백서

2023년 사이버 위협 전망

FortiGuard Labs 전망

네트워크 및 보안 통합에는 "소소익선"이 핵심 전략으로 통하는 반면, "다다익선"은 사이버범죄자들이 의지하는 주문이 된 것처럼 보입니다.

사이버 위협 동향을 살펴본 결과 가장 문제가 되는 추세는 모든 종류의 위협이 점점 더 장소를 가리지 않고 나타나는 현상이 앞으로도 지속될 것으로 보인다는 것입니다. RaaS(서비스형 랜섬웨어)에서 엣지 디바이스 같은 새로운 목표에 대한 새로운 형태의 공격은 물론 점차 증가하고 있는 삭제 도구의 사용에 이르기까지, 사이버 위협의 종류와 양은 2023년 이후에도 보안 팀을 애타게 만들 전망입니다.

2022년도 전망 되돌아보기

작년에 FortiGuard Labs에서 전망했던 것들 가운데에는 공격 전 활동에 더욱 노력을 쏟는 공격자에서 운영 기술에 영향을 주는 공격 시도의 양적 증가부터 위협 동향이 어떻게 진화할지에 관한 내용이 몇 가지 있었습니다. 이때의 전망이 얼마나 정확했었는지와 2023년을 준비하며 이러한 위협이 어떻게 발전할 것으로 전망했는지를 확인해 봅니다.

지능적이고 지속적인 사이버 범죄의 증가

FortiGuard Labs에서는 새로운 취약성의 증가와 아울러 CaaS(서비스형 범죄)로서의 성장 일로를 걷고 있는 공격자들이 "수면 아래" 공작 또는 공격 전 정찰 및 무기화라 할 수 있는 작업을 더욱 많이 할 것으로 전망했습니다. 2022년 상반기에만 해도 FortiGuard Labs에서 식별한 새로운 변형 랜섬웨어의 수가 이전 6개월에 비해 거의 100% 증가하여 2021년 하반기의 5,400건에 비해 2022년 상반기에는 10,666개의 새로운 변형 랜섬웨어를 기록한 바 있습니다.

이렇게 새로운 변형 랜섬웨어가 폭증한 배경에는 다크웹의 RaaS가 점점 많은 이용자를 보유하게 된 것이 일차적 원인일 수 있습니다. 맞는 말입니다. 스트리밍 미디어나 음식 배달 앱과 마찬가지로 사이버 범죄 조직에서도 구독 모델 서비스를 활용하고 플러그-앤-플레이 방식의 랜섬웨어를 구매해 빠르게 돈을 뜯어내려 할 것이라 예상합니다. 피해자에게 압박을 가중하기 위해 RaaS 운영자는 자신들의 요구가 이루어지지 않을 경우에 훔친 데이터를 다크웹에 유포하겠다는 위협을 하는 경우가 많습니다.

지금까지 파악된 변형 랜섬웨어의 수가 RaaS를 주요 원인으로 하여 폭증하는 동안 랜섬웨어에 지급된 비용도 따라 오르고 있습니다. 미국 금융 범죄 단속 네트워크의 발표에 따르면 기업에서 2021년 상반기에 랜섬웨어에 지불한 금액은 거의 6억 달러에 이르며 이는 미국에서 지난 10년간 지불된 총액을 1년 만에 넘어서는 것입니다.[1] 최근 설문에 따르면 응답자의 72%는 랜섬웨어 정책이 준비되어 있으며 이들 중 49%에서는 무방비로 랜섬을 지불하는 것이 그 절차입니다.[2]

이제 FortiGuard Labs에서는 2023년이 되면 CaaS 시장이 현저히 커지는 가운데 새로운 취약점 공격, 서비스, 체계적 프로그램이 구독 모델을 통해 위협 행위자 측에 곧바로 제공될 것이라 전망합니다.

내 환경을 지키는 방법

우리 모두는 이미 CaaS의 성장이 공격량의 증가에 기여하고 있음을 확인하고 있습니다. 이제 기업에서는 공격을 당하는 것이 더 이상 "가능성"의 문제가 아닌 "시점"의 문제로 봐야 합니다. 표준 보안 도구의 범주에 들어가는 EDR 기술, MITRE ATT&CK 매핑으로 강화된 샌드박스 솔루션, AI 탐지 시그니처를 활용한 멀웨어 대비 엔진, 지능형 IPS(침입 방지 시스템) 탐지, NGFW는 이렇게 늘어가는 사이버 위협에 대처하기 위해 확장이 가능한 상태여야 합니다. 기업이 공격당하기 전에 이러한 공격을 저지하는 데에는 침입당한 자격 증명을 판매용으로 내어놓는 등의 다크 웹 활동을 감시하는 새로운 정찰 도구 및 서비스가 필수적입니다. 이상적인 것은 통합 솔루션으로서 위협을 관측하고 나누고 상관관계를 파악하여 대응할 수 있는 통합 보안 플랫폼을 통해 이러한 기술을 데이터 센터에서 지사에 이르기까지 어느 기업의 운영 범위에 포함되는 모든 영역에 배포하는 것입니다. 최종적으로는 디코이 등의 기만 기술을 사용하는 것이 안전한 인프라를 개발하고 킬체인 초기에 공격자 활동을 탐지하는 데 있어 필수적입니다.

