IBM Security

X-Force 위협 인텔리전스 지표 2020

IBM

작성: IBM X-Force 사고 대응 및 인텔리전스 서비스(IRIS)

목차

목차

개요 및 주요 동향

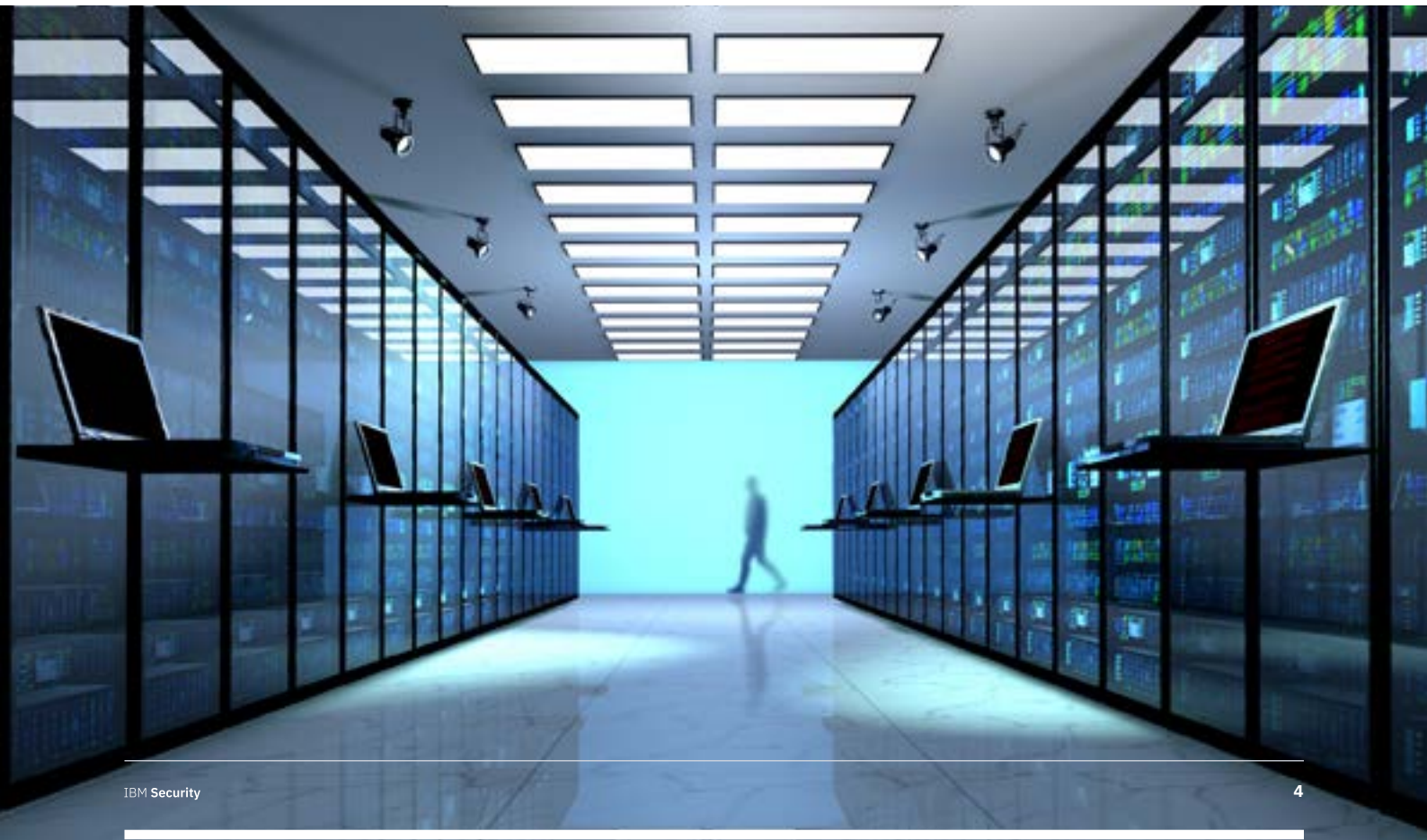
IBM Security는 지능형 엔터프라이즈 보안 솔루션 및 서비스를 개발해, 고객의 비즈니스가 현재의 탄력성 구축을 통해 미래의 사이버 보안 위협에 대비하도록 도와줍니다.

보안 전문가에게 가장 관련성이 높은 위협에 대한 가장 최근의 정보를 제공하기 위해, IBM® X-Force®는 정기적으로 블로그, 백서, 웨비나 및 팟캐스트를 통해 새로 등장한 위협, 공격자의 전술, 기술 및 절차(TTP)에 대한 자료를 공개합니다.

IBM Security®는 매년 다양한 연구 팀이 제기한 가장 두드러진 위협에 기준해 전년도를 정리한 IBM X-Force 위협 인텔리전스 지표를 발표해 보안 팀에 조직의 보안을 강화할 수 있는 정보를 제공합니다.

이 보고서에 제시된 데이터 및 해석은 IBM Security 관리 보안 서비스, 사고 대응 서비스, 침투 테스트 용역 및 취약성 관리 서비스를 통해 얻었습니다.

IBM X-Force 연구 팀은 스팸 센서나 허니넷 같은 비 고객 자산에서 도출된 데이터와 함께, 수천만 개에 달하는 보호형 엔드포인트 및 서버의 데이터를 분석합니다. IBM Security Research는 또 전 세계에서 스팸 트랩을 실행하고 매일 수천만 건의 스팸 및 피싱 공격을 모니터링하면서 수십억 개의 웹 페이지 및 이미지를 분석해서 공격 작전, 사기 활동 및 브랜드 악용을 탐지함으로써 고객과 우리가 사는 서로 연결된 세계를 더 효과적으로 보호합니다.



IRIS(X-Force 사고 대응 및 인텔리전스 서비스)가 지난 해 IBM 보안 소프트웨어 및 보안 서비스 분석을 해석한 결과 2019년은 예전 위협이 새로운 방법으로 이용돼 다시 출현한 해였습니다.

— X-Force 데이터에 따르면 2019년 운영 기술(OT)을 표적으로 한 사고의 2,000% 증가로 2020년으로 넘어갈 때는 산업 시스템을 공격하려는 위협 활동가의 관심이 높아질 수가 있다고 합니다.

— 2019년에는 85억 개가 넘는 기록이 손상되었는데 이 수치는 2018년에 손실된 기록 수보다 200% 이상 큰 수치입니다. 이런 큰 증가는 대부분 내부자에게 책임이 있을 수 있습니다. 잘못 구성된 서버(퍼블릭 액세스가 가능한 클라우드 스토리지, 보안이 되지 않은 클라우드 데이터베이스 및 부적절한 보안이 된 rsync 백업 또는 오픈 인터넷 연결 네트워크 영역 스토리지 장치 포함) 때문에 노출된 기록이, 2019년에는 손상된 기록의 86%를 차지했습니다.

— 2019년에는 위협 활동가가 랜섬웨어로 다시 봇넷 구축을 하면서 맬웨어 환경이 바뀌었습니다. 2019년 내내 X-Force IRIS는 13개 산업에 걸쳐 5개 대륙의 12개 국가에서 랜섬웨어 용역에 응했습니다. 또 파괴적인 맬웨어 활동은 이런 잠재적으로 치명적인 맬웨어 동향이 계속적으로 증가하는 위협이 되고 있음을 보여 줍니다.

— 2019년 X-Force IRIS 용역에서 발견된 3대 최초 감염 벡터는 서로 매우 근소한 차이로, 1위, 2위 및 3위는 다음과 같습니다. 최초 감염 벡터에서 1위, 2위 및 3위는 각각 피싱(31%), 취약점 스캔 및 익스플로잇(30%) 및 자격 증명 도난 사고(29%)입니다. 피싱은 2018년에는 전체 사건 중 거의 절반을 차지했던 것이 2019년에는 3분의 1 미만으로 이 점은 가장 눈에 띄었습니다. 이와 반대로, 취약점 스캔 및 익스플로잇은 2018년에는 8%에 그쳤던 것이 거의 전체 사건의 3분의 1 수준까지 증가했습니다.

— 글로벌 스팸 활동에 대한 X-Force 분석에 따르면 스팸 이메일은 오로지 다음과 같은 두 CVE에만 특별한 중점을 두고 취약점의 제한된 서브세트를 계속 이용한다고 합니다. 그 두 CVE는 2017-0199와 2017-11882입니다. 이 두 CVE는 모두가 다 패치가 된 취약점으로 공격자들이 스팸 작전을 통해서 악용하려는 취약점의 거의 90%를 차지했습니다.

— 2019년 금융 서비스는 가장 많이 표적이 된 부문의 자리를 유지했지만 산업별 표적 대상에서는 소매, 미디어, 교육 및 정부가 모두 가장 많이 표적이 된 부문의 글로벌 차트에서 상승해, 위협 활동가의 우선 순위 변화가 눈에 띄었습니다.

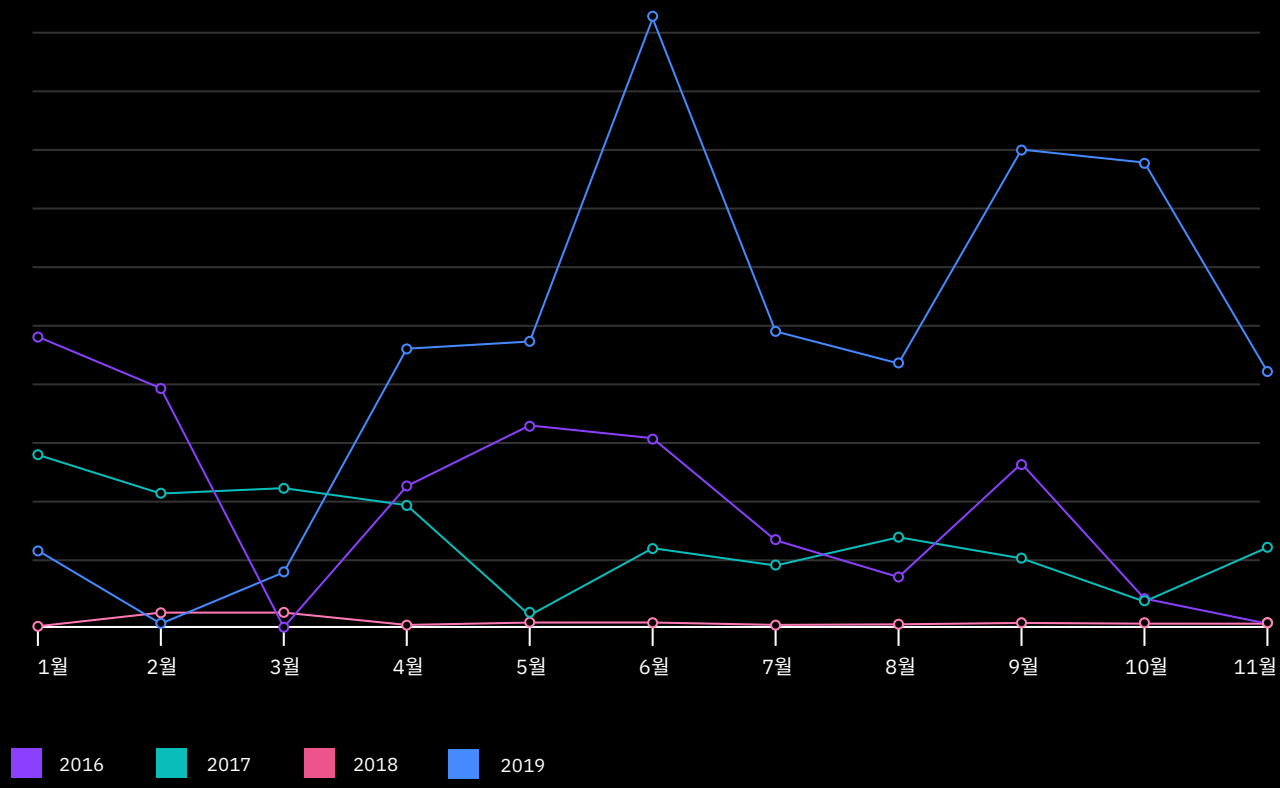
— 올해에는 X-Force 위협 인텔리전스 지표에 새롭게 지역 중심의 해석을 도입해서 전 세계에서 관찰된 동향 데이터를 제공합니다. IBM Security는 모든 지역을 표적으로 하는 여러 위협 활동가를 계속 추적하고 있고, 이 보고서에서는 각 지역을 표적으로 하는 주요 위협 활동가, 2019년에 관찰된 공격 및 2020년의 사이버 보안적 관심의 가능한 시기에 대한 내용에 역점을 두었습니다.

이 연간 보고서의 다음 섹션에서는 최상위 동향을 검토하고 2019년의 동향을 이룬 내용에 대한 정보를 세부적으로 다룹니다.

표적 대상 및 최초 감염 벡터

그림 1:
운영 기술(OT) 공격 동향

2016 ~ 2019년 월별 OT 공격량 비교(출처: IBM X-Force)



운영 기술(OT) 인프라 표적 대상의 폭발적인 증가

IBM X-Force 데이터에 따르면 위협 활동가가 산업 제어 시스템(ICS) 및 유사 운영 기술(OT) 자산을 표적으로 한 이벤트가 2018년 이후 2,000% 이상 증가했다고 합니다. 실제로 2019년에는 OT 자산을 표적으로 했던 이벤트 횟수가 이런 활동에 대해 지난 3년간 관찰된 활동량보다 많았습니다.

관찰된 공격의 대부분은 SCADA와 ICS 하드웨어 구성 요소 내에 알려진 취약점 조합 및 ICS 표적에 무차별 대입 로그인 전술로 비밀번호를 뿌려대는 공격을 통해서 이루어졌습니다.

ICS 공격에 중점을 둔 일부 보고된 활동은 알려진 두 위협 활동가와 연관되어 있었고, 원격 측정으로 관찰한 공격 타임라인에서 급격한 증가가 발생한 것과도 일치했습니다. 두 특정 작전의 주체는 Xenotime 그룹 및 IBM Hive0016(APT33)로 보고된 바에 따르면 이들은 자신의 공격 범위를 확대해 ICS 표적을 공격했습니다.

2019년에는 프로그래밍 가능 로직 컨트롤러(PLC)와 ICS처럼 IT 인프라와 OT가 중복되면 이런 하이브리드 인프라를 사용하는 조직에게는 계속 위험이 따랐습니다.

IT/OT 인프라 융합으로 IT 유출이 물리적 자산을 제어하는 OT 장치를 표적으로 하면서 복구 비용이 크게 증가할 수 있습니다. 예를 들어 2019년 초에 IBM X-Force IRIS에서는 IT 시스템에서 시작된 랜섬웨어 감염이 OT 인프라로 측면 이동해, 공장 운영이 중단된 글로벌 제조 회사가 유출에 대응하는 것을 도왔습니다. 이 공격은 회사 자체의 운영뿐만 아니라 세계 시장에도 파급 효과를 일으켰습니다.

2019년 고객에게 제공된 X-Force IRIS 보안 평가는 보통 레거시 소프트웨어와 하드웨어를 사용하는 OT 시스템의 취약점을 강조했었습니다. 더 이상 패치를 할 수가 없고 오래 전에 공개된 오래된 취약점이 가득 찬 생산 시스템을 유지한다는 것은, OT 시스템이 인터넷에 연결돼 있지 않더라도 패치가 되어 있지 않은 OT 시스템이 쉽게 위협 활동가의 먹잇감이 될 수 있음을 의미합니다. 측면 이동의 경우 공격자가 첫 발판을 얻은 다음에는 네트워크 내부에서 이러한 시스템에 액세스할 수 있게 돼 비교적 간단한 악용 기술에도 피해가 발생할 수 있습니다.

X-Force는 그림 1의 ICS 네트워크 공격 동향이 2019년 10월 초 하락했었지만 다양한 위협 활동가가 전 세계 산업 네트워크에서 새로운 작전을 계획하고 개시하고 있어, 2020년도에도 OT/ICS 표적에 대한 공격이 계속해서 증가할 것으로 예상하고 있습니다. 2019년에는 200개가 넘는 새로운 ICS 관련 CVE가 릴리스돼 IBM X-Force 취약점 데이터베이스에 따르면 2020년에도 ICS에 대한 위협이 계속해서 증가할 것으로 보입니다.

X-Force에서는 다양한 위협 활동가가 전 세계 산업 네트워크에 대한 새로운 작전을 계획하고 개시하고 있어, 2020년에도 ICS 표적 대상에 대한 공격이 계속 증가할 것으로 예상하고 있습니다.

유출 기록의 급격한 증가

유출 기록의 수는 85억 건이 넘는 노출으로 2019년에 크게 증가했는데 2018년의 전년 대비 기록보다 3배 이상 큽니다. 이러한 큰 증가의 가장 큰 이유는 잘못된 구성으로 인해 노출된 기록이 전년과 대비했을 때 거의 10배가 증가했기 때문입니다. 이런 기록이 2019년에는 손상된 기록의 86%를 차지했습니다. 이는 잘못된 구성으로 인해 노출된 기록이 2017년보다 52% 감소한 것으로 나타났고 이 기록이 전체 기록의 절반 미만을 차지했던 2018년과도 크게 다릅니다.

눈에 띄는 것은 실제로 전년과 비교했을 때 2019년 한 해 동안 잘못된 구성의 사고 횟수 자체는 14%가 감소했다는 것입니다. 이 사실은 잘못된 구성으로 유출이 발생했을 때 2019년에는 유출의 영향을 받은 기록 수가 상당히 많았음을 나타냅니다. 1억 개 이상 기록 유출 건 3/4은 잘못된 구성으로 발생했습니다. 전문 서비스 부문에서 발생한 두 건의 잘못된 구성 사고에서 노출된 기록의 수는 두 사고 모두 각각 수십억에 달했습니다.

