Keep up with Ransomware

Hive 닮은꼴 Hunters 의 활동 개시

■ 개요

2023 년 10 월 랜섬웨어 공격으로 인한 피해 사례 발생 건수는 전월(496 건) 대비 약 30% 감소한 349 건으로 나타났다. 그러나, LockBit 이 활발한 활동을 하고 있으며 다양한 랜섬웨어 이슈들이 계속해서 발생하고 있어 여전히 긴장감은 유지되고 있다.

이번 달에는 악성코드 Qakbot[1]의 유포 정황이 다시 포착됐다. 지난 8 월 말, FBI 가 국제 공조를 통해 'Duck Hunt' 작전을 실행해 Qakbot 관련 인프라와 암호화폐 자산을 압수하고 활동을 무력화시킨 것으로 알려졌으나, 이번달 피싱 이메일을 통해 Qakbot 이 유포되고 있는 것이 확인됐다. 이번 유포 공격은 Qakbot 계열사의 소행으로 추정되나, 일각에서는 Knight 를 유포하는 조직이 Qakbot 을 이용하고 있는 것으로도 추측되고 있다.

Qakbot 공격은 공격자가 LNK 파일을 첨부한 피싱 이메일을 통해 Knight 랜섬웨어와 Remcos RAT[2]를 유포하는 방식으로 진행되고 있다. LNK 파일에는 PowerShell 을 실행시켜 C2 서버[3]에서 Knight 랜섬웨어를 다운로드 하는 명령어가 담겨있다. 따라서 LNK 파일을 실행만 해도 Knight 랜섬웨어에 감염될 수 있어 주의가 필요하다. Knight 랜섬웨어 그룹은 Cyclops 랜섬웨어 그룹의 리브랜딩으로, 올해 8 월 새롭게 활동을 시작한 이후 자체 랜섬웨어를 비롯해 다양한 전략을 사용한 적극적인 공세를 펼치면서 영향력을 확대하고 있다.

이번 달 다크웹의 XSS 해킹 포럼에서 HelloKitty 랜섬웨어의 초기 버전 소스코드가 유출됐다. HelloKitty 는 DeathRansom, FiveHands 등의 계열로 알려져 있는 서비스형 랜섬웨어로, 이번 소스코드 유출로 인해 누구나 악용 가능하게 됐다. 과거 HiddenTear, Conti 랜섬웨어 등 랜섬웨어 소스코드 유출로 인해 변종 공격이 발생한 사례가 다수 존재하기 때문에 주의가 필요하다.

---

[1] Qakbot : 자격 증명 탈취 수행과 랜섬웨어를 전달하는데 사용하는 악성코드

[2] Remcos RAT : 감염된 PC 를 원격으로 제어하는 데 사용되는 악성코드

[3] C2 서버 : 공격자가 원격지에서 명령을 내리고 통제하기 위해 사용하는 서버

해당 소스 코드를 유출한 유저는 'kapuchin0'라는 공격자로 알려져 있으며, 'Gookee'라는 별칭을 사용하고 있다. 이 유저는 이전부터 해킹 범죄에 가담한 이력이 있으며, 특히 2020 년 Sony Network Japan 에 대한 초기 침투 경로 및 RaaS(Ransomware-as-a-Service)[4]로 운영되는 GooKee 랜섬웨어를 판매하기도 했다. 또한, 그는 재정적 지원을 받으면 더 많은 랜섬웨어를 개발하겠다는 의지를 밝힘과 동시에 올해 말에 출시될 예정인 랜섬웨어의 암호화 기능에 대해 자랑하는 등 적극적인 활동 의지를 나타내기도 했다.

최근 랜섬웨어 공격 동향을 살펴보면, 단일 종류가 아닌 두 가지 종류의 랜섬웨어를 사용해 공격을 시도하는 이중 랜섬웨어 공격 사례가 빈번하게 발견되고 있다. 이중 랜섬웨어 공격은 공격자가 최초 공격을 수행한 후 평균적으로 이틀 이내에 다른 종류의 랜섬웨어 공격을 수행하는 특징이 있다. 단일 랜섬웨어 공격으로도 데이터 유출, 시스템 암호화, 다운타임(Down-time) 등으로 인한 상당한 피해가 발생하는 상황에서 이중 랜섬웨어 공격의 피해를 입는다면 이러한 손실이 두 배 이상으로 증가하여 매우 심각한 피해를 초래할 수 있다. 따라서 랜섬웨어 감염 예방에 적극적으로 힘써야 한다.

이번 달에도 Hunters, KeyLock, BlackDream, Ran 등 다양한 신규 랜섬웨어가 발견됐다. 특히, Hunters 랜섬웨어가 올해 초에 폐쇄된 Hive 랜섬웨어와의 연관성이 발견돼 이목을 끌고 있다. Hunters 는 Hive 버전 6 의 샘플과 약 56% 유사도 보이고 있으며, 특히 암호화 로직의 유사한 패턴으로 Hunters 가 Hive 의 리브랜딩이라는 의혹이 제기되고 있다. 하지만, Hunters 측은 Hive 랜섬웨어의 소스코드를 구매하여 개발한 것이라고 주장하며 리브랜딩 의혹을 부인하고 있다. 그럼에도 불구하고 여러 부분에서 두 랜섬웨어 간의 연관성을 보여주는 증거가 있어, Hunters 의 주장은 다소 신빙성이 떨어진다.

