FIREEYE™

규정 준수를 넘어:

사이버 위협과 의료

주요 내용 요약

의료 산업계는 다양한 위협 범죄자와 악의적인 활동에 노출되어 있습니다 . 사회에서 의료 산업이 수행하는 역할의 중요성과 가장 민감한 개인 정보를 다룬다는 점을 고려하면 이 산업에 대한 위험은 특히 막대한 피해를 초래할 수 있습니다 . 범죄자들이 개인 신원 확인 정보 (PII) 와 보호되는 의료 정보 (PHI) 를 금전화하려는 시도를 하고 , 첩보 수집을 목적으로 국가 차원에서 중요한 연구 기록과 대량 기록을 빼내기 위한 침입 작전을 펼치는 경우가 있습니다 . 또한 랜섬웨어와 같은 파괴적인 위협은 병원 네트워크에서 막대한 피해를 입히는 한편 중요한 생체의료 장비와 시스템에 영향을 미칩니다 . 이 산업 부문의 조직이 기존의 규정을 준수하는 데 그치지 않고 끊임없이 변화하는 위협 환경에 대처하려면 위협 인텔리전스를 활용하여 끊임없이 진화하는 이 같은 위협을 파악하고 위험을 적절하게 최소화해야 합니다 .

FireEye 가 이 산업 부문 전반에서 위협 활동을 관찰한 결과 , 의료 기관에 대한 위협을 다음과 같이 분류할 수 있었습니다 .

데이터 도용

- 금전적 동기의 위협 활동은 의료 기관에서 발생 빈도가 높고 피해도 큽니다 . 금전적 동기의 위협 활동은 의료 기관에서 발생 빈도가 높고 피해도 큽니다 . 사이버 범죄자는 중요한 환자 기록과 데이터가 저장되어 있거나 그러한 정보에 액세스할 수 있는 특정 표적을 집중적으로 공격하거나 , 보안이 허술한 조직과 네트워크를 표적으로 기회를 엿보는 공격을 감행합니다 .

- 사이버 범죄 활동과 비교했을 때 사이버 스파이 작전은 그 빈도는 낮지만 특히 업계의 일부 의료 기관에게는 유의해야 할 정도의 피해를 초래할 수 있습니다 . FireEye 가 이 같은 위협 범죄자 (특히 중국과 연관이 있는 범죄자) 에서 관찰한 활동 중 상당수는 잠재적으로 인텔리전스 운영을 위해 의료 조사 데이터를 입수하고 대규모 정보 데이터 세트를 수집하는 데 그 목적이 있는 것으로 보입니다 .

- 2018 M-Trends 보고서에서 FireEye 는 사고 발생 후 다시 표적이 되는 사례가 산업 부문 중 의료 산업에서 세 번째로 많이 나타난다는 것을 관찰했습니다 .

파괴적인 위협

- 사이버 갈취범과 국가 차원의 범죄자로 인해 발생하는 파괴적인 위협은 이 산업 분야에서 의료 서비스 제공자와 기타 조직의 운영 연속성을 꾸준히 위협하고 있습니다 .

- 침해 후에는 랜섬웨어와 같은 표적 활동이 수행되었고 , WannaCry 같이 빈도는 낮지만 광범위한 국가 차원의 위협이 보안이 허술한 인프라를 위협할 수 있습니다 .

- 중요 인프라 내의 운영 기술 네트워크와 마찬가지로 , 의료 서비스 제공자 내부의 보안 조직은 이 같은 시스템을 노리는 위협에 대한 가시성을 유지하는 데 어려움을 겪고 있습니다 .

앞으로 병원 및 의료 서비스 제공자 내에서 중요 기능에 사용되는 생체의료 장비가 늘어나면서 보안 문제도 갈수록 커지게 됩니다 . 게다가 그 중요성과 가치를 고려했을 때 , 사이버 범죄를 저지르고자 하는 의지의 증가로 인해 , 또는 지정학적 긴장이 고조되는 기간에 국가 차원의 범죄자들이 파괴적인 도구를 배포하려는 행위는 오늘날까지 관찰된 이러한 위협으로 인한 피해를 현저히 증가시킬 수도 있습니다 .

동기별 위협 활동

사이버 범죄

- 금전적 동기의 위협 활동은 거의 대부분의 경우 의료 기관에서 발생 빈도가 높고 피해도 큽니다 . 주로 PII, PHI, 중요 시스템에 대한 액세스 등이 표적이 됩니다 .
- 관찰된 활동으로는 인증 도용 악성코드 배포 , 크립토마이닝 , 공격을 통해 입수한 의료 시스템에 대한 액세스 판매 , 랜섬웨어를 통한 병원 시스템의 암호화 , 갈취 캠페인 등이 있습니다 .
- 여러 지역에서 다양한 사이버 범죄자들이 의료 산업을 노립니다 . 관찰 및 추적된 그룹으로는 TEMP.Demon 과 thedarkoverlord 가 있습니다 .

