마이크로소프트의 안티 멀웨어 연구 및 대응

멀웨어 예방 센터에 대한 소개

Microsoft®

마이크로소프트의 안티 멀웨어 연구 및 대응

멀웨어 예방 센터에 대한 소개

Microsoft®

마이크로소프트의 안티 멀웨어 연구 및 대응

이 문서에 들어 있는 정보는 발행 시점에 논의된 문제점에 대한 마이크로소프트사의 최근 견해를 소개하고 있으며 마이크로소프트가 시장 상황의 변화에 반드시 대처해야 하므로, 이 내용을 마이크로소프트사가 제시하는 약속사항으로 해석하지 말아야 하며, 발행일 이후에 제공된 어떠한 정보에 대해서도 마이크로소프트는 정확성을 보장하지 않습니다.

이는 단지 정보 제공만을 목적으로 하는 백서이며, 마이크로소프트는 이 문서에서 어떠한 명시적, 묵시적 보장도 하지 않습니다.

목 차

안티 멀웨어에 대한 전망

바이러스, 트로이 목마, 기타 악의적인 소프트웨어는 물론 스파이웨어와 원치 않는 소프트웨어들은 모두 IT 전문가들의 끊임없는 관심 대상입니다. 사회 공학 기법을 악용한 공격 방식들도 계속 증가해 가고 있으며, 각종 위협들도 시스템을 감염시키려는 시도에 있어서 갈수록 치밀해져 가고 있는 추세입니다. 공격자의 시야도 사용자로까지 확장되어, 간혹 재정 정보나 기타 기밀 정보를 훔치려는 경우마저 있습니다. 따라서 이처럼 빠르게 변하는 멀웨어의 특성을 볼 때, 새로이 등장하는 위협들에 대처할 수 있는 잘 정의된 방법론과 프로세스를 갖추는 것이 매우 중요한 일이 아닐 수 없습니다.
효과적인 안티 멀웨어 보호 방식은 네트워크와 게이트웨이, 응용 프로그램 및 운영 체제 수준에서의 계층화된 보안을 요구합니다. 그 동안 마이크로소프트는 기업과 개인 사용자들을 위해 정보를 보호하고 액세스를 제어하는 데 도움이 되는 다양한 보안 솔루션들을 개발해 왔습니다. 마이크로소프트의 안티 멀웨어 솔루션들은 전문적인 기술과 지원팀 및 지원 프로세스를 통해 지원되는 데, 그 중에서도 특히 다음 두 요소가 매우 중요합니다:

- **마이크로소프트 멀웨어 예방 엔진(Microsoft Malware Protection Engine):** 멀웨어 정의를 기반으로 각종 위협을 검사하고 감지하여 삭제하는 핵심 소프트웨어*(백서, 안티 멀웨어 기술의 이해 참조).*

- **마이크로소프트 멀웨어 예방 센터(Microsoft Malware Protection Center):** 새로운 멀웨어를 조사하여 고객에게 신속한 대응 방법을 제시하는 팀.

본 문서에서는 고객들을 위해 지속적인 멀웨어 연구 조사 작업을 수행하고 있는 마이크로소프트 멀웨어 예방 센터의 역할과 활동 및 그 비전에 대해 자세히 살펴 보도록 하겠습니다.

마이크로소프트 멀웨어 예방 센터

마이크로소프트 멀웨어 예방 센터는 고객에게 바이러스와 스파이웨어 및 기타 새로운 멀웨어는 물론 기존의 멀웨어들에 대한 종합적인 보호 방법들을 제공하는 기관입니다. 이 센터는 풍부한 경험을 갖춘 전문 분석가들과 새로운 위협들을 조사하여 이에 대처하며, 고객을 보호하는 데 필요한 보안 기술과 인프라를 제공하는 마이크로소프트 보안 기술자들로 구성되어 있습니다.

마이크로소프트 멀웨어 예방 센터는 Forefront™ Client Security, Forefront Server Security, Windows® Live OneCare™ , Windows Defender와 기타 마이크로소프트 보안 솔루션 및 기술들을 위해 중요한 안티 멀웨어 기술(검사 엔진과 멀웨어 정의 업데이트 포함)을 제공합니다.

그리고 이들의 세계적인 멀웨어 조사 시스템은 전 세계의 마이크로소프트 보안 제품 사용자들로부터 전달되는 피드백을 기반으로 한 생생한 보안 자료들과 뛰어난 자동 분석 기술을 통해, 각종 위협을 신속하게 발견하여 대처하는 데 도움을 주고 있습니다. 또 여러 곳에서 수집된 정보들을 분석하기 때문에 항상 전 세계 동향을 한 눈에 모니터링할 수 있습니다.