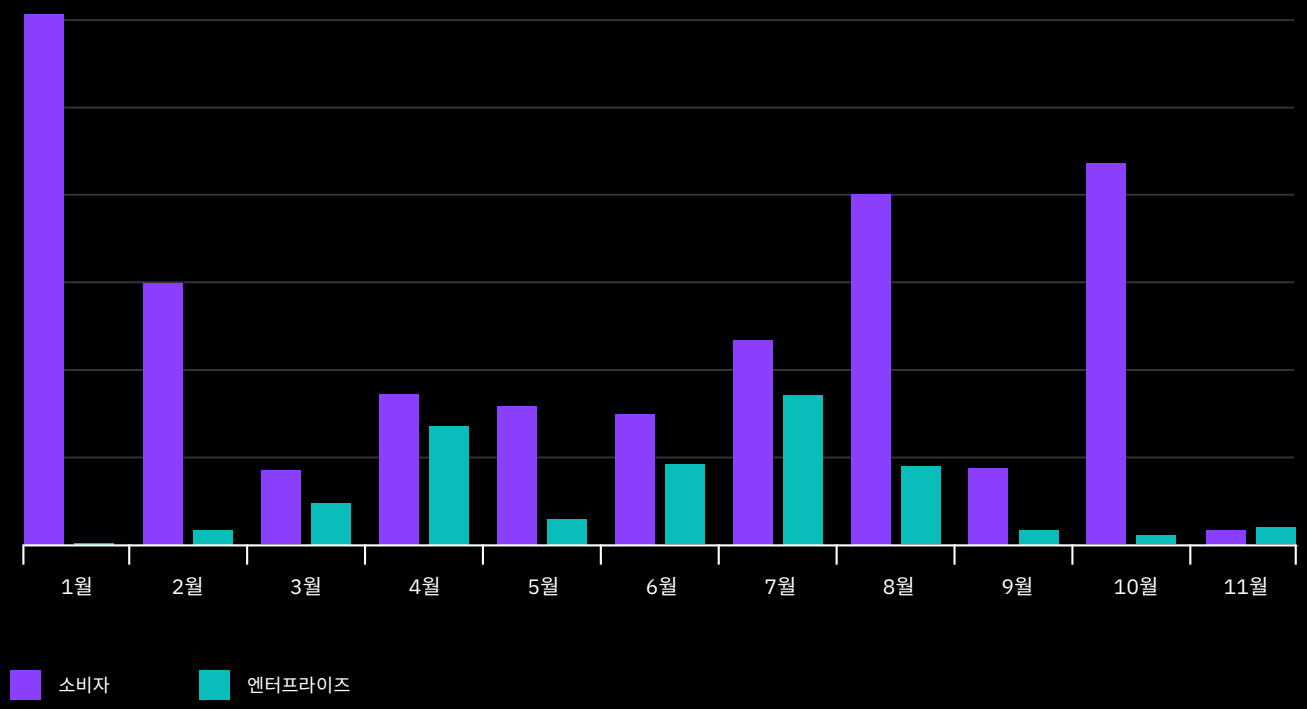
산업 전반에서 기록의 손실이 크게 증가함에 따라 일반적으로 주요 표적으로 간주되지 않은 부문의 조직에서도 데이터 유출 위험이 커지고 있음을 알 수 있습니다.

2019년 유출 기록 수

85억

그림 2:
소비자와 엔터프라이즈 IoT 공격량 비교

2019년 월간 소비자와 엔터프라이즈 IoT 공격량 비교(출처 : IBM X-Force)



엔터프라이즈 영역을 포함시킨 IoT 장치 표적 대상

2020년에는 380억 대 이상의 장치가 인터넷에 연결될 것으로 예상됨에 따라 사물 인터넷(IoT) 위협 환경은 점차적으로, 비교적 단순한 맬웨어와 보통 스크립트된 자동화된 공격을 이용해 소비자와 기업 수준의 운영에 영향을 미칠 수 있는 위협 벡터 중의 하나로 전개되어 가고 있습니다.

2019년 IBM X-Force 연구는 IoT 장치를 감염시키는 데 이용된 맬웨어 영역에서 여러 미라이(Mirai) 맬웨어 작전을 추적했는데 소비자 전자 제품에서 엔터프라이즈 수준의 하드웨어로 역시 눈에 띄게 표적이 바뀌었고 이런 활동은 2018년에는 관찰되지 않았습니다. 공격자는 네트워크에 액세스가 가능한 손상된 장치를 조직 내 발판을 마련하려는 잠재적 시도 지점으로 사용할 수 있습니다.

Mirai는 2016년부터 여러 공격자가 사용한 다수의 IoT 맬웨어로 대량의 중단 사태를 유발하기 위해 많은 IoT 장치를 감염시키고 분산 서비스 거부(DDoS) 공격에 이용합니다. 2019년 작전 분석에서, 우리는 Mirai 맬웨어를 이용하는 이들의 TTP가 2018년 이후 크게 바뀌었으며, 2019년에는 가전 제품뿐 아니라 엔터프라이즈 하드웨어를 표적으로 하는 데에도 초점을 두었음을 발견했습니다.

2019년 IoT 장치에 영향을 주는 공격을 조사한 결과, 다양한 유형의 IoT 장치를 표적으로하는 악성 페이로드의 다운로드 지침을 포함한 명령 삽입(CMDi) 공격이 널리 이용된 것으로 나타났습니다. 이런 삽입 공격의 대부분은 대량으로 장치를 스캔하고 감염시키려는 스크립트에 의해 자동화되어 있습니다. 표적 IoT 장치가 이런 삽입 공격에 취약한 경우에는 페이로드가 다운로드되고 실행되어, 효과적으로 이 장치가 대형 IoT 봇넷에 동원되어 쓰이도록 합니다. 이러한 공격의 가장 일반적인 원인 중 하나는 약한 비밀번호나 기본 비밀번호가 걸려 있는 IoT 장치로, 이런 경우 변변치 않은 사전 공격으로도 쉽게 추측을 할 수가 있습니다.

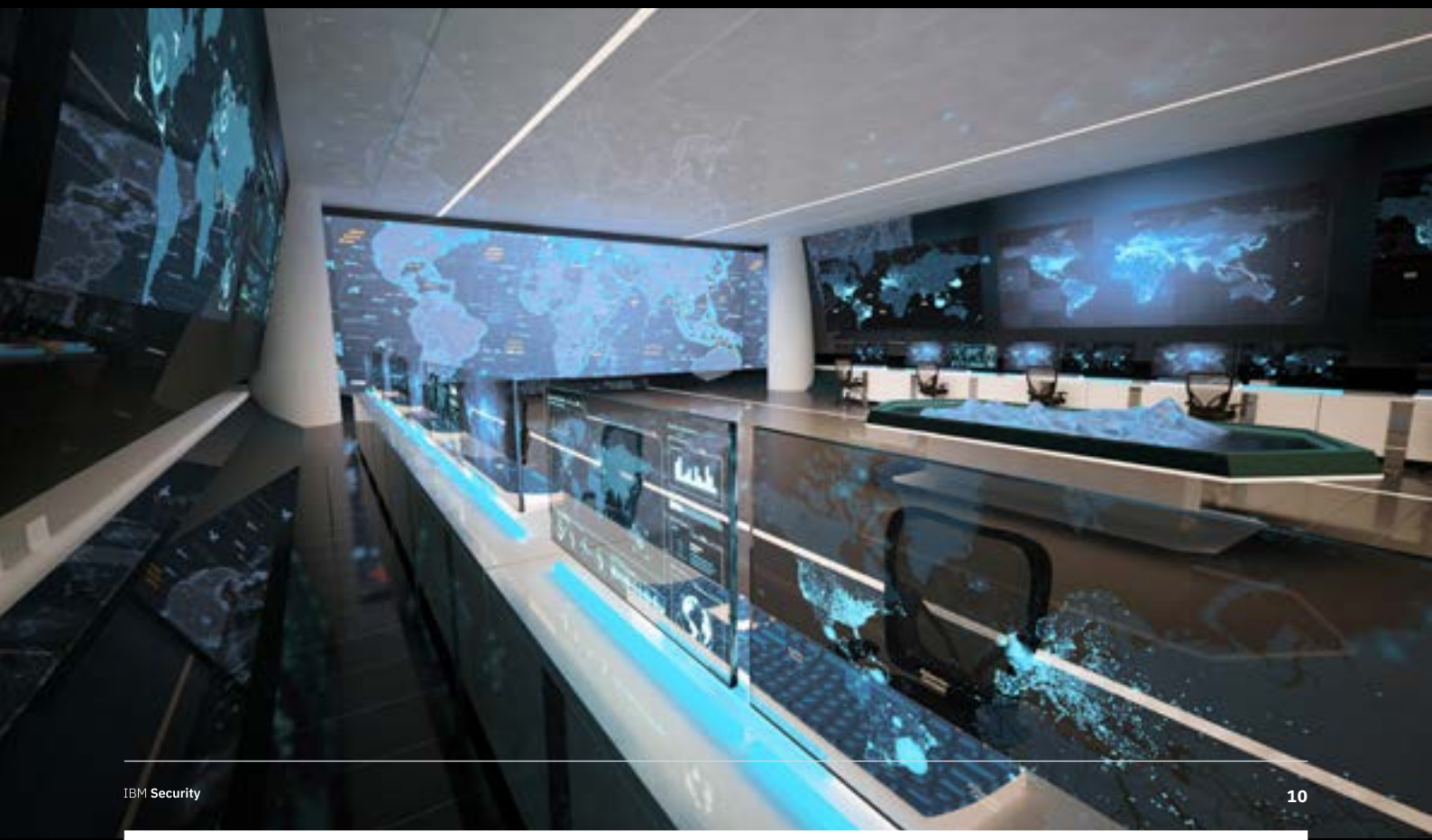
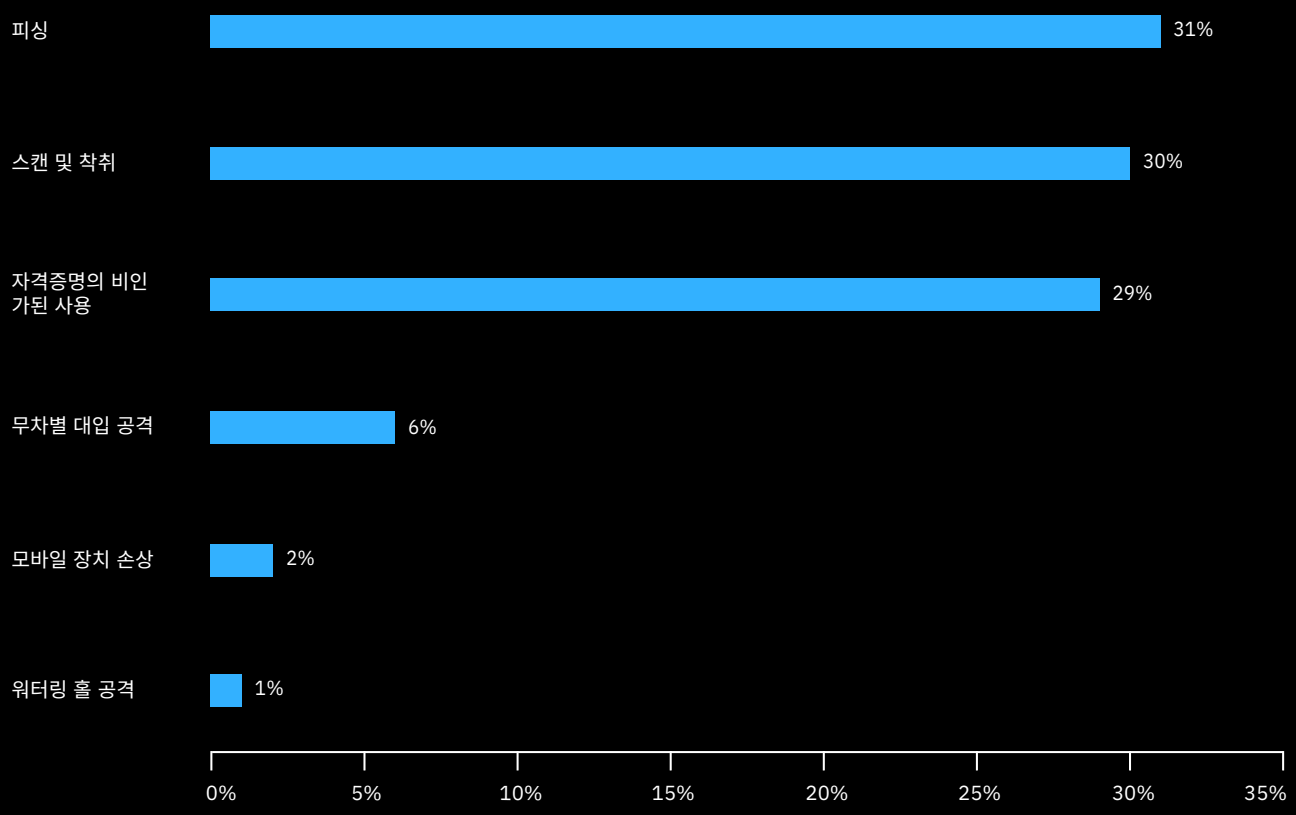


그림 3:
주요 최초 액세스 벡터

2019년 6대 최초 공격 벡터에 대한 액세스 벡터 비율 분석(출처 : IBM X-Force)

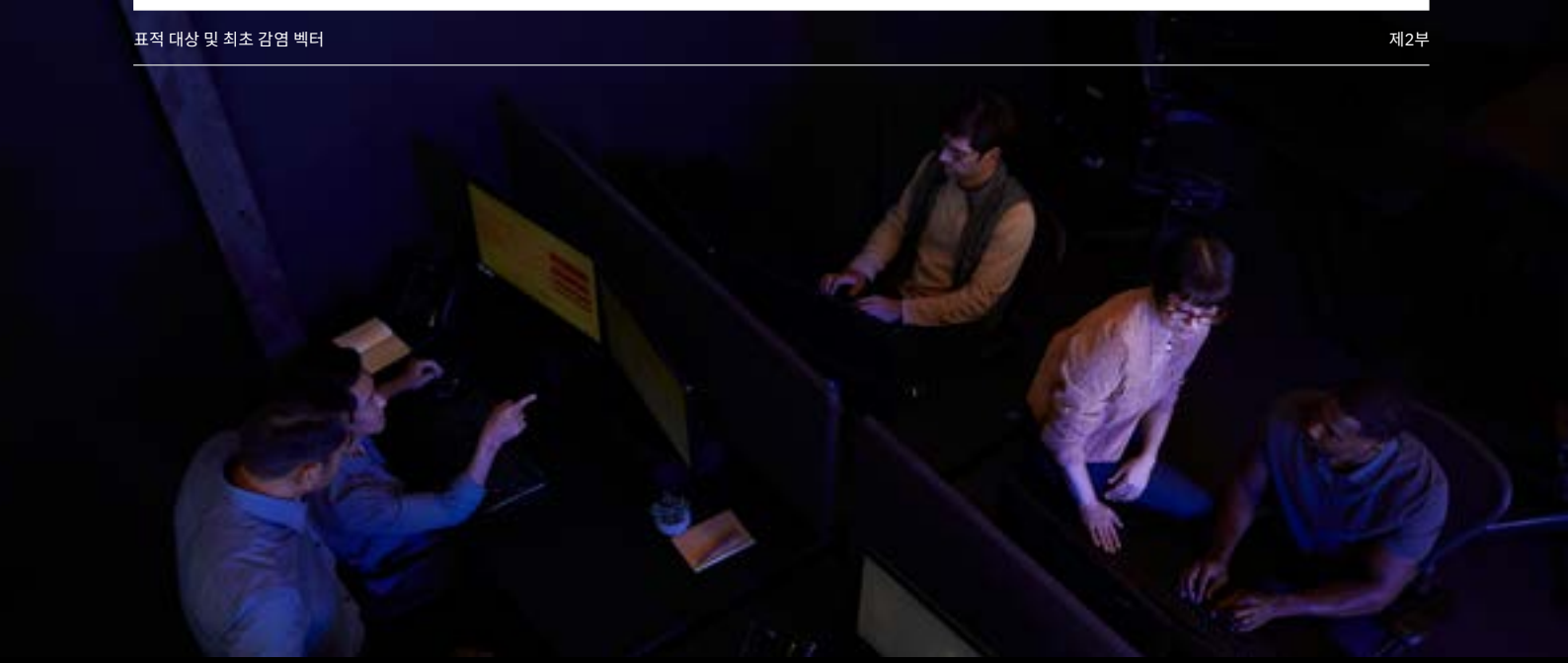


2019년 공격 최초 액세스 벡터 1위를 기록한 피싱

IBM X-Force IRIS는 광범위한 사고에 대응하는 역량을 통해 공격자의 공격 방법 및 동기에 대한 귀중한 통찰력을 제공합니다.

31%의 피싱은 2019년에 최초 액세스에 가장 많이 사용되었던 벡터지만, 전체의 거의 반이 손상된 2018년보다 감소했습니다.[1]

1 2019년 X-Force 위협 인텔리전스 지표는 X-Force IRIS가 분석한 공격의 거의 1/3(29%)이 피싱 이메일을 통한 손상과 관련이 있다고 발표했습니다. 이후, 이 수치는, 2018년의 경우, 몇 건의 사후 게시 후 표면화가 44%로 증가했다는 추가 증거를 설명하기 위해 조정되었습니다.



가장 눈에 띄는 것은 2019년에는 공격자가 대상 환경에서 악용할 취약점이 있는지를 점점 더 많이 검색했으며, 사고 대응자에 따르면 이 기술이 30%의 사건에서 이용된 것이 발견되었는데 전년도에는 총 사건의 8%에만 이용되었습니다.

위협 활동가에게 스캔 및 악용 대상은 많은데, IBM X-Force는 공개적으로 공개된 150,000개 이상의 취약점을 추적했습니다. 정교한 공격자는 제로 데이 익스플로잇을 개발할 수도 있지만, 이러한 익스플로잇은 새로운 TTP를 제작하기 위해 리소스를 소비하지 않고도 초기 발판을 확보할 수 있기 때문에 알려진 익스플로잇에 더 자주 의존하고 그렇게 해서 최고의 무기는 가장 강력하게 방어된 네트워크에 쓰기 위해서 아껴둡니다. 또 공격자들은 한동안 패치 사용이 가능한 취약점에도 패치 애플리케이션을 최신 유지하지 않는 조직에 기대를 겁니다. 예를 들어 워너크라이(WannaCry) 감염 사례는 최초 감염 및 패치(MS17-010) 보급 이후에도 2년 이상 계속 관찰되었습니다.