사이버 스파이 활동과 국가 차원의 위협

- 의료 부문을 표적으로 삼는 일반적인 빈도 수의 스파이 활동도 주목할 만한 피해를 입힐 수 있습니다 .
- 의료 부문을 표적으로 삼는 것으로 관찰된 범죄자로는 중국과 관련된 APT10(Menupass), APT41, 러시아와 관련된 APT28(Tsar) 과 APT29(Monkey), 베트남과 관련된 APT32(OceanLotus) 등이 있습니다 .
- 이 부문 , 특히 의료 서비스 제공자를 표적으로 한 파괴적인 캠페인은 상당한 피해부터 엄청난 피해까지 초래할 수 있습니다 .

핵티비즘과 정보 작전

- FireEye Intelligence 는 의료 부문에서 핵티비스트 캠페인은 흔하지 않은 위협으로 , 표적이 된 조직에 무시해도 될 정도이거나 약소한 피해만 초래한다고 진단합니다 (보통 신뢰도 수준).
- 의료 부문에 영향을 미치는 정보 작전은 대개 낮거나 보통 수준의 심각도로 영향을 미치고 자주 발생하지 않는 위협임이 거의 확실합니다 .
- 최근 몇 년 사이에 의료 관련 메시지를 전파한 것으로 관찰된 범죄자는 러시아와 관련된 공격자인 CyberBerkut 와 @pravsector 가 있습니다 .

데이터 도용

어느 산업 부문에서든 , 위협 범죄자는 원하는 데이터 또는 액세스 권한을 입수하기 위해 에코시스템의 가장 보안이 취약한 지점으로 이끌리기 마련입니다 . 그런 점에서 사이버 범죄자들은 PII 와 PHI 를 입수하기 위해 보험회사 외에 , 보안이 취약한 의료 서비스 제공자에게로 많이 끌릴 것입니다 . 사이버 스파이 범죄자는 이 데이터를 첩보 수집용으로 이용하여 유력 인사나 , 중요 정보에 액세스할 수 있는 사람을 최종 목표로 삼을 수도 있습니다 . 또한 치료법 , 의료 기기 , 생명공학 , 기타 해당 산업 부문의 하위 분야와 관련해 연구 개발에 참여하는 기관은 경제 스파이 활동의 대상이 되는 중요한 지적 재산을 보유하고 있습니다 . 특히 , 중국이 전략적으로 추진하고 있는 " 중국제조 2025" 계획에는 의료 기술과 기기의 국산화를 촉진한다는 내용이 포함되어 있는데 , 이는 이러한 기술의 IP 소유자 및 제작자를 대상으로 한 위협 활동의 동기가 될 수 있습니다 .

사이버 범죄 위협

FireEye Intelligence 는 매우 민감한 개인 신원 확인 정보 (PII), PHI 및 금융 데이터를 대량으로 침해하여 막대한 피해를 입히는 금전적 동기의 사이버 위협 활동이 잦은 위협으로 나타난다고 진단합니다 (높은 신뢰도 수준).

의료 기관과 서비스 제공자로부터 빼낸 PII 및 PHI 를 암시장에서 매매하는 범죄자들은 매우 흔하며 , 이 데이터가 신원 도용과 금융 사기부터 맞춤형 피싱 미끼를 만드는 것까지 다양하게 활용될 수 있다는 점에서 앞으로도 그럴 것임이 거의 확실합니다 .

- FireEye Threat Intelligence 는 2018 년 10 월 1 일부터 2019 년 3 월 31 일까지 여러 건의 의료 관련 데이터베이스가 암시장 포럼에서 대부분 2,000 달러 미만의 가격으로 판매되는 것을 관찰했습니다 . 특히 판매자의 설명에 따르면 이 같은 데이터베이스를 광고하는 시점은 실제 데이터 침해가 발생한 시점과 일반적으로 연관성이 없다고 합니다 . 관찰된 광고 중 많은 수는 지난 몇 달 또는 몇 년 사이에 침해된 데이터베이스에 대한 것이었습니다 .

