악성코드 경유지/유포지 실시간 분석 및 검증 장비

저자
(Authors)

오동엽, 김현우, 정승일, 박재경

출처
(Source)

한국컴퓨터정보학회지 22(1), 2014.6, 7-14 (8 pages)
KSCI Review 22(1), 2014.6, 7-14 (8 pages)

발행처
(Publisher)

한국컴퓨터정보학회
The Korean Society Of Computer And Information

URL

http://www.dbpia.co.kr/Article/NODE06527679

APA Style

오동엽, 김현우, 정승일, 박재경 (2014). 악성코드 경유지/유포지 실시간 분석 및 검증 장비. 한국컴퓨터정보학회지 , 22(1), 7-14.

한국컴퓨터정보학회지
제22권 제1호, 2014. 6.

악성코드 경유지/유포지 실시간 분석 및 검증 장비

• 오동엽(한국과학기술원 CSRC)
• 김현우(한국과학기술원 CSRC)
• 정승일(한국과학기술원 CSRC)
• 박재경(한국과학기술원 CSRC)

I. 서론

최근 다양한 웹서비스의 증가와 함께 공격적이고 심각한 악성코드 또한 그 수를 판단 할 수 없을 정도로 빠르게 확산되어 가고 있다. 그리고 이러한 악성코드들에 의한 피해는 날로 증가하는 추세이다. 이는 개인정보 유출 등의 문제와 연계되어 인터넷에 대한 불신이 가중되고 있는 실정이다. 이러한 현상은 국내뿐만 아니라 미국 등의 선진국에서도 일어나는 현상으로 2013년 12월 미국의 유명 대형 할인점인 타겟(Target)사의 고객 개인정보와 신용카드 정보가 해킹으로 유출되는 사건이 발생했다. 타겟사는 월마트에 이어 미국 내2위의 소매업체로 미국과 캐나다에서 1,900여개 매장을 운영하고 있다. 당초 피해자는 4천만 명 수준으로 알려졌으나 이 업체의 공식 성명서에 따르면 발생한 오프라인 방문 고객들의 계좌정보 유출사건으로 최대 7천만 명의 피해자가 발생했다.[1]

이러한 문제점을 해결하기 위해서 악성코드 경유지/유포지 실시간 분석 및 검증 장비인 웹큐어(WebCure)를 소개하고자 한다. 웹큐어는 단순한 형태의 탐지가 아닌 다중 필터를 통한 검사 방식을 도입하여 실시간으로 악성코드의 유포지/경유지를 탐지하는 기법을 도입한 장비이다. 또한 공신력 있는 카이스트 사이버보안 연구센터의 악성코드분석 시스템(SIMon)에서 탐지된 악성코드 경유지/유포지에 대한 데이터베이스를 실시간으로 제공받아 1차 검사를 우선적으로 실시하도록 설계하였다.

최근에 악성코드를 이용한 대표적인 공격 유형이 APT (Advanced Persistent Threat) 공격이며, 이 공격은 목표를 정하여 공격하는 방식으로 노골적인 공격을 감행하고 있다. 또한, 사이버전과 같은 국가 간의 전쟁의 양상으로도 확대되고 있는 추세이다. 이에 대한 기술적인 대응책으로 악성코드를 차단하기 위한 기술 개발이 이루어지고 있으나 단순히 악성코드에 대한 패턴을 이용한 시스템이거나 악성코드의 배포지에 대한 URL을 차단하는 수준에 머물고 있다. 2013년 7월에 발표된 악성코드 유형별 비율을 보면 악성코드 유형 중 원격제어가 59%의 비율로 가장 높았으며, 그 이외에도 다운로더 14%, 드롭퍼 8%, 감염PC 정보탈취 8%, 온라인 게임계정 탈취 4% 등의 악성코드 유형이 다양하게 나타났다[2]. 현재까지 악성코드 탐지기법은 크게 두 가지 기법으로 구분 할 수 있다. 디컴파일러, 디어셈블러, Signature Base 등을 활용한 정적 분석 기법과 API Hooking, Behavior Based/Similarity Based 탐지 등을 활용한 동적 분석기법이다.