주요 멀웨어 동향

마이크로소프트 멀웨어 예방 센터는 이들의 주요 업무 중 하나로 악의적이고 기본적으로 원치 않는 소프트웨어들에 대한 연구 조사를 실시하여 이들이 고객에게 영향을 미칠 수 있는 일련의 동향들을 파악하기 위해 노력합니다. 그리고 이를 통해 각종 위협과 소프트웨어 취약점에 관한 주요 동향들을 기술한 보고서도 발표합니다. 가장 최근에 발표되었던 *Microsoft Security Intelligence Report* (마이크로소프트 보안 인텔리전스 보고서, 보다 자세한 정보는 부록을 참조하시기 바랍니다)는 2006년 7월에서 12월까지의 데이터를 기반으로 한 것으로 다음과 같은 몇 가지 새로운 동향들을 알려 주고 있습니다:

- 동기 부여 요인으로 작동하는 돈: 그 동안 많은 멀웨어 프로그램들이 공공물 훼손이나 자기 만족을 위해 이루어져 왔습니다. 그러나 스파이웨어와 다른 원치 않는 소프트웨어들의 진화는 이러한 소프트웨어 개발자들의 주요 동기로 점차 재정적 수입을 강조하게 되었습니다. 데이터를 파괴하는 대신 이제 스파이웨어는 종종 돈을 목적으로 개인 정보를 수집하거나 광고를 전달하기 시작하고 있습니다.
  현재 파악된 악의적인 행동들만을 살펴 보아도 원치 않는 소프트웨어의 설치를 위한 권한 확보에서부터 사용자의 개인 금융 정보를 사용한 사기 행위에 이르기까지 그 형태가 매우 다양해졌습니다.

- 특정 대상을 목표로 하는 멀웨어 배포: 멀웨어 배포 특성도 변화했습니다. 과거 블래스터(Blaster)나 새서(Sasser) 같은 웜들은 전 세계를 대상으로 급속하게 전파되어, 수백만 대의 기기들을 감염시키고 미디어나 대중의 주목을 받곤 하였습니다.
  그러나 오늘날에는 새로운 멀웨어들의 상당수가 복제되지 않는 트로이 목마의 형태를 띠며, 특히 사용자나 보안 업체들의 주목을 끌지 않도록 교묘하게 설계되고 있습니다. 멀웨어 작성자들은 중단이나 많은 양의 네트워크 트래픽 등과 같이 명확한 감염의 흔적들을 남기지 않으려고 노력하고 있으며 데이터 유출과 같은 다소 눈에 띄지 않는 증상들로 그 형태가 변화해 가고 있습니다.

- 갈수록 복잡해지는 위협들: 멀웨어를 생성하는 데 사용되는 기술들이 시간이 갈수록 점점 복잡해지고 있습니다. 과거 멀웨어 작성자들은 보안 소프트웨어가 감지할 경우 이에 따라 자신들의 생성 내용을 변화시켰습니다. 그러나 오늘날 멀웨어 작성자들은 발각되는 것 자체를 피하기 위한 시간을 벌기 위해 미리부터 수천 종의 변종들을 만들어 두는 경우도 있습니다.
  멀웨어 작성자들은 루트킷이나 패커 같은 도구들을 사용하여 위협들을 감지하고 분석하기 더 어렵게 만들고 있습니다. 뿐만 아니라 멀웨어 작성자들은 사회 공학 기법을 활용해 사용자들이 소프트웨어를 설치하도록 사용자들을 속이기도 합니다.

멀웨어에 대해 현재 진행되고 있는 데이터 분석과 조사 작업은 무엇보다 오늘날의 위협들이 전에 비해 더 교묘해지고 더 빈번히 발생하며 경제적 이익에 의해서 더 많이 유발된다는 점에서 매우 중요합니다. 마이크로소프트 멀웨어 예방 센터는 핵심적인 동향과 새로 등장하는 위협들을 파악함으로써 사용자들을 속이려는 각종 위협들로부터 사용자를 보호하는 작업에 최선의 노력을 다하고 있습니다.

마이크로소프트 멀웨어 예방 센터에 대하여

마이크로소프트 멀웨어 예방 센터는 연구 조사 및 대응 프로세스를 통해 세계 여러 곳에서 전달되는 사항과 보고서들을 모니터하고, 의심스러운 멀웨어를 분석하며, 최신 보호 능력을 갖출 수 있도록 각종 업데이트를 제공합니다. 그림 1은 안티 멀웨어 연구 조사와 대응에 대한 마이크로소프트의 수준 높은 접근 방식을 보여 줍니다.

그림 1: 마이크로소프트 안티 멀웨어 대응 과정

마이크로소프트 멀웨어 예방 센터는 고객 및 보안 업계와 여러 과정에서 다각도로 상호 작용하는 데, 다음은 그러한 과정과 역할들은 간략하게 설명한 것입니다:

- **업계와의 공동 작업:** 이제 보안은 모든 이들의 관심사입니다. 사용자가 어떤 보안 업체를 선택했든, 네트워크로 연결되어 있는 컴퓨터들은 감염된 한 대의 기기가 수천 통의 스팸 메시지들을 전송한다거나 DoS(denial-of-service) 공격의 사용되는 것과 같은 식으로 감염되지 않은 정상 기기들을 공격할 수 있는 하나의 환경 안에 존재합니다. 그러므로 업계에서는 보안 능력을 보다 향상시키기 위해 각종 연구 조사 자료들을 공유하는 것이 매우 중요합니다.
  업계의 협력을 더욱 장려하기 위해 마이크로소프트는 멀웨어에 대항하기 위한 업계 파트너들 간의 협력이라는 목표 하에 Anti-Spyware Coalition (ASC, 안티 스파이웨어 연합)의 창설 회원 단체이자 Anti-Phishing Working Group(안티 피싱 워킹 그룹)의 정회원 단체이기도 한 Virus Information Alliance(VIA, 바이러스 정보 연합)를 설립하였습니다.