위협 활동가가 이전에 습득한 자격 증명을 사용해서 표적 대상 조직의 액세스하는 자격 증명 도난 사고는 29%로, 거의 3분의 1에 도달했습니다. 이런 자격 증명은 타사 사이트에서 도난이 될 수도 있고 표적 대상 조직에 대한 피싱 시도를 통해서 얻어질 수도 있습니다. 위협 활동가는 도난된 자격 증명을 사용해서, 합법적인 트래픽과 혼합해 탐지를 더욱 어렵게 만들 수 있습니다.

무차별 대입 공격은 표적 대상 조직에 대한 최초 액세스 지점에 대한 전체 사례의 6%로 4위를 차지해 전년과 대비했을 때 크게 떨어졌고 2%의 BYOD 장치가 그 뒤를 이었습니다.

X-Force 연구원들은 2019년 6월과 7월 위협 활동가 활동이 1월 ~ 5월 합계보다도 더 많아, 눈에 띄게 증가했음을 발견했습니다. 이 급격한 활동 증가의 이유는 알 수 없지만 여름에는 스팸도 더 활발한 것으로 보이며 2019년 8월 최대 스팸량을 기록했습니다. 위협 활동가가 단순히 더 큰 잡음을 냈거나 더 쉽게 탐지되었을 수도 있고 위협 활동가 전술 또는 도구의 변경으로 인해 상당한 활동이 발생했을 수도 있습니다. 활동의 단기적 피크 현상이 새로운 위협 활동가의 시장 진입 결과일 가능성은 적습니다. 신규 진입은 일시적 급증보다는 활동의 지속적 증가를 가져올 것으로 예상되기 때문입니다.

맬웨어 동향

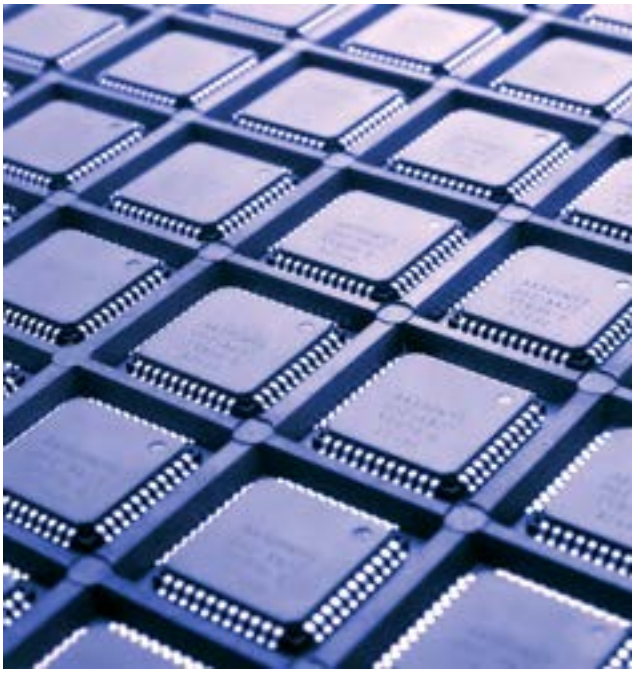
파괴적인 맬웨어 공격의 급격한 증가

IBM X-Force IRIS 조사에 따르면, 2019년 파괴적인 맬웨어 공격이 점점 빈번해지고 지역 및 범위가 증가했다고 합니다.

사이버 범죄자와 국가 소속 활동가가 모두 사용하는 파괴적인 맬웨어는 영향을 받는 시스템의 작동을 불가능하게 해 복원을 요구할 수 있는 기능을 갖춘 악성 소프트웨어입니다. 대부분의 파괴적인 맬웨어 변종은 운영 체제의 실행 능력에 중요한 파일을 삭제하거나 덮어 쓰기해, 파괴를 초래합니다. 경우에 따라 파괴적인 맬웨어가 해당 목적에 잘 맞게 짜여진 메시지를 산업용 장비로 보내 오작동을 일으킬 수 있습니다. 우리는 기계 데이터를 지우거나 기계 데이터를 복구할 수 없게 암호화하는 랜섬웨어 유형도 파괴적인 맬웨어로 정의합니다.

2018년 하반기에서 2019년 하반기 사이에 X-Force IRIS에서 전년과 같은 횟수의 파괴적인 공격에 대응하면서, 잠재적으로 치명적인 맬웨어 동향은 조직을 계속 위험에 빠뜨린다는 점을 강조했습니다.

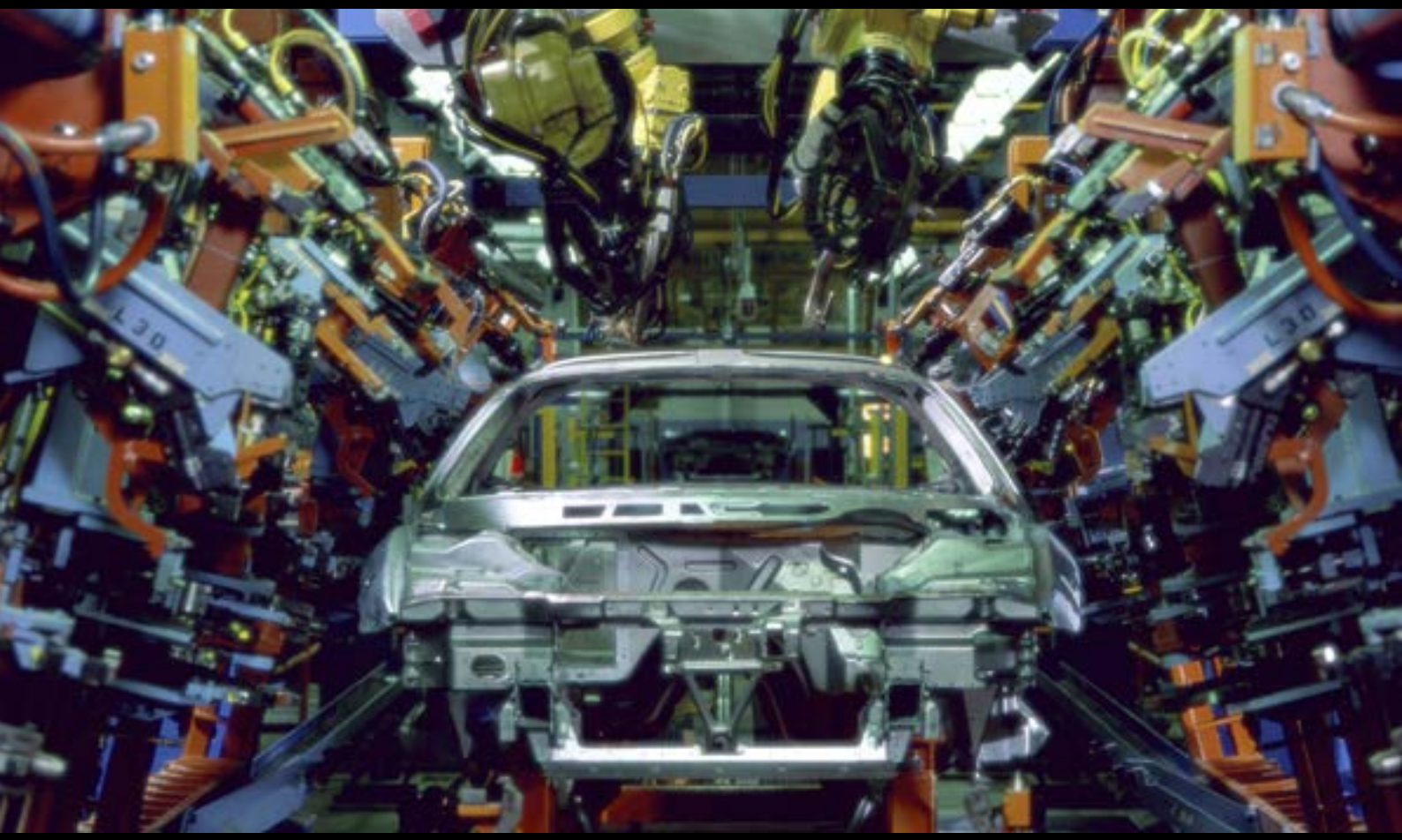
파괴적인 공격의 역사적 시초는 보통 국가 소속 공격자입니다. 하지만 재정적 동기의 랜섬웨어가 공격에 파괴 요소를 통합한 동향을 관찰되었는데, LockerGoga 및 MegaCortex 등의 변종이 파괴적인 공격을 시작한 것이 2018년 말과 2019년 초입니다.



파괴적인 공격은 평균 데이터 유출 비용의 60배 이상이 되는 평균 239백만 달러의 비용을 발생시키는 것으로 추정됩니다.

2019년 말 X-Force IRIS는 파괴적인 신종 맬웨어 발견을 강조해 ZeroCleare라고 이름을 붙였습니다. 이 와이퍼 맬웨어는 중동의 에너지 부문을 표적으로 했으며 IBM에 따르면 이 와이퍼 맬웨어의 원인 제공자는 이란 계열 지능형 지속 공격(APT) 그룹 ITG13[2]로, APT34/OilRig라고도 알려져 있습니다.

X-Force IRIS가 추정하는 바로는 파괴적인 맬웨어 공격으로 발생할 비용은 기업의 경우에는 특히 높을 수 있다고 하는데, 대규모 다국적 기업의 경우 사고당 평균 239백만 달러의 비용이 발생합니다. 이 비용 추정치는 2019 데이터 유출 평균 비용의 60배가 넘으며 이 데이터 유출 평균 비용은 Ponemon Institute의 계산에 따른 것입니다. 데이터를 훔치거나 노출하는 데이터 유출과 달리 파괴적인 공격에서는, 일반적으로 피해를 입은 조직의 네트워크에서 최대 3/4 이상의 장치가 파괴됩니다.



2 ITG는 IBM 위협 그룹(IBM Threat Group)의 약자로 이 용어는 “가장 빈번하게 표적이 되는 산업 부문”에서 추가로 논의됩니다. X-Force에서는 ITG 이름을 사용하고, ITG 이름 뒤에 괄호 안에 이 이름을 대신할 수 있는 위협 그룹의 대체 이름을 표시합니다.

2019년 랜섬웨어 및 암호 화폐의 공세

맬웨어를 이용한 맬웨어 변종과 공격의 수가 1년 동안 올랐다 내렸다 해도, 우선 순위를 정해야 할 위협 유형에 대한 해석이 조직에게는 위험을 더 잘 관리하는 데 도움이 될 수 있습니다.

2019년 상반기에 우리가 관찰한 공격의 약 19%는 랜섬웨어 사고와 관련이 있었으며, 랜섬웨어 사고가 2018년 하반기의 공격 중 10%에 불과했던 것과 대조를 보였습니다. 2019년 4분기에는 전년도 4분기에 비해 랜섬웨어 용역이 67% 증가했습니다. 2019년 내내 X-Force IRIS는 13개 산업에 걸쳐 5개 대륙의 12개 국가에서 랜섬웨어 용역에 응했습니다.

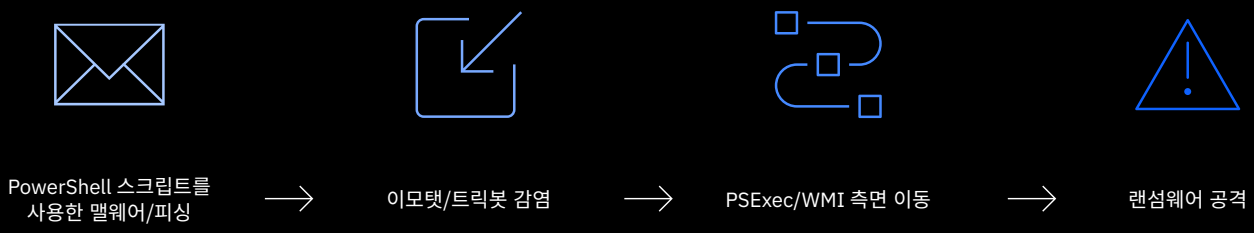
이런 급격한 증가는 2019년 위협 활동가와 다양한 조직에 대해서 시작된 작전의 수의 증가로 인한 것일 수 있습니다. 주목할 것은 랜섬웨어 공격을 받은 자치 단체 및 공공 기관으로 그것은 지방 정부 기관 및 의료 서비스 제공 업체도 마찬가지입니다. 이런 유형의 조직에 대한 공격은 보통, 상대가 대응할 준비가 안돼 몸값 지불 가능성도 높고 경우에 따라 공공 안전과 인명 위협으로 복구에 심한 스트레스를 받을 때를 포착했습니다.

X-Force 데이터에 따르면 랜섬웨어 공격의 경우 2019년 최상위 공격 벡터가 Windows 서버 메시지 블록(SMB) 프로토콜에 있는 취약점을 악용해 네트워크를 통해 전파된 것으로 나타났습니다. 이전 WannaCry 공격에 사용된 이러한 전술은관찰된 공격 시도의 80% 이상을 차지했습니다.

2019년 4분기에는 2018년 4분기에 비해 랜섬웨어 용역이 67% 증가했습니다.

그림 4:
다단계의 랜섬웨어 감염

다단계의 감염 루틴을 통한 랜섬웨어 공격(출처 : IBM X-Force)



취약한 버전의 SMB 프로토콜에 대한 공격은 자동가 가능한데 그래서 이 공격은 위협 활동가에게는 저비용 옵션으로, 확장도 쉬워 한 번의 공격으로 가능한 한 많은 시스템에 영향을 줍니다.

또한, 위협 행위자들은 보통 Emotet 및 TrickBot 등과 같은 상품 다운로더를 사용해 대상 시스템에서 랜섬웨어를 실행했습니다. 이 기술은 보통 PowerShell을 활용해 맬웨어를 다운로드하고 탐지하기 어려운 PSExec 또는 Windows 관리 계측(WMI) 같은 기본 기능을 사용해 맬웨어를 확산시켰습니다.

공격자는 랜섬웨어로 직접 공격하는 대신 여러 단계를 사용해 사용자를 감염시켜 공격을 좀더 효과적으로 제어하고 제어 및 탐지를 회피하며, 피해자에게 몸값 지불을 유도하기에 충분할 많은 장치들을 아우르게 될 랜섬웨어 작전의 씨앗을 뿌립니다. 인내와 계획의 투자는 수익이 큽니다. Ryuk 공격자들은 5개월 만에 370여만 달러를 자신의 범죄 집단을 위해 축적했습니다. 또 다른 예로, 미국의 요양원에 대한 공격에서는 1,400만 달러를 Ryuk 운영자가 몸값으로 요구했습니다.

랜섬웨어가 2019년 급증한 유일한 맬웨어 유형은 아닙니다. 2019년에 매우 인기가 있었던 또 다른 유형의 맬웨어는 암호화폐 마이닝 코드였습니다.

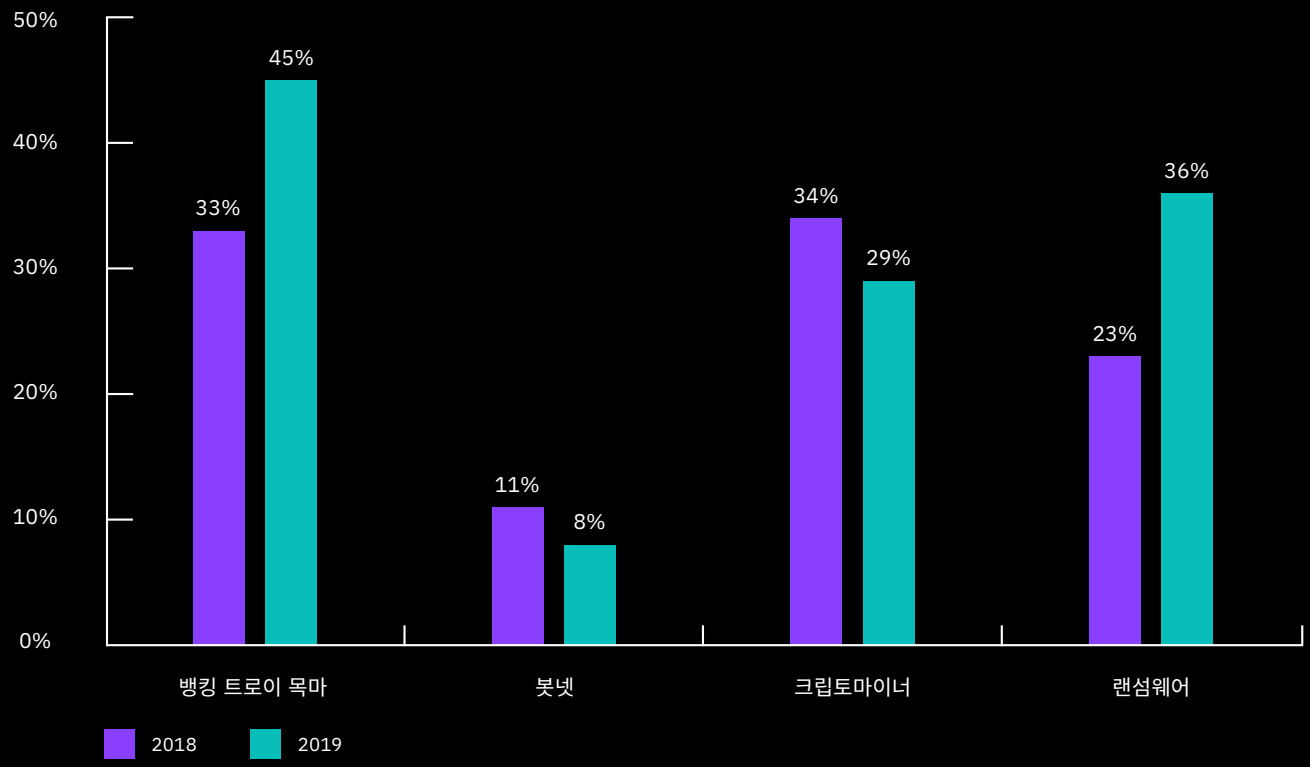
X-Force의 원격 측정에 따르면 암호화 활동은 2019년 중반에는 전례 없는 수준으로 급증했고, 특히 6월의 암호화 활동량은 1년 내내 있었던 다른 모든 암호화 활동 전체를 거의 능가했습니다.

