히트의 해커 라이프

~새로운 시대, 새로운 보안 멘로시큐리티와 만나다~

Story

서울 시, 해커 조직들이 사이버 공격을 위해 모이는 지역이다.
최근에 전 세계적으로 보안 조치가 강화되었지만, 계속해서 보안 위기를 맞고있다.
치명적인 보안 공격을 위해 , 서울 시에서 가장 강력한 해킹 조직은 '히트'라는 천재 소녀 해커를 스카우트했다.
과연, 천재라 불리는 이 해커가 서울 시의 보안스택을 뚫을 수 있을까?

등장인물

천재 소녀 해커 히트

아담, 보안 담당자, 보안 제일 회사

해킹 집단


서울시
109
セキュリティNo.1
Security City
NO ! HACKER
우리 해킹 조직은 새로 들어온 멤버 히트와 함께
더 강해질 것입니다!
음, 네…
여기가 바로 우리만의 비밀장소예요
여기요?
ギィ
ギロッ
네, 이제 오늘부터 당신의 비밀장소이기도 해요


우리 다 모였나요?자, 오늘 새로운 멤버를 소개하려 합니다.
어…
오늘부터 히트가 우리 팀을 이끌게 될겁니다.
PON!
다 들었죠?
히트, 본인을 소개해주세요
네…
저의 이름은 히트이고 오늘부터 팀을 이끌게 되었습니다.
히트,..HEAT
ざわ・・・・
히트 님, 전에 본 적 없지만, 이렇게 어린 줄은 몰랐습니다.
히트,.. HEAT
히트, 우리 멤버들에게 하고 싶은 말이 있나요?
네,
오늘부터 공격의 새로운 기술에 대해
알려드리겠습니다.
최근들어 강화된 서울시의 보안 시스템을 여러분들이 뚫지 못하고 있다고 들었습니다.

맞아요, 보안이 요즘 많이 강화됐어요.

어떻게 성공적으로 공격을 할 수있나요?

음,

첫째로 그들을 대상 사이트로 이끌 수 있도록하는 링크를 클릭하게 만들어야됩니다.

ペラ

ペラ

ペラ

모두가 요즘 이메일 링크가 믿을만하지 못하다고 생각하고 있기때문에 요즘에는 SNS를 이용합니다.

우리가 이메일로 링크를 보내면, 쉽게 의도가 읽혀지고,

이를 통해 우리가 의도를 읽혀지지 않으면서 사람들이 이것이 위험하다는 생각이 들지 않도록 만들 수 있습니다.

!?

그렇군요,

처음 듣는 공격 내용이군요!

?

그런데 링크가 클릭된 후에, URL필터링에 의해 탐지되지 않나요?

요즘 많은 회사들이 잘 알려지지 않은 웹사이트는 차단하던데요?

괜찮습니다.

우리에게는 이런 상황을 대비하여 몇 달 동안이나 작동되어온 동영상 사이트가 있습니다.

물론 단지 동영상 사이트기 때문에, 어떠한 URL필터링이 이걸 동영상 사이트로 분류할겁니다.

즉, 우리가 공격 도중에 공격 코드를 심고, 나중에 즉시 삭제할 수 있음을 의미합니다.

정말 준비돼 있으시네요!

좋네요!

그리고… 우리는 CAPTCHA도 사용할겁니다

CAPTCHA요?

네, CAPTCHA를 알고 계시죠?

사용자가 웹 사이트에 로그인할 때 보행자 횡단로나 신호등 등의 이미지를 선택하도록 하는 것입니다.

이렇게 함으로써, 공격 코드를 보안 도구로 분석할 수 없게 하며,

사람들이 안전한 느낌을 받도록 합니다.

다음 질문으로 어떻게 컴퓨터로 파일을 접근시키는 지에 대해 묻고 싶습니다.

최근 기업 네트워크는 의심되는

파일을 분석하고 차단하는 백신이나 샌드박스로 철처히 보안을 강화하고있습니다.

네, 그것도 문제가 되지않습니다.

바로 네트워크로 파일을 보내지 않는 한 괜찮습니다.

