McAfee
Together is power.

위협 보고서

맥아피 연구소

악성코드의 회피 기법 및 추세

탐지 회피를 위한 악성코드 기법들은 광범위하게 사용되고 있으며 더 강력해지고 있습니다.

회피 기법의 역사

1980
Cascade 바이러스
콘텐츠를 스크램블하기 위해 암호화를 사용하는 최초의 바이러스

1990
Chameleon 바이러스
최초의 다형성 바이러스

1998
변형 악성코드
Regswap이 동일한 함수들에 여러 다른 레지스터를 사용해 변형

1990s
Packers
RAM과 디스크의 소형화로 인해 암호화 및 압축을 하는 패커스가 보편화됨

1999~2003
루트킷
1999년 최초의 윈도우 루트킷 NTRootkit 출현, 이어 2003년에는 HackerDefender 등장

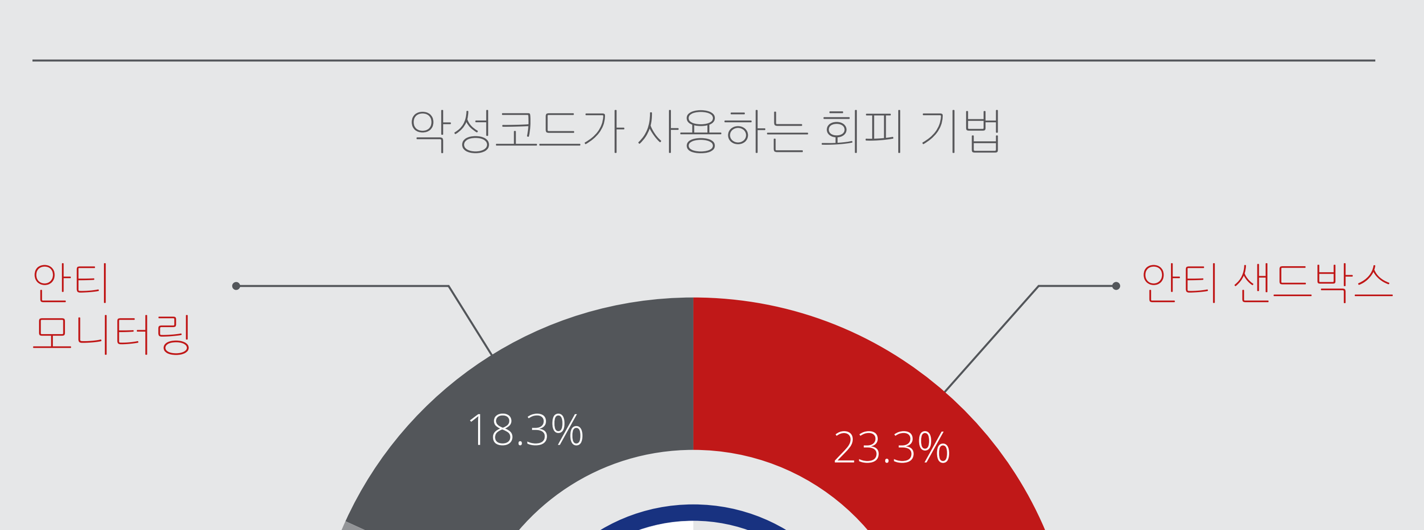
2008
도메인 생성 알고리즘 (DGA)
Conficker 웜이 네트워크 탐지 회피에 DGA 사용

2011
상용 악성코드 시장
회피형 악성코드 제품 및 서비스를 판매하는 최초의 다크넷 암시장 실크로드 등장

2015~2017
Dridex, Locky
최초의 대규모 난독화 악성코드로 PowerShell 사용, 샌드박스 회피

2015~2017
펌웨어 악성코드
Equation Group과 Hacking Team의 유출을 통해 탐지되지 않는 펌웨어 악성코드의 사용 사실이 밝혀짐

악성코드가 사용하는 회피 기법



회피
회피 기법 코드는 암시장에서 구매가 가능하며 무료로 얻을 수도 있습니다.

펌웨어
펌웨어 감염의 사용이 증가하고 있습니다.

머신 러닝
공격자들은 머신 러닝 보안을 회피하는 기법들을 개발하고 있습니다.

잘 보이는 곳에 숨기: 스테가노그래피의 숨겨진 위협

스테가노그래피 - 비밀을 숨기는 예술이자 과학

디지털 스테가노그래피 과정

1. 은닉 파일/숨겨진 메시지
2. 알고리즘 내장
3. 스테가노 그래피 파일
4. 통신 매체
5. 스테가노 그래피 파일
6. 알고리즘 추출
7. 숨겨진 메시지

악성코드에서의 디지털 스테가노그래피

2010 | 2012 | 2014 | 2016

- Duqu, Shady RAT, Alureon 루트킷
- Zbot, Lurk, ZeusVM, MiniDuke, CosmicDuke
- Vawtrak, Stegoloader, Sundown, AdGholas, Magento CC, DNSChanger

비밀 메시지
정상적으로 보이는 메시지 속에 비밀 메시지 숨김

440 BC
스테가노그래피는 약 기원 전 440부터 다양한 형태로 사용

2011
2011년 Duqu가 디지털 스테가노그래피 사용

네트워크
네트워크 스테가노그래피가 악성코드에 의해 사용되는 최신 디지털 스테가노그래피 유형

비밀번호 도둑 파레이트의 커지는 위험

비밀번호 탈취 기법은 거의 모든 공격의 초기 단계에서 사용됩니다. 파레이트가 2016년 미국 민주당 전당 대회 침해 사고에서 사용되었을 가능성이 높습니다.

