Keep up with Ransomware

빠르게 진화하는 Vanhelsing 랜섬웨어

■ 개요

2025 년 3 월 랜섬웨어 피해 사례 수는 지난 2 월(1067 건)에 비해 약 28% 감소한 773 건을 기록했다. 3 월에 피해 사례가 감소한 이유는 Clop 그룹이 Cleo 의 파일 전송 솔루션 취약점을 악용하여 발생시킨 피해자를 2 월에 모두 공개했기 때문이다. 지난달에 비해 감소했지만 773 건은 평균적으로 높은 수치이며, 이러한 이유는 다수의 신규 랜섬웨어 그룹이 등장하고 활동하기 때문이다.

3 월에도 국내 랜섬웨어 위협이 확인됐다. NightSpire 그룹은 3 월에 새로 등장한 그룹으로 3 월에만 15 건의 피해자를 게시했으며, 그 중에는 국내 영상 콘텐츠 제작 업체가 포함되어 있었다. 공개한 샘플 데이터는 해당 업체에서 제작한 드라마의 대본 1 회분이었으며, 공개 예정일이 지났음에도 전체 데이터는 공개되지 않은 상태다. 4 월 기준으로 다크웹 유출 사이트는 비활성화 됐다.

BlackLock 을 운영하는 그룹이 Mamona 라는 신규 랜섬웨어 서비스를 발표했다. BlackLock 은 23 년 9 월에 LostTrust 로 처음 등장했으며, 이후 24 년 6 월에 ElDorado, 24 년 9 월에는 BlackLock 으로 리브랜딩한 그룹이다. 이들은 BlackLock 과 별개로 Mamona RIP 이라는 신규 그룹을 만들어 러시아 해킹 포럼에 홍보하기 시작했으나, Mamona 서버의 보안 설정이 미흡하여 Mamona 의 다크웹 유출 사이트가 해킹되고 BlackLock 의 유출 사이트는 비활성화되는 일이 발생했다. 현재는 BlackLock 의 유출 사이트만 접속이 가능한 상태이다.

RansomHub 랜섬웨어가 최근 SocGholish(FakeUpdates)라는 멀웨어 서비스 프레임워크를 통해서 배포된 정황이 확인됐다. SocGholish 는 2018 년에 등장했으며, 정상적인 웹사이트에 악성 스크립트를 주입한 뒤 사용자의 트래픽을 하이재킹하는 방식을 사용한다. 사용자가 해당 웹사이트를 방문하면 브라우저 업데이트 알람으로 위장한 가짜 페이지에 접속하게 되고, ZIP 형태로 압축된 SocGholish 스크립트 파일을 다운로드 하도록 유도한다. 사용자가 해당 스크립트 파일을 실행하게 되면 공격자는 데이터 탈취나 원격 명령 실행이 가능해지며, 이를 통해서 RansomHub 랜섬웨어를 배포한 것으로 확인됐다.

Akira 그룹이 최근 웹캠을 활용해 랜섬웨어 공격에 성공한 사례가 확인됐다. Akira 그룹은 자신들이 주로 사용하는 전략인 취약한 원격 접속 솔루션에 노출된 자격 증명을 이용하거나 무차별 대입을 통해서 시스템에 침입한 다음 랜섬웨어 페이로드 배포를 시도했다. 하지만 랜섬웨어 배포 행위가 EDR[1] 솔루션에 의해 차단되어 EDR 솔루션 우회를 위해 접근 가능한 시스템 중에서 취약한 웹캠을 식별했고, 웹캠에는 EDR 솔루션이 존재하지 않는다는 점을 이용해 원격 쉘 접근을 통해 랜섬웨어를 배포했다.

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

■ 랜섬웨어 뉴스

RansomHub 그룹, SocGholish 멀웨어 서비스를 이용한 랜섬웨어 배포

- SocGholish는 정상 웹사이트에 스크립트를 삽입하여 사용자의 트래픽을 가로채는 방식
- 감염된 웹사이트에 방문하면, 브라우저 업데이트로 위장한 SocGholish 스크립트를 다운 및 실행하도록 유도
- 파일 실행 시 공격자는 데이터 탈취나 원격 명령 실행이 가능

Akira 그룹, 웹캠을 활용해 랜섬웨어 공격 성공

- EDR 솔루션을 우회하기 위해 초기 침투 이후 네트워크에 연결된 웹캠을 통해서 랜섬웨어 페이로드 배포
- 웹캠으로 원격 쉘 접근이 가능하며, EDR 솔루션이 존재하지 않는 점을 이용

북한 위협 그룹 Moonstone Sleet, Qilin 랜섬웨어 배포 정황 발견

- Moonstone Sleet은 자체 제작 랜섬웨어인 FakePenny 랜섬웨어를 배포한 이력이 있는 그룹
- 25년 2월 말부터 Qilin 랜섬웨어를 배포하기 시작

Mamona 랜섬웨어 서비스, DragonForce 그룹에 의해 해킹

- Mamona는 BlackLock으로 알려진 그룹이 새로 공개한 랜섬웨어 서비스
- 미흡한 보안 설정으로 인해 관리자 페이지 및 패널이 노출
- Mamona의 다크웹 유출 사이트는 DragonForce에 의해 해킹당했으며, BlackLock DLS는 비활성화
- 해킹 이후 약 2주 뒤, BlackLock DLS 복구

신규 Vanhelsing 그룹 파트너 모집

- 러시아 해킹 포럼 Ramp 포럼에서 RaaS 파트너를 모집하는 글 게시
- 출시 3주만에 공격 대상 플랫폼 확대
- 약 한달간 총 8명의 피해자 게시

신규 NightSpire 그룹, 국내 영상 콘텐츠 제작 업체 공격

- 3월에만 15건의 피해자를 게시했으며, 그 중에는 국내 영상 콘텐츠 제작 업체 포함
- 샘플 데이터로 업체에서 제작한 드라마의 대본 1회분 공개
- 데이터 공개 기한이 지났음에도 전체 데이터 공개되지 않은 상태

Mimic 랜섬웨어 v.10 업데이트 공개

- RAMP 포럼을 통해서 업데이트 내용 공개 및 파트너 모집 시작
- 랜섬웨어 서비스를 이용할 파트너 외에도, 초기 침투 전문가와 광고 담당자 등 함께 일할 구성원도 모집

신규 랜섬웨어 Oxthief, skira, Crazyhunter 그룹 등장

- Oxtheif 그룹, 피해자 1건 게시 후 3월 중순부터 비활성화
- Skira 그룹, 피해자 5건 게시 후 3월 말부터 비활성화
- Crazyhunter 그룹, 피해자 10건 게시 후 4월부터 비활성화

