌로 인한 오작동을 방지하고 빠른 속도로 암호화를 수행할 수 있다.

최근 랜섬웨어 개발에 사용되는 비주류 언어 중에서는 또 다른 특이점도 확인된다. 1 분기에는 Go 와 Rust 언어로 제작된 랜섬웨어뿐만 아니라 Nim 언어로 개발된 DarkPower 랜섬웨어가 발견되기도 했는데 한가지 눈여겨볼 점은 세 언어 모두 크로스 컴파일 기능을 지원한다는 점이다. 크로스 컴파일 기능은 다양한 운영체제를 타깃으로 프로그램 제작을 가능하게 해주는 기능으로 랜섬웨어 개발자들은 이 기능을 통해 코드를 재활용하고 다양한 운영체제를 타깃으로 랜섬웨어를 제작함으로써 효율적으로 공격을 수행할 수 있다.

비주류 언어로 개발된 랜섬웨어들은 기존의 주류 언어로 작성된 랜섬웨어보다 분석 데이터가 부족해 탐지 확률이 낮은 경향이 있으며 안정성을 보장하면서도 뛰어난 동시성과 병렬성을 통해 빠르게 암호화가 가능하여 공격자들은 이 점을 간파하고 공격을 수행하고 있다. 이러한 움직임은 과거부터 지속적으로 발견되어 왔으며 앞으로도 다양한 비주류 언어를 사용해 탐지를 회피하고 분석을 방해하는 랜섬웨어들이 꾸준히 발견될 것으로 추측된다.

✓ DarkBit 랜섬웨어

1) Background



- DarkBit 그룹은 2월 12일 이스라엘의 Technion 대학교를 공격하며 활동을 시작했다. 이 과정에서 22개 학과에서 총 4TB 이상의 데이터가 유출되었으며 텔레그램을 통해 추가 데이터 유출을 예고했다.
- 외부에서 접근 불가능한 내부 도메인과 Technion 대학교에 재직중인 네트워크 전문가 및 보안 전문가들이 사용하는 컴퓨터 호스트 이름이 암호화 제외 리스트로 지정되어 있어 공격자들은 공격 대상의 내부구조를 간파한 상태에서 공격을 수행한 것으로 추측된다.
- 다크웹, 텔레그램을 통해 인종차별, 정리해고 등에 대한 문제를 제기하고 반이스라엘 성향을 나타내는 등 핵티비즘(Hacktivism)의 성격을 보이고 있으며 트위터를 통해 특정 산업에 대한 정리해고 문제를 여러 번 지적해 개인적인 원한에 의한 보복으로 추측했으나 이란 배후 해킹 조직인 MuddyWater의 소행으로 드러났다.
- MuddyWater 해킹 조직은 2017년부터 Static Kitten, Mercury, Seedworm, Earth Vetala 등의 해킹 캠페인을 수행해왔으며 특히 아시아, 아프리카, 유럽 지역의 정부 및 민간 조직을 대상으로 공격을 수행해왔다. 또한 지난 4분기부터는 이스라엘의 기관들을 대상으로 공격을 수행하고 있으며 주로 Log4j 취약점을 초기 침투에 사용하고 있다.

2) 특징

```
Usage of Darkbit.exe:
  -all
        run on all without timeout counter
  -domain string
        domain
  -force
        force blacklisted computers
  -list string
        list
  -nomutex
        force not checking mutex
  -noransom
        Just spread/No Encryption
  -password string
        password
  -path string
        path
  -t int
        threads (default -1)
  -username string
        username
```

- 원본 파일에는 압축파일(.zip)과 바로가기(.lnk) 파일이 포함되어 있으며 바로가기 파일 실행 시 Windows 운영체제에서 프린터 마이그레이션 도구인 PrintBrm.exe의 명령어를 사용해 압축을 해제하고 랜섬웨어를 실행한다.
- Go 언어로 개발되었으며 Windows 운영체제를 타깃으로 제작되었다. 프로그램 실행 시 vssadmin –delete /all /Quiet 명령어를 사용해 Volume Shadow Copy를 삭제한 뒤 입력된 인자에 따라 지정된 동작을 수행한다.
- 랜섬웨어가 실행되고 있는 PC의 호스트 이름과 랜섬웨어 내부에 하드코딩 되어있는 블랙리스트를 비교해 동일 할 경우 암호화를 하지 않고 종료한다. 해당 블랙리스트에는 외부에서 접근 불가능한 내부 도메인 뿐만 아니라 Technion 대학교에 재직 중인 네트워크 전문가 및 보안 전문가들이 사용하는 컴퓨터의 호스트 이름이 포함되어 있다.

