MANDIANT

위협 인텔리전스
보고서

첩보 활동을 위해 사이버 범죄로 자금을 조달하는 북한의 공격 그룹 APT43

개요

- APT43 은 북한 정권의 이익을 위해 활발히 활동 중인 사이버 작전 단체입니다 . 이 그룹은 비교적 정교한 기술력과 공격적인 소셜 엔지니어링 전술을 결합하여 특히 한반도의 지정학적 문제를 다루는 한국과 미국의 정부 기관 , 학계 및 싱크 탱크를 집중적으로 공격합니다 .
- APT43 은 첩보 캠페인에 더해 전략적 정보 수집이라는 일차적인 목적을 지원하기 위해 사이버 범죄 작전을 통해 자금을 조달하는 것으로 판단됩니다 .
- 이 그룹은 소셜 엔지니어링에 동원하기 위해 수많은 스푸핑 및 사기 페르소나를 만들고 운영 툴 및 인프라 구매를 위해 위장 신분을 만듭니다 .
- APT43 은 여러 작전에서 다른 북한 첩보 조직과 협력해 왔으며 , 이를 통해 APT43 이 북한 정권의 사이버 조직에서 중요한 역할을 수행하고 있음을 알 수 있습니다 .

위협 세부 정보

Mandiant 는 APT43 이 북한 정권의 이익을 위해 활동하는 비교적 정교한 사이버 운영자일 것으로 평가하고 있습니다 . APT43 에서 수행한 것으로 보이는 캠페인으로는 평양의 지정학적 이익에 부합하는 전략적 인텔리전스 수집 , 첩보 활동을 지원하기 위한 크리덴셜 확보 및 소셜 엔지니어링 , 운영 자금을 마련하기 위한 금전적 목적의 사이버 범죄가 있습니다 . 2018 년부터 추적해 온 APT43 단체의 정보 수집 우선순위는 북한의 주요 해외첩보국인 정찰총국 (RGB) 의 임무와도 일치합니다 . APT43 이 주목하는 외교 정책과 핵 안보 이슈는 북한의 전략과 핵무장에 대한 입장을 지지합니다 . 그러나 이 그룹이 2021 년에 대부분의 공격을 보건 관련 분야에 집중한 것은 아마도 팬데믹 대응 노력을 지원하기 위한 것으로 보이며 , 북한 정권의 우선순위 변화에 따른 이들의 대응을 잘 보여줍니다 .

- APT43 의 활동은 김수키 (Kimsuky) 또는 탈륨 (Thallium) 이라는 이름으로 보고되는 경우가 많으며 , 북한 지도부에 현재 지정학적 상황에 대해 알리기 위한 것으로 보이는 크리덴셜 수집과 첩보 활동이 포함됩니다 .
- 가장 자주 관찰되는 활동은 소셜 엔지니어링 전술의 일부로 스푸핑한 도메인과 이메일 주소를 이용한 스피어 피싱 캠페인입니다 . 합법적인 사이트로 위장한 도메인이 크리덴셜 수집 작업에 사용됩니다 .
- APT43 이 제로데이 취약점을 악용한 사례는 관찰되지 않았습니다 .
- APT43 은 빠른 속도로 작전을 전개하며 피싱 및 크리덴셜 수집 캠페인을 활발히 수행하고 있으며 , 북한 사이버 생태계의 다른 첩보 조직과 협력하는 모습도 보여주었습니다 .
- 특히 다음과 같은 부문에서 한국 , 미국 , 일본 , 유럽 같은 지역에 작전이 집중되고 있습니다 .
  - 정부
  - 지정학 및 핵 정책에 초점을 맞춘 교육 기관 / 연구 기관 / 싱크 탱크
  - 비즈니스 서비스
  - 제조

전반적인 표적의 범위가 넓긴 하지만 , APT43 캠페인의 궁극적인 목표는 북한의 무기 프로그램 지원을 중심으로 할 가능성이 가장 높은데 , 여기에는 북한의 핵 야망에 영향을 줄 수 있는 국제 협상 , 대북 제재 정책 , 다른 나라의 외교 및 국내 정치에 대한 정보 수집이 포함됩니다 .

표적의 변화

APT43 의 소행으로 보이는 캠페인은 북한 정권의 이익과 밀접한 관계가 있으며 , 김정은과 은둔 국가 북한의 지배 엘리트에게 영향을 미치는 지정학적 상황과 긴밀하게 연결되어 있습니다 . Mandiant 가 APT43 을 추적한 이래 이들은 한반도 안보 문제에 이해관계가 있는 한국 및 미국 조직을 대상으로 지속적으로 첩보 활동을 수행해 왔습니다 .

- 2020 년 10 월 이전에 APT43 은 주로 한국과 미국에서 한반도에 영향을 미치는 외교 정책 및 안보 문제에 이해관계가 있는 관공서 , 외교 기관 및 싱크 탱크 관련 단체를 표적으로 삼았습니다 .
- 2020 년 10 월부터 2021 년 10 월까지 APT43 활동의 상당 부분은 의료 관련 분야 및 제약 회사를 표적으로 삼았으며 , 이는 북한의 코로나 19 대응 노력을 지원하기 위한 것일 가능성이 높습니다 . 표적이 된 정보가 북한 정권에 어떻게 도움이 되었는지는 불분명하지만 , 다른 북한 사이버 작전 세력과의 협력은 코로나 19 팬데믹 기간 동안 북한이 전염병 대응에 우선순위를 두었으며 상당한 자원이 투입되었음을 어느 정도 암시합니다 .
- 이 기간에 한국 , 미국 , 유럽 , 일본을 대상으로 한 APT43 의 첩보 활동은 계속되었습니다 .
- 특히 , 관찰된 APT43 활동은 배포된 멀웨어에 차이가 있는 등 대상에 따라 약간씩 달랐습니다 . 예를 들어 , VENOMBITE(로더), SWEETDROP(드로퍼) 및 BITTERSWEET(백도어) 는 코로나 19 팬데믹 기간에 한국을 대상으로 한 APT43 활동에서만 사용되었습니다 .

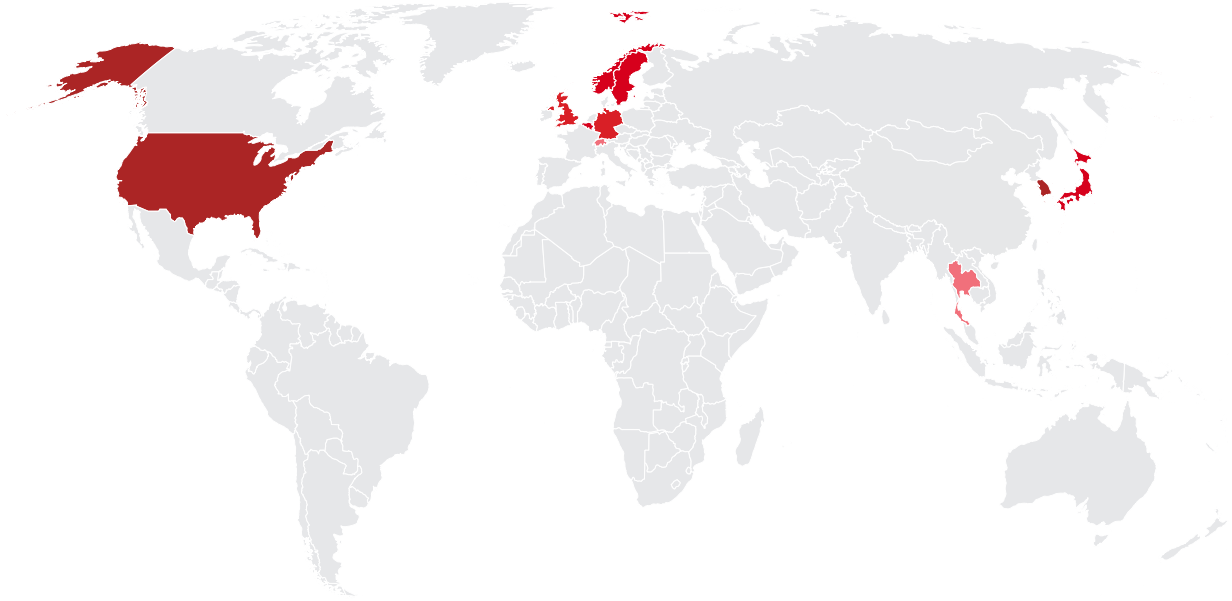

그림 1. APT43 의 표적이 된 국가 (활동이 더 자주 관찰된 국가는 진한 빨간색으로 표시됨).