그림 1. 랜섬웨어 동향

■ 랜섬웨어 위협

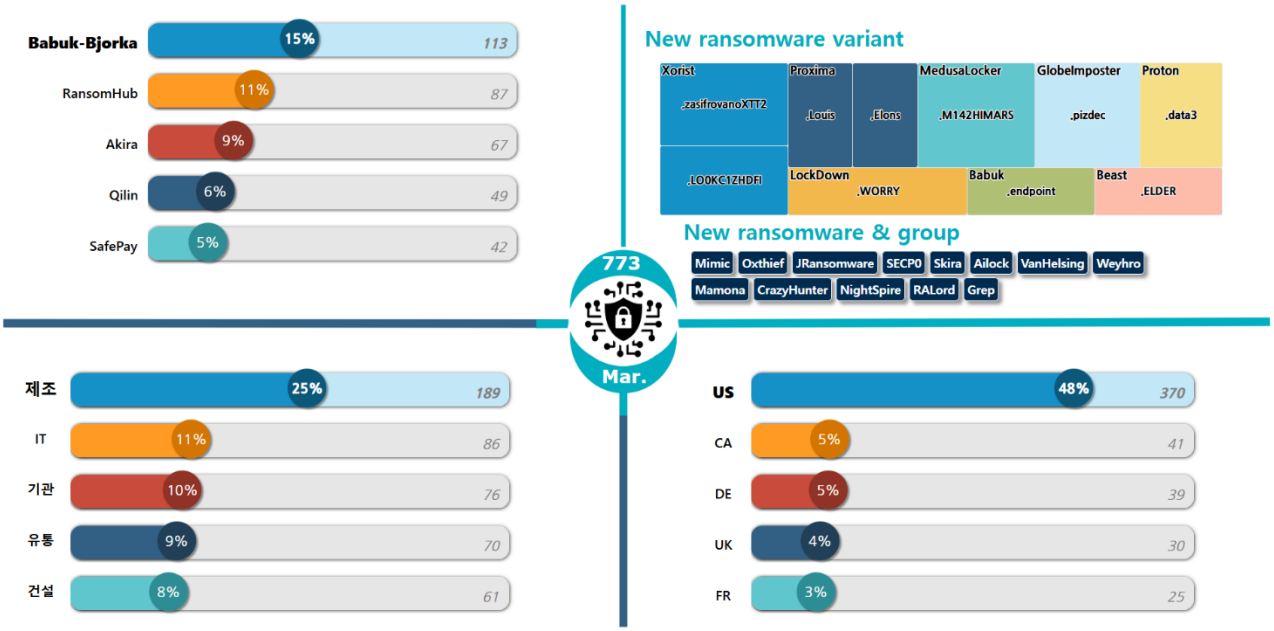


그림 2. 2025 년 3 월 랜섬웨어 위협 현황

새로운 위협

3 월에는 기존 랜섬웨어 그룹의 업데이트 소식도 확인됐으며 다수의 신규 랜섬웨어 그룹이 발견됐다. 총 6 개의 신규 랜섬웨어 그룹이 확인됐으며, 그 중 3 개의 그룹 Oxthief, Skira, CrazyHunter 는 4 월을 기준으로 현재 접근이 불가능한 상태이다. Oxtheif 그룹과 Skira 그룹의 경우 3 월 초 등장해 각각 1 건, 5 건의 피해자를 업로드했으나, 3 월부터 다크웹 유출 사이트가 비활성화 됐으며, CrazyHunter 의 경우 4 월에 다크웹 유출 사이트가 비활성화 됐다.

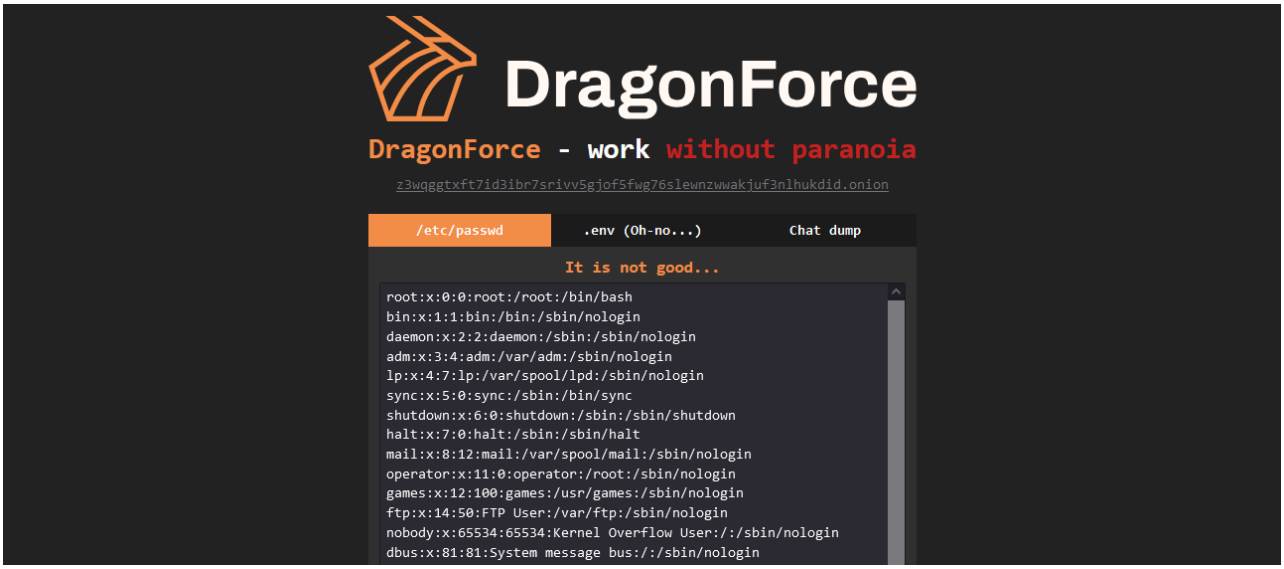


그림 3. DragonForce 에 의해 해킹된 Mamona 다크웹 유출 사이트

BlackLock 을 운영하는 그룹이 공개한 Mamona 라는 신규 랜섬웨어 서비스의 보안 설정이 미흡하여 Mamona 관리자 페이지는 물론 관리 패널이 노출됐다. 러시아 해킹 포럼에서 해당 이슈가 공유되어 포럼 유저들이 서비스에 무단으로 접근하거나 데이터를 조회할 수 있었으며, BlackLock 의 유출 사이트는 비활성화 되고 DragonForce 그룹이 Mamona 의 다크웹 유출 사이트를 변조하기도 했다. 약 2 주 뒤 BlackLock 은 비활성화된 다크웹 유출 사이트를 복구했으며, Mamona 는 더 이상 운영되지 않고 있다.

러시아 해킹 포럼에서 자신들의 랜섬웨어 서비스를 홍보하는 신규 그룹도 1 개 확인됐다. Vanhelsing 그룹은 3 월 초 러시아 해킹 포럼에서 자신들의 RaaS[2] 를 이용할 파트너를 모집하기 시작했으며, 출시한지 3 주만에 공격 대상 플랫폼을 추가했다. 또한 이들은 한 달간 8 명의 피해자를 게시했다.