봇넷을 운영하는 이들의 동기와 리소스에 따라, 맬웨어 동향이 오르고 내리는 가운데, 이런 급증은 맬웨어 마이너가 자주 쓰는 Monero 암호 화폐 가치가 3배 뛴 것과 관련이 있을 수 있습니다.

그림 5:

맬웨어 유전자 코드 혁신

2018-2019 범주별 신종(전에 관찰되지 않았던) 코드 비율(출처: Intezer)



2019년 맬웨어 코드 진화의 최고 혁신가

신종 맬웨어 변종 탐지를 위한 이전 X-Force 협업에 의지해서 Intezer는 맬웨어 유전자 분석 기술을 활용하여 모든 소프트웨어 코드의 유전자 기원을 밝히고 코드 유사성과 재사용을 식별해 맬웨어 "혁신"을 측정했습니다. 이 혁신 기술에 대한 측정 척도는 위협 활동가가 신종 코드 개발에 투자한 정도로 이것은 공격자의 위협 기능 확장 및 탐지 회피하기 위해 노력했다는 것을 의미합니다.

Intezer의 데이터에 따르면 2019 년에 위협 행위자는 주로 뱅킹 트로이 목마와 랜섬웨어의 코드 베이스를 개발하고 발전시키는 데 중점을 두면서도 암호화 맬웨어 균주를 수정 및 생성하는 데 많은 노력을 기울이고 있습니다.

이 보고서 섹션은 IBM X-Force와 Intezer 연구원이 공동으로 작성했습니다. Intezer는 맬웨어 이진 코드에 대한 유전자 분석을 수행합니다.

2019년에는 뱅킹 트로이 목마가 신종 코드 중의 최고 수준(45%)이었고 랜섬웨어(36%)가 뒤를 이었습니다. 역사적으로, IBM은 기업 이용자에게 먹힐 만한 맬웨어 유형에 대한 위협 활동가의 관심과 투자를 봐왔고 이는 이 맬웨어군이 2020년에는 기업을 표적 대상으로 할 수도 있음을 시사합니다. 시간이 지나면 맬웨어는 더 빨리 탐지되고 공격의 투자 수익은 감소하기 때문에, 뱅킹 트로이 목마와 랜섬웨어 운영자는 계속 발전하지 않으면 멸종 위기를 맞을 것입니다.

2019년, 크립토마이너는 혁신이 감소하지만 마이닝 활동량은 여전히 높아 위협 활동가는 계속 신규 버전의 크립토마이너를 개발하지만 이전 코드에 점점 더 의존하고 있음을 시사합니다. IBM의 경험으로는, 이런 단순한 맬웨어 코드는 보통 다른 악의적이지 않은 시조 코드에 의존하는데 그 예로 수정한 XMRig 등을 이용해서 불법적인 방법으로 코인을 수확합니다. 새로운 마이너는 다른 목적으로도 작성되는데 그 목적의 예로는 코인 수확 대상이 IoT 장치인 경우가 있고또 그와 극단적 반대의 경우의 예를 들면 수확 대상이 감염 서버인 경우가 있는데이런 경우에 CPU 능력은 작은 장치 및 개별 PC 보다 더 큽니다.

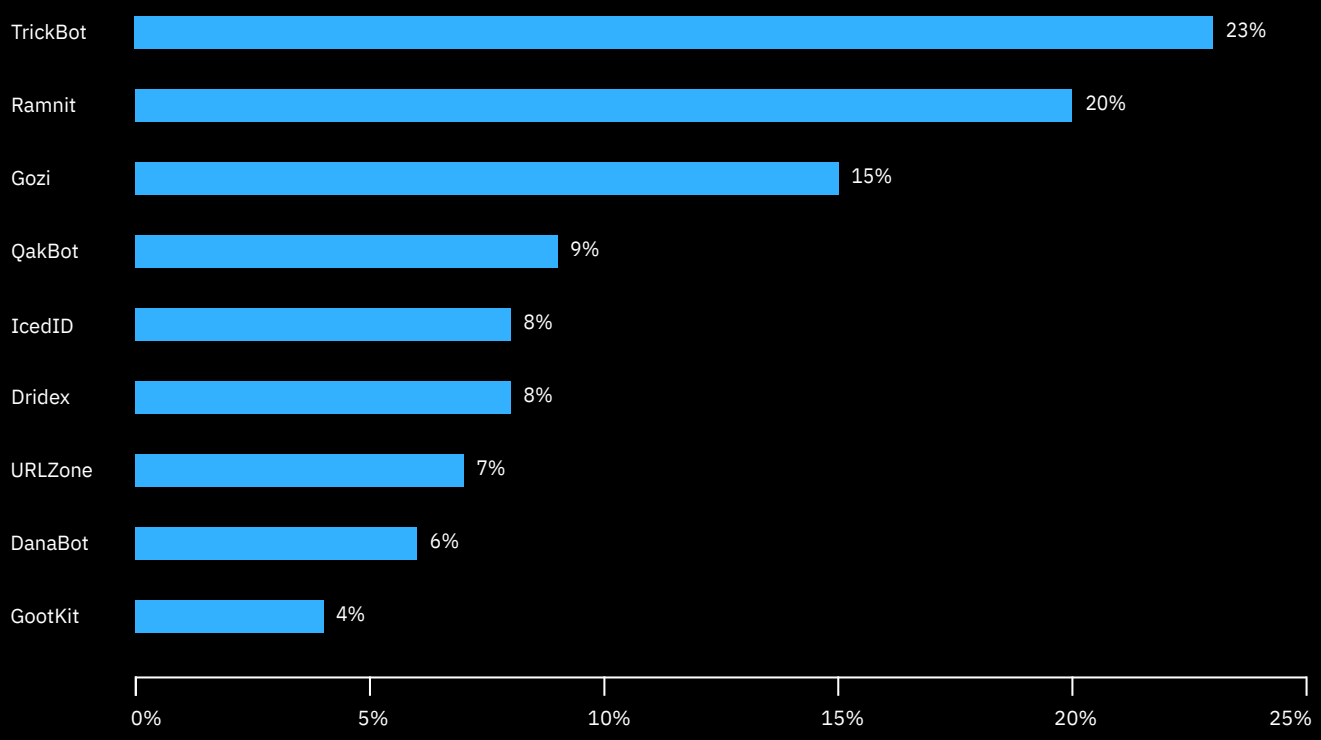
반면, 일반 봇넷 맬웨어(11%)는 전년에 비해 코드 혁신이 적었고 이는 기능 수정에 대한 투자가 줄었음을 뜻합니다. IBM은 이런 유형의 코드가 스팸 또는 악성 광고에서 사용자에게 푸시되는 것을 관찰했습니다. 일반적인 봇넷 맬웨어의 주요 역할은 감염된 장치에서 약간의 발판을 확보하는 것입니다. 하지만 기능은 최소한으로 유지됩니다. 이를 통해 높은 수준의 "코드 진화"가 보이지 않는 이유를 설명할 수 있습니다.

2020년에 이 코드 혁신 동향은 코드를 계속해서 발전시키기 위한 투자로 인해 해당 맬웨어를 식별하고 포함하기 위해 더 많은 노력이 요구되는 맬웨어 유형을 나타낼 수 있습니다.

2019년에는 위협 행위자가 뱅킹 트로이 목마 및 랜섬웨어 코드베이스를 개발하고 발전시키는 데 중점을 두었습니다.

그림 6:
주요 뱅킹 트로이 목마 패밀리

2019년 9대 뱅킹 트로이 목마 패밀리에 대한 비율 분석(출처: IBM X-Force)



뱅킹 트로이 목마와 랜섬웨어 – 계속되는 악성 조합

금융 맬웨어 분야는 10년 전에 약간 주된 이슈가 되었고, 당시 사이버 범죄 세계에서 최초로 상용화된 뱅킹 트로이 목마였던 Zeus Trojan과 같은 맬웨어가 등장했습니다. 2019년 금융 범죄 상황을 검토한 결과 최고의 뱅킹 트로이 집단 동향이 분명해졌습니다. 이 맬웨어 봇넷은 표적을 노린, 고위험 랜섬웨어 공격 전 성문을 여는 데 점점 더 많이 쓰이고 있습니다.

2019년 이 범주에서 가장 활발한 트로이 목마의 차트는 2018년 연간 보고서에서 나온 것과 비슷합니다. TrickBot, Gozi 및 Ramnit은 상위 3위를 유지합니다. 이들 트로이 목마는 봇넷 서비스 방식과 손상된 자산을 통한 배포 등 다른 사이버 범죄자들에게 다양한 비즈니스 모델을 제공하는 조직화된 그룹에 의해 운영됩니다.

TrickBot을 운영하는 조직은 2019년 사이버 범죄 분야에서 가장 활발한 범죄 그룹입니다. 이 활동은 다음과 같은 다양한 측면으로 나타났습니다.

- 코드 업데이트 및 수정 빈도(코드, 버전 및 기능 진화)
- 감염 공격 빈도 및 규모
- 공격 활동 빈도 및 양

2019년 고위험 랜섬웨어 공격으로 헤드라인을 장식한 집단은 또한 2015년 사이버 범죄 분야에 고위험 사기 공격을 도입한 이들입니다. 어떤 의미에서, 전반적인 전략은 같고 시간이 지나면서 전술만 수정됩니다. 즉 더 큰 현상금을 위한 비즈니스를 목표로 합니다.

랜섬웨어로 다각화하는 뱅킹 트로이 목마의 주요 예는 다음과 같습니다.

Dridex
전에는 LokiBot을 사용자 장치에 배포했고 이제 기업 네트워크에 BitPaymer/DopplePaymer를 배포합니다.

GootKit
엔터프라이즈 네트워크에서의 LockerGoga 배포가 의심됩니다. LockerGoga는 2019년 초 등장한 비즈니스에 대한 치명적인 공격의 일부였습니다.

QakBot
엔터프라이즈 네트워크에 MegaCortex를 배포합니다.

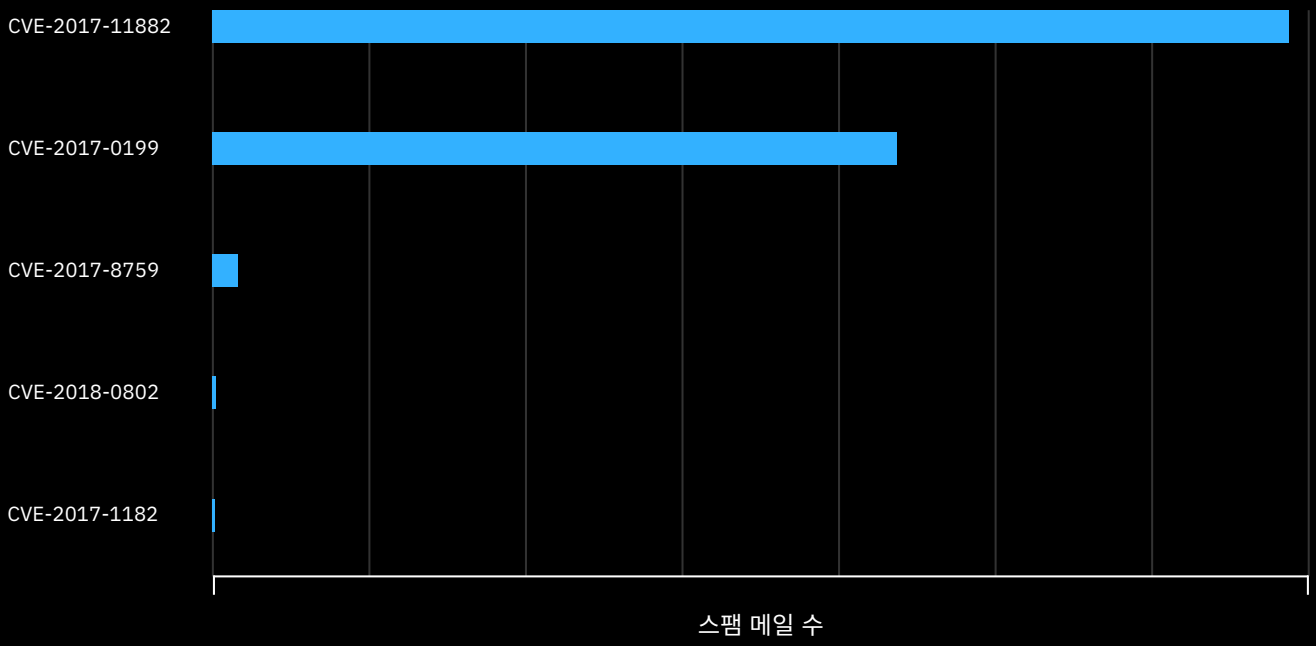
TrickBot
엔터프라이즈 네트워크에 Ryuk을 배포합니다.

또한 2019년 후반의 보고서에 따르면 역사적으로 지불 카드 데이터의 대량 도난에 중점을 둔 ITG08 (FIN6)은 TTP 도다양화하고 있습니다. 이 그룹은 이제는 엔터프라이즈 네트워크에 대한 랜섬웨어 배포를 포함하는 것을 목표로 합니다. 랜섬웨어 공격은 한 번 실수에 수백만 명을 엮을 만한 잠재력을 가지고 있으며 더 많은 집단이 랜섬웨어 및 사이버 추출 경로를 이용할 수도 있습니다.

스팸 및 피싱 동향

그림 7:
악성 스팸에 활용된 주요 취약점

2019년 주요 악성 스팸 첨부 파일 활용 취약점 정량 분석(출처: IBM X-Force)



2019년 스팸에서도 그대로 발생한 2017년의 취약점

IBM X-Force는 매일 전 세계 곳곳에 스팸 트랩을 설치하며 수천만 건의 스팸 메시지 및 피싱 이메일을 모니터링하고 있습니다. 우리 팀과 기술은 수십억 개의 달하는 웹 페이지 및 이미지를 분석하여 부정 활동 및 브랜드 악용을 감지합니다.

글로벌 스팸 행위에 대한 X-Force 분석에 따르면 스팸 이메일은 오로지 다음과 같은 두 CVE에만 특별한 중점을 두고 취약점의 제한된 서브세트를 계속 이용한다고 합니다. 두 가지 CVE는 2017-0199와 2017-11882입니다. 이러한 두 가지 CVE는 모두가 다 패치가 된 취약점으로 공격자들이 스팸 작전을 통해서 악용하려는 취약점의 거의 90%를 차지했습니다. 이러한 두 가지 CVE는 모두 Microsoft Word에 영향을 미치며 부비트랩된 문서를 여는 것 외에 아무 사용자 상호 작용도 필요치 않습니다.

이벤트 데이터에 따르면 2019년 공격자가 이 두 가지 취약점을 사용한 빈도가 다른 Microsoft Word 원격 코드 실행 취약점 사용 빈도를 거의 5:1 비율 초과한 것으로 나타났습니다.

이 두 가지 취약점은 상당한 양의 스팸 이메일에 표시되지만 사용자를 얼마나 성공적으로 악용하는지는 알 수 없습니다. 즉 스팸은 보통은 숫자 게임입니다. 충분한 양으로 밀면 작은 성공률도 위협 활동가에게는 가치를 창출하기에 충분합니다. 많은 사용자뿐만 아니라 조직도 특정 문제를 패치하는 데는 뒤쳐질 수 있기 때문에 오래된 버그로 인해 장치가 손상되는모습은 여전히 볼 수 있습니다.

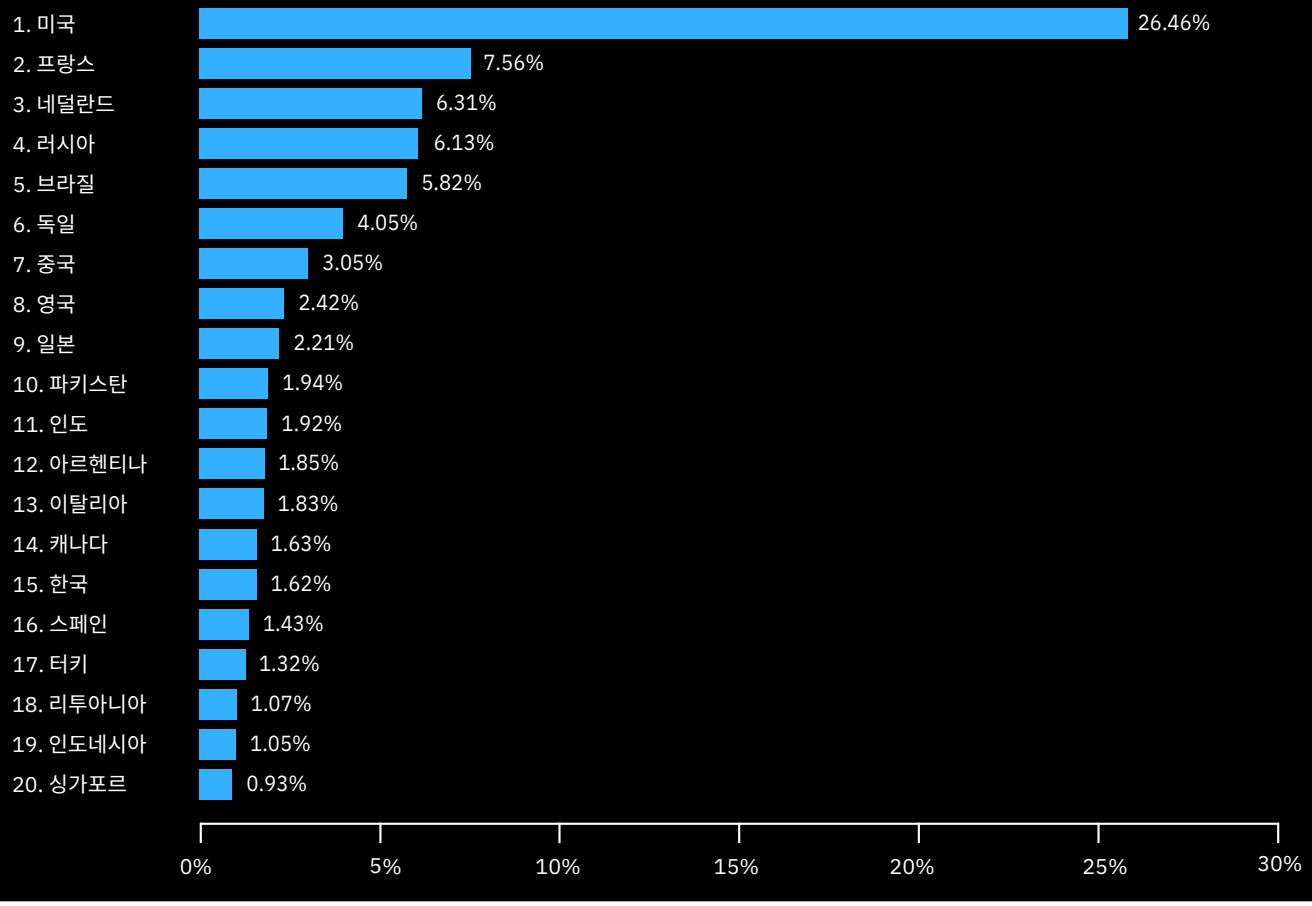
오래된 취약점의 인기에 대해서는 많은 설명이 있을 수 있는데 무료 문서 작성 도구의 통합 및 사용 용이성, 지속적 효과 또는 다양한 악의적 페이로드를 삭제하는 다목적성이 포함됩니다.