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

■ 랜섬웨어 뉴스

infosec

FBI 및 유로폴, RagnarLocker 랜섬웨어 폐쇄 후 개발자 체포

- FBI, 유로폴 등이 공조하여 RagnarLocker 그룹 폐쇄
- RagnarLocker는 19년 말에 발견된 랜섬웨어 그룹
- 23년 이전까지는 상당히 위협적인 그룹이었으나, 23년에는 활동에 적극성을 보이지 않음

하마스 옹호 핵티비스트, BiBi-Linux Wiper로 이스라엘 타깃

- 이스라엘의 리눅스 시스템을 타깃으로 한 Wiper 'BiBi-Linux' 발견
- Wiper는 파일 암호화를 가장하나 실제로는 데이터와 운영체제를 파괴
- BiBi-Linux는 파일 내용을 덮어쓰고 'BiBi' 문자열로 파일 이름을 변경

* 핵티비스트 : 해킹을 투쟁 수단으로 사용하는 행동주의자

LockBit, Boeing 공격 후 데이터 탈취

- 항공기 제조 대기업 Boeing이 사이버 공격을 당했으며, LockBit 그룹이 데이터를 탈취했다고 주장
- Boeing은 비행 안전에 영향을 미치지 않았다고 발표하며, 수사 기관과 협력하고 있다고 주장

새로운 LostTrust 랜섬웨어, MetaEncryptor의 리브랜딩 가능성 제기

- 두 랜섬웨어는 거의 동일한 데이터 유출 사이트와 랜섬웨어 샘플을 사용하므로 리브랜딩 의혹 제기
- LostTrust는 특정 기업들을 대상으로 데이터를 탈취하며, 몸값을 지불하지 않으면 데이터를 유출

이중 랜섬웨어 공격에 FBI 경고

- FBI, 두 개 이상의 랜섬웨어가 한 번의 공격으로 동시에 타격하는 이중 랜섬웨어 공격에 대해 경고
- 피해를 두 배로 만들어 방어 및 대응을 어렵게 만듦
- 랜섬웨어 공격자들은 피해자의 몸값 지불에 대한 압력을 가하기 위해 데이터를 손상시키거나 삭제하기도 함

Knight 랜섬웨어 배포로 제기되는 Qakbot의 부활 의혹

- Qakbot이 폐쇄되었다고 알려졌으나, 최근 스팸 메일을 통해 계열사가 활동하는 정황 포착
- 인프라와 계열사가 잔존해 있어 부활 가능성 제기

우크라이나 핵티비스트 단체, Trigona 랜섬웨어 폐쇄

- 우크라이나 핵티비스트 단체는 Trigona 랜섬웨어 그룹의 데이터를 탈취 후 폐쇄 시킴
- Trigona는 22년 10월에 등장하여 활발한 활동을 보이던 그룹

핵티비스트 그룹 GhostSec, GhostLocker 랜섬웨어 출시

- 핵티비스트 그룹 GhostSec과 SiegedSec은 GhostLocker RaaS를 제공
- Stormous와 같은 일부 랜섬웨어 그룹은 GhostLocker를 사용할 것이라고 선언
- 핵티비스트들은 자신들의 뜻을 선전하고 싶어하나 비용적인 문제로 사이버 범죄에 가담하기도 함

해킹 포럼에서 HelloKitty 랜섬웨어 소스 코드 유출

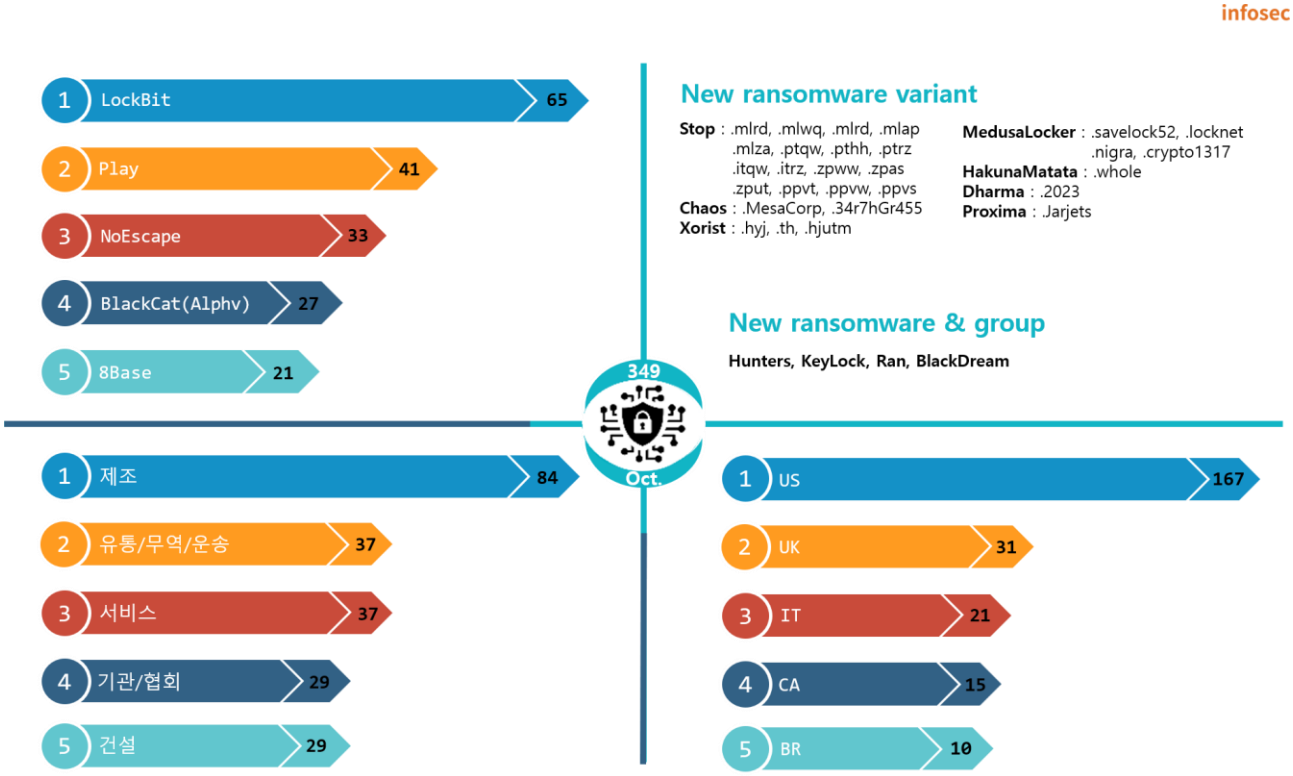
- HelloKitty 랜섬웨어 제작자는 초기 버전의 소스 코드를 공개
- 거기에 뛰어난 성능의 새로운 랜섬웨어를 개발 중이라고 주장
- 해당 제작자는 이전에도 랜섬웨어 소스 코드를 판매한 이력이 있음