시민사회 및 비영리
교육
정부
미디어 및 엔터테인먼트
건설 / 소재
방위 / 항공우주
통신
하이테크 산업
제약
컨설팅 / 전문가 서비스

그림 2. APT43 이 직접 표적으로 삼은 산업 분야

사이버 작전

APT43 은 맞춤형 스피어 피싱 이메일을 가장 일반적으로 활용하여 피해자 정보에 접근합니다 . 그러나 이 그룹은 크리덴셜 수집을 위해 스푸핑된 웹 사이트를 이용하고 자금 조달을 위해 사이버 범죄를 수행하는 등 전략적 정보 수집을 지원하기 위해 다른 다양한 활동에도 관여합니다 .

- 공격자들은 정기적으로 유인 콘텐츠를 업데이트하고 특히 핵 안보 및 비확산과 관련된 특정 표적 대상에 맞춰 콘텐츠를 조정합니다 .
- APT43 은 표적 영역 (예 : 안보 및 국방) 내에서 핵심적인 인물로 가장하고 도난당한 개인 식별 정보 (PII) 를 활용하여 계정을 만들고 도메인을 등록하는 등 설득력 있는 페르소나를 만드는 데 능숙합니다 .
- APT43 은 스푸핑된 이메일 주소로 관련성이 높은 유인 콘텐츠를 사용합니다 .
  - APT43 은 또한 해킹을 당한 개인에게서 훔친 연락처 목록을 활용하여 스피어 피싱 작업의 추가 표적을 식별합니다 .
- APT43 은 자력 갱생이라는 북한의 주체 국가 사상에 부합하는 방식으로 운영 인프라를 구매하기 위해 암호화폐를 훔치고 세탁함으로써 북한 중앙정부의 재정 부담을 줄입니다 .

첩보

Mandiant 는 사이버 첩보 활동이 APT43 의 주요 임무라고 생각하며 , 제공된 데이터에 따르면 이 그룹의 다른 활동은 전략적 정보 수집을 지원하기 위해 수행됩니다 .

- 이 그룹은 주로 미국의 군사 , 정부 , 방위산업기반 (DIB) 내에 개발 및 저장된 정보와 핵 안보 정책 및 비확산에 초점을 맞춘 미국 학계 및 싱크 탱크에서 개발한 연구 및 안보 정책에 관심이 있습니다 .
- APT43 은 한국 내 유사한 산업 , 특히 글로벌 및 지역 정책에 중점을 둔 비영리 단체 및 대학뿐 아니라 대북 수출이 제한된 상품에 대한 정보를 제공할 수 있는 제조업과 같은 기업에 관심을 보였습니다 . 여기에는 연료 , 기계류 , 금속 , 운송 차량 및 무기가 포함됩니다 .
- APT43 은 기자 및 싱크 탱크 분석가로 가장하여 표적으로 삼은 인물들과 관계를 구축하고 정보를 수집합니다 (그림 3). 이 그룹은 학자들이 전략 분석 자료를 아무 의심 없이 첩보 조직에 직접 전달했으며 이는 공개 보고에서도 입증되었습니다 .

날짜: 2022년 10월 14일 금요일 03:13:48 -0400
제목: 의견 요청
발신자 X: <redacted>@voanews[.]live

안녕하세요.
잘 지내고 계시리라 생각합니다! <redacted> 소속의 <redacted> 입니다.
북한이 10월 4일 새로운 세계에서 오래된 플레이북을 사용하여 강력한 미사일 발사했습니다. 북한이 마지막으로 일본 상공으로 무기를 발사한 것은 2017년 도널드 J. 트럼프 대통령 재임 당시였고 김정은이 미국과의 갈등을 고조시키려는 것처럼 보였던 때였습니다.

이와 관련하여 몇 가지 질문이 있습니다.
1) 10월 중순 중국 공산당대회 직후 북한이 차기 핵실험을 실시할 것인가?
2) 북한의 도발에 대해 보다 조용한 접근 방식이 보장될 수 있는가?
3) 일본은 국방예산을 증액하고 보다 적극적인 국방정책을 펼칠 것인가?
5일 이내에 답변을 보내주시면 대단히 감사하겠습니다.
좋은 주말 보내세요.

감사합니다.
<redacted>

그림 3. APT43 이 언론인으로 가장하여 잠재적 피해자와 관계를 구축하는 이메일 예시

- APT43 과 관련된 기술 지표는 특히 2022 년 한국의 대선을 앞두고 가능한 정책 변화에 대한 인사이트를 얻기 위해 한국의 정치 단체를 표적으로 삼았다는 한국어 보고서를 부분적으로 뒷받침합니다 .

Mandiant 는 APT43 이 사이버 활동 이외에 다른 북한 활동에 대한 내부 감시도 수행한다는 것을 확인했습니다 . APT43 은 함께 작전을 수행하는 사람들을 포함하여 개별 첩보원들을 해킹하기도 했습니다 . 그러나 이것이 자체 모니터링 목적으로 의도된 것인지 또는 우발적이며 열악한 운영 보안을 나타내는 것인지는 확실하지 않습니다 .

크리덴셜 수집

APT43 은 특히 한국에서 학계 , 제조 및 국가 안보 산업 내의 기관에서 재무 데이터 , 개인 식별 정보 (PII) 및 고객 데이터를 직접 해킹하는 크리덴셜 수집 캠페인을 운영합니다 . 특히 해당 표적 국가에서 인기 있는 검색 엔진 , 웹 플랫폼 및 암호화폐 거래소로 가장한 도메인을 등록합니다 . Mandiant 는 이러한 크리덴셜이 APT43 의 임무 수행을 위한 활동을 지원하는 데 사용된다고 보고 있습니다 .

- 수집된 크리덴셜 데이터는 온라인 페르소나를 생성하고 사이버 첩보 활동을 위한 인프라 (예 : 합법적 서비스를 스푸핑하는 사이트) 를 구성하는 데 사용되었습니다 (그림 4).

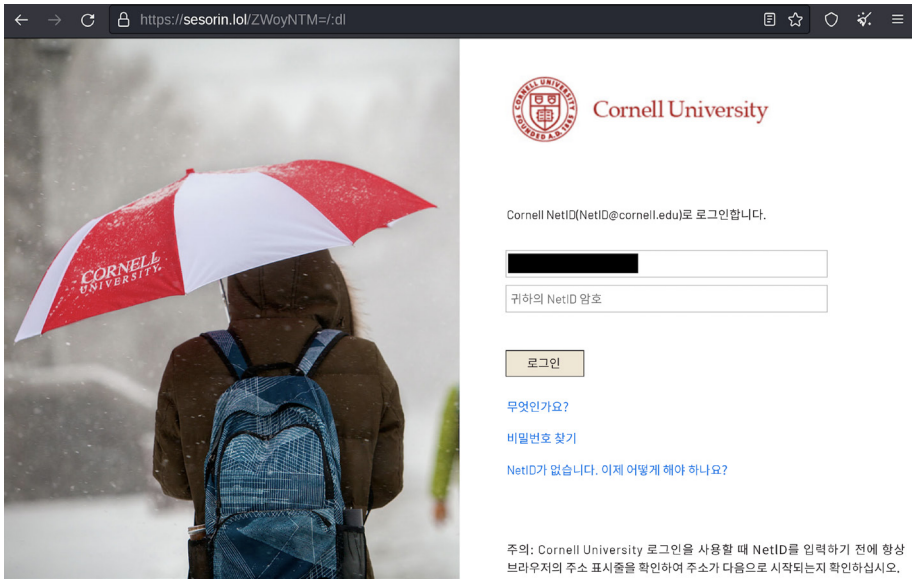

그림 4. APT43 이 제어하는 sesorin.lol 의 크리덴셜 수집 웹사이트 , Cornell University 스푸핑

- 이 그룹은 해킹한 인프라와 공격자 소유 인프라를 모두 활용하여 멀웨어를 호스팅 및 대상에 전달하고 크리덴셜을 수집했습니다 .
  - 2018 년에는 해킹한 웹사이트를 네트워크 인프라의 일부로 사용하여 PASSMARK 및 LATEOP 멀웨어를 전달했습니다 .