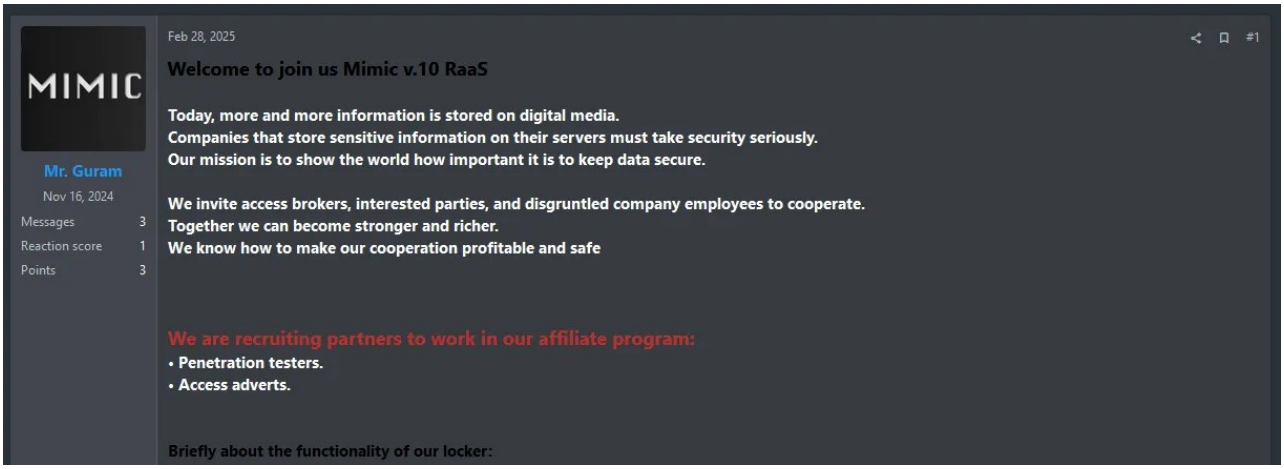


그림 4. Mimic v.10 홍보글

22 년 6 월부터 활동한 것으로 알려진 Mimic 랜섬웨어가 v.10 버전을 출시했으며, 러시아 해킹 포럼에서 함께 일할 초기 침투 전문가와 접근 권한 광고 담당자를 모집하고 있다. 이들이 제공하는 랜섬웨어는 Windows, ESXi[3] ,NAS[4] ,FreeBSD[5] 와 같은 다양한 운영체제를 지원한다. 랜섬웨어 제공뿐만 아니라 피해자에게 협박 전화를 하는 서비스나, 각종 작업에 필요한 소프트웨어도 제공한다.

랜섬웨어 그룹이지만, 별도의 데이터 유출 사이트는 운영하지 않고 몸값 협상을 위한 채팅 페이지만 운영하는 그룹이 2 개 발견됐다. JRansomware 와 Ailock 그룹이 이에 해당한다. 이들은 랜섬노트에 채팅 페이지 주소와 로그인에 필요한 세션 ID 를 제공해 각 피해자 별로 채팅 페이지를 관리하고 있다.

[2] RaaS (Ransomware-as-a-Service): 랜섬웨어를 서비스 형태로 제공해서 누구나 쉽게 랜섬웨어를 만들고 공격할 수 있도록 하는 비즈니스 모델

[3] ESXi: VMware 에서 개발한 호스트 컴퓨터에서 다수의 운영체제를 동시에 실행시킬 수 있는 UNIX 기반의 논리적 플랫폼

[4] NAS: 네트워크를 통해 접근할 수 있는 다수의 저장장치가 연결된 스토리지

[5] FreeBSD: 유닉스 계열의 오픈 소스 운영체제

Top5 랜섬웨어

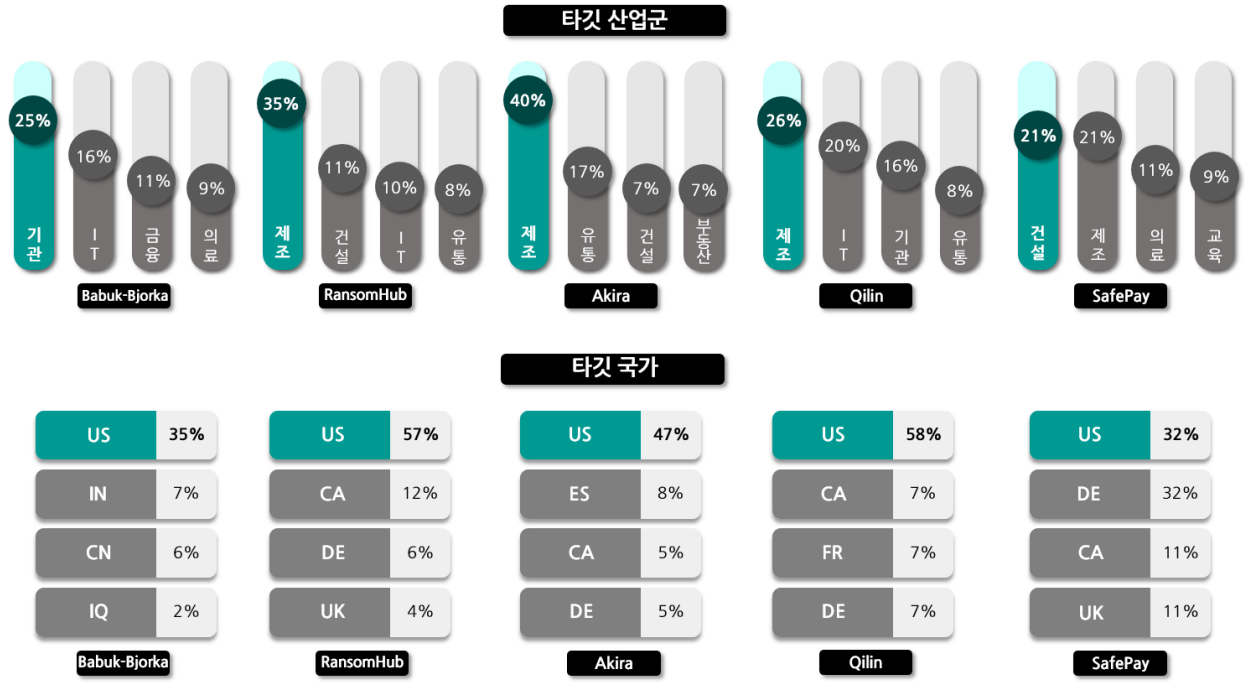


그림 5. 산업/국가별 주요 랜섬웨어 공격 현황

Babuk-Bjorka 그룹은 자신들이 Babuk2 라고 주장하는 그룹으로, 1 월부터 활동을 시작했다. 이들은 3 월에만 113 건의 피해자를 게시하며 가장 많은 활동을 보였는데, 다수의 피해자가 과거 RansomHub, Meow, Everest, Babuk, Funksec, LockBit 등 다른 그룹에 의해 데이터가 공개된 이력이 확인됐다. 따라서 이들이 실제로 해당 기업을 공격해 데이터를 탈취한 것인지, 아니면 이미 공개된 데이터를 재활용해 몸값을 요구하는 것인지 지켜볼 필요가 있다.