	가격
2019 년 3 월 19 일 , 범죄자 **InfoMerchant** – 이름이 알려지지 않은 " 의료 카드 " 회사와 관련한 확인되지 않은 양의 데이터 , PII 및 의료 정보 포함 .	해당 없음
2019 년 2 월 21 일 , 범죄자 **NetFlow** – 미국 의료 기관과 관련한 4.31GB 의 데이터 , 운전 면허 , 의료 보험 , 우편 번호 등의 환자 데이터 포함 .	$2,000
2019 년 2 월 12 일 , 범죄자 **specfvol** – 미국 의료 기관과 관련한 50,000 건의 기록 , 의료 기록 , PII, 의료 보험 정보 포함 .	$500
2019 년 2 월 6 일 , 범죄자 **the.joker aka Achilles** – 호주 의료 기관과 관련한 128,764 건의 기록 , 신용카드 데이터 및 제한적인 PII 포함 .	$1,500
2019 년 2 월 2 일 , 범죄자 **fallensky519** – 인도 의료 기관 웹 사이트와 관련한 6,800,000 건의 기록 , 환자 정보 및 PII, 의사 정보 및 PII, 인증 정보 포함 .	$1,700
2019 년 1 월 28 일 , 범죄자 **x999x** – 캐나다 의료 웹 사이트와 관련한 확인되지 않은 양의 기록 , 도메인 관리자에 대한 액세스 정보 , 네트워크에 대한 액세스 정보 , 서버 이름 , IP 주소 , 플랫폼 정보 포함 .	$5,500
2019 년 1 월 22 일 , 범죄자 **emoto -** 미국 의료 기관과 관련한 58,000 건의 기록 , PII 포함 .	$480
2019 년 1 월 16 일 . 범죄자 **ping** 개인 신원 확인 정보 (PII) 가 포함된 100,000 건의 기록 광고 . 광고에 따르면 이 범죄자는 270 여 개의 미국 병원이 이용하는 서버에서 데이터를 입수했다고 함 .	$500
2018 년 12 월 15 일 , 범죄자 **emoto** - 미국 의료 기관과 관련한 19,000 건의 기록 , 금융 데이터 , 이메일 주소 , 직원에 대한 정보 포함 .	$300
2018 년 12 월 4 일 , 범죄자 **the.joker aka Achilles** – 호주 의료 기관과 관련한 11,700 건의 기록 , 직원 정보 포함 .	$500
2018 년 11 월 15 일 , 범죄자 **Lavanda** – 미국 의과대학과 관련한 20,000 건의 기록 , 직원 데이터 및 PII 포함 .	해당 없음
2018 년 11 월 4 일 , 범죄자 **Merky** – 영국 의료 기관과 관련한 180,000-200,000 건의 기록 , PII 포함 .	$200

사이버 범죄자들은 의료 기관에서 빼낸 데이터를 직접 판매하는 것은 물론 , 이들 기관에 대한 불법 액세스 정보를 암시장에서 판매하는 경우도 많습니다 . 다른 범죄자들은 이 액세스 정보를 민감한 정보를 빼내거나 , 침해한 네트워크의 다른 장치를 감염시키거나 , 침해한 네트워크의 연결 및 정보를 사용함으로써 표적 조직과 다른 기관 간의 신뢰 관계를 이용하여 다른 네트워크를 침해하는 등의 사후 악용 활동에 이용할 수 있습니다 .

- TEMP.Demon 은 최소 2018 년 7 월부터 침투 작전을 펼치며 의료 부문을 비롯한 여러 산업 분야에 피해를 입히고 있습니다 . 이들은 공개적으로 제공되는 툴을 사용하여 피해자의 환경에 침투하고 이동합니다 .
- 2019 년 2 월 6 일 , 유명 러시아어 포럼에서 “Jendely” 는 미국 의료 기관에 대한 액세스 정보를 광고했습니다 . 광고에 따르면 이 범죄자는 3,000 개의 호스트로 이루어진 네트워크에 대한 도메인 관리자의 액세스 정보를 입수했습니다 . 이 액세스 정보는 9,000~20,000 달러의 가격으로 경매에 붙여졌습니다 . 2018 년 11 월 , “Jendely” 는 600 개 이상의 호스트로 이루어진 여러 미국 회사의 네트워크에 대한 액세스를 15,000 달러의 가격으로 판매한다고 광고했습니다 .

초기에 “thedarkoverlord“ 의 활동은 기록에 대한 액세스 정보를 판매하고 갈취를 시도하는 등 주로 의료 부문을 표적으로 한 공격과 연관되어 있었습니다 . thedarkoverlord 는 나중에 다른 부문으로 표적을 다각화했지만 의료 부문은 2017 년 그룹의 몇몇 알려진 구성원이 체포될 때까지 여전히 주요 표적이었습니다 . 2018 년 말에 thedarkoverlord 의 암시장 활동이 제한적으로 재개되었고 , 2019 년에는 극히 적은 활동만 관찰되었기 때문에 현재 thedarkoverlord 가 어느 정도로 활동하고 있는지는 명확하지 않습니다 .