이러한 분석 기법은 이미 인터넷상에 퍼져있는 악성코드를 수집하여 분석하는데 사용되는 기법들로써, 악성코드가 배포가 되어 피해를 입은 이후에 분석이 진행이 되고, 분석이 완료된 이후에 해당 악성코드에서 추출한 고유의 패턴을 활용하여 백신 제작/배포해야하는 문제에서 탈피하지 못한다.

이를 보완하기 위하여 허니팟과 같은 환경을 구축하여 해

커들의 공격 유도를 통해 악성코드를 수집/분석을 하고 있지만 현실적으로 이러한 방식으로는 인터넷상에 존재하는 무수히 많은 악성코드들을 모두 수집/분석하기에는 무리가 따르는 것이 현실이다.

그리고 악성코드의 바이너리 파일을 압축하거나 특정 패턴을 숨기는 Polymorphic 기법, 바이너리 파일 자체를 변화시켜 고유 바이너리 패턴을 제거하는 Metamorphic기법, 스스로 악성코드 분석 도구를 감지하거나 탐지를 차단하는 분석 도구 탐지 기법 등을 통해 수 없이 변조/은닉되어 다양한 변종 악성코드로 출현을 한다는 점 또한 해결과제로 남고 있다.

여기서 제안 하고자 하는 웹큐어는 기존 시스템과 달리 시그니쳐 기반의 탐지뿐만 아니라 악성코드의 유포 방법을 미리 정의 하여 유포이전에 접근부터 막는 방식을 구현하여 탐지율을 높였으며 웹(URL) 크롤링을 이용하여 시드(Seed) URL 뿐만 아니라 하위 URL까지 상세하게 분석하여 악성코드의 감염을 사전에 방지 할 수 있도록 설계하였다. 또한, 인라인이 아닌 아웃오브패스(Out-of-Path) 방식의 환경에서 동작하도록 설계 하였다. 이는 웹큐어를 도입하기 전의 기존 네트워크 망에 간섭을 주지 않는 범위 내에서 악성코드 감염을 막을 수 있도록 하기 위함이다.

전체 구성은 다음과 같다. 2장에서는 악성 코드 사례에 및 관련 연구에 대해서 살펴본다. 3장 에서는 제안한 시스템 웹큐어의 구성 및 필터링 엔진의 기능, 웹(URL) 크롤링 기법에 대해 설명하며, 4장 에서는 결론 및 활용 방안에 대하여 기술한다.

II. 관련 연구

1. 최근 동향

2014년 7월까지 8,640 건의 악성코드 은닉사이트가 탐지되었다[1]. 이는 2012년 탐지된 건수보다 증가한 수치이며, 악성코드 은닉 사이트는 매년 증가하는 추세이다.

악성코드 은닉 사이트 특성을 살펴보면 대량의 경유지와 연결되는 유포지가 확인 된다. 대량의 경유지를 통해서 짧은 시간 내에 대규모 좀비 PC를 신속하게 확보하고 이 PC들을 악성코드 유포를 위한 경유지로 이용하고 있다.

2013년 발생된 대량의 경유지 악용 악성코드 유포 사고 시점을 살펴보면 대규모 악성코드 유포 공격이 주로 주말(금요일 18시 이후 ~ 일요일)에 집중적으로 발생하고 있다는 것을 확인(전체 사고의 70%가 주말에 발생)할 수 있다.

이렇게 주말을 이용하여 악성코드를 유포하는 이유는 서버에 대한 기술적인 조치가 주말에 미흡하기 때문이다. 실제 악성코드 유포에 악용된 서버를 섭외하여 분석을 수행하려 해도 담당자가 연락이 되지 않거나 차주 업무시간에 진행을 해야 한다는 답변을 받게 된다. 공격자들은 이를 악용하고 있는 것이며, 따라서 악성코드 탐지 및 방어는 담당자의 근무시간인 주간보다 그 이후에 더 집중되어야한다는 결론을 얻을 수 있으며, 그에 맞도록 보안 정책을 수립해야한다.

2. 악성코드 유포사고 악성코드 유형

2014년 현재까지 주말에 유포된 악성코드는 원격제어와 다운로더, 드롭퍼, 정보수집 악성코드가 주를 이루었고, DDoS공격, 금융정보탈취, 금융사이트 파밍, 온라인 게임 계정탈취 악성코드도 다수 확인되었다. 특히 원격제어 악성코드의 비중이 상당히 높은 것을 알 수 있다.