- **세계적인 동향 파악:** 분석 작업의 첫 번째 단계는 멀웨어에 대한 정보를 수집하는 일입니다. 이러한 정보는 자동화된 정보 수집 도구, 제품 지원, 업계 샘플 공유 등을 통해 수집할 수 있습니다. 그러나 유용한 데이터들의 상당 부분은 고객들이 보내 준 정보들이며, 이러한 정보들은 대개 자신들이 일상적인 기기 사용 중에 발견한 문제들을 기반으로 한 것들입니다.

- **멀웨어 연구 분석:** 연구 조사 팀은 obfuscation(소스 코드나 개체 코드에 대한 역공학을 어렵게 할 목적으로 원본 파일을 조작하는 것)과 같이 멀웨어가 현재 사용하는 전술과 기술들을 조사합니다. 기존 멀웨어에서 수집한 정보는 추가 정의를 작성하고 안티 멀웨어 엔진을 향상시키는 지침으로 사용될 수 있습니다. 예를 들어, 한 연구 조사자가 멀웨어가 새로운 obfuscation 기술을 사용하고 있다는 사실을 알아 내면, 그에 대항하는 새로운 엔진 강화 기능을 제안할 수도 있다는 것입니다.

- **멀웨어 대응:** 대응팀은 신속하게 고객 문제를 해결할 솔루션을 개발하는 데 역점을 둡니다. 대응팀은 수집한 데이터를 자동화된 분석 기술을 통해 분석함으로써 신속하게 고객들에게 영향을 미치는 기존의 위협들과 새로이 등장한 위협들에 대응합니다.
  새로운 위협이 등장했을 때, 대응팀은 멀웨어 샘플들을 분석하여 적절한 엔진 정의를 작성합니다. 대응팀은 실제 고객들에게 일어난 문제들을 기반으로 조사해야 할 중요한 항목들을 결정하기 위해 수집된 정보들을 사용할 수도 있습니다.

- **서명 정의:** 멀웨어 분석이 완료되고 나온 최종 결과치가 바로 위협을 확인하고 제거하는 엔진에서 사용하게 될 데이터인 멀웨어 정의입니다. 이 정의에는 멀웨어 내의 여러 패턴들은 물론 감염된 기기를 원래 상태로 복원하는 데 필요한 삭제 및 치료 과정들이 포함되기도 합니다.

- **테스트:** 정의가 생성된 후엔 다양한 테스트 과정을 거쳐 서명이 예상대로 작동하는가를 확인하게 됩니다. 마이크로소프트 멀웨어 예방 센터는 서명이 위협들을 정확하게 구분하는지를 테스트하는 데 필요한 다양한 종류의 파일들을 보유하고 있습니다.

  정확한 구분에 실패했다는 결과가 나오면 업데이트는 롤 포워드(roll-forward) 모델을 수행합니다. 그런 다음 정의 내용을 다시 수정하고 테스트한 후 이전 것과 대체하여 발표합니다. 이런 식으로 고객들은 그 정의 파일 안에서 다른 위협들에 대한 보호 기능도 함께 제공받게 되는 것입니다.
  정의 업데이트에는 중요 안티 멀웨어 엔진에 대한 업데이트도 포함될 수 있는데, 그러한 업데이트들은 멀웨어 검사, 감지, 삭제 등의 능력을 강화시켜 줍니다. 그리고 이러한 경우, 엔진은 표준적인 정의 테스트 외에 별도의 철저한 테스트 과정을 거치게 됩니다.

- **발표:** 정의가 테스트를 거쳐 인정을 받고 나면, 디지털 서명을 하고 배포를 위한 패키지 과정을 거치게 됩니다. 디지털 서명은 파일의 신뢰성과 무결성을 보장하고, 배포 패키지 과정은 클라이언트를 위한 다양한 종류의 전체 업데이트와 부분 업데이트를 작성합니다. 클라이언트의 업데이트 빈도에 따라 정의에 완전 업데이트가 아닌 약간의 변경 사항만 적용하게 되는 경우도 있습니다.

  정의 업데이트는 마이크로소프트에 의해 하루에도 여러 차례 발표됩니다. 관리자들은 Windows 소프트웨어 업데이트 서비스와 그룹 정책(보다 자세한 정보는 부록에 있는 Microsoft Forefront Client Security 웹 사이트를 참조하시기 바랍니다)을 사용하는 것처럼, 기존의 업데이트 프레임워크와 정책을 사용해 업데이트를 관리하고 설치할 수 있습니다.

- **사용자 교육:** 더불어 분석가들은 멀웨어 백과 사전(Malware Encyclopedia)에 관련 정보들을 입력하여, 고객들에게 위협의 특성이나 부작용, 구체적인 치료 방법들에 대한 세부 사항들을 제공할 수 있습니다. 비록 분석가는 한 번에 하나의 위협 내지는 같은 종류의 위협들만을 추가할 수 있을지 몰라도, 발표되는 정의 내용에는 여러 개의 멀웨어 프로그램들에 대한 통합된 데이터들이 들어 있을 수 있습니다.