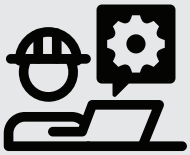
엣지 공격의 주류화

OT 시스템이나 위성 기반 인터넷 네트워크 같은 엣지 기기는 한때는 실력 있는 공격자들에게 비전통적인(따라서 인기가 없던) 목표였습니다. 하지만 지난 10년이 지나는 동안 이러한 목표에 대한 사이버 공격의 시도가 질적 및 양적 측면에서 늘고 있음을 목격했습니다. IT 네트워크와 OT 네트워크 간 융합이 거의 동일한 수준까지 이르게 되면서 공격자들이 침입당한 홈 네트워크와 원격 작업자 기기를 통해 OT 시스템에 액세스하는 일이 더욱 수월해졌습니다. 게다가 현재 포티넷 2022 운영 기술 상태 및 사이버 보안 보고서에 따르면, 93%의 기업이 지난 12개월간 자신들의 OT 인프라를 노리고 자행된 공격을 경험한 적이 있으며 이들 가운데 83%는 이러한 공격을 세 건 이상 경험했습니다.[3]

작년에 FortiGuard Labs에서는 위협을 가하는 측에서 목표 엣지 환경에 대해 EAT(엣지 액세스 트로이 목마)를 이용하는 경우가 증가할 것으로 전망했고, 이러한 사례를 몇 건 확인했습니다. FortiGuard Labs에서 확인한 이러한 사례 가운데 하나는 2022년 3월에 있었던 것으로 StartPage라고 하는 일반적인 트로이 목마입니다. 이것은 프라우저의 홈페이지를 변경하여 광고를 표시하도록 하거나 잘못된 경로로 유도하는 애플리케이션이나 악의적인 애플리케이션을 홍보하거나 공격 당한 브라우저를 악용하여 위협을 실행하도록 합니다. 이것은 OT 기기에 대한 멀웨어 전달을 전 세계적으로 증가시킵니다.

FortiGuard Labs에서는 위성 기반 인터넷 네트워크 역시 사이버 범죄자의 새로운 목표가 될 것이라 전망했습니다. 이러한 네트워크의 크기나 규모가 계속해서 성장하는 만큼 공격 시도 역시 늘어나고 있습니다. 올해 초에는 해커들이 AcidRain이라고 하는 새로운 파괴적 삭제 도구 멀웨어를 사용하여 위성 통신 회사의 인프라를 공격하는 일이 우크라이나에서 벌어져 유럽 일대의 위성 기반 인터넷 연결에 영향을 미쳤습니다. 이 공격으로 인해 독일에서도 거의 6천 기에 이르는 풍력발전 터빈이 위성 연결에 침입을 당해 오프라인 상태가 되어 제어를 못 하게 되기도 했습니다. FortiGuard Labs에서는 이러한 형태의 위성 기반 공격이 계속될 것이라 예상하는 가운데 가장 큰 목표는 크루즈나 화물선, 항공사, 유정 및 가스정과 파이프라인, 원격 현장 사무소와 같이 지연이 적은 활동을 지원하기 위해 위성 기반 연결에 의지하는 기업이 될 것이라고 보고 있습니다.

사이버 범죄자들이 엣지 기기를 공격하려고 하는 동기는 간단합니다. OT 시스템이나 위성 기반 네트워크 같은 목표는 공격자들에게 기업 환경에 진입할 수 있는 새로운 진입 지점을 제공하기 때문입니다. 네트워크 엣지의 증가란 LOtL(자급자족형) 위협이 숨을 만한 장소가 많아진다는 의미도 되며, 이에 따라 공격자들은 자신들의 악의적 활동을 정상적 네트워크 활동으로 가장해 탐지되지 않을 수 있게 됩니다.



내 환경을 지키는 방법

OT 및 엣지 시스템은 공격자들에게 있어 상당히 매력적인 목표이며 앞으로도 매력적인 목표일 것입니다. 많은 공격자들이 용도에 맞게 빌드된 도구를 이용해 이러한 시스템을 노리지만 IT 플랫폼을 노리던 공격 시도가 OT에 손상을 입히게 되는 경우도 있습니다. 이렇게 공격당한 IT 시스템은 이제 OT 플랫폼을 감시하고 제어하는 데 사용됩니다. OT를 제대로 방어하려면 IT도 함께 지켜야 합니다. 보안은 반드시 제로데이부터 IT/OT 융합 전략의 일부로 구성되어 있어야 합니다.

보안 팀의 책임자들이 자신들의 OT/IT 환경을 확실히 지키기 위해 취할 수 있는 기본적인 몇 가지 단계가 있습니다. 모범 사례에는 네트워크 매핑 및 연결성 분석 실행, 의심스러운 활동 탐지, 제로 트러스트 프레임워크의 구현, 올바른 원격 액세스 도구의 정렬, 강력한 IAM(ID 및 액세스 관리) 전략의 실행이 포함되어 있습니다.

랜섬웨어와 삭제 도구의 기승

랜섬웨어는 점점 악랄해지고 비용도 계속해서 높아집니다. 포티넷에서 실시한 세계 랜섬웨어 설문조사에 따르면 67%의 기업에서 랜섬웨어로 인한 공격을 겪고 있다고 답했습니다.[4] 더욱 우려스럽게도, 거의 절반의 기업이 한 번 이상 목표가 되었고 1/6의 기업은 세 번 이상 공격을 당했다고 답했습니다.[5]

2021년에는 공격자들이 삭제 도구 멀웨어를 자신들의 랜섬웨어 공격에 추가하여 비용을 올리려고 하는 초기 징후를 처음으로 확인했습니다. 10년 전에 처음으로 확인된 삭제 도구 멀웨어는 사이버 범죄자들에게 데이터를 삭제하여 랜섬 요구를 들어주지 않으면 OT나 제조 장비 및 서버 같은 중요 시스템 가용성을 무력화할 수 있도록 합니다. FortiGuard Labs에서 확인한 다양한 공격 방법과 APT(지능형 지속 공격) 간 융합의 수준으로 미루어 보면 더욱 많은 수의 랜섬웨어 공격이 삭제 도구 멀웨어 같은 보다 파괴적인 기능과 합쳐질 것이라 예상됩니다.

