Free Thanatos Ransomware Decryption Tool Released

2018. 06. 26

https://thehackernews.com/2018/06/free-ransomware-decryption-tools.html

[기사 요약]

시스코의 보안 연구원은 Thanatos Ransomware 분석 후 코드의 허점을 발견하여 피해자가 감염되어 있는 상태에서 돈을 지불하지 않고 파일을 무료로 복호화 할 수 있는 도구를 개발하였습니다. 이 도구는 ThanatosDecryptor 라고 불리며 오픈소스이고 GitHub 웹사이트에서 다운로드 할 수 있으며, Thanatos Ransomware 버전 1이나 1.1에서만 작동됩니다. Thanatos에서 사용된 암호화 키는 시스템이 마지막으로 부팅된 후 밀리초 단위로 파생되고 있습니다. 연구원은 이를 리버싱하여 무차별 대입이나 Windows 이벤트 로그를 사용하여 동일한 32비트 암호화 키를 성공적으로 복구하는 14분이 걸렸습니다. 또한 대부분의 랜섬웨어는 피싱 전자메일, 웹 사이트의 악의적인 광고나 타사 응용 프로그램을 통해 전파되는데 이러한 랜섬웨어를 막기 위해서는 이메일로 보내지는 초대받지 않은 문서를 항상 의심해야하며 내용을 확인하지 않는 한 해당 문서 내의 링크를 클릭해서는 안됩니다.

[기술적인 내용]

- 타나토스 랜섬웨어 : 시스템에 침투해 파일을 암호화하면서 Thanatos 라는 확장자를 덧붙이며, 암호화가 끝난 후에는 특정 URL에 경과를 보고합니다. 그러므로 공격자들은 피해자의 수가 얼마나 되는지, 암호화가 어느 만큼 진행되었는지를 알 수 있게 됩니다. 또한
- 피싱 : fishing에서 유래하였으며 private data와 fishing의 합성어로 사용자의 금융 정보와 패스워드를 낚는다는데서 유래되었으며 온라인 신원 도용의 한 종류 입니다. 피싱 사기는 메일과 사기 웹 사이트를 이용하여 신용카드 번호, 암호, 계정 데이터, 그 밖의 정보 등 개인 데이터나 정보를 훔치는 범죄입니다.
- - Windwos Event Log : 윈도우의 운용과정에서 발생하는 동작(이벤트)을 체계적으로 기록한 바이너리 로깅 시스템입니다. 시스템 방화벽, 응용 프로그램 관리 등에 관한 로그를 텍스 트 형태로 기록하고 있지만, 이벤트 로그에서는 시스템의 전반적인 동작을 보다 종합적이 고 체계적으로 기록합니다.

Two Zero-Day Exploits Found After Someone Uploaded 'Unarmed' PoC to VirusTotal

2018. 07. 02

https://thehackernews.com/2018/07/windows-adobe-zero-exploit.html

[기사 요약]

Microsoft의 보안 연구원들이 악의적인 PDF파일을 VirusTota에 업로드한 후 최근에 발견된 두가지 중요한 제로 데이 취약점에 대한 세부 정보를 공개했습니다. 두 가지 취약점에 대한 패치가 5월 둘째 주에 릴리즈 되었으므로 사용자에게 취약점을 업데이트할 수 있는 충분한 시간을 제공한 후 취약점에 대한 세부 사항을 발표했습니다. 문제의 제로데이 취약점은 AdobeAcrobat Reader(CVE-2018-4990)의 원격 코드 실행 결함과 Microsoft Windows의 권한 상승 버그 (CVE-2018-8120)입니다.

첫번째 공격은 AdobeJavaScript 엔진을 공격하여 해당 모듈의 컨텍스트에서 쉘을 실행합니다. Windows 10과 같은 최신 플랫폼에 영향을 미치지 않는 두번째 익스플로잇은 쉘코드가 Adobe Reader 샌드 박스를 벗어나고 Windows 커널 메모리의 상승된 권한으로 실행되도록 합니다.

샘플에는 최종 페이로드가 포함되어 있지 않으므로 초기 개발 단계에서 발견되었습니다. 샘플에 실제 악성 최종 페이로드가 포함되어 있지는 않지만 작성자는 취약점 검색 및 쓰기에 있어 높은 수준의 기술을 보여주었습니다. Microsoft와 Adobe는 5월에 두 가지 취약점에 대한 해당 보안 업데이트를 발표했습니다.

[기술적인 내용]

- CVE-2018-4990 : Adobe Acrobat 및 Reader에서 발생하는 취약점 중의 하나로 임의 코드 실행으로 이어질 수 있는 Double Free 취약점
- CVE-2018-8120 : Win32k 구성 요소가 메모리 객체를 제대로 처리하지 못해 발생하는 권한 상승 취약점
- Adobe Acrobat 및 Reader 익스플로잇은 PDF 문서에 JavaScript 악성 스크립트가 포함된 악의적으로 제작된 JPEG2000 이미지로 통합되어 쉘 코드를 실행하는 소프트웨어에서 Double-Free 취약점을 유발합니다.
- 공격자는 첫 번째 취약점으로부터 쉘 코드 실행을 활용하여 두 번째 Windows 커널 취약점 Exploit을 사용하여 AdobeReader 샌드박스를 중단하고 권한 상승을 하여 실행합니다.
- Double Free : Free를 두번 할 때 발생하는 버그로 free() 함수가 수행되는 과정 중 unlink라는 매크로에 의해 발생합니다.