고객은 연구 조사팀과 대응팀의 피드백 고리 안에서 매우 중요한 요소입니다. 고객이 정의를 설치하고 악의적인 소프트웨어를 검사할 때, 이들은 분석을 위해 원격 측정 정보와 샘플을 마이크로소프트 멀웨어 예방 센터로 보낼 것인지 여부를 선택할 수 있습니다. 연구 조사와 대응 프로세스에 대한 고객의 적극적인 참여는 현재 멀웨어 동향을 파악하는 데 큰 도움이 될 것이며, 마이크로소프트 멀웨어 예방 센터가 업데이트를 통한 신속한 대응을 통해 고객을 보호하는 데에도 중요한 역할을 할 것입니다.

주요 대응 사례

그림 2에는 마이크로소프트 멀웨어 예방 센터와 글로벌 멀웨어 연구 조사 시스템을 특징짓는 몇 가지 내용들이 요약되어 있습니다.

그림 2: 마이크로소프트 멀웨어 예방 센터의 주요 특징들

세계적인 기관

마이크로소프트 멀웨어 예방 센터에는 Symantec이나 McAfee, Computer Associates, F-Secure나 기타 다른 업체들에서 근무했던 경험 많은 분석가들과 마이크로소프트의 플랫폼과 응용 프로그램 및 인프라 보안을 향상시켜 줄 최상의 지침들을 숙지하고 있는 마이크로소프트의 기술 전문가들이 소속되어 있습니다. 특히 센터는 바이러스 백신 업계에서 10년 이상의 경력을 쌓아 온 Vinny Gullotto에 의해 이끌어지고 있는데, Gullotto는 과거 McAfee의 Anti-Virus Emergency Response Team (AVERT)에서 이사로 근무한 적도 있습니다. 현재 Gullotto가 이끄는 센터에는 다음과 이들이 소속되어 있습니다:

- **Jimmy Kuo, 수석 보안 연구원.** Kuo는 바이러스 연구 경력만 12년이 넘는 연구원으로, 과거 McAfee의 AVERT 연구소에서 연구원으로, Symantec의 NAV 연구소에서 담당자로 근무하였으며, IBM과 Computer Associates에서 근무한 적도 있습니다. Kuo는 AVAR 2000과 Virus Bulletin Conference에서 기조 연설을 한 적도 있으며, 멜리사 바이러스에 대한 그의 연구를 인정받아 Fed 100 Award를 수상하기도 했습니다. 뿐만 아니라 Presidential Y2K Council의 Information Coordination Center에서 근무한 경험도 있습니다. .

- **Katrin Tocheva, 마이크로소프트 유럽 연구소 소장.** Tocheva는 바이러스 연구 경력만 15년이 넘습니다. 그녀는 F-Secure Corporation과 불가리아 국립 과학원의 컴퓨터 바이러스 국가 연구소에서 근무하였습니다. CARO (Computer Anti-virus Researchers' Organization)와 AVAR (Association of anti Virus Asia Researchers)의 회원이자, AVED (AntiVirus Emergency Discussion Network)의 상임 이사이기도 합니다.

센터는 유럽과 아메리카, 아시아의 여러 지역으로 그 분석 범위를 확장해 가고 있으며 하루 24시간 1년 365일의 서비스를 원칙으로 하고 있습니다. 이들은 여러 마이크로소프트의 보안 제품 및 기술 – Forefront Client Security, Forefront Server Security, Windows Live OneCare, Windows Defender 등등 – 에 대한 지원을 책임지고 있기 때문에, 전 세계 수백 만대의 컴퓨터들을 지원하고 보호하면서 얻은 지식과 경험들을 멀웨어 예방 업무에 활용할 수 있습니다. 고객들은 블로그를 통해서 마이크로소프트 멀웨어 예방 센터의 활동들에 대해 보다 자세히 살펴 볼 수 있으며, 현재 센터의 연구 조사 작업에 대한 업데이트 내용들도 제공받을 수 있습니다(보다 자세한 정보는 부록을 참조하시기 바랍니다).

또 마이크로소프트 멀웨어 예방 센터는 Microsoft Security Response Center (MSRC)와 Product Support Services Security (PSS Security)를 통합하여 멀웨어 관련 문제들에 관한 각종 정보와 절차들을 공유하고 있습니다(그림 3):

그림 3: 멀웨어로부터 고객들을 보호하기 위한 그룹 간 관계

Microsoft Security Response Center (MSRC)는 보안 업체에 취약점 정보를 제공하는 업계 최고의 기관입니다. 마이크로소프트 멀웨어 예방 센터에서도 다른 보안 협력 업체들과 같은 방식으로 이러한 정보들을 입수하고 있습니다.

마이크로소프트 멀웨어 예방 센터 팀은 일반적인 MSRC 절차들을 매우 잘 알고 있기 때문에 새로운 문제들에 신속하게 대응할 수 있도록 그 프로세스들을 최적화할 수 있습니다. 뿐만 아니라 기존 멀웨어에 대한 연구 조사에 유용한 정보와 절차들을 공유할 수도 있습니다.