RansomHub 그룹은 말레이시아의 엔지니어링 서비스 기업 HexcoSys Group 을 공격해 계약서, 청사진, 소스 코드, 제품 개발 데이터가 포함된 336GB 데이터를 탈취했다. 또한 일본의 자동차 부품 제조 업체 Japan Rebuilt 를 공격해 생산 데이터와 재무 정보, 결제 세부 사항, 고객 기록이 포함된 200GB 의 데이터를 유출했다.

Akira 그룹은 3 월에 벨기에의 산업 기계 제조 업체 CS Plastics 를 공격해 감사 보고서, 재무 보고서와 같은 재무 데이터와 직원 및 고객의 개인정보가 포함된 민감한 데이터를 유출했다. 또한 최근에는 웹캠을 이용해서 EDR 솔루션의 탐지를 우회하는 등 새로운 공격 전략을 사용하는 모습도 확인됐다. Akira 그룹의 세부 공격 전략과 대응방안은 SK 쉴더스 KARA 랜섬웨어 동향 보고서 2024 4Q 에서 자세하게 확인할 수 있다.

Qilin 그룹이 최근 북한의 위협 그룹 Moonstone Sleet 과 연관이 있는 것으로 밝혀졌다. Moonstone Sleet 의 경우 이전에 자체 제작한 FakePenny 랜섬웨어를 배포한 이력이 있는 위협 그룹으로, 25 년 2 월 말부터 Qilin 랜섬웨어 페이로드를 배포한 정황이 확인됐다.

SafePay 그룹은 3 월 30 일에만 31 개의 피해자를 일괄적으로 게시했다. 영국의 하이 와이컴 소재의 중등학교 Sir Willian Ramsay School 는 이번 공격으로 183GB 에 달하는 데이터가 유출되었으며, 호주의 건설 계약 업체 Brighton Australia 는 재무 제표, 회계 기록, 인사 및 고객 파일이 포함된 160GB 데이터가 유출됐다.

■ 랜섬웨어 집중 포커스

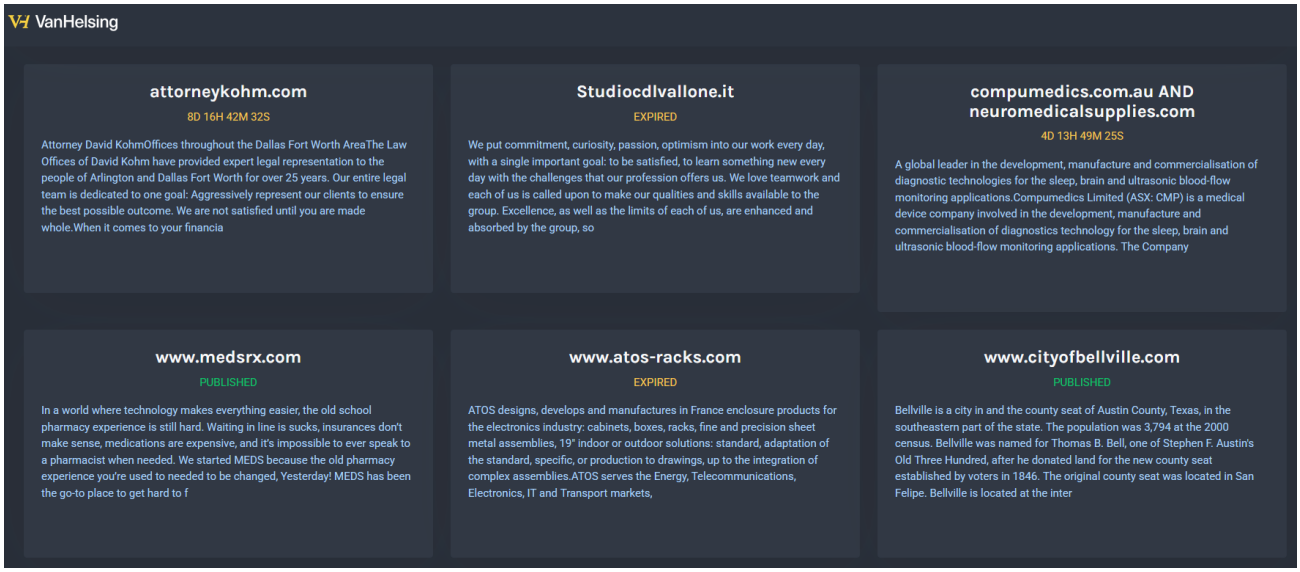


그림 6. Vanhesling 다크웹 유출 사이트

Vanhelsing 그룹은 3 월 7 일 등장한 랜섬웨어 그룹으로 러시아 해킹 포럼인 RAMP 포럼에서 계열사 모집을 시작했다. 이들은 어느정도 평판이 있는 사람은 별도의 가입 비용을 받지 않으며, 그 외에는 5,000 달러(한화 약 730 만원)에 해당하는 보증금을 지불해야 가입할 수 있는 형태이다. 포럼 홍보글에 따르면 이들은 CIS 국가에 대한 공격을 금지하고 있으며, 탈취한 몸값의 20%만 수수료로 요구하고 있다.