SEIKO, BlackCat(Alphv)의 공격으로 인해 발생한 피해 사실 공개

- 올해 7월에 발생한 BlackCat(Alphv)의 SEIKO 공격으로 인해 고객 및 파트너 사의 데이터가 유출
- BlackCat(Alphy)은 IAB로부터 SEIKO의 초기 침투 경로 구매
- SEIKO는 향후 유사한 사고 발생 예방을 위해 보안을 강화할 것을 선언

* IAB(Initial Access Broker) : 초기 침투 경로를 판매하는 개인 혹은 집단

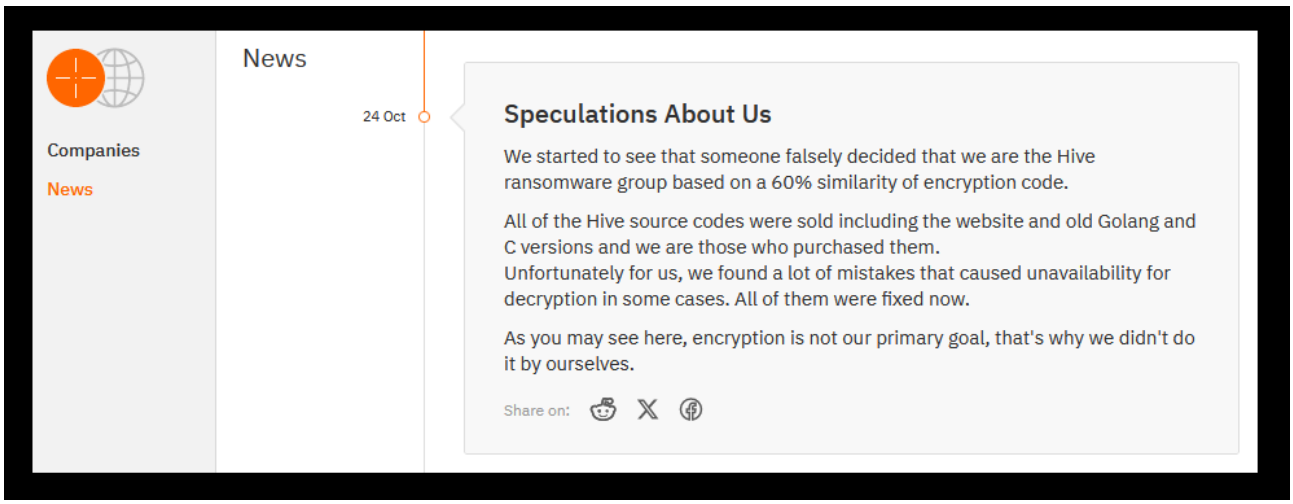
■ 랜섬웨어 위협



새로운 위협

이번 달에 새롭게 발견된 랜섬웨어 KeyLock 과 BlackDream 랜섬웨어는 AES 알고리즘을 사용하여 파일을 암호화하고 사용된 키를 RSA 알고리즘으로 암호화한다. 이후 VSC[5] 삭제를 통해 시스템 복구를 어렵게 만든 뒤 금전을 요구하는 특징을 가지고 있다. Ran 랜섬웨어는 하드코딩 된 Base64 값(“This.Is.For.petrolimex.com.vn.2023”)을 키로 사용하여 AES 알고리즘을 통해 파일을 암호화한다. 이 때 암호화에 사용되는 키 값이 하드코딩 되어있으므로 복호화가 가능하다는 특징이 있다. Ran 랜섬웨어와 앞서 설명한 KeyLock 은 15 년 8 월에 발견된 HiddenTear 계열의 랜섬웨어라는 공통점을 가지고 있다. HiddenTear는 교육 목적으로 공개된 오픈소스 프로젝트이지만 공격자들이 악용하여 아직까지도 변종이 쏟아져 나오고 있다. BlackDream 은 20 년 1 월에 발견된 WannaScream 계열의 랜섬웨어로 WannaScream 은 DarkCrypt 랜섬웨어로도 알려져 있으며 Harma, FOB, Snc, AWT 등의 랜섬웨어와 같은 계열에 속해 있다.

[5] VSC(Volume Shadow Copy) : Windows 시스템에서 파일이나 폴더의 백업 복사본을 생성하여 데이터가 손상되거나 삭제될 경우 이전 상태로 복원할 수 있는 기능