올해 우크라이나에서 벌어진 전쟁은 중요 인프라를 먼저 노리는 위협 행위자들 사이에 디스크 삭제 멀웨어의 증가를 크게 부채질했습니다. FortiGuard Labs에서는 2022년 상반기 여섯 달 동안 정부, 군사 시설, 민간 기업을 상대로 한 다양한 공격 캠페인에서 사용되었던 최소 일곱 종류의 변종 주요 삭제 도구를 새로 확인했습니다. 이는 2012년 이래 10년 동안 공개적으로 발견된 변종 삭제 도구의 수를 모두 합친 것과 비슷하다는 점에서 상당한 수입니다. 게다가 이러한 삭제 도구는 특정 지역에서 집중적으로 포착된 것이 아니라 우크라이나 이외에도 24개국에서 발견되었습니다.

삭제 도구 멀웨어의 추세는 공격 기술이 점점 더 파괴적이면서도 정교해지는 불편한 진화가 일어나고 있음을 보여줍니다. 삭제 도구 멀웨어가 점점 만연하는 것은 이렇게 무기화된 페이로드가 나중에는 단일 목표나 지역에 머무르지 않고 다른 사이버 범죄와 합쳐지는 형태로 이용될 가능성이 있음을 보여줍니다. 랜섬웨어에 결합된 삭제 도구 멀웨어는 피해자들에게서 돈을 갈취하려는 범죄자들이 그 금액을 올릴 수 있는 악랄하고 새로운 조합으로 나타날 것입니다.

내 환경을 지키는 방법

이러한 삭제 도구 멀웨어의 영향을 최소화하기 위해 기업에서 시행해야 하는 몇 가지 모범 사례들이 있습니다. 인라인 샌드박스를 사용하는 것은 랜섬웨어와 삭제 도구 멀웨어로부터의 보호를 위한 출발점으로 탁월합니다. 이렇게 하면 무해한 파일만 엔드포인트에 전달됩니다. 백업을 가능한 상태로 두는 것 역시 중요한 조치입니다. 단, 멀웨어가 컴퓨터상의 백업(Windows Shadow Copy 등)이나 네트워크를 파괴하기 위해 적극적으로 검색하는 경우도 적지 않습니다. 그러므로 백업은 반드시 사이트 외부, 오프라인에 보관해야 정교한 공격에서도 살아남을 수 있습니다. 적절한 네트워크 세그멘테이션도 도움이 됩니다. 공격이 발생했을 때 세그멘테이션은 발생한 인시던트를 네트워크 내의 일부 구역에 격리할 수 있습니다. 유비무환의 자세로 기울인 노력이 데이터 손실을 성공적으로 저지하느냐 데이터를 완전히 파괴당하느냐의 기로에서 차이점을 만들어 내는 경우가 많기 때문에 재해 복구 및 인시던트 대응 플랜을 구비하도록 합니다.

마지막으로, 항상 시스템을 패치합니다. 성공적인 공격은 대부분 패치가 준비된 부분의 취약성을 노리고 자행됩니다. 사이버 위생과 관련된 모범적 업무 처리는 악의적인 공격이 알려진 취약성을 노리고 있을 때 그 값어치를 톡톡히 할 것입니다.

인공지능의 무기화

AI는 일반적으로 봇넷에 의한 공격으로 의심할 수 있는 비정상적인 IoT 행위를 탐지하기 위한 방어적 목적으로 이미 사용되고 있습니다. 그리고 FortiGuard Labs에서 전망한 것처럼 사이버 범죄자들도 점차 AI를 이용해 다양한 악의적 활동을 보조하기 시작했는데 이러한 활동은 비정상 네트워크 활동을 탐지하는 알고리즘을 차단하는 것에서 인간의 행동을 모방하는 것까지 다양합니다.

공격자들이 AI를 무기화하는 일례가 딥페이크의 개발입니다. "딥페이크"라는 말이 처음 사용된 것은 5년 전입니다. 이러한 공격 벡터는 점점 더 많은 걱정을 낳습니다. 딥페이크를 만드는 데에는 몇 가지 방법이 있고 그 기술은 빠르게 향상되고 있습니다. 가장 유명한 방법 가운데 하나는 GAN(생성적 적대 신경망)을 이용하는 것으로 가짜 이미지를 생성하는 데에도 사용할 수 있는 알고리즘을 이용해 패턴을 인식하도록 AI가 스스로를 학습시키는 것입니다. 다른 방법으로는 안면 대체 및 안면 교체 기술에 이용되는 인코더라고 하는 AI 알고리즘을 이용하는 것입니다. 디코더는 얼굴 이미지를 가져와 교체함으로써 어떤 사람의 얼굴을 완전히 다른 사람의 신체에 합성할 수 있게 만듭니다.

NVIDIA가 컴퓨터에서 생성한 영상을 이용하여 CEO인 Jensen Huang이 주방에서 기자회견을 하는 것 같은 모습을 연출하는 것과 같이 작년에 헤드라인을 장식했던 다양한 딥페이크 예시들은 사이버 범죄자들이 중요한 정보를 훔치기 위해 만든 것들은 아니었습니다. 하지만 딥페이크에는 분명히 보안 팀과 그들이 속한 기업이 고려해야 할 위협 벡터로서의 또 다른 가능성이 내재합니다. FortiGuard Labs에서는 이미 해커들이 이러한 전략을 사용해 범죄 행위를 지원하는 몇 가지 사례를 확인하고 있습니다.

내 환경을 지키는 방법

웹 필터링, 안티바이러스 소프트웨어, EDR 기술은 모두 무기화된 AI로부터 기업을 지키는 역할을 수행합니다. 하지만 AI 관련 공격을 가장 효과적으로 방어하는 방법 가운데 한 가지는 사이버 보안 경각심 교육입니다. 수많은 기업이 직원들에게 기본적인 보안 교육 프로그램을 운영하지만, 기업은 AI에 초점을 맞춘 위협을 콕 집어 교육하는 새로운 모듈을 추가하는 것도 고려해야 합니다. 예를 들어 딥페이크에 관한 세션에서는 눈의 움직임이 부자연스럽다거나, 눈을 깜빡이지 않는다거나, 얼굴 위치가 일정하지 않다거나 하는 등의 딥페이크 동영상을 식별하는 팁을 제공할 수 있습니다.