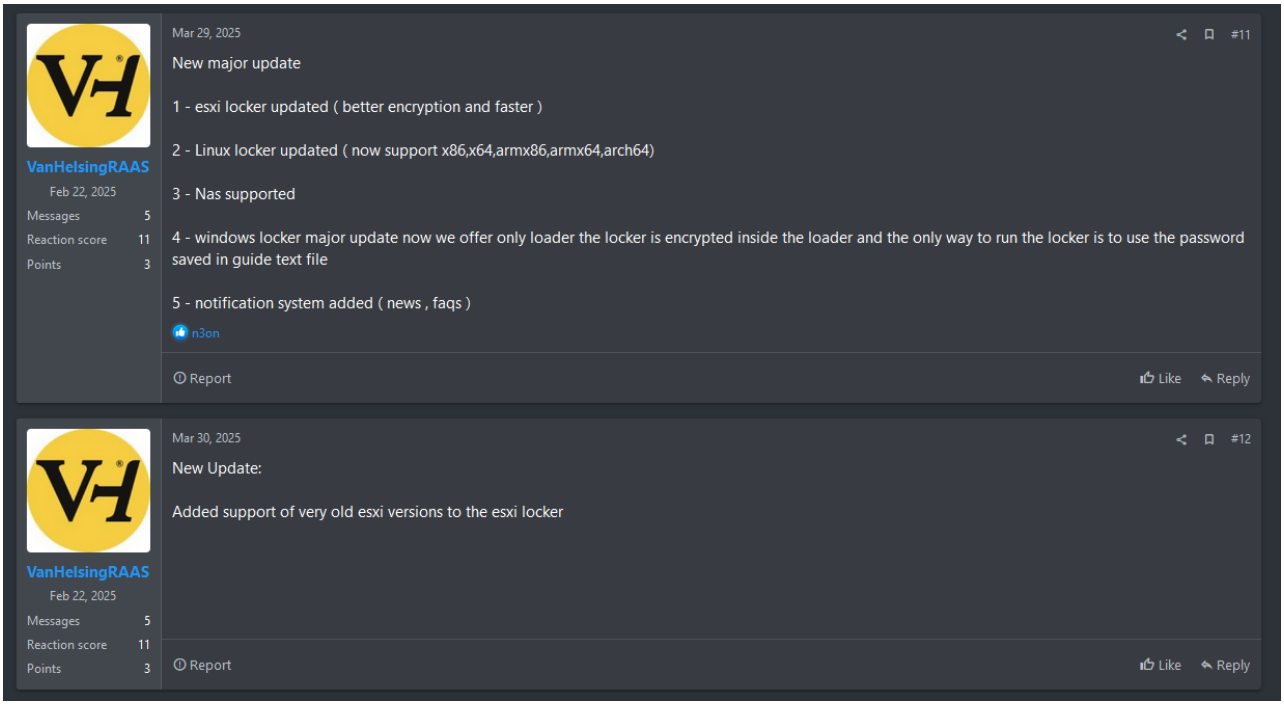


그림 7. Vanhelsing 기능 업데이트

출시 초기부터 이들은 Windows, Linux, BSD[6] , ARM[7] , ESXi 를 포함한 다양한 플랫폼을 대상으로 암호화를 지원한다고 소개했다. 3 월 말 운영자가 게시한 업데이트 내역에 따르면, Linux 와 ESXi 의 경우 더 다양한 버전과 아키텍처를 공격할 수 있으며, NAS 또한 공격 지원 대상에 추가됐다.

현재까지는 vanhelsing, vanlocker 라는 암호화 확장자를 사용하는 Windows 버전의 랜섬웨어만 확인됐다. 확인된 두 버전의 랜섬웨어는 약 5 일 간격으로 제작됐으며, 최신 버전에서는 기존에 없던 내부 네트워크 전파 기능이 추가됐다. 이 외에도 아직 기능이 구현되지는 않았지만, vCenter[8] 전파와 관련된 인자도 확인됐다. 랜섬웨어 기능이 빠른 속도로 업데이트되고 있을 뿐만 아니라, 랜섬웨어 홍보글에 따르면 향후 더 다양한 플랫폼을 대상으로 한 공격도 가능할 것으로 보인다. 이에 따라, 다가올 위협에 대비하기 위해 우선적으로 Windows 버전 랜섬웨어에 대한 분석 내용을 살펴보고자 한다.

[6] BSD: UC 버클리에서 개발한 유닉스 계열의 운영체제

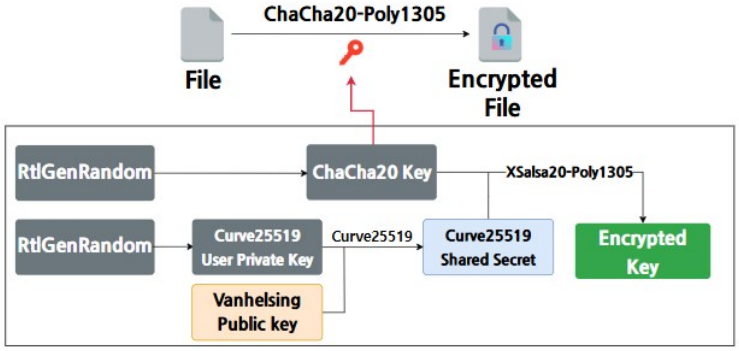
[7] ARM: 모바일 기기, IoT 장비 등에 주로 사용되는 저전력 고효율 프로세서 아키텍처

[8] vCenter: VMware 에서 개발한 중앙 집중식 관리형 유틸리티로 여러 ESXi 호스트 및 종속 요소를 관리하기 위해 사용

Vanhelsing Ransomware

암호화 키

ChaCha20-Poly1305 알고리즘으로 암호화를 하고, 해당 키를 Curve25519 공유 비밀로 보호



암호화 방식

1GB 이하: 전체 암호화
1GB 초과: 전체 크기의 30%만 암호화

특징

- 부분 암호화
- 백업 복사본 삭제
- 내부 전파
- 네트워크 공유 폴더 암호화
- ChaCha20/Xsalsa20 암호화
- 프로세스 우선순위 변경
- 바탕화면 및 아이콘 변경

랜섬노트

README.txt - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

```
--= No news is a good news ! =--

Your network has been breached and all your  files Personal data, financial reports and important documents  has been stolen , encrypted

if you willing to continue your bussines and make more money and keep bussines secret safe you need to restore your files first, And to re
don't bother your self and wast your time or make it more harder on your bussines , we developed a locker that can't be decrypted using

making your self geek and trying to restore the files with third part decrypter this will leads to lose all your date ! and then the even you

to chat with us :

1 - Download tor browser https://www.torproject.org/download/
2 - go to one of these links above
        http://vanhelcbxqt4tqie6fuevfng2bsdtxgc7xslo2yo7nitaacdfrlpxnqd.onion
        http://vanhelqmjstkvlhrjwzgjzpq422iku6wlggiz5y5r3rmfdeiaj3ljaid.onion
        http://vanhelsokskrlaacilyfmtuqqa5haikubsjaokw47f3pt3uoivh6cgad.onion
        http://vanheltarnbfjhuvggbncniap56dscnzz5yf6yjmxqivqmb5r2gmllad.onion

3 - you will be asked for your ticket id to enter the chat this for you : TICKET ID [redacted]

usefull links :
#OUR TOR BLOG :
http://vanhelvuuo4k3xsiq626zkqvp6kobc2abry5wowxqysibmqs5yjh4uqd.onion
http://vanhelwmbf2bwzw7gmseg36qqm4ekc5uuhqbsew4eihzcahyq7sukzad.onion
http://vanhelxjo52qr2ixcmtjayqqrcodkuh36n7uq7q7xj23ggotyr3y72yd.onion
```

README.txt

변경 확장자

.vanhelsing, .vanlocker

제작 언어

C/C++

그림 8. Vanhelsing 랜섬웨어 개요

Vanhelsing 랜섬웨어 전략

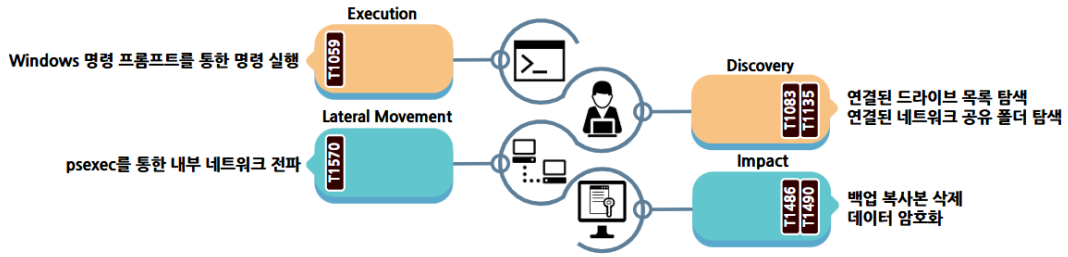


그림 9. Vanhelsing 랜섬웨어 공격 전략

Vanhelsing 랜섬웨어는 다양한 실행 인자를 사용해 암호화 대상이나 방식을 설정할 수 있으며, 바탕화면 변경이나 백업 복사본 삭제와 같은 기능의 사용 여부도 결정할 수 있다. 다만, 랜섬웨어에서 보여주는 도움말 메시지와 실제 인자가 다르며, 일부 인자는 확인만 하고 사용하지 않거나 기능이 구현되지 않은 경우도 있다. 실제 확인하는 인자와 기능은 아래 표와 같다.

