Microsoft

Microsoft 보안 인텔리전스 보고서

제24호
2018년 1월~12월

목차

저자 및 기고자 . . . 3
머리말 . . . 4
섹션 I: 랜섬웨어, 암호화폐 마이닝, 자금 . . . 6
랜섬웨어 공격 감소 . . . 7
암호화폐 마이닝 증가 . . . 10
브라우저 기반 암호화폐 마이너: 새로운 종류의 위협 . . . 11
원치 않는 암호화폐 마이닝의 영향 . . . 12
섹션 II: 위험에 빠진 소프트웨어 공급망 . . . 13
위험에 빠진 신뢰 . . . 16
소프트웨어를 넘어: 클라우드 개체를 통한 공급망 손상 . . . 17
사이버 인시던트 조사: 전문 서비스 . . . 18
섹션 III: 피싱은 여전히 만연 . . . 19
피싱은 2018년에도 여전히 선호되는 공격 벡터입니다. . . . 20
사이버 인시던트 조사: 제조 . . . 23
섹션 IV: 전 세계의 맬웨어. . . . 24
사이버 인시던트 조사: 금융 서비스 . . . 27
지침 . . . 28
데이터 원본 . . . 33

이 문서는 정보를 제공하는 목적으로만 사용됩니다. MICROSOFT는 이 문서의 정보에 대해 명시적이거나 묵시적이거나 법적인 어떠한 보증도 하지 않습니다.

이 문서는 "있는 그대로" 제공됩니다. 이 문서에 표기된 정보 및 보기(URL, 인터넷 웹 사이트 참조 포함)는 사전 통보 없이 변경될 수 있습니다. 이를 사용함으로써 발생할 수 있는 위험은 사용자가 감수합니다.

Copyright © 2019 Microsoft Corporation. 무단 전재 금지.

여기에 언급된 실제 회사 및 제품의 이름은 해당 소유자의 상표일 수 있습니다.

저자 및 기고자

Abhishek Agrawal
정보 보호

David Fantham
정보 보호

Debraj Ghosh
Microsoft 보안 마케팅

Diana Kelley
사이버 보안 솔루션 그룹

Elia Florio
Windows Active Defense

Eric Avena
Windows Defender 연구팀

Eric Douglas
Windows Defender 연구팀

Francis Tan Seng
Windows Defender 연구팀

Jonathan Trull
사이버 보안 솔루션 그룹

Joram Borenstein
사이버 보안 솔루션 그룹

Karthik Selvaraj
Windows Defender 연구팀

Kasia Kaplinska
Microsoft 보안 마케팅

Kristina Laidler
보안 인시던트 대응

Matt Duncan
Windows Active Defense 데이터 엔지니어링 및 분석

Mark Simos
사이버 보안 솔루션 그룹

Paul Henry
Wadeware LLC

Pragya Pandey
Microsoft 보안 마케팅

Ram Pliskin
Azure 보안

Ryan McGee
Microsoft 보안 마케팅

Seema Kathuria
사이버 보안 솔루션 그룹

Steve Wacker
Wadeware LLC

Tanmay Ganacharya
Windows Defender 연구팀

Volv Grebennikov
Bing

Yaniv Zohar
Azure 보안

머리말

안녕하세요. Microsoft 보안 인텔리전스 보고서(SIR) 제24호에 오신 것을 환영합니다. 실무자이자 보안 설계 전문가로서 본인은 이와 같은 보고서를 읽으며 환경에 대한 이해를 높이고 그러한 지식을 활용해 조직을 보다 효과적으로 방어하고 보호하는 방법에 대한 실제적인 조언을 얻고자 합니다.

SIR팀은 이 보고서에 사이버 복원력 개선을 위한 교육을 제공하고 1년 간 데이터를 면밀히 조사해 가장 중요한 교훈을 얻었습니다.

이 보고서에는 1년 동안의 보안 데이터 분석 및 실습에서 얻은 교훈에 관한 인사이트가 담겨 있습니다. 분석된 데이터에는 Microsoft 클라우드에서 매일 발생하는 6.5조 개의 위협 신호와 전 세계에 있는 Microsoft 보안 연구자 및 대응자 수천 명의 연구와 실제 경험이 포함됩니다. 2018년 공격자들은 새로운(코인 마이닝) 또는 기존(피싱)의 부정한 수법을 다양하게 활용하여 지속적으로 고객과 조직으로부터 데이터 및 리소스를 도용하고자 하였습니다. Ursnif 캠페인처럼 복합적인 공격은 사회적 접근법과 기술적 접근법을 혼용하였습니다. 소란스럽고 파괴적인 공격 형태인 랜섬웨어에 방어자들이 보다 스마트하게 대응함에 따라 범죄자들은 더 '은밀'하지만 여전히 수익성 있는 코인마이너로 중심을 옮겼습니다.

그 "중심"은 공격자가 항상 한 걸음 앞서 있기 때문에 좌절감을 줄 수 있습니다. 그러나 다른 렌즈로 보면 이 이야기는 긍정적입니다. 독자와 같은 방어자와 사이버 보안 전문가들이 방어 기법을 구현하여 공격자가 자신들이 선호하는 페이로드를 변경하고 랜섬웨어를 사용하지 못하도록 하였습니다.

사이버 범죄자들이 활동을 늘린 또 다른 분야는 공급망입니다. 가장 주목할 만한 것 중 하나인 도포일 코인마이너 공격은 2018년 3월 6일 감염된 P2P(peer-to-peer) 응용 프로그램에 의해 처음 시작되었습니다. 공급망에 대한 우려는 응용 프로그램을 넘어 클라우드로 이어졌으며 악성 브라우저 확장, Linux 저장소 손상, 백도어 모듈 다중 인스턴스 등이 있습니다. 이러한 위협을 해결하기 위해 조직에서는 투명하고 신뢰할 수 있는 공급망 모델을 지향합니다.

데이터는 중요할 뿐만 아니라 때로는 실제 조직에서 일어난 일을 알아내는 데 도움이 됩니다. 따라서 이 보고서에는 탐지대응팀(DART)을 통해 현장에서 배운 교훈이 포함되어 있습니다. 여기에는 어떻게 대형 제조회사가 제어 기능을 구현해 수 개월 동안 괴롭히던 다단계 피싱 캠페인을 차단할 수 있었는지 또 금융서비스 업체가 고급 조사 도구 및 엔드포인트 모니터링을 사용해 위협 행위자를 시스템에서 근절할 수 있었는지에 관한 내용이 있습니다.

마지막으로 피싱 클릭은 계속 증가했지만 머신 러닝 모델이 계속 진화해 피싱이 사용자 상자에 도달하기 전에 피싱을 감지하고 클릭 후에는 피해를 막습니다. 또 다른 좋은 소식은 점점 더 많은 기업에서 다단계 솔루션을 구현하고 자격 증명 도난 피싱 이메일의 성공을 제한하고 있습니다.

공격자들은 기회를 찾아 다니기 때문에 그들의 기법과 기술에 대해 많이 알수록 보다 신속하게 방어 및 대응 태세를 갖출 수 있습니다. 중요한 작은 단계는 조직의 전반적인 사이버 보안 상태에 큰 차이를 만들 수 있습니다. 따라서 이 보고서에는 맬웨어 및 공격 환경 변화에 대한 심층적인 인사이트와 함께 권장 단계 및 기타 모범 사례 지침이 제공됩니다. 그것이 바로 실무자가 나쁜 악당과 싸울 때 필요한 것이기 때문입니다. 독자에게도 필요한 것이기를 바랍니다.

Diana Kelley
Microsoft 사이버 보안 현장 *CTO*

P.S. 우리는 항상 SIR 개선을 모색합니다. 피드백이 있는 경우 회사로 연락해 알려 주시기 바랍니다.

섹션 I

랜섬웨어, 암호화폐 마이닝, 자금

2017년 화제가 된 보안 관련 기사는 주로 랜섬웨어에 관한 것이었습니다. 전 세계적으로 관심을 끌었던 WannaCrypt 및 Petya의 발생으로 컴퓨터를 잠그거나 암호화한 후 액세스 복원을 위해 돈을 요구하는 맬웨어의 일종인 랜섬웨이에 대해 일반적인 인식이 생겨났으며 많은 사람들은 앞으로 문제가 더욱 커질 것으로 추측하였습니다. 그런데 랜섬웨어 발생이 2018년에 크게 줄어들었습니다.

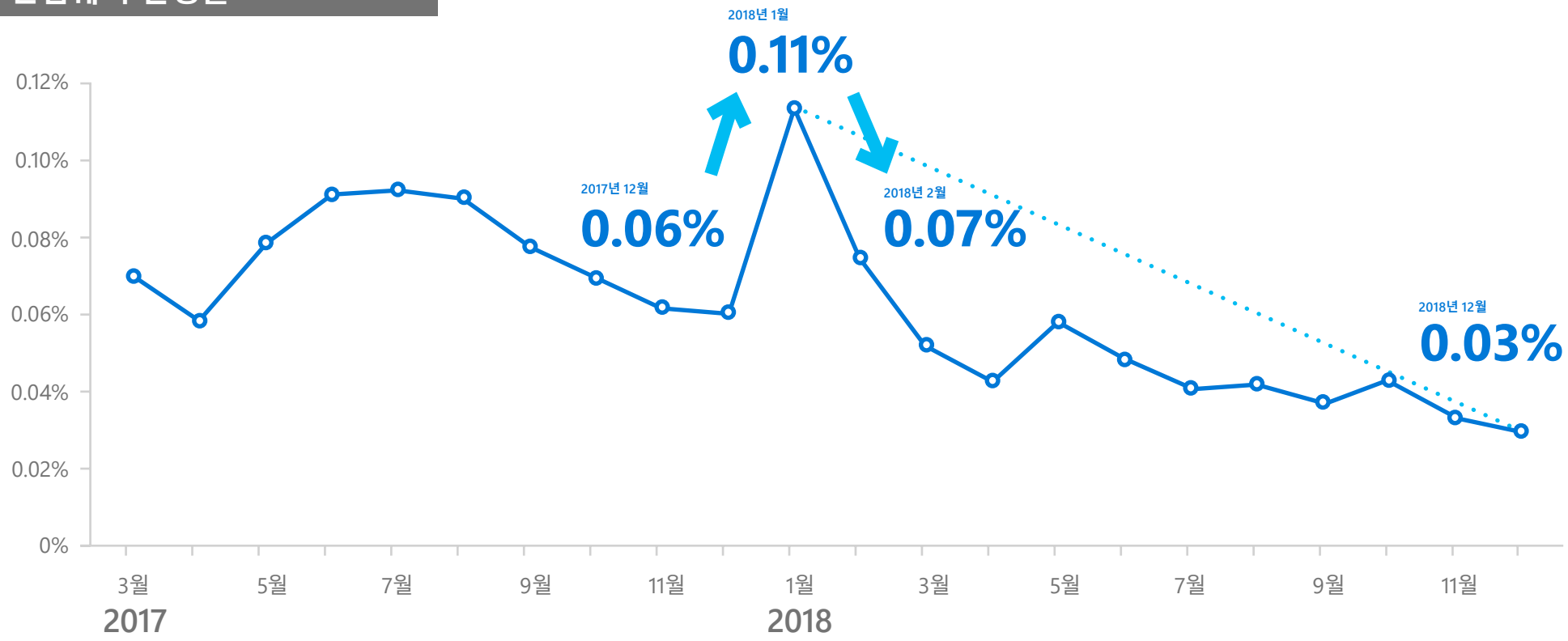
랜섬웨어 발생이 줄어든 부분적인 이유는 감지 및 교육의 개선으로 공격자들이 랜섬웨어에서 수익을 창출하기가 더 어려워졌기 때문입니다. 그 결과 공격자들은 랜섬웨어에서 벗어나 피해자의 컴퓨팅 리소스를 사용하여 공격자를 위한 디지털 화폐를 만드는 암호화폐 마이닝 같은 접근방식으로 노력을 전환하기 시작하였습니다. 이러한 전환은 가장 수익 지향적인 사이버 범죄자의 기회주의적 본성을 보여줍니다. 그들은 가장 쉽게 돈을 벌 수 있는 방법을 추구하는 경향이 있으며 사이버 범죄의 자본 조건이 바뀌면 재빨리 그 변화를 따라갑니다.