암호 화폐 도난

은행 거래와 이체가 사이버 범죄자들의 주요 표적이던 때가 있었습니다. 하지만 은행들이 거래를 암호화하고 MFA(다단계 인증)를 요구하는 등 점차 보안 수단을 개선하면서 이제는 해커들이 이런 거래를 가로채기가 점점 쉽지 않게 되었습니다. 그러나 "닫히는 문이 있으면 열리는 문도 있는 법"입니다. FortiGuard Labs에서는 전에 예측했던 것처럼 보관 중인 암호 자격 증명을 노려 디지털 지갑을 빼내기 위해 설계된 멀웨어 관련 인스턴스를 더 많이 목격했습니다. 디지털 지갑은 보안이 허술한 경향이 있어 해커들에게 쉬운 먹잇감이 됩니다.

FortiGuard Labs에서는 2022년에 일어난 주요 NFT(대체 불가능 토큰) 해킹의 수많은 사례를 들 수 있습니다. 2월에는 공격자들이 OpenSea 사용자들에 대한 피싱 공격을 감행하여 NFT로 170만 달러를 훔치는 일이 있었습니다. 그로부터 불과 몇 달 뒤에는 해커들이 Premint 사용자들에게서 NFT 40만 달러를 훔치는 데 성공하기도 했습니다. 유명한 소셜 플랫폼인 Discord에서 일어난 몇 건의 NFT 해킹은 뉴스로 보도되기도 했습니다. 즉, 이러한 블록체인의 취약성과 이를 추가적으로 악용하는 행위는 아직 널리 퍼지지 않은 것뿐이라는 의미로 암호화폐 시장에 더욱 회의감을 주고 있습니다.

내 환경을 지키는 방법

암호 지갑을 안전하게 지키는 일은 소유자에게서 시작됩니다. 비 수탁형 지갑을 쓰는 것은 암호화폐 사용자에게 개인 키를 통해 자신이 보유한 화폐의 소유권과 제어를 확보할 수 있다는 점에서 바람직합니다. 수탁형 지갑이나 타인이 지갑을 소유하는 방식은 사용자가 자신의 지갑을 온전히 제어하지 못한다는 점에서 위험성이 더 큽니다.

2023년에 주의해야 할 새로운 공격 양상

해커들이 검증된 특정 공격 방식 몇 가지, 그중에서도 특히 실행하기 쉬우면서 빠르게 돈을 갈취할 수 있도록 해 주는 방식에 계속해서 의존할 것이란 사실은 누구나 알고 있습니다. 하지만 저희 FortiGuard Labs 팀에서는 2023년에 나타날 분명하고 새로운 공격 양상 몇 가지를 전망합니다. 아래의 내용들은 내년 한 해 동안 FortiGuard Labs에서 지켜볼 독특한 보안 공격 발전상 가운데 일부입니다.

새로운 CaaS 제품

RaaS를 통해 사이버 범죄자들이 톡톡히 재미를 보아왔음을 생각하면 추가적인 공격 벡터가 다크웹을 통해 서비스로 제공되는 경우가 늘어날 것으로 전망합니다. 랜섬웨어와 기타 MaaS(서비스형 멀웨어) 제품의 판매에 더해 FortiGuard Labs에서는 새로운 범죄용 솔루션을 주목하기 시작하는 동시에 미리 침입당한 목표에 대한 액세스 권한을 판매하는 사례의 증가도 확인할 것입니다.

CaaS는 위협을 가하는 측에게는 매력적인 비즈니스 모델이 될 수 있습니다. 저희는 더욱 많은 턴키 형, 구독 기반 제품이 위협 행위자들에게 제공될 것으로 전망합니다. 이러한 새로운 모델을 통해 수준이 다양한 사이버 범죄자들이 자신만의 계획을 세우느라 시간과 자원을 투자하는 일 없이도 보다 정교한 공격을 펼칠 수 있게 될 것입니다. 또한, 실력 있는 사이버 범죄자라면 "서비스형" 공격 포트폴리오를 제작해 판매함으로써 간단하고 빠르게 반복적인 수익을 낼 수 있습니다.

결국, 2023년 이후 새롭게 등장할 CaaS 포트폴리오의 확장에 대비해야 합니다. 또한, FortiGuard Labs에서는 위협 행위자들이 딥페이크 등의 새로운 공격 벡터를 이용하기 시작하면서 이러한 영상과 음성 및 관련 알고리즘을 더욱 폭 넓게 판매할 것이라 예상합니다. 위협 행위자들이 유명 인사와 공직자를 노리는 수준을 넘어서서 인플루언서, 특히 디지털 존재감이 뚜렷한 인플루언서까지로 범위를 확장할 것으로 전망합니다. 이렇게 넓은 범위에 그물을 던져 놓으면 사칭을 통해 팬들이 의심 없이 허위 상품을 "구매"하는 등의 행위를 하도록 유도할 기회가 사이버 범죄자들에게는 더 많아집니다.

딥페이크뿐만 아니라 RaaS(서비스형 정찰) 역시 더욱 많이 사용될 것으로 예측됩니다. 공격이 대상을 특정하는 경우가 많아지면서 위협 행위자들이 다크웹에서 "탐정"을 고용해 공격을 시작하기 전에 지정된 목표에 대한 정보를 얻을 가능성이 큽니다. 사설탐정을 고용해 얻을 수 있는 인사이트와 마찬가지로 RaaS 제품 역시 목표 기업의 보안 스키마, 핵심 보안 요원, 보유 서버의 수, 알려진 외부 취약점, 심지어는 침입당한 자격 증명 중에 이미 상품으로 판매되는 내용 등과 같은 공격 청사진을 제공하여 사이버 범죄자가 세심하게 지정된 목표에 대해 효과적인 공격을 진행하도록 할 수 있습니다.