2016 년 “thedarkoverlord” 가 판매한 의료 데이터베이스 (지역별)

의료 서비스 제공자의 위치	총 기록 수	가격
애틀랜타	396,459	300 비트코인
중부 / 중서부	207,572	170 비트코인
미주리주 파밍턴	47,864	60 비트코인
뉴욕 브롱크스	34,621	25 비트코인
미국	9,278,352	300 비트코인
일리노이주 페어뷰	23,565	35 비트코인

사이버 스파이 위협

의료 연구에 지속적으로 관심을 보이는 중국 APT

FireEye 는 여러 중국 APT 그룹이 의료 연구 데이터를 입수하는 데 매우 집중함을 보여주는 정황을 계속 목격하고 있습니다 . 특히 관심을 보이는 분야는 암 관련 연구로 , 암과 사망률의 증가에 대한 중국의 우려가 커지고 있고 그에 수반되는 국민 건강 관리 비용에 대한 우려가 반영된 것으로 보입니다 . 공개된 소식통에 따르면 암 사망률이 최근 수십 년간 급격히 증가해 암이 사망 원인 중 가장 큰 것으로 나타났습니다 .

2020 년까지 중국이 보편적 의료 서비스를 계속 추구함에 따라 비용 및 국내 산업을 통제하는 것이 중국의 정치적 안정 유지 전략에 영향을 미칠 것이 분명합니다 . APT 활동의 또 하나 가능한 동기는 금전적인 것입니다 . 중국은 세계에서 가장 빠르게 성장하고 있는 제약 시장 중 하나이며 , 국내 기업 , 특히 종양 치료나 관련 서비스를 제공하는 기업들에게 수익성 있는 기회를 창출하고 있습니다 . 의학 연구와 그 데이터를 표적함으로써 중국 기업들이 서양의 경쟁업체보다 더 빨리 신약을 시장에 내놓을 수도 있게 됩니다 .

- 2019 년 4 월 초 , 중국의 사이버 스파이 범죄자들은 EVILNUGGET 악성코드를 통해 암 연구에 집중하는 미국 의료 센터를 표적으로 삼았습니다 . 유인 문서 중 하나는 표적 조직이 주최하는 컨퍼런스를 언급하고 있습니다 . 꾸준히 목격되는 의료 산업에 영향을 미치는 동향과 일맥상통하게 , 이 조직은 과거에 여러 중국 위협 범죄자들의 표적이 되었습니다 .
  - » 2018 년 1 년 전 , 중국과 연관된 APT41 은 CROSSWALK 악성코드를 사용하여 이 기관의 개인들에게 스피어피싱 공격을 실시했습니다 .
  - » 예전에는 생체의학 , 제약 및 의료 기관에 집중했으며 현재도 지속적으로 활동하고 있는 중국 그룹인 APT22 도 이전에 이 동일한 조직을 표적으로 삼았습니다 .
- 수년간 의료 관련 기업에 대한 APT41 의 관심은 수많은 침해 사례로 확대되었습니다 .
  - » 2014 년 7 월부터 2016 년 5 월 사이에 APT41 은 대기업 의료 기기 자회사를 표적으로 공격을 실시했습니다 . APT41 은 처음에는 모회사를 대상으로 했지만 , 피해 호스트의 30% 는 의료 기기 제조 전문 자회사와 관련이 있었습니다 . 작전에 사용된 암호 문자열과 스푸핑된 도메인은 모회사가 아닌 자회사를 대상으로 하는 집중적인 작전임을 나타냅니다 . APT41 이 관심을 보인 표적 호스트의 특성이 정보 기술 담당 직원과 의료 기기 자회사가 사용하는 소프트웨어라는 사실을 바탕으로 몇 가지 징후를 파악했습니다 . 먼저 GEARSHIFT 라는 키로거가 이 의료 기기 회사에 배포되었습니다 . 또한 피해자의 디지털 인증서가 유출되어 이 산업 부문을 대상으로 한 다른 작전에 사용된 악성코드에 서명하는 데 사용되었습니다 . 그 자세한 내용은 아래와 같습니다 .
  - » 이러한 몇몇 작전과 동시에 , 인수를 추진 중인 생명공학 회사가 2015 년 5 월 APT41 의 표적이 되었습니다 . 인사 데이터와 세금 정보 , 인수 관련 문서 등 기업 운영에 대한 매우 민감한 정보가 표적이 되었습니다 . 특히 개발된 의약품의 임상시험 데이터 , 학술 데이터 , 연구개발 자금 지원 관련 문서도 유출됐습니다 . 시간대 , 동일한 GEARSHIFT 샘플 사용 , 앞서 언급한 의료 기기 회사의 디지털 인증서는 이 두 캠페인이 동일한 범인에 의해 동시에 진행되었음을 시사합니다 .
- 2017 년 말 , 중국과 관련된 APT10 은 스피어피싱 캠페인의 일환으로 , 이 업계와 관련이 있는 것으로 보이는 일본 기업을 대상으로 의료를 주제로 한 문서 3 건을 배포했습니다 . 그 문서들 중 두 가지는 암 연구 컨퍼런스와 관련된 것이었습니다 .
- 적어도 2013 년부터 APT18(Wekby) 은 생명공학 및 제약 관련 조직과 암 전문 연구 조직을 표적으로 공격을 실시했습니다 . FireEye 가 한 의료 제조사에서 조사한 사건에서 APT18 은 탐지되기 전까지 최소 60 일 동안 조직의 네트워크에서 활동한 것으로 파악되었습니다 . 이 기간 동안 이 범죄자들은 약 14 개의 사용자 계정을 사용하거나 액세스했고 , 450 개 이상의 시스템에 액세스하거나 백도어를 설치했습니다 . 또한 이 제조사의 네트워크에서 몇 기가바이트의 의료용 영상 장비 파일을 수집하고 아카이브 파일로 압축하여 정보를 빼내려 했습니다 .
- 우리가 목격했던 다른 사례들과 마찬가지로 , 사이버 공간을 통한 의료 데이터 및 연구 데이터 도용은 주요 혁신 기술을 획득하기 위한 보다 광범위한 중국의 전략을 구성하는 요소 중 하나일 것입니다 . 2019 년 4 월 , 중국 정부를 대신해 의학 연구 데이터를 훔쳐낼 우려가 있다는 판단에 따라 MD Anderson Cancer Research 의 연구원 여러 명이 해임됐습니다 .

