KARA
Korea Anti Ransomware Alliance

2022.09.

KARA 랜섬웨어 동향 보고서

목차

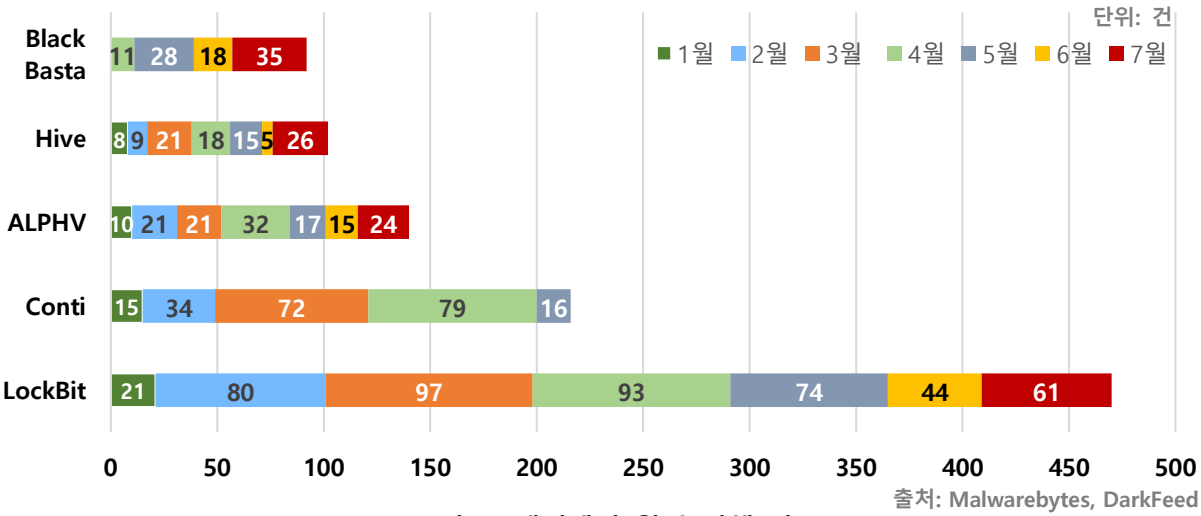
■ 랜섬웨어 트렌드

✓ 랜섬웨어 트렌드 분석

랜섬웨어 공격은 주로 금전적 이익을 얻을 수 있는 기업들을 주요 타겟으로 삼고 있으며 지능화된 공격으로 진화하고 있다. 전세계적으로 랜섬웨어 감염으로 인한 피해액이 계속해서 증가하고 있으며 Ransomware-as-a-Service(RaaS) 발전으로 Lockbit, Conti 랜섬웨어와 같이 세분화되고 조직화되고 있다.

랜섬웨어는 다양한 전략과 방법을 사용하여 많은 감염 사례를 유도하기 위해 고도화되고 있으며 BlackCat 랜섬웨어와 같이 Re-branding을 통한 수사 회피, Lockbit 랜섬웨어와 같이 기술적으로 고도화하기위해 업데이트하는 경우를 확인할 수 있다. 또한 더 많은 피해를 입히기 위해 Cross-platform 랜섬웨어(Conti, BlackCat, Deadbolt 등)를 제작하여 다양한 플랫폼을 공략하기도 한다. 파일 암호화와 정보 유출을 통한 다크웹에 게시하는 이중 협박 전략, 정보 유출을 위한 Custom 툴 사용, Anti-Anaysis & Evasion으로 실행 시 특정 키 값을 사용하거나 MSI, NSIS 등 유포 방식을 변화시키는 등 랜섬웨어는 계속해서 진화하고있다.

Lockbit 랜섬웨어는 지속적으로 증감을 하며 활발한 활동을 하고 있는 것으로 확인된다. Conti 랜섬웨어는 활동 중단 선언 후 6월 다크웹 사이트를 최종 폐쇄하였다. Conti의 활동 중단 영향으로 Hive, ALPHV(BlackCat) 등 기존에 활동하던 랜섬웨어와 4월경부터 확인된 신규 그룹인 Black Basta 랜섬웨어 등 중·소규모 그룹으로 분산된 현상을 확인할 수 있다.