랜섬웨어 공격 감소

10여 년 전 지하에서 초기 악성코드를 지배했던 해커와 장난꾼들이 조직 범죄 및 기타 이익 지향적인 관심사로 대체되었습니다. 초기 맬웨어는 요란하고 실체가 확실한 경우가 많았지만 수익지향적 맬웨어는 기능을 지속적이고 가능한 한 오래 수행하도록 조용히 작동하고 관심을 피하려는 경향이 강했습니다. 해당 기능에는 스팸 전송, 민감한 정보 도용, 서비스 거부 공격, 기타 악의적 활동 등이 있습니다.

랜섬웨어는 이러한 추세를 거슬렀습니다. 랜섬웨어는 눈에 띄지 않으려는 노력 대신 피해자가 몸값을 지불할 때까지 컴퓨터와 중요 파일에 대한 피해자의 접근을 공개적으로 거부합니다. (그리고 몸값을 지불한 후에도 공격자가 컴퓨터 제어를 해제하지 않는 경우가 종종 있습니다.) 랜섬웨어가 2017년 절정에 달하자 이러한 형태의 개방형 공격이 공격자 기술의 새로운 단계를 대변하는 것처럼 보였습니다. 그러나 최근 데이터에 따르면 랜섬웨어는 감소 추세에 있는 것처럼 보입니다. 공격자들이 점점 더 과거에 사용했던 은밀한 작동 방식으로 돌아가 암호화폐 마이닝 같은 공격을 효과적으로 수행하기 위해 잠복 상태를 유지하려고 합니다. 랜섬웨어 발생률이 줄어들었지만 이것이 반드시 공격의 심각도가 감소했다는 의미는 아닙니다.

랜섬웨어 발생률



랜섬웨어 발생률은 2017년 3월과 2018년 12월 사이에 약 60% 감소했으며 해당 기간에 간헐적인 증가가 있었습니다.

▲ **그림 1.**

랜섬웨어 발생 현황 (2017년 3월 ~ 2018년 12월)

이러한 전반적인 감소에는 다양한 원인이 있을 수 있습니다. 물론 Microsoft 보안 연구자들은 주요 요인 중 하나로 최종 사용자와 조직에서 랜섬웨어 위협에 대한 인식이 높아지고 이에 보다 지능적으로 대응하고 있는 것을 꼽습니다. 예를 들어 신중하게 중요 파일을 다루고 백업해 랜섬웨어로 암호화되더라도 복원이 가능하도록 합니다. 또한 앞에서 설명한 대로 사이버 범죄자들은 기회주의적입니다.

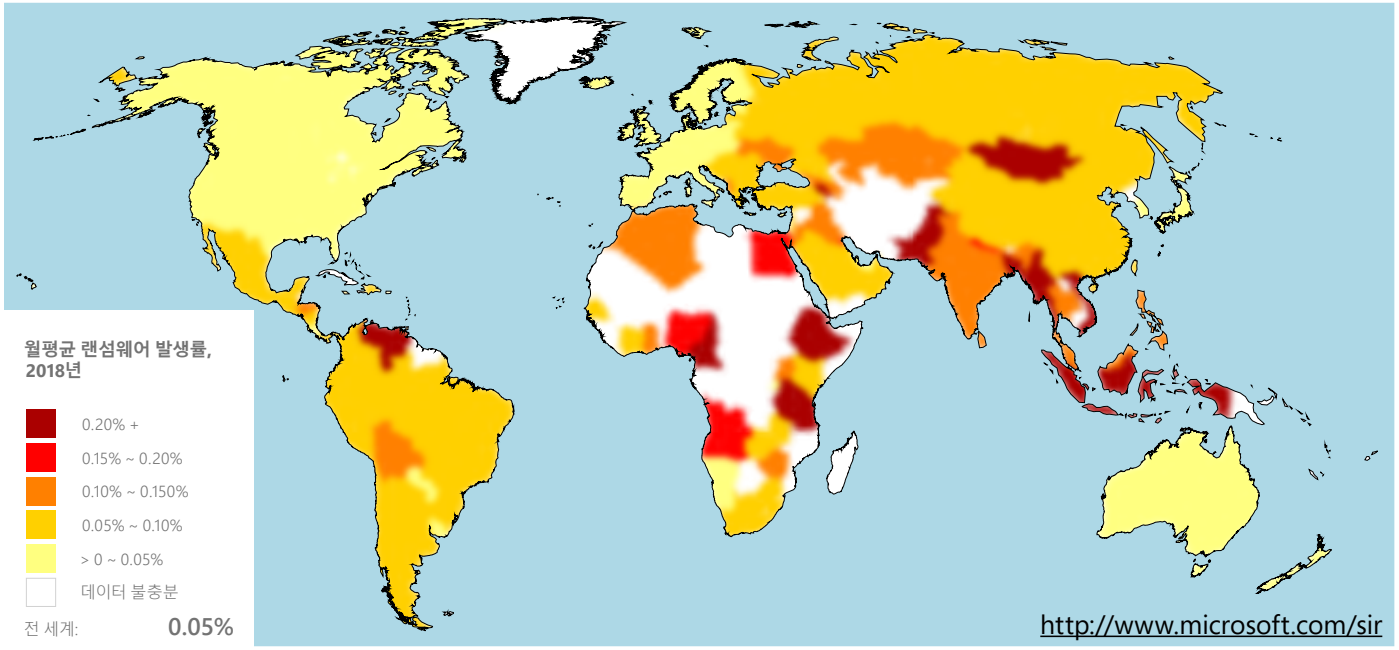
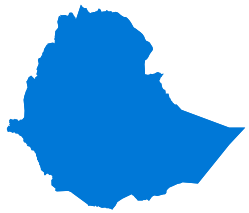


그림 2.

전 세계 월평균 랜섬웨어 발생률
(국가/지역별, 2018년)

랜섬웨어 피해가 가장 심각한 국가: 에티오피아



월평균 발생률: 0.77%

2018년 월평균 랜섬웨어 발생률이 가장 높았던 5개 국가는 에티오피아(0.77), 몽골(0.46), 카메룬(0.41), 미얀마(0.33), 베네수엘라(0.31)로 각각 해당 기간 동안 월평균 랜섬웨어 발생률이 0.31% 이상이었습니다.1 몇 년 전에는 랜섬웨어 공격이 유럽과 북아메리카의 부유한 국가 및 지역에 집중되는 추세였습니다. 그러나 공격자들이 더 이상 랜섬웨어를 선호하지 않게 되면서 발생 패턴이 전반적으로 맬웨어와 더욱 비슷해졌습니다.

2018년 월평균 랜섬웨어 발생률이 가장 낮았던 국가는 아일랜드(0.01), 일본(0.01), 미국(0.02), 영국(0.02), 스웨덴(0.02)으로 각각 해당 기간 동안 월평균 랜섬웨어 발생률은 0.02% 이하였습니다. 발생률이 낮은 곳은 사이버 보안 인프라가 성숙하고 주요 인프라를 보호하고 기본 보안에 관해 시민들과 소통하는 프로그램이 잘 갖춰져 있는 경향이 있습니다.

각주

[1] 발생률은 맬웨어 발생을 보고하는 Microsoft 실시간 보안 제품을 운용하는 컴퓨터의 비율입니다. 위협이 발생한다고 해서 컴퓨터가 감염되었다는 것을 의미하지는 않습니다. Microsoft에 데이터를 제공하기로 사용자가 선택한 경우에만 해당 컴퓨터가 발생률 계산에 포함됩니다.

암호화폐 마이닝 증가

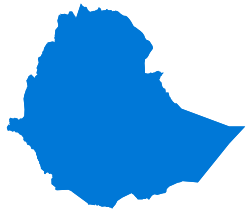
암호화폐는 익명으로 온라인과 현실 세계 모두에서 상품과 서비스를 사고 파는 데 사용할 수 있는 가상 화폐입니다. 여러 가지 다양한 종류의 암호화폐가 존재하지만 모두 블록체인 기술을 기반으로 합니다. 이 기술로 전 세계에 있는 수천만 또는 수백만 대의 컴퓨터에 의해 관리되는 분산 원장에 모든 거래가 기록됩니다. 복잡한 계산을 하고 블록체인 거래 확인 기능도 수행하는 컴퓨터에 의해 새로운 코인이 생성 즉 "마이닝"됩니다.

코인 마이닝은 수익성이 매우 높습니다. 가장 오래되고 가장 인기 있는 암호화폐인 비트코인은 2018년에 개당 가치가 미화 수천 달러에 달했습니다. 하지만 코인 마이닝에 필요한 계산 수행이 리소스 집약적이며 새로운 코인이 마이닝될 때마다 그 정도가 심화됩니다. 비트코인처럼 인기 있는 화폐의 경우 대부분의 개인과 소규모 집단이 쉽게 접근하지 못하는 방대한 컴퓨팅 리소스에 대한 액세스 없이 코인 마이닝이 거의 불가능합니다. 이 때문에 불법 이익을 얻으려는 공격자는 피해자의 컴퓨터를 사용해 암호화폐 코인을 마이닝할 수 있는 맬웨어에 점점 크게 의존하게 되었습니다. 이 접근법을 사용하면 한두 대가 아닌 수십만 대에 해당하는 컴퓨터 처리 능력을 활용할 수 있습니다. 사소한 감염이 발견되더라도 암호화폐의 익명성 때문에 책임 있는 당사자를 추적하기 위한 노력이 복잡해집니다.

2018년 전 세계 월평균 암호화폐 코인 마이닝 발생률을 0.12%였으며, 반면 랜섬웨어는 발생률이 0.05%에 불과했습니다. 맬웨어에 대한 페이로드로 마이닝이 인기를 끌게 된 데에는 많은 요인이 있습니다. 랜섬웨어와는 달리 암호화폐 마이닝은 사용자 입력이 필요하지 않습니다. 사용자가 다른 작업을 수행하거나 컴퓨터에서 멀어지면 백그라운드에서 작동합니다. 또한 컴퓨터 성능이 충분히 저하되지 않는 한 전혀 알아채지 못할 수도 있습니다. 결과적으로 사용자가 위협 제거 조치를 취할 가능성이 낮아지고 마이닝이 지속되어 공격자가 오랜 시간 동안 이익을 얻게 됩니다.