FireEye 가 의료 부문을 표적으로 하는 중국 사이버 스파이 범죄자들 사이에서 관찰한 한 가지 테마는 바로 , 2015 년 미국 조직에 대한 몇 건의 유명한 침해 사건으로 대표되는 대규모 PII 및 PHI 의 도용입니다 . 2018 년 SingHealth 침해 사건에서 알 수 있듯이 , 대량 데이터 도용은 중국 사이버 스파이 범죄자들이 특정 개인 집단을 표적으로 이용하는 전술로 판단됩니다 .

- 2018 년 Singaporean Health 침해 사건에서 설명된 악성코드와 TTP 는 세간에 "Mofang" 으로 알려진 중국과 연관된 사이버 스파이 활동과 매우 유사하게 일치합니다 . FireEye Intelligence 는 이전에 QUASIFOUR 및 DUOBEAN 이라는 이름으로 추적 중인 Mofang 캠페인이 이 악성코드를 동남아의 정부 , 미디어 , 운송 , 건설 및 통신 부문을 대상으로 배포한다고 보고한 바 있습니다 .
- 중국과 관련된 한 사이버 스파이 범죄자는 미국인에 대한 대규모 기밀 데이터를 수집하기 위한 것으로 여겨지는 여러 건의 침해 사례에 연루되어 있다고 판단되는데 , 이 사람은 항공 부문과 더불어 PII 를 보유하고 있는 의료 기관과 미국 공무원의 민감한 데이터를 표적으로 활동을 수행했습니다 . FireEye 는 이 범죄자가 표적 인물을 식별하고 추적하며 활용하기 위해 데이터를 수집한다고 보고 있습니다 . 정부 데이터만으로도 중국에서 활동하는 비밀 요원을 식별하거나 , 미국에서 정보원과 이중 간첩을 모집하거나 , 기밀 취급 권한을 가진 미국인의 가족을 찾아내 괴롭히거나 위협하는데 사용될 수 있습니다 .

FireEye Intelligence 는 중국과 관련된 그룹 외에도 다음과 같은 다양한 사이버 스파이와 국가 차원의 범죄자가 의료 부문을 표적으로 한 공격에 연루된 것으로 관찰했습니다 .