오래된 취약점을 지속적으로 사용하면 악의적인 활동의 긴 꼬리와 공개 및 패치 릴리스 이후 몇 년 동안 사용자에 대해 얼마나 많은 취약점이 활용될 수 있는지만 강조됩니다.

그림 8:

20대 스팸 C2 호스팅 국가

20개 국가 비율로 2019년 상위 20개 스팸 명령 및 제어 호스팅 국가의 비율(20개 국가의 총 C2 서버 비율 = 80.6%)으로 분류됨(출처: IBM X-Force)



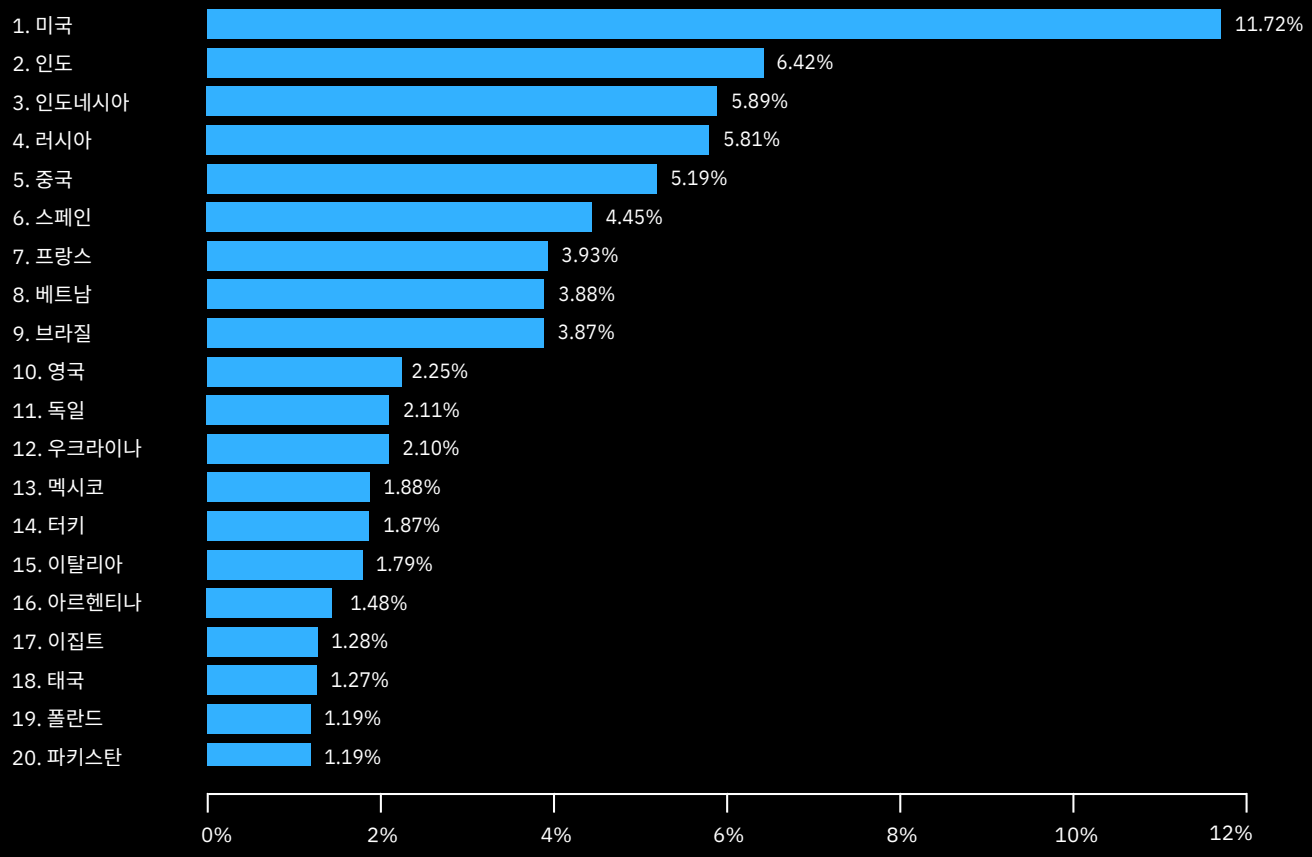
서구 국가에서 호스팅돼 전 세계를 뒤흔든 스팸 봇넷

스팸 봇넷에 대한 IBM X-Force의 연구는 스팸 봇넷 명령 및 제어(C2) 인프라와 연결된 다양한 지역별 데이터 포인트를 조사합니다. 우리가 살펴본 매개 변수 중 하나는 봇넷 C2가 호스팅되는 지리적 위치입니다. 2019년에는 C2가 주로 북미와 서유럽 국가에서 호스팅되었고 2019년에 관찰된 모든 C2 인스턴스의 반 이상을 차지했습니다. 나머지 C2 호스팅은 좀더 다양한 지역까지 퍼져 있습니다.

대부분 스팸 봇넷 C2 인프라는 손상된 서버에서 호스팅되고 북미와 유럽 서버 사용은 보통 서버 업타임이 더 일관된다는 공통된 견해와도 일치합니다. 또한 사이버 범죄자들은 이러한 서버의 트래픽이 대상 지리의 장치 및 네트워크와 상호 작용할 때 적신호가 발생할 가능성이 적은 로컬 리소스에 대한 공격을 호스팅하는 것을 선호합니다.

그림 9:
20대 스팸 봇넷 피해 국가

20개 국가 비율로 2019년 상위 20개 봇넷 클라이언트(피해 국가) 국가의 비율(20개 국가의 총 보셋 클라이언트 비율 = 69.6%)으로 분류됨
(출처: IBM X-Force)



지역별 스팸 피해자

2019년 스팸 봇넷의 피해자는 전 세계로 퍼져 나갔으며 미국이 가장 많은 피해를 입었고, 인도, 인도네시아, 러시아 및 중국이 그 뒤를 이었습니다. 이런 표적 대상 분포는 대량 스팸 작전을 통해 최대한 많은 수신자에게 도달하려는 스패머의 동기와 일치합니다. 당연히 인구가 많은 국가는 다수의 스팸 이메일이 밀려옵니다.

익명 서비스 보급에 열을 올리는 차단 당한 악성 도메인

온라인 위협으로부터 네트워크를 더 안전하게 유지하기 위한 한 가지 일반적인 관행은 사용자 및 자산이 잠재적이거나 알려진 악의적인 도메인과 통신하지 못하게 하는 것입니다. 위험을 최소화하기 위해 대부분의 조직은 차단 목록을 사용하여 의심스러운 IP 주소를 차단합니다. 전 세계적으로 동일한 개념으로 무료로 제공되는 도메인 네임 서버(DNS) 서비스[3]Quad9는 매일 악성 사이트에 대한 평균 1,000만 개의 DNS 요청을 차단합니다.

IBM 보안 위협 인텔리전스와 관련된 Quad9 데이터 샘플링에 따르면, 스팸 이메일에서 발견된 URL이 대다수의 의심스러운 DNS 요청을 구성했으며 2019년 전체 요청의 69%를 차지했습니다. 스팸 URL 범주는 2018년 77%에서 감소했지만 여전히 전체적으로 가장 중요한 악성 도메인 범주를 이룹니다. DNS 서비스의 24%를 차지하는 익명 서비스 범주로 인해 8% 포인트가 감소했을 수 있습니다.

이메일 스팸은 Necurs 봇넷과 같은 대규모 스팸 봇넷으로 하루에 수백만 개의 스팸 이메일을 뿌릴 수가 있기 때문에 잠재적으로 최대 다수의 피해자에게 접근할 수 있는 가장 효과적인 방법 중 하나입니다. 악성 도메인은 종종 맬웨어를 확산시켜 랜섬웨어, 자격 증명 도용 스크립트 또는 추가 사기에 대한 링크를 배포하며 최종 사용자가 알고 있는 브랜드를 사칭하거나 합법으로 위장해 최종 사용자를 속이도록 설계되었습니다.

스팸 이메일에서 악성 URL에 연결하는 것은 또한 재정적으로 동기 부여된 대다수의 활동가가 선택하는 방법으로 이를 통해 활동가는 최소한의 노력으로 광범위한 그물을 치거나, 지역별 표적 대상을 선택해 사기가 들통나는 것을 제한할 수 있습니다.

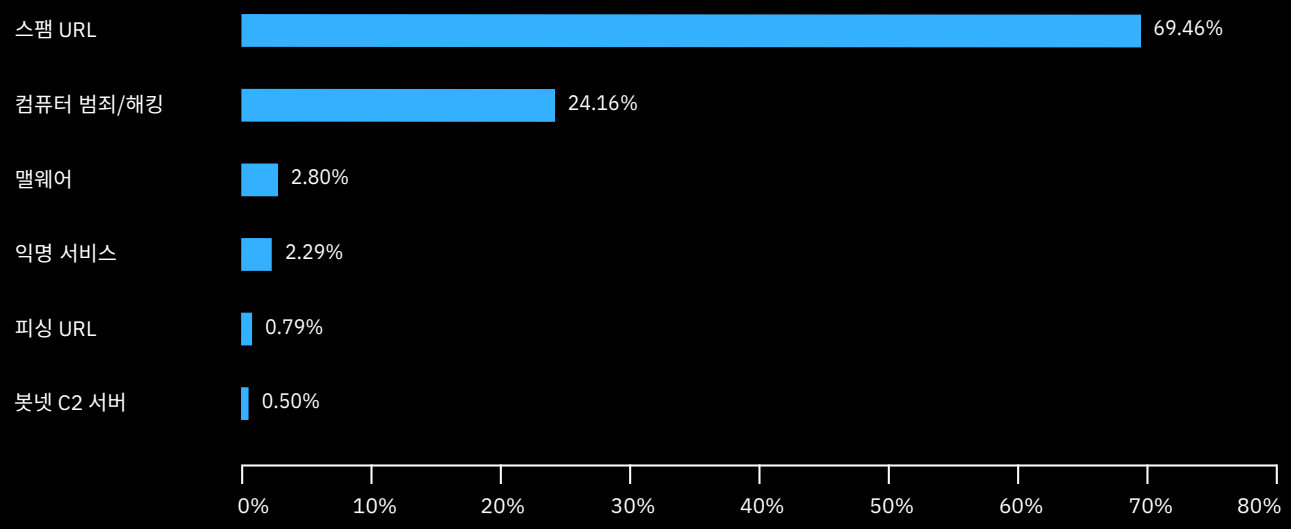
그림 10의 차트는 2019년 IBM Security에서 기록한 악성 도메인 유형의 분포를 보여줍니다.

이메일 스팸은 잠재적인 최대 다수의 피해자에게 접근할 수 있는 가장 효과적인 방법 중 하나입니다.

3 Quad9는 IBM, Packet Clearing House(PCH) 및 Global Cyber Alliance(GCA) 간의 협업을 통해서 만들어지고 후원되었습니다.

그림 10:
주요 악성 도메인 위협 유형

2019년 6대 악성 도메인 위협 유형에 대한 유형 비율 분석(출처: IBM X-Force 및 Quad9)



스팸 URL:
스팸 작전과 관련된 사이트로 연결되는 도메인으로, 보통은 성가시기는 해도 그 이상의 범죄 행위와 관련이 없는 도메인

익명 서비스:
트래픽을 더 볼 수 없도록 숨기는 익명 공급자와 연결된 도메인

컴퓨터 범죄/해킹:
웹 브라우저 악용 스크립트를 호스팅하는 사이트와 같이 범죄 행위에 연루된 것으로 식별된 도메인

피싱 URL:
보통은 사용자로부터 자격 증명 데이터 또는 기타 민감한 정보를 얻으려는, 다른 합법적 도메인으로 위장한 도메인

봇넷 명령 및 제어:
봇넷 활동에 연결되어 잠재적으로 방문자를 감염시키는 도메인

맬웨어:
알려진 악성 코드를 호스팅하는 도메인

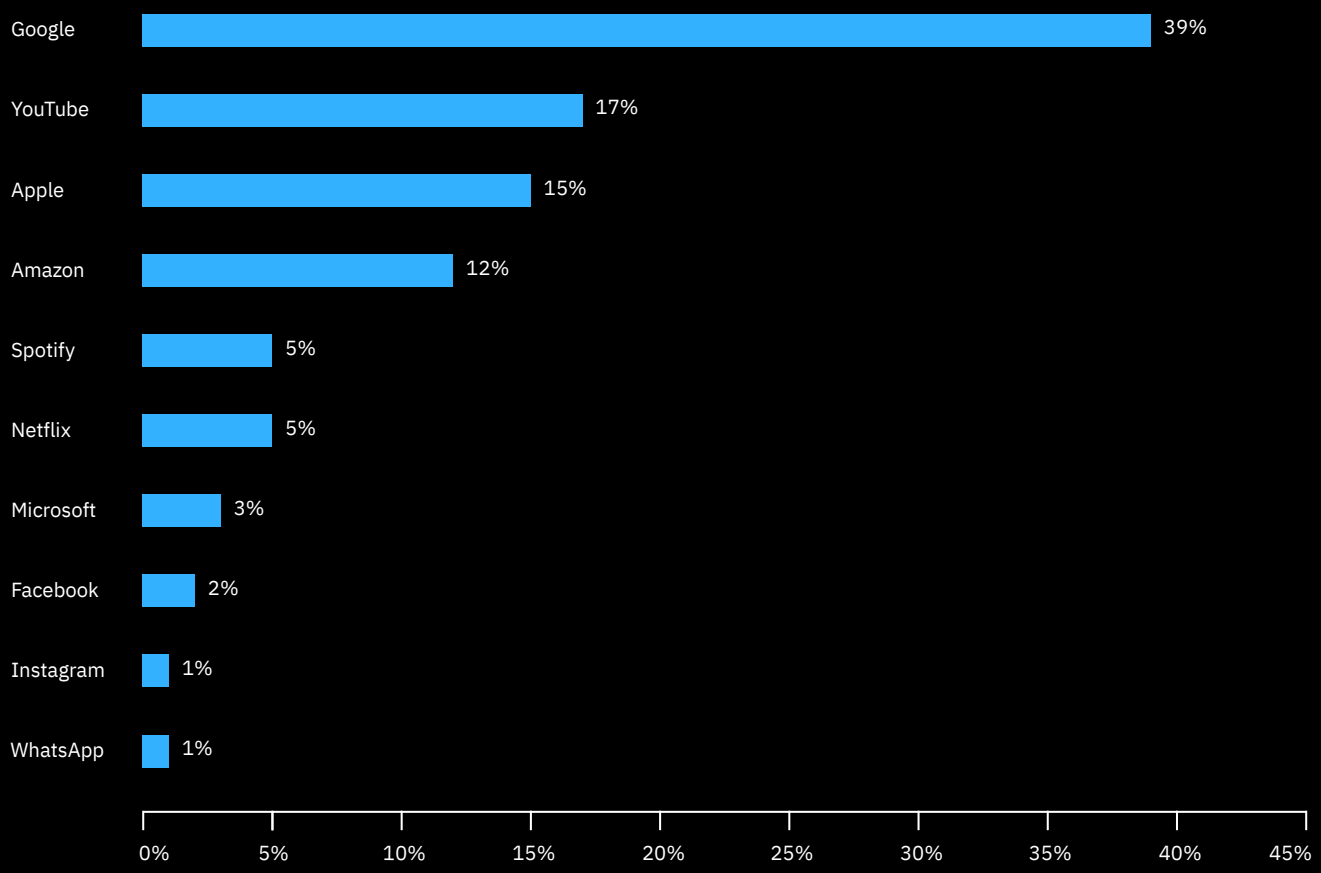
예를 들어, Tor 등의 익명화 제공자는 이용자가 다른 활동가가 운영하는 노드를 탐색해서 인터넷 트래픽 출처를 익명화할 수 있도록 합니다. 익명화 서비스는 웹 브라우징 활동에 대한 향상된 개인 정보 보호 기능을 이용자에게 제공하는 데 대해, 합법적인 목적을 제공할 수 있고 보통 그리 한다지만 그래도 악의적인 활동을 추적하고 차단하는 것이 더 어려워 지게 만들 수도 있습니다.

익명화는 악의적인 링크를 애매해 지게 만들거나, 데이터 손실 방지(DLP) 규칙을 트리거하지 않으면서 데이터를 유출하거나 원격 서버 IP가 차단되기 전에 추가 악성 페이로드를 회수하기 위해, 이력을 감추려는 사이버 범죄자의 일반적인 전술입니다.

악의적인 DNS 요청의 4%는 컴퓨터 범죄 또는 블랙햇 해킹 웹 페이지로 분류되었으며, 일부 범죄자는 웹 브라우저 악용 시도, 사기 정보 배포 또는 다른 유형의 온라인 범죄에 관여한 것으로 알려져 있습니다. 이 링크는 익명화 링크를 통해 라우팅되거나 회사 프록시 및 방화벽에 의해 감지 및 차단돼 결과적으로 차단되기 때문에 상대적으로 수가 적습니다.