표적의 변경은 수집 요구 사항의 전술적 변화를 반영하는 것일 수 있습니다 .

- 2021 년 말 , APT43 은 종교 단체 , 대학 , 비정부 기구 (NGO) 를 대상으로 크리덴셜 수집 캠페인을 재개했으며 , 이는 이러한 캠페인이 북한과 한국 및 일본의 협의체 간의 ' 트랙 2' 외교 채널을 표적으로 삼고 있음을 보여줍니다 . 특히 , 이런 활동은 일시적으로 코로나 19 관련 조직에 초점을 맞췄던 전략에서 기존의 첩보 표적으로 다시 돌아왔음을 의미합니다 .
- 2022 년 초 , Mandiant Intelligence 는 주로 한국에서 학계 , 언론인 , 정치인 , 블로거 및 기타 민간 부문 개인을 대상으로 하는 여러 크리덴셜 수집 캠페인을 확인했습니다 .
- 2022 년 중반에는 크리덴셜 도용 캠페인의 표적이 한국 문제 , 인권 , 학계 , 종교 및 암호화폐와 관련된 한국 블로거 및 소셜 미디어 사용자로 바뀌었습니다 .

암호화폐 표적 공격

APT43 은 암호화폐 및 암호화폐 관련 서비스를 표적으로 삼았습니다. APT38 과 같이 주로 정권을 위한 자금 조달을 담당하는 다른 북한 그룹과는 달리, APT43 은 자체 운영을 유지하기 위해 이러한 활동을 수행할 가능성이 높습니다.

- Mandiant 에서는 APT43 이 훔친 자금을 세탁하기 위해 암호화폐 서비스를 악용하는 것을 확인했습니다. 관련 활동에는 식별된 결제 방법, 별칭, 구매에 사용된 주소 (그림 5) 가 포함되며, 훔친 암호화폐를 깨끗한 암호화폐로 세탁하기 위해 해시 렌탈 및 클라우드 마이닝 서비스를 사용할 가능성이 있습니다.

B 님께,

귀하의 Namecheap 계정에 Bitcoin 결제 $120.00가 추가되었음을 알려드립니다. 이제 계정 잔액을 사용하여 Namecheap.com 에서 제품을 구매하거나 갱신할 수 있습니다.

사용자 이름: BRoyal1990
트랜잭션 아이디: 82073030
트랜잭션 참조: GKRwiyWiTTUXreqpvxNv4A
금액: $120.00

이 거래에 대한 자세한 정보는 (https://manage.www.namecheap.com/myaccount/reports/funds-report.asp)에 있는 자금 추가 내역 페이지에서 확인할 수 있습니다.

질문이 있으시면 (http://www.namecheap.com/support)에서 당사의 지원팀에 문의하십시오.

감사합니다.

Namecheap.com지원팀 드림

그림 5. 훔친 비트코인으로 Namecheap 서비스 비용을 결제했을 가능성이 높은 APT43

  - 이러한 해시 렌탈 및 클라우드 마이닝 서비스는 수수료를 받고 해시 파워를 제공합니다. 구매한 해시 파워를 사용하면 암호화폐를 채굴하여 구매자와 연결되지 않은 깨끗한 지갑에 채워 넣을 수 있습니다.
  - 인프라 및 하드웨어 구매에는 PayPal, American Express 카드 및 이전 활동에서 확보한 것으로 보이는 비트코인과 같은 여러 결제 수단이 사용되었습니다.
- APT43 은 악성 Android 앱을 사용하여 암호화폐 대출을 찾는 중국 사용자를 표적으로 삼았을 가능성이 높습니다. 그림 6 과 같이 앱과 관련 도메인에서 크리덴셜을 수집했을 수 있습니다.

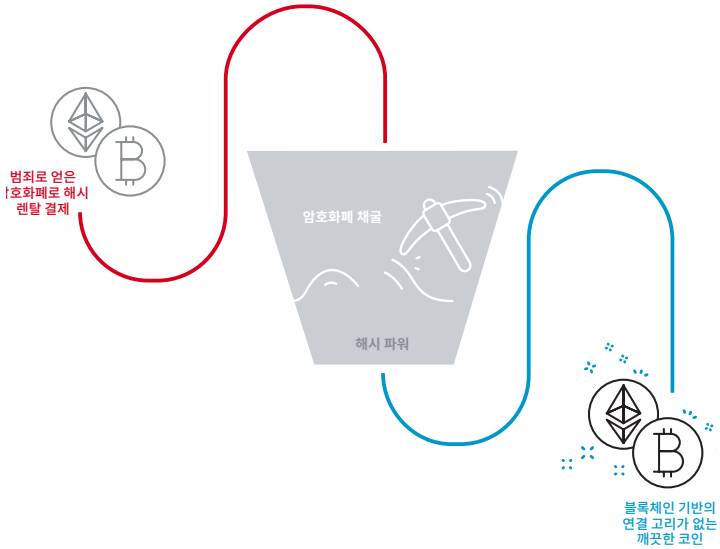

그림 6. APT43 이 사용하는 해시 렌탈 서비스를 통한 암호화폐 세탁

- 역사적으로 사이버 첩보 활동에 집중해 온 북한 그룹들 사이에서도 금전적 동기로 유발된 활동이 만연하고 있다는 사실은 자체적인 자금 조달이 필수적이며 추가 자원 지원 없이 스스로를 유지하기를 요구한다는 점 시사합니다.

속성

Mandiant 는 APT43 이 북한 정부의 광범위한 지정학적 목표를 위해 움직이는 국가 후원을 받는 사이버 공격 그룹일 것으로 평가하고 있습니다 .

- 이 그룹의 주요 활동은 북한의 주요 적대국인 한국에 대한 정보를 수집하는 것이지만 , 이 그룹의 목표는 북한의 변화하는 이해관계와 일치합니다 .
  - 더 나아가 한국에 대한 미국의 지원도 한국을 최우선 표적으로 삼게 만듭니다 .
- APT43 은 알려진 다른 북한 스파이 조직과 인프라 및 툴을 공유하였으며 , 이는 정부 후원을 받는 사이버 기관과 APT43 의 역할 및 임무가 일치함을 보여줍니다 .

보다 구체적으로 , Mandiant 는 APT43 이 북한 제 1 의 해외첩보국인 정찰총국 (RGB) 과 관련된 그룹이라고 평가합니다 .

- APT43 의 일부가 다른 RGB 관련 사이버 첩보 단체 , 즉 TEMP. Hermit(예 : UNC1758) 과 협력하는 것으로 확인되었습니다 . 이에 대해서는 다음 섹션에서 자세히 설명합니다 .

다른 첩보 조직과의 관계

APT43 의 활동은 다른 북한 사이버 첩보 조직의 활동과 겹치기도 했습니다 . 그러나 Mandiant 는 이러한 그룹이 별개로 분리되어 있다고 평가하며 중복된 활동은 일시적인 협력 또는 기타 제한된 자원 공유로 인한 결과일 가능성이 높다고 생각합니다 . 이러한 중복된 활동은 주로 역사적으로 추가 공격자가 채택하는 단일 북한 클러스터에서 사용되었던 멀웨어 계열의 형태를 취합니다 .