인자	설명
-h	실행 인자 도움말 출력
-v	로그 출력
--skipshadow	백업 복사본 삭제 생략
--Driver <driver>	지정한 드라이버만 암호화
--Directory <directory>	지정한 폴더만 암호화
--File <file>	지정한 파일만 암호화
--Force	랜섬웨어 중복 실행 허용
--no-priority	랜섬웨어 우선순위 설정 생략
--no-wallpaper	바탕화면 변경 생략
--no-local	로컬 파일 암호화 생략
--no-mounted	고정된 로컬 드라이브만 암호화
--no-network	네트워크 공유 폴더 암호화 생략
--spread-smb	내부 네트워크 전파
--no-logs	로그 미출력
--no-admin	관리자 권한 여부 상관없이 실행
--Silent	모든 대상 파일 암호화 후 확장자 일괄 변환
--system	기능 미구현
--no-autostart	기능 미구현
--spread-vcenter	기능 미구현

표 1. Vanhelsing 랜섬웨어 실행 인자

실행 인자를 확인한 이후 암호화 중 오류 방지를 위해 몇 가지 작업을 수행한다. 바탕화면, 아이콘 변경과 네트워크 공유 폴더 접근 등 관리자 권한이 필요한 경우가 있으므로, 현재 관리자 권한으로 실행 중인지 확인한다. 만약 관리자 권한으로 실행 중이지 않으면 랜섬웨어를 종료하지만, "--no-admin" 인자를 사용하면 관리자 권한이 없더라도 랜섬웨어를 종료하지 않는다. 또한 랜섬웨어가 중복으로 실행되는 것을 방지하기 위해 "Golbal\\VanHelsing" 문자열로 뮤텍스[9] 를 생성하고, 암호화 속도를 높이기 위해 랜섬웨어 프로세스의 우선순위를 가장 높은 우선순위로 설정한다. 이 두 기능은 각각 "--Force", "--no-priority" 인자로 비활성화가 가능하다.

또한 암호화된 파일을 사용자가 임의로 복구하지 못하도록 백업 복사본을 삭제한다. 마찬가지로 "--skipshadow" 인자를 사용하면 백업 복사본을 삭제하지 않는다. 백업 복사본을 삭제하기 위해 사용하는 명령어는 아래와 같다.

cmd.exe /c C:\\Windows\\System32\\wbem\\WMIC.exe shadowcopy where "ID='%s'" delete

표 2. 백업 복사본 삭제 명령어

"--spread-smb" 인자를 사용하면 내부 네트워크로 전파가 가능하다. 내부 네트워크에 연결된 PC 나 서버에서 랜섬웨어를 실행하기 위해 psexec[10] 를 사용한다. 해당 프로그램은 랜섬웨어에 함께 저장되어 있기 때문에, 해당 프로그램을 임시 폴더에 저장한 후 활용한다.

```
network_list = WSAStartup_sub_40CA90(pMemoryBlock: pMemoryBlock_1);
GetTempPathW(nBufferLength: 0x1F4u, lpBuffer: temp_path);
m_format_string_sub_40D890(Buffer: psexec_path, Format: L"%s\\psexec.exe", temp_path);
m_print_message_sub_4011D0(L"[*]\tpsexec_path : %s \n");
memset(buf: stream, value: 0, n0x20: 0xB0u);
m_wfsopen_sub_40BB30(buf: stream, Buffer: psexec_path, n48: 0x30, v43, Buffer: psexec_path);// open %TEMP%psexec.exe stream
m_write_stream_sub_40BD50(this: stream, &psexec_data, 0xAED90i64);
m_close_stream_sub_406660(buf: stream);
```

그림 10. psexec 저장

[9] 뮤텍스(Mutex): 하나의 자원에 여러 스레드 혹은 프로세스가 동시에 접근하지 못하도록 하는 동기화 매커니즘으로, 랜섬웨어에서는 흔히 중복 실행 방지를 위해 사용한다.

[10] psexec: Windows 시스템에서 프로세스를 원격으로 관리하고 실행할 수 있도록 하는 명령줄 도구

psexec 를 저장한 이후에는 현재 랜섬웨어가 실행중인 시스템의 IP 주소를 가져온 이후, 마지막 옥텟[11] 에 해당하는 값을 1 부터 255 까지 변경하며 접근이 가능한 내부 네트워크가 존재하는지 확인한다. 접근 가능한 내부 네트워크 주소가 확인되면 해당 주소의 네트워크 폴더 중 쓰기 권한이 있는 폴더에 랜섬웨어를 "vanlocker.exe" 라는 이름으로 복사하며, psexec 를 활용해 내부 네트워크에 연결된 PC 나 서버에 랜섬웨어를 실행한다. 이 때 실행 인자로 "--no-mounted", "--no-network"를 사용하며, 사용하는 실행 명령어는 아래와 같다.

```
cmd.exe /c %TEMP%psexec.exe -accepteula \\${shared_folder} -c -f
${shared_folder}\vanlocker.exe -d --no-mounted --no-network < NUL
```

표 3. 내부 전파 명령어

내부 네트워크 전파 외에도 여러가지 실행 인자를 통해서 파일 암호화 대상 설정이 가능하며 크게 파일, 폴더, 로컬 드라이브, 네트워크 공유 폴더로 구분된다. "--File" 인자를 사용하면 지정한 1 개의 파일만 암호화하며, "--Directory" 인자를 사용하면 지정한 폴더와 그 하위 폴더를 암호화하고, "--Driver" 인자를 사용하면 지정한 드라이버 전체를 암호화한다. 만약 암호화와 관련된 실행 인자를 아무것도 사용하지 않으면 모든 드라이버와 네트워크 공유 폴더를 암호화하고, "--no-network" 인자를 사용해 네트워크 공유 폴더 암호화를 비활성화 하거나 "--no-local" 인자를 사용해 로컬 파일 암호화를 생략할 수 있으며, "--no-mounted" 인자를 사용해 고정된 로컬 드라이브만 암호화하는 것도 가능하다.