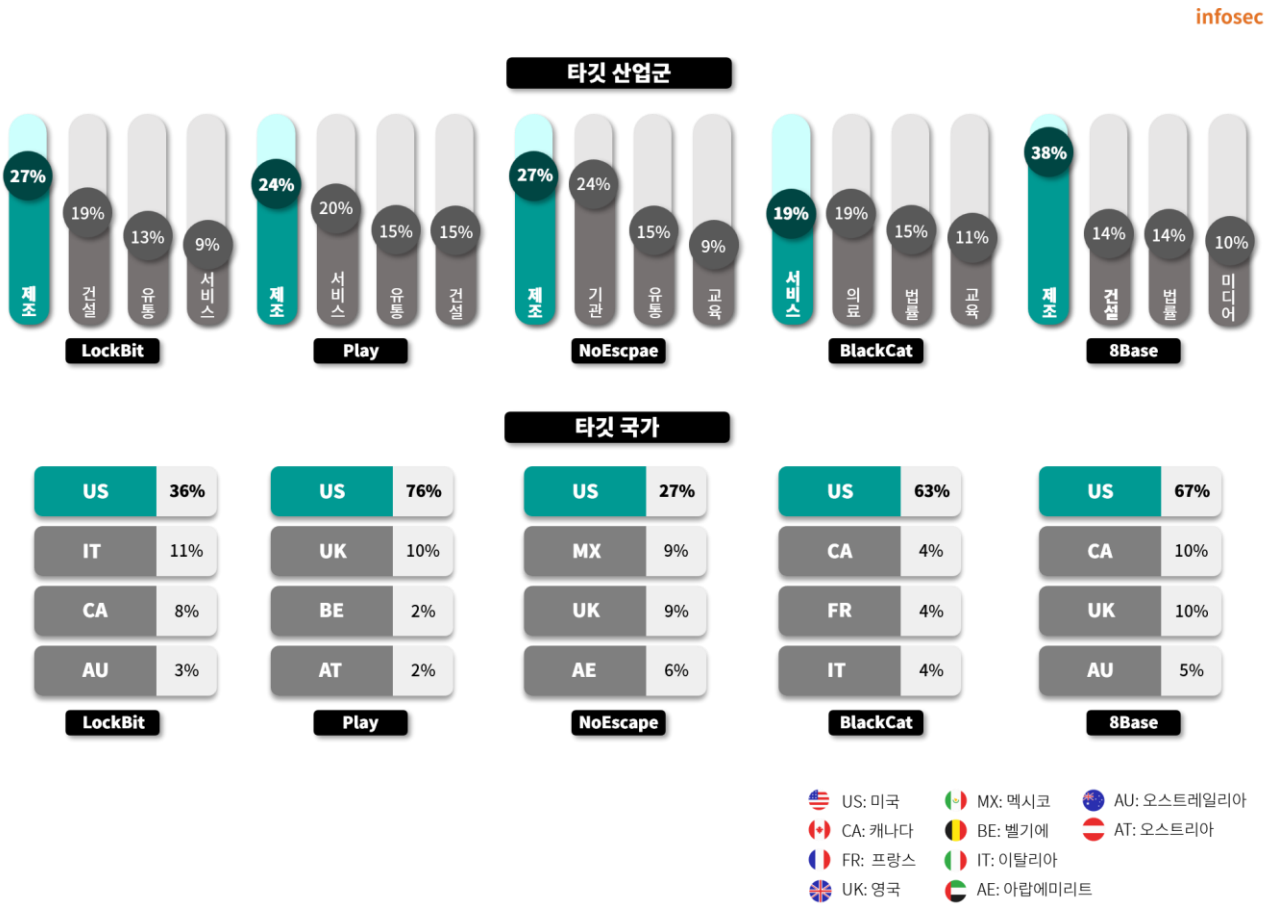


* 출처 : Hunters International 다크웹 유출 사이트

이번 달 발견된 신규 랜섬웨어 그룹 중 Hunters International(이하 Hunters) 랜섬웨어 그룹은 올해 초 폐쇄된 Hive 의 리브랜딩이라는 의혹이 제기되고 있다. Hunters 와 Hive 간의 소스 코드 유사도가 약 56%이고, 암호화 루틴이 상당히 유사하여 의심스러운 상황이다. 이러한 논란을 의식하기라도 한 듯, Hunters 는 다크웹 유출 사이트에 "세간의 추측은 틀렸으며, 단지 Hive 가 판매한 소스 코드를 구매했을 뿐이다."라는 취지의 짧은 글을 게시했다.

Hive 랜섬웨어 그룹은 러시아에 기반을 둔 RaaS 그룹으로, 2021 년 등장한 이후 전 세계 1,500 건 이상의 피해 사례를 야기해 1 억 달러(약 1,295 억 원) 이상의 범죄 수익을 거뒀다. 특히, Hive 는 의료계 뿐만 아니라 중요 인프라 등을 타깃으로 삼으며 광범위한 활동을 펼쳐 많은 피해를 발생시켰다. 이러한 영향력으로 인해 발 빠르게 국제 공조가 이루어져 올해 1 월 말에 폐쇄되는 결말을 맞이한 것으로 알려졌다. 그러나, Hunters 가 Hive 와 유사한 구조의 랜섬웨어를 가지고 등장하여 혼란이 야기되고 있다. Hive 가 Hunters 와 소스코드 및 인프라를 비밀리에 거래했을 가능성도 있으나, 일반적인 RaaS 그룹들은 딥웹, 다크웹 포럼, 텔레그램 등에서 계열사를 구하거나 거래 글을 올리는 등의 방식으로 활동하는데 Hive 는 게시한 소스코드 게시글이나 흔적 등은 발견되지 않아 의문을 자아내고 있다. 따라서 Hunters 의 향후 행보가 두 그룹 간의 관계성을 풀어낼 수 있는 단서가 될 것으로 보인다.

Top5 랜섬웨어



LockBit 은 다양한 기업의 유출 데이터를 게시하며 이번 달 가장 많은 피해 사례를 발생시킨 랜섬웨어 그룹이다. 특히 세계 최대 항공기 제작 회사인 Boeing 의 데이터를 탈취했다 밝히고 몸값을 요구해 화제가 됐다. 한때 LockBit 의 유출 사이트에 Boeing 에 대한 게시글이 삭제된 바 있었고, Boeing 측은 비행 안전에 대한 영향은 없다고 밝혀 문제가 없는 듯 했으나, 이후 Boeing 의 홈페이지에 접속했을 시에 기술적 이슈로 홈페이지가 다운되었다는 메시지를 확인할 수 있었다. 또한 협상이 결렬된 탓인지 LockBit 은 11 월 10 일자로 Boeing 의 것으로 추정되는 43GB 상당의 데이터를 유출 사이트에 게시하여 실질적으로 Boeing 측이 공격을 당한 것으로 파악된 상황이다.

Play 는 꾸준한 활동을 보이는 랜섬웨어 그룹 중 하나로 알려져 있다. 이번 달에도 예외 없이 다수의 기업 데이터를 유출했는데, 그중 미국 텍사스의 댈러스 카운티에 대한 데이터를 탈취했다고 주장하며 논란이 일고 있다. 댈러스는 텍사스에서 인구가 두 번째로 많은 카운티로 약 200 만 명의 주민이 살고 있는 큰 도시다. Play 는 댈러스의 기밀문서를 탈취했다고 주장하는 글을 게시했다.