또 한 가지 주목할 부분은 정보수집 악성코드의 비중이다. 정보수집 악성코드가 주로 수집하는 정보는 감염된 PC의 시스템 정보이다. 시스템 정보에는 일반적으로 PC가 위치한 네트워크 환경 및 사용자에 대한 정보가 포함되어 있다. 즉, 이러한 정보들을 통해 공격자는 감염된 PC에 대한 다양한 환경 정보 수집이 가능하며, 공격 대상을 선별할 수 있게 된다. 악성코드 유형을 APT 관점으로 바라보게 된다면 주말 악성코드 유포 대응이 곧 APT 공격 대응이라고 할 수 있다.

3. 악성코드 유포 방법

악성코드는 사용자의 PC가 가지고 있는 취약점을 통해서 설치가 된다. 이러한 취약점을 이용하여 악성코드가 설치가 되면 시스템 변조 및 정보를 유출 할 수 있는 권한을 공격자에게 빼앗기게 되는 것이다. 공격자가 악성코드를 PC에 감염시키기 위해 악용한 취약점은 다양하게 파악된다.

이 취약점들은 MS IE 취약점(인터넷 웹브라우저 취약점), Adobe Flash Player 취약점(웹서핑 시 브라우저로 비디오, 애니메이션 등을 볼 수 있게 해주는 플러그인 취약점), Java Applet 취약점(웹페이지 상에서 실행 되는 자바 프로그램 취

1) 카이스트 SIMon에 의해 탐지된 악성코드

약점), MS Windows Media 취약점(윈도우 미디어 플레이어 취약점), MS XML 취약점(인터넷에서 사용되는 XML언에 해석 도구 취약점) 5가지로 분류된다.

4. 악성코드 유포 사례

4.1 국내 소프트웨어 대상 제로데이 취약점 증가

최근 국내 소프트웨어를 대상으로 한 취약점과 이를 악용한 악성코드가 증가하기 시작했고, 이러한 추세는 가속화하고 있다. 예를 들어 인터넷 뱅킹에 많이 쓰이는 소프트웨어의 취약점이 발견됐고(특히 Active-X), 이 외에도 곰플레이어와 같은 동영상 플레이어 프로그램에서 취약점이 보고되어 업데이트가 권고되기도 했다. 국내 문서작성 소프트웨어의 취약점을 이용한 경우도 발생하였는데 전 세계적으로 많이 사용하고 있는 문서관련 프로그램(워드 및 PDF)의 취약점을 이용한 공격도 꾸준히 발생하고 있으며 전자우편을 이용하여 자극적인 문구로 공격을 감행한다.

4.2 파밍과 결합된 온라인 게임 계정정보 탈취 악성코드 등장

2014년 상반기에 발견된 보안 위협들의 특징 중 하나는 개인정보를 탈취하기 위한 공격이 활발했다는 점이다. 상반기 국내에서 가장 많이 발견된 개인정보 탈취 형태의 악성코드는 인터넷 뱅킹 정보를 탈취하는 형태와 온라인 게임 계정정보를 탈취하는 악성코드라고 할 수 있으며 공인인증서의 탈취도 많이 이루어진 것으로 보고되고 있다. 특히 온라인 게임 계정을 탈취하는 악성코드는 윈도우 시스템 파일을 변경하거나 패치하는 형태로 유포됐는데, 이는 사용자에게 발각되지 않도록 위장하기 위한 기법이다. 그리고 보안 소프트웨어의 진단을 피하기 위해 셀 수 없이 많은 변형들을 유포하거나, 목적 달성을 위해 다양한 보안 소프트웨어를 무력화시키는 기법들이 날로 발전하고 있는 실정이다. 또한 인터넷 뱅킹 정보 탈취 형태의 악성코드는 정상적인 은행 사이트와 구분이 어려울 정도로 유사한 피싱(Phishing) 웹사이트를 이용한 방법에서부터 호스트(hosts) 파일 변조 형태, IP차단을 피하기 위해 주기적으로 서버(C&C)와 통신하는 등 점점 고도화되고 있다.