다양한 암호화폐의 은밀한 마이닝에 "기성품"을 사용할 수 있다는 것이 이러한 추세의 또 다른 동인입니다. 진입 장벽이 낮은 이유는 코인 마이닝 소프트웨어의 광범위한 가용성 때문입니다. 사이버 범죄자가 맬웨어로 리패키징하고 이를 알아채지 못하는 사용자의 컴퓨터로 전달합니다. 그런 다음 무기화된 마이닝 소프트웨어가 피해자에게 배포되는데 이 때 소셜 엔지니어링, 익스플로잇, 드라이브 바이 다운로드 등 다른 위협을 전파하기 위해 공격자가 사용하는 것과 동일한 여러 기법이 활용됩니다. 마이닝 소프트웨어가 설치된 후 피해자의 컴퓨터 백그라운드에서 실행되어 블록체인 계산을 수행하면 공격자는 이익을 얻게 됩니다.

암호화폐 마이닝 피해가 가장 심각한 국가의 월평균 발생률



에티오피아: **5.58%**

탄자니아: **1.83%**

파키스탄: **1.47%**

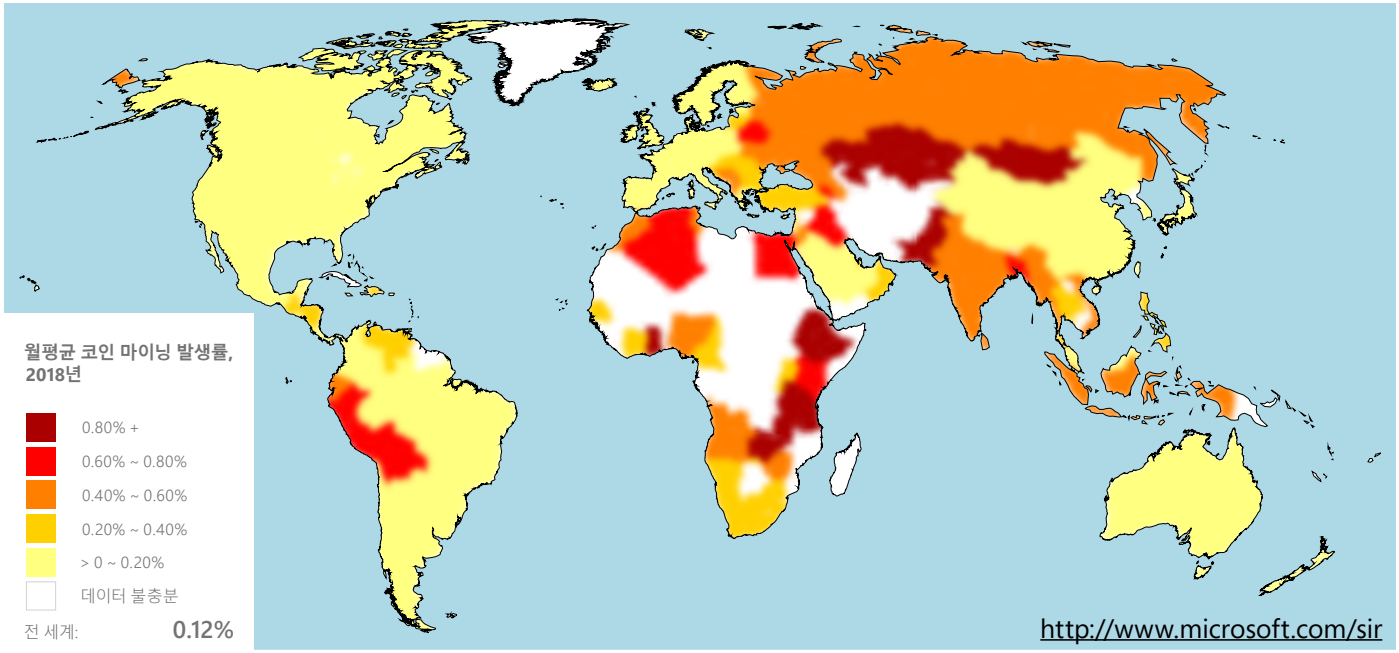


그림 3.

전 세계 월평균 코인 마이너 발생률
(국가/지역별, 2018년)

암호화폐 마이닝 피해가 가장 적은 국가의 월평균 발생률

아일랜드: 0.02%

일본: 0.02%

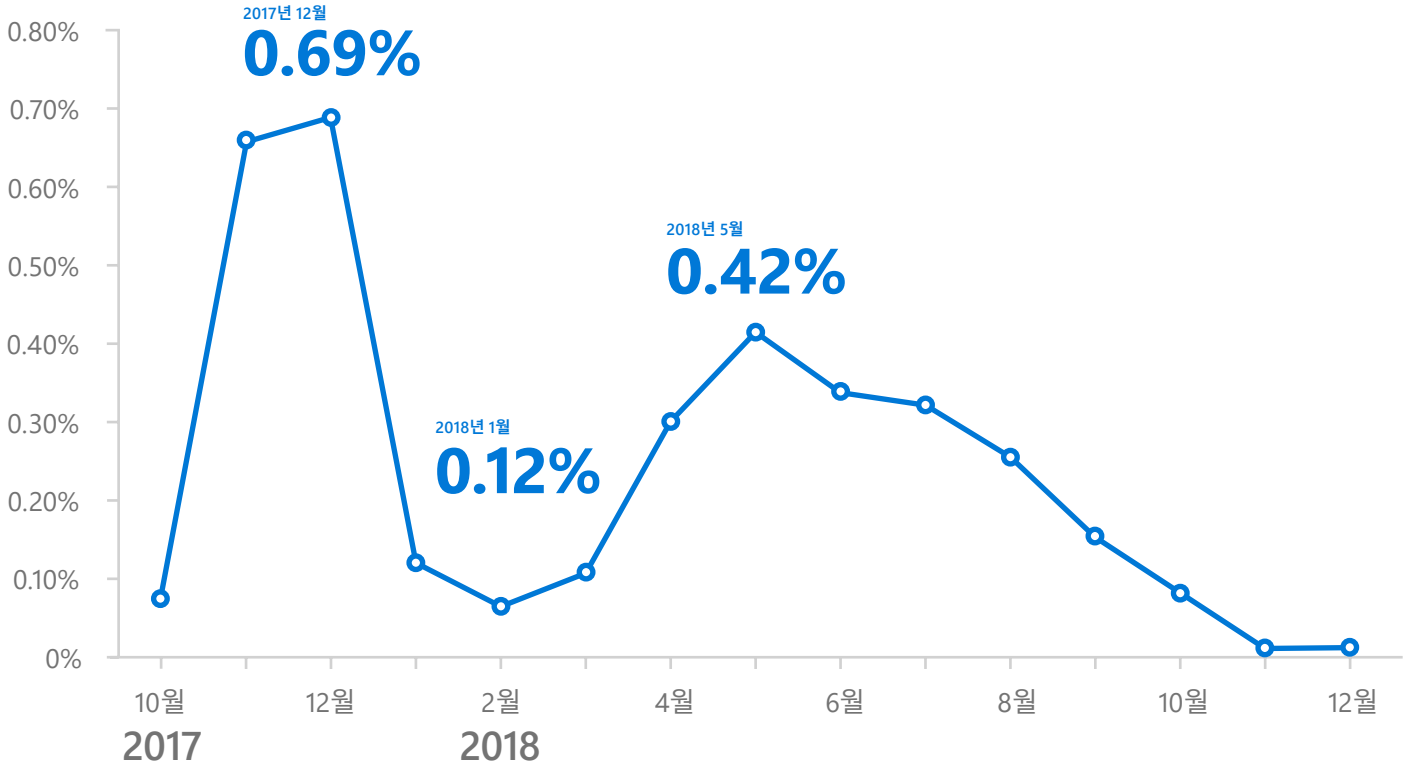
미국: 0.02%

2018년 암호화폐 코인 마이닝 발생률이 가장 높았던 5개 국가는 에티오피아(5.58), 탄자니아(1.83), 파키스탄(1.47), 카자흐스탄(1.24), 잠비아(1.13)로 각각 해당 기간 동안 월평균 코인 마이닝 발생률이 약 1.13% 이상이었습니다. 2018년 코인 마이닝 발생률이 가장 낮았던 국가는 아일랜드, 일본, 미국, 중국으로 각각 해당 기간 동안 월평균 코인 마이닝 발생률은 약 0.02%였습니다.

브라우저 기반 암호화폐 마이너: 새로운 종류의 위협

이 섹션에 제시된 통계는 피해자의 컴퓨터에 맬웨어로 설치되도록 설계된 악성 암호화폐 마이너를 포함합니다. 그러나 가장 중요한 암호화폐 마이닝 중 일부는 전적으로 웹 브라우저 내에 기반을 두고 있으며 설치가 전혀 필요하지 않습니다. 수많은 서비스에서 브라우저 기반 암호화폐 마이닝을 웹 사이트 소유자가 광고에 의존하지 않고 해당 사이트에 대한 트래픽에서 수익을 창출하기 위한 방법이라고 광고합니다. 사이트 소유자는 사용자가 사이트를 방문하는 동안 백그라운드에서 암호화폐를 마이닝하는 JavaScript 코드를 페이지에 추가해야 하며, 사이트 소유자와 해당 서비스가 수익을 나눕니다. 안타깝게도 공격자들은 재빠르게 이러한 서비스를 이용해 최종 사용자의 동의 없이 암호화폐를 마이닝하였으며 합법적인 웹 사이트를 손상시키고 악성 마이닝 코드를 소스 코드에 삽입하는 경우가 종종 발생하였습니다. 이러한 브라우저 기반

브로코이너 발생률



마이너는 최종 사용자의 컴퓨터를 손상시킬 필요가 전혀 없고 JavaScript 가능 웹 브라우저가 있는 모든 플랫폼에서 실행됩니다. 암호화폐 마이닝 트로이 목마처럼 브라우저 기반 마이너는 사용자가 감염된 웹 페이지를 방문하는 동안 컴퓨터 성능을 크게 저하시키고 전기를 낭비할 수 있습니다.

그림 4.

가장 보편적인 브라우저 기반 암호화폐 마이너브로코이너 발생률

원치 않는 암호화폐 마이닝의 영향

악성 암호화폐 마이닝으로 인해 피해자가 직면하는 가장 명백한 위협은 컴퓨팅 리소스 소비로, 전기를 낭비하고 컴퓨터 성능을 현저하게 저하시킬 수 있습니다. 사용자와 조직은 다음과 같은 코인 마이닝의 위험에도 직면해 있습니다.

미래에 더 큰 피해를 줄 기반 확보
다른 형태의 맬웨어와 마찬가지로 암호화폐 마이닝은 공격자의 진입점이 될 수 있습니다. 컴퓨터가 백그라운드에서 암호화폐 마이닝을 수행하는 동안 사이버 범죄자는 환경에 대해 배우고 다른 목적으로 악용하기 위한 보안상의 허점을 발견할 수 있습니다.

인터넷 연결 디바이스는 손상되고 암호화폐 마이닝 봇으로 전환될 수 있습니다.
이러한 디바이스에는 맬웨어 위협 감지와 같은 기본 제공 보안이 없기 때문에 공격자가 원하는 공격 대상이 될 수 있습니다.