지난 5 월 댈러스는 Royal 의 타깃이 되어 3 만 명 이상의 개인정보가 유출된 사건이 있었다. 당시 복구기간만 약 5 주가 걸렸으며, 복구비용 역시 약 850 만 달러(한화 약 110 억)에 달하는 등 상당한 피해를 입은 것으로 알려졌다. 200 만 명 이상의 시민이 거주하고 있는 대규모 도시임에도 불구하고 두 차례나 랜섬웨어 사고가 발생한 것으로 보아 댈러스는 보안에 있어 취약한 부분을 점검하고 조치하는 대처가 부족했던 것으로 보인다. 만약 이번 사태의 유출 데이터에 시민들의 개인 정보가 포함되어 있다면 댈러스 시민들은 이를 악용한 추가 범죄에 노출될 수 있어 피해를 최소화하기 위해서는 신속한 사태 파악 및 대응이 필요하다.

NoEscape 는 지난 6 월 활동을 개시한 랜섬웨어 그룹으로, Avaddon 랜섬웨어 그룹의 리브랜딩이다. 개시 이후 이들의 활동 양상을 살펴보면, 다크웹에 게시하는 유출 데이터의 건수가 매월 증가하는 양상을 보이고 있어 등장 이후 4 개월이라는 기간에 비해 끼치는 영향력은 상당한 그룹이라고 할 수 있다. 특히, 최근에는 국내 한 기업을 대상으로 145GB 상당의 데이터를 탈취했다고 밝히며 협상에 응하지 않으면 큰 피해가 있을 것이라는 협박성 문구를 포함한 글을 게시했다. 해당 글에는 기업이 추진 중인 프로젝트 관련 문서, 데이터베이스, 계약서 등이 포함된 유출 데이터가 노출됐다. 또한 이들은 프랑스의 한 농구 팀에 대해 공격을 수행했다고 주장하며 선수들의 개인 정보와 여권을 비롯한 신분증 등 32GB 의 문서를 탈취 후 공개하기도 했다.

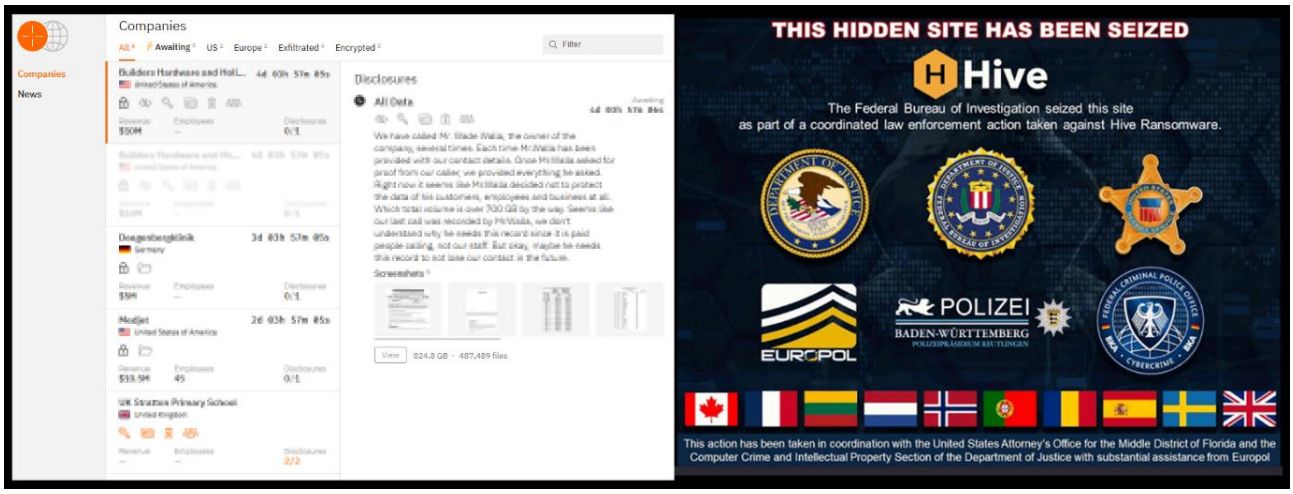
BlackCat(Alphv)도 꾸준히 활동을 이어오고 있는 랜섬웨어 그룹으로 호텔, 의료계, 금융업, 제조업 등 다양한 분야에 대해 공격을 지속적으로 수행하고 있다. 특히, 이들은 지속적으로 랜섬웨어 변종을 개발하고 있으며 다양한 도구들을 활용하여 공격을 수행하고 있다는 특징이 있다. 최근에는 Munchkin 이라는 이름의 Virtual Box ISO 파일[6]을 공격에 사용한 것으로 확인됐다. 이 공격은 초기 침투를 수행한 후 각종 스크립트와 유틸리티가 포함된 Munchkin 을 통해 새로운 가상머신을 생성하여 비밀번호 탈취, 네트워크 전파, 랜섬웨어 배포 절차로 진행된다. ISO 파일을 이용하기 때문에 용도 및 대상에 따라 쉽게 조정이 가능하여 다양한 공격을 펼칠 수 있다는 특징이 있다. 이는 BlackCat(Alphv)의 전략이 나날이 발전해 나가고 있다는 것을 알 수 있는 대목이다.

8Base 는 지난해 4 월부터 활발한 활동을 보이고 있는 그룹으로, 이번 달에만 21 건의 피해 사례를 게시하여 영향력을 과시하고 있다. 특히, 이들은 Phobos 계열의 랜섬웨어를 사용하여 제조 업계를 중심으로 집중적으로 공격을 수행하고 있는 정황이 확인됐으며, 미국을 주된 타깃으로 삼아 집중 공격을 펼치고 있는 것으로 확인됐다.

[6] Virtual Box ISO 파일 : 가상 머신에서 운영 체제를 설치하기 위해 사용되는 디스크 이미지 파일

■ 랜섬웨어 집중 포커스

Hunters 랜섬웨어 개요



* 출처 : Hunters International, Hive 다크웹 유출 사이트

Hunters 랜섬웨어는 Hunters International 그룹이 사용하는 랜섬웨어로, Hive v6 의 샘플과 약 56% 정도의 소스코드 유사도를 띠고 있다. Hunters 그룹은 랜섬웨어 공격의 주목적을 암호화가 아닌, 피해자들에게 몸값을 요구하기 위한 데이터 탈취에 초점을 맞추고 있다. 이들은 피해자들의 몸값 지불을 재촉하기 위해 미국의 성형외과를 공격하여 탈취한 환자들의 수술 전 사진을 유출하는 등 공격적인 전술을 사용하고 있다. 또한, 이들은 몸값 지불을 서두르게 하기 위해 병원 환자들에게 대량의 이메일을 전송할 계획 중이라고 밝히기도 했다. 이 공격 방법은 과거 BlackCat(Alphv) 그룹이 암 환자의 사진을 유출시켜 도덕적으로 비난받았던 사례와 유사하다.