4.3 드라이브 바이 다운로드 공격

드라이브 바이 다운로드 공격은 궁극적으로 사용자컴퓨터의 취약점을 이용하여 악성코드를 유포하는 방법이다. 공격자는 사용자 PC를 악성코드 유포사이트로 유도하기 위해 취약점을 가진 웹 서버에 SQL인젝션(SQL injection)과 같은 방법으로 침투한 후 웹 페이지에 직접 악성코드유포지로 연결 되는 코드를 삽입하거나, 광고 배너나 제3의 위젯과 연결되어 있는 링크를 변조하여 공격을 실행한다.[3] 드라이브 바이다운로드 공격은 사용자의 컴퓨터가 해킹된 웹 사이트인 최초 접속지에 접속하면 공격자가 삽입해 놓은 유도코드 또는 변조한 링크에 의해 수단계의 경유지를 거쳐 자동으로 악성코드 유포사이트로 연결된다. 사용자 컴퓨터가 유포사이트로 접속되면, 사용자 컴퓨터의 웹 브라우저나 어도비 플래시 플러그인과 같은 어플리케이션 취약점이 존재하는 사용자 컴퓨터로 실행 파일이 다운로드 되고 컴퓨터는 악성코드에 감염된다.

III. 본론

이번 장에서는 제안하고자 하는 웹큐어에 대해서 소개한다. 본 시스템은 서론에서 언급한 바와 같이 악성코드 자체를 분석하는 시스템이 아니라 악성코드 감염(유포) 이전 단계에서 미리 악성코드 위협으로부터 보호하는 방법을 구현한 것이다.

웹큐어는 악성코드의 유포지/경유지를 차단하고 실시간으로 탐지하는 것을 목표로 하고 있는 미러링 기반의 전용장비 시스템이다. 이 시스템은 크게 두 가지 메인 기능을 탐재하고 있으며, 각각의 기능을 구현하기 위한 부가 기능들로 이루어져 있다. 첫 번째 기능으로는 악성코드 유포지/경유지 사이트로의 접근을 탐지하는 악성URL 탐지 기능이며, 두 번째 기능은 현재까지 알려지지 않았지만 웹큐어를 도입한 사내/관내에서 관리하고 있는 주요 URL(사이트)가 악성코드 유포지/경유지로 이용되고 있는지 여부를 분석하는 URL 분석 기능이다. 위의 두 핵심 기능은 의심 URL을 추출/분류하고 해당 URL이 악성코드 유포지/경유지인지를 파악하는 다중 필터를 통해 탐지 및 검증하는 과정을 수행한다. 그러기 위해서는 사내/관내 네트워크에서 발생하는 트래픽을 웹큐어로 미러링하여 실시간으로 패킷을 분석하면서 URL을 추출하고,

해당 URL의 악성코드 은닉여부를 판단 할 수 있도록 망을 구성해야 한다. 그림 1은 웹큐어 시스템을 적용한 망의 구성을 보여주고 있다.

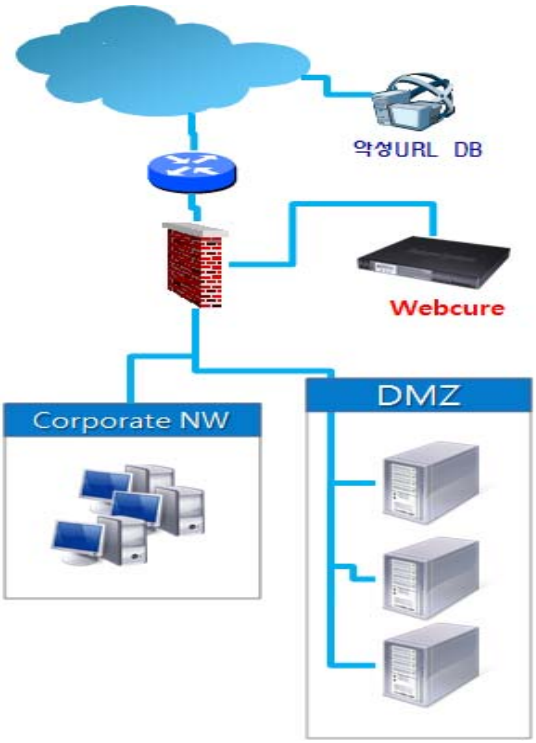

그림 1. 웹큐어 망 구성도

위와 같이 기존 망의 변경 없이 방화벽이나 스위치 등에 미러링을 구성하여 웹큐어로 트래픽을 복제하여 전달하게 구성을 하게 된다. 이러한 망 구성은 기존 구성과 비교하여 웹큐어 시스템을 도입한 이후에도 URL 분석에 의한 네트워크 트래픽의 성능(속도) 저하가 일어나지 않도록 한 것이다.

