

1. 기사 내용

제목	암호화폐 노리는 사이버 공격자들, 최근 웹 인젝트 사용 시작
기사 날짜	2018년 3월 23일
스크랩 담당자	손우규
요약	<ul style="list-style-type: none">• 웹 인젝트로 암호화폐 관련 웹사이트 변경시켜 로그인 정보 탈취• 암호화폐 훔치기 위한 각종 공격 기법 앞으로 계속 등장할 것 <p>사이버 범죄자들이 여러 가지 방법을 동원해 지금의 암호화폐 열풍을 누리고 있다. 그 중 하나는 웹 인젝트(Web inject)를 사용해 사용자의 브라우저와 암호화폐 거래소 사이트 사이의 트래픽을 가로채 조작하는 것이다. 이렇게 함으로써 코인을 훔쳐 자신들의 계좌로 옮길 수 있게 된다.</p> <p>코소반은 "웹 인젝트는 그 자체로 하나의 멀웨어가 아니며 '서비스'이기 때문에 다양한 멀웨어에 접목되어 사용될 수 있다"고 설명한다. "제우스(Zeus)와 램닛(Ramnit)과 특히 많이 결합되고 있다. 하지만 이 둘은 수많은 예시 중 하나일 뿐이다. 사실 어떤 멀웨어를 운영하는 자라도 웹 인젝트를 사용하는 데 제한이 없다."</p>
출처	http://www.boannews.com/media/view.asp?idx=67804&kind=1&search=title&find=%BE%CF%C8%A3%C8%AD%C6%F3+%B3%EB%B8%AE%B4%C2+%BB%E7%C0%CC%B9%F6+%B0%F8%B0%DD%C0%DA%B5%E9%2C+%C3%D6

2. 용어

용어	설명
웹 인젝트(Web inject)	사용자의 브라우저에 페이지가 만들어지기 전에 악성 콘텐츠를 웹 페이지 내에 주입시키는 코드
맬웨어	맬웨어는 "악성 소프트웨어 (malicious software)"의 줄임말이다. 맬웨어는 사용자의 적절한 동의 없이 설치된 모든 종류의 원치 않는 소프트웨어를 말한다. 바이러스와 웜, 트로이 목마는 통칭하여 맬웨어로 부르는 악성 소프트웨어의 예이다.

3. 관련 기술(맬 웨어)

3.1 개요

맬웨어는 정상적인 작동을 방해하거나 사용자의 컴퓨터, 휴대폰, 태블릿 또는 기타 디바이스를 감염시키도록 설계된 악성 코드를 총칭하는 이름이다. 웜, 트로이 목마, 스파이웨어, 키로거 등 다양한 카테고리로 나뉜다. 이런 용어들은 주로 혼용되며, 늘어가는 멀웨어 변형에 서로 다른 기법이 결합되어 사용되고 있다.

현재 알려진 멀웨어의 대부분은 멀웨어 제작자의 경제적 이득이 주 목적이다. 멀웨어 공격은 사용자 이름, 암호, 신용 카드 세부 정보 또는 기타 금융 정보와 같이 대외비 데이터를 훔치는 방식으로 수행된다. 그런 다음 이런 민감한 정보는 개인과 기업에 추가적인 공격을 가하는 데 사용되거나 다른 악의적 공격자들에게 판매된다. 디바이스를 잠근 다음 암호화를 해제하려면 돈을 지불하라고 요구하는 멀웨어의 일종인 랜섬웨어는 금전적 이득을 취할 수단으로 점점 널리 악용되고 있다.



3.2 공격 형태

3.2.1 배포

멀웨어는 보안 시스템을 우회하고 탐지를 피하도록 설계되어 있기 때문에 보안 팀에서 사용자와 더 광범위한 비즈니스가 악영향을 받지 않도록 보장하기가 매우 어렵다. 멀웨어 제작자는 애매한 파일 이름 사용, 파일 특성 수정, 정상적인 프로그램 동작 모방, 프로세스 및 네트워크 연결 숨기기 등 다양한 방법으로 우회한다. 이와 같은 위장술과 회피 기법들은 엄청난 양의 새로운 멀웨어의 지원을 받고 있으며, 매일 390,000개의 새로운 변형 버전이 발견되는 것으로 추정된다.