예를 들어, 알려진 취약점들을 사용하는 멀웨어들을 분석하고자 할 때 각종 도구와 과정 및 학습 내용들을 잘 조화시킴으로써 감지 능력을 높이며 취약점에 대한 추가 정보들을 확보할 수 있는 것입니다. 그리고 이는 멀웨어에 대한 보다 완벽하고 철저한 분석을 가능케 하며, 고객을 위한 멀웨어 감지 및 삭제 능력을 향상시킵니다.

1996년 설립 이래 효과적으로 보안 정보를 제공해 온 MSRC는 멀웨어 관련 문제들에 대한 대응 측면에서 업계의 신뢰와 인정을 받고 있습니다. 그리고 시간이 흐르면서 마이크로소프트가 고객의 보안 문제에 대응하는 방식도 점점 더 나아지고 있습니다. Security Development Lifecycle (SDL) 프로세스 같은 주요 이니셔티브와 최상의 지침들은 앞으로도 계속해서 마이크로소프트의 보안 프로세스를 더욱 강화해 나갈 것입니다.

마이크로소프트 지원 기관인 Product Support Services Security (PSS Security)는 멀웨어 문제와 관련된 고객 지원에 있어 다양한 경험을 가지고 있습니다. PSS Security는 Windows 환경 안에서 멀웨어 문제를 해결하는 데 필요한 융통성과 전문성은 물론, 소프트웨어 제한 정책, 그룹 정책, 기타 마이크로소프트 기술들과 통합된 솔루션들의 설치와 관련된 지식들도 갖추고 있습니다. PSS Security는 Forefront Client Security를 지원하며, 기업이 자신들의 능력을 잘 활용할 수 있도록 돕고 있습니다.

마이크로소프트 멀웨어 예방 센터는 PSS Security와 통합 프로세스를 공유하는 데, 이는 Forefront Client Security 고객들이 분석을 위해 마이크로소프트에 멀웨어를 전송하는 작업을 통해 이루어집니다. 먼저 고객들은 콘텐츠 포털을 통해 마이크로소프트 대응팀에 직접 의심되는 파일들을 전송합니다(이에 관한 내용은 뒷부분에 자세히 나와 있습니다). 그럼 우선 분석가들이 전송 내용을 확인하고 파일에 대한 사전 판단 내용을 다시 고객에게 전송합니다. 그런 다음 분석가들이 최종 결정을 내려 그 결과를 고객들에게 전송하게 되는 데, 여기에는 기업에서 그에 상응하는 조처를 취하고자 할 때 그 업데이트 정의를 설치하는 데 도움이 될 보충 자료들도 포함됩니다.

신속하게 대응해야 하는 멀웨어에 대해서는 Forefront Client Security 고객들이 직접 PSS Security에 연락해, 지원 담당자와 함께 파일을 분석하는 경우도 있습니다. PSS 엔지니어가 Forefront Client Security 고객을 대신해 파일을 전송할 수도 있고, 정의 관련 사항이나 우선 해결 문제를 위한 중앙의 연락처 역할을 할 수도 있습니다.

Windows Defender와 Microsoft Windows Live OneCare가 수집한 샘플들이 일반적인 분석이나 경향 파악을 위해 사용되는 반면, Forefront Client Security 고객들이 제공한 데이터는 다른 것들보다 우선적으로 처리되는 편이며 개별 응답을 받을 수도 있습니다. Microsoft Malware Protection Center와 PSS Security의 협력은 기업 고객들이 멀웨어 관련 보안 문제들에 관해 만족스러운 대답을 들을 수 있게 해 줍니다.

원격 측정

마이크로소프트 멀웨어 예방 센터는 다양한 곳에서 수집된 피드백 분석을 통해 전 세계의 멀웨어 동향을 파악합니다. 이러한 정보들을 수집하는 경로로는 Microsoft Forefront Client Security, Microsoft Forefront Server Security, Malicious Software Removal Tool (MSRT), Windows Live OneCare, Hotmail®, Microsoft Exchange Hosted Services나 기타 마이크로소프트 보호 기술 등과 같은 각종 마이크로소프트 발표 제품 및 기술들, 그리고 PSS Security 지원 기관과 기타 데이터 수집 도구들 같은 내부 출처들을 들 수 있습니다.

마이크로소프트는 정보 공유와 동향 파악을 위해 VirusTotal이나 AV-Test.org, KISA, VIA 같은 기관들과도 협력합니다. 뿐만 아니라 *Microsoft Security Intelligence Report* 같은 출판물들을 통해 새로운 멀웨어 동향에 대한 정보들을 제공하기도 합니다.

멀웨어가 점점 교묘히 감시를 피해가는 순간적인 형태를 띠기 때문에, 매일 또는 시간별의 행동 양식들을 파악하고 적절한 조처를 취하는 것이 매우 중요합니다. 또 다양한 곳에서 수집한 데이터들을 활용해 멀웨어에 대한 사항들을 종합적으로 판단하고 새로운 위협들을 찾아낼 수 있습니다.