1. 다중 필터 시스템 구성

본 시스템에서 구현한 필터링 방식은 총 3가지의 단계로 이루어져 있다. 커널 레벨의 필터링과 seed URL 을 기반으로 하는 분석 필터링, seed URL을 바탕으로 크롤링한 URL를 필터링하게 된다. 각각의 레벨에서의 필터링을 통해 성능 지연을 최소화하여 실시간으로 처리할 수 있도록 설계하였다. 다음절에서 각 레벨별 필터에 대한 구성을 설명하도록 한다.

1.1 커널 기반의 URL필터링

웹큐어 시스템은 상용OS를 사용하지 않고, 자체적 임베디드 OS를 제작하여, 장비 운용상에 불필요한 부분을 제거하였고, 경량화되고, 보다 안전한 OS를 탑재 하였으며, 필요시에 따라 다양한 형태로 변형이 가능하도록 설계 되었다. 또한 커널 레벨로 구현한 1차 필터링 엔진의 경우 커널 TCP/IP 스택을 수정하는 것이 아니라 NF_HOOK (PRE_ROUTIING) 지점에 모듈형태로 탑재하여 개발되었다. 미러링 트래픽을 처리하기 위해서 일부 TCP/IP 스택의 코드를 주석 처리하고, 이를 제작한 엔진 모듈에 추가를 하였다. 커널 소스를 전혀 수정하지 않고 개발을 진행하지는 않았으나 이를 최소화하여, 간단한 수정만으로 추후 커널 버전 업그레이드 이슈가 발생했을 시 업그레이드 진행에 보다 능동적이고 즉각적으로 대응하기에 좋은 구조로 설계/개발되었다.

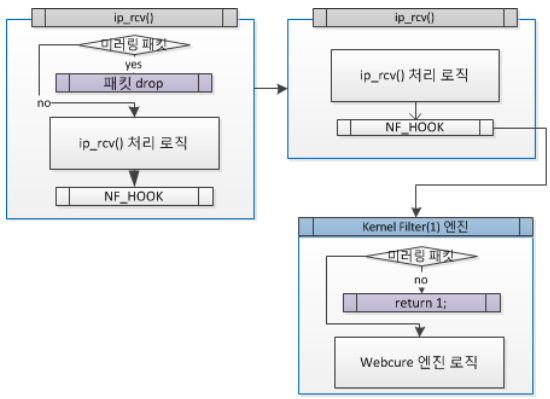

그림 2. kernel TCP/IP 스택 일부 수정

그림 2은 kernel network stack의 L4 Layer의 IP packet 수신 시작 함수인 ip_rcv() 함수의 코 드 중 미러링 packet을 핸들링하고 있는 부분을 제거 하고, 이를 webcuer의 kernel filter 엔진에 적절히 이식한 다는 것을 간략히 보여주고 있다.

기존의 커널에서의 URL 필터링은 단순히 패턴매칭에 의한 URL 필터링으로 해당 URL의 유무에 따라 추가 검사 여부를 결정하는 구조였으나 본 시스템에서 구현된 URL 필터링은 URL prefix 해시 트리를 이용한 방식으로 기존에 방식에 비해 검색 속도를 향상시켰다.[5] 또한 커널로부터 요청되어지는 HTML에서 URL을 추출하여 트리형태의 테이블을 유지하여 해당 URL이 의심코드 추출을 위해 방문한 이력이

있는지 없는지를 판단하는 검사를 진행한다. 이 과정을 통해 향후 해당 URL을 크롤링하여 방문할 때 모든 페이지를 일일이 검사하는 불합리함을 개선하였다. 그림 3에서와 같이 특정한 URL에서 악성코드가 별견되었을 경우 하위 디렉터리 또한 감염되었다고 판단하는 것이 올바른 판단일 것이다.