자동화를 통해 더욱 빨라진 자금 세탁

그 리더와 협력 프로그램에서는 범죄 조직을 키우기 위해 보통 송금책을 운용합니다. 송금책은 알게 모르게 범죄 조직을 대신해 자금 세탁을 돕는 데 이용됩니다. 송금책은 광고를 통해 뽑는 경우가 많고 익명으로 어느 나라나 은행 계좌에서 다른 곳으로 돈을 옮길 때 이용됩니다. 이런 식의 돈 섞기는 무기명 계좌 이체 서비스나 암호화폐 거래를 통해 탐지를 피하는 식으로 이루어지는 게 일반적입니다. 자신이 송금책인지도 모르는 송금책을 거래에 이용하고 돈을 물리적으로 재배치하면 디지털 흔적을 남기는 일을 피할 수 있기 때문에 여전히 이런 방식은 흔히 사용됩니다. 돈은 소액으로 분할되어 다양한 채널을 통해 이체되는 방식으로 돈세탁 방지법을 통해 필연적으로 경보가 발령되는 일을 회피하는 경우가 많습니다.

송금책을 모집하는 일은 일을 합법적으로 보이도록 하고 제대로 송금책을 모집하며 법망을 피할 수 있도록 가짜 기업 웹사이트를 제작하고 수금책의 계정을 비롯한 후속 작업 목록을 작성하는 등 사이버 범죄 조직의 리더에게 있어서는 예전부터 시간이 오래 걸리던 프로세스였습니다. FortiGuard Labs에서는 사이버 범죄자들이 이러한 송금책을 물색하는 데 머신러닝을 이용해 잠재적인 대상을 더 잘 식별하면서도 시간은 덜 들이기 시작할 것으로 예상합니다.

또한 FortiGuard Labs에서는 수동으로 이루어지던 송금책 업무를 자동화된 서비스가 대신하여 다단계의 암호화폐 거래를 통해 돈을 옮김으로써 프로세스 시간은 줄이고 추적은 더욱 어렵게 만들 것으로 전망합니다. 코인세탁소에서 세탁기에 동전을 추가하는 것처럼 사이버 범죄자는 요금을 결제하여 자동화된 캠페인을 시작하면서 수동 작업 소요를 줄이거나 아예 프로세스에서 배제할 수 있게 될 것입니다.

서비스형 돈세탁도 머지않은 일임이 분명합니다. 이러한 형태는 성장 중인 CaaS 포트폴리오에서 재빠르게 한 부분을 차지하게 될 것입니다. 동시에, 이러한 형태의 사이버 범죄의 표적이 될 개인이나 기업에서는 자동화로 옮겨가는 것이 곧 돈세탁을 추적하기 어렵게 만들어 잃어버린 돈을 찾을 기회가 낮아짐을 의미합니다.

새로운 사이버 범죄의 조류를 반기는 가상 도시

메타버스는 온라인 세계에서의 새롭고 완전한 몰입 경험을 창출하고 있으며 AR(증강현실), VR(가상현실), MR(혼합현실) 기술을 통해 펼쳐지는 새로운 인터넷에 처음 뛰어드는 도전자들 가운데는 도시들이 있습니다. 두바이를 필두로 하는 이러한 가상 도시들은 현실 세계의 경험과 장소를 고스란히 옮겨 놓을 것을 약속하고 있습니다. 사람들은 가상 공간에 작업이나 오락, 쇼핑 등을 할 수 있는 아바타를 만들 수 있습니다. 리테일 업계들은 이러한 가상 세계에서 구매할 수 있는 디지털 상품을 출시하고 있습니다. 작년 말에 디자이너인 랄프 로렌은 온라인 게임 플랫폼인 Roblox에 독점 디지털 의류 컬렉션을 출시하기도 했습니다.

하지만 이렇게 새로운 온라인상의 목적지들이 가능성의 세계를 열어나가는 동안 사이버 범죄와 관련해 전례 없는 증가도 함께 이루어졌습니다. 어떤 개인의 아바타는 필연적으로 그 아바타의 소유자에 대한 개인 식별 정보(PII)로 이어지는 통로일 수밖에 없음을 생각해 본다면 공격자들은 아바타를 주요 목표로 삼게 될 것입니다. 개인이 가상 도시에서 재화와 물건을 구입할 수 있기 때문에 디지털 지갑, 암호화폐 거래, NFT를 비롯한 어떤 거래 수단이라도 위협 행위자들에게는 또 하나의 공격면을 제공하는 셈입니다. 이러한 가상 재화나 자산은 도난도 재판매도 모두 가능합니다. 가상 도시의 AR 및 VR 기반 요소로 인해 생체 정보 해킹 역시 일어날 가능성이 있으며 이에 따라 사이버 범죄자들이 지문 매핑, 안면 인식 데이터, 홍채 스캔 정보를 갈취하기가 더욱 쉬워져서 결국에는 이런 것들을 악의적인 목적에 사용할 수 있게 됩니다.

기나긴 공방전

FortiGuard Labs에서는 특정한 신기술들이 사이버 범죄자들에게 새로운 침입 기회를 제공할 것이라는 사실을 예측할 수 있습니다. Web3 등 새로운 기술에 대해 여기서 알아본 내용과 아울러 그 어느 때보다도 걷잡을 수 없고 파괴적으로 보이는 내용을 바탕으로 하여 FortiGuard Labs에서는 앞으로의 12개월에 그치지 않고 몇 해 정도로 더욱 장기적인 관점에서 위협 동향이 어떠한 양상으로 발전해 나갈 것인가에 대해 몇 가지를 전망하고자 합니다.