출처: Malwarebytes, DarkFeed

그림 1. 랜섬웨어 월별 피해 사고

Conti, Grief, Pysa, DopplePaymer, Onyx, DeadBolt 등의 크고 작은 랜섬웨어 그룹들이 사라지고 운영을 중단하였다. 랜섬웨어 그룹 활동을 완전히 종료했을 수도 있지만 새로운 랜섬웨어와 다시 나타날 가능성도 존재한다. 체포되거나 코드 유출, 취약점 발견, 수사를 회피하는 목적 등 다양한 이유로 랜섬웨어가 사라지고 운영을 중단하지만 신규 랜섬웨어 및 중·소규모의 랜섬웨어 그룹들은 계속해서 발견되고 있다.

운영을 중단했던 대규모 랜섬웨어 그룹인 REvil 은 2022 년 4 월 REvil 의 다크웹 인프라 재개 및 소스코드로부터 컴파일된 추정 샘플이 발견되는 등 활동을 재개하는 모습을 보였으며 8 월초 국내 대기업을 해킹하였다고 주장하며 관련 내용을 블로그에 게재하였으나 이미 매각된 회사로 해당 대기업과는 무관한 회사로 확인되었다. BlackCat, Lockbit 3.0, Redeemer 등의 랜섬웨어들은 실행 시 키 값 사용 같은 일부 기능을 업데이트하거나 버전을 올려 새로운 기능을 추가하여 고도화 작업을 통한 활동이 포착되기도 하였다.

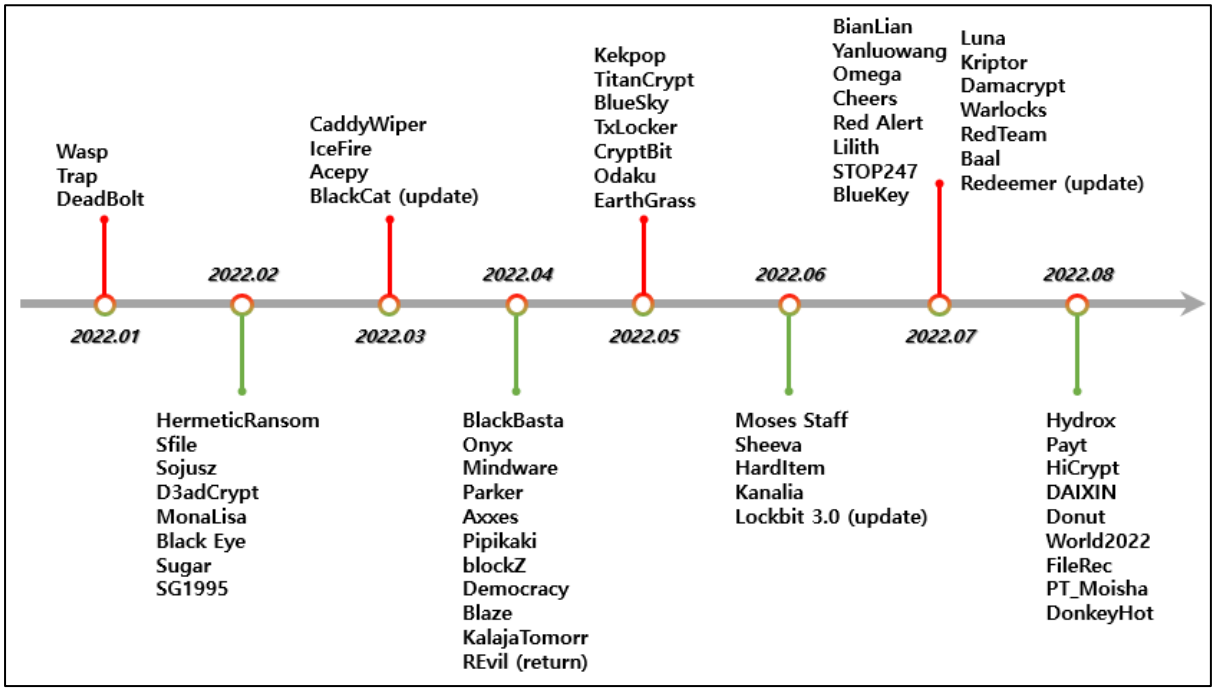


그림 2. 신규 랜섬웨어 및 그룹

먼저 랜섬웨어 분석 사례를 통해 랜섬웨어 공격자 그룹의 전략을 살펴본 후 최근 다크웹에서 가장 활발히 활동하고있는 랜섬웨어 그룹인 Lockbit 3.0 과 국내에서 가장 영향력 있는 VenusLocker 그룹의 활동, 꾸준히 변종이 발견되고 있는 Phobos 랜섬웨어와 국내 특정 대기업을 타겟으로 감염을 시켜 큰 이슈를 불러온 GWISIN 랜섬웨어를 분석하여 트렌드와 특징을 간략히 알아보고 랜섬웨어를 예방하기위해 완화할 수 있는 방안을 제공하고자 한다.

