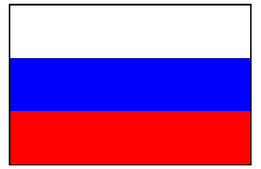
Lockbit의 역사

LOCKBIT 3.0

존 디마지오

ANALYST1



제휴 계열사
(도우미들)

액세스 브로커
투자자

Conti

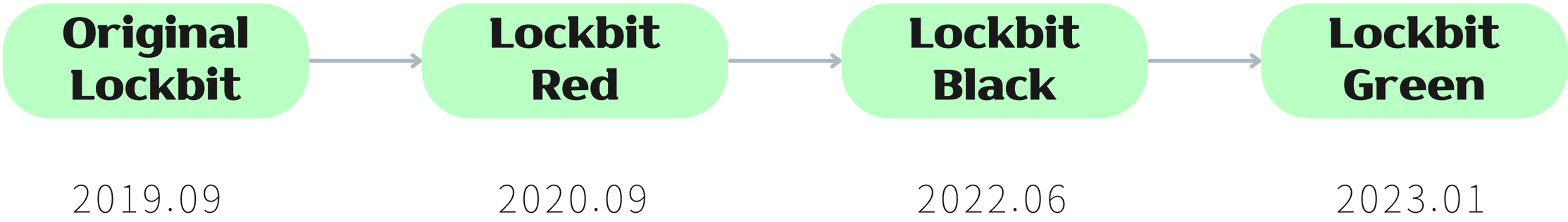
Darkside

REvil

Blackmatter

Lockbit

blackcat


Original Lockbit
Lockbit Red
Lockbit Black
Lockbit Green
2019.09
2020.09
2022.06
2023.01

2019.09

Original Lockbit

도구 사용 PowerShell으로 command 및 Script 실행

자체 확산 Mechanism ARP 테이블을 사용하여 피해자 host를 식별하고, SMB를 사용하여 랜섬웨어를 식별하여 피해자 환경 전체의 공유 리소스/네트워크 장치에 확산

2019.09

Original Lockbit

도구 사용 PowerShell으로 command 및 Script 실행

자체 확산 Mechanism ARP 테이블을 사용하여 피해자 host를 식별하고, SMB를 사용하여 랜섬웨어를 식별하여 피해자 환경 전체의 공유 리소스/네트워크 장치에 확산

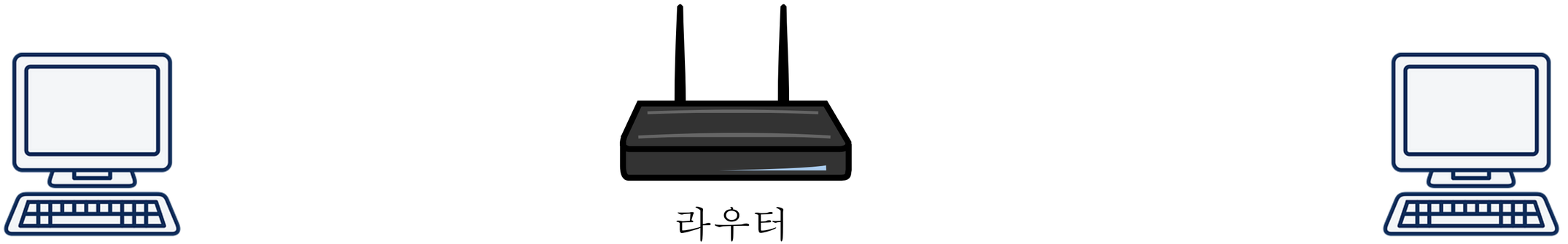


그림1. Address Resolution Protocol

2019.09

Original Lockbit

도구 사용 PowerShell으로 command 및 Script 실행

자체 확산 Mechanism ARP 테이블을 사용하여 피해자 host를 식별하고, SMB를 사용하여 랜섬웨어를 식별하여 피해자 환경 전체의 공유 리소스/네트워크 장치에 확산