예를 들어 Microsoft Windows Malicious Software Removal Tool (MSRT)은 고객 컴퓨터에서 유행하는 특정 멀웨어들을 검사하고 삭제하도록 설계되었으며, Windows 라이선스를 가진 고객들에게는 무료로 제공됩니다. 2005년 1월 처음 발표된 이래, 그 사용자 기반은 무려 3억 1천만대의 컴퓨터로까지 확대되었으며, 이들이 도구를 실행한 횟수도 약 55억 회가 넘는 것으로 조사되었습니다. MSRT는 마이크로소프트 멀웨어 예방 센터가 사용하는 위협 원격 측정 소스 중 하나이며, 컴퓨터에서 악의적인 소프트웨어를 삭제하는 매우 효과적인 도구입니다. 12개의 멀웨어 변종군들 중 75%에 해당하는 멀웨어들에 대한 검사를 실시했을 때 정리가 필요한 컴퓨터들의 숫자가 2006년 1사분기에서 2006년 2사분기 사이에 약 33~70%나 줄어 들었습니다.

> ***"멀웨어가 점점 교묘히 감시를 피해가는 순간적인 형태를 띠기 때문에, 매일 또는 시간별의 행동 양식들을 파악하고 적절한 조처를 취하는 것이 매우 중요합니다."***

Windows Defender Voting Network(SpyNet이라고도 함)는 마이크로소프트 연구 조사자들이 새로운 위협들을 파악하는 방법에 대한 또 다른 예를 제시합니다. Windows Defender 사용자들은 새로운 위협을 발견하고 이를 보고하기 위해 전 세계 사용자 네트워크에 참가할 수 있습니다.

SpyNet에 참가하기로 결정한 고객들은 연구 조사팀의 멀웨어 샘플 요청에 신속하게 응답하는 것은 물론 자신들이 발견한 의심되는 파일들도 전송합니다. Windows Defender 사용자들은 지난 2006년 하반기에만 원치 않는 소프트웨어를 약 3천 8백만 개 이상 발견하여 보고하였습니다. 마찬가지로 Windows Live OneCare 고객들 역시도 자신들의 기기 상에서 발견되는 다양한 위협들에 관해 마이크로소프트와 정보를 공유할 수 있습니다. Windows Defender와 Windows Live OneCare를 통해 이루어지는 이러한 고객 중심의 원격 측정은 분석가들이 가장 많이 나타나고 있는 문제들을 파악하여 이를 해결하는 데 초점을 맞출 수 있게 도와 줍니다.

이러한 기술들과 그 밖의 다른 기술들이 분석가들로 하여금 고객들의 기기 상에서 나타나는 여러 행동 패턴들을 서로 연관 짓고 파악할 수 있게 해 줍니다. 예를 들어 트로이 목마가 검사를 피하기 위해 매우 작은 규모로 만들어졌을 때, 심지어 그것이 겨우 수백 내지는 수천 명 정도의 고객들에게만 영향을 주는 것일지라도 이에 대한 동향 분석이 약간의 의심스러운 행동에서 커다란 위협을 발견할 수도 있게 해 주는 것입니다. 뿐만 아니라 분석가들은 의심스러운 현상들이 증가하는 것을 감지하여 멀웨어가 확산되기 전에 이에 대한 조사를 실시할 수도 있습니다.

신속한 대응

팀은 자동 분석, 보안 전문가, 각종 테스트 프로세스들을 적절히 활용하여 수집된 데이터들을 철저하게 분석함으로써 최신 멀웨어 위협들을 찾아 낼 수 있습니다. 이를 위해서는 효과적인 분석 리소스 활용과 신속한 대응을 위한 자동화 과정에 대한 상당한 투자가 요구됩니다. 이러한 자동화 과정에는 전송된 멀웨어들에 대한 처리 작업도 포함됩니다. 자동 멀웨어 전송 저장 및 검색 기능을 수행하는 시스템이 중복된 전송 내용 처리, 전송 내용 그룹화, 분석 시간 단축을 위한 사전 샘플 분석 작업 등을 수행합니다.

"팀은 자동 분석, 보안 전문가, 각종 테스트 프로세스들을 적절히 활용하여 수집된 데이터들을 철저하게 분석함으로써 최신 멀웨어 위협들을 찾아 낼 수 있습니다."

행동 분류 조사는 분석가들이 비슷한 특징들을 기준으로 멀웨어들을 관련 멀웨어군으로 자동 분류할 수 있게 해 줍니다. 이는 멀웨어 작성자가 검사를 피하기 위해 같은 프로그램의 변종들을 여러 개 만들었을 때 특히 의미가 있습니다. 그리고 플러그형(pluggable) 인프라에서는 수동 작업도 줄고 추가 데이터 샘플 삽입도 쉽게 이루어집니다.

더불어 이러한 기능들은 멀웨어 행동(파일, 레지스트리, 네트워크 이벤트에 미치는 영향 등도 포함) 분석 작업을 자동화하는 데 도움이 됩니다. 반복되는 작업들을 자동화하고 대량의 데이터를 빠르게 분석함으로써 대응팀은 멀웨어를 신속하게 찾아 내고 고객에게 필요한 서명들을 제공할 수 있습니다.