일반적으로 랜섬웨어 그룹들은 도덕적으로 문제가 될 수 있는 행위나 생명에 지장을 줄 수 있는 공격은 사법 기관에 적발될 가능성이 높아 피하는 경향이 있다. 특히 LockBit 의 경우 관련 규정을 엄격하게 설정하여 이를 준수하지 않는 계열사를 제명하고 있다.

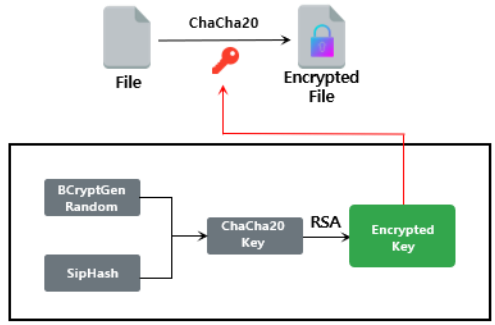
한편, 지금은 폐쇄된 Hive 그룹은 의료계에 공격하는 것을 서슴지 않는 모습을 보이기도 하여 논란이 되었는데, 최근 Hive 의 리브랜딩 의혹을 사고 있는 Hunters 역시 마찬가지의 행보를 보이고 있어 소스 코드 유사도와 더불어 충분히 연관성을 의심할 수 있는 단서가 추가적으로 확인되고 있다.

Hunters 그룹은 암호화 대신 데이터 탈취가 자신들의 주목적이기에 자체 랜섬웨어를 개발하지 않고 RaaS 로 판매되었던 Hive 의 소스 코드와 인프라를 구매한 것이라고 주장하고 있다. 그러나, Hive v6 와의 높은 코드 유사성을 비롯해, 랜섬노트에 기재된 다크웹 사이트의 백엔드 코드가 이전 Hive 가 사용하던 것과 거의 동일하고, 특정 업계에 공격을 치중되지 않는 행동 등이 Hunters 가 Hive 의 리브랜딩일 가능성에 대한 의심을 더욱 강화시키고 있다.

Hunters Ransomware

암호화 키

ChaCha20으로 파일 암호화를 수행하고 RSA로 키를 암호화

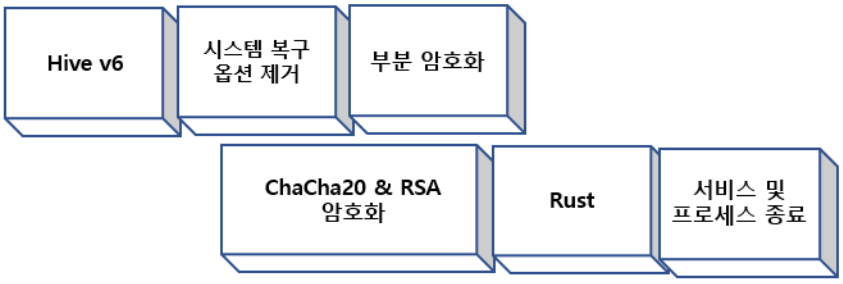


암호화 방식

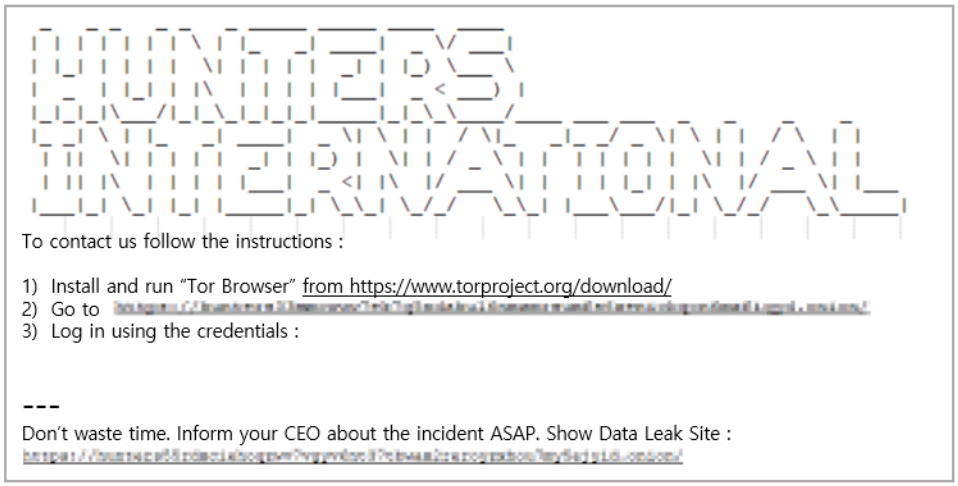
파일 크기 5.25MB 이상 : 최초 54Byte 제외하고 파일 크기의 10% 암호화 후 남은 파일 크기의 10%에 대해 파일 끝부분 암호화