그림 11:
10대 스푸핑 피해 브랜드

10대 브랜드의 비율로 2019년 10대 스팸 스푸핑 피해 브랜드에 대한 비율 분석(출처: IBM X-Force)



기술 기업과 소셜 미디어를 가장한 피싱

피싱은 2019년에도 여전히 주요 위협 요소가 되었고 X-Force 데이터는 피싱 작전에서 가장 일반적으로 스푸핑된 브랜드가 기술 및 소셜 미디어 플랫폼이었음을 보여줍니다. 스푸핑된 도메인은 사용자에게는, 가장된 회사에서 사용하는 합법적인 도메인과의 시각적인 식별이 어려울 수가 있습니다. 실제처럼 보이는 웹사이트가 원본과 매우 유사하다면 사용자가 개인 데이터를 악의적 웹사이트에 공개하게 만들 수 있습니다.

이 데이터는 2019년 Quad9에서 차단했던 모든 악성 도메인을 분석하고 IBM X-Force의 도메인 스쿼팅 탐지를 기반으로 해서 얻은 것입니다.

Instagram 및 Spotify와 같은 소셜 미디어 또는 콘텐츠 스트리밍 사이트를 표적으로 해도 위협 활동가에게 Google 또는 Amazon 계정 도용 등 쉽게 수익이 나는 데이터 제공은 안될 듯 보입니다. 그래도 위협 활동가는 개인이 계정과 서비스 간에 비밀번호를 재사용하길 바라며 수집된 자격 증명을 사용해 같은 사용자가 보유한 더 가치 있는 계정에 액세스하려고 할 수가 있습니다.

가장 빈번하게 표적이 되는 산업 부문

오늘날의 위협 환경에서 위협 활동가 동기에 따른 일부 유형의 공격의 특이성은 사이버 보안 위험 관리가 부문마다 매우 다른 모습일 수 있음을 의미합니다.

X-Force 연구진은 매년 가장 많이 표적이 되는 산업을 조망하기 위해 각 부문에서 관찰된 공격량을 평가합니다. X-Force 관리 네트워크의 공격 및 보안 사고 데이터, 사고 대응 서비스에서 얻은 데이터와 해석, 대중에 공개된 사고에 근거해 가장 빈번하게 표적이 되었던 산업이 결정되었습니다.

그림 12:
10대 표적 대상 산업

2018년 대비 2019년 공격량에 따른 10대 표적 대상 산업
(출처: IBM X-Force)

부문	2019년 순위	2018년 순위	변경
금융 서비스	1	1	–
소매업	2	4	2
운송업	3	2	-1
미디어	4	6	2
전문 서비스업	5	3	-2
정부	6	7	1
교육	7	9	2
제조업	8	5	-3
에너지 산업	9	10	1
의료업	10	8	-2

그림 12는 2019년에 가장 많이 공격 당한 업계 및 각 업계 순위를 2018년의 각 업계 순위와 비교한 비교 차트입니다.

금융 서비스 측면에서 놀라운 일은 없었지만 소매 산업은 공격자의 관심을 끌고 있음을 쉽게 알 수 있습니다. 미디어 및 엔터테인먼트 회사, 교육 기관 및 정부 기관도 마찬가지입니다.

다음 섹션에서는 다양한 데이터 소스를 기반으로 한 표적화의 상대적 빈도와 2019년 각 산업별 조사 결과에 대해 자세히 설명합니다. 일부 업계 설명에서는 최근 몇 년간 그 분야를 겨냥한 활동을 펼친 위협 활동가가 강조되지만 이 목록이 전부가 아니라 2019년 이전의 데이터를 포함합니다. X-Force IRIS는 수십 개의 국가에 소속되어 후원을 받는 집단 및 사이버 범죄 집단을 추적하고 프로파일링합니다. 원인 불명의 활동 및 무법 지대에서 발견된 작전은 활동 “HIVEs” 범위 내에서 추적됩니다. 활동이 엄격한 분석 임계 값을 충족하면, TTP, 인프라, 타겟팅 및 트레이드 크래프트 모음에 근거한 IBM 위협 그룹(ITG)으로 전환됩니다.

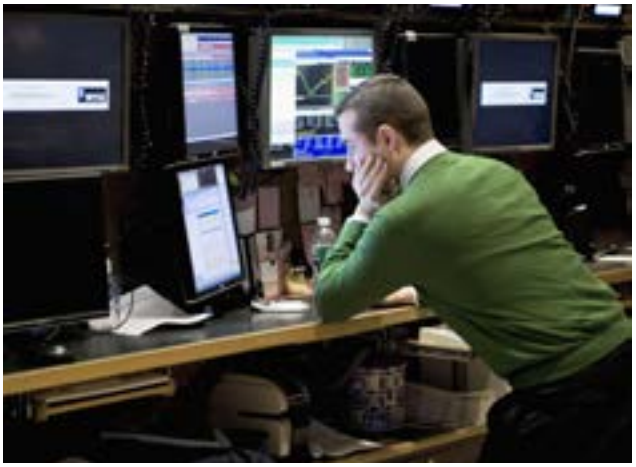
금융 및 보험

2019년 금융 및 보험 부문은 4년 연속 가장 많이 공격 당한 산업이었습니다. 이 부문에 대한 공격은 10대 공격 피해 산업에 대한 전체 공격의 17%를 차지했습니다.

재정적 동기가 부여된 사이버 범죄자가 금융 기관을 표적으로 하는 적극적인 사이버 위협 활동가의 대다수를 이룰 가능성이 높으며 사이버 범죄에서 금융 회사가 갖는 매력은 분명합니다.

X-Force 사고 대응 용역 데이터에 따르면 대중에 공개된 데이터 유출 건수가 적음에도 불구하고, 금융 및 보험이 최고 표적 대상 산업 중 첫 번째로 나타났습니다

이는 금융 및 보험 회사가 다른 산업에 비해 더 많은 공격을 경험하는 경향이 있지만 주요 사건으로 전환하기 전 위협을 탐지하고 억제하는 더 효과적인 도구와 프로세스를 보유할 가능성이 있음을 시사합니다. 금융 회사는 또한 공격 시 대응 계획을 시험하고 많은 조직이 IBM Security Command Centers를 사용해서 사이버 공격에 대비하고 연습하는 경향이 있습니다. Ponemon Institute에서 실시하고 IBM Security에서 후원하는 2019년 데이터 유출 비용 보고서[4] 내용에 따르면 관련 시나리오에 대해 사고 대응 계획과 팀을 광범위하게 테스트하면 데이터 유출로 인한 재정적 피해를 완화하는 데 효과적이었습니다. 예를 들어 사이버 범위 환경에서 사고 대응 계획을 광범위하게 시험한 유출 조직은 데이터 유출 총 평균 비용 390만 달러보다 적은 평균 320,000달러의 손실을 입었습니다.



2019년, 금융 부문 조직을 겨냥한 지배적인 위협 그룹은 ITG03(Lazarus), ITG14(FIN7) 및 다양한 Magecart 집단입니다. TrickBot, Ursnif 및 URLZone과 같은 뱅킹 트로이 목마는 2019년에 고객의 계정을 탈취해서 은행을 괴롭혔던 가장 커다란 위협 중 하나였습니다.

4 연간 데이터 위반 비용 보고서는 Ponemon Institute에서 수행하고 IBM이 후원합니다.

소매업

2019 X-Force 데이터에 따르면 소매 산업은 전체 산업 중에서 두 번째로 많이 공격을 받았습니다. 이 부문은 10대 산업에 대한 전체 공격의 16%에 해당하는 영향을 받아, 2018년 4위 및 11%에서 크게 증가했습니다. 이 업계는 2019년 두 번째로 많은 네트워크 공격을 받았습니다.

소매 업계는 X-Force IRIS 데이터와 공개된 데이터 유출 정보를 통해 알려진 바에 따르면 2019년에 2위를 차지하게 되었습니다. 소매 조직을 표적으로 하는 가장 일반적 유형의 위협 활동가는 재정적 동기가 부여된 사이버 범죄자로서, 이 업계를 표적으로 소비자 개인 식별 정보(PII), 지불 카드 데이터, 재무 데이터 및 쇼핑 기록 그리고 로열티 프로그램 정보 등을 얻으려고 합니다. 사이버 범죄자는 일반적으로이 데이터를 이용해, 고객 계정을 탈취하고 사기를 유발하며 다양한 신원 도용 시나리오를 통해 데이터를 재사용합니다.

사이버 범죄자가 2019년 소매 업체를 표적으로 하는 데 사용된 인기 있는 공격 방법은 POS(판매 시점) 맬웨어 및 전자 상거래 결제 카드 스키밍으로, 각각 물리적 결제 단말기 또는 온라인을 통한 거래 중에 결제 카드 정보를 빼돌리는 것을 목표로 합니다.

특히, 통칭 Magecart집단으로 분류된 사이버 범죄 집단은 제3자 지불 플랫폼 및 잘 알려진 온라인 소매 업체를 표적으로 웹사이트의 카드 지불 페이지에 악성 JavaScript 코드를 직접 삽입합니다. 이 코드는 결제 프로세스의 일부로 실행돼, 피해자의 지불 카드 정보를 사이버 범죄자에게 전송하고 의도된 벤더를 확보합니다.

X-Force IRIS 사고 대응자들은 2019년에, 여러 번의 유출로 이러한 유형의 공격을 직접 관찰했으며 악성 코드 스니펫이 다소 기본적일 수는 있지만 기본 플랫폼의 백엔드 타협으로 범죄자는 전반적으로 동일한 기술을 통해 수천 개의 상점을 방문할 수 있었습니다.

소매 부문을 대상으로 한 대표적인 위협 그룹은 다음과 같습니다.

ITG14 (FIN7)	Hive0061 (Magecart 10)
HIVE0065 (TA505)	Hive0062 (Magecart 11)
ITG08 (FIN6)	Hive0066 (Magecart 12)
Hive0038 (FIN6)	Hive0067 (FakeCDN)
Hive0040 (Cobalt Gang)	Hive0068 (GetBilling)
Hive0053 (Magecart 2)	Hive0069 (Illum Group)
Hive0054 (Magecart 3)	Hive0070 (PostEval)
Hive0055 (Magecart 4)	Hive0071 (PreMage)
Hive0056 (Magecart 5)	Hive0072 (Qoogle)
Hive0057 (Magecart 6)	Hive0073 (ReactGet)
Hive0058 (Magecart 7)	Hive0083 (Inter Skimmer)
Hive0059 (Magecart 8)	Hive0084 (MirrorThief)
Hive0060 (Magecart 9)	Hive0085 (TA561)

온라인 전자상거래 스키머 외에도, POS 맬웨어는 거래 중이거나 데이터가 메모리에 기록될 때, POS 시스템과 백엔드 서버의 결제 카드 데이터를 빼돌리기 위해 그들의 브릭과 모르타르 위치에서 소매점을 대상으로 하는 사이버 범죄자가 사용하는 인기 있는 기술입니다.

운송업

운송 부문은 모든 국가의 중요한 인프라의 일부로 간주됩니다. 이 분야의 기업들은 산업 서비스 및 소비자 서비스 모두에 대해 지상, 해상, 항공 운송 등 3가지 주요 교통 수단을 통해 경제를 동원하고 있습니다. 이 부문은 2019년에 세 번째로 많은 공격을 받았으며, 공격 빈도는 2018년 13%에서 2019년 10%로 감소했습니다.

금융 및 소매업에 이어 3위라는 것으로 운송 산업 순위는 운송 회사가 운영하는 데이터 및 인프라의 매력이 높아지고 있음이 강조됩니다. 이러한 자산은 사이버 범죄자와 국가 소속 위협 활동가 모두를 유혹합니다. 운송 회사가 보유한 정보는 PII, 약력, 여권 번호, 로열티 프로그램 정보, 지불 카드 데이터 및 여행 일정을 포함해 잠재적으로 사이버 범죄자에게는 매력적인 대상입니다.

특히, 이 분야 내에서, 항공사와 공항은 점점 더 여행자의 개인 정보를 다크 웹에서 판매함으로써 관심 있는 여행자들을 추적하거나 돈을 벌기 위해 노력하는 사이버 범죄자들과 국가 적국들의 표적이 되고 있습니다.

운송 산업에 대한 사이버 위협은 공격에 미칠 수 있는 잠재적인 운동 효과, 인간의 생명을 위험에 빠뜨릴 수 있는 가능성, 작업을 수행하기 위해 운송 서비스에 의존하는 다른 산업에 영향을 줄 수 있는 가능성을 고려할 때 다른 부문에 비해 추가적인 위험이 따릅니다.

2019 년에는 사이버 범죄 그룹과 국가 소속 공격자가 전 세계 조직에 대한 공격을 개시하면서 운송 부문을 표적으로 하는 위협 활동가 그룹이 다양했습니다.

운송 부문을 겨냥한 유명한 위협 그룹은 다음과 같습니다.

ITG07 (Chafer)	ITG17 (Muddywater)
ITG09 (APT40)	Hive0016 (APT33)
ITG11 (APT29)	Hive0044 (APT15)
ITG15 (Energetic Bear)	Hive0047 (Patchwork)

미디어 및 엔터테인먼트

2019년 X-Force 순위에서 4번째로 많이 공격된 산업은 미디어 부문으로 10대 산업에 대한 전체 공격 중 10%를 차지했습니다. 미디어 부문은 2018년 8%로 6위에서 4위로 상승했습니다.

미디어 부문에는 통신과 같은 유명 하위 산업과 뉴스 미디어 및 엔터테인먼트를 생산, 가공 및 배포하는 회사가 포함됩니다. 미디어 및 엔터테인먼트 산업은 여론에 영향을 미치거나 정보 흐름을 제어하거나 조직 또는 국가의 평판을 보호하려는 사이버 공격자에게 중요한 대상입니다. 특히, 국가-소속 집단은 부정적인 미디어 콘텐츠를 국가 안보에 심각한 위협으로 간주할 수 있는 반면 사이버 범죄자는 미디어 및 엔터테인먼트에 대한 공격을, 사전 방송된 미디어를 몸값을 받기 위해 훔칠 수 있기 때문에 재정적으로 유리할 것으로 보고 있습니다.

기회주의적 사이버 범죄자와 국가 소속 공격자는 일반적으로 2019년에 이 부문을 목표로 삼았습니다.

미디어 및 엔터테인먼트 부문을 겨냥한 유명한 위협 그룹은 다음과 같습니다.

ITG03 (Lazarus)

Hive0003 (Newscaster)

Hive0047 (Patchwork)

전문 서비스업

전문 서비스 산업에는 다른 분야에 전문 컨설팅 서비스를 제공하는 다양한 회사가 있습니다. 법률, 회계, HR 및 전문화된 고객 지원을 제공하는 회사를 그 예로 들 수 있습니다. X-Force에 따르면 이 부문은 10대 산업에 대한 전체 공격의 10%를 차지해 2018년 12%에서 10%로 줄였습니다.

대중에 공개된 데이터 유출 정보는 전문 서비스업도 우리 순위의 전체 산업에서 최대 다수의 기록 유출이 있었음을 나타냅니다. 이런 회사 중 상당수는 법적 절차, 회계 및 세금 목적의 데이터를 포함해 고객으로부터 매우 중요한 데이터를 얻습니다. 이러한 정보는 금전적 이익 또는 내부 정보를 모색하는 공격자의 수익 높은 표적이 될 수가 있습니다.

또한 이 산업에는 타사 액세스로 인해 점점 더 많은 표적이 되는 기술 회사가 포함돼, 더 큰 규모의 잠재적으로 더 안전한 조직을 공격하려는 공격자가 이를 활용할 수 있습니다.

또한 전문 서비스 회사의 일상적인 워크플로는 피싱 이메일 및 악성 매크로를 통해 범죄자를 위한 자연스러운 공격 경로를 만드는 경향이 있습니다. 많은 전문 서비스 회사는 Word 및 Excel 문서 첨부 파일과 같은 생산성 파일에 크게 의존해 계약을 작성하고 고객과 소통하며 일상적인 작업을 완료합니다. 매크로의 사용은 사이버 범죄자들이 악의적인 스크립트를 파일 형식으로 심어 조직이 완전히 차단할 수 없는 악의적 공격 경로 중 하나입니다.

2019년 전문 서비스를 겨냥한 주목할 만한 위협 활동가 그룹은 다음과 같습니다. ITG01 (APT10, Stone Panda)는 중국에 기반한 것으로 보이는 국가에 소속되어 후원 받는 그룹입니다.

정부

정부 부문은 우리 순위에서 6번째로 많이 공격 받은 산업으로, 10개 산업 기준 8%의 공격을 받아 전년 대비 변경은 없지만 2018년 7위였던 전체 순위는 상승했습니다.

정부 부문은 인식된 적에 비해 우위를 점하려는 국가 사이버 행위자, 보안이 약화된 정보를 노출하거나 기술력을 입증하려는 해커, 강탈이나 도난 데이터를 통해 금전적 이득을 추구하는 사이버 범죄자들에게는 높은 가치를 지닌 대상입니다.

사이버 범죄자들이 민간 부문만큼 안전하지 못한 조직들로부터 강탈금을 거두려 하기 때문에, 지방 자치 단체는 특히 최근 몇 년 동안 공격을 받고 있습니다. 정부 기관은 위협 행위자에 대한 가치 자산, 주로 기밀 정보 및 가능한 국가 기밀 정보를 보유하고 있으며, 여기에는 공무원 및 대리인에 대한 PII, 재무 정보, 내부 통신 및 중요 네트워크의 기능이 포함될 수 있습니다.

국가별 행위자들은 정부 부문 기업을 공격하는 데 대한 장기적인 관심을 보여주었고, X-Force IRIS는 그들이 그렇게 할 수 있는 능력이 있다고 평가합니다. 하지만, 2019년에는 사이버 범죄 단체들이 정부 기관들을 겨냥하기도 했습니다. 특히 지방 자치 단체나 시 차원에서 정부가 운영해야 할 랜섬 데이터를 암호화하여 보유하려고 했습니다.

2019년, 1월과 7월 사이에만 70개 이상의 정부 기관이 랜섬웨어 공격을 받았습니다.사이버 범죄자들은 또한 국방 웹사이트에서 데이터를 훔쳐 나중에 다크 웹에 누출시켰습니다. 해커들은 정부가 매력적인 목표라고 악명높게 생각하고 있는데, 특히 그들이 성명을 발표하고자 하는 논란이 있는 문제가 있다면 더욱 그렇습니다. 정부 기관에는 보통 민간 부문과 동일한 수준의 사이버 보안 자금이 부족하지만 여전히 구성 요소에 대한 일관된 서비스를 유지해야 하므로 위협 활동가로 인해 이러한 조직에 제기되는 문제가 더욱 악화됩니다.