1. VenusLocker 그룹, Makop & Lockbit 3.0 랜섬웨어

VenusLocker 그룹은 2016년부터 스피어 피싱 메일의 첨부 파일을 이용하여 VenusLocker 랜섬웨어를 유포한 이래로 사회공학기법을 이용하여 지금까지도 꾸준히 활동하고 있는 그룹이며 국내를 대상으로 활동하고 있다.

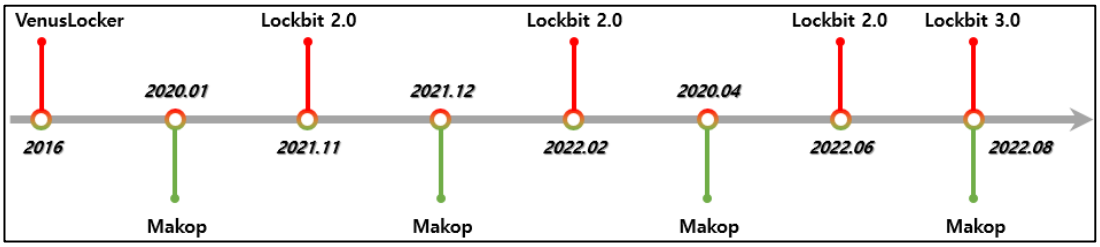


그림 3. VenusLocker 그룹이 사용하는 랜섬웨어 변화

2020년 VenusLocker 그룹은 Makop 랜섬웨어를 유포하기 시작했으며 공정거래위원회 등 기관 사칭, 이미지 저작권 위반, 입사지원서 관련 이력서와 포트폴리오 등으로 위장하여 첨부파일을 통해 랜섬웨어를 유포하기 시작하였다.

VenusLocker 그룹은 2021년 11월, 2022년 2월, 2022년 5월~7월 등 Makop 랜섬웨어를 유포하다 Lockbit 2.0 랜섬웨어를 간간히 유포하기 시작하였다. 특히 6월에 Lockbit 랜섬웨어가 3.0으로 버전이 업데이트 되었지만 해당 그룹은 Lockbit 2.0 랜섬웨어를 계속 사용하였다. 그 후 2022년 8월 VenusLocker 그룹은 이력서를 위장한 첨부파일로 Lockbit 3.0을 사용하기 시작하였다.

Lockbit 3.0은 2019년 9월에 Lockbit ABCD로 처음 발견되었으며 이후 v1.1, v1.2, v1.3을 거쳐 Lockbit 2.0으로 2021년 6월 업데이트 되었으며 그로부터 1년 뒤 2022년 6월 Lockbit 3.0으로 업데이트되어 활발히 활동 중이다.

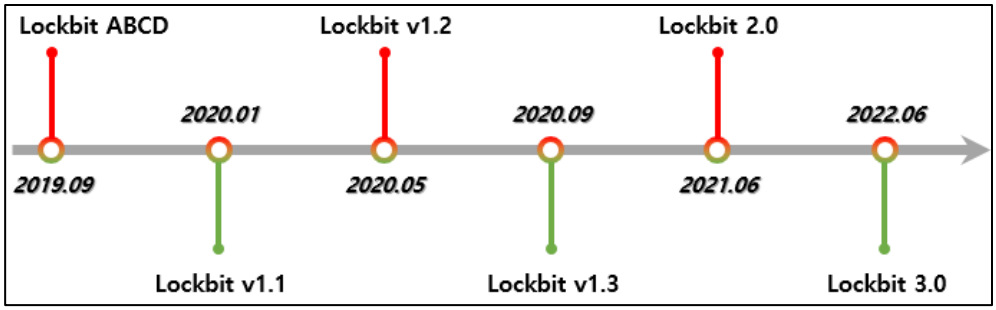


그림 4. Lockbit 랜섬웨어 변화

최근 랜섬웨어들은 Ransomware-as-a-Service(RaaS), 공격자와 제작자가 구분되어 수익을 나눠가지는 구조를 보이는 형태의 서비스를 통해 활동하며 조금 더 나아가서는 조직화된 하나의 기업처럼 움직이는 그룹이 늘고 있다. 그 중 Lockbit 또한 RaaS 형태의 랜섬웨어를 사용하는 조직화된 그룹으로 다크웹 2차 유출, 감염자 수를 바탕으로 보면 현재 가장 활발히 활동하며 가장 파급력이 있는 그룹으로 볼 수 있다.