파일 크기 5.25MB 이하 : 최초 54Byte 제외한 파일 전체 암호화

특징



랜섬노트



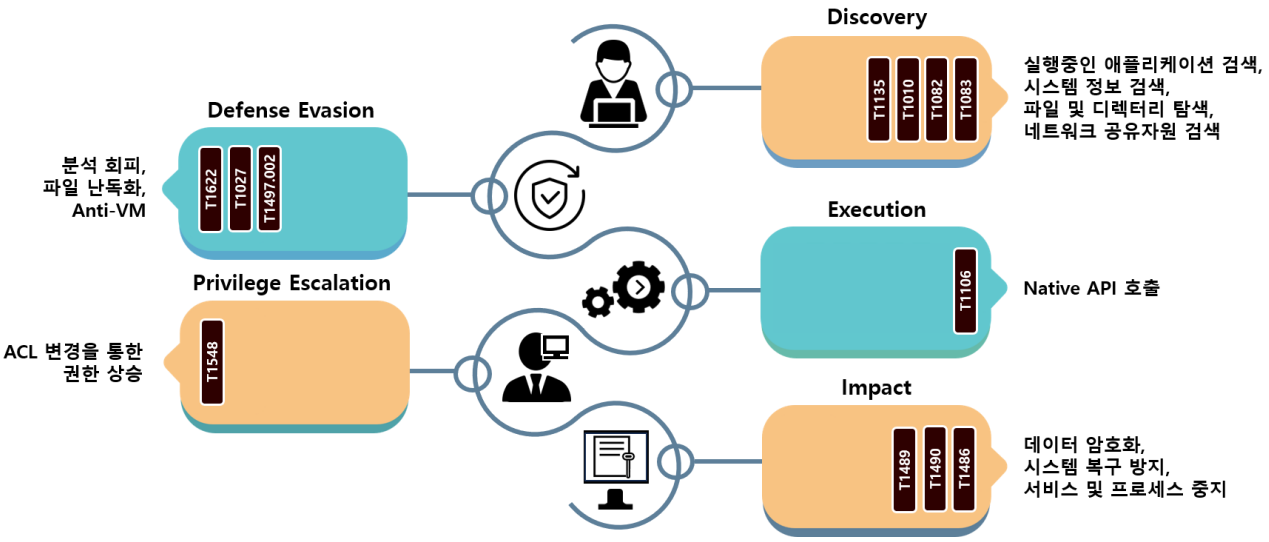
Contact Us.txt

변경 확장자

.locked

제작 언어

Rust



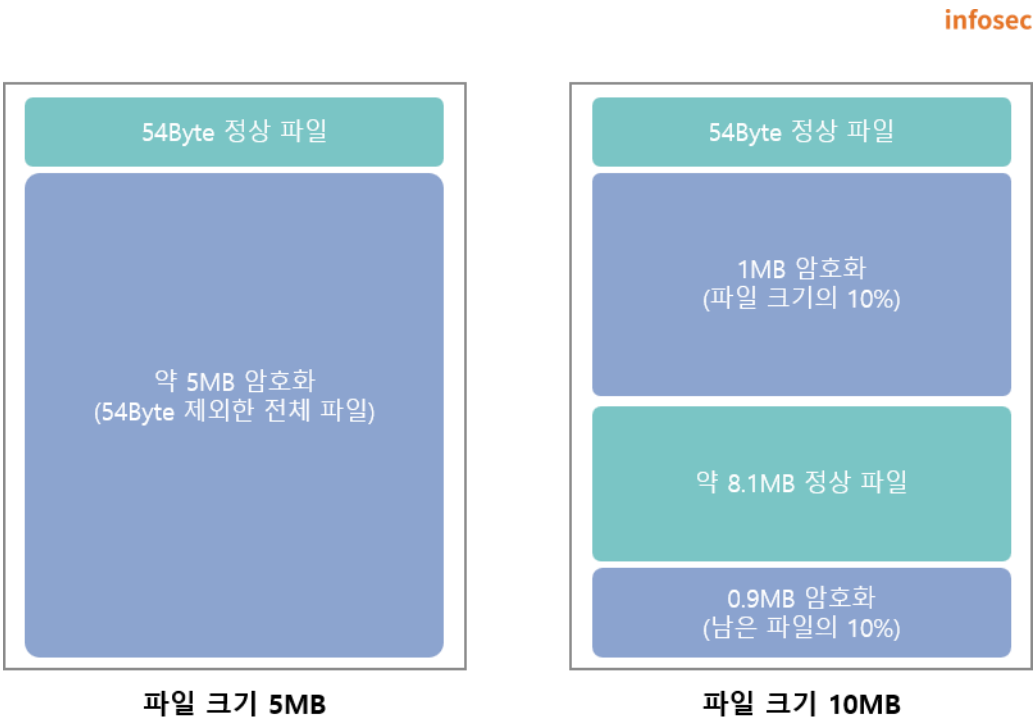
Hunters 랜섬웨어는 랜섬웨어 공격을 위해 다양한 기술적 전략을 사용하고 있다. 먼저, 시스템 정보 검색을 통해 실행 중인 애플리케이션을 파악하고 네트워크 공유자원을 비롯한 각종 파일 및 디렉터리를 탐색하여 실행 중인 파일 또한 암호화시키기 위한 목적으로 특정 서비스 및 프로세스를 종료한다.

내부에서 사용하는 문자열은 난독화되어 있으며, 실행 중에 연산을 통해 난독화를 해제하는 방식으로 구성되어 있어 시그니처 기반의 탐지를 회피하는 전략을 사용하고 있다. Native API[7]를 사용하게 된다면 시퀀스 및 시그니처 패턴이 Windows API[8]를 사용할 때와 달라져 보안 솔루션이 이를 탐지하기가 어려워지므로 Hunters 는 Native API 사용을 통해 탐지를 회피하는 방식을 적용했다.