그림1. Address Resolution Protocol

2019.09

Original Lockbit

도구 사용 PowerShell으로 command 및 Script 실행

자체 확산 Mechanism ARP 테이블을 사용하여 피해자 host를 식별하고, SMB를 사용하여 랜섬웨어를 식별하여 피해자 환경 전체의 공유 리소스/네트워크 장치에 확산

그림1. Address Resolution Protocol

2019.09

Original Lockbit

도구 사용 PowerShell으로 command 및 Script 실행

자체 확산 Mechanism ARP 테이블을 사용하여 피해자 host를 식별하고, SMB를 사용하여 랜섬웨어를 식별하여 피해자 환경 전체의 공유 리소스/네트워크 장치에 확산

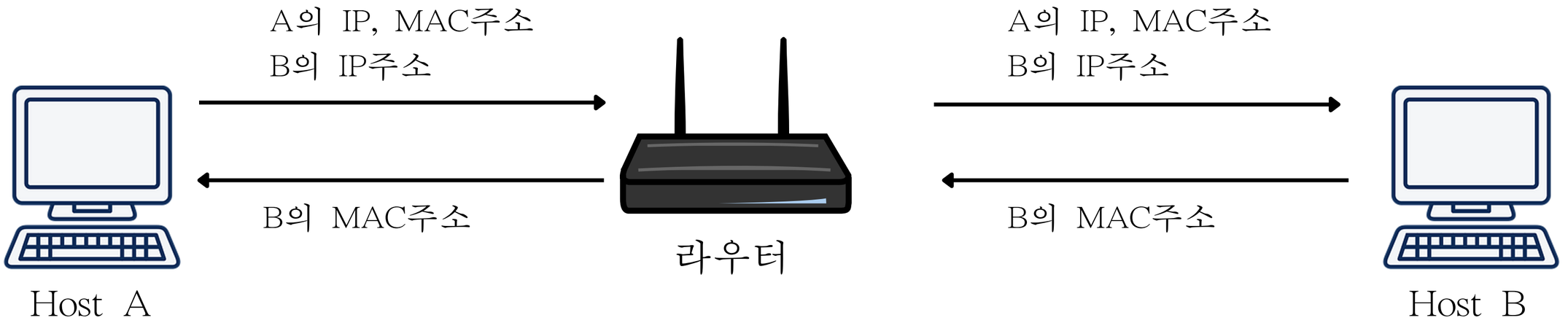


그림1. Address Resolution Protocol

2019.09

Original Lockbit

도구 사용 PowerShell으로 command 및 Script 실행

자체 확산 Mechanism ARP 테이블을 사용하여 피해자 host를 식별하고, SMB를 사용하여 랜섬웨어를 식별하여 피해자 환경 전체의 공유 리소스/네트워크 장치에 확산

IP 주소	MAC 주소
192.168.0.1	64-d5-99-a2-b6-02
192.168.0.2	92-f5-91-42-8a-30
192.168.0.3	14-25-ac-1f-86-82

그림2. ARP Table

2019.09

Original Lockbit

도구 사용 PowerShell으로 command 및 Script 실행

자체 확산 Mechanism ARP 테이블을 사용하여 피해자 host를 식별하고, SMB를 사용하여 랜섬웨어를 식별하여 피해자 환경 전체의 공유 리소스/네트워크 장치에 확산

SMB

- 네트워크 상 존재하는 노드들 간에 자원을 공유할 수 있도록 설계된 프로토콜.
- 호환성의 이유로 윈도우에 종속되어 있으며, 많은 취약점과 수정할 수 없는 낡은 코드로 인하여 골치덩어리.