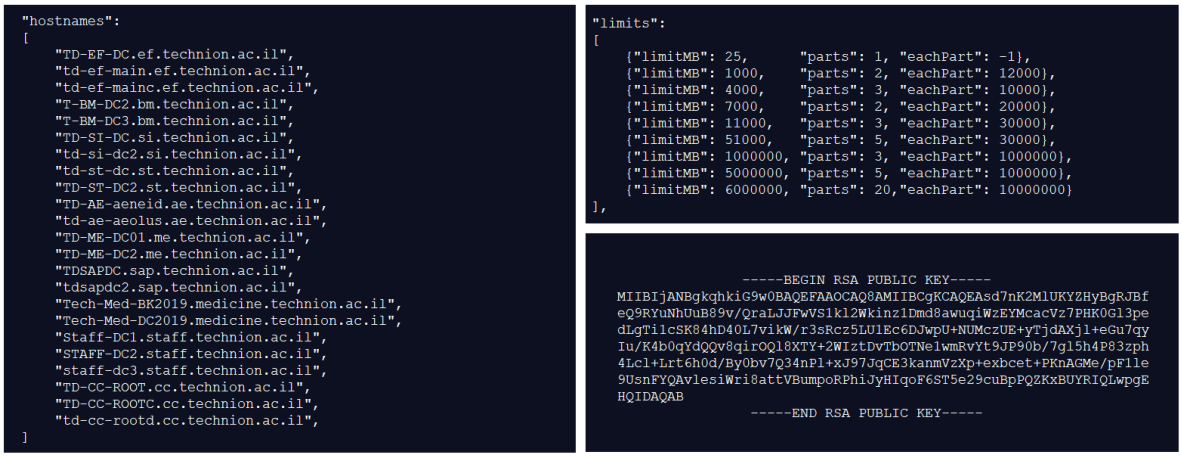


그림 8. 블랙리스트, 암호화 단위, RSA 공개키

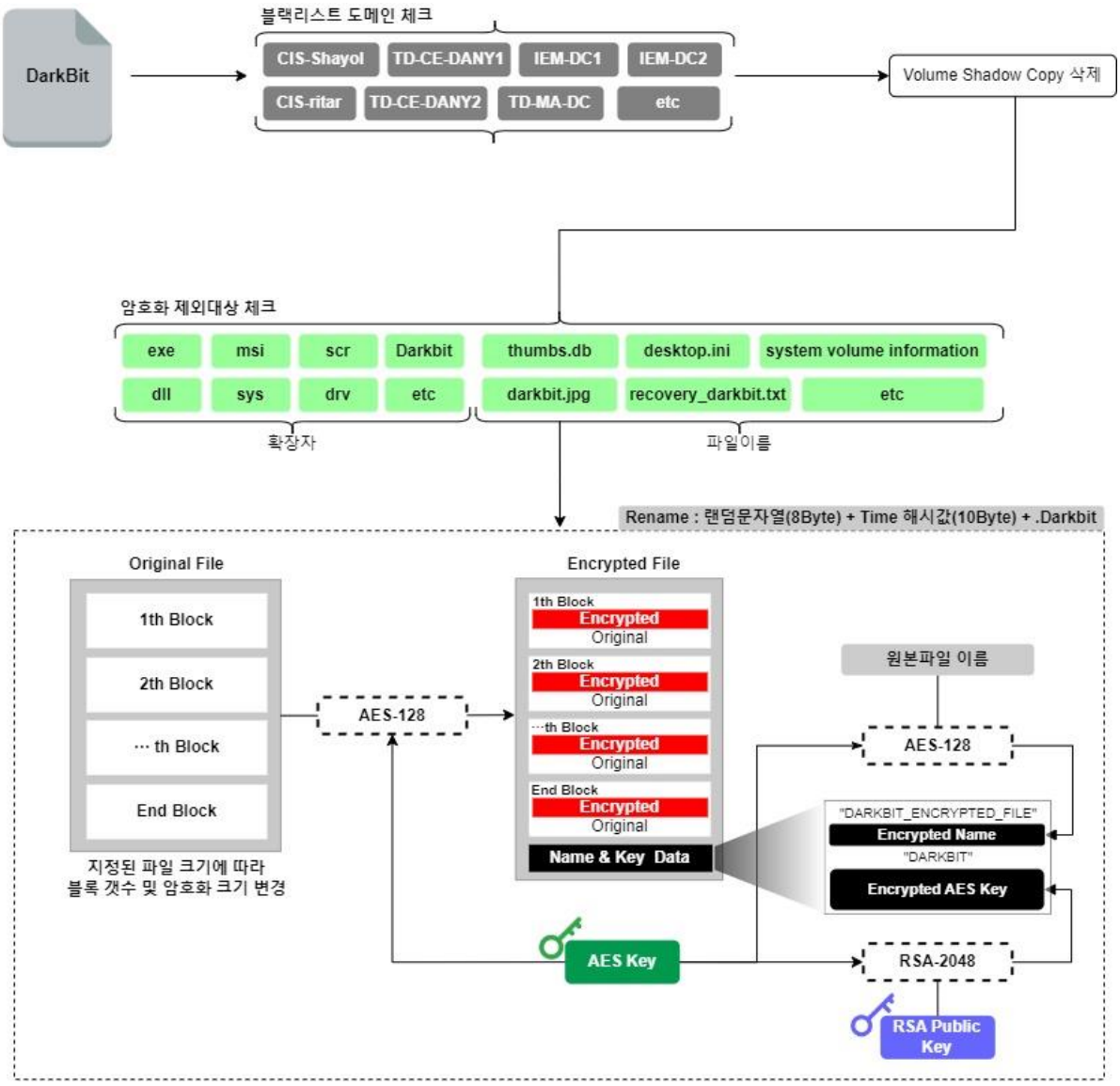


그림 9. DarkBit 랜섬웨어 암호화 로직

- 암호화 진행 전 실행 중인 랜섬웨어 프로세스의 우선순위를 높여 암호화를 빠르게 수행할 수 있도록 하며 암호화 진행 시 컴퓨터에 존재하는 프로세서 개수만큼 암호화 작업을 수행하는 Goroutine을 생성해 파일을 암호화한다.
- 지정된 확장자 및 파일 이름 또는 16바이트 이하의 파일인 경우 암호화 대상에서 제외되며 암호화 전 파일의 이름을 랜덤 문자열(8바이트) + Time 해시값(10바이트)으로 교체하고 확장자를 .Darkbit으로 변경한다. 이후 파일의 크기에 따라 파일을 블록 단위로 나눠 각 블록 내에서 지정된 바이트만큼만 AES-128 알고리즘을 사용해 암호화한다.