서명을 통한 신속한 대응과 함께 분석가들은 마이크로소프트 안티 멀웨어 엔진의 여러 기능들을 사용해 뛰어난 삭제 기능들을 제공할 수도 있습니다. 감염된 기기를 다시 깨끗하게 만들기 위해 각종 부작용(예를 들어, 변경된 설정 내용 이라든가)들을 원상 복구시키는 것 같은 작업들이 이에 해당합니다.

연구 조사의 또 다른 영역인 동적 변환을 통해 안티 멀웨어 엔진은 자신의 콘텐츠를 뒤섞어 버리려던 멀웨어를 해독합니다. 자동화된 해독 기능은 완벽하긴 하나 시간이 많이 걸리고, 직접 만든 방식은 빠르긴 하나 유지에 상당한 노력이 필요합니다(늘어나는 멀웨어 변종 수에 맞춰 확장되지 않음). 동적 변환은 멀웨어 명령 분석 방식을 최적화함으로써 속도를 높이고 해당 범위를 확장시켜, 신속한 멀웨어 해독을 가능케 해 줍니다. 또한 동적 변환은 멀웨어 샘플의 행동 기반 분석 등의 영역으로도 확장될 수 있습니다.

마이크로소프트는 고객 문제에 신속하게 대응하고 실제 적용 가능한 고객 지침들을 제공하기 위해 PSS Security과의 통합된 통신 방식을 통해 고객들에게 지침들을 전달합니다. 2007년 4월 시작된 마이크로소프트 멀웨어 예방 센터 웹 포털은 각종 위협에 대한 최신 정보와 뉴스 및 마이크로소프트 멀웨어 예방 센터의 각종 연구 결과들을 제공합니다. 고객들은 자신들의 환경에 있어 가장 위험한 위협들을 파악하고 멀웨어 백과 사전을 통해 구체적인 정보들을 살펴 볼 수 있습니다. 고객들은 또한 이 포털을 통해 분석용 멀웨어 샘플들을 전송할 수도 있습니다.

그림 4:
마이크로소프트 멀웨어 보호 포털

향후 전략과 비전

마이크로소프트의 비전은 세계적인 멀웨어 연구 조사 기관 중 하나가 되어, 고객들에게 정확하고 시기 적절한 업데이트들을 안정적이고 꾸준히 제공하는 것입니다. 마이크로소프트 멀웨어 예방 센터는 세계적인 수준의 보안 대응을 통해 고객들에게 영향을 미치는 위협들을 해결하는 작업에 있어 품질과 시기 적절성, 그리고 정확성이라는 3가지 원칙을 지켜 나가고자 노력하고 있습니다.

단기 전략

단기적으로 마이크로소프트 멀웨어 예방 센터는 다른 멀웨어 연구 기관들과 마찬가지로 일관된 멀웨어 지원 기능들을 제공할 것입니다. 그리고 그 외 다른 영역에서의 단기 전략들에는 다음과 같은 것들이 있습니다:

- **정의 품질과 범위:** 업계의 다른 선두 업체들과 비교해 마이크로소프트 멀웨어 예방 센터는 위협의 여러 측면들 중에서 고객 시스템 내에서의 멀웨어 검색에 역점을 둡니다. 마이크로소프트 연구 조사팀은 여러 테스트 기관들과 협력하여 비교에 사용되는 방법들을 이해하고 현재 고객들이 겪고 있는 가장 위협적인 문제들(바이러스, 웜, 트로이 목마 등)에 초점을 맞추고자 노력하고 있습니다.

- **안티 멀웨어 응답 시간:** 마이크로소프트 대응팀은 고객의 기대에 부응하거나 때로는 고객의 기대를 뛰어넘는 신속한 응답 및 업데이트를 제공하기 위해 노력하고 있습니다. 대응팀의 목표는 심각한 위협들이 발견된 지 몇 시간 내에 고객들에게 이에 대한 정의들을 제공하여 적절히 대응하며, 앞서 설명한 대로 기업 고객들에게 그에 상응하는 각종 지원 기능들을 제공하는 것입니다.

향후 계획

이러한 단기 계획과 함께 연구 조사 및 대응팀은 향후 동향과 고객들의 필요를 파악하여 차세대 보호 기능들을 제공하고자 합니다.

- **위협의 범위:** 현재 업계에 나와 있는 도구들은 멀웨어 감염 결과에 초점을 맞춘 것들입니다. 즉 고객의 기기에 설치된 프로그램이나 파일들에 대한 것들이란 뜻입니다. 그러나 보다 정확한 분석과 예측을 위해서는 감염을 야기하는 전체적인 상황에 대한 검사가 있어야 향후 멀웨어 행동에 대한 예측과 경고가 가능할 것입니다. 예를 들어, 스팸 메일 안에 피싱 URL이 포함되어 있다면, 이것이 자체 업데이트되는 트로이 목마를 다운로드 할 수도 있는 것입니다.
  다양한 데이터 소스와 위협이 전파되는 데 사용되는 통로들을 조사함으로써 연구 조사 및 대응팀은 단순히 하나의 설치 세부 사항을 넘어 멀웨어 행동 패턴을 확인하고 이에 대처할 수 있을 것입니다. 따라서 장기적으로 마이크로소프트 멀웨어 예방 센터는 위협이 감지되었을 때 다양한 응답 채널을 통해 이에 대해 종합적이고 즉각적인 대처할 수 있는 능력을 배양하고자 합니다.

