EFF

멀웨어

자세한 내용은: SEC.EFF.ORG
프로젝트THE ELECTRONIC FRONTIER FOUNDATION

악성 소프트웨어의 약자인 **멀웨어**는 기기에서 원치 않는 동작을 수행하도록 설계된 프로그램입니다.
멀웨어의 예는 다음과 같습니다:

- 컴퓨터 바이러스
- 비밀번호를 훔치는 프로그램
- 비밀리에 당신을 기록하는 프로그램
- 비밀리에 데이터를 삭제하는 프로그램

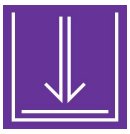
피싱을 통한 악성 코드

피싱은 공격자가 무해해 보이지만 실제로는 악의적인 메시지, 전자 메일 또는 링크를 공격자가 보내는 경우입니다. 피싱은 종종 알고있는 사람을 사칭하거나 신뢰하는 플랫폼을 사칭하는 것과 관련이 있습니다.
참고 : 모든 피싱에 멀웨어가 포함 된 것은 아닙니다. 때때로 공격자는 서비스에 대한 암호 탈취를 원하며, 상황에 따라 공격자는 사용자의 장치에 멀웨어를 설치하지 않고도 웹 사이트를 가장하는 방식으로 암호를 훔칠 수 있습니다.

멀웨어가 설치되는 일반적인 방법

악성 첨부 파일 또는 파일 열기
악성 첨부 파일은 종종 피싱 메시지에서 포함되어 있습니다.

악성 링크 클릭
악성 링크는 종종 피싱 메시지에 포함되어 있습니다.



라이센스가없는 소프트웨어 다운로드
보안 업데이트를받을 수없는 소프트웨어는 위험을 증가 시킵니다 (예 : Apple App Store 또는 Google Play Store가 아닌 불법경로).

손상된 웹사이트 방문
때로는 해킹된 웹사이트가 악성 콘텐츠를 배포하는 데 사용됩니다.

자동 컨텐츠 다운로드
공격자는 네트워크에 액세스 할 수 있으며 이 네트워크를 사용하여 멀웨어를 유포 할 수 있습니다.

USB 장치 공유 또는 의심스러운 포트에 연결카페, 공항 등에 있는 충전기 또는 포트를 통해서도 멀웨어 감염이 가능합니다.

악성 코드 유형

애드웨어
어디에나 있는 광고

이 악성 소프트웨어는 일반적으로 팝업폭탄 또는 기타 방법을 통해 사용자에게 광고를 표시하려고 시도합니다. 일부 애드웨어는 사용자 정보를 추적하거나 개인 정보를 추출합니다. 애드웨어는 다른 멀웨어와 마찬가지로 다른 소프트웨어와 함께 번들로 제공 될 수 있으며, 종종 공식 앱 스토어처럼 인증된 곳이 아닌, 소스를 알 수 없거나 신뢰할 수 없는 사이트에서 다운로드 될 수 있습니다.

스토커웨어
기기가 스토커를 도울 때

스토커웨어는 자동으로 실행되며 공격자가 기기를 완전히 제어 할 수 있습니다. 스토커웨어는 누군가가 귀하의 기기(예 : 가족이나 파트너와 같은사람에게 “휴대전화를 잠시 동안 빌려서 사용할 수 있을까요?" 라며 접근)에 물리적으로 접근하여 스토커웨어 앱을 설치하거나, 또는 사용자가 앱을 다운로드 하도록 속이는 경우 설치 될 수 있습니다.

트로이 목마
선물로 위장한 공격

트로이 목마 소프트웨어를 다운로드하면 합법적인 응용 프로그램처럼 작동 할 수 있지만, 실제로는 백그라운드에서 악의적인 작업을 수행합니다. 이것은 종종 불법 복제 소프트웨어, 또는 "해적판"소프트웨어 또는 가짜 바이러스 백신 소프트웨어에서 발견됩니다.

랜섬웨어
당신을 인질로 삼는 공격

이 악성 소프트웨어는 다운로드된 컴퓨터에 저장되어 있는 회사, 조직 또는 개인 데이터를 인질로 삼아 보상을 요구합니다. 랜섬웨어는 지난 10 년 동안 인기를 얻었으며 현재 전 세계의 공격자들을 위한 수백만 달러 규모의 비즈니스입니다.

A.P.T. 공격
고급 지속적 위협

A.P.T. 공격은 주로 정교한 역량을 바탕으로 목표 달성 (시스템 손상 등)에 전념하기 위해 실질적으로 더 많은 자원과 기술을 가진 공격자들의 멀웨어입니다. A.P.T. 공격은 종종 그들이 목표로하는 시스템에 대한 지속적이고 장기적 접근을 유지하려고 시도하는 국가 활동세력에 의해 사용됩니다.

EFF

보호

자세한 내용은: SEC.EFF.ORG
프로젝트 THE ELECTRONIC FRONTIER FOUNDATION

멀웨어 방어를 위한 5 가지 팁

팁 # 1 : 소프트웨어 업데이트

(& 라이센스가있는 소프트웨어를 사용하고 있는지 확인하십시오)

대부분의 멀웨어는 알려진 취약점을 이용합니다. 소프트웨어 회사는 종종 이러한 취약점을 해결하고 업데이트를 통해 사용자에게 제공합니다.

따라서 소프트웨어 업데이트는 공격자가 사용할 수 있는 알려진 취약성을 해결하는 가장 확실한 방법이므로 사용자 기기 보안에중요합니다.