그림 5. Lockbit 유출 사이트 게시 일부

Lockbit 3.0으로 업데이트 되면서 랜섬웨어 최초로 버그바운티를 도입하고 복호화 지불 방법으로 Zcash 코인 도입, 탐지 회피 전략으로 서비스 형태로 동작하며 다양한 Anti-Analysis & Evasion 전략을 추가되어 더욱 강력한 기능을 가지고 유포 중이다. 또한 BlackMatter 랜섬웨어와 권한 상승, 프로세스 종료 API 체크, 안티 디버깅 등 여러 루틴의 유사성이 확인되며 감염 후 변경되는 바탕화면에 LockBit Black으로 표기하고 있어 BlackMatter 그룹과의 연계 혹은 코드 등의 리소스를 활용한 것으로 보인다.

■ 국내 기업 타겟형 랜섬웨어 분석

그림 6. 랜섬웨어 Tactics

✓ GWISIN 랜섬웨어

1. Background

- 2021년 상반기 최초로 발견되었으며 국내 기업들을 타겟으로 AD 서버, 기업의 취약 부분 등을 공격하여 랜섬웨어를 감염시킨다.
- 2022년 하반기 특정 대기업들의 피해 사례들이 일부 공개되어 이슈가 된 랜섬웨어이다.
- 사고가 발생한 업체들은 금융, 제약, 전자, 미용 등 상장 회사 위주로 타겟팅하여 공격을 하였다.
- 이벤트 로그 삭제, 키 값 사용 등 탐지를 회피하기 위한 방법을 다수 사용하며 사고 분석을 방해하기 위한 전략을 사용하는 그룹이다.
- 한글 키보드를 통해 영문으로 타이핑한 한글 사용 흔적이 발견되었으며 국내 보안 솔루션, 환경 등 시장을 잘 알고 있어 한국어를 사용하거나 한국어에 능통한 해커가 포함된 그룹으로 보인다.
- 일부 공격 기법의 유사성, 한글 사용 등 정황상 증거를 통해 업계에서는 북한과의 관련성을 의심하고 있지만 코드 유사성, 북한 IP 등 정확한 근거가 확인되지는 않았다.