즉, 그림 3에서처럼 /upload 디렉터리의 하위 페이지나 /main의 하위 페이지는 모두 동일한 형태로 감염이 되었으므로 동일한 검사를 반복할 필요는 없을 것이다. 따라서 도메인을 트리 형태로 유지하여 관리할 경우 불필요한 경로를 줄일 수 있는 방안이 된다.

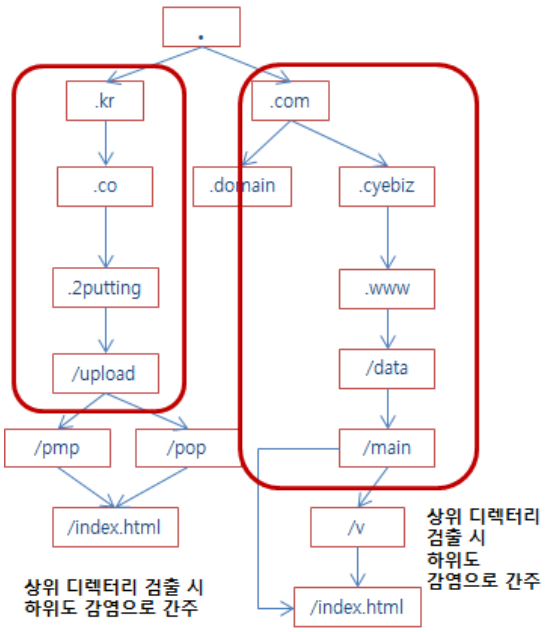

그림 3. 트리 구조에 의한 하위디렉터리 검출

이때 추가적으로 하위 디렉터리가 최종적으로 가리키는 곳이 기 검출된 악성코드 포함 페이지 인지를 확인하는 절차가 추가적으로 이루어져야 한다. 단순히 하위 디렉터리라는 것만으로는 모두 악성코드 연관 페이지라고 볼 수는 없기 때문이다. 또한 향후 해당 페이지에서 악성코드가 제거되었을 경우에는 해당 트리의 정보값을 초기화하여야 정상적으로 이용할 수 있는 과정도 필요하다.

1.2 L7 레벨 실시간 다단계 필터링

L7 레벨에서의 필터링은 두 단계로 나뉘어 동작하게 된다. 첫 번째 단계에서는 기존 악성코드 탐지 연구 방법에서는 해당 웹 페이지를 다운로드하고 그 페이지 내에 숨김 iframe과 같은 비정상 태그의 존재 여부를 확인하여 처리하였다[6]. 해당 방법은 SpiderMonkey[7]를 기반으로 스크립트 에뮬레이팅 모듈을 통해 페이지 내의 모든 URL을 추출하여 반복적으로 링크를 발견하지 못 할 때까지 반복하는 크롤링 기반의 탐지 방법이었다. 하지만, 이 방법의 경우는 시스템의 실시간 트래픽을 분석 시 적용하기에는 성능적인 한계가 있을 수 있다. 즉 하나의 페이지 요청에 따른 이후의 처리 시간이 무한적으로 길어질 수 있다는 단점이 있으므로 1차 L7실시간 필터링 엔진에서는 그림 4처럼 크롤링 방식을 배제하고 현재 요청된 페이지만 검사하는 방식을 채택하였다.

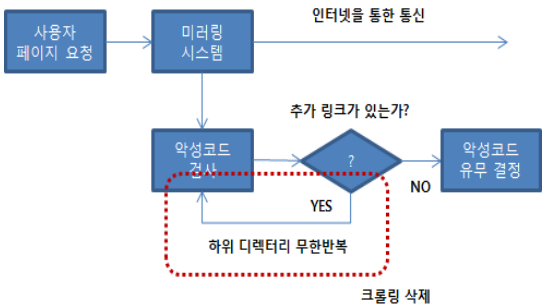

그림 4. 크롤링 배제 후 실시간 페이지 검사 1

만약 사용자가 악성코드가 포함된 페이지를 요청하였을 경우에 인바운드로 유입되는 패킷을 분석하면 즉시 해당 페이지에 악성코드가 포함되어 있다는 것을 알 수 있기 때문이다.