완전한 삭제

삭제 도구 멀웨어는 공격자들이 10년도 더 된 이 구식 공격 방식에 새로운 변종을 들여온 덕분에 올해 들어 극적인 부활에 성공했습니다. 삭제 도구 멀웨어의 확대 자체도 위험한 소식이지만 FortiGuard Labs에서는 위협 행위자들이 점차 다양한 위협 수단을 합쳐 자신들이 야기할 수 있는 파괴적 행위의 수준을 극대화하는 일이 늘어날 것으로 예상합니다. 예를 들어, 사이버 범죄자가 컴퓨터 웜을 삭제 도구 멀웨어와 간단히 합칠 수 있게 되면 해당 멀웨어를 빠르게 복제하여 더욱 먼 곳까지 전염시키는 일이 더욱 쉬워지게 됩니다. 적당한 취약점이 존재하는 경우, 이러한 방식의 공격은 단기간에 광범위한 파괴로 이어질 수 있습니다. 이렇게 되면 탐지 시간과 보안 팀의 복구 속도가 무엇보다 중요한 요소가 됩니다.

앞으로의 일을 전망하자면, 삭제 도구를 기타 공격 벡터와 섞어 사용하는 방식이 보안 커뮤니티로서 우리가 마주하고 있는 가장 거대한 위협으로 부상하고 있습니다. 삭제 도구는 잠재적으로는 사이버 영역을 몰아치듯 점령해 버리면서 전세계의 공공 및 민간 영역에서 이용하는 IT 네트워크에 충격을 던질 수 있습니다. 삭제 도구의 상품화로 말미암아, 이러한 방식은 기하급수적인 규모로 네트워크에 충격을 전할 가능성이 있습니다.

거칠고 사나운 Web3의 세계

디지털 경제의 소유권을 탈중심화하는 것을 목적으로 인터넷에 새로이 등장한 블록체인 기반 반복에 대한 개념인 Web3는 Web3 도구를 사용한 실험에 착수한 기업들이 점차 늘어나면서 빠르게 주류를 형성하고 있습니다. 그 이유는 간단합니다. Web3는 기업에 개발팀이 프로세스를 지원하기 위한 새로운 인프라를 관리하거나 유지하지 않고도 애플리케이션을 쉽게 배포할 수 있는 등의 여러 가지 장점을 제공합니다.

하지만 신기술이 늘 그렇듯, Web3 역시도 보안 위협에서 자유로울 수는 없습니다. Web3는 사용자가 자신의 데이터를 제어하는 것과 관련 있는 개념입니다. 그리고 과거의 보안 인시던트를 통해 얻게 된 교훈을 여기에 하나 적용하자면 사용자가 가장 약한 고리인 경우가 꽤 많다는 것입니다. 블록체인의 비가역성이 약간의 도움을 줄 수는 있지만 새로운 문제들이 생겨나는 것도 사실입니다. 예를 들어, 오늘날의 Web3 지갑에서는 MFA를 사용하지 않고 오로지 암호에만 의존하는데 암호를 잊어버리면 복구가 어려워집니다.

FortiGuard Labs에서는 Web3가 완전한 주류가 되기 전에 네트워크의 상태를 유지할 책임이 있는 네트워크 노드에서 사기 행위와 도난 데이터를 어떻게 해결할지에 대한 몇 가지 규정이 도입될 것이라 예상합니다. 사기 행위가 일어날 때 이를 마치 은행에서 미승인 개인이 신용카드를 사용했을 때 대처하는 것과 마찬가지로 추적해 격리할 수 있도록 하는 프로토콜도 제대로 갖추어져야 합니다.

양자 시대를 맞이하는 준비 목록

양자 컴퓨팅이 시작된 지 40년도 더 되었지만, 최근 몇 년 동안 공공 부문과 민간 부문을 가리지 않고 모든 기업에서 이 기술에 더 많은 투자를 하고 있습니다. 최근의 McKinsey & Company 보고서에서는 "양자 컴퓨팅이 기존의 고성능 컴퓨터의 속도와 도달 범위를 넘어선 문제를 해결하는 데 있어 기업에 확실히 도움이 되겠지만, 지금과 같은 초기 단계에서 그 사용 사례는 대부분 실험적이고 가설 단계에 국한되어 있다"라고 주장합니다.[6] 이미 양자 컴퓨팅은 예전에는 해결할 수 없던 암호화 알고리즘의 해결 등의 분야에는 돌파구를 제시하고 있습니다.

비록 양자 컴퓨팅의 특정 기능들은 현재로서는 널리 적용하거나 활용하기 힘들 수도 있겠으나 전문가들은 양자 컴퓨터가 기본의 암호화 메커니즘을 해결하기에 충분한 능력을 갖추게 되는 시점인 양자 시대(또는 Q-Day)가 빠르게 다가오고 있다고 경고합니다. 보안 커뮤니티가 양자 컴퓨터를 견디기 위해 새로운 암호 알고리즘을 설계하고자 노력하고는 있지만 이러한 노력도 중간 단계에 머무르고 있습니다.

예를 들어 불과 몇 달 전에 NIST에서는 수년 간 열린 경연대회에서 참가자들에게 양자 컴퓨터의 공격을 막을 수 있는 새로운 암호화 표준을 설계하도록 주문하여 그 우승자를 발표했습니다. 이러한 양자 내성 암호화 알고리즘 가운데 하나인 초단수 이소젠 키 캡슐화(Supersingular Isogeny Key Encapsulation, 줄여서 SIKE)가 암호를 풀어낸 단일 코어 컴퓨터에 의해 빠르게 사이버 공격을 당했습니다. 수개월 후, 미국의 국가안보국에서는 오늘날 사용되는 암호화 알고리즘을 대체하기 위해 설계된 암호화 알고리즘 컬렉션인 CNSA(상업용 국가 안보 알고리즘 세트) 2.0을 배포했습니다. 여기에 속한 모든 알고리즘은 양자 컴퓨터에 대해 분석되고 안전하다고 여겨졌습니다. NSA에서 이러한 알고리즘 세트의 구현에 대한 지침과 타임라인 관련 제안을 발표하던 당시는 새로운 암호화 표준의 구현율과 성공을 이해하기에는 너무 이른 시기였습니다.