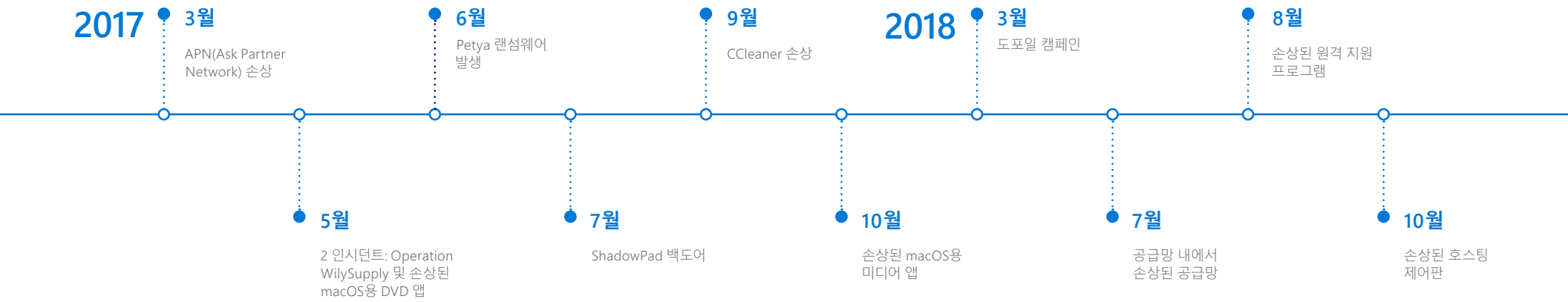
컴퓨터 손상
암호화폐 마이닝 소프트웨어가 지속적으로 몇 개월 이상 실행되면 성능이 저하될 수 있으며 과도한 전력 소비 및 CPU 사용으로 인해 발생하는 열은 컴퓨터를 손상시킬 수 있습니다.

섹션 II

위험에 빠진 소프트웨어 공급망

수 년 동안 Microsoft는 공급망 손상을 공격 진입점으로 사용하는 보안 위협자를 추적하였습니다. 공급망 공격에서 공격자는 합법적인 소프트웨어 게시자의 개발 또는 업데이트 프로세스를 손상시키는 데 집중합니다.

성공한 경우 공격자는 손상된 구성 요소를 합법적인 응용 프로그램 또는 업데이트 패키지에 통합하여 소프트웨어의 사용자에게 배포할 수 있습니다. 그런 다음 악성 코드는 소프트웨어와 동일한 신뢰와 권한으로 실행됩니다. 지난 몇 년 동안 소프트웨어 공급망 공격 건수 증가가 많은 사이버 보안 대화에서 중요한 주제가 되었으며 여러 IT 부서에서 주로 우려하는 부분입니다.



▲ **그림 5.**

2017년 및 2018년 소프트웨어 공급망 공격

2017년 주요 소프트웨어 공급망 공격

2017년 공급망 공격들은 이목을 끌었던 여러 인시던트로 인한 것이었습니다. 가장 주목할 만한 것은 6월에 발생한 Petya 랜섬웨어로, 최초 감염은 우크라이나에서 인기를 끌었던 세무 회계 응용 프로그램에 대한 업데이트 프로세스 손상에서 시작되었습니다. 5월에 Operation WilySupply가 텍스트 편집기의 소프트웨어 업데이트 도구를 손상시키고 금융 및 IT 부문의 대상 조직에 백도어를 설치하였습니다. 7월에는 ShadowPad라는 백도어가 서버 관리 소프트웨어 패키지에 잠복해 공격자들이 데이터 도용과 기타 악의적 활동을 위한 추가 맬웨어 페이로드를 설치하였습니다. 9월에는 대중적인 프리웨어 도구인 CCleaner가 손상되었고 백도어 버전이 해당 사용자 기반으로 유포되었습니다.

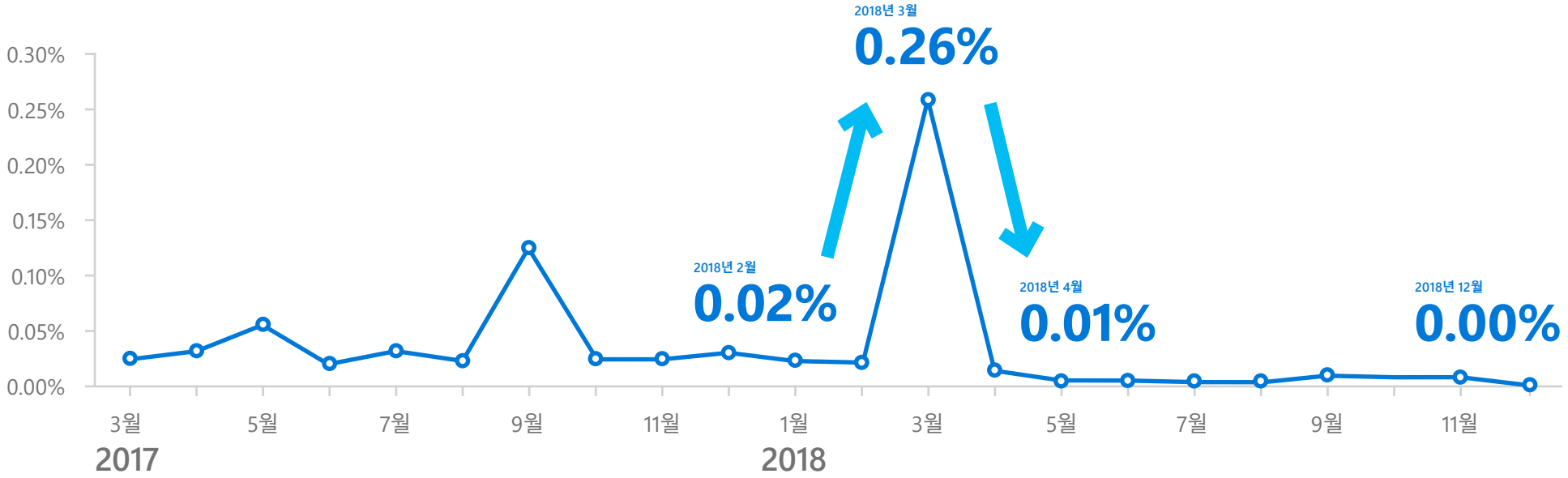
2018년 소프트웨어 공급망 공격 – 근본 원인과 영향

2018년 첫 번째 주요 소프트웨어 공급망 공격 인시던트는 3월 6일에 발생하였습니다. 당시 Windows Defender ATP가 도포일 트로이 목마(스모크로더라고도 알려짐)를 유포하는 대규모 캠페인을 차단하였습니다. 대규모 맬웨어 캠페인은 감염된 P2P(peer-to-peer) 응용 프로그램에서 시작되었습니다. 이 응용 프로그램의 업데이트 패키지가 손상된 코드를 다운로드한 악성코드로 대체되었고, 이후 도포일 맬웨어가 설치되었습니다. 정교한 트로이 목마는 코인 마이닝 페이로드를 운반했고, 고급 교차 프로세스 주입 기술과 지속성 메커니즘 및 회피 방법을 선보였습니다.

그림 6.

2018년 도포일(Smoke Loader) 발생 추세에 따르면 3월에 인스턴스 차단이 급증하였습니다.

도포일 발생률



캠페인 시작 첫 12시간 동안 Windows Defender Antivirus는 전 세계적으로 400,000개 이상의 감염 시도를 차단하였습니다. 러시아가 글로벌 발생의 73%를 차지하였고 터키와 우크라이나가 각각 18%와 4%를 기록하였습니다.

2018년에 손상된 소프트웨어 공급망을 유포 메커니즘으로 사용한 공격이 몇 건 더 감지되었으며 그 중 일부가 다음 표에 나와 있습니다.

기간	공격	설명	감염된 소프트웨어
2018년 3월	도포일 코인 마이닝 캠페인 (Microsoft에서 보고)	공격자는 P2P(peer-to-peer) 앱의 업데이트 프로세스를 감염시켜 도포일을 설치하였고 이어 코인 마이닝 맬웨어를 설치하였습니다.	P2P(peer-to-peer) 앱
2018년 7월	공급망 내에서 손상된 공급망 (Microsoft에서 보고)	공격자는 PDF 편집기 응용 프로그램 공급업체와 해당 소프트웨어 공급업체 파트너 중 한 곳이 공유하는 인프라를 손상시켰습니다.	PDF 편집기 응용 프로그램 및 타사 파트너 공급업체
2018년 8월	손상된 원격 지원 프로그램 (Operation Red Signature, Trend Micro및 IssueMakersLab에서 보고)	원격 지원 솔루션 공급업체의 업데이트 서버가 9002 RAT이라는 원격 액세스 도구를 유포를 위해 손상되었습니다.	원격 지원 프로그램
2018년 10월	손상된 호스팅 제어판 솔루션 (ESET에서 보고)	자격 증명 도용을 위해 호스팅 제어판 솔루션의 설치 스크립트가 변경되었습니다.	호스팅 제어판 솔루션

그림 7.

2018년 기타 소프트웨어 공급망 공격

위험에 빠진 신뢰

공급망 공격은 자신들이 사용하는 소프트웨어에 대한 사용자와 IT 부서의 신뢰를 이용하기 때문에 교활합니다. 손상된 소프트웨어는 공급업체가 서명과 인증을 하는 경우가 빈번하고 잘못된 사항에 대한 표시가 없어 감염을 감지하는 것이 훨씬 더 어려워 집니다. 기업 사용자든 가정 사용자든 관계없이 공급망과 고객 간의 관계에 해를 끼칠 수 있습니다. 소프트웨어를 감염시키고 공급 또는 업데이트 인프라를 손상시킴으로써 공급망 공격은 조직이 제공하는 상품과 서비스의 무결성과 보안에 영향을 줄 수 있습니다.

공급망 공격은 다양한 부문과 지리적 위치에 있는 광범위한 소프트웨어와 대상 조직에 영향을 주었습니다. 공급망 공격의 위협은 업계 전반의 문제로, 여러 이해관계자의 주의를 요합니다. 코드를 작성하는 소프트웨어 개발자 및 공급업체, 소프트웨어 설치를 관리하는 시스템 관리자, 공격을 찾아내고 이러한 공격으로부터 사람과 소프트웨어를 보호하는 솔루션을 창조하는 정보 보안 커뮤니티 모두 주의를 기울여야 합니다.

소프트웨어를 넘어: 클라우드 개체를 통한 공급망 손상

신뢰를 훼손하는 공급망 공격의 능력은 클라우드에서 증폭되고 훨씬 더 복잡해집니다. 2018년에 클라우드 개체, 서비스, 인프라가 손상된 여러 인시던트가 이러한 복잡성을 잘 보여줍니다.