디바이스를 감염시키는 멀웨어가 배포되는 방법은 매우 다양하며, 다음과 같은 방법을 예로 들 수 있다.

- 피싱 이메일에 첨부된 악성 파일 – 이메일은 소셜 엔지니어링 기법을 사용하므로 수신자가 첨부 파일을 열어볼 가능성이 높다. 열게 되면 멀웨어 코드가 전송된다.
- 이메일의 본문에 포함된 악성 URL 링크 – 이메일은 소셜 엔지니어링 기법을 사용하므로 수신자가 링크를 클릭할 가능성이 높다. 클릭하면 URL이 멀웨어 전송 사이트인 웹 페이지로 안내한다.
- 반자동 다운로드 – 사용자가 멀웨어 전송 사이트로 직접 이동하거나 악성 광고(malvertising)를 통해 해당 페이지로 리디렉션되는 경우 멀웨어 코드가 전송된다.
- 감염된 USB 디바이스.
- 경계 방화벽의 열린 포트를 악용하여 직접 네트워크 침투.
- 디바이스의 운영 체제 또는 설치된 애플리케이션의 취약점 – 예를 들어, 사용자의 브라우저에 있는 오래되거나 잘못 구성된 플래시 플러그인을 활용한다. 감염된 웹사이트는 사용자가 해당 페이지에 접속하자마자 사용자 디바이스에서 이런 취약점을 스캔하도록 설계될 수 있다. 이런 페이지의 멀웨어는 어떤 취약점을 활용할 수 있는지 식별한 후 찾아낸 취약점을 악용하여 특정 멀웨어 코드를 전송한다.

3.2.2 스파이웨어

탐색 활동을 추적하고 개인 또는 기업에 관한 정보를 수집합니다. 이와 같이 수집된 정보를 향후 악의적 사용을 위해 다른 사람에게 보내거나 사용자가 모르는 사이에 디바이스의 제어 기능을 장악합니다.

3.2.3 키로거

사용자의 키보드 입력을 기록하여 사용자 이름, 암호 및 다른 민감한 정보를 알아냅니다. 이 정보는 주로 사이버 범죄자들의 추가적인 악의적 공격에 사용됩니다.

3.2.4 트로이 목마

데이터의 유출, 삭제, 차단, 수정뿐만 아니라 디바이스 또는 네트워크 성능 저하 목적으로 정상적인 소프트웨어로 가장하여 사용자 시스템을 염탐하거나 접속 권한을 가로챍니다. 트로이 목마는 감염된 디바이스의 전체 원격 제어 기능을 사이버 범죄자에게 제공하는 백도어 트로이 목마, 디바이스를 봇넷에 통합한 후 DOS 공격을 감행하는 데 사용되는 트로이 목마-DDoS, 스팸 이메일 공격에 디바이스를 사용하는 이메일 트로이 목마 등 다양한 유형이 있습니다.

3.2.5 웜

네트워크 연결을 통해 한 디바이스, 드라이브 또는 네트워크 자체를 다른 동일 요소로 복제합니다. 웜은 사람이 시작하지 않아도 자동으로 확산되고 스스로 복제할 뿐 아니라 대역폭을 소비하고 웹 서버에 과부하를 일으킵니다.