- 러시아와 관련된 APT28 은 국제 스포츠 경기 및 운동 선수 약물 테스트와 관련된 글로벌 스포츠 규제 기관 및 기타 기관을 표적으로 한 공격에 연루되었습니다 .
- 2017 년 8 월 , APT28 등 러시아 관련 스파이 범죄자들과 연계되어 있는 것으로 판단되는 (보통 신뢰도 수준) CyberBerkut 라는 핵티비스트 그룹은 미국 당국 , 우크라이나 당국 , 계약업체 , 의학 중심의 비정부기구 (NGO) 가 우크라이나에서 생물학 무기 실험을 공모하고 있다는 근거 없는 주장의 게시물을 작성했습니다 . 이와 유사한 주장은 2016 년 8 월 , 오하이오에 위치한 한 클리닉에서 유출된 문서를 통해 미국 군사 기관들이 우크라이나에서 생물학 무기를 실험하고 있다는 사실이 증명되었다고 주장한 러시아 연계의 가짜 핵티비스트 페르소나인 @pravseector 에 의해 제기된 바 있습니다 .
- APT29 는 한 건 이상의 캠페인에서 의료인과 의료 정책 관련인에 대한 피싱 사기를 저질렀습니다 .
- 베트남과 관련된 APT32 는 영국의 한 의료 기관에서 확인된 유인 문서를 사용했습니다 .

파괴적인 위협

랜섬웨어 또는 갈취 캠페인은 환자나 건강 정보에 대한 접근을 제한하거나 중환자 진료에 지장을 줄 수 있다는 점에서 범죄자의 성공률과 이득의 상승으로 이어질 가능성이 있기 때문에 이 산업 부문을 공격하는 데 특히 유용한 것으로 인식될 수 있습니다. WannaCry 및 EternalPetya 공격에서 보여졌던 것처럼, 파괴적 공격 또는 큰 피해를 입히는 와해성 공격을 수행할 경우 미래의 활동은 상당한 피해부터 대재앙 수준의 피해까지 초래할 수 있습니다.

랜섬웨어

랜섬웨어 감염은 많은 다른 산업 부문의 기업보다 의료 기관에 더 큰 위험을 야기합니다. 거의 실시간으로 일관되게 환자 데이터에 액세스할 필요가 있고 조직이 중요한 파일, 시스템 및 장치에 액세스하지 못할 경우 환자에게 해를 끼칠 수 있기 때문입니다. 랜섬웨어 공격자들도 이처럼 중요도가 높아진 사실을 이미 알겠지만, 특히 우발적인 인명 피해로 이어질 경우 사법 당국의 면밀한 수사로 확대될 수 있다는 점을 우려해 일부 범죄자들 사이에서는 병원에 대한 랜섬웨어 공격을 꺼리는 현상이 나타나고 있습니다. 하지만 사후 침해 표적 랜섬웨어 캠페인의 증가로, 일부 범죄자들은 의료 사업자에게 지불 수단과 의지가 있다고 보고, 더 많은 위험을 감수하고서 이들을 상대로 작전을 수행할 수도 있습니다.

- 2018 년 11 월, FireEye 는 GandCrab 과 관련된 미국의 한 병원에서 발생한 침해 사고에 대응했습니다. GandCrab 은 최근 해당 범죄자들이 20 억 달러 이상을 벌었다고 주장한 후 작전을 중단한다고 발표한 랜섬웨어군입니다.
- 텍사스에 위치한 Altus Brown Hospital(ABH) 은 2018 년 11 월에 병원 시스템을 감염시키고 환자 정보를 포함한 병원 기록 등을 암호화한 Dharma 랜섬웨어 공격에 당한 사실을 시인했습니다.
- 2018 년 9 월, FireEye 는 미국의 한 의료업체에서 워크스테이션 93 개가 영향을 받은 Samas 랜섬웨어 사건에 대응했습니다.
- 2018 년 1 월 초, 미국의 한 병원은 백업본이 있음에도 불구하고 IT 시스템의 잠금을 해제하기 위해 4 비트코인 (당시 시세로 약 55,000 달러) 의 몸값을 지불했습니다. 병원 직원들이 랜섬웨어를 빠르게 탐지했지만, 병원 이메일 시스템과 전자 의료 기록, 내부 운영 체제로 감염이 확산되는 것을 막기엔 너무 늦었습니다.
- 다른 여러 의료기관에서도 최근 몇 년 사이 랜섬웨어 캠페인의 피해를 입었다는 신고가 접수됐습니다. 이에 대한 대응은 몸값을 지불하거나 데이터 손실 및 관련 비용을 수용하는 것부터, 신속한 문제 해결을 가능하게 하는 효과적인 보안 시스템 구현으로 피해를 최소화하는 것까지 다양했습니다.
- 어떤 경우에는 위협 범죄자들이 의도적으로 의료 부문을 표적으로 하는 것을 회피하기도 합니다. 2019 년 한 지하 포럼에 게시된 bitpaymer 랜섬웨어 서비스를 광고하는 게시물에서 범죄자 dihlofoss 는 " 우리는 병원, 교육 기관 및 정부 기관을 표적으로 하지 않는다 " 고 구체적으로 언급했습니다.