- APT43 은 코로나 19 팬데믹이 한창일 때 TEMP.Hermit 클러스터 (라자루스 (Lazarus) 라고 불리는 경우가 많음) 와 관련된 멀웨어를 사용했습니다 . 이는 APT43 과 TEMP.Hermit 클러스터가 일부 리소스를 공유했음을 보여주었지만 , 이러한 연결 고리는 일시적인 것으로 평가됩니다 (그림 7).
  - 구체적으로 그러한 활동에는 코로나 19 대응과 관련된 글로벌 조직을 표적으로 한 캠페인이 포함되었습니다 . 이러한 작전 중 일부에서 APT43 의 하위 집단은 기존 멀웨어 툴을 공유하고 , 확장된 활동에서 처음 사용된 새로운 툴을 개발하고 , 의료 연구 및 관련 조직을 대상으로 지속적인 캠페인을 수행하는 등 다른 RGB 관련 조직과 긴밀하게 협력한 것이 거의 확실합니다 .
    - 이러한 캠페인에 사용하기 위해 다운로더 PENCILDOWN 과 같은 APT43 멀웨어에서 파생된 고유한 툴에는 PENDOWN, VENOMBITE 및 EGGHATCH 가 포함되었습니다 (모든 다운로더는 그림 7 참고).
    - 이러한 툴은 LOCABIN 및 LATEOP 와 같은 핵심 APT43 툴링과 함께 사용되었습니다 .
    - APT43 이 일반적으로 TEMP.Hermit 과 연결된 HANGMAN 백도어의 파생물인 HANGMAN.V2 와 같은 멀웨어 변종을 사용하는 것은 2020 년에 협력 작업 중에 어느 정도 교류가 발생했음을 시사합니다 .
- 이러한 명백한 그룹 간 활동은 'Bureau 325' 로 공개적으로 보고되었으며 'Cerium' 으로 보고된 활동과도 일치했습니다 .
- 또한 , 분류되지 않은 클러스터가 APT43 과 동일한 툴 중 일부를 활용하는 것으로 확인되었습니다 . 예를 들어 , PENCILDOWN 을 사용하는 클러스터는 암호화폐를 훔치기 위해 Android 모바일 지갑 앱을 해킹했습니다 .
- 반대로 , 별도의 사례에서 APT43 이 UNC1069 암호화폐 표적 공격과 밀접하게 관련된 툴인 LONEJOGGER 를 배포하는 것을 관찰했습니다 .
  - UNC1069 는 APT38 과의 연관성이 있다는 증거는 부족하지만 , 북한 사이버 범죄 조직으로 의심되는 조직입니다 .

오픈 소스에는 'Kimsuky' 로 알려진 추가 활동이 포함되는 경우가 많습니다 . 그러나 Mandiant 는 이러한 활동 , 특히 KONNI 및 관련 툴 CABRIDE 와 PLANEPATCH 같은 멀웨어 계열을 악용하는 활동을 개별적으로 계속 추적하고 있습니다 . 이러한 활동 클러스터가 APT43 과 겹치지만 , 연결 고리는 약하며 별도 그룹의 작업으로 판단됩니다 .

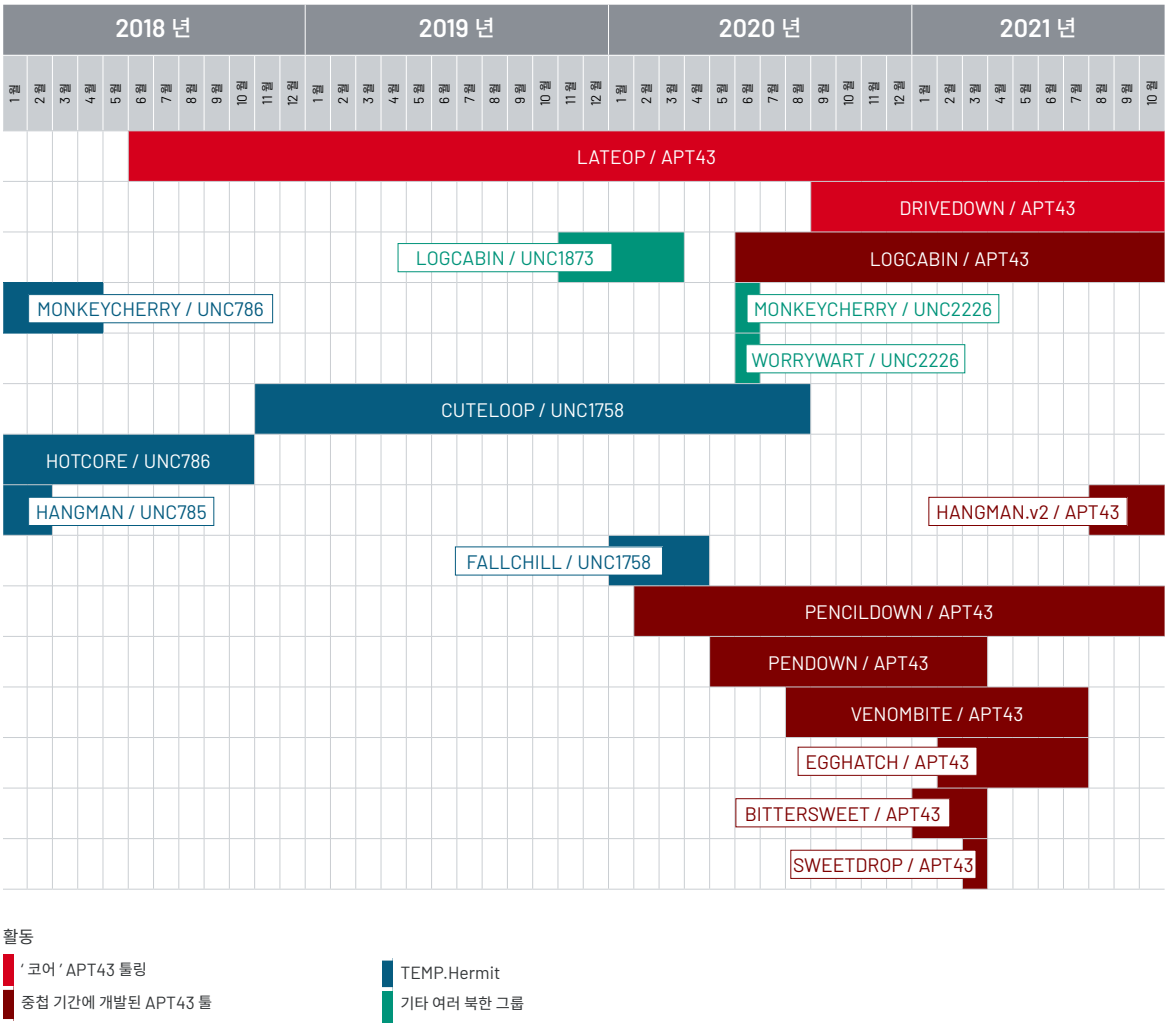

그림 7. 멀웨어 배포를 기반으로 APT43, TEMP.Hermit 및 기타 추적된 북한 클러스터 간 융합

멀웨어

APT43 은 비공개 멀웨어와 널리 사용되는 툴로 이루어진 상대적으로 큰 툴키트를 사용합니다 . APT43 에 대한 대부분의 오픈 소스 보고는 이 그룹이 LATEOP('BabyShark' 라고 알려짐) 를 사용한다고 추적했지만 , Mandiant 는 시간이 지남에 따라 이 그룹의 멀웨어 라이브러리가 꾸준히 진화 및 확장되는 것을 관찰했습니다 . 일부 툴은 이전 툴에서 코드를 많이 차용하여 개선 사항을 구현하고 기능을 추가했습니다 (그림 8).

- 이 그룹은 gh0st RAT, QUASARRAT 및 AMADEY 를 포함하여 공개적으로 사용 가능한 멀웨어를 배포했지만 , VisualBasic 스크립트를 기반으로 하는 백도어인 LATEOP 와 관련된 활동으로 훨씬 더 잘 알려져 있습니다 .
- APT43 은 일부 툴의 다양한 변종을 개발하여 다중 플랫폼을 표적으로 하는 공격을 지원했습니다 . 예를 들어 , Windows 기반 다운로더인 PENCILDOWN 의 Android 변종을 확인했습니다 .