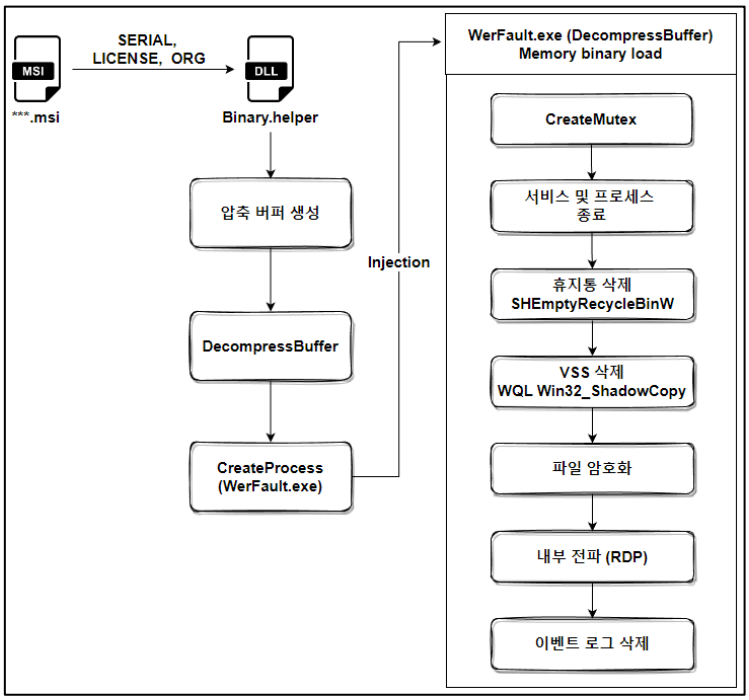


그림 7. GWISIN 랜섬웨어 실행 흐름

2. GWISIN 특징

- 국내 특정 기업을 대상으로 침투하여 랜섬웨어를 유포하였으며 해당 기업만을 위한 config 및 랜섬노트를 사용한다.
- 탐지 회피를 위해 Microsoft Software Installer(MSI) 파일 형태로 유포하며 MSI의 Custom Action 테이블을 이용하여 dll의 Export 함수를 호출하여 동작한다. MSI 파일 실행 시 특정 인자 값이 존재 해야하며 해당 키/값 들이 일치해야 정상적인 압축 버퍼를 생성하여 압축을 해제 후 다음 동작을 수행한다. 키/값 들이 없거나 일치하지 않을 경우 실행이 되지 않도록 설계되어 있어 샌드박스 및 분석을 방해하는 기법을 사용하고 있다.
- 정상적으로 쉘코드를 생성하게 되면 윈도우 정상 시스템 프로세스(WerFault.exe)에 메모리 인젝션하여 동작하며 AES-256 암호화 알고리즘을 사용하여 RDP 세션을 통해 확보한 토큰으로 네트워크 및 로컬 드라이브 파일 암호화 작업을 수행한다.
- 암호화 작업 후 원본 파일명의 확장자 뒤에 감염 대상 회사의 이름이 추가되며 추가로 파일 암호화에 사용된 AES 암호화 키를 특정 알고리즘을 이용하여 보호 후 감염 대상 회사의 이름이 추가된 변경 파일명에 '0'을 붙여 파일을 생성하여 저장한다.
- 랜섬웨어 감염 후 사고 사실을 랜섬노트에 NPA(경찰청), SMPA(서울경찰청), FSC(금융위원회), KISA(한국인터넷진흥원), NIS(국정원), SKInfosec(SK쉴더스) 등 수사 기관에 신고하지 말라는 내용이 적혀져 있고 한글을 영문 변환한 단어를 사용한 점 등을 미루어보아 국내 보안 시장을 잘 알고 있는 특징을 보이고 있다.
- Data Loss Prevention(DLP, 데이터 유출 방지)를 우회하여 민감한 데이터를 탈취하였다고 주장하며 이중 협박 전략을 사용하고 있다. 추가로 귀신 랜섬웨어는 협상 단계에서 복호화 키 전달 / 민감하고 중요한 정보 등 유출된 데이터 비공개 / 침투 경로 등 취약점 리포트 제공과 같이 지불 비용에 따라 제공하는 항목을 구분하고 있다.

✓ Phobos 랜섬웨어

1. Background

- Phobos 랜섬웨어는 RaaS(Ransomware-as-a-Service) 랜섬웨어로 2017 년 10 월 21 일 처음 발견되었으며 2018 년 12 월부터 활성화된 것으로 확인된다. 이후 2019 년 4 월 4 일 업데이트를 진행하고 2019 년 4 월 11 일 포럼을 통해 새로운 파트너를 모집하는 공고를 올리고 활발하게 활동 중이다.

- 최초에 발견된 랜섬노트에는 Phobos 문구가 표기되어 있었으나 최근 발견되고 있는 변종 랜섬웨어는 해당 문구는 사라지고 유사한 랜섬노트를 사용하고 있다.

- Phobos 랜섬웨어는 Dharma 랜섬웨어와 코드 베이스, 랜섬노트 등의 기술적 유사성과 운영적 측면의 유사성이 높아 같은 계열의 랜섬웨어로 알려져 있다.

- Dharma 랜섬웨어는 2016 년 처음 발견된 CrySis 후속 버전으로 그 해 제작자가 소스 코드를 공개하면서 리뉴얼 되었으며 2018 년 복호화 툴 및 암호키의 접근이 가능해진 후 후속 주자로 Phobos 랜섬웨어가 표면으로 들어나게 된다.