랜섬웨어 감염으로 인한 피해를 줄이려면 조직, 특히 병원처럼 고가용성이 요구되는 조직은 강력한 백업 정책 시행과 백업 구현뿐 아니라 이중화되고 적절하게 세그먼트화되어 격리된 네트워크 및 시스템을 갖춰야 합니다. 이 경우 네트워크의 한 세그먼트 또는 하나의 장치 세트가 손상되더라도 가용성을 유지할 수 있습니다. 다른 시스템 및 데이터가 보호 상태를 유지하고 문제를 해결하는 동안 적어도 제한적인 용량으로는 작동할 수 있기 때문입니다.

크립토마이닝 멀웨어

2017 년 말, 크립토마이닝 작전으로 인해 여러 의료 기관들이 피해를 입었다는 사실도 확인했습니다. 이는 최소한 지난 몇 년 동안 사이버 범죄자들 사이에서 크립토마이닝 악성코드가 인기를 끈 것과 일치합니다. 하지만 의료 기관의 경우, 처리 및 네트워크 부하 증가, 시스템 안정성 저하, 감염된 장치의 수명 단축 등을 통해 크립토마이닝 악성코드가 중요한 시스템에 미치는 영향 때문에 이러한 유형의 활동으로 인한 피해가 가중될 수 있습니다.

국가 차원의 파괴적인 공격

충돌이 발생하거나 긴장이 고조된 시기에는 랜섬웨어나 와이퍼 악성코드를 사용하여 특정 지역이나 국가의 의료 기능을 방해하거나 파괴함으로써 이익을 얻을 수 있으며, 특히 공격 스폰서들에게 그럴듯한 부인 근거를 부여하기 위해 본인의 소행이라고 주장하는 가짜 범죄자나 해커와 결합할 경우 더욱 이득이 됩니다.

- 많은 의료 기관들이 2017 년에 널리 퍼진 EternalPetya 와이퍼 및 WannaCry 랜섬웨어 캠페인으로 인해 피해를 입은 것으로 알려져, 이러한 유형의 캠페인에 의해 발생할 수 있는 피해를 단적으로 보여줍니다.

의료 사이버 물리 시스템 (MCPS) 을 표적
특히 의료 부문 내에서 파괴적인 위협을 위한 표적에는 의료 사이버 물리 시스템 또는 생체의학 장치가 포함됩니다 . 심박조율기 및 인슐린 펌프와 같은 이식 장치를 비롯하여 , 이러한 장치는 의사가 원격으로 관리하고 침습적 시술의 필요성을 줄이기 위해 네트워크에 점점 더 많이 연결되는 추세입니다 . 이러한 기능은 이점을 제공하지만 , 해당 장치를 대상으로 한 악의적인 사이버 활동으로 인해 피해를 받을 위험성도 내포하고 있습니다 .

FireEye Intelligence 는 현장에서 개인 의료 기기에 대한 어떠한 악의적인 활동도 포착하지 못했습니다 . 하지만 이러한 시스템에 영향을 미치는 위협 및 취약점에 대한 연구 자료가 많습니다 .

- ICS-CERT 는 2016 년부터 Philips, Roche, Medtronic, Smiths Medical, General Electric, Abbot Laboratories 와 같은 주요 공급업체의 제품에 대한 수천 건의 의료 권고 사항을 발표했습니다 . 의료 취약점 공개가 급증하고 있음에도 불구하고 사이버 물리 네트워크 보호를 위한 규제와 지침은 여전히 개발 초기 단계에 머물러 있습니다 .
- MCPS 의 취약점은 적어도 2010 년부터 공개되었지만 , 지난 2 년 동안 주요 공급업체의 제품과 관련한 발표가 여러 건 공개되고 있습니다 . 예를 들어 2017 년과 2018 년 , Abbott Laboratories 와 St. Jude Merlin, 그리고 Medtronic 은 심박조율기 , 프로그래머 , 환자 모니터에 영향을 미치는 일련의 취약점을 해결해야 하는 과제에 직면했습니다 .

네트워킹 기능과 원격 액세스의 존재는 의도적인 표적 공격을 통해 또는 본의 아니게 장치 액세스 중 장치 소프트웨어와 활동 간의 기대하지 않은 상호 작용을 통해 , 개인이나 그룹을 해치는 데 이용될 것으로 추측됩니다 .