- 악성 크롬 확장이 클릭 사기 맬웨어 설치 (ICEBRG에서 보고)
- 다양한 리눅스 저장소 손상(몇몇 온라인 포럼에서 보고)
- 공격자가 WordPress 사이트에 콘텐츠를 게시하도록 허용하는 등 다양한 악의적인 활동에 사용되는 악성 WordPress 플러그인 (Wordfence에서 보고)
- 암호화폐 코인 마이닝 맬웨어를 다운로드하고 Docker Hub 계정에 업로드하는 스크립트가 포함된 악성 Docker 이미지(Fortinet 및 Kromtech에서 보고)
- 공식 Python 저장소의 타이포스쿼팅 악성 패키지. 클립 보드에 있는 코인 마이닝 주소 하이재킹에 사용되는 맬웨어를 다운로드하는 악성 스크립트 포함 (Medium에서 보고)
- 손상된 StatCounter 스크립트. StatCounter를 사용하는 웹 사이트에 공격자가 악성 스크립트를 삽입하도록 허용(ESET에서 보고)
- 백도어 npm 모듈 관련 여러 인시던트(npm 블로그, Medium). 익스플로잇인 경우 공격자가 작동 중인 서버에 임의 코드를 입력하여 실행

이러한 인시던트는 공급망 손상이 어떻게 공격 노출 영역을 크게 넓히는지를 보여줍니다. 보안 조치를 하지 않으면 클라우드 개체는 예기치 않은 항목 벡터가 될 수 있습니다. 예를 들어 Docker Hub 인시던트는 숨겨진 코인 마이닝 백도어가 포함된 Docker 이미지를 업로드하는 악성 계정이 포함됩니다. Docker 이미지는 Docker Hub에서 거의 1년 동안 호스팅 되었고 수백만 번 다운로드 되어 이를 알지 못하는 관리자와 사용자가 사용하였습니다.

공급망 위험은 클라우드 코드, 오픈 소스, 웹 라이브러리, 컨테이너 및 클라우드 타 개체로 확장됩니다. 이러한 위험은 밝혀진 소프트웨어 및 하드웨어 공급망 손상 인시턴트 간 큰 차이와 결부되어 공급망 공격을 하나의 광범위한 위협 카테고리로 만듭니다. 이러한 공격 유형 전체에 대한 단일 솔루션은 없지만 조직에서는 예방적 보호 및 사후 공격 감지 체계를 구축하고 손상된 하드웨어/소프트웨어 공급업체, 벤더 및 인수업체, 오픈 소스 소프트웨어 공급업체, 클라우드 서비스 및 인프라 공급업체로부터의 공급망 공격을 막아야 합니다.

DART를 통한 사이버 인시던트 조사

Microsoft 탐지대응팀(DART)은 사이버 보안 전문가 및 인시던트 대응자로 구성된 글로벌 팀으로 조직의 사이버 보안 인시던트 감지, 조사, 대응을 지원합니다. 이 섹션에서는 DART가 작년에 처리한 고객 사례 중 일부를 예로 들어 일반적인 공격자 성향, Microsoft과 고객이 그들을 저지했던 방법에 관해 설명합니다.

민족 국가의 데이터 유출 공격을 경험한 전문 서비스 조직

한 전문 서비스 조직이 정교하고 국가가 지원하는 지속적 고급 위협(APT)의 공격을 받았습니다. 이 위협은 해당 조직의 권한 있는 자격 증명에 액세스할 수 있는 권한이 있었습니다. 공격자들은 암호 스프레이 공격으로 네트워크에 액세스하였습니다. 그들은 취약하거나 널리 사용되는 소수의 암호(예: 'p@ssword' 또는 '123456')를 사용하여 많은 수의 사용자 계정을 대상으로 Office 365 관리 자격 증명을 얻었습니다. (암호 스프레이 공격은 각 계정의 로그인 시도 횟수를 제한함으로써 감지를 피하는 데 사용됩니다.) APT는 네트워크에 침투한 후 직원 메일함에서 정교하고 자동화된 데이터 추출을 수행하였습니다. 사내에서 이 공격자들을 퇴출시키려고 여러 가지 시도를 했지만 공격자들은 200일 이상 네트워크에 남아 있었습니다. 공격자는 공격의 일환으로 조직의 공급망 소프트웨어를 활용하고 데이터를 자동 추출하였습니다.

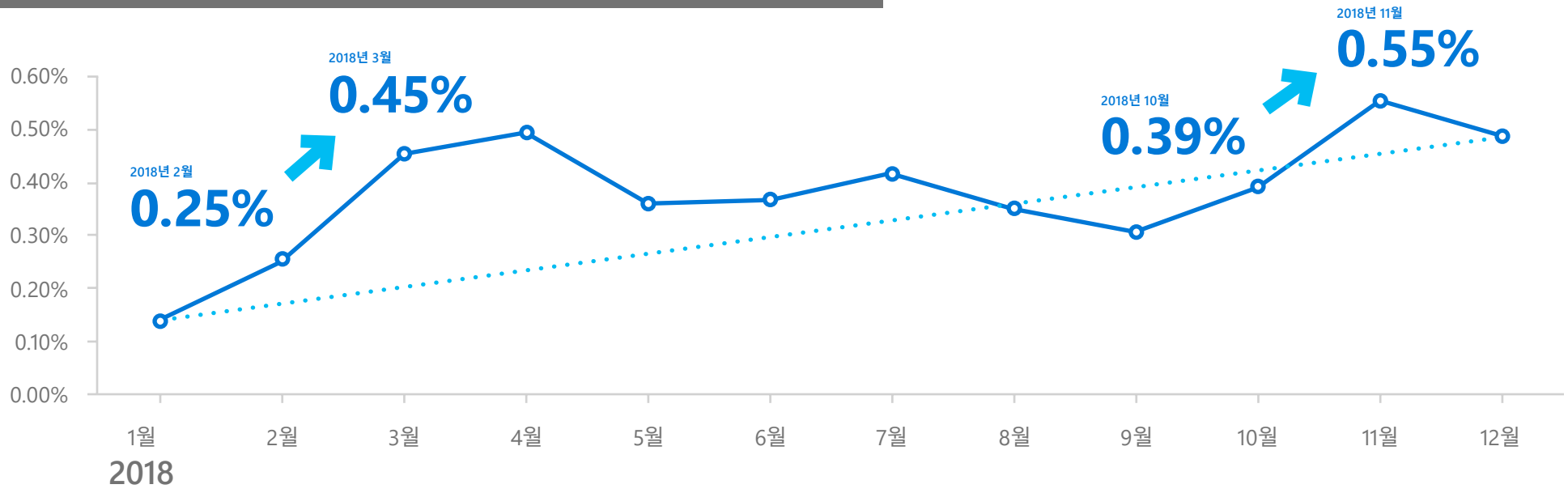
조직에서는 고객 데이터가 유출된 것으로 보고 DART팀에 조사 및 추가 피해 방지 지원을 요청하였습니다. DART는 공격 대상 Office 365 메일함, 손상된 계정, 공격자 명령 및 제어 채널을 확인하였습니다. 이 인시던트로부터 고객이 얻은 핵심 교훈은 클라우드 서비스를 ID 기반 위협 및 공격자로부터 보호하기 위한 제어 기능 배포였습니다. 해당 조직에서는 MFA(다중 요소 인증), 특정 클라우드 응용 프로그램에 대한 조건부 액세스 정책, Office 365 로깅을 채택하였습니다. 향후 유사한 위협으로부터 스스로를 보호하기 위해 조직에서는 엔드포인트 위협 감지 및 대응(EDR) 솔루션을 도입하고 네트워크를 악용하려는 공격자를 감지할 수도 있습니다. 또한 이 조직은 적절한 사용자 인증 정책을 관리 및 시행할 클라우드 거버넌스 기구 또는 글로벌 ID팀을 지정하여 조직 보안 태세를 감독하고 보다 효과적으로 위험을 줄이도록 해야 합니다.

섹션 III

피싱은 여전히 만연

2018년에 Microsoft 위협 분석가들은 공격자들이 선호하는 공격 방법으로 피싱을 계속 사용하고 있는 증거를 발견하였습니다. 피싱은 가까운 미래에도 여전히 문제가 될 것으로 보입니다. 피해자를 유혹하려는 사이버 범죄자의 지속적인 노력 앞에 인간이 내리는 결정과 판단을 포함하기 때문입니다.

피싱 비율은 여전히 증가하고 있습니다.
총 인바운드 피싱 이메일 비율



피싱은 2018년에도 여전히 선호되는 공격 벡터입니다.

Microsoft는 Office 365에서 매월 4700억 건 이상의 이메일 메시지를 분석하고 피싱 및 맬웨어 여부를 보안 검색합니다. 이는 분석자에게 공격자의 추세와 기술에 대한 상당한 인사이트를 제공합니다. 피싱 메시지 인바운드 이메일의 비중이 2018년 1월에서 12월 사이 250% 증가하였습니다. 피싱은 여전히 사용자에게 악성 제로데이 페이로드를 유포하는 데 사용되는 최고의 공격 벡터 중 하나입니다. Microsoft는 계속해서 이러한 공격에 강경하게 대처하고 있습니다. 추가적인 피싱 방지 보호, 감지, 조사 및 응답 기능을 통해 사용자를 안전하게 보호합니다.

▲ **그림 8.**

2018년 피싱 이메일

피싱 공격 방법의 진화

피싱으로부터 사람들을 보호하는 도구와 기술이 더욱 정교해지면서 공격자는 이에 적응할 수 밖에 없습니다. 피싱 공격은 점점 더 다양한 형태를 띠게 되었습니다. 즉, 공격자는 단일 URL, 도메인 또는 IP 주소로 메일을 보내지 않고 공격 지점이 여러 개 있는 다양한 인프라를 사용합니다. 공격의 성격 자체도 진화하여 현대 피싱 캠페인은 단 몇 분만 활성화되는 짧은 스팬 공격에서부터 훨씬 더 길고 규모가 큰 캠페인에 이르기까지 다양합니다. 다른 연속적인 변종 공격에서는 공격자가 며칠 동안 연달아 짧은 양의 메일을 발송합니다.

또한 Microsoft는 공격자들이 호스팅된 인프라와 기타 공용 클라우드 인프라를 사용하는 추세를 관찰하였습니다. 이는 합법적인 사이트 및 자산 사이에 숨어 감지를 더 쉽게 피할 수 있는 방법입니다. 예를 들어 널리 사용되는 문서 공유 및 공동 작업용 사이트 및 서비스를 통해 사용자 자격 증명 도용에 사용되는 악성 페이로드와 가짜 로그인 양식을 배포하는 공격자가 늘어나고 있습니다. 또한 조직 내부와 외부에서 악성 이메일을 추가로 유포하기 위해 손상된 계정을 사용하는 사례가 늘어났습니다.

대상에 따라 다양한 피싱 캠페인

전반적인 악성 코드 배포와 마찬가지로 피싱 캠페인은 표적 공격부터 광범위한 일반 공격까지 다양하게 나타납니다. 매우 정교한 피싱 공격은 계정당 금전적 이득이 더 많이 발생하는 반면 일반적인 공격은 계정당 수익이 적지만 보다 광범위한 사용자를 대상으로 합니다.

정교한 표적 캠페인의 예로는 Ursnif가 있습니다. 이 캠페인에서는 공격자가 문서 파일명을 익숙한 조직 또는 공격 대상이 속한 산업으로 특정합니다. 이러한 공격은 대상이 광범위한 캠페인과는 상당히 다르며 적법성과 신뢰성이 더 높아 보입니다.

2018년에 발생한 광범위한 캠페인 중 일부는 BEC(비즈니스 이메일 손상)과 대상 조직 또는 정교한 스푸핑 캠페인 내에서 알려진 브랜드, 도메인 또는 사용자 사칭과 관련이 있었습니다. 도메인 사칭은 일반적인 공격 전술의 하나로, 해당 이메일이 신뢰할 만 하고 열어봐야 한다고 믿도록 조직을 유인합니다.