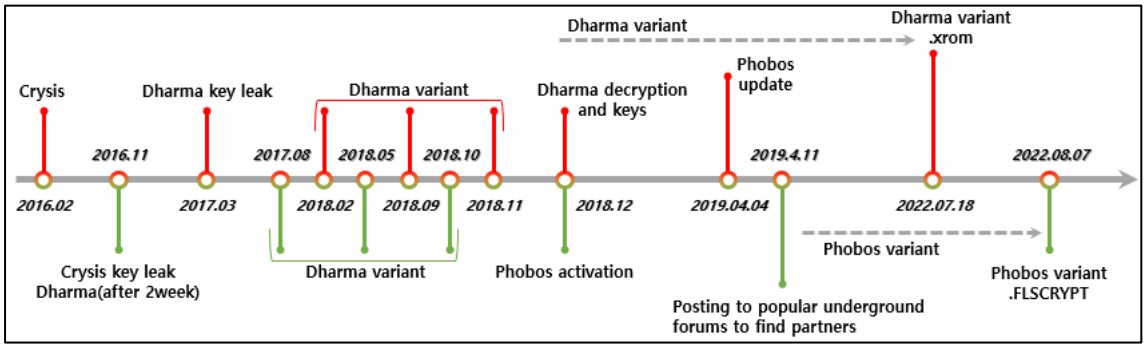


그림 8. Phobos timeline

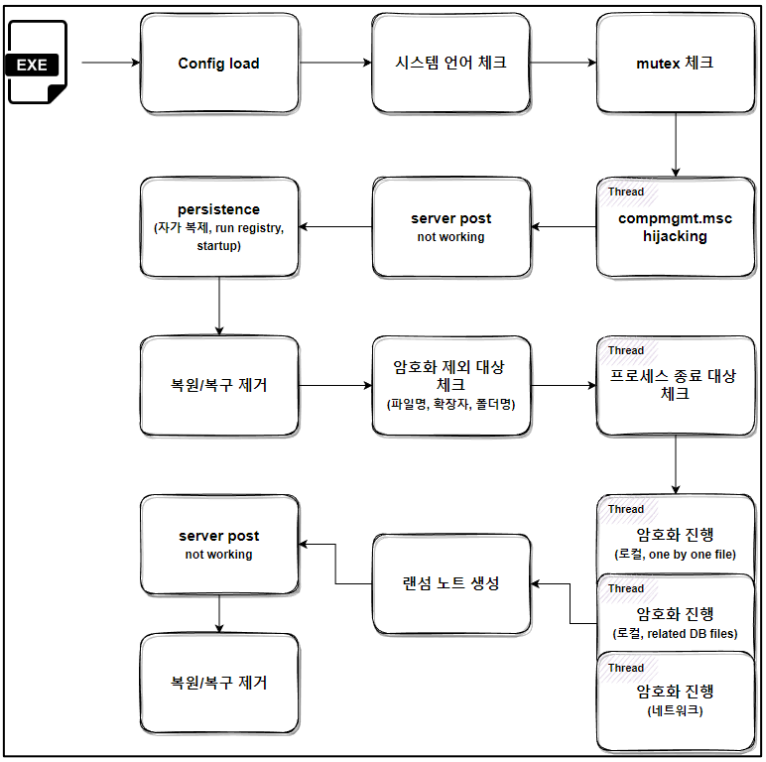


그림 9. Phobos 랜섬웨어 실행 흐름

2. Phobos 특징

- Ransomware-as-a-Service 형태의 랜섬웨어로 확장자와 버전 값 등 일부 config 만 변경되어 지속 유포되고 있으며 탐지 회피를 위해 암호화 되어있는 config 값을 사용한다.
- AES-256 알고리즘을 사용하여 파일을 암호화하며 RSA 공용키를 통해 파일 암호화에 사용된 AES key 를 보호하여 공격자의 RSA 개인키가 있어야 복호화가 가능하다.
- 파일 사이즈에 따라 암호화 방식을 구분하고 시스템 전체 파일에 대해 one by one 암호화를 진행하는 스레드 이외 데이터베이스 관련 파일에 대해 추가로 암호화 스레드를 생성하여 속도를 향상시키고 새로운 로컬 드라이브, 네트워크 드라이브를 감지하여 암호화를 수행한다. 암호화 작업 후 '.id[<<ID>>-3373].[decrypt2022@onionmail.org].FLSCRYPT' 형태로 원본 파일명의 확장자 뒤에 추가한다.
- info.txt, info.hta 랜섬노트를 생성하여 복호화 방법을 안내하며 기존과 다른 점으로는 메일을 통한 연락 방법 이외 ICQ, Tox Chat messenger 를 추가로 안내하고 있으며 데이터 유출 관련한 문구가 추가되었다.

■ 랜섬웨어 Mitigations

공격자는 공격대상을 선정하기위해 공격자 그룹이 수립한 전략을 통해 다양한 방법으로 정찰을 수행하며 이후 내부 인프라에 침입하여 파일을 암호화시키고 자산을 위협하며 데이터 유출을 통한 협박을 시도한다. 이러한 피해를 예방하기위해 타겟형 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