- **향후 동향 예측:** 지난 10년 동안 멀웨어는 엄청난 변화를 보여 주었고, 특히 과거 몇 년 사이에는 그 정도가 더 심했습니다. 만약 과거가 미래를 알려 주는 지표가 된다면, 기술이 진보하고 그에 대한 동기들이 다양해지면서 새로운 위협들은 늘어갈 것입니다. 스파이웨어나 피싱, 기타 경제적인 이유에 의해 이루어지는 각종 공격들이 오늘날 멀웨어 작성자들의 현재 목표를 보여 주는 것처럼 말입니다. 마이크로소프트 연구자들은 앞으로도 계속해서 새로운 동향과 잠재적인 감염 요소들을 조사하고 감시하면서, 미래의 잠재적 공격들에 대한 경계를 늦추지 않을 것입니다.

- **지속적인 업계의 참여:** 보안은 업계 차원의 문제이며 업계 차원의 솔루션들을 필요로 합니다. 오늘날과 같이 네트워크화된 세상에서는 고객들도 같은 환경 안에 존재하며 서로 소통합니다. 따라서 멀웨어 위협에 대한 보호도 그만큼 꼭 필요한 요소가 된 것입니다. 위협 내용들이 복잡해져 감에 따라 보안 업계가 사용자 보호를 위해 협력하는 일도 갈수록 더 중요해질 것입니다.

  Microsoft Virus Initiative (MVI), Virus Information Alliance (VIA), Anti-Spyware Coalition (ASC) 같은 포럼들은 보안 업체들이 멀웨어 예방을 위한 도구와 정보 및 최상의 지침들을 공유할 수 있는 수단들을 제공합니다. 그리고 이 단체들의 설립 회원으로서 마이크로소프트는 고객들에게 안티 멀웨어에 대한 다양한 선택의 폭을 제공할 것을 약속합니다.

결 론

오늘날 멀웨어의 동향은 시시각각 변화하고 있습니다. 위협들은 갈수록 진화하여 보다 교묘해지고 있으며 경제적 이유를 동기로 한 멀웨어들도 늘어나고 있는 추세입니다. 동시에 기업과 사용자들은 고도의 네트워크화된 환경 속에서 일하고 있습니다. 마이크로소프트는 이 같은 현재의 위협과 앞으로 등장할 새로운 위협들로부터 고객들을 보호할 것이며, 컴퓨터 사용 환경을 위하여 업계 차원의 협력을 도모하기 위해 노력할 것입니다.

풍부한 경험을 갖춘 팀과 뛰어난 원격 측정 기술, 자동화 기능, 통합 프로세스 등을 통해 마이크로소프트 멀웨어 예방 센터는 앞으로는 계속 안정적이고 정확하며 효율적이고 일관된 방식을 통해 다양한 연구 조사를 실시하고 각종 문제에 대응해 나감으로써 고객의 필요를 충족시켜 나갈 것입니다.

부록: 관련 자료

마이크로소프트 멀웨어 예방 센터의 역할과 멀웨어 보호 방법들에 대한 추가 보안 정보는 다음 자료들을 참조하시기 바랍니다.

웹 사이트

- 마이크로소프트 멀웨어 예방 센터 포털(Microsoft Malware Protection Center Portal): 이 사이트는 고객에게 최근에 발견된 멀웨어들과 최신 동향에 대한 정보들을 제공합니다.
  http://www.microsoft.com/security/portal
- Forefront Client Security: 이 사이트에서는 업무용 데스크톱과 랩톱, 서버 운영 체제의 보호를 위한 Microsoft Forefront Client Security와 바이러스 백신 및 안티 스파이웨어 솔루션 등에 관한 정보들을 제공합니다.
  http://www.microsoft.com/clientsecurity
- 안티 멀웨어 팀 블로그: 이 사이트에서는 최신 멀웨어 동향에 대한 보고서와 연구 조사 문건들을 살펴 볼 수 있습니다.
  http://blogs.technet.com/antimalware/

각종 보고서 및 백서

- *Microsoft Security Intelligence Report*: July–December 2006 (마이크로소프트 보안 인텔리전스 보고서: 2006년 7–12월)
  http://www.microsoft.com/technet/Security/default.mspx
  (이전 보고서는 다음 주소에서 찾아 보실 수 있습니다: http://go.microsoft.com/?linkid=6543860)
- *Understanding Anti-Malware Technologies* (안티 멀웨어 기술의 이해)
  http://www.microsoft.com/forefront/whitepapers/default.mspx
- *Unified Protection for Clients* (클라이언트를 위한 통합 보호 방식)
  http://www.microsoft.com/secureclient/default.mspx
- *Defeating Polymorphism: Beyond Emulation* (다형성 파괴: 에뮬레이션을 넘어)
  http://microsoft.com/downloads
- *Behavioral Classification* (행동 분류)
  http://microsoft.com/downloads

Microsoft®

One Microsoft Way
Redmond, WA 98052-6399
microsoft.com/security/portal