피싱 유인의 다양한 형태

Microsoft 연구자들은 캠페인에서 다음과 같은 다양한 유형의 피싱 유인 또는 페이로드가 사용되고 있음을 발견했습니다.

- **도메인 스푸핑** (이메일 메시지 도메인이 원래 도메인 이름과 정확하게 일치하는 경우)
- **도메인 사칭** (이메일 메시지 도메인이 원래 도메인 이름과 유사하게 보이는 경우)[2]
- **사용자 사칭** (이메일 메시지를 신뢰하는 자가 보낸 것처럼 보이는 경우)
- **텍스트 유인** (문자 메시지가 은행, 정부기관 또는 기타 회사처럼 합법적인 출처에서 나온 것으로 보여 내용에 적법성을 부여하고 통상적으로 피해자에게 사용자 이름, 비밀번호 또는 민감한 재무 데이터와 같은 민감한 정보를 제공하도록 요청하는 경우)
- **자격 증명 피싱 링크** (이메일 메시지에 합법적인 사이트의 로그인 페이지와 유사한 페이지에 대한 링크가 있어 사용자가 로그인 자격 증명을 입력하게 되는 경우)
- **피싱 첨부파일** (이메일 메시지에 발신자가 피해자로 하여금 첨부파일을 열어보도록 유인하는 악성 첨부파일이 포함된 경우)
- **가짜 클라우드 저장 위치에 대한 링크** (이메일 메시지가 합법적인 출처에서 발신된 것으로 보이며 가짜 클라우드 저장소 위치에 액세스하는 대가로 사용자가 권한을 부여 및/또는 자격 증명과 같은 개인 정보를 입력하도록 유인하는 경우)

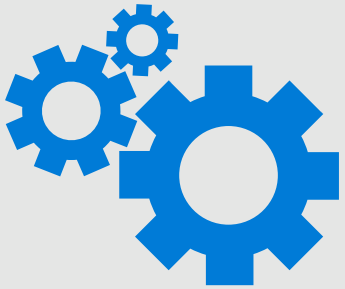
공격자가 사용할 수 있는 이러한 다양한 유인은 조직에서 처리해야 할 피싱 위협의 복잡성을 증가시킵니다.

각주

[2] 도메인 사칭은 도메인이 이메일 표시 이름에 나타나는 경우를 제외하고 도메인 스푸핑(원래 도메인 이름과 정확히 일치)과 유사하게 보일 수 있습니다.

DART를 통한 사이버 인시던트 조사

표적 피싱 인시던트로 타격을 입은 대형 제조업체



한 제조업체는 몇 개월 동안 여러 단계의 피싱 캠페인을 경험했습니다. 이러한 접근법은 흔하지 않습니다. 첫 번째 단계에서는 공격자가 정찰을 수행하고 두 번째 단계에서는 고가치 자산을 공격 대상으로 정합니다. 이 캠페인의 첫 번째 단계에서는 잘 알려진 피싱 사기를 활용하여 조직 내에 있는 소규모 대상 그룹에 보낸 이메일에 포함된 웹 페이지 링크를 기반으로 하였습니다. 해당 이메일에는 대상에게 검토 대기 중인 중요한 전자 문서가 있으며 수신자는 도메인 자격 증명으로 인증을 받아 액세스 해야 한다고 되어 있습니다. 대상이 이른바 '중요 문서'를 검토하도록 설정된 이 가짜 랜딩 페이지는 실제로 자격 증명을 수집하였고 공격자가 전 세계 어디에서든 Office 365 계정에 액세스할 수 있도록 허용하였습니다. 피싱 캠페인의 두 번째 단계는 대상 제조업체 내에 있는 고가치 자산에 유사한 피싱 이메일을 보내 더 중요한 데이터에 액세스하기 위한 것이었습니다. Microsoft는 피싱 캠페인의 두 번째 단계에서 이 클라이언트를 지원하였습니다. 이 인시던트로부터 고객이 얻은 핵심 교훈: 여전히 피싱이 가장 효과적인 공격 방법 중 하나이며 사용자는 가장 취약한 링크입니다. 사용자가 피싱 사기에 주의하도록 교육하고 공격자를 식별하고 행동할 수 있는 도구를 갖추며 정기적으로 시스템을 패치하는 것이 모두 중요합니다. 조직에서 이 중 하나라도 처리하지 않으면 취약해질 수 있습니다.

이 경우 고객의 가장 중요한 관심사는 손상된 계정에 대한 액세스를 즉시 차단해야 한다는 것입니다. Azure Identity 및 Office 365 팀과의 협력 하에 DART는 네트워크에서 침입자를 근절하고 새로 배포된 Microsoft Azure Log Analytics 솔루션을 사용하여 명령 및 제어 채널에 대한 트래픽을 모니터링하는 계획을 수립했습니다. 팀은 불과 3시간 만에 이 상황을 해결할 수 있었습니다. 공격자의 접근이 차단되었고 조직은 피해 평가 및 복구로 관심을 돌릴 수 있었습니다. DART는 Azure Log Analytic 도구를 사용하여 공격자의 행동을 추적하고 조직이 직면한 많은 구성 문제를 발견하도록 하였습니다. 예를 들어 DART는 중요한 서버의 패치에서 갭을 확인하고 인터넷에서 잘 알려진 악성 호스트와 통신하는 네트워크상의 컴퓨터를 발견했으며 맬웨어 방지 기능이 없는 몇 가지 중요한 서버도 파악하였습니다.

섹션 IV

전 세계의 맬웨어

맬웨어는 유용성 손상, 데이터 손실, 지식 재산 도용, 금전적 손실, 정신적 고통 등의 형태로 조직 및 개인에게 위험을 초래하며 심지어 인간의 생명을 위협할 수 있습니다. Microsoft는 다양한 도구 및 기술을 사용하여 발견된 모든 맬웨어 감염을 식별, 차단 및 근절합니다.

맬웨어 발생률은 약 5%에서 2017년에 7% 이상으로 증가했습니다. 2018년 초에 상승세를 보이다가 감소해 연중 대부분 4% 보다 약간 높은 수준에 머물렀습니다. 전반적으로 2018년 맬웨어 발생률이 감소한 몇 가지 잠재적 이유는 Windows 10 채택이 증가하였고 보호를 위해 Windows Defender 사용이 늘었기 때문입니다. 발생률은 Windows Defender Antivirus 실행 중 해당 월에 Defender가 차단한 감염 시도를 포함해 맬웨어가 발생했다고 보고한 컴퓨터의 비율입니다.

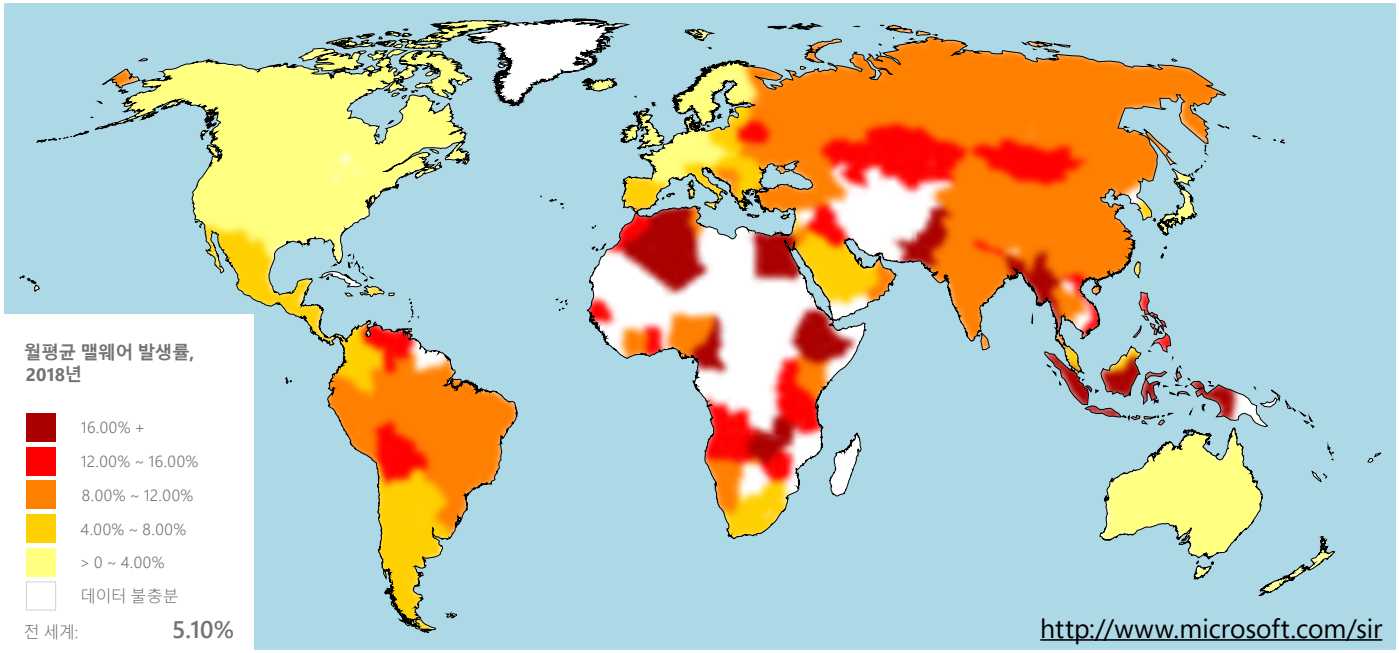


그림 9.

전 세계 월평균 맬웨어 발생률 (국가/지역별, 2018년)

2018년 1월~12월 기간 동안 맬웨어 발생률이 가장 높았던 5개 국가는 에티오피아(26.33), 파키스탄(18.94), 팔레스타인 영토(17.50), 방글라데시(16.95), 인도네시아(16.59)로, 각각 해당 기간 동안 월평균 발생률이 약 16.59% 이상이었습니다. 감염률은 인간 개발 요인 및 사회의 기술 준비성과 상관관계가 높은 경향이 있습니다. 2018년에 가장 높은 발생률을 기록한 모든 지역은 유엔국제전기통신연합(ICT)에서 발표한 2017년 정보통신기술(ICT) 지수에서 국가 및 지역별 하위 40%를 차지하였습니다.

같은 기간에 맬웨어 발생률이 가장 낮았던 국가는 아일랜드(1.26), 일본(1.51), 핀란드(1.74), 노르웨이(1.79), 네덜란드(1.82)로, 각각 해당 기간 동안 월평균 발생률은 1.82% 이하였습니다. 이러한 국가들은 사이버 보안 인프라가 성숙하고 주요 인프라를 보호하고 기본 보안에 관해 시민들과 소통하는 프로그램이 잘 갖춰져 있는 경향이 있습니다.