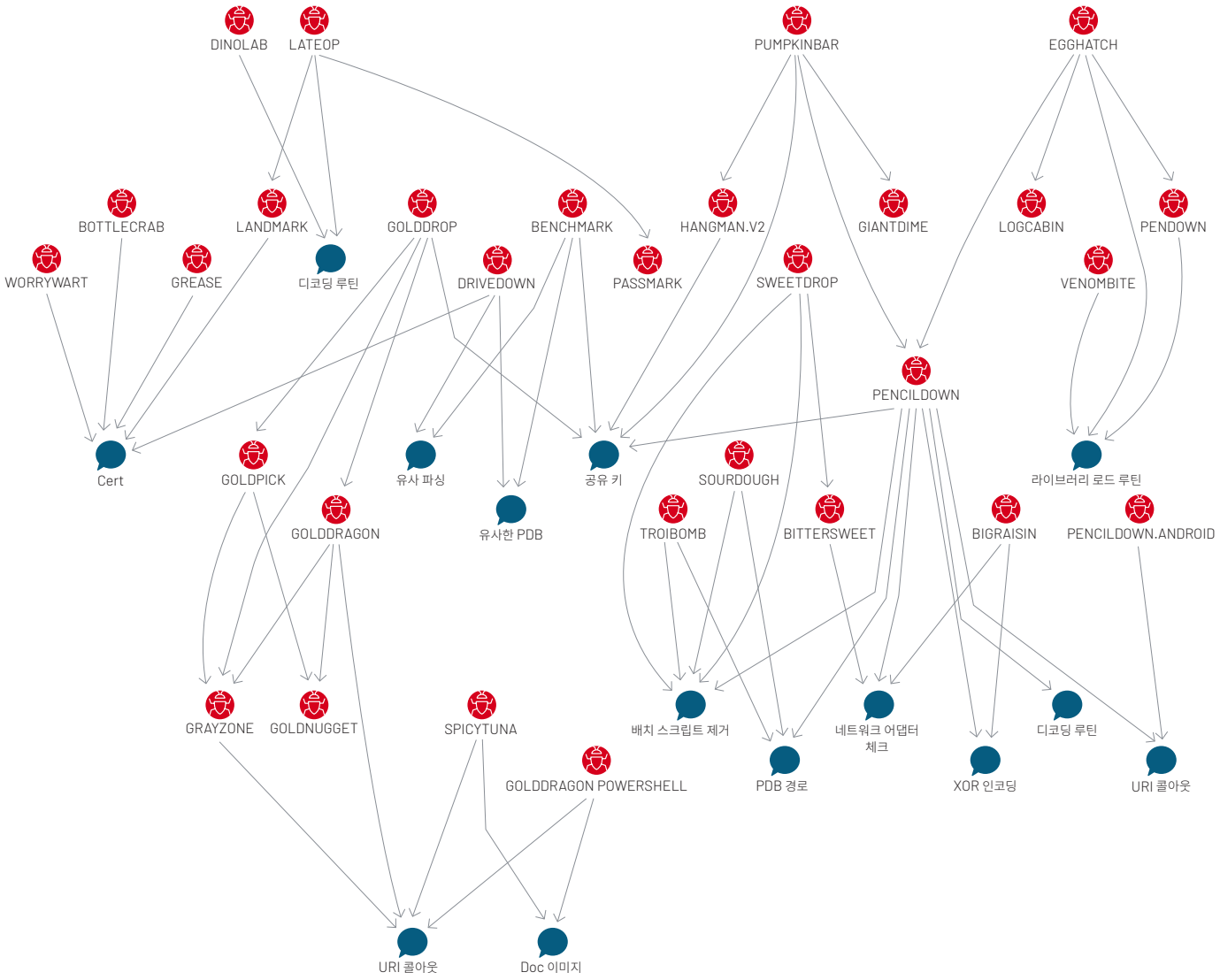

그림 8. APT43 이 사용하는 툴에서 중첩되는 코드 패밀리

전망 및 분석

북한의 국가적 우선순위에 급격한 변화가 없다면 , APT43 이 첩보 활동과 이를 지원하기 위한 금전적인 동기의 활동도 계속해서 매우 활발하게 수행할 것으로 예상합니다 . 사이버 역량에 대한 북한의 의존도가 증가하고 있으며 , APT43 이 부단히 작전을 전개하는 상황은 북한이 APT43 과 같은 그룹에 꾸준히 투자하고 의존하고 있음을 반영합니다 .

APT43 이 갑작스럽지만 , 일시적으로 의료 및 제약 관련 표적으로 전환한 것에서 알 수 있듯이 이들은 평양 지도부의 요구에 매우 민감하게 반응합니다 . 정부 , 군대 및 외교 기관을 대상으로 하는 스피어 피싱 및 크리덴셜 수집이 APT43 의 핵심 임무이지만 , 금전적 동기의 사이버 범죄를 수행하는 등 궁극적으로 후원자인 북한 정권을 지원하기 위해 필요에 따라 표적 , 전술 , 기술 및 절차를 수정합니다 .

기술 부록 : 공격 라이프사이클

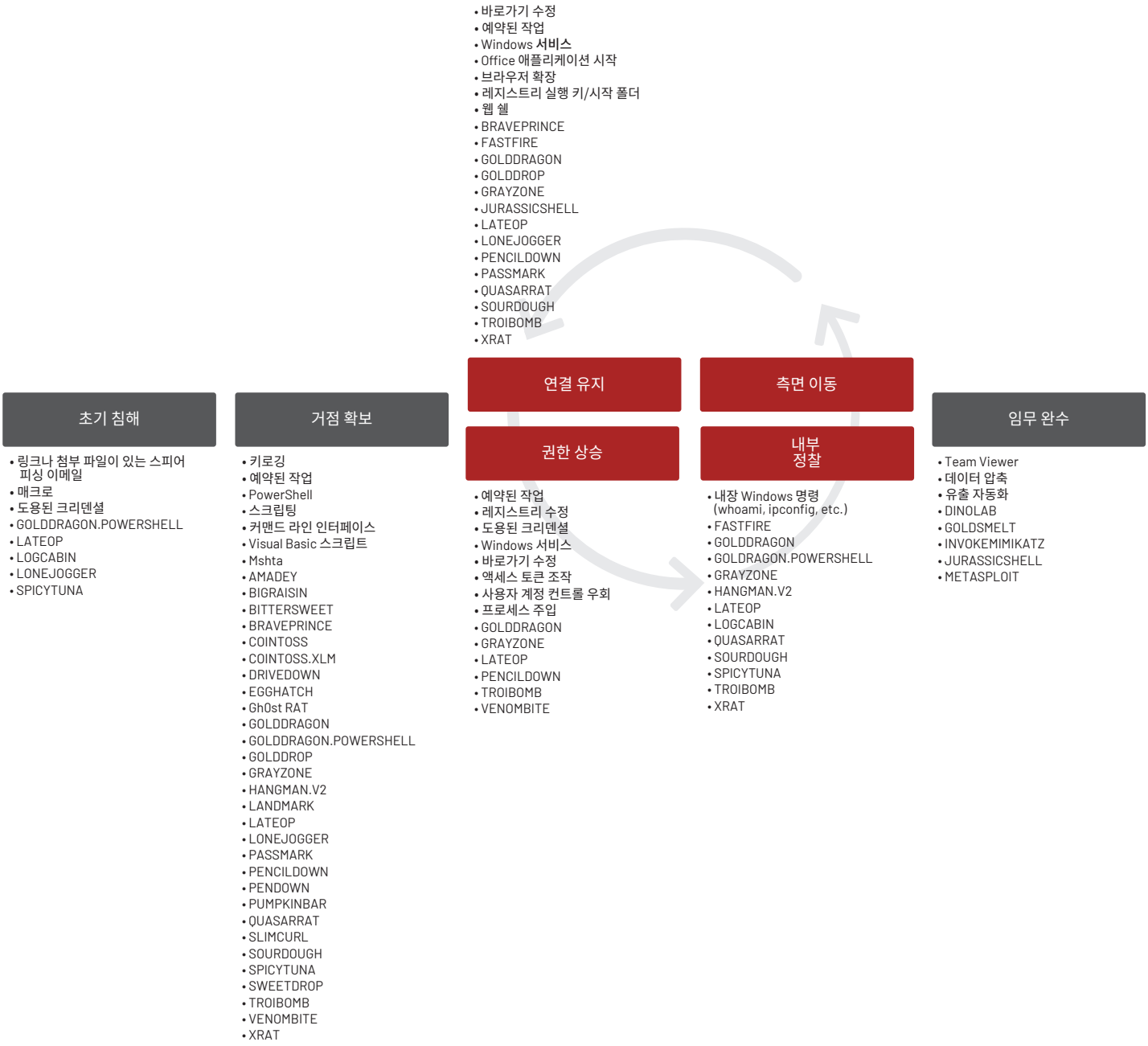

그림 9. APT43 공격 라이프사이클

기술 부록 : MITRE ATT&CK

초기 액세스	
T1566	피싱
T1566.001	스피어피싱 첨부 파일
T1566.002	스피어피싱 링크

리소스 개발	
T1583.003	가상 사설 서버
T1584	인프라 침해
T1588.003	코드 서명 인증서
T1588.004	디지털 인증서
T1608.003	디지털 인증서 설치
T1608.005	표적 링크

실행	
T1047	Windows 관리 도구
T1053.005	예약된 작업
T1059	커맨드 및 스크립트 인터프리터
T1059.00:	PowerShell
T1059.003	Windows 커맨드 셸
T1059.005	Visual Basic
T1059.007	JavaScript
T1129	공유 모듈
T1203	클라이언트 실행을 위한 익스플로잇
T1204.001	악성 링크
T1204.002	악성 파일
T1569.002	서비스 실행

