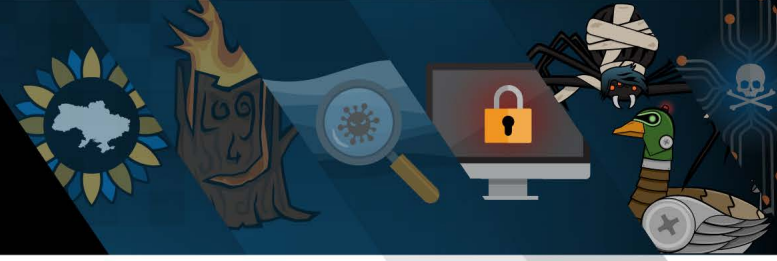
랜섬웨어와 COMMODITY LOADERS



전문 다운로드

랜섬웨어 위협 환경

랜섬웨어는 지정학적 환경, 방어 조치, 사법 당국 활동 등에 유동적으로 대응하고 있는데, 특히 2022년에는 사법 당국의 활동이 범위와 강도 면에서 크게 증가했습니다. 이는 공격 단체들이 새로운 이름으로 리브랜딩을 진행하고 사업장을 닫고 새로운 전략적 파트너십을 구축하는 계기가 되었습니다. Cisco Talos는 2022년에 나타난 몇몇 관련 동향을 관찰했습니다.

Talos는 12곳 이상의 RaaS(Ransomware-as-a-Service) 단체를 추적합니다**(그림 1)**. 조사 결과에 따르면 2022년에 가장 왕성한 활동을 보인 단체는 LockBit로, 전체 다크웹 피해자 게시글의 20% 이상을 차지했으며, Hive와 Black Basta가 그 뒤를 바짝 쫓았습니다. 이러한 결과는 소수의 단체가 시장을 독점하던 작년까지와 달리 랜섬웨어 공격자들 사이의 평준화가 이루어졌음을 보여줍니다. 랜섬웨어 어필리에이트는 더 이상 사일로화되어 있지 않고 여러 단체에 걸쳐 활동합니다. 기술 역량이 높은 행위자일수록 여러 공격 및 조직과 함께할 기회를 더 많이 얻을 수 있습니다.

우크라이나 전쟁으로 많은 공격자들이 진영을 선택하고 친러시아와 친우크라이나 타깃 중 하나를 공격해야 하는 상황에 놓이면서 커뮤니티 전체의 갈등도 고조되었습니다. Conti는 가장 강경한 RaaS 단체 중 하나로 러시아의 우크라이나 침공을 방해하려고 시도하는 누구든 공격할 것이라고 경고했습니다. Conti와 관계가 있는 한 개인이 이 랜섬웨어 단체에게 앙갚음을 하기 위해 멀웨어의 소스 코드와 어필리에이트 사이의 대화를 포함한 정보를 유출한 적도 있습니다. 또한 Talos는 LockBitBlack이라는 LockBit 3.0 랜섬웨어 암호생성기의 유출 빌더가 공개된 일도 확인했습니다. LockBit에 따르면, 범인은 급여 체계에 불만을 품은 LockBit 개발자 중 한 명인 것으로 알려졌습니다.

이러한 갈등은 랜섬웨어 단체들의 리브랜딩 또는 신종 단체의 출현으로 이어지는 경우가 많습니다. Conti가 운영을 중단하고 Conti의 인프라 가동이 멈추자 Talos의 텔레메트리에서도 탐지 건수가 전반적으로 감소하긴 했으나, 얼마 안 되어 리브랜딩된 Black Basta가 출현했습니다. 연구자들은 이 두 단체의 결제 및 유출 웹사이트와 커뮤니케이션 스타일이 유사하다고 지적합니다**(그림 2)**.

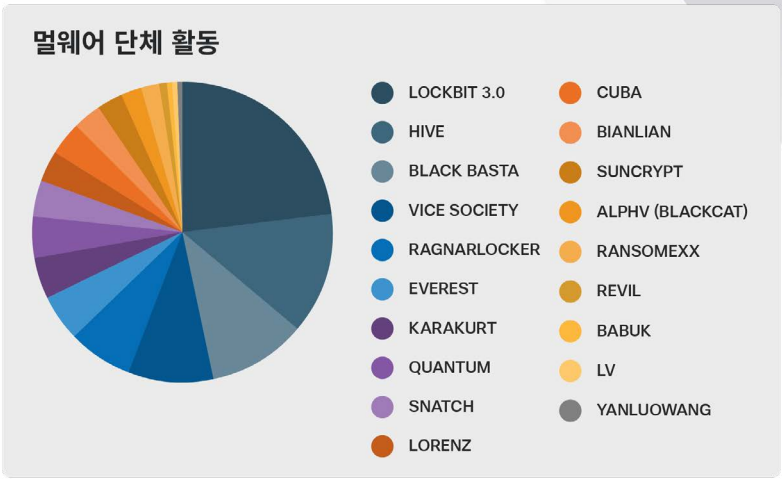


그림 1.1월부터 10월까지 Talos가 추적한 랜섬웨어 데이터 유출 사이트에 올라온 게시글 수.