맬웨어 피해가 가장 심각한 국가의 월평균 발생률

에티오피아: **26.33%**

파키스탄: **18.94%**

팔레스타인 영토: **17.50%**

DART를 통한 사이버 인시던트 조사

여러 금융 서비스 기관에서 민족 국가의 공격으로 운영에 차질

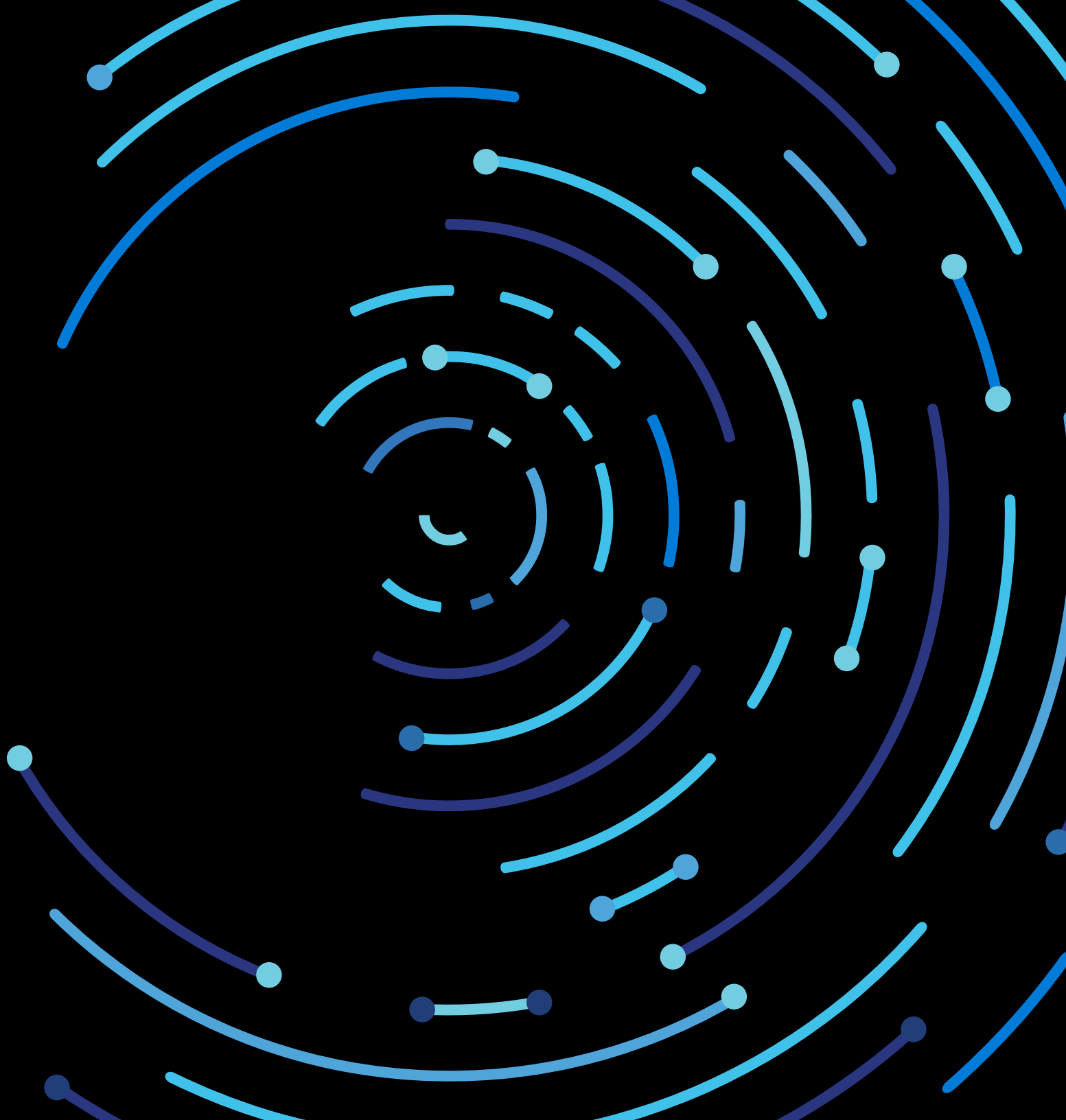
DART가 목격한 더 파괴적인 인시던트에서 여러 금융 서비스 조직들이 국가가 지원하고 작동 방식이 유사한 APT(이전에 언급한 전문 서비스 조직을 대상으로 한 그룹과는 다른 그룹)의 공격 대상이 되었습니다.

이 APT는 스피어 피싱 이메일을 통해 유포된 고도로 표적화 및 난독화된 백도어 임플란트로 기계를 최초 감염시킨 후 관리 액세스를 얻었습니다. 그 후 APT는 다수의 사기 거래를 수행하여 많은 액수의 현금을 외국 은행 계좌로 이체했습니다. 경우에 따라 공격자는 100일 이상 동안 발견되지 않았습니다. 공격자가 감지된 사실을 알게 된 후 공격자는 신속하게 사전 공격을 전개하고 환경에 있는 시스템 절반 이상에 파괴적인 맬웨어를 유포하였으며, 해당 고객의 작업은 며칠 동안 중단되었습니다.

이러한 인시던트로 고객은 몇 가지 핵심 교훈을 얻었습니다. 첫 번째는 시스템의 정기적인 업데이트(운영 체제 및 보안), 패치, 감사를 포함해 소프트웨어 수명주기 관리가 특히 중요하다는 것입니다. 한 예로, 유난히 많은 수의 워크로드가 실행되고 있었던 조직의 Linux 시스템 환경은 전혀 관리가 되지 않아 공격 위험이 매우 높았습니다. 두 번째 교훈은 기본 데이터가 손실될 경우 오프라인 위치에서 시스템 데이터의 백업을 유지하는 것이 중요하다는 것입니다. 또 다른 교훈은 공격 행위에 대해 알아야 할 경우 전통적인 바이러스 백신 솔루션으로는 충분하지 않을 수 있다는 것입니다

정상적인 운영 모드로 복귀하는 것이 이러한 조직의 최우선 과제였습니다. DART는 먼저 피해 상황을 조사하고 감염된 시스템에서 맬웨어를 제거하는 등 필요한 완화 조치를 취한 후 시스템을 정상 상태로 되돌려 서비스 복원을 지원하였습니다. 이 팀은 또한 EDR 등 Microsoft 위협 조사 도구 사용법에 대해 고객 교육을 실시하고 고객들이 네트워크에서 비정상적인 동작 및 공격자 활동을 발견할 수 있도록 하였습니다. DART는 전통적인 바이러스 백신 솔루션으로 감지되지 않는 정교하고 표적화된 공격 방어에 엔드포인트 모니터링이 중요하다고 강조하였습니다.

지침



지침

조직의 복원력 강화와 유의미한 위험 감소를 위해 예방, 감지 및 대응을 포함하는 보안 접근 방식이 필요합니다. 권장 보안 모범 사례 및 제어는 다음과 같은 범주로 구성됩니다.

예방:

예방 제어는 전반적인 방어 전략에서 핵심적인 역할을 합니다. 적절한 투자가 이루어지면 사이버 범죄자의 공격 비용이 증가하고 시간이 경과하더라도 늘어난 공격 비용이 유지되기 때문입니다(산출을 모니터링하고 해석하는 전문 분석가 불필요). 예방 제어 투자는 비용이 낮고 효과적인 공격 기술을 꾸준히 제거하기 위해 최저 비용 기술을 대상으로 해야 합니다.

예방을 위해 고려해야 할 네 가지 사항은 다음과 같습니다.

1. **보안 위생은 매우 중요합니다. 이 보고서에 공유된 일부 사이버 인시던트에서 볼 수 있듯이 일반적인 위생 문제는 고급 보안 기능을 훼손 할 수 있으므로 다음 팁을 따르면 위험을 줄일 수 있습니다.**

- 익숙하지 않은 무료 및/또는 불법 복제된 소프트웨어는 사용하지 않습니다. 신뢰할 수 있는 소스의 소프트웨어만 사용합니다.

- 권한 있는 관리자 계정 보안 조치 등 자격 증명 도용 위험을 완화합니다. 해당 방법에 대해 알아보려면 이 블로그를 읽어보십시오. 당사 보안 태세 안내 및 개선을 위해 Microsoft가 사용하는 몇 가지 원칙과 도구, 사용자의 이니셔티브 계획을 지원하는 규정 로드맵이 간략히 설명됩니다.

- 소프트웨어 판매업체가 제공하는 보안 구성 기준을 적용합니다.

- 운영체제 및 응용 프로그램에 최신 업데이트를 신속하게 적용하여 컴퓨터를 최신 상태로 유지하고 OS, 브라우저 및 이메일에 대한 중요 보안 업데이트를 즉시 배포합니다. 업데이트 또는 패치가 불가능한 컴퓨터는 격리(또는 폐기)합니다.

- 고급 이메일 및 브라우저 보호 기능을 구현합니다. 고급 위협 방지 기능이 있는 보안 이메일 게이트웨이 배포하고 최신 피싱 변종을 방어합니다.

- 호스트 맬웨어 방지 및 네트워크 방어를 사용하여 클라우드에서 실시간에 가까운 차단 대응을 합니다 (솔루션에서 사용 가능한 경우).

2. 액세스 제어를 구현합니다. 다음을 살펴보겠습니다.

- 네트워크 세분화 구현, 최종 사용자로부터 로컬 관리자 권한 제거, 컴퓨터에서 실행 중인 응용 프로그램에 대해 사용 권한을 부여할 때 주의 등 최소 권한 원칙을 적용합니다.
- 신뢰할 수 있는 출처(공식 앱 스토어)의 응용 프로그램으로 다운로드를 제한합니다.
- 사용자가 실행할 수 있는 응용 프로그램 제한을 포함하여 강력한 코드 무결성 정책을 실시합니다. 가능한 경우, 시스템 코어(커널)에서 실행되는 코드를 제한하고 서명되지 않은 스크립트 및 기타 신뢰할 수 없는 코드를 차단할 수 있는 보안 솔루션을 채택합니다. 응용 프로그램 허용 목록을 사용합니다.
- 소프트웨어 공급망 공격과 이러한 공격으로부터 보호하는 방법에 대해 알아보려면 Microsoft 연구자가 작성하는 이 블로그를 읽어 보십시오.

3. 백업을 유지합니다.

- 중요한 시스템과 데이터 파괴 방지 백업을 생성합니다.
- 클라우드 스토리지 서비스를 사용하여 온라인에서 데이터를 자동으로 백업합니다. 온프레미스에 있는 데이터의 경우, 3-2-1 규칙을 사용하여 중요한 데이터를 정기적으로 백업합니다. 데이터 백업 세 개 파일을 두 가지 상이한 스토리지 유형으로 하나 이상의 백업 오프 사이트에 보관합니다.

4. 무엇이든 의심이 든다면 신중하게 행동합니다.

- 직원에게 민감한 정보를 요청하는 의심스러운 커뮤니케이션을 경계하고 어떻게 대응하는지 교육하며 즉시 조직의 보안 운영팀에 보고하도록 지시합니다. 또한 교육은 소셜 엔지니어링과 스피어 피싱 공격 완화에 도움이 될 수 있습니다.
- 웹 링크를 클릭할 때 주의하십시오. 안전한 웹 브라우징 습관을 실천하고 안전하지 않은 사이트에 대한 경고 또는 차단을 제공하는 솔루션을 사용하면 암호화폐 마이닝과 관련된 웹 사이트를 대면할 가능성이 줄어듭니다.
- 컴퓨터가 매우 느리게 실행 되는 경우, 실행 중인 의심스러운 파일을 찾아 언제든지 운영체제 판매업체에 샘플을 제출합니다. 맬웨어 분석을 위해 파일을 https://www.microsoft.com/wdsi/filesubmission에서 Microsoft에 제출할 수 있습니다.