2019.09

Original Lockbit

도구 사용 PowerShell으로 [illegible]and 및 Script 실행

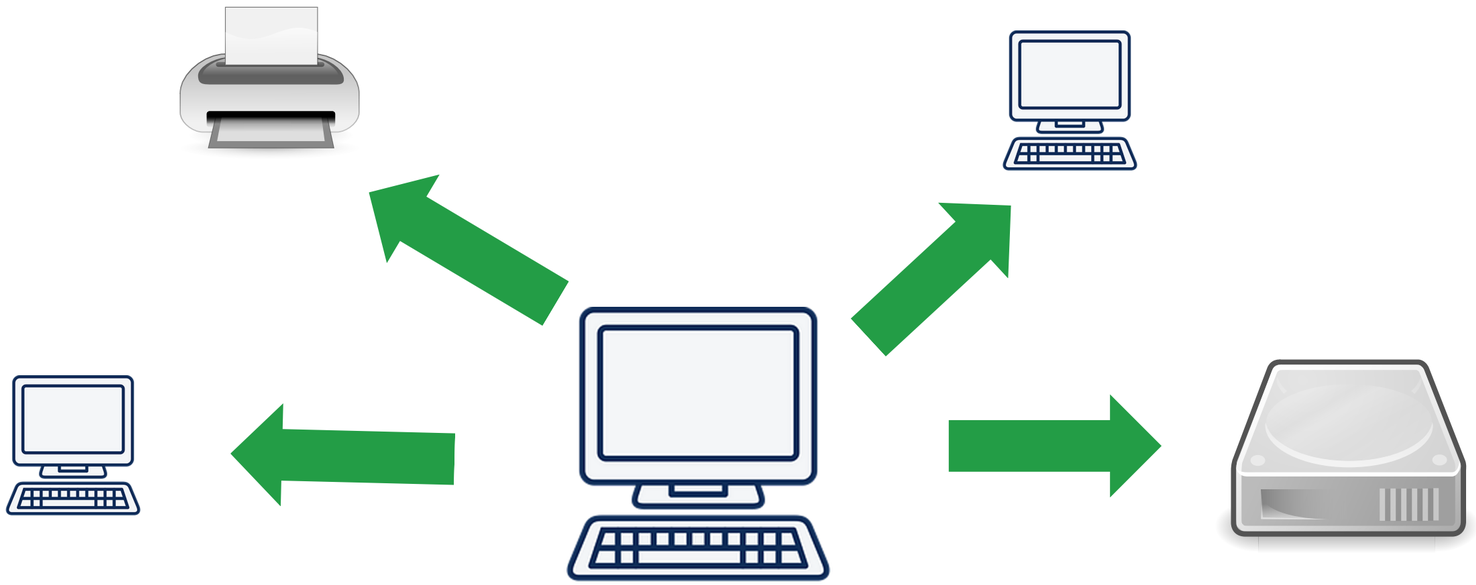
자체 확산 Mechanism ARP 테이[illegible] 피해자 host를 식별하고, SMB를 사용하여 랜섬웨어를 식별하여 피[illegible]크 장치에 확산

SMB

- 네트워크 상 존재하는 노드들 간에 자원을 공유할 수 있도록 설계된 프로토콜.
- 호환성의 이유로 윈도우에 종속되어 있으며, 많은 취약점과 수정할 수 없는 낡은 코드로 인하여 골치덩어리.