그러나 2단계 필터링 엔진에서는 위에서 언급한 크롤링 기능을 포함하여 분석을 진행한다. 여기서 말하는 2단계는 기능적으로 미러링 URL를 검사하는 로직과는 별개로 관리자/장비운용자가 검사하고자하는 내부 사이트나, 관리 대상 사이트의 URL을 직접 입력하여, 해당 사이트의 위변조, 악성코드 유포지/경유지로 사용되고 있는지를 항상 모니터링하는 기능으로 설명 될 수 있다. 이 경우에는 실시간 트래픽을 분석하는 경우가 아니므로 시간적 제약이 덜하기 때문에 크롤링 기능을 적용하여 보다 깊이 있는 분석을 하도록 설계하였다.

이 시스템에서 사용하는 필터로는 다음과 같은 조건에 의

해 실시간으로 해당 페이지만을 필터링한다[5].

필터는 탐지 조건에 따라 확정 탐지 및 의심탐지로 분류된다. 확정 탐지는 시그니쳐 탐지를 기반으로 확인되며 의심탐지는 라인당 글자 수 초과 탐지, 비정상 문자열 포맷 스트링 탐지, 숨김 iframe 탐지, 숨김 applet 탐지, 숨김 object 탐지에 의해 확인 된다.

- 시그니쳐 탐지

  최초 패킷이 왔을 시 해당 URL의 웹 페이지 소스를 다운받은 후 악성코드 판단 기준이 되는 시그니쳐와 매칭되는 부분이 있으면 악성 코드가 심어져 있는 것으로 판단 및 해당 정보를 저장한다.

- 라인당 글자수 초과 탐지

  한 라인에 특정 바이트의 초과 및 해당 라인에 25% 이상이 숫자로 이루어져 있으면 의심탐지로 분류한다.

- 비정상 문자열 포맷 스트링 탐지

  다운로드 받은 웹 페이지 소스코드 내에 평문 및 난독화된 스크립트 안에서 문자열 포맷을 추출하여 메모리 주소 및 다른 정보를 보여줄 수 있는 포맷의 사용 및 해당 라인이 특정 바이트 수를 초과할 시 의심탐지로 분류한다.

- 숨김 iframe 탐지

  숨김 iframe 탐지는 다운로드 받은 웹 페이지 소스 코드 내에 숨겨진 iframe이 있는지 확인한다. 소스코드 내에서 iframe tag를 추출한 후 width, heigth의 값이 0인 tag만 확인, 정상 iframe 이 아닌 숨겨진 iframe을 추출하여 의심탐지로 분류한다.

- 숨김 applet 탐지, 숨김 object 탐지

  소스 코드내에 applet 및 object tag를 추출하여 width, heigth의 값이 0인 tag만 확인, 숨겨진 applet tag 및 object tag를 추출하여 의심탐지로 분류한다.

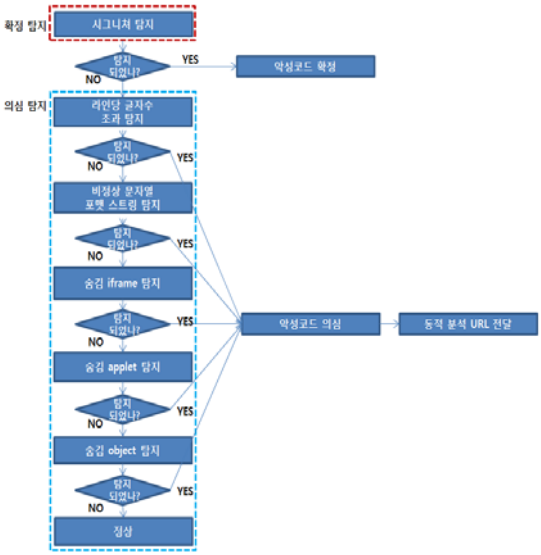

그림 5. 웹 페이지 검사 필터 조건

확정 탐지인 시그니쳐 탐지로 분류된 URL은 악성코드로 분류되며 의심 탐지인 라인당 글자수 초과 탐지, 비정상 문자열 포맷 스트링 탐지, 숨김 iframe 탐지, 숨김 applet 탐지, 숨김 object 탐지로 분류된 URL은 악성인지를 정확히 판단하기 위하여 동적분석 모듈에 URL을 전달하여 악성 URL인지 확인한다.