커맨드 및 컨트롤	
T1071.001	웹 프로토콜
T1071.004	DNS
T1090.003	멀티홉 프록시
T1095	비 애플리케이션 계층 프로토콜
T1102	웹 서비스
T1102.002	양방향 통신
T1105	인그레스 툴 전송
T1132.001	표준 인코딩
T1573.002	비대칭 암호화 방식

검색	
T1007	시스템 서비스 검색
T1010	애플리케이션 창 검색 (Application Window Discovery)
T1012	쿼리 레지스트리
T1016	시스템 네트워크 구성 검색
T1033	시스템 관리자 / 사용자 검색
T1057	프로세스 검색
T1082	시스템 정보 검색
T1083	파일 및 디렉터리 검색
T1087	계정 검색
T1518	소프트웨어 검색
T1614.001	시스템 언어 검색

수집	
T1056.001	키로깅
T1113	화면 캡처
T1115	클립보드 데이터
T1213	정보 리포지토리의 데이터
T1560	저장된 수집 데이터
T1560.001	유틸리티를 통해 저장

지속성	
T1137	Office 애플리케이션 시작
T1505.00	웹 셸
T1543.003	Windows 서비스
T1547.001:	레지스트리 실행 키 / 시작 폴더
T1547.004	Winlogon Helper DLL
T1547.009	바로가기 수정

보안 회피	
T1027	난독화된 파일 또는 정보
T1027.001	바이너리 패딩
T1027.002	소프트웨어 패킹
T1027.005	툴에서 지표 제거
T1027.009	임베디드 페이로드
T1036	가장
T1036.001	잘못된 코드 서명
T1036.007	이중 파일 확장자
T1055	프로세스 주입
T1055.001	동적 링크 라이브러리 주입
T1055.003	실행되는 스레드 하이재킹
T1070.004	파일 삭제
T1070.006	타임스톰프 (Timestomp)
T1112	레지스트리 변경
T1134	액세스 토큰 조작
T1140	파일 또는 데이터 복호화 / 디코딩
T1218.005	Mshta
T1497	가상화 / 샌드박스 회피
T1497.001	시스템 점검
T1548.002:	사용자 계정 제어 우회
T1553.002	코드 서명
T1564.003	숨겨진 창
T1564.007	VBA 스톰핑
T1620:	반사 코드 로딩
T1622	디버거 회피

영향	
T1489	서비스 중단
T1529	시스템 셧다운 / 재부팅

유출	
T1020	유출 자동화

크리덴셜 액세스 :	
T1110	무차별 대입
T1555.003	웹 브라우저의 크리덴셜

기술 부록 : APT43 이 사용하는 멀웨어

멀웨어군	역할	가용성	설명
AMADEY	다운로더	공개	AMADEY 는 C 로 작성된 다운로더로 , HTTP 를 통해 페이로드를 검색합니다 . 다운로드된 페이로드를 디스크에 쓰고 실행합니다 .
BENCHMARK	드로퍼	비공개	BENCHMARK 는 C/C++ 로 작성된 드로퍼로 , 파일 이름을 읽고 하드 코딩된 경로에서 Base64 로 인코딩된 페이로드를 추출하고 페이로드를 디코딩하여 디스크에 드롭합니다 .
BIGRAISIN	백도어	비공개	BIGRAISIN 은 C\C++ Windows 기반 백도어입니다 . 다운로드한 명령 실행 , 다운로드한 파일 실행 및 파일 삭제가 가능합니다 .
BITTERSWEET	다운로더	비공개	BITTERSWEET 는 C/C++ Windows 다운로더입니다 . 다음 단계를 디스크에 다운로드하고 실행하기 전에 기본 시스템 정보를 수집합니다 .
BRAVEPRINCE	다운로더	공개	BRAVEPRINCE 는 C/C++ 다운로더입니다 . 수집한 시스템 정보를 업로드하고 파일을 다운로드하기 위해 Daum 이메일 서비스를 이용합니다 .
COINTOSS COINTOSS.XLM	다운로더	비공개	COINTOSS 는 C/C++ 다운로더입니다 . WMIC(Windows Management Instrumentation 명령줄) 유틸리티를 사용하여 FTP 를 통해 페이로드를 다운로드합니다 . 그런 다음 COINTOSS 는 배치 스크립트를 생성하고 실행하여 자체적으로 제거합니다 .
DINOLAB	빌더	비공개	DINOLAB 은 C/C++ 빌더입니다 . 파일을 암호화 및 복호화하고 , VBS 스크립트를 난독화하고 , 파일을 감염시키는 데 사용됩니다 .
DRIVEDOWN	다운로더	비공개	DRIVEDOWN 은 포함된 스크립트를 실행하고 OneDrive 에서 단계를 다운로드할 수 있는 C/C++ Windows 다운로더입니다 .
EGGHATCH	다운로더	비공개	EGGHATCH 는 C/C++ Windows 다운로더입니다 . mshta.exe 를 사용하여 스크립트를 다운로드하고 실행합니다 .
FASTFIRE	백도어	비공개	FASTFIRE 는 서버에 연결하고 침해된 장치의 세부 정보를 커맨드 및 컨트롤 (C2) 로 다시 보내는 악성 APK 입니다 .
Gh0st RAT	백도어	공개	GH0ST 는 C++ 로 작성된 백도어로 , TCP 또는 UDP 를 통해 사용자 지정 바이너리 프로토콜을 사용하여 통신합니다 . 각 메시지의 시작 부분에 패킷 서명이 있는데 , 일반적으로 샘플마다 다릅니다 .
GOLDDRAGON GOLDDRAGON. POWERSHELL	다운로더	비공개	GOLDDRAGON 은 C 로 작성된 다운로더 , HTTP 를 통해 원격 서버에서 페이로드를 검색합니다 . 다운로드한 페이로드는 디스크에 기록되고 실행됩니다 . GOLDDRAGON 은 또한 Hangul 워드프로세서 문서에서 페이로드를 추출해 시작 디렉터리에 기록합니다 . 결과적으로 현재 사용자가 로그인하면 새 파일이 실행됩니다 .
GOLDDROP	드로퍼	비공개	GOLDDROP 은 C/C++ Windows 드로퍼입니다 . 리소스 파일을 복호화하여 파일 시스템에 저장한 다음 다른 프로세스에 삽입합니다 .
GOLDSMELT	유틸리티	비공개	GOLDSMELT 는 rundll32.exe 프로세스를 닫고 로그에 사용되는 파일을 삭제하는 데 사용되는 C/C++ 유틸리티입니다 .
GRAYZONE	백도어	비공개	GRAYZONE 은 C/C++ Windows 백도어로 시스템 정보를 수집하고 , 키보드로 입력하는 내용을 몰래 기록하고 , C2 서버에서 추가 단계를 다운로드할 수 있습니다 .
HANGMAN.V2	백도어	비공개	HANGMAN.V2 는 백도어 HANGMAN 의 변종입니다 . HANGMAN.V2 는 HANGMAN 과 매우 유사하지만 , 네트워크 통신에 HTTP 를 사용하고 C2 서버로 전달되는 데이터 형식이 다릅니다 .
Invoke-Mimikatz	크리덴셜 도용	공개	Invoke-Mimikatz 는 Mimikatz 크리덴셜 유출 DLL 을 메모리에 반사적으로 로드하는 PowerShell 스크립트입니다 .
JURASSICSHELL	유틸리티	비공개	JURASSICSHELL 은 공격자가 파일을 다운로드하고 업로드할 수 있는 PHP 파일 관리 웹 셸입니다 .