3.2.6 루트키트

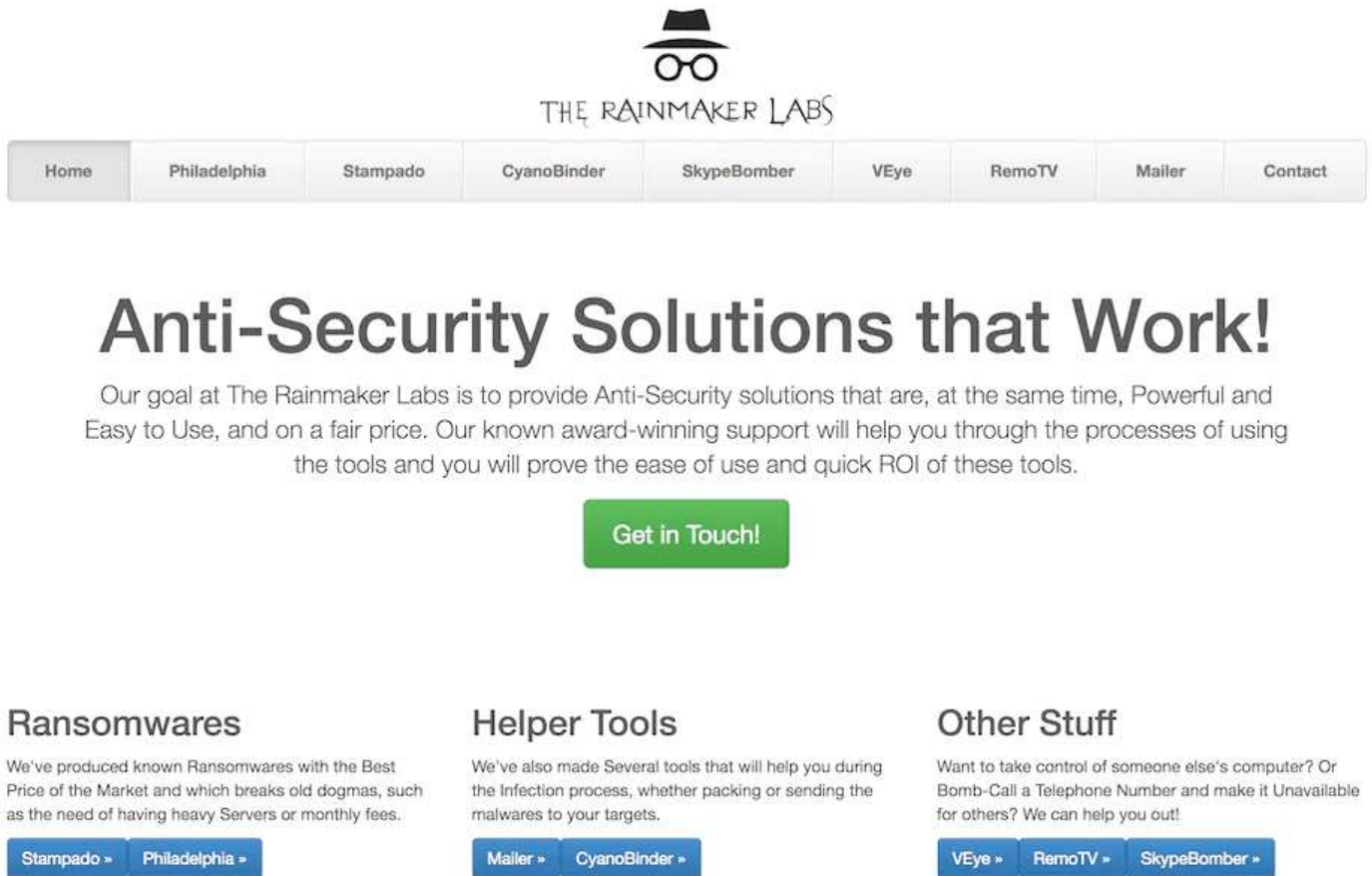
디바이스의 원격 관리 기능을 장악하도록 설계되어 있습니다. 일단 설치되면, 루트키트(Rootkit)를 조종하는 악의적 공격자들이 디바이스에서 수행되는 모든 작업을 추적하고, 파일을 실행하고, 프로그램 및 추가적인 멀웨어를 설치하고, 안티바이러스 프로그램과 같은 소프트웨어를 수정할 수 있습니다. 루트키트는 탐지와 제거가 불가능한 멀웨어로 악명이 높습니다.

3.2.7 랜섬웨어

사용자 디바이스 또는 네트워크 스토리지 디바이스의 파일을 암호화합니다. 암호화된 파일에 대한 접속 권한을 복구하려면 사용자가 일반적으로 추적이 어려운 비트코인과 같은 전자 결제 방식을 통해 '랜섬(몸값)'을 사이버 범죄자에게 지불해야 합니다.

3.3 공격 원인

불과 몇 년 전까지만 해도, 사이버 범죄자들은 소프트웨어 엔지니어링, 보안 및 네트워킹과 관련된 해박한 지식이 있어야만 멀웨어 공격을 가할 수 있었다. 그러나 악의적 공격자들이 단지 39달러만 지불하면 멀웨어를 구축·배치하거나 경제적 수단으로 이용할 수 있는 전체 에코시스템이 발전하게 되었다. 실제로 MaaS(Malware-as-a-Service)와 RaaS(Ransomware-as-a-Service)는 이미 저렴한 가격에 구입하고 다운로드할 수 있으며 주요 사이트에서 버젓이 광고되고 있다. 일례로 다양한 MaaS 옵션을 판매 중인 웹사이트가 아래에 있다.