- 개인이 생존을 위해 의존하는 중요한 의료 장치가 점점 더 네트워크화되고 원격으로 액세스하게 되면서 , 리소스를 충분히 확보한 악의적인 범죄자가 장치 사용자를 다치게 하거나 아프게 하거나 죽이도록 고안된 고도의 표적 캠페인을 수행할 가능성도 높아지고 있습니다 . 이러한 공격은 이론적으로 원격으로 수행할 수 있지만 , 장치 또는 관련 하드웨어에 근접해야 할 수도 있으며 , 사이버 위협 활동의 대폭적인 증가를 수반합니다 .
  - » 또한 감시 , 호기심 또는 테스트를 목적으로 하는 범죄자는 실수로 장치를 오작동시키거나 작동을 중지하는 방식으로 상호 작용함으로써 의도적인 공격과 유사한 결과를 초래할 수 있습니다 .
- 재고 추적 " 스마트 " 스토리지 , 원격 환자 모니터링 및 추적 시스템 , 원격 데이터 액세스 장치와 같은 의료 중심의 사물 인터넷 (IoT) 장치도 마찬가지로 의료 기관에 대한 이론적 공격 영역을 증가시킵니다 . 이러한 장치의 침해는 잘못된 환자 경보를 생성하여 혼란을 일으키고 , 재고 데이터를 변경하여 도용을 용이하게 하며 , 네트워크를 통해 내부적으로 이동하여 보안되지 않은 장치를 침해한 후 추가적인 침해 공격을 수행하는 등의 다양한 목적으로 이용될 수 있습니다 .
- 의료 기기 개발자는 전력 소비량 , 신뢰성 , 비용 등 설계상 여러 요인의 균형을 맞춰야 합니다 . 하지만 의료 서비스 제공자를 위한 데이터 액세스를 늘리고 의사가 환자에게 이식한 장치에 접근하는 데 있어서 장벽을 줄이기 위해 설계상 일부 장치의 보안에 허점이 있다고 이전에 평가한 바 있습니다 . 그리고 다른 종류의 의료 기기에도 유사한 보안 결함이 있다고 생각합니다 .

현재 MCPS 를 위한 표준 네트워크 아키텍처는 없습니다 . 그러나 NIST(National Institute of Standards and Technology) 특수 간행물 (SP) 1800-8B 에서는 이러한 네트워크의 구조를 이해하는 데 유용한 기준선을 제공합니다 . 이 접근 방식에 따르면 , 세그먼트화는 의료 네트워크 전반에서 보안 제어를 구현하는 데 핵심적인 역할을 합니다 .

맺음말

의료 기관은 다양한 사이버 위협 범죄자의 의도와 행동을 파악하고 대응해야 합니다 . 의료 기관이 보유하고 있는 풍부한 데이터 때문에 , 의료 부문에서 발생하는 보안 침해와 유출은 소비자들에게 큰 피해를 입힐 수 있습니다 . 이들 기관들 중 일부에서 진행 중인 중요한 연구는 자국 산업 발전을 도모하려는 국가 정부들에게 꾸준히 매력적인 표적이 되고 있습니다 . 앞으로 생체의학 기기의 사용이 증가함에 따라 , 특히 더 큰 위험을 감수하려는 범죄자들에게 이러한 기기는 파괴적인 사이버 공격의 매력적인 표적이 될 가능성이 있습니다 . 그에 따라 공격 영역에 대한 경쟁도 치열해질 것입니다 .

공격	지능화	영향				
		침해	데이터 도용	성능 저하	방해	파괴
표적	낮음	인터넷에 연결된 장치에 로그인 (예 : Shodan 사용)	위협 범죄자가 의료 네트워크에 대한 RDP 액세스 정보 판매			
	보통		FIN7 캠페인		의료 기기 작동 중단	
	높음		APT28, APT29, APT10 및 기타 국가 차원의 캠페인			
비표적	낮음			크립토마이닝 악성코드	Wanna Cry (2017)	
	보통					EternalPetya (2017)
	높음					

부록 그래픽 : 의료 사이버 보안 사고 매트릭스

FireEye에 대한 자세한 정보: **www.FireEye.com**

FireEye Korea
서울특별시 강남구 테헤란로 534 글라스타워 20층/
02.2092.6580/
korea.info@fireeye.com/www.fireeye.kr

FireEye 소개
FireEye는 인텔리전스 기반의 보안 회사입니다. FireEye는 혁신적인 보안 기술, 국가 수준의 위협 인텔리전스 및 세계적으로 유명한 Mandiant® 컨설팅을 결합한 단일 플랫폼을 제공하여 고객 보안 운영의 완벽한 확장을 지원합니다. 이를 통해 FireEye는 사이버 공격에 대비하고 이를 방어 및 대응하고자 노력하는 조직의 사이버 보안 부담을 줄이고 간소화합니다.

FIREEYE™