Beware! Fortnite Cheat Hijacks Gamers' PCs to Intercept HTTPS Traffic

2018.07.03

https://thehackernews.com/2018/07/fortnite-v-bucks-cheat.html

[기사 요약]

Rainway(이하 레인웨이)라는 웹기반의 게임 스트리밍 사이트에서 공격자에 의해 포트나이트(FPS 게임) 플레이어의 HTTPS 웹 세션을 가로채어 방문하는 모든 대상에게 멀웨어를 감염 시켰습니다. 레인웨이의 CEO인 Andrew Sampson이 게시한 블로그에 따르면 지난주 서버 로그에 수십만 개의 오류보고가 나왔고 사용자를 공격하는 에드웨어는 모두 포트나이트를 사용하고 있었습니다. 또한 악성 에드웨어는 유튜브 광고를 통해 포트나이트 가짜 해킹툴, 에임봇 등을 설치하게 유도했는데 OS중 윈도우에서만 영향을 받고 있었습니다. 멀웨어는 감염된 PC에는 루트인증서를 설치했으며 중간자 공격에 사용되는 멀웨어도 발견되었습니다. 이를 통해 암호화가 되어 있을지라도 네트워크 트래픽을 수정할 수 있습니다. 레인웨이는 멀웨어를 다루는 회사에 알리고 제거했으며 감염된 사용자에게는 경고를 발송했으며 해킹도구나 치트를 사용하지 말도록 알렸습니다. 해결방법으로는 해킹도구나 치트 등을 사용하지 않으며 개발자가 제공하는 게임 외의 다운로드하면 안된다고 제시하였습니다

[기술적인 내용]

- Malware : 정상적인 작동을 방해하거나 사용자의 컴퓨터, 휴대폰, 태플릿 또는 기타 디바이스를 감염시키도록 설계된 악성코드를 총칭하는 이름
- Adware : 원래는 프로그램 실행 중 광고를 보여주고, 이를 봄으로써 비용 납부를 대신하는 형태의 프로그램
- 중간자 공격 : 네트워크 통신을 조작하여 통신 내용을 도청하거나 작하는 공격 기법, 많은 암호 프로토콜은 중간자 공격을 막기 위하여 인증을 사용합니다. 예를 들어 TLS/SSL 프로토콜은 공개 키를 기반으로 한 인증을 사용합니다.
- 루트 인증서 : 루트 인증 기관 (CA)에서 관리하는 공개 키 인증서나 자체 서명 인증시로 공개키 기반 계획의 일부입니다. 가장 상업적으로 공통되는 ITU-t X.509 표준형, 일반적으로 루트 인증기관(CA)에서 나온 디지털 서명을 포함합니다.

Beware! Fortnite Cheat Hijacks Gamers' PCs to Intercept HTTPS Traffic

2018.07.26.

https://thehackernews.com/2018/07/netspectre-remote-spectre-attack.html

[기사 요약]

대상 시스템에서 로컬 코드를 실행해야 하는 일반적인 Spectre 변형들과 달리 네트워크를 통해 공격이 가능한 새로운 Spectre 가 발견되었습니다. 이 공격은 bound check bypass 를 수행하기 위해 추측 실행을 악용하고 원격 시스템에서 ASLR 을 무력화하는데 사용될 수 있습니다. 투기적 실행은 현대 프로세서 설계의 핵심 구성 요소로 사실일 것으로 추정되는 가정을 기반으로 추측 실행합니다. 가정이 유효한 것으로 밝혀지면 실행은 계속되고 그렇지 않으면 폐기됩니다. 이 문제는 공격자가 암호, 암호화키 및 기타 중요한 정보를 포함하여 이전에 보안된 CPU 메모리에서 데이터를 추출하는데 악용될 수 있는 악의적인 코드를 작성하고 실행할 수 있게 합니다. 이 팀은 올 3 월 인텔에 이 취약점을 보고했으며, NewSpectre 공격은 투기 실행 설계 상의 초기 패치 세트 동안 인텔에 의해 수정되었습니다. 따라서 Spectre 공격을 완화하기 위해 코드와 어플리케이션을 이미 업데이트 한 경우 NetSpectre 공격에 대해 걱정할 필요가 없습니다. 올해 5 월 Microsoft 와 Google 의 보안 연구원은 Apple 에서 판매 한 컴퓨터를 포함하여 수백만 대의 컴퓨터에서 최신 CPU 에 영향을 미치는 Spectre Variant 4 를 보고했습니다 지금까지 Spectre 또는 Meltdown 변종이나 하위 변종을 악용 한 악성 코드는 발견되지 않았습니다.

[기술적인 내용]

- Spectre : Intel, ARM 및 AMD 프로세서에 존재하는 취약점으로, 프로세서로 하여금 실행해서는 안되는 코드를 실행하도록 유도해 다른 어플리케이션 메모리 공간에 존재하는 정보를 유출시킬 수 있는 취약점
- 추측 실행 : 프로그램의 논리 흐름상 실행여부가 불확실한 상태에서, 예측에 의하여 먼저 실행하는 기법, 성능의 최적화가 목적
- Bound Check Bypass : 예측 실행 기법에 있는 취약점을 이용하여 배열의 범위를 벗어난 값을 읽어내는 기법으로 이러한 해킹 기법 중에서 Cache Side Channel 기법이 자주 사용됨, 이 기법을 사용하면, 예측 실행의 내용이 폐기되더라도 예측 실행 과정에서 Cache의 상태가 어떻게 변했는지를 살펴보고 예측 실행 중에 읽은 값을 알아낼 수 있음
- Cache Side Channel 기법 : 메모리에서 어떤 값이 읽혀지면 그 내용은 Cache에 들어가게 되며 Cache에 들어간 값을 읽을 때는 그렇지 않은 값을 읽을 때보다 시간이 더 짧게 걸린다. 해커들은 이 읽기 시간의 차이를 악용하여 캐시 메모리의 저장된 정보를 확인할 수 있음