The Rainmaker Labs website features a navigation bar with links to Home, Philadelphia, Stampado, CyanoBinder, SkypeBomber, VEye, RemoTV, Mailer, and Contact. The main heading is "Anti-Security Solutions that Work!". Below this, a paragraph states: "Our goal at The Rainmaker Labs is to provide Anti-Security solutions that are, at the same time, Powerful and Easy to Use, and on a fair price. Our known award-winning support will help you through the processes of using the tools and you will prove the ease of use and quick ROI of these tools." A green button labeled "Get in Touch!" is positioned below the text. The website is divided into three sections: "Ransomwares" (featuring Stampado and Philadelphia), "Helper Tools" (featuring Mailer and CyanoBinder), and "Other Stuff" (featuring VEye, RemoTV, and SkypeBomber). Each section includes a brief description of the services offered.

3.4 보완 방법(해결방안)

3.4.1 취약점 교육

대부분의 멀웨어는 페이로드를 활성화할 수 있는 사람을 필요로 한다. 직원들에게 사이버 공격을 인지하고 방어하는 방법을 교육하는 것이 중요하다. 다수의 공격들은 이메일 및 소셜 엔지니어링 기법을 통해 직원을 속여 멀웨어를 다운로드하거나 사용자 이름 및 암호를 유출하도록 유도한다. 따라서 이런 공통 공격 벡터에 주안점을 두고 교육을 진행해야 한다. 직원들에게 가짜 피싱 이메일을 보내 연습을 시키면 제목 줄에 '송장 첨부 - 반드시 열어서 확인 요망'이라는 제목의 피싱 이메일과 진짜 공급업체와의 커뮤니케이션 이메일을 구분하는 데 효과가 있다.

3.4.2 패치 적용

최근 WannaCry 및 Petya 공격에서 알 수 있듯, 알려진 취약점의 패치를 적용하는 적극적 대응에 나서지 못하면 기업이 위험에 노출된 상태로 유지될 수밖에 없다. WannaCry 및 NotPetya 공격에서 EternalBlue 취약점이 악용된 지 몇 달이 지난 후에도 3,800만 대 이상의 PC에 패치가 아직 적용되지 않은 것으로 추측된다. 사이버 범죄자가 기업 네트워크에서 패치가 적용되지 않은 디바이스 및 소프트웨어를 식별하는 것은 상대적으로 간단하며, 일단 식별되면 알려진 취약점을 쉽게 활용할 수 있다.



3.4.3 데이터 백업

누군가에게 이 지침은 말할 필요도 없겠지만, 멀웨어는 네트워크 서버에 저장된 백업을 암호화할 수 있다. 따라서 기업은 백업과 관련된 현재 접근 방식을 검토해야 한다. 직원들이 중요한 파일을 네트워크 드라이브에 백업하고 있는가? 이런 디바이스의 백업과 파일 서버가 그 이후에 클라우드 백업 서버에 보관되는가? 백업을 복원할 수 있는지 테스트하고 있는가? 이 방식에서는 멀웨어가 모든 로컬 파일 및 백업을 암호화하는 경우에도 비즈니스에 최소한의 영향을 주면서 신속하게 복원할 수 있다.

3.4.4 방어 레이어 구축

사이버 범죄자들은 회사의 보안 방어막을 우회하도록 설계된 보다 교묘한 형태의 첨단 멀웨어를 개발하는 데 막대한 시간과 돈을 들인다. 단일 보안 레이어만으로 빠르게 발전하는 공격에 대비하는 것은 무모하다고 할 수 있다. 여러 보안 레이어를 사용하면, 한 레이어에서 공격을 방어하지 못해도 위협을 차단할 수 있는 다른 오버레이가 있기 때문에 훨씬 안전하다. 그렇다면, 지금 회사는 어떤 보안 방어 레이어를 배포했는가? 공격의 모든 단계에서 리스크를 차단하도록 지원하는 서로 다른 솔루션을 구비하고 있는가? 악의적 공격자들이 악용할 수 있는 취약점이 보안 환경에 존재하는가?

4. 참고 자료

- https://ko.wikipedia.org/wiki/SQL_%EC%82%BD%EC%9E%85