1.3 GUI 기반의 관리기능

본 시스템은 관리자의 편의성을 제공하기 위해 web 기반의 GUI 인터페이스를 제공하고 있다. 시스템 설정, 환경설정 등의 메뉴를 통하여 보다 쉽게 관리자가 웹큐어를 동작시키고 데시보드, 보고서 메뉴를 통해 시스템의 동작상태를 모니터링 할 수 있다.

특히 보고서 메뉴는 특정 기간 동안의 분석 및 탐지 결과를 출력물 형태로 변환하여 각종 통계를 자동으로 생성해주는 기능을 포함하고 있다.

그림 6. 웹큐어 GUI

1.4 웹큐어 활용 방안

본 시스템은 GUI기준으로 크게 2가지 기능으로 나뉠 수 있다. 내부 트래픽을 모니터링하여 악성코드 유포지/경유지로 향하는 트래픽을 탐지하는 기능과 관리자가 지정한 사이트(URL)을 설정한 주기별로 검사를 진행하여 안전하게 사이트를 보호하는 기능이다.

이러한 기능들을 활용하여 기업/기관의 네트워크 망을 악성코드 피해로부터 안전하게 보호 할 수 있다.

Ⅳ. 결론

기존의 악성코드를 직접 분석하거나 패턴에 의해 탐지하는 것이 아니라 악성코드를 웹 사이트에 숨겨 놓거나 해킹을 통해 사용자가 인지하지 못하는 방식으로 배포하는 것을 원천적으로 차단할 수 있는 시스템을 제시하였다.

공격을 받은 후 치료하고 차단하는 방어적인 자세에서 능동적으로 검사하고 사전에 차단하여 대응하는 시스템이다. 크롤링 기술을 이용하여 지속적이고 방대한 데이터를 수집 및 분석하고, 탐지된 악성링크를 차단하여 감염에 대한 위험을 예방하는 것이 이 시스템의 장점이라고 하겠다.

본 시스템에서는 커널 레벨에서의 기존 URL을 차단하는 필터와 실시간으로 방문할 시점의 사이트를 크롤링 기법에 의해 추적하는 필터를 종합하여 다중 필터 형태로 의 시스템을 제작하였다. 본 제안된 시스템을 통해 실제 네트워크에서 활용할 경우 기업과 기관 및 개인에 악성코드에 대한 예방 및 방어를 할 수 있을 것으로 기대한다.

참고문헌

[1] http://www.ahnlab.com/kr/site/securityinfo /*secunews/secuNewsView.do?menu_dist=2&seq=22325*

[2] Hyo-Nam Kim, Realtime hybrid analysis based on multiple profile for prevention of malware, Hongik Univ., Feb. 2014

[3] rovos, N., McNamee, D., Mavrommatis, P., Wang, K., and Modadugu, N. “The ghost in the browser analysis of web-based malware,” Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets, pp. 4-4, Apr. 2007.

[4] Sang-Yong Choi, Multi-level emulation for malware distribution networks analysis, Journal of The Korea Institute of Information Security & Cryptology, VOL.23, NO.6, Dec. 2013

[5] Chang-Wook Park, First URL lookup using URL prefix hash tree, Journal of The Korea Institute of Information Science, Vol. 35, No.1, pp. 67-75, Oct. 2007.

[6] Chen, K.Z., Gu, G., Zhuge, J., Nazario, J., and Han, X.., “WebPatrol: Automated collection and replay of web-based malware scenarios,” Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, pp.186-195, Mar. 2011.

[7] SpiderMonkey, “https://developer.mozilla.org/en-US/ docs/Mozilla/Projects/SpiderMonkey”

저 자 소 개

오 동 엽

2011: 제주대학교
컴퓨터공학과 공학사.
현재: 한국과학기술원
사이버보안연구센터 연구원.
Email: oh51dy@kaist.ac.kr

김 현 우

현 재: 한국과학기술원
사이버보안연구센터
연구원.
Email: babisss@kaist.ac.kr

정 승 일

현 재: 한국과학기술원
사이버보안연구센터
연구원.
Email: sijung@kaist.ac.kr

박 재 경

1994: 동국대학교
컴퓨터공학과 공학사
1996: 홍익대학교
전자계산학과 이학석사.
2002: 홍익대학교
전자계산학과 이학박사
현 재: 학국과학기술원
사이버보안연구센터
책임연구원
관심분야: 네트워크 보안,
사이버 보안
Email: wildcur@kaist.ac.kr