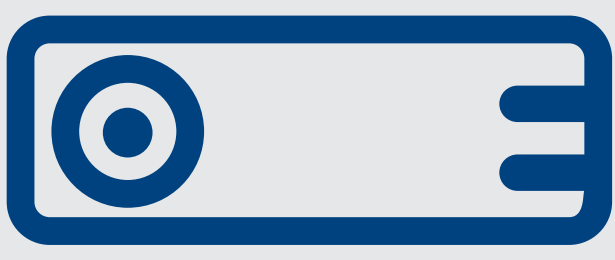
2015년 5월

위협 보고서

맥아피 연구소

하드 드라이브 펌웨어 익스플로잇

이퀘이션 그룹(Equation Group)의 악성코드는 하드 디스크와 SSD를 감염시키며 제거 또는 검출이 불가능합니다.



1단계
웹 기반 사이트 악용
사용자가 감염된 웹사이트를 방문합니다. 목표 시스템이 1단계 악성코드에 감염됩니다.

2단계
1단계 DoubleFantasy 설치/이식
목표를 확정하고 2단계 악성코드를 전달합니다.

3단계
2단계 EquationDrug/GrayFish 설치/이식
HDD/SSD 펌웨어 모듈의 설치 및 유지보수를 관리합니다.

4단계
HDD/SSD 펌웨어 모듈
펌웨어를 재프로그래밍하고 숨겨진 스토리지 영역을 관리합니다.

이퀘이션 그룹(Equation Group) HDD/SSD 공격 모듈:

- **강한 생존성:** 재프로그래밍된 펌웨어는 디스크 재포맷과 운영 체제 재설치 후에도 살아 남습니다.
- **확인 불가:** 숨겨진 스토리지 영역은 재프로그래밍된 펌웨어에만 인식되며 HDD/SSD 재포맷 후에도 존속합니다.
- **감지 불가:** 재프로그래밍된 펌웨어와 숨어있는 악성코드는 드라이브를 감염시킨 후 보안 소프트웨어에 의해 감지되지 않습니다.

맥아피 연구소에서는 이것을 지금까지 발견된 펌웨어 공격 중 가장 뚜렷하고 진일보한 예 중 하나로 간주하고 있습니다.

랜섬웨어의 귀환

새로운 랜섬웨어의 주도로 공격이 빠르게 증가하고 있습니다.

랜섬웨어는 갈수록 강력해지고 있습니다.

가상 화폐 사용
지불 비용에 대한 추적이 불가능합니다.

대량 저장 장치 표적 공격
가치가 큰 목표물이 증가하고 있습니다.

Tor 네트워크 이용
공격자들이 자신의 제어 서버 위치를 감출 수 있습니다.

모바일로 이동
피해자 수가 증가하고 있습니다.

맥아피 연구소의 조사 결과, 1분기에 랜섬웨어가 165%나 증가했는데, 주로 CTB-Locker의 것이었습니다. 이 것은 다른 어느 분기보다도 샘플 수가 거의 2배에 달하는 것입니다.

Adobe Flash 취약성

사용자들이 직접 패치가 힘든 취약 요소로 인해 공격이 급속도로 증가하고 있습니다.

인텔 시큐리티(Intel Security)가 본 Flash .swf 샘플 수

악성코드 개발자가 Adobe Flash를 공격 대상으로 삼는 이유는?

- Flash의 인기가 악성코드 개발자들의 주의를 끌고 있다.
- 사용자가 취약 요소를 없애줄 소프트웨어 패치 설치를 미루고 있다.
- 모바일 기기의 수가 가파르게 증가하고 있다.
- 새로운 Flash 악용 방법이 등장하고 있다.

317%

새로운 Flash .swf 샘플의 수는 2015년 1분기에 317%나 급증했습니다.

2015년 1분기에 새로운 Flash CVE가 42개 추가되었는데 이것은 2014년 4분기를 기준으로 50% 증가한 것입니다. 모두 Adobe가 제공한 것들입니다.

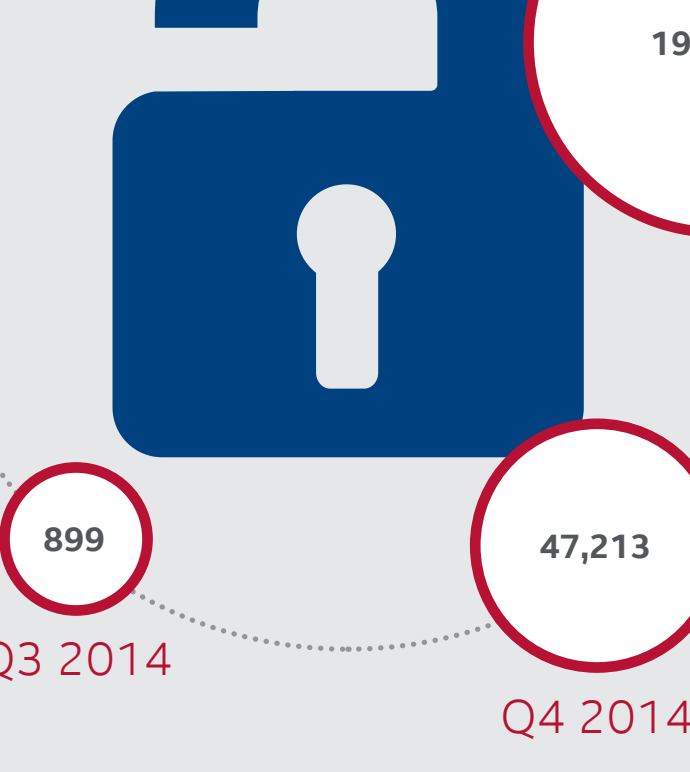
위협 통계

2015년 5월

1분에 362가지 위협이 새로 생겨나고 있는데, 1초에 6가지 이상이 새로 생겨나고 있는 셈입니다.

맥아피 연구소 악성코드 'zoo'는 2014년 4분기부터 2015년 1분기까지 13% 증가했습니다. 이제, 샘플 수만 해도 4억 개를 돌파했습니다.

새로운 모바일 악성코드 샘플의 수가 2014년 4분기부터 2015년 1분기까지의 기간 동안 49%나 급증했습니다.



전송된 스팸은 2015년 1분기에도 6조 건을 유지했습니다.

새로운 주의 대상 URL도 다시 급증하기 시작해 2014년 4분기부터 2015년 1분기까지 81%나 늘어났습니다.

맥아피 연구소 위협 보고서: 2015년 5월호

보고서 전문은 **www.mcafee.com/May2015ThreatsReport**에서 확인할 수 있습니다.

61955info_qtr-q1_0615_fnl_PAIR

McAfee는 현재 인텔시큐리티(Intel Security)에 통합되어 있습니다.