멀웨어군	역할	가용성	설명
LANDMARK LANDMARK.NET	런처	비공개	LANDMARK 는 desktop.r5u 로 저장된 디스크에 파일을 로드하고 실행하는 C/C++ Windows 시작 프로그램입니다 .
LATEOP LATEOP. V2	데이터 마이너	비공개	LATEOP 는 표적 시스템의 다양한 특성을 열거하고 임의의 추가 Visual Basic 콘텐츠를 실행할 수 있는 데이터 마이닝 Visual Basic 스크립트입니다 . LATEOP 의 일부 배포로 인해 PASSMARK 크리덴셜 도용 페이로드가 다운로드 및 실행되었습니다 . 반대로 LATEOP.v2 의 일부 배포는 BENCHMARK 소스 감염에서 비롯되었습니다 .
LOGCABIN	백도어	비공개	LOCABIN 은 여러 단계로 구성된 파일리스 모듈식 백도어입니다 . 단계는 다운로드 및 실행되는 여러 Visual Basic 및 PowerShell 스크립트로 구성됩니다 . LOCABIN 은 자세한 시스템 정보를 수집하여 추가 명령을 수행하기 전에 C2 로 전송합니다 .
LONEJOGGER	다운로더	비공개	LONEJOGGER 는 암호화폐 서비스 (거래소 및 투자 회사 포함) 를 표적으로 하는 것으로 관찰된 다운로더 / 드로퍼이며 .lnk 바로 가기를 사용하여 보호된 HTML 애플리케이션 페이로드를 다운로드합니다 .
METASPLOIT	프레임워크	공개	METASPLOIT 는 취약성 테스트 , 네트워크 열거 , 페이로드 생성 및 실행 , 방어 회피 기능을 제공하는 침투 테스트 프레임워크입니다 .
PASSMARK	프레임워크	공개	PASSMARK 는 웹 브라우저 및 이메일 애플리케이션에서 사용자 이름과 암호를 훔치는 자격 증명 수집기입니다 . PASSMARK 는 PassView 도구에서 파생된 것 같습니다 .
PENCILDOWN PENCILDOWN. ANDROID	다운로더	비공개	PENCILDOWN 은 C/C++ Windows 기반 다운로더입니다 . PENCILDOWN 은 기본 시스템 정보를 수집하여 다음 단계를 받기 전에 C2 서버로 전송합니다 . 다음 단계는 메모리에 로드되거나 응답의 플래그를 기반으로 직접 실행됩니다 .
PENDOWN	다운로더	비공개	PENDOWN 은 C++ 로 작성된 다운로더로 , HTTP 를 통해 페이로드를 검색합니다 . 다운로드한 파일은 디스크에 저장되고 실행됩니다 .
PUMPKINBAR	드로퍼	비공개	PUMPKINBAR 는 C/C++ 드로퍼입니다 . PUMPKINBAR 는 그 안에 인코딩 및 임베디드된 여러 페이로드를 포함할 수 있습니다 . 각 페이로드를 디코딩하는 키는 PUMPKINBAR 실행 파일 끝에 추가됩니다 . 페이로드가 디스크에 드롭되고 실행됩니다 .
QUASARRAT	백도어	공개	QUASARRAT 는 공개적으로 사용 가능한 Windows 백도어입니다 . 웹 사이트를 방문하여 파일을 다운로드 , 업로드 및 실행할 수 있습니다 . QUASARRAT 는 시스템 정보를 획득하거나 , 원격 데스크톱 또는 셸 역할을 하거나 , 웹캠을 원격으로 활성화할 수 있습니다 . 이 백도어는 키 입력을 기록하고 일반적으로 사용되는 브라우저 및 FTP 클라이언트에서 암호를 훔칠 수도 있습니다 . QUASARRAT 은 2015 년 8 월 개발자가 이름을 바꾸기 전에 원래 xRAT 로 불렸습니다 .
SLIMCURL	다운로더	비공개	SLIMCURL 은 C/C++ 다운로더입니다 . Base64 로 인코딩된 Google 드라이브 링크로 다음 단계를 포함합니다 . 다음 단계는 cURL 을 사용하여 다운로드됩니다 .
SOURDOUGH	백도어	비공개	SOURDOUGH 는 C 로 작성된 백도어로 , HTTP 를 통해 통신합니다 . 그 기능에는 키로깅 , 스크린샷 캡처 , 파일 전송 , 파일 실행 및 디렉터리 열거가 포함됩니다 .
SPICYTUNA	다운로더	비공개	SPICYTUNA 는 VBA 다운로더입니다 . 기본 시스템 정보를 수집하고 추가 단계를 다운로드하여 실행할 수 있습니다 .
SWEETDROP	드로퍼	비공개	SWEETDROP 은 C/C++ Windows 드로퍼입니다 . 포함된 바이너리 리소스를 파일 시스템에 드롭하고 실행합니다 .

멀웨어군	역할	가용성	설명
TROIBOMB	백도어	비공개	TROIBOMB 은 시스템 정보를 수집하고 C2 서버에서 명령을 수행할 수 있는 C/C++ Windows 백도어입니다 .
VENOMBITE	다운로더	비공개	VENOMBITE 는 PENDOWN 에서 진화한 C/C++ Windows 다운로더입니다 . 동일한 사용자 지정 인코딩 루틴을 사용하지만 , 네트워크 기능이 포함된 실행 파일로 이동되었습니다 . 다운로드한 파일은 메모리에 로드되어 실행됩니다 .

기술 부록 : 샘플 APT43 침해 지표 (IoC)

멀웨어군	샘플 MD5	SHA1	SHA256
AMADEY	982fc9ded34c854 69269eacb1cb4ef26	e205ed81ccb99641dcc 6c2799d32ef0584fa2175	557ff6c87c81a2d2348bd8d667ea8412a1a 0a055f5e1ae91701c2954ca8a3fdb
BENCHMARK	de9a8c26049699d bbd5d334a8566d38d	47a32bc992e5d4613b3 658b025ab913b0679232c	43c2d5122af50363c29879501776d907ea a568fa142d935f6c80e823d18223f5
BIGRAISIN	144bd7fd423edc3 965cb0161a8b82ab2	1087efbd004f65d226bf 20a52f1dc0b3e756ff9e	2b78d5228737a38fa940e9ab19601747c68 ed28e488696694648e3d70e53eb5a
BITTERSWEET	cd83a51bec0396f 4a0fd563ca9c929d7	f3b047e6eb3964deb04 7767fad52851c5601483f	fb7fb6dbaf568b568cd5e60ab537a42d59 82949a5e577db53cc707012c7f20e3
BRAVEPRINCE	33df74cbb60920d 63fe677c6f90b63f9	539acd9145befd7e670f e826c248766f46f0d041	94aa827a514d7aa70c404ec326edaaad4b 2b738ffaea5a66c0c9f246738df579
	ebaf83302dc78d9 6d5993830430bd169	bc6cb78e20cb2028514 9d55563f6fdcf4aaafa58	5cbc07895d099ce39a3142025c557b7fac 41d79914535ab7ffc2094809f12a4b
COINTOS	b846fa8bc3a55fa 0490a807186a8ece9	c0c6b99796d732fa534 02ff49fd241612a340229	855656bfecc359a1816437223c4a133359e 73ecf45acda667610fbe7875ab3c8
COINTOSS.XLM	f92a75b98249fa61 cf62e8b63cb68fae	e5b312155289cdc6a80 a041821fc82d2cca80bcd	d0971d098b0f8cf2187feeed3ce049930f 19ec3379b141ec6a2f2871b1e90ff7
DRIVEDOWN	1dcd5afeccfe204 0895686eefa0a9629	40826e2064b59b8b7b3 e514b9ef2c1479ac3b038	07aed9fa864556753de0a664d22854167a 3d898820bc92be46b1977c68b12b34
	5fe4da6a1d82561a1 9711e564adc7589	e79527f7307c1dda62c4 2487163616b3e58d5028	8d0bafca8a8e8f3e4544f1822bc4bb08ce aa3c7192c9a92006b1eb500771ab53
EGGHATCH	e8da7fcdf0ca67b 76f9a7967e240d223	b0c2312852d750c4bce b552def6985b8b800d3f3	9dac6553b89645ac8d9e0a3dc877d1264 1e6d05fb52e8de6ae5533b2bdf0abc9
FASTFIRE	2bf26702c6ecbd4 6f68138cdcd45c034	1b9a4c0a5615a4f96a04 1d771646c1a407b17577	38d1d8c3c4ec5ea17c3719af285247cb1d8 879c7cf967e1be1197e60d42c01c5
Gh0st RAT	2d330c354c14b39 368876392d56fb18c	a1f72c890d0b920f4f4c b2d59df6fa40734de90d	f86d05c1d7853c06fc5561f8df19b53506b 724a83bb29c69b39f004a0f7f82d8
GOLDDRAGON	15ec5c7125e6c74f 740d6fc3376c130d	fb09b89803da071b7b7e b23244771c54d979a873	4a1c43258fe0e3b75afc4e020b904910c9 4d9ba08fc1e3f3a99d188b56675211
GOLDDRAGON. POWERSHELL	2a5562de1d3e734 d9328a1c78b43c2e5	4b0d0ebb0c676efe855 bed796221dd475a39ba40	203ea478fa4d2d5ef513cad8b51617e0c9f 7571bf3a3becf9c267a0d590c6d72
GOLDDROP	0cc0aa5877cec91 09b7a5a0e3a250c72	1d49d462a11a00d8ac96 08e49f055961bf79980d	1324acd1f720055e7941b39949116dfe72ce 2e7792e70128f69e228eb48b0821
	2c530adb84111436 6ce6177ce964a5e6	5b69e3e5f4f49cf8b635 a57a8c92e17a4f130d50	873b8fb97b4b0c6d7992f6af1565329578 8526def41f337c651dc64e8e4aeebd
GOLDSMELT	c066b81c4b8b070 3f81f8bc6fb432992	2508f5ff0c28356c0c3f 8e6cae7b750d53495bca	63b4bd01f80d43576c279adf69a5582129 e81cc4adbd0367590581643765ea8
GRAYZONE	1d30dfa5d8f21d14 65409b207115ded6	942fd7b4ef1ccf7032a4 0acad975c7b5905c3c77	ed0161f2a3337af5e27a84bea85fb4abe35 654f5de22bcb8a503d537952b1e8a
HANGMAN.V2	21cffaa7f9bf224ce 75e264bfb16dd0d	862abce03f7f5de0c466 fdbd24ad796578eaa110	a605570555620cea6d6be211520525fc95 a30961661780da4cc4bafe9864f394