감지 및 대응:

감지 및 대응은 공격자가 리소스에 액세스할 수 있는 시간을 제한함으로써 복원력에 기여합니다. 이로 인해 공격자 비용이 늘어나고 (작업을 재시도하거나 수정해야 함) 수익이 떨어져(목표 달성 확률을 제한) 공격자의 ROI가 줄어듭니다.

비즈니스 조직이 시장 요구를 보다 잘 충족할 수 있는 동일한 클라우드 기술을 사용하면 공격자에 대한 대응을 개선하도록 보안 운영을 수행할 수 있습니다.

그림 10.

SOC의 진화 궤도

보안운영센터(SOC) 진화의 궤적을 살펴보면 기술이 SOC 결정 및 행동의 속도와 품질을 지속적으로 향상시켜왔다는 것을 알 수 있습니다. 이러한 혁신의 대부분은 USAF John Boyd 대령이 기록한 OODA(Observe Orient Decide Act) '루프'의 각 단계에 매핑될 수 있습니다.[3]

관찰 – SOC는 Microsoft 및 기타 소스에서 제공되는 방대한 보안 인텔리전스를 활용하여 조직 및 외부 환경에서 시야를 크게 늘릴 수 있습니다.

지향 - 이 새로운 데이터 소스가 이미 과부하된 SOC에서 사용 가능해짐에 따라 머신 러닝(인공 지능의 하위 집합)이 방대한 데이터 집합을 분석하고 조사할 가치가 있는 문제를 파악하는 데 중요한 도구가 됩니다. 보안 판매업체(Microsoft 포함)는 머신 러닝 기술을 채택하여 이벤트 우선 순위를 빠르게 지정(하고 이러한 개별 이벤트를 전체 인시던트에 통합)합니다.

결정 – 공격량과 복잡성으로 인해 SOC가 빠르게 과부하 걸릴 수 있으므로 분석가와 인시던트 대응자는 경보 및 감지에 대응하여 다양한 의사 결정을 내리고 신속하게 조치해야 합니다. Microsoft와 타 판매업체는 자동화된 조사 기능과 지침을 통합해 분석가가 신속하게 올바른 의사결정을 내릴 수 있도록 있습니다(예: 감염 가능성이 있거나 손상된 디바이스를 격리). 지금은 자동화를 우선순위가 낮은 인시던트의 신속한 해결에 집중시킴으로써 복잡한 문제에 전문기술을 적용할 수 있습니다.

행동 – 대응을 위해서는 다양한 기술과 플랫폼을 신속하고 정확하게 수행해야 합니다. 이것이 바로 보안 조정 및 대응 자동화 기술이 구현하는 바입니다. Microsoft와 여러 기업들이 현대식 위협 감지 및 자동 응답 솔루션을 비롯해 이러한 기술에 지속적으로 투자하고 있습니다.

각주

[3] http://www.militaryhistoryveteran.com/colonel-john-boyd-ooda-loop/

현대식 SOC에 적용되는 몇 가지 다른 동향은 다음과 같습니다.

- **경고 피드의 양 보다 질** – 조직이 '정보 부족' 관리에서 '정보 과다' 관리로 이동함에 따라 고도로 전문화된 SOC 분석가의 시간과 관심이 점점 더 중요해지고 있습니다. 이 때문에 경고의 품질에 대한 요구가 높아져 계층 1 및 계층 2 분석가의 참여가 필요합니다. 추가 데이터 피드는 조사 및 선제적 사냥에 항상 유용하지만 Microsoft의 기업 IT SOC는 분석가 대응이 필요한 경고 피드의 민감도를 측정합니다(현재 90% 이상의 민감도 필요).

- 데이터 중력 – 대규모 데이터 집합(보안 데이터 포함)에 대한 분석은 기본 원시 데이터에 대한 액세스가 없으면 수행하기가 어렵습니다. 더 많은 보안 데이터를 사용할 수 있게 되면 보안 분석을 클라우드에서 수행하는 것이 온프레미스 시스템에서 데이터를 백홀링하는 것보다 경제적이고 실용적입니다. 이는 SIEM 및 SOC 아키텍처의 진화로 이어져 하이브리드 SIEM 접근 방식 또는 서비스로서의 원시 클라우드 SIEM 채택이 포함될 수 있습니다.

- **높은 컨텍스트** – 이러한 유형의 검색은 데이터 집합을 보다 효과적으로 상호 연결할 수 있기 때문에 훨씬 유용합니다. 전통적인 네트워크 트래픽 기반 감지는 여전히 보안상 가치가 있지만, 원시 네트워크 트래픽은 일반적으로 합법적인 활동과 비정상적인 활동을 구별하기 위한 컨텍스트가 부족합니다. SOC는 다음과 같이 컨텍스트가 풍부한 감지에서 훨씬 더 많은 가치가 있는 것으로 보입니다.

  - **EDR(엔드포인트 감지 및 대응)** 솔루션. 호스트 활동에 대한 심층적인 컨텍스트를 보유합니다.
  - ID 기반 감지. 일반 사용자 인증 패턴(위치, 시간, 액세스된 서비스 등)에 대한 인사이트를 포함하고 행동 분석을 적용합니다.

이러한 컨텍스트가 풍부한 감지는 (IP 트래픽의 몇 가지 기술 특성에 비해) 훨씬 복잡한 작업을 모방해야 하기 때문에 공격자가 피해가기가 더 어렵습니다.

고객에 대한 중대한 침입으로부터 배운 또 다른 교훈은 IT 기능이 부분적으로 또는 완전히 아웃소싱될 때 인시던트에 신속하게 대응하는 것이 어렵다는 것입니다. IT 아웃소싱 계약 및 서비스 수준 계약(SLA) 뿐만 아니라 공급망 판매업체를 검토하여 신속한 보안 대응과 호환되는지 확인하는 것이 좋습니다. 고객 인시던트 조사에 대한 자세한 내용은 https://aka.ms/IRRG에 있는 인시던트 대응 참조 가이드(IRRG)를 참조하십시오.

데이터 원본

데이터 원본

Microsoft는 Microsoft 보안 인텔리전스 보고서에 포함된 데이터를 다양한 Microsoft 제품 및 서비스를 제공하는 과정에서 수집하였고 이는 Microsoft 개인정보처리방침에 명시되어 있습니다. 이 데이터는 Microsoft 제품 및 서비스의 보안과 운영에 대한 중요한 정보는 물론 사이버 보안 위협 환경에 대한 인사이트를 제공합니다. 이 데이터에는 다음 소스의 분석이 포함됩니다.[4]

- **Azure Security Center**는 클라우드 워크로드의 보안에 대한 가시성을 높이고 고급 분석 및 위협 정보를 사용하여 공격을 감지함으로써 조직이 위협을 예방, 탐지 및 대응할 수 있도록 돕는 서비스입니다.
- **Bing**은 악성 콘텐츠를 찾기 위해 수십억 개의 웹 페이지 검색을 수행하는 검색 및 의사결정 엔진입니다. 그러한 콘텐츠가 검색된 후 Bing은 감염을 방지하기 위해 사용자에게 경고를 표시합니다.
- **Exchange Online**은 Microsoft에서 호스팅하는 이메일 및 생산성 서비스입니다. Exchange Online 맬웨어 방지 및 스팸 방지 서비스는 스팸 및 맬웨어를 식별하고 차단하기 위해 매년 수십억 개의 메시지를 검사합니다.
- **MSRT(Microsoft 소프트웨어 제거 도구)**는 Microsoft가 고객 컴퓨터에 널리 퍼진 특정 맬웨어 패밀리를 식별하고 제거하도록 설계된 무료 도구입니다. MSRT는 주로 Windows 업데이트, Microsoft 업데이트 및 자동 업데이트를 통해 중요 업데이트로 배포됩니다. 이 도구의 버전은 Microsoft 다운로드 센터에서도 제공됩니다. MSRT는 최신 실시간 바이러스 백신 솔루션을 대체할 수 없습니다.
- **Microsoft 안전 스캐너**는 주문형 검색을 제공하고 맬웨어 및 기타 악성 소프트웨어를 제거하는 데 도움이 되는 무료 다운로드 보안 도구입니다. Microsoft 안전 스캐너는 실시간 보호 기능을 제공하지 않으며 컴퓨터가 감염되는 것을 방지할 수 없기 때문에 최신 바이러스 백신 솔루션을 대체할 수 없습니다.

각주

[4]특히 이 데이터는 보안을 위해 사용되기 전 항상 엄격한 개인정보보호 및 규정 준수 여부가 검토됩니다.

- **Microsoft Security Essentials**은 무료로 쉽게 다운로드가 가능한 실시간 보호 제품으로, Windows Vista 및 Windows 7에 대한 기본적이고 효과적인 바이러스 방지 및 스파이웨어 방지 기능을 제공합니다.

- **Microsoft System Center Endpoint Protection**(구, Forefront Client Security and Forefront Endpoint Protection)는 엔터프라이즈 데스크톱, 노트북, 서버 운영 체제에서 맬웨어 및 원치 않는 소프트웨어로부터 보호를 제공하는 통합 제품입니다. Microsoft Malware Protection Engine 및 Microsoft 바이러스 백신 서명 데이터베이스를 사용하여 실시간, 예약, 온디맨드 보호 기능을 제공합니다.

- **Office 365**는 조직과 가정 사용자를 위한 Microsoft Office 구독 서비스입니다. 구독 계획 선택에는 Office 365 Advanced Threat Protection에 대한 액세스가 포함됩니다.

- Windows 10의 Windows Security는 맬웨어 및 원치 않는 소프트웨어를 실시간으로 검색하고 제거하는 기능을 제공합니다. 또한 최신 버전의 Windows는 컴퓨터 구성, 디바이스 성능 및 상태 등의 다양한 컨텍스트 데이터와 기타 정보를 활용하여 고객의 보안을 강화합니다. 또한 Microsoft는 고객이 Windows 10에서 자신의 개인정보에 관해 더 많은 정보를 얻도록 합니다. Microsoft가 수행하는 몇 가지 방법에 대해 알아보려면 이 블로그를 읽어보십시오.

- **Windows Defender Advanced Threat Protection**은 Windows 10주년 업데이트 이후 버전에 기본 제공되는 서비스로, 엔터프라이즈 고객은 네트워크에서 정교하고 지속적인 위협과 데이터 유출을 감지, 조사, 해결할 수 있습니다.

- **Windows Defender Offline**은 부팅 가능한 CD, DVD 또는 USB 플래시 드라이브를 만드는 데 사용할 수 있는 다운로드 가능한 도구로, 컴퓨터에서 맬웨어 및 기타 위협을 검색합니다. 실시간 보호 기능을 제공하지 않으며 최신 맬웨어 방지 솔루션을 대체할 수 없습니다.

- **Windows Defender SmartScreen**은 Microsoft Edge 및 Internet Explorer의 한 기능으로, 피싱 사이트 및 맬웨어 호스팅 사이트에 대한 사용자 보호 기능을 제공합니다. Microsoft는 Microsoft Edge, Internet Explorer 및 기타 Microsoft 제품 및 서비스 사용자가 보고한 피싱 및 맬웨어 사이트 데이터베이스를 유지 관리합니다. 사용자가 필터를 사용하도록 설정한 상태에서 데이터베이스의 사이트 방문을 시도하면 브라우저에 경고가 표시되고 페이지 탐색이 차단됩니다.