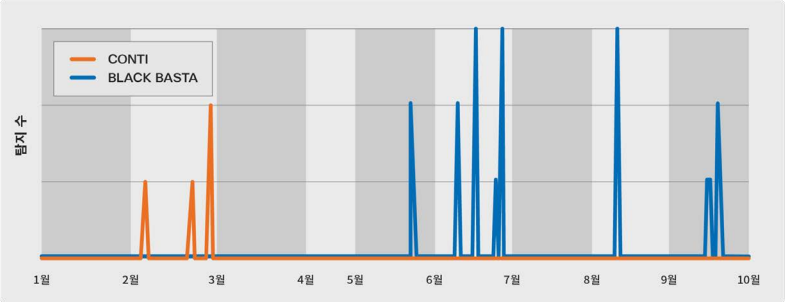
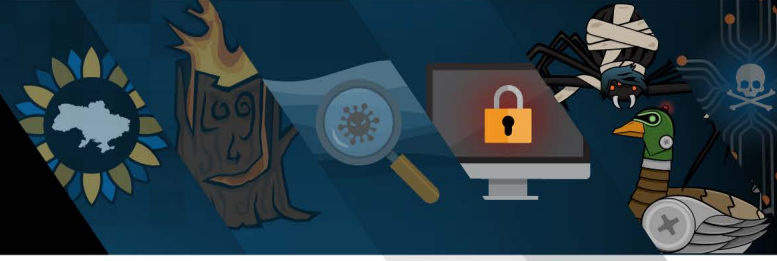


그림 2. Secure Malware Analytics의 Conti 랜섬웨어 및 Black Basta 레지스트리 변경 행동 지표 탐지 수.

COMMODITY LOADER

2단계 멀웨어를 배포하는 상용 트로이목마 바이러스인 Commodity Loader는 지속적으로 전 세계에 영향을 미치고 있습니다. 원래는 돈을 목적으로 단체들을 공격하도록 설계된 뱅킹 트로이목마 바이러스로 개발되었다가 시간이 지나면서 강력한 보안 조치에 대응하며 훨씬 정교한 위협으로 발전했습니다. 현재는 모듈 기능을 갖춘 로더로 운영되는데, 공격자들은 이를 이용해 다양한 오픈소스 툴과 새로운 멀웨어를 유연하게 활용할 수 있습니다. 몇몇 네트워크 및 엔드포인트 텔레메트리 세트에 대한 Talos의 분석에 따르면 2022년에 가장 많이 발생한 Commodity Loader는 Qakbot, Emotet, IcedID 및 Trickbot이었습니다**(그림 3)**.

랜섬웨어와 COMMODITY LOADERS



당사 텔레메트리가 Trickbot과 연관된 활동을 탐지하기는 했으나 이 멀웨어 운영자가 2022년 초부터 활동을 중단해 온 만큼 상당 부분은 과거에 감염된 엔드포인트가 탐지되었을 가능성이 높다고 보고 있습니다. 마찬가지로 Emotet도 아직 운영 중이긴 하지만, 2021년 1월 초에 사법 당국이 봇넷을 해체한 이후로는 활동이 크게 줄었습니다. 이들의 공백은 Qakbot이나 IcedID와 같은 멀웨어가 채웠습니다.

2022년의 핵심 동향 중 하나는 운영자들이 ISO, ZIP 또는 LNK 파일을 이용해 Qakbot, Emotet 및 IcedID를 제공하는 경우가 많아졌다는 점입니다. 이는 Microsoft의 매크로 지원 문서 차단을 우회하기 위함일 가능성이 높습니다. Talos가 확인한 또 다른 동향은 Qakbot, Emotet 및 IcedID 운영자들이 피해자 환경에서 발견한 LoLBins를 이용해 악성 페이로드를 다운로드하고 실행한다는 점이었습니다. 일부 Qakbot 및 Emotet 어필리에이트들은 여러 LoLBins로 실험하며 공격 시퀀스를 개선하여 탐지 확률을 줄이기도 했습니다.

당사 텔레메트리가 Trickbot과 연관된 활동을 탐지하기는 했으나 이 멀웨어 운영자가 2022년 초부터 활동을 중단해 온 만큼 상당 부분은 과거에 감염된 엔드포인트가 탐지되었을 가능성이 높다고 보고 있습니다. 마찬가지로 Emotet도 아직 운영 중이긴 하지만, 2021년 1월 초에 사법 당국이 봇넷을 해체한 이후로는 활동이 크게 줄었습니다. 이들의 공백은 Qakbot이나 IcedID와 같은 멀웨어가 채웠습니다.

Commodity Loader별 심층 리뷰는 전체 보고서에서 확인하실 수 있습니다.

Commodity Loader

	Qakbot	IcedID	Emotet	Trickbot
별명	Quackbot, Qbot, Pinkslipbot	BokBot	Geodo, Heodo	해당 없음
소속	유라시아 사이버 범죄자에 의해 개발되었을 가능성이 높은 Commodity 멀웨어	알 수 없음	러시아 국가 주도 사이버 범죄 단체인 Mummy Spider가 개발한 Commodity 멀웨어	러시아 국가 주도 사이버 범죄 단체인 Mummy Spider가 개발한 Commodity 멀웨어
활동 시작 연도	2007 년	2014 년	2017 년	2016 년

목표

- 초기 액세스 획득 및 추가 공격 활동을 위한 지속성 구축.
- 랜섬웨어를 포함한 다음 단계 멀웨어 배포.

타깃 범위

- 전 세계 전 분야.
- 러시아-우크라이나 전쟁 발발 후 Trickbot은 러시아 국민을 겨냥한 공격 시 복수하겠다고 협박함.

주요 TTP

- 피싱, 악성 스팸, 소셜 엔지니어링, 취약점 공격, 금융 데이터나 자격 증명과 같은 데이터의 탈취, 웜 방식 확산.
- 운영자가 다양한 공격을 할 수 있도록 고도로 모듈화.

멀웨어 및 툴

- 멀웨어 변종들은 서로 다른 멀웨어 패밀리를 배포하거나 다른 멀웨어 패밀리에 의해 배포됨.
- 공격 라이프사이클의 여러 단계에서 Cobalt Strike나 LoLbins와 같은 상용 툴 이용.

그림 3. Commodity Loader 위협 매트릭스.