2019.09

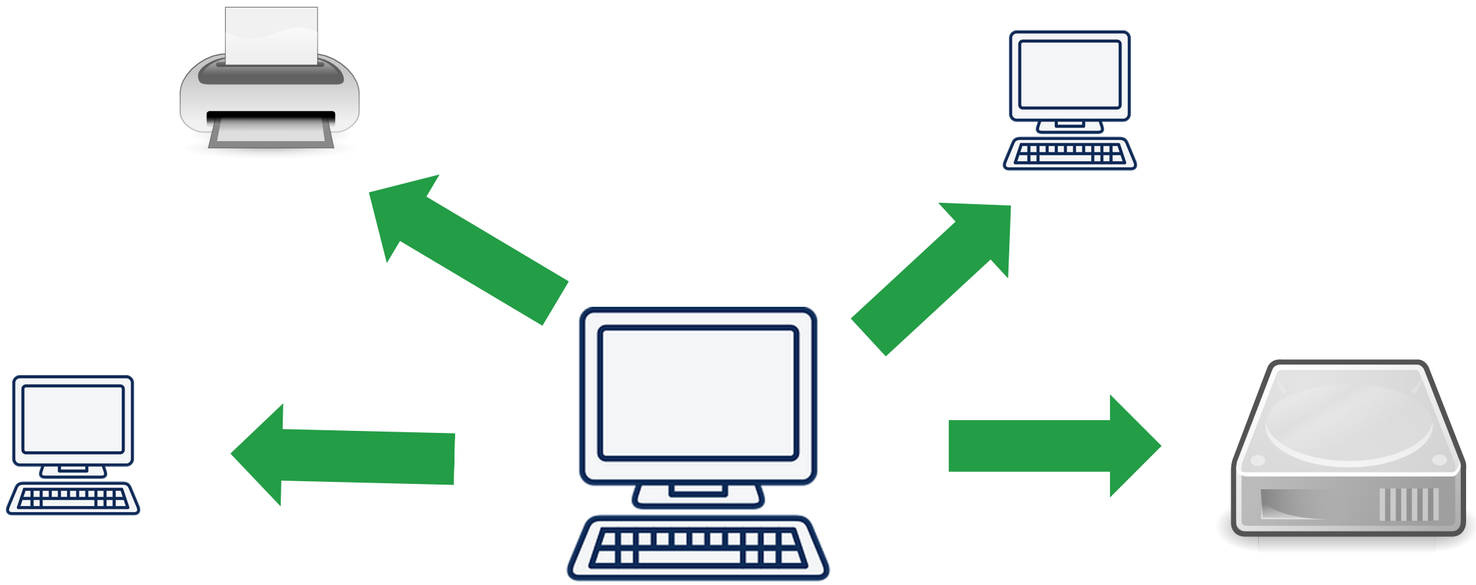
Original Lockbit



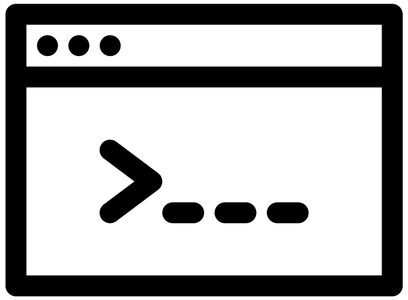
Host A

2019.09

Original Lockbit



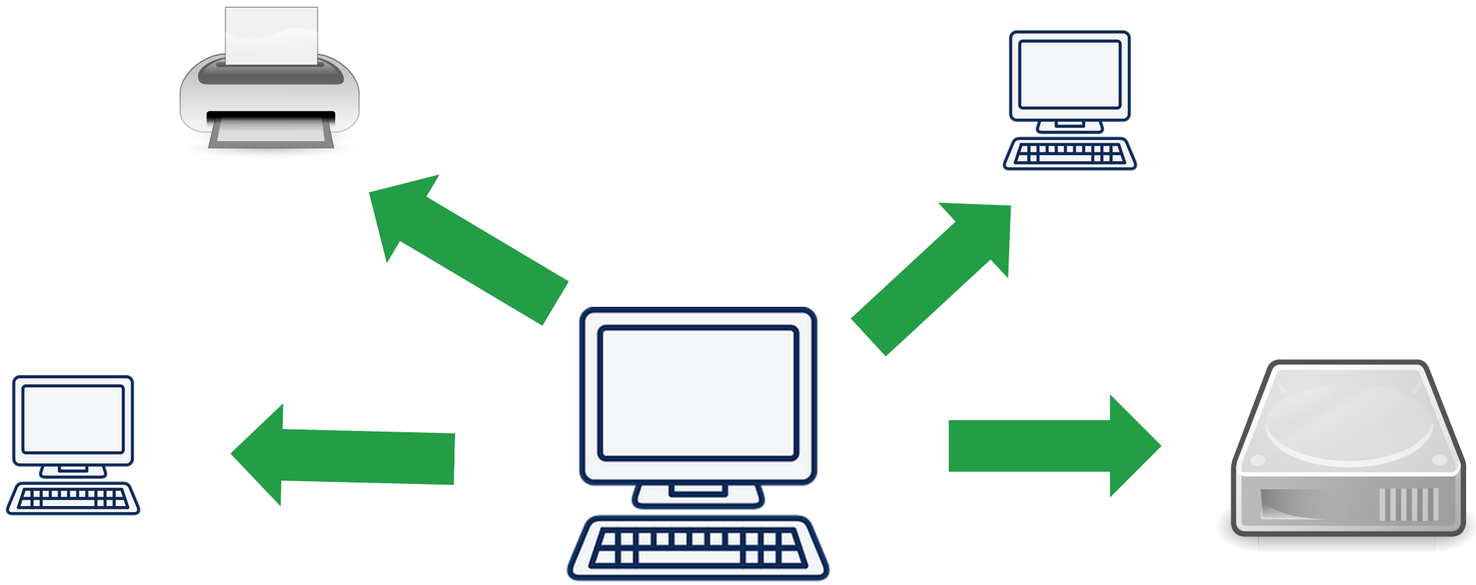
Host A



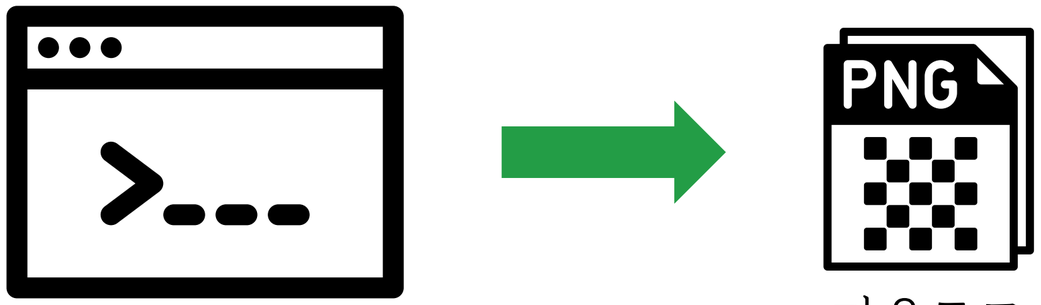
웹 사이트 연결

2019.09

Original Lockbit



Host A

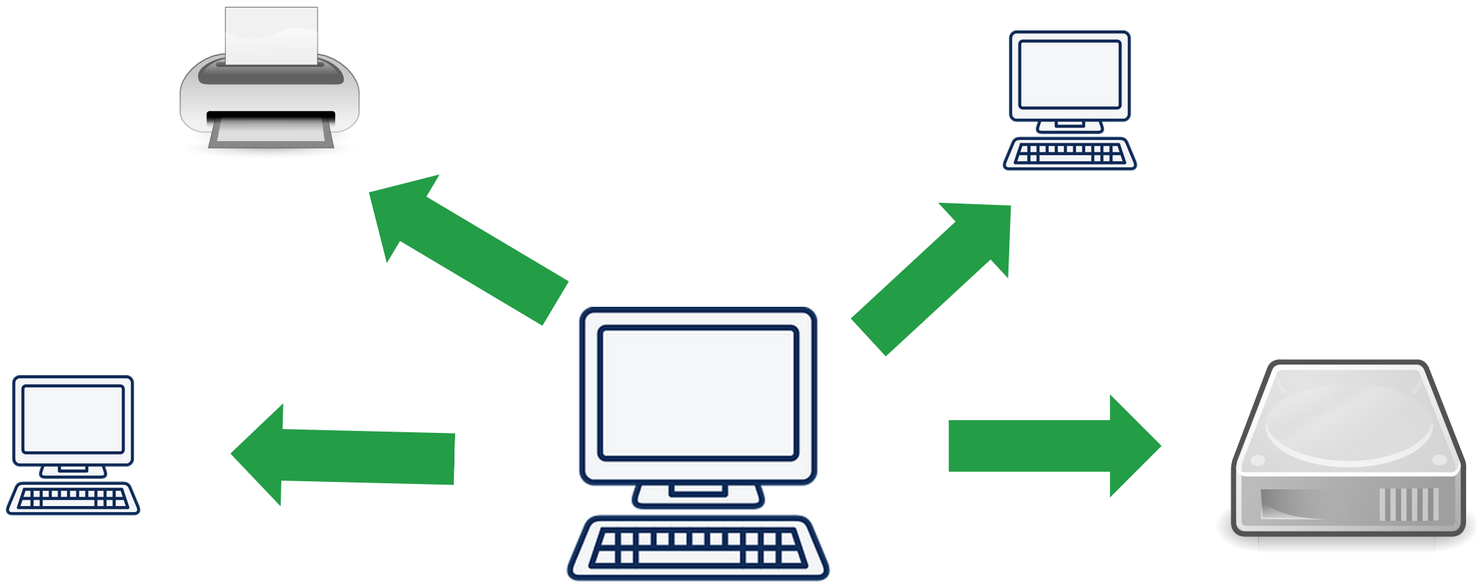


웹 사이트 연결

다운로드

2019.09

Original Lockbit