암호화 대상을 설정했으면, 각 디렉터리를 순회해 예외 항목에 해당하는지 확인한다. 우선적으로 대상 디렉터리가 예외 항목인지 확인하며, 디렉터리 확인이 끝났다면 각 디렉터리에 존재하는 파일이 예외 항목인지 확인한다. 확인하는 암호화 예외 대상은 아래 표와 같다.

폴더명	확장자 및 파일명
tmp, winnt, temp, thumb, $Recycle.Bin, $RECYCLE.BIN, System Volume Information, Boot, Windows, Trend Micro, program files, program files(x86), tor browser, windows, intel, all users, msocache, perflogs, default, microsoft	.vanlocker, .exe, .dll, .lnk, .sys, .msi, .bat, .bin, .com, .cmd, .386, .adv, .ani, .cab, .ico, .bod, .msstyles, .msu, .nomedia, .ps1, .rtp, .syss, .prf, .deskthemepack, .cur, .cpl, .diagcab, .diagcfg, .dll, .drv, .hlp, .pdb, .hta, .key, .lock, .ldf, .icns, .ics, .idx, .mod, .mpa, .msc, .msp, .nls, .rom, .scr, .shs,. spl, .theme, .themepack, .wpx, boot.ini, autorun.inf, bootfont.bin, bootsect.bak, desktop.ini, iconcache.db, ntldr, ntuser.dat, ntuser.dat.log, ntuser.ini, thumbs.db, GDIPFONTCACHEV1.DAT, d3d9caps.dat, LOGS.txt, .README.txt

표 4. 암호화 예외 대상

[11] 옥텟: 32 비트로 이루어진 IP 주소에서 8 비트씩 구분해 표현하는 단위

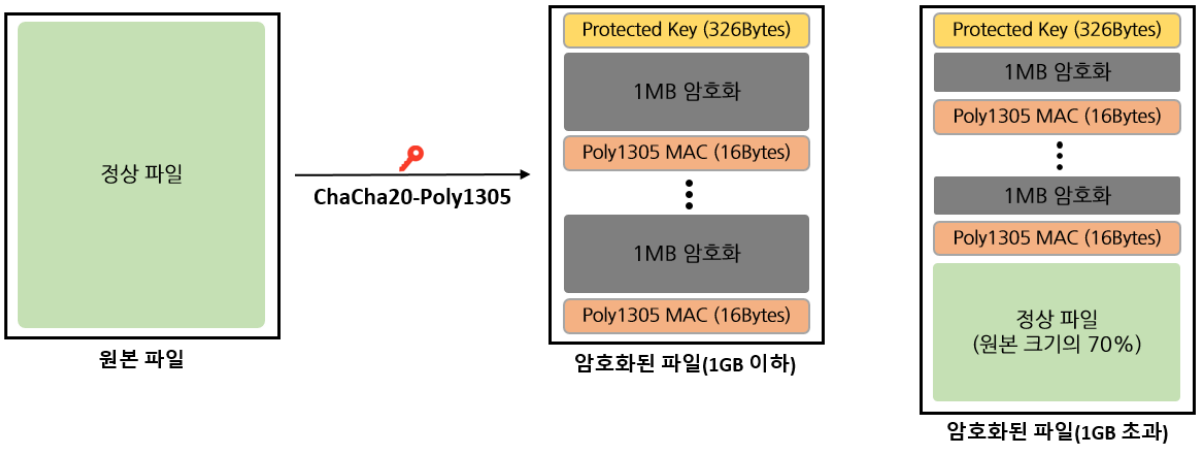
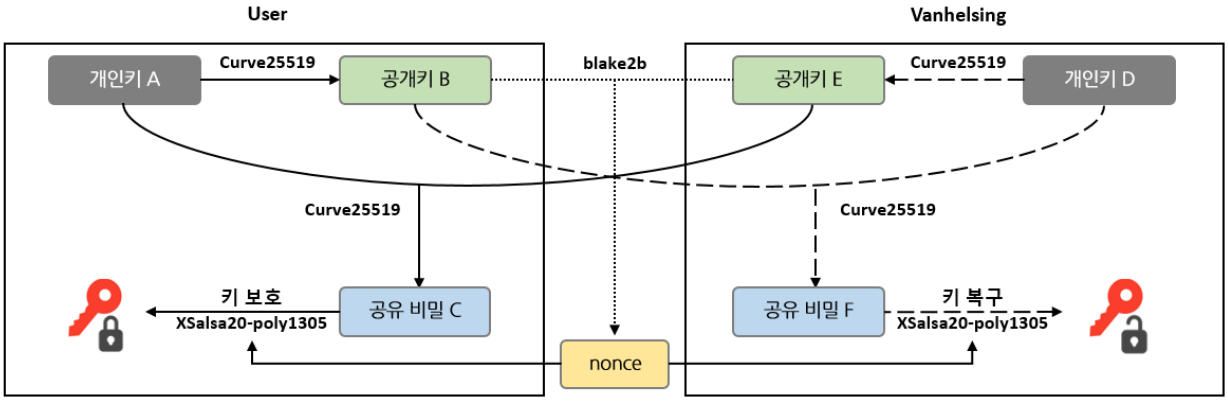


그림 11. 크기 별 파일 암호화 방식

파일 암호화는 1GB 이하의 파일은 전체를 암호화하고, 1GB 보다 큰 파일은 전체 크기의 30%만 암호화한다. 각 파일마다 랜덤한 32bytes 키와 12bytes nonce 를 만들고, ChaCha20-Poly1305 알고리즘을 사용해 파일을 암호화한다. 암호화는 1MB 단위로 진행하며, ChaCha20-Poly1305 의 특성상 데이터 무결성을 보장하기 위한 메시지 인증 코드(MAC)가 함께 생성되므로, 암호화된 파일에는 1MB 단위마다 16bytes 의 MAC 이 함께 저장된다.



공유 비밀 C = 공유 비밀 F

그림 12. 키 보호 방식

또한 암호화에 사용된 키를 보호해 파일의 맨 앞에 저장하는데, 이 때 Curve25519 를 통해서 생성한 공유 비밀로 암호화 키와 nonce 를 보호하고 키를 복구할 수 있는 사용자의 공개키를 함께 저장하는 방식을 사용한다. 파일 암호화 키와 별개로 각 파일마다 랜덤한 개인키를 하나 생성한 다음, 하드코딩된 Vanhelsing 의 공개키를 사용해 공유 비밀을 생성할 수 있다. 자신의 개인키와 상대방의 공개키로 만든 공유 비밀이 자신의 공개키와 상대방의 개인키로 만든 공유 비밀과 동일한 값을 가지는 Curve25519 의 특성을 이용한 것이다. 키 보호에는 XSalsa20-Poly1305 알고리즘을 사용하는데, 해당 알고리즘은 키 외에도 nonce 로 사용할 추가 데이터가 필요하다. nonce 는 사용자의 공개키와 Vanhelsing 의 공개키를 이어 붙인 다음 blake2b 알고리즘으로 12bytes 크기의 해시를 생성해 사용한다.