[7] Native API : Windows 운영 체제의 핵심 기능에 접근하는 LowLevel API

[8] Windows API : 개발자들이 사용하기 쉬운 고수준 인터페이스를 제공하는 API

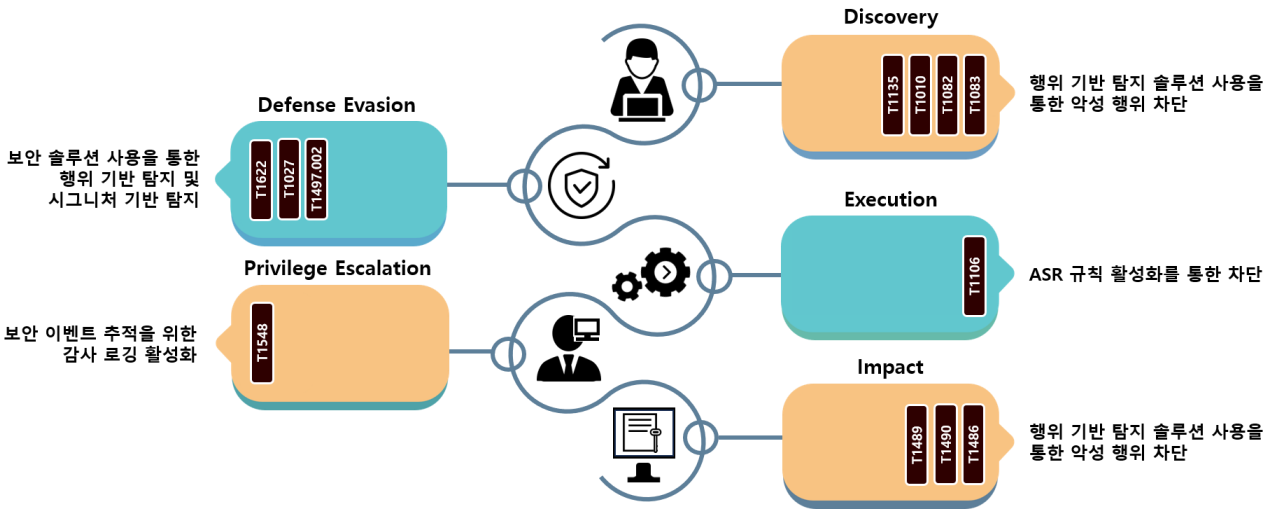
또한, Hunters 랜섬웨어는 악성코드 분석이 가상 환경에서 이루어진다는 특성을 악용하여 가상 머신에서 사용하는 파일의 존재 유무를 탐색하는 Anti-VM 기법을 적용하는 치밀함을 보였다. 데이터 암호화를 수행할 시에 여러 시스템 파일에 접근하기 위해서 ACL[9] 변경을 통해 권한을 상승시켜 암호화 작업을 수월하게 만들었으며, 사용자가 만일 백업 파일이나 VSC 를 설정했을 경우를 대비하여 해당 요소들을 삭제하여 시스템을 복구할 수단을 제거하는 작업을 수행한다.



[그림] 파일 크기에 따른 암호화 과정 예시

이후 암호화를 수행할 때는 빠른 암호화 속도를 위하여 파일의 크기에 따라 암호화 방식을 다르게 적용하고 있다. 파일 크기가 5.25MB 이하일 경우에는 파일 앞 부분의 54Byte 를 제외한 다음 부분부터 파일의 끝부분까지 전체를 암호화하고, 만약 파일의 크기가 5.25MB 이상일 경우라면 마찬가지로 파일 앞 부분의 54Byte 를 제외한 다음 부분부터 파일 크기의 10%에 해당하는 크기만큼 암호화를 수행하고 남은 파일의 크기에 대해서 또다시 10%만큼의 크기에 대해 파일 끝부분을 암호화시키는 작업을 수행한다.

[9] ACL(Access Control List) : 파일이나 디렉터리에 대한 접근 권한을 세밀하게 제어하기 위해 사용자나 그룹별로 접근 권한을 지정하는 보안 메커니즘



Hunters 랜섬웨어는 비주류 언어인 Rust 로 제작되었으나, 대부분의 행위 기반 보안 솔루션을 활용하여 탐지하고 예방할 수 있다. Native API 사용을 통한 탐지 우회는 ASR[10] 규칙 활성화를 통해 악성코드의 행위를 차단하는 방법 또한 적용시킬 수 있다.

권한 상승 시에는 ACL 변경이 수행되므로 이때 발생하는 보안 이벤트를 기록할 수 있는 감사 로깅 정책을 활성화시키는 것을 통해 추후 사고 조사에 도움을 줄 수 있다. 또한, Hunters 는 시스템 백업 본과 VSC 를 삭제하므로 데이터가 암호화될 경우를 예방하기 위해 공격자가 쉽게 접근하기 어려운 원격지에 소산 백업[11]을 하는 것을 권장한다. 백업 중이 아닐 경우에는 백업 시스템이 꺼져 공격자의 접근을 차단하는 기술 등이 적용된 보안 백업 시스템 사용을 권장한다.

마지막으로 Hunters 는 네트워크 공유 자원까지 암호화시키므로 랜섬웨어 감염이 의심되면 해당 시스템을 네트워크에서 분리 조치하여 추가 감염을 예방해야 한다. 더불어 네트워크 공유 자원 접근 권한을 최소화하여 필요한 리소스에만 접근할 수 있도록 조치를 취해야 한다. 랜섬웨어에 감염되는 것은 큰 피해를 야기할 수 있으므로 이러한 대응 방안이 적용되었는지 환경을 점검하여 미흡한 부분에 대하여 조치를 취할 것을 권장한다.

[10] ASR(Attack Surface Reduction) : 악성코드의 공격 경로를 차단하는 규칙

[11] 소산 백업(Vaulting Backup) : 백업 데이터를 로컬 시스템과 물리적으로 멀리 떨어진 곳에 보관하는 것

■ 참고 사이트

URL : https://thehackernews.com/2023/10/qakbot-threat-actors-still-in-action.html

URL : https://www.bleepingcomputer.com/news/security/hellokitty-ransomware-source-code-leaked-on-hacking-forum/

URL : https://ransomware.org/blog/fbi-issues-warning-on-dual-ransomware-attacks/

URL : https://www.scmagazine.com/brief/play-ransomware-attack-confirmed-by-dallas-county

URL : https://www.infosecurity-magazine.com/news/boeing-lockbit-ransomware-breach/

URL : https://therecord.media/white-house-counter-ransomware-initiative-summit-new-measure

URL : https://thehackernews.com/2023/10/pro-hamas-hacktivists-targeting-israeli.html?&web_view=true

URL : https://www.bleepingcomputer.com/news/security/new-hunters-international-ransomware-possible-rebrand-of-hive/

URL : https://www.theregister.com/2023/10/25/rebuilt_hive_ransomware_gang_stings/

URL : https://www.darkreading.com/threat-intelligence/ragnar-locker-ransomware-boss-arrested-paris

URL : https://cybersecuritynews.com/blackcat-hacker-tool-remote-machines/

URL : https://www.bleepingcomputer.com/news/security/ukrainian-activists-hack-trigona-ransomware-gang-wipe-servers/