2019년 정부 기관을 겨냥한 주목할 만한 위협 활동가 그룹은 다음과 같습니다. 다양한 사이버 범죄자 및 국가에 소속되어 후원 받는 집단

교육

교육 부문은 10대 산업에 대한 전체 공격의 8%를 받아, 2018년 6%에서 8%로 증가했고 순위는 7번째로 가장 많이 공격을 받은 산업입니다.

교육 산업은 재정적 동기를 가진 국가 소속 활동가들에게 귀중한 자산을 제공합니다. 지적재산권(IP)에서 PII 까지, 교육 조직은다양한 유형의 위협 행위자의 충분한 대상입니다.

각기 다른 동기 부여를 가진 공격자는, 다양한 초기 감염 벡터를 사용하여 학술 기관의 네트워크를 침입했지만 가장 일반적으로 관찰되는 방법은 여전히 피싱 이메일이며 특정 학술 기관 또는 연구 분야에 맞게 조정됩니다.

교육 부문 조직에는 종종 다양한 IT 인프라와 디지털 공간이 있습니다. 교육 부문 조직은 직원부터 학생 및 계약자에 이르기까지 많은 사용자에게 서비스를 제공하는 다양한 자산을 운영합니다. 위협 활동가가 다양한 악성 활동에 활용할 수 있는 이 방대한 공격 영역은 보안을 유지하기가 더 어렵습니다. 2019년 10월에 발표된 보고서에 따르면 미국에서만 2019년에 적어도 500개의 학교가 사이버 공격(대부분 랜섬웨어)을 받았습니다.

이 부문의 더욱 정교한 공격의 예로는 대학 네트워크를 손상시킨 후 미디어 조직과 군 계약자를 감염시키기 위한 준비 장소로 사용한 국가 위협 행위자를 들 수 있습니다. 마찬가지로 미국이 자금을 지원하는 연구를 찾는 공격자들은 정기적으로 대학 네트워크를 침입하여 종종 귀중한 지적 재산을 훔칠 수 있는 방법을 찾고 있습니다.

교육 부문을 겨냥한 유명한 위협 그룹은 다음과 같습니다.

ITG05 (APT28)
ITG12 (Turla Group)
ITG13 (APT34)
ITG15 (Energetic Bear)
ITG17 (Muddywater)
Hive0075 (DarkHydrus)

IBM X-Force IRIS는 귀중한 정보에 대한 액세스 권한을 얻으려는 재정적 동기가 있는 활동가 및 국가 계열의 활동가가 계속 이 산업을 목표로 삼을 것이라고 확신합니다.

2019년 이 분야를 표적으로 하는 주목할 만한 위협 활동가 집단에는 기회주의적 사이버 범죄 집단과 중국, 러시아 및 이란의 국가 소속 공격자가 포함되었습니다

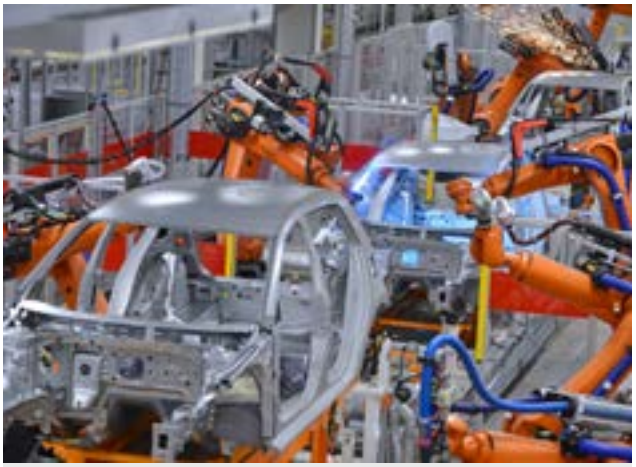
제조업

금속, 화학, 자본재 및 전자 제품을 통해 경제를 이동시키는 제조업체는 연결된 OT 층에 영향을 미치는 IT 위협 및 위협으로부터 면제되지 않습니다. 피해 비율이 2018년 10대 공격 피해 산업에 대한 전체 공격의 10%에서 8%로 떨어진 제조업은 순위로는 8번째로 가장 많이 공격을 당한 산업입니다.

이 부문에서 전년 대비 공격이 줄어들었을 가능성이 있지만 숫자의 감소는 많은 경우 제조업 부문 데이터 유출이 반드시 법적 공개 및 규제 대상인 정보를 포함하지 않는다는 사실을 반영할 수 있습니다. 결과적으로 공격이 항상 공개되는 것은 아니라서 제조업체가 실제 공격보다 덜 자주 공격을 받는 것처럼 보일 수 있습니다.

또한 제조업체는 IT 및 OT 환경을 모두 운영하는 조직이므로 ICS 및 SCADA 시스템에 영향을 주는 위협과 동일한 위협에 노출됩니다. 그러나 이 부문의 정보 보안은 과거에 뒤쳐져 있지만, 노르웨이 제조업체가 2019년 대대적인 랜섬웨어 공격에 성공적으로 대응한 것은 이 업계에 의한 사이버 보안에 대한 접근방식이 바뀌었다는 것을 보여주는 것일 수 있습니다.

금융 이익 및 IP 데이터를 노리는 사이버 범죄자 또는 국가 소속 활동가가 아마 제조 부문 회사에 가장 큰 위협이 될 수 있습니다. 2019년 제조업체를 대상으로 한 가장 일반적인 공격 기법 중 하나로 특히 그들이 외국 공급업체와 자주 거래하는 경우 BEC(Business Email Compromise) 사기를 들 수 있습니다. 이러한 경우, 회사 전자 메일 서버 또는 전자 메일 계정은 기존 통신 스레드에 자신을 삽입해서, 궁극적으로 자신이 제어하는 계정으로 수백만 달러를 돌려놓는 공격자에 의해 손상됩니다.



제조 산업을 겨냥한 주목할 만한 위협 그룹은 다음과 같습니다.

ITG01 (APT10)
ITG09 (APT40)
HIVE0006 (APT27)
Hive0013 (OceanLotus)
Hive0044 (APT15)
Hive0076 (Tick)

제조업체는 또한 연쇄 공격에 취약하며 제조하고 다른 나라로 배송하는 제품에 백도어나 맬웨어를 심는 국가의 적에 의해 악용될 수 있습니다.

공격자는 재정적 동기 측면에서 거래 기밀과 지적 재산권을 얻기 위해 제조업체를 대상으로 삼을 수 있습니다. 조직이 수년에 걸쳐 실시간 연구는 다크 웹 상에서 사이버 범죄자들에게 빠른 이익을 가져다 주거나 국가의 경제적 또는 국방적 이점을 증대시킬 수 있습니다. 특히 국방 및 군사 장비 제조업체의 경우 그렇습니다.

X-Force 데이터에 따르면 랜섬웨어, 피싱 공격 및 SQLi 삽입 공격도 빈번하게 제조 산업에 영향을 미쳤습니다.

에너지 산업

에너지 부문은 2019년 순위 10위의 산업으로 2019년 10대 산업에 대한 전체 공격 및 사건 중의 6%를 공격 받았습니다. 이 부문 순위는 2018년에도 6%의 공격을 받아 전과 같습니다.

에너지 부문의 기업은 모든 국가의 주요 인프라의 중추로서의 중요성 때문에 사이버 공격 표적이 되는 것이 입증되었습니다. 에너지는 다양한 형태로 도시와 산업의 경제적, 국가 안보적, 일상적 기능에 가장 중요합니다.

에너지 부문에 대한 공격의 목표는 다양합니다. 고객 데이터, 재무 자료, 영업 비밀 및 독점 기술 정보 같이 에너지 회사 내의 일부 수익성 있는 자산들은 다른 산업의 회사에서 발견되는 자산들과 가치가 비슷합니다.

에너지 산업이 다른 산업과 다른 것은 ICS 시스템과 그 관리를 하는 SCADA 시스템의 물리적 중단 및 파괴 가능성입니다. 이러한 시스템은 특히 사이버 전쟁 상황과 경쟁국들의 핵 시설을 만질 때, 목표 시설 내에서 운영을 감시하거나 통제하기를 원하는 적들에게 매우 귀중한 대상이 될 수 있습니다. 이 산업은 ZeroCleare 등 파괴적인 맬웨어의 표적이었습니다.

시스템 운영 중단을 노려 설계된 ICS 시스템에 대한 성공적인 공격은 전력, 가스, 석유 또는 에너지 부문에서 제공하는 기타 자원에 의존하는 고객에게 치명적인 영향을 줄 수 있습니다. 우크라이나의 발전소를 대상으로 한 일련의 사건에서 그러한 공격과 그들의 해로운 영향이 과거에도 관찰되어 왔으며, 이는 러시아가 실행하고 물리적인 파괴를 목표로 하고 있다고 알려져 있습니다.

이 부문을 표적으로 한 주목할 만한 위협 그룹은 다음과 같습니다.

- ITG01 (APT10)
- ITG09 (APT40)
- ITG07 (Chafer)
- ITG11 (APT29)
- ITG12 (Turla Group)
- ITG13 (APT34)
- ITG15 (Energetic Bear)
- ITG17 (Muddywater)
- Hive003 (APT35)
- HIVE0006 (APT27)
- Hive0016 (APT33)
- Hive0044 (APT15)
- Hive0045 (Goblin Panda)
- Hive0047 (Patchwork)
- Hive0076 (Tick)
- Hive0078 (Sea Turtle)
- Hive0081 (APT34)

의료업

10번째 최다 표적 산업인 건강 관리 산업은 10대 산업에 대한 전체 공격의 3%를 받아 2018년 8위 및 6%에서 감소했습니다.

증거를 통해 재정적으로 동기화된 사이버 범죄자들이 의료 산업 네트워크와 의료기기에 대한 주요 공격자이며, 다크 웹 상에서 의료 기록을 훔쳐서 판매하거나, 활동을 방해하고 회사를 몸값으로 유지하기 위해 네트워크로 연결된 장치를 암호화하는 것을 목표로 한다는 사실을 알 수 있습니다.

병원과 요양원 네트워크의 중단을 통해 의료 기관이 운영을 빨리 복구해 인명을 보호할 목적으로 랜섬웨어 공격에 대해 비용을 지불하도록 압박할 수 있었습니다. 어떤 경우에는 2019년 Ryuk 공격으로 1,400만 달러를 요구하는 등 몸값은 터무니 없이 많은 금액이었습니다.

2020년으로 넘어가면서 의료 부문은 데이터를 보호하기 위해 보안 상태를 계속 발전시켜야 합니다. 병원들은 잦은 랜섬웨어 공격을 감안하여 사고 대응 능력을 강화해야 하며, 공격 동기가 부여된 공격자가 쉽게 타협하고 우회하기 위해 활용할 수 있는 불안정한 의료기기에 대한 새로운 공격을 경계해야 합니다.

이 분야를 겨냥한 주목할 만한 위협 활동가 집단에는 Ryuk 랜섬웨어를 운영하는 이들과 같이 재정적으로 동기 부여된 사이버 범죄 그룹이 포함되었습니다. 랜섬웨어 공격은 병원이 영향을 받을 때 발생할 수 있는 위기를 강조하지만, 이 부문에 대한 국가 소속 집단의 지속적인 관심은 보이지 않고 있습니다.

지역별 해석

위협 행위자는 2019년에 모든 지역을 대상으로 했으며 북미, 아시아 및 유럽에서 가장 높은 수준의 활동이 관찰되었습니다.

X-Force 연구원들은 2019년 중동과 남미를 겨냥한 위협 행위자 활동을 발견했으며, 중동은 더 많은 해커와 국가간 공격으로 구성되어 있으며 남미는 주로 재정적 동기가 부여된 행위자의 영향을 받았습니다.

이 섹션에서는 X-Force가 관찰한 대상의 성격을 이해하고 각 영역에 초점을 맞춘 주요 위협 행위자 및 위협 행위자 활동의 잠재적 증가에 대해 2020년에 인식할 주요 날짜를 더 잘 이해하기 위해 이러한 지역에서 공격에 대해 보다 심층적으로 다룰 예정입니다. 일부 지역에서는 최근 몇 년간 그 지역을 겨냥한 활동을 펼친 위협 활동가가 강조되지만 이 목록이 전부가 아니라 2019년 이전의 데이터를 포함합니다. 이 섹션에서는 위에서 설명한 대로 IBM 위협 그룹 명명법을 사용하며, 공개된 유출 데이터뿐 아니라 IBM의 글로벌 사고 대응 데이터도 사용합니다.

북미

북미는 2019년 사건의 44%를 차지하면서 위협 행위자의 대상에 대한 모든 부문에서 가장 높은 순위를 차지했습니다.

북미는 수많은 잠재적인 대상을 포함하고 있으며 상당한 양의 인터넷 인프라를 유지하여 범죄 행위자에게 좋은 대상이 되고 있습니다. 2019년 북미는 50억 개가 넘는 기록이 손상되었습니다.

IBM은 2019년 지하 시장에서 구매하거나 무료로 구입할 수 있는 코드화된 상용 맬웨어를 사용한 여러 북미 사고에 대응했습니다. 상용 맬웨어는 속이기 어려울 수 있지만 범죄 목표를 달성하는 데 매우 효과적 일 수 있습니다.

북미를 대상으로 하는 국가 행위자 활동은 일정하게 유지되었지만 2019년에는 중대한 사건이 관찰되지 않았습니다. 최근 미국과 중국 간의 무역 협상으로 인해 두 지역 모두에서 사업을 하는 조직을 대상으로 하는 공격이 증가할 수 있으며, 이러한 협상에 결말이 나지 않는 한 이러한 조직은 경계를 유지해야 합니다.

역사적인 사이버 보안이 중요한 다음 행사:

7월 13일
(미국 민주당 전당 대회)

8월 24일
(미국 공화당 전당 대회)

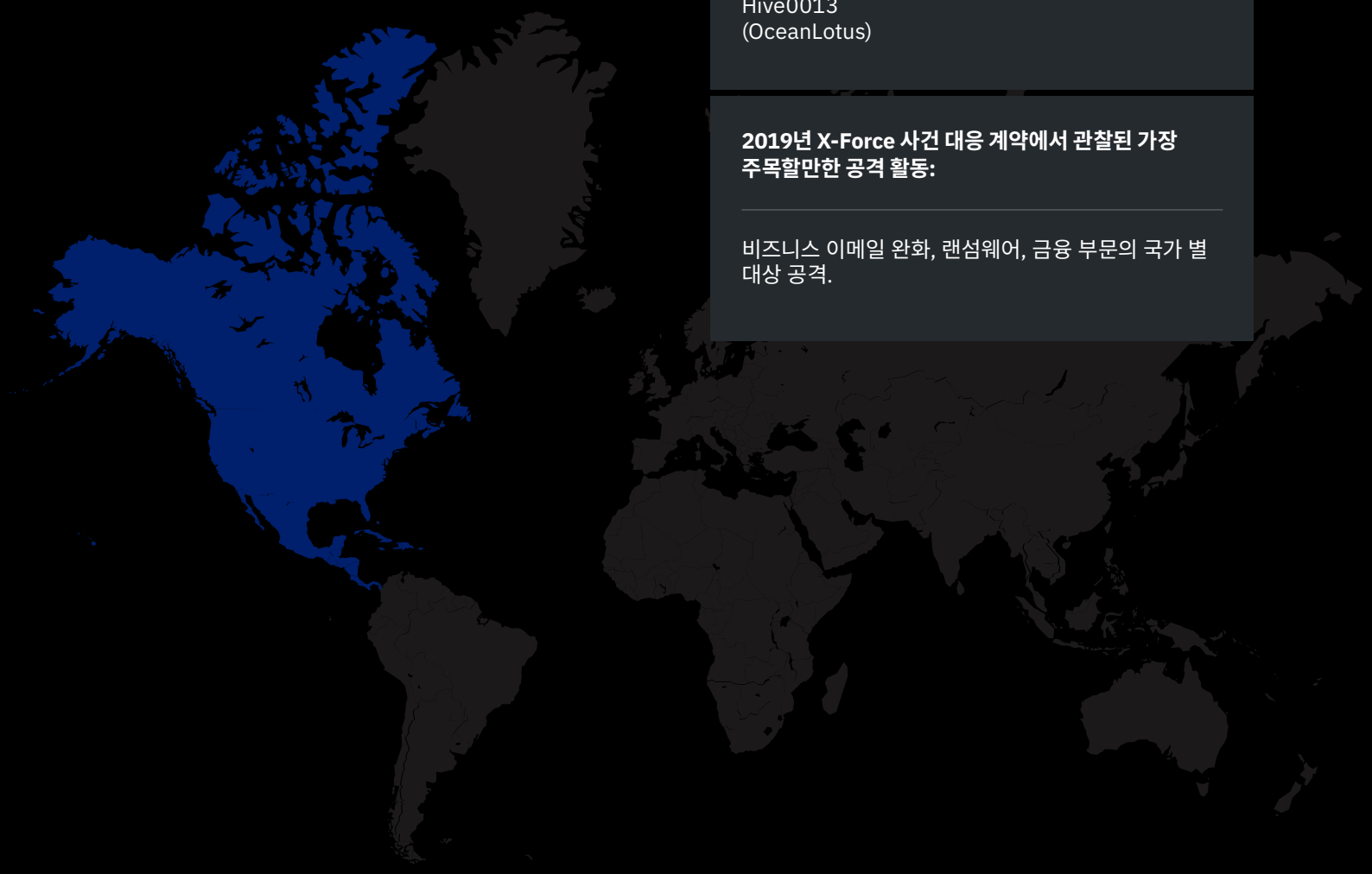
11월 3일
(미국 대통령 선거)

이 지역을 대상으로 한 위협 행위자 그룹은 다음과 같습니다.