Host A

웹 사이트 연결

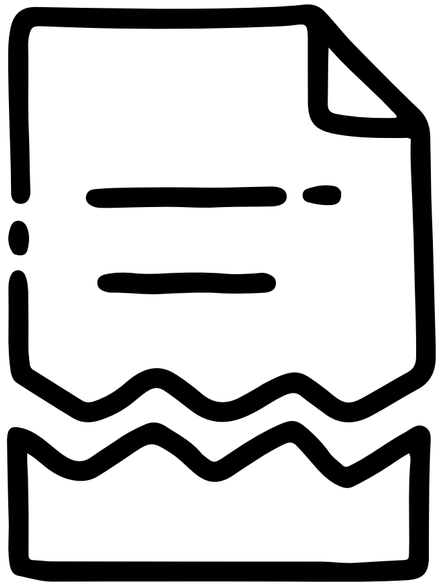
다운로드

Payload

2019.09

Original Lockbit

해결책



파일명.lockbit → 파일명1

2020.09

Lockbit Red

- 포트 및 취약점 스캐너
- 로그 지우기 및 삭제 기능
- 보안 서비스 종료
- 사용자가 데이터를 복원할 수 있는 섀도 복사본 제거 기능

2020.09

Lockbit Red

Wake-on-Lan

이 기능이 존재하기 전에는 피해자의 서버에 백업 데이터가 저장되어 있고 감염 당시 전원이 꺼진 경우 공격자는 랜섬 페이로드를 오프라인 서버에 배포할 수 없었습니다. 그런 다음 공격 후 피해자는 몸값을 지불하지 않고도 서버를 부팅하고 이를 사용하여 데이터를 복원할 수 있었습니다. 이제 이 기능을 통해 공격자는 대상 환경에서 사용 가능한 모든 시스템을 감염시킬 수 있습니다.

2020.09

Lockbit Red

데이터 추출 도구

Rclone과 같은 합법적이고 공개적으로 사용 가능한 도구는 데이터를 훔치고 추출하는 작업에 오버헤드가 발생한다.

StealBit에는 방어 회피 기술도 내장되어 있으며 사용 후 스스로 삭제할 수 있습니다.

사소한 세부 사항은 단일 그래픽 인터페이스 내에 많은 공격 기능을 통합하는 중앙 관리 콘솔을 공격자에게 제공하기 때문에 중요합니다. 이를 통해 랜섬웨어 공격 수행에 따른 오버헤드와 복잡성이 줄어듭니다.

2020.09

Lockbit Red