양자 컴퓨팅은 의심할 바 없이 발전해 나가 앞으로 더욱 강력한 모습이 될 것이며, 이러한 발전은 그 능력이 암호화 알고리즘을 무너뜨릴 정도의 성능을 갖춘 뒤에도 멈추지 않을 것입니다. 양자 컴퓨팅이 가늠할 수 없을 만큼 프로세싱 능력을 향상했기 때문에 결국에는 사이버 범죄자들이 추가적인 활동을 벌이는 데 사용될 수도 있습니다. 가능성 있는 예시 가운데 하나로 범죄자들이 양자 컴퓨팅을 AI 무기화에 이용해 이를 새로운 제로데이 취약성 관련 작업 중에 애플리케이션 퍼징에 적용하는 일이 생길 수 있습니다.

진화하는 위협 동향에 대항해 방어하기

위협 행위자들이 사용할 카드를 점점 늘려갈 수 있지만, 다행인 소식은 이러한 사이버 범죄 생태계를 몰아내려는 수많은 노력도 진행 중이라는 것입니다. 미국 법무부는 올해 랜섬웨어 운영자들과의 전쟁에서 중요한 승리를 거뒀습니다. 지난 1월 악명 높은 REvil 사이버 보안 갱단원 14명이 미국 당국의 요청을 받아 러시아에서 체포된 것입니다. REvil은 Kaseya 공격의 주범이었으며 해커 중 한 명은 Colonial Pipeline 사건에도 연루되어 있었습니다. 한 달 후에는 가상 화폐 거래소에서 도난당해 2,000건의 미인가 거래를 개시한 비트코인 119,754 BTC에 해당하는 금액을 세탁하려 한 혐의로 두 명이 뉴욕시에서 체포되었습니다. 지금까지 해당 해킹과 관련된 암호화폐 36억 달러 이상이 공권력을 통해 확보되었습니다.

국가 간 및 공급업체 간의 제휴도 사이버 범죄조직을 식별하는 데 도움이 되고 있습니다. WEF(세계 경제 포럼)의 PAC(대 사이버 범죄 파트너십)의 창립 멤버로서, 포티넷은 사이버 범죄 조직의 생태를 매핑하여 이들의 청사진을 파악한 뒤 저지하기 위한 사이버 범죄 세계지도(ATLAS) 프로젝트에 매진하고 있습니다. 이 외에도 FortiGuard Labs에서 정보와 협력을 보태고 있는 다음과 같은 기업이 있습니다. Microsoft Active Protections Program(MAPP), FIRST(인시던트 대응 및 보안 팀 포럼), CTA(사이버 위협 연합), 인터폴 GCEG(글로벌 범죄 전문가 그룹) 및 게이트웨이 프로젝트, NICP(NATO 산업 사이버 파트너십), 세계 경제 포럼 사이버 보안 센터, MITRE Engenuity 위협 정보 기반 방어 센터.

공격자와 그 전술을 추적하면 공격에 대해 어떻게 대처해야 할지 더욱 쉽게 알 수 있습니다. 암호 지갑과 통화 흐름을 비롯한 자금 흐름을 추적하는 것 역시 도움이 됩니다. 또한, 범행을 운영하는 주체에만 집중하는 대신, 메시지를 전달함으로써 역시 기소 대상이 될 수밖에 없는, 공범들을 쫓는 수사도 많아지고 있습니다.

이러한 진전을 통해 긍정적 조짐이 보이는 만큼, 실제로도 사이버 범죄자들이 영영 도망칠 수는 없습니다. 하지만 우리가 목격하고 있는 대다수의 위협은 단지 위협 행위자들이 오랫동안 의지해 왔던 것으로 보고 있던 전형적인 방식이 발전한 것일 뿐입니다. 사이버 범죄자들이 자행하는 제로데이 공격조차도 목적은 한 가지입니다. 바로 네트워크에 침투해 중요한 정보를 훔치는 것입니다. 위협의 양과 속도에 맞춰가며 대처하는 것은 힘겨운 전투와 같을 때가 많긴 하지만 좋은 소식은 이러한 공격을 펼치기 위해 범죄자들이 사용하는 방법이 대개는 대동소이하여 보안 팀에 유리한 입지를 안겨 준다는 것입니다.

지금 사용 중인 환경을 보호하고 범죄자들보다 한 발짝 앞서기 위한 최상의 조언을 드립니다.

사이버 공격의 기승전결을 이해하기

기업을 효과적으로 방어하려면 사이버 범죄자들 자체는 물론, 이들의 동기와 전술, 행동 양상까지 제대로 이해해야 합니다. MITRE ATT&CK 프레임워크는 기업 네트워크를 상대로 하여 발전된 지속적 위협이 자주 사용하는 전술과 기술 및 절차(TTP)를 문서로 남겨 도움을 줍니다. ATT&CK는 다양한 방식을 통해 보안 운영, 위협 인텔리전스, 보안 아키텍처를 지원합니다.