ITG05 (APT28)
ITG08 (FIN6)
ITG11 (APT29)
ITG15 (Energetic Bear)
Hive0082 (Cobalt Dickens)
Hive0042 (Kovter)
Hive0016 (APT33)
Hive0013 (OceanLotus)
Hive0006 (APT27)
Hive0003 (APT35)
ITG01 (APT10)
ITG03 (Lazarus)
ITG04 (APT19)
ITG09 (APT40)
ITG07 (Chafer)

2019년 X-Force 사건 대응 계약에서 관찰된 가장 주목할만한 공격 활동:

비즈니스 이메일 완화, 랜섬웨어, 금융 부문의 국가 별 대상 공격.



아시아

아시아는 X-Force 분석에서 두 번째로 높은 위험 등급을 받았으며, 이는 공공 침해에서 두 번째로 높은 사건 수를 기록하며 2019년에는 22%의 사건이 발생했습니다. 아시아는 2019년에 20억 건이 넘는 기록 침해가 발생했으며, 이는 올해 북미에 이어 두 번째입니다.

상당수의 위협 행위자들이 특히 한반도, 일본 및 중국의 아시아 관련 조직을 대상으로 하였습니다. 이 지역 내에서 관측된 상당 수의 공격은 국가별 행위자 TTP와 관련이 있었습니다. 하나의 예로 ITG10을 들 수 있는데, 이는 한국 기업을 목표로 하는 북한 행위자일 가능성이 높습니다. 또 다른 예로는 ITG01을 들 수 있는데, 이는 일본을 목표로 하는 중국 행위자일 가능성이 높습니다.

최근 아시아의 지정학적 사건으로 인해 이 지역에서 국가 간 제휴 활동의 가능성이 높아졌습니다. 홍콩의 민주주의 시위와 그에 따른 단속으로 중국이 우위를 점했습니다. 북한과 주변국 간의 긴장이 고조되면서 이러한 구조가 더욱 강화되었습니다. 인도의 카슈미르 지역 흡수는 이 지역의 긴장을 고조시켰습니다.

2020년으로 넘어가면서, 이 지역에서 운영되는 조직에서 발생할 수 있는 리스크를 파악하기 위해서는 이러한 잠재적인 지정학적 리스크에 대한 모니터링이 매우 중요합니다.

역사적인 사이버 보안이 중요한 다음 행사:

7월 24일
(2020 도쿄 올림픽)

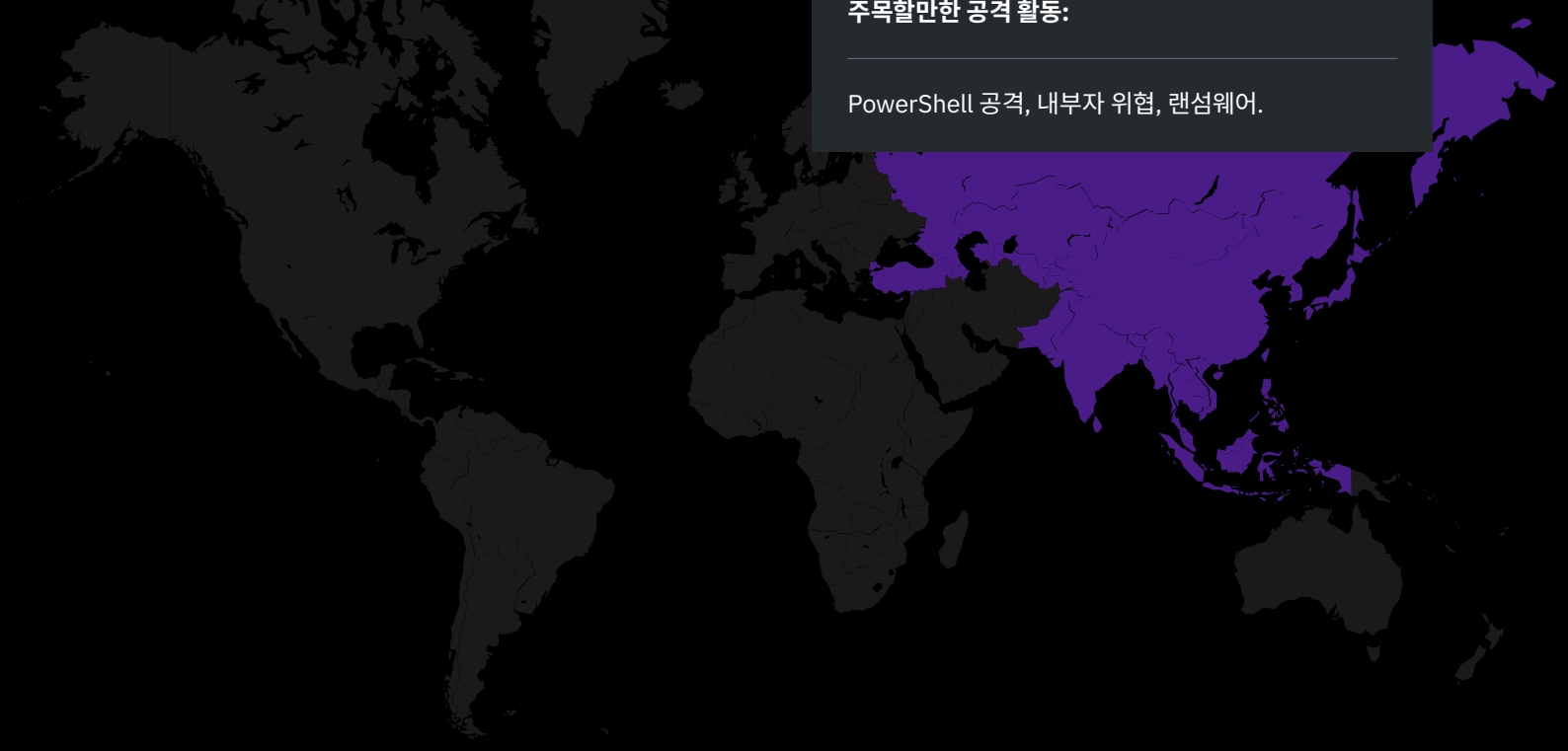
10월 10일
(대만 독립 기념일).

이 지역을 대상으로 한 위협 행위자 그룹은 다음과 같습니다.

Hive0013 (OceanLotus)
Hive0044 (APT15)
Hive0045 (Goblin Panda)
Hive0049 (Samurai Panda)
ITG01 (APT10)
ITG03 (Lazarus)
ITG05 (APT28)
ITG06 (APT30)
ITG09 (APT40)
ITG10 (APT37)
ITG11 (APT29)
ITG16 (Kimsuky)
Hive0016 (APT33)
Hive0040 (Cobalt Gang)
Hive0047 (Patchwork)
Hive0063 (DNSpionage)
Hive0076 (Tick)
Hive0079 (Labryinth Cholima)
Hive0006 (APT27)
Hive0003 (APT35)
ITG15 (Energetic Bear).

2019년 X-Force 사건 대응 계약에서 관찰된 가장 주목할만한 공격 활동:

PowerShell 공격, 내부자 위협, 랜섬웨어.



유럽

유럽은 아시아와 비슷한 수준의 악의적 활동에 희생되어 21%의 사건이 발생했습니다.

경쟁 국가들에 의해 주로 영향을 받는 아시아와는 달리, 유럽은 주로 재정적으로 동기를 부여 받은 위협 행위자들의 대상이 되는 것으로 나타났습니다. 이러한 차이는 환율에 근거한 유럽계 기업들로부터의 도난 가능성이 더 크다는 데서 설명될 수 있습니다. 또한 범죄 동기는 지적 재산을 추구하는 것일 수 있으며, 이는 상당한 이익을 얻기 위해 경쟁업체에 판매될 수 있습니다.

영국의 유럽 연합에서의 탈퇴(브렉시트)는 2020년에 활동하는 해커 집단에서 반향을 일으킬 수 있지만, 2019년에 발생한 활동은 관측되지 않았습니다. 또한, 주요 유럽 국가(독일, 프랑스)에서 다가오는 선거는 잠재적으로 이들 국가의 정책에 영향을 미치려는 국가 행위자들의 목표가 될 수 있습니다.

역사적인 사이버 보안이 중요한 다음 행사:

1월 31일
(제 50조에 의거 유럽 연합을 탈퇴하는 영국)

6월 28일
(우크라이나 헌법의 날/NotPetya 기념일).

이 지역을 대상으로 한 위협 행위자 그룹은 다음과 같습니다.

ITG05 (APT28)
ITG08 (FIN6)
ITG12 (Turla)
ITG15 (Energetic Bear)
ITG09 (APT40)
ITG07 (Chafer)
ITG11 (APT29)
ITG14 (FIN7)
ITG17 (Muddywater)
Hive0006 (APT27)
Hive0003 (APT35)
Hive0013 (OceanLotus)
Hive0044 (APT15)
Hive0063 (DNSpionage)

2019년 X-Force 사건 대응 계약에서 관찰된 가장 주목할만한 공격 활동:

RDP 손상, POS 맬웨어, 내부자 위협

중동

X-Force IRIS는 2019년 중동의 조직에 영향을 미치는 여러 국가 관련 사건을 관찰했지만, 2019년에는 이 지역에서 발생한 사고의 7%로 위협 행위 활동에 대한 전체 지표가 상대적으로 낮았습니다.

이러한 위협 활동이 감소된 것을 설명하는 여러 가지 설명이 존재합니다. 예를 들어, 다른 지역에서는 사이버 범죄 활동에 대한 높은 투자 수익률을 제공합니다. 하지만 다른 지역과는 달리, 중동은 세계의 다른 지역들에 비해 해커와 국가 활동의 비율이 더 높았습니다.

해커의 활동은 2019년 이 지역의 정치적 불안과 관련이 있을 수 있으며 이란과 관련된 여러 가지 주요 사건이 있습니다. 마찬가지로, 이란의 국가 이익을 추구하는 ITG13과 같은 국가 간 활동은 파괴적인 공격으로 이 지역의 에너지 분야의 조직을 목표로 하는 국가 목표를 따랐습니다.

예멘의 정치적 불안과 지금도 진행 중인 전쟁은 사이버 위협 활동의 위험을 계속 초래하고 있습니다. 분쟁의 모든 측면에서 활동하는 행위자들은 사이버 공격을 통해 메시지를 전파하고 수익을 창출하고 있습니다. 다른 당사자들이 진행 중인 갈등 속에서 서로를 공개적으로 위협함에 따라 이러한 위험은 2020년까지 계속될 것입니다.

역사적인 사이버 보안이 중요한 다음 행사:

11월 21일
(2022 클럽 월드컵 축구 토너먼트, 카타르)

이 지역을 대상으로 한 위협 행위자 그룹은 다음과 같습니다.

Hive0044
ITG07 (Chafer)
ITG13
Hive0081 (APT34
Hive0078 (Sea Turtle)
Hive0075 (DarkHydrus)
Hive0063 (DNSpionage)
Hive0047 (Patchwork)
Hive0022 (Gaza Cybergang)
Hive0016 (APT33)
Hive0006 (APT27)
Hive0003 (APT35)
ITG17 (Muddywater)
ITG12 (Turla)
ITG11 (APT29)
ITG10 (APT37)
ITG09 (APT40)
ITG05 (APT28)
ITG01 (APT10)

2019년 X-Force 사건 대응 계약에서 관찰된 가장 주목할만한 공격 활동:

파괴적인 맬웨어, DDOS 공격, 웹 스크립트.

남미

남미는 2019년에 상당한 사이버 범죄 활동으로 어려움을 겪었지만, 사건의 5%를 차지하면서 상위 3개 지역과 같은 수준의 집중력을 얻지 못했습니다. 하지만 이 지역에서 매년 활동이 증가하고 있습니다. X-Force는 특히 소매 및 금융 서비스 부문에서 중요한 사고 대응 활동의 상승세를 관찰하고 있습니다.

이 지역에서 관측된 사건에는 2019년 내내 인기를 끌었던 랜섬웨어 활동이 포함되었습니다.

역사적인 사이버 보안이 중요한 다음 행사:

6월 12일
(2020년 코파 아메리카 축구 토너먼트, 콜롬비아 및 아르헨티나).

이 지역을 대상으로 한 위협 행위자 그룹은 다음과 같습니다.

Hive0081 (APT34)
Hive0044 (APT15
Hive0016 (APT33)
Hive0013 (OceanLotus)
Hive0003 (APT35)
ITG17 (Muddywater)
ITG12 (Turla)
ITG11 (APT29)
ITG05 (APT28)
ITG03 (Lazarus)
ITG01 (APT10)

2019년 X-Force 사건 대응 계약에서 관찰된 가장 주목할만한 공격 활동:

비즈니스 이메일 완화, 랜섬웨어, 금융 부문의 국가 별 대상 공격.

2020년의 유연성을 위한 준비

이 보고서의 IBM X-Force 조사 결과에 따르면, 위협 인텔리전스에 대응하고 강력한 대응 능력을 구축하는 것은 어떤 산업 또는 국가에서 운영하든 상관없이 변화하는 환경에서 위협을 완화하는 데 영향을 미치는 방법입니다.

우리 팀은 각 조직이 2020년에 사이버 위협에 보다 효과적으로 대비하기 위해 취할 수 있는 다음과 같은 여러 단계를 취하도록 권장합니다.

- 위협 행위자의 동기와 전술을 보다 잘 이해하기 위해 위협 인텔리전스를 활용하여 보안 리소스의 우선 순위를 정합니다.
- 조직 내에서 사고 대응 팀을 구축하고 교육시킵니다. 불가능할 경우 효과적인 사고 대응 기능을 사용하여 영향력이 큰 사고에 신속하게 대응합니다. 2019년 IBM Security는 영향을 포함하면 관련 비용을 상당히 줄일 수 있으며, 팀이 MegaCortex 감염에 신속하게 개입하여 랜섬웨어 공격을 중류에서 중지하고 수천 달러의 피해를 방지할 수 있다는 사실을 발견했습니다.
- 조직의 사고 대응 계획을 테스트하여 근육 기억(muscle memory)을 개발합니다. 팀은 테이블탑 훈련이나 사이버 공격 경험을 통해 대응 시간을 개선하고 가동 중지 시간을 줄이며 위반 시 궁극적으로 비용을 절감할 수 있습니다.
- 다단계 인증(MFA) 구현은 조직에서 가장 효율적인 보안 우선 순위 중 하나입니다. 2019년에는 자격증명 도용 또는 재사용이 위협 행위자가 가장 많이 사용하는 공격 방법 중 하나였으며 MFA는 이 공격이 이행되기 전에 이를 효과적으로 억제할 수 있습니다.
- 공격 벡터로 피싱이 널리 퍼져 있기 때문에 조직에 Quad9와 같은 스푸핑된 도메인을 탐지하고 차단할 수 있는 솔루션을 제공해야 합니다.
- 백업을 하고 백업을 테스트하며 백업을 오프라인에 저장하십시오. 실제 테스트를 통해 백업의 존재 여부뿐만 아니라 백업의 효과까지 보장하는 것은 조직의 보안을 유지하는 데 있어 중요한 차이를 만듭니다.

주요 시사점을 통한 앞으로의 발전

2020년에 조직은 오래된 위협과 새로운 위협을 염두에 두어야 합니다.

- 위험은 2020년에도 계속 증가할 것이며, 현재 150,000개 이상의 취약성과 새로운 취약성이 정기적으로 보고될 것입니다.
- 2018년에 비해 2019년에 4배 이상 많은 기록이 침해되었기 때문에 2020년에는 위반과 공격으로 인해 또 다른 많은 수의 기록이 손실될 수 있습니다.
- 위협 행위자들은 IoT 기기, OT(운영 기술) 및 연결된 산업 및 의료 시스템을 점점 더 대상으로 설정하여 몇 가지 명칭을 지정함으로써 다양한 공격 벡터에 지속적으로 눈을 돌리고 있습니다.
- 2019년 랜섬웨어, 크립토마이너 및 봇넷 등이 모두 다른 지점에서 주도권을 잡는 등 위협 행위자들의 악성 소프트웨어 사용이 계속 요동치고 있습니다. 우리는 이러한 추세가 2020년에도 계속될 것으로 예상하고 있습니다. 즉, 조직은 시간 경과에 따라 변화하는 다양한 위협으로부터 스스로를 보호해야 합니다.
- 랜섬웨어 및 크립토마이너를 위한 높은 수준의 코드 혁신 기술은 이러한 위협이 2020년에도 계속 진화하고, 이에 따라 더 나은 탐지 및 격리 기능이 필요함을 암시합니다.
- 스팸 활동은 지속적으로 증가하며, 조직에 의한 부지런한 블랙리스트 작성, 취약성 패치 및 위협 모니터링이 요구됩니다.
- 산업별 대상 공격의 연도별 변화는 모든 산업 부문에 대한 위험과 사이버 보안 프로그램의 의미 있는 발전과 성숙도에 대한 필요성을 강조합니다.
- 조직은 지리적 위치를 사용하여 가장 가능성이 높은 공격자와 공격 동기를 식별하여 직면할 수 있는 관련 위험을 예측하고 완화할 수 있습니다.

X-Force 정보

IBM X-Force는 최신 위협 추세를 연구하고 모니터링하여 고객과 일반 대중에게 신종 및 중요 위협에 대해 알리고 보안 콘텐츠를 전달하여 IBM 고객을 보호합니다.

인프라, 데이터 및 애플리케이션 보호에서 클라우드 및 관리형 보안 서비스에 이르기까지, IBM Security 서비스는 귀사의 귀중한 자산을 보호할 전문 기술력을 보유하고 있습니다. IBM Security는 최고의 기술 인력을 채용하여 세계에서 가장 정교한 일부 네트워크를 보호합니다.

기고자

Michelle Alvarez
Dave Bales
Joshua Chung
Scott Craig
Kristin Dahl
Charles DeBeck
Ari Eitan (Intezer)
Brady Faby (Intezer)
Rob Gates
Dirk Harz
Limor Kessem
Chenta Lee
Dave McMillen
Scott Moore
Georgia Prassinos
Camille Singleton
Mark Usher
Ashkan Vila
Hussain Virani
Claire Zaboeva
John Zorabedian

IBM Security에 대한 자세한 정보 →

IBM Security
New Orchard Rd
Armonk, NY 10504
Produced in the United States of America
February 2020

Produced in the United States of America
February 2020

IBM **Security**