파일을 여러 데이터로 쪼개서 자바스크립트에서 작성한다면, 공격에 성공할 것입니다.

자바스크립트를 읽을 수 있는 브라우저가 스스로 읽고 컴퓨터로 다운로드 될 수 있습니다.

파일로 탐지되지 않다보니, 분석되지도 않습니다.

JS

JS

와우!

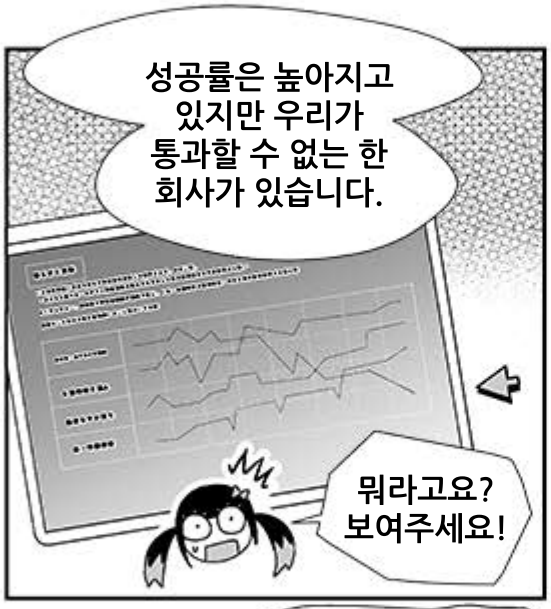
그런 경우 공격 계획은 완벽합니다!

자바스크립트와 데이터를 모두 난독화하면 웹 페이지 소스 코드를 분석하는 것은 불가능할 것 입니다.

제가 개발한 이러한 공격 방법은 HEAT 이라고 불립니다.

Highly Evasive Adaptive Threats

HEAT 공격 방식!!


성공률은 높아지고 있지만 우리가 통과할 수 없는 한 회사가 있습니다.
뭐라고요? 보여주세요!


뭐라고요? 정말요?
만약 새로운 보안 시스템이라면,
우리가 다른 회사들이 이를 도입하기 전에 통과해야합니다.

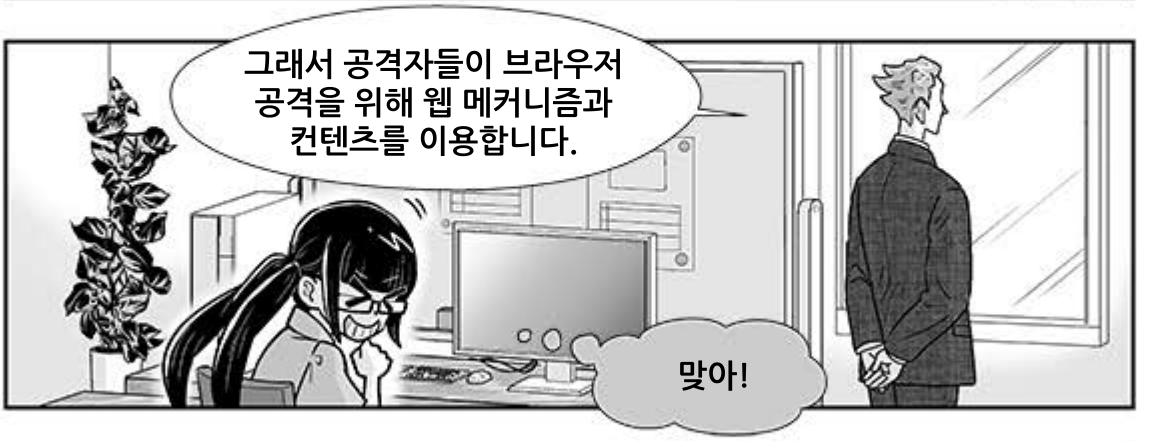

제가 이 회사의 보안스택을 분석해 보겠습니다.
히트, 위험을 감수하고 싶은게 확실합니까?


괜찮습니다!
제가 가서 발견하여 돌아올게요.
히트님 매우 멋지다…


安全ファースト株式会社
내가 유일하게 공격에 실패한 회사 보안 팀에 들어왔다.