사이버보안 메시 플랫폼의 수용

복잡성은 줄이면서도 보호 효과는 강화하려면 광범위하고 통합적이며 자동화된 사이버보안 메시 플랫폼이 필수적이며, 특히 네트워크의 규모는 증대되고 범죄자들은 취약점을 공격하기 위해 점차 새로운 방법을 찾고 있는 상황에서는 말할 것도 없습니다. 사이버보안 방어는 오랫동안 한 번에 하나의 솔루션으로 배포되어 왔으며 일반적으로는 하나의 문제가 나올 때마다 이에 대응하는 식으로 배포되어 왔습니다. 그러나 하나의 문제에만 전담하는 솔루션을 모아놓은 형태로는 오늘날의 위협 동향에서 제 효과를 발휘할 수 없습니다. 단일 사이버보안 플랫폼으로의 단일화, 융합을 통해 더욱 촘촘히 통합하고, 더욱 많이 자동화하며, 네트워크 전체에 대한 위협에 맞서 더욱 빠르고 협력적이며 효과적으로 보호함과 동시에 대처하는 것이 필수적입니다. 빠르면서도 협력적인 대처를 가능하도록 만들기 위해 AI를 통해 보안 솔루션을 개선함으로써 실시간으로 공격 패턴을 탐지하고 위협을 차단할 수 있도록 해야 합니다. 또한, 솔루션은 늘어나는 공격 건수에 대처하기 위해 확장할 수 있어야 합니다. 기업에서는 다음과 같은 솔루션을 배치하여 활용하는 것이 이상적입니다.

- 정찰 단계에서 공격을 차단하기 위해 설계된 DRPS(디지털 위험 보호 서비스)와 기만 기술
- 웹, DNS 및 C2 보호
- AI 탐지 시그니처를 탑재한 멀웨어 대비 도구
- 지능형 IPS(침입 방지 시스템) 탐지
- EDR(엔드포인트 탐지 및 대응)
- MITRE ATT&CK 매핑을 사용하는 AI 기반 인라인 샌드박싱 기술

이상적인 것은 데이터 센터, 캠퍼스, 지사, 멀티 클라우드, 홈 오피스, 엔드포인트를 비롯하여 분산된 네트워크 전반에 지속적으로 솔루션을 배포하는 것입니다.

네트워크 세그멘테이션과 마이크로 세그멘테이션의 구현

네트워크 세그멘테이션에는 비즈니스와 관련된 다양한 장점이 있습니다. 세그멘테이션은 네트워크 전체로 공격이 확산되는 것과 보호하지 않는 기기에 공격이 침투하는 것을 막아 보안을 향상합니다. 공격이 발생한 경우에도 세그멘테이션은 멀웨어가 기업 내의 다른 시스템에 퍼지지 않도록 합니다.

마이크로 세그멘테이션은 보안 아키텍처를 같은 브로드캐스트 영역 내의 모든 자산과 관련해 횡적인 가시성을 확보할 수 있는 환경으로 세밀하게 분리할 수 있도록 하는 네트워크 보안 기술입니다. 네트워크 환경을 개인 사용자 워크로드 수준까지 타고 내려가는 뚜렷한 보안 세그멘트로 논리적 분할을 하면 세분화가 가능합니다. 정책이 개인 워크로드에 적용되기 때문에 마이크로 세그멘테이션은 공격에 대한 저항 수준을 높일 수 있습니다. 설사 침해가 발생한 경우라도 해커가 운신할 수 있는 범위를 침입한 애플리케이션으로만 제한하는 효과가 있습니다.

FortiGuard Labs

FortiGuard Labs는 포티넷의 위협 인텔리전스 및 리서치 조직입니다. 포티넷 고객에게 업계 최고의 위협 인텔리전스를 제공하여 유해한 활동 및 정교한 사이버 공격을 차단하도록 지원하는 것을 목적으로 합니다. FortiGuard Labs는 업계 최대의 지식으로 무장한 위협 헌터, 연구자, 분석가, 엔지니어, 데이터 공학자로 구성되어 있으며 이들은 전 세계에 퍼져 있는 전담 위협 연구소에서 열심히 일하고 있습니다. FortiGuard Labs에서는 수백만 개의 네트워크 센서와 수백 개의 인텔리전스 공유 파트너사를 통해 지속적으로 전 세계 공격면을 감시합니다. FortiGuard Labs는 AI와 기타 새로운 위협에 대한 데이터를 마이닝하기 위한 혁신 기술을 이용해 정보를 분석하여 처리합니다. 이러한 노력은 시의적절하고 실천 가능한 위협 인텔리전스로서 포티넷 보안 제품 업데이트, 고객에게 자신들이 맞닥뜨린 위협과 그 주도 세력을 더욱 제대로 이해할 수 있도록 하는 선제적 위협 연구, 고객에게 자신이 처한 위협 동향을 더욱 제대로 이해하고 방어할 수 있도록 하는 위협 인텔리전스라는 형태로 나타납니다. 자세한 사항은 포티넷, 포티넷 블로그, FortiGuard Labs에서 확인할 수 있습니다.

[1] "2021년도 1월부터 6월까지의 은행 보안법 데이터 상 랜섬웨어 추세," 미국 금융 범죄 단속 네트워크, 2021년 10월 15일.
[2] "포티넷 랜섬웨어 설문조사를 통해 드러난 여러 기업의 미비 실태," 포티넷, 2021년 9월 29일.
[3] "2022 운영 기술 상태 및 사이버 보안 보고서," 포티넷, 2022년 6월 21일.
[4] "포티넷 랜섬웨어 설문조사를 통해 드러난 여러 기업의 미비 실태," 포티넷, 2021년 9월 29일.
[5] "포티넷 랜섬웨어 설문조사를 통해 드러난 여러 기업의 미비 실태," 포티넷, 2021년 9월 29일.
[6] "양자 컴퓨팅: 새로운 생태계와 업계 사용 사례," McKinsey & Company, 2021년 12월.

www.fortinet.com/kr

서울특별시 강남구 영동대로 325 에스타워 14 /15층 **전화:** 080-559-8989 **Email:** kr-callcenter@fortinet.com