*** 라이센스가 부여 된 소프트웨어를 얻는 방법을 잘 모를 경우 친근한 디지털 보안 담당자에게 유용한 정보와 리소스를 요청하십시오.**

팁 # 2 : 미래를위한 백업

장치를 잃어버린 경우 (악성코드 감염, 도난 또는 장치가 켜져 있지 않은 경우)에도 모두 손실되지 않게 하기 위해서, 오늘과 미래의 데이터를 백업하십시오. 강력한 비밀번호와 암호화를 사용하여 백업을 보호하십시오.

팁 # 3 : 클릭하기 전에 일단 멈춤

링크 및 파일 공유는 일반적인 행위이지만 링크를 받거나 공유 할 때는 항상 주의하십시오. 클릭하기 전에 질문하십시오. 이상한 점은 없습니까?

다음과 같은 경우를 조심하십시오:

- ***단축 링크***
  - 링크와 이메일은 컴퓨터에서 볼 때 보다 모바일 기기에서 볼 때 더 짧게 미리 볼 수 있습니다. bit.ly 및 유사한 서비스와 같은 링크 단축기는악의적인 사이트로 연결시킬 수 있습니다.
    팁 : https://unshorten.it와 같은 서비스를 사용하여 전체 확장URL을 확인하십시오!
- ***사칭은 속임수의 가장 좋은 유형입니다***
  - 오타, 비슷한 문자 및 복사된 브랜드 사칭이 당신을 속이려고합니다. 실제 서비스인지 확인하십시오.
    팁 : 공식 서비스를 사용하는 경우 즐겨찾기를 사용하면 합법적인 웹사이트 주소를 컴퓨터가 쉽게 기억할 수 있습니다.

    팁 : 비밀번호 관리 프로그램에 올바른 링크를 저장하십시오. 비밀번호 관리 프로그램은 지정된 사이트를 기억하고 비밀번호를 저장할 수 있습니다.
  - 친구인 척하는 사람으로부터 메시지를받는 것과 같이 “사회 공학적 해킹시도”에 주의하십시오.
    팁 : 다른 형태의 연락을 통해 친구에게 연락해서 실제로 친구인지 확인하십시오.
- ***우연한 클릭***
  - 장치에서 링크를 검사 할 때 한 번의 터치 또는 클릭으로 실수로 링크가 열릴 수 있습니다!
    팁 : 마우스를 사용하는 경우 호버링 (hovering: 마우스 커서를 이미지나 링크에 올려만 놓고 클릭하지 않는 것)을 활용하여 전체 링크를 보십시오.

팁 # 4 : 신체적 접근에 주의하십시오

때때로 우리의 적들은 우리가 아는 사람들이거나, 또는 우리가 주의를 기울이지 않을 때 장치에 액세스 할 수있는 사람들입니다. 전체 디스크 암호화 및 강력한 암호를 사용하여 장치를 보호하면 원하지 않는 물리적 액세스로부터 장치를 보호 할수 있습니다. 잠금 해제 된 장치를 다른 사람에게 대여 할 때는 주의하십시오. 자세한 내용은 ssd.eff.org를 확인하십시오.

팁 # 5 : 바이러스 백신 사용

모든 바이러스 백신이 동일한 것은 아닙니다. 안티 바이러스로 판매되는 일부 소프트웨어는 위장된 멀웨어 일 수 있습니다. 기기 제조업체의 바이러스 백신을 사용하는것이 좋을수도 있습니다. 타사 바이러스 백신 소프트웨어를 선호하는 경우 다음을 확인하십시오.

- 소프트웨어에 대한 독립적인 검토
- 바이러스 백신 웹 사이트에 멀웨어 유형 및 당신이 관심있는 악성 프로그램 유형에 대한 최신 멀웨어 목록 * 이 있는지 여부 확인

*** 공개 된 연구에 따르면 바이러스 백신 팀에 이러한 유형의 멀웨어를 방어하는 활성 팀이 있음을 알 수 있습니다**

악성 코드가 있다고 생각합니다. 어떻게 해야합니까?

기기에 이상한 일이 있습니까? 소셜 미디어와 같은 특정 계정입니까, 아니면 전체 장치입니까? 멀웨어처럼 보이는 경우 나중에 감염된 기기를 어떻게 사용하고 휴대하는 것을 주의하십시오. 그런 다음 다른 기기*를 사용하여 전문가에게 도움을 요청하십시오.

***멀웨어의 영향을받는 장치에 연결되지 않은 장치 예를 들어 도서관의 공용 컴퓨터 또는 신뢰할 수 있는 친구의 휴대전화 일 수 있습니다.**

신뢰할 수 있는 기술자에게 문의하십시오

원래 형식으로받은 이상한 메시지와 같은 기록을 보존하시길 바랍니다 (예 : 이메일인 경우 원본 이메일을 스크린샷이 아닌 헤더 메타 데이터와 함께 전달). 또한 세부 사항을 포함한 정보들 (예 : 날짜, 시간 및 설명) 을 신뢰할 수 있는 기술자에게 보내십시오.

피해 평가

어떤 민감한 정보가 손상되었을 수 있습니까? 비밀번호 나 계정을 변경해야합니까? 리스크평가 (일명“위협 모델링”)를 수행하여 다음 안전 단계를 계획하십시오 .

추가자료 읽기

SEC.EFF.ORG > SECURITY EDUCATION 101
Software updates and why they’re important

SSD.EFF.ORG:
How do I protect myself against malware
How to avoid phishing attacks