아담
보안 담당자
히트님, 우리 회사에 처음이신데,
요즘 보안은 대부분 네트워크를 통해 이루어지는 것 아시죠?
네
방화벽, IPS, URL필터링, 백신, 샌드박스…
여러가지가 있는데요,
이런 보안 솔루션이 공격을 막을 수 있는 이유는
네트워크를 통해 들어오는 데이터를 분석 하기 때문입니다.
그게 무슨 뜻이죠?
예를 들어, 그것들이 좋은지 나쁜지 확인하기 위해 트래픽에서 파일을 가져오고,
신호들을 체크하고,
가상 장치를 통해 실행시켜보는 겁니다.
하지만 파일을 추출할 수 없다면, 분석도 할 수 없습니다.
또한 추출할 수 있더라도, 무해한 파일인지 유해한 파일인지 판단하는데 실수할 수 있습니다.
OK
NG
그러면 공격이 들어오고 데미지를 입히게 되죠. 그것이 현실입니다.
맞아, 그게 우리가 공격한 방식이야!
최근 뉴스에서 이런걸 볼 수 있죠.
큰 회사들조차도 랜섬웨어 공격을 당하고 있어요.
회사 A, B, C…모두 우리가 공격한 회사들이군!


오늘날 대부분의 공격은 브라우저를 통해 발생하지 네트워크로 발생하지 않습니다.
セキュアWEBゲートウェイ
URLフィルタ
アンチウイルス
サンドボックス
TLSインスペクション
WWW
최근 클라우드 서비스가 원격 근무와 함께 점점 더 많이 사용되고 있습니다.
그래서 직원들이 앱와 데이터를 이용해 어디서든지 클라우드에 액세스 할 수 있죠.
클라우드
APP
브라우저에서 앱과 데이터 실행하기


그래서 공격자들이 브라우저 공격을 위해 웹 메커니즘과 컨텐츠를 이용합니다.
맞아!

따라서, 네트워크가 아닌 브라우저를 통해 공격을 확인함으로써

유해한지 무해한지 판단하는 부분을 건너뛸 수 있습니다.

네? 브라우저를 통해 확인한다는게 무슨 뜻이죠?

설명해드릴게요… 컴퓨터와 인터넷 사이에 프록시 서버가 설치됩니다.

모든 컨텐츠가 실행되고

있고 유해 여부와 관계없이

오직 안전한 컨텐츠만이브라우저에 전달 됩니다.


이를 통해, 프록시 서버는 대상 브라우저에 어떤 일이 일어날지 탐지할 수 있습니다.
그리고 오직 격리된 안전한 자료만이 대상 브라우저에 도달할 수 있기때문에,
SECURITY
이 사람, 말이 많네…
절대! 랜섬웨어에 감염되지 않는다는 것을 의미합니다.
파일이 의미없는 데이터로 쪼개지고 난독화되어도,
프록시 브라우저는 여전히 파일을 볼 수 있습니다.
안돼…
그래서어떤 루트를 통해 링크가 전송되었는 지는 상관없고 결국 프록시 브라우저에 의해 열리게 됩니다.
좋죠? 네트워크에서는 이걸 볼 수 없습니다.
현재 보안 시스템은 탐지하고, 정지시키는 것만 할 수 있지만, 그것만으로는 충분하지 않습니다.
뭔가 새로운 것이 실행되어야만 해요.
우리 보안 솔루션은 이걸 할 수 있습니다.
오 안돼!


이것이 바로 Menlo Security의 격리 기술입니다!
MENLO
SECURITY
알겠나요? 천재 소녀 해커 히트씨?
눈치를 채고있었군…
HEAT 공격이 사라졌군..
히트씨, 얼른 돌아와주세요!
요즘 더 많은 회사들이 해킹 공격을 막을 수 있게 되었습니다.

MENLO SECURITY

メンロ・セキュリティ・ジャパン株式会社

〒100-0004 東京都千代田区大手町1-6-1 大手町ビル4階 FINOLAB
www.menlosecurity.jp

お問い合わせ