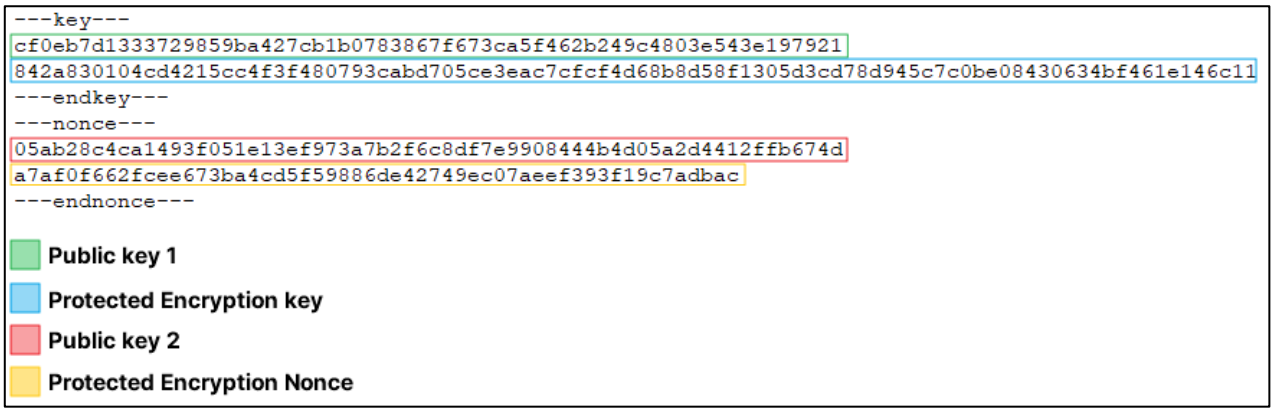


그림 13. 보호된 키 저장 방식

보호된 키는 복구를 위한 공개키와 함께 암호화된 파일의 맨 앞에 텍스트 형태로 저장된다. ---key---, ---nonce--- 와 같이 사용한 키와 nonce를 구분하며, 공개키와 보호된 키를 순차적으로 저장한다.

그림 14. 변경된 바탕화면

파일 암호화 이후에는 랜섬웨어에 저장된 이미지와 아이콘 파일로 바탕화면과 암호화된 파일의 아이콘을 변경한다. 배경화면은 “vhlocker.png”로 저장되며, 아이콘 이미지는 “vhlocker.ico”로 저장된다. --no-wallpaper” 인자를 사용하면 배경화면과 아이콘 이미지 변경은 생략한다.

Vanhelsing 랜섬웨어 대응방안

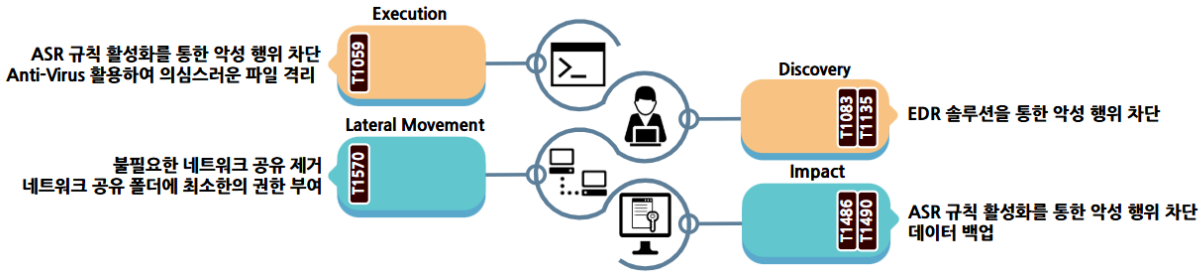


그림 15. Vanhelsing 랜섬웨어 대응방안

Vanhelsing 랜섬웨어는 Windows 명령 프롬프트를 활용해 백업 복사본 삭제와 내부 전파를 위한 명령어를 실행한다. 따라서 ASR[12] 규칙 활성화를 통해서 비정상적인 프로세스를 차단해 악성 행위를 막을 수 있다. 또한 랜섬웨어에 저장된 프로그램을 임시 폴더에 저장하거나 랜섬웨어 자체를 네트워크 공유 폴더에 복제하기 때문에 Anti-Virus 를 활용하여 의심스러운 파일을 격리할 수 있다.

내부 전파와 네트워크 공유 폴더 암호화를 위해서 현재 시스템의 내부 네트워크 대역을 탐색하고, 연결이 가능한 네트워크 주소와 공유 폴더에 접근을 시도한다. 뿐만 아니라 파일 암호화의 경우 모든 드라이브를 탐색한 뒤 실행 인자에 따라서 암호화할 드라이브를 구분하는데, EDR 솔루션을 통해 공격자의 악성 행위를 막을 수 있다.

또한 내부 전파는 랜섬웨어 쓰기 권한이 있는 공유 폴더에 복사한 뒤 실행하기 때문에, 별도의 접근 권한이 없다면 내부 전파 차단이 가능하다. 따라서 네트워크 공유 폴더 접근 권한을 최소한으로 부여하는 것도 하나의 방법이다. 그 외에 네트워크 공유 폴더와 같은 네트워크 서비스가 필요하지 않다면, 서비스 자체를 비활성화 하거나 SMB 포트(445)를 차단해 피해를 최소화해야 한다.

암호화된 파일을 사용자가 임의로 복구하는 것을 방지하기 위해 시스템에 존재하는 모든 백업 복사본을 삭제한 뒤 파일을 암호화한다. ASR 규칙 활성화를 통해서 백업 복사본을 삭제하는 프로세스와 파일을 암호화는 것을 차단할 수 있다. 뿐만 아니라 백업 복사본을 별도의 네트워크나 저장소에 소산 백업하여, 시스템이 암호화되더라도 복구할 수 있도록 조치해야 한다.

[12] ASR (Attack Surface Reduction): 공격자가 사용하는 특정 프로세스와 실행 가능한 프로세스를 차단하는 보호 기능

IoCs

Hash(SHA-256)
86d812544f8e250f1b52a4372aaab87565928d364471d115d669a8cc7ec50e17
99959c5141f62d4fbb60efdc05260b6e956651963d29c36845f435815062fd98

■ 참고 사이트

• BleepingComputer (https://www.bleepingcomputer.com/news/security/microsoft-north-korean-hackers-now-deploying-qilin-ransomware/)

• Cyber Daily (https://www.cyberdaily.au/security/11919-exclusive-contractor-brighton-australia-listed-on-safepay-s-ransomware-leak-site)

• S-rm (https://www.s-rminform.com/latest-thinking/camera-off-akira-deploys-ransomware-via-webcam)

• BleepingComputer (https://www.bleepingcomputer.com/news/security/ransomware-gang-encrypted-network-from-a-webcam-to-bypass-edr/)

• Trend Micro (https://www.trendmicro.com/en_us/research/25/c/socgholishs-intrusion-techniques-facilitate-distribution-of-rans.html)