파레이트의 진화

2011
- 인증 정보 탈취 및 DDoS 역량을 가진 최초의 파레이트 변종 출현

2012
- BHEK가 Zeus, FakeAV으로 파레이트 확산

2013
- 파레이트 Medfos, Nymaim, 스팸 공격으로 확산
- 파레이트 비트코인 마이닝 시작

2014
- Pony Loader 1.9 소스 코드 유출
- 비트코인 지갑 탈취가 가능한 포니 로더 2.0
- 화면 잠금 랜섬웨어 인증정보 탈취에 파레이트 사용

2015
- Pony Loader 2.0 소스 코드 유출
- 파레이트 DNS 포이즈닝 통해 확산
- DNC, Onion Duke로 공격 받음

2016
- 스테고로더를 통해 파레이트 인증정보 탈취 모듈 발견
- W97, PowerShell, JavaScript, MHT를 사용해 파레이트 확산
- 그리즐리 스텝 작전과 파레이트 관련

2017
- 많은 개별화된 포니 로더 변종 출시, 최신 버전 포니 로더 2.2

5,599
파레이트는 2011년 처음 발견되었으며, 지난해에만 5,599건의 파레이트 사고가 발생했습니다.

Fareit has several capabilities:
- 비밀번호 탈취
- 다른 악성코드 다운로드 및 실행
- DDoS 공격 수행
- 암호화된 화폐 지갑 강탈
- FTP 인증정보 탈취

위협 통계

1분기에는 1분에 244개, 1초에 4개 이상의 새로운 위협이 발견됐습니다.

사고 건수
1분기에는 301건의 보안 사고가 발생한 것으로 보고되었습니다. 지난 4분기 대비 53% 증가한 수치입니다. 보건, 공공 및 교육 분야가 50% 이상을 차지합니다. 1분기에 보고된 보안 사고의 78%는 미주에서 발생했습니다.

53%

악성코드 (22%)
1분기에는 새로운 악성코드 샘플이 3,200만 개로 증가했습니다. **악성코드의 총 샘플 수는 지난 4개 분기 대비 22% 증가한 6억 7,000만 개였습니다.**

Mac OS 악성코드 (53%)
윈도우 위협 대비 적은 수치지만 지난 3개 분기 동안 Mac OS 악성코드는 넘쳐나는 애드웨어로 인해 부쩍 늘었습니다.
총 Mac OS 악성코드 샘플 수는 1분기에 53% 증가했습니다.

모바일 악성코드 (79%)
1분기 아시아에서 보고된 모바일 악성코드 수는 두 배 증가해 세계적인 감염율 증가에 57% 기여를 했습니다. **총 모바일 악성코드 샘플은 지난 4개 분기 동안 79% 증가된 1,670만 개였습니다.**

매크로 악성코드 (66,000)
새로운 매크로 악성코드는 3년 평균으로 내려왔습니다. **1분기에는 6만 6,000개의 새로운 매크로 악성코드 샘플이 발견되었습니다.**

랜섬웨어 (59%)
1분기에는 새로운 랜섬웨어 샘플이 증가했습니다. Android OS 장치들에 대한 Congur 랜섬웨어 공격이 주원인입니다. **총 랜섬웨어 샘플 수는 960만 개로 지난 4개 분기 동안 59% 증가했습니다.**

McAfee Global Threat Intelligence

맥아피 GTI는 1분기 하루 평균 550억 건의 쿼리를 수신했습니다.

9,500만
중간 정도 위험의 URL에 대한 McAfee GTI 보호는 향상된 정확성 덕분에 **4분기에 1일 1억 700만 건에서 1분기에는 9,500만 건으로 감소했습니다.**

5,600만
잠재적으로 원치 않는 프로그램에 대한 McAfee GTI 보호는 **4분기에 1일 3,700만 건에서 1분기에는 5,600만 건으로 증가했습니다.**

McAfee GTI

3,400만
악성 파일에 대한 맥아피 GTI의 보호는 조기 악성코드 탐지와 더 효과적인 현지 인텔리전스 덕분에 **4분기에 1일 7,100만 건이었던 것이 1분기에는 3,400만 건으로 줄었습니다.**

5,900만
위험한 IP 주소에 대한 맥아피 GTI의 보호는 조기 탐지 덕분에 **4분기에 1일 8,800만 건이었던 것이 1분기에는 5,900만 건으로 줄었습니다.**

맥아피 연구소 위협 보고서: 2017년 6월호

www.mcafee.com/June2017ThreatsReport에서 보고서 전문을 확인할 수 있습니다.

McAfee
Together is power.

3181_0517_info-threat-report-malware-evasion_PAIR