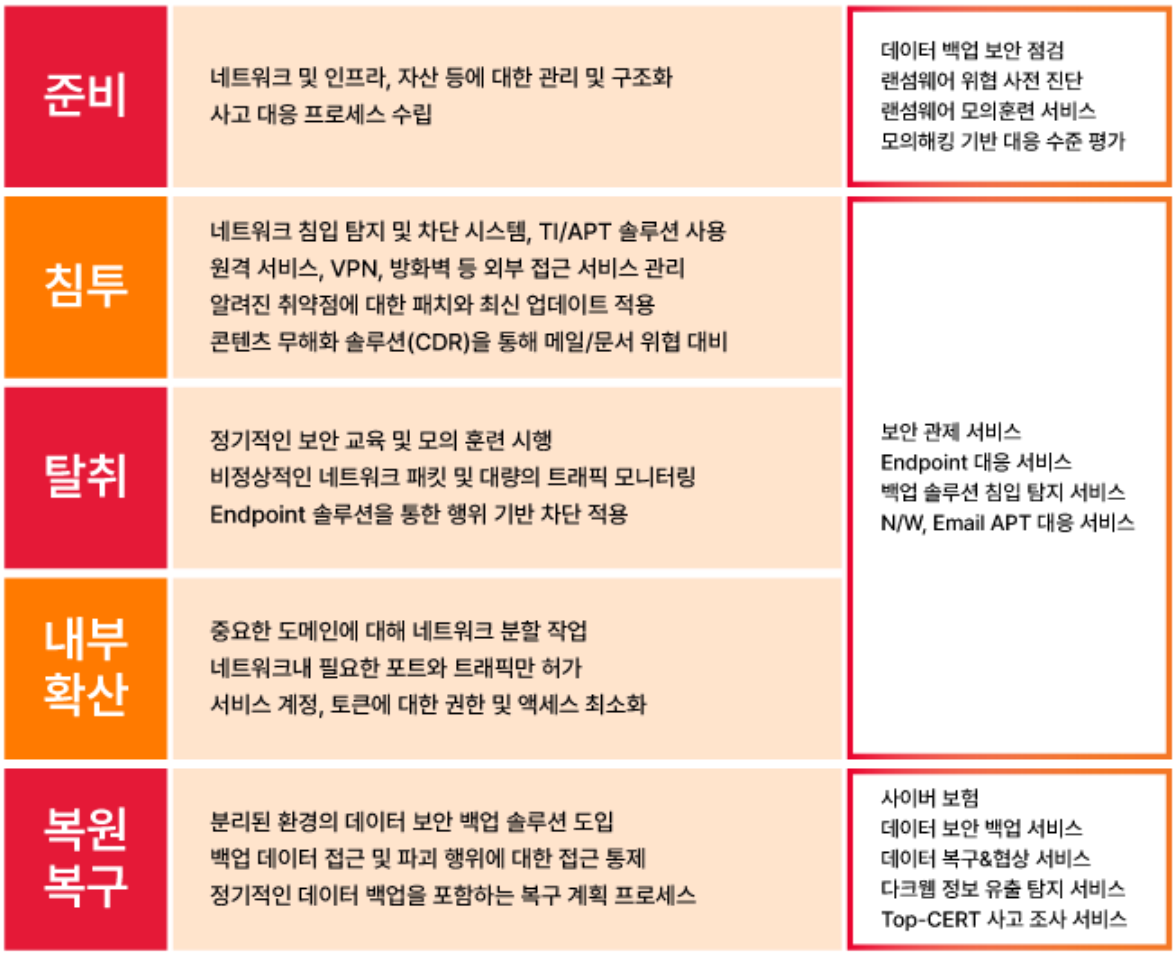
- 원본 파일 이름도 동일한 키를 통해 AES-128 알고리즘으로 암호화되며 사용된 키값은 랜섬웨어 내부에 존재하는 2,048 비트 RSA 공개키로 보호되어 "DARKBIT_ENCRYPTED_FILE | 암호화된 파일이름 | DARKBIT", 보호된 키값 순으로 파일 마지막 부분에 저장된다.

3) IoC

SHA256	9107be160f7b639d68fe3670de58ed254d81de6aec9a41ad58d91aa814a247ff Bc5954d7da18a20405e994bce05d927e7599b8a9a95d4412cab6fbc6324c3558 81c1bf78ab59bd78f615eeb3bc9f17ec2d82ba46d0224da63c855a9e7202116b
File name	8thcurse.exe HR-Update.exe hr-update.iso

■ 랜섬웨어 Mitigations

공격자는 공격대상을 선정하기위해 공격자 그룹이 수립한 전략을 통해 다양한 방법으로 정찰을 수행하며 이후 내부 인프라에 침입하여 파일을 암호화 시키고 자산을 위협하며 데이터 유출을 통한 협박을 시도한다. 이러한 피해를 예방하기위해 타깃형 APT 공격에 대한 대비와 침입에 대한 각 단계별 적절한 보안 요소 및 프로세스를 마련하여 공격자 그룹이 목표를 달성하기 전에 탐지하고 차단할 필요가 있다.



안녕을 지키는 기술 | SK 쉴더스

SK쉴더스㈜ 13486 경기도 성남시 분당구 판교로227번길 23, 4&5층
https://www.skshieldus.com

발행인 : SK쉴더스 EQST사업그룹 & KARA(Korea Anti Ransomware Alliance)
제　작 : SK쉴더스 커뮤니케이션그룹