멀웨어군	샘플 MD5	SHA1	SHA256
Invoke-Mimikatz	20bc53deb7b12145 80e9d9efeaa5e9d7	e74b816f1c6d6347cb40 121e0b50dadd0d8f1f97	908777e581616156576636568 61c212ac2569 6741ef69411021474158fa2b4cf
JURASSICSHELL	9cdda333432f403 b408b9fe717163861	d80be054a569df5f20 1191dcc4fea0dde9622da5	d2f4bf0caed5a442198fcdc43c83c7b27ae 04f341a72b270c9ed40778aa77afe
	ddae18c65d583b4 1a2157d496a4bde61	63e113f0a906af82903 dbfac3e78bdd2d146e738	a4ba1e6ab678a1bdf8bc05bea8310d74392 8a4e2c05bad104e61afdd9cccf9a1
LANDMARK	1ffccf6cb3b74d68 df2b899fd33127a5	a61f009e73ae81a18751e 9aee39f8121a3902280	da22d327124a0ee6a93cd07e85f9804fbc 98eda87824ddcf7c8a63d349e87034
LANDMARK.NET	60efecf4e1b5b2c5 80329e9afa05db15	12c508ace6e8aa42be0 2750d759e720b800bf796	034d29fb89a8f68ba714f1868b2181c4cd5 9d4a2604630ef1554a6ccf3fe6d75
LATEOP LATEOP. V2	0f77143ce98d0b9 f69c802789e3b1713	7da4e8b743478370fa41 fe39a45e3ff2ca2194b3	54a8b8c933633c089f03d07cfbd5cafbf7 6a6d7095f2706d6604e739bb9c950f
LOGCABIN	0b558ee89a7bb32 968ef78104f6b9a28	b7fdb5e5b31adfc5ada0 de1e05b0c069968e5bce	79c0fe1467dada33e0b097dd772c362296 18b7091baa5f10da083f894192a237
LONEJOGGER	139d2561f5c72fab b099a12c16b8960c	2dd269608dd7f4da171d 1a220fe97347162008c7	2c338055e8245057169f1733846e0490bc 4ae117d1dadefe0a3f07a63dc87520
	14a00f517012279a f53118a491253e5c	98040f42103ce3b840d d54bf3490587f141a0bc3	26a98b752fd8e700776f11bad4169a06708 24d5b5b9337f3c8f46fac33bc03e8
METASPLOIT	37e7d679cd4aa78 8ec63f27cb02962ea	7d66c1f36b4b48d99046 1ec44d626793ade6a8d1	b55e9d65a3130f543360a9c488d35475d4 789ee7a32a4e94d02f33c21a172bcb
PASSMARK	b077ba5af1dfbd4a c523923eab56bcd4	4e93797dd3b383050cf 0ee585aa5b5525efb2380	4a08b78d410bc3d9b78dd63b146767f293 dc3f3f6f8092352d2aa2f589e9c772
PENCILDOWN	04d0856afb1aa916 8377d6aa579c5403	f3b774e921eaad9335b9 c057dd49b918c5dae4a6	e637c86ae20a7f36a0ad43618b00c48f47 b5591a03af3fb689a16c45afa43733
PENCILDOWN. ANDROID	4626ed60dfc8dea f75477bc06bd39be7	a9ff1ebb548f5bba600d 38e709ff331749fa9971	2365a48f7d6cf6dcc83195f06ea11b93c95 5c3a491c60b50ba42788917ba22e2
PENDOWN	768c84100d6e318 1a26fa50261129287	6f4b6938ac8fd9591fc3 99219dbaf4347d8b444b	780e7edbfad5f68051c2039036b00b304d 3f828fdbee85d2d09edbcc6d07ea34
PUMPKINBAR	946f787c129bf469 298aa881fb0843f4	d3b233d6d8b11235929e 4a0cbdb12eefdd47d927	32beeda8cffc2ecc689ea2529194cf80695 5879a334ec68176864d1e6c09800c
	c9d70bf37017260 9da848fa785989939	851ba2182b37bc738042 0a986840e16f73947413	ba3c79dbeca0234fa838ae4c95640911555 6f437372aeeb0737206d71caf4a38
QUASARRAT	0085bc8ce16ef176 43909c4799ead02b	25d94c9ab7635ff330da be96780f330f7f2ba775	a9c404e100bfd2716a8f6bfafc07b0bd617 5bedb047d10b94390c79249258272
SLIMCURL	68ce092f1a3d1985 2ea32db8388de5c7	700acc4e48eae84f80f 4dbaf74bf60b79efd49bd	25c2f4703cbaa1ff4dbcfcc16a10b29ef35c cc174b71b21de360d898540889f8
SOURDOUGH	7e609404cc258bb e283bea6ddd7af293	6618e25dd49b68f7b2 b266eb2d787e6f05c964bc	502136707a70b768800640224e48c6340 57dc651892113b62522f0dd2fcf1e87

멀웨어군	샘플 MD5	SHA1	SHA256
SPICYTUNA	0821884168a644f3 c27176a52763acc9	1f6c7c9219f6b6ea30c d481968ae1a038789be67	e7fae41c0bd8d3d95253bd75dce9901559 9ecc404bd8d737cec305fc3e4dd018
	8ca84c206fe8436 dcc92bf6c1f7cf168	636f2c20183b45691b 742949d49b3d6c218c9cce	7943bf9cc7b2adf50f7f92dd37347381e6d 0aef23b34a3cd0a3afcda1d72e16d
SWEETDROP	해당 없음	해당 없음	해당 없음
TROIBOMB	18df13900f118158c33	11f646095495d625e7d	98d4471fe549bb3067a
	df904c662e875	71038578cc838a6d5e111	c2f2d9afd50ed1baaddab41ec427083498 9e7f1ade14d
VENOMBITE	107f917a5ddb4d3947 233fbc9d47ddc8	75c516dde8415494c2 88e349d440ce778dede8e3	2d41b04f5d86047dc2353a10595418b0d5 239c22112f36eb9d253b2e8b6eb0d0

자세한 정보 : **www.mandiant.kr**

Mandiant
서울특별시 강남구 테헤란로 518 섬유센터빌딩 13 층 101 호

02-2138-3191
korea@mandiant.com

Mandiant 소개

Mandiant 는 역동적 사이버 방어, 위협 인텔리전스 및 침해 사고 대응 서비스 분야에서 인정받는 리더로서, 수십 년간 사이버 보안의 최일선에서 쌓아온 경험을 확장하여 조직이 사이버 위협에 맞서 대응 태세를 갖출 수 있도록 지원합니다. Mandiant 는 이제 Google Cloud 의 자회사가 되었습니다.

MANDIANT
NOW PART OF Google Cloud