악성코드 종류와 특징

- Worm

  자가 복제 가능. 숙주 없이 독자적으로 실행됨. 네트워크를 통해 전파됨. 웜에 감염된 컴퓨터로 인해 전체 네트워크의 속도가 느려지거나 감염된 컴퓨터를 이용해서 대규모 사이버 공격을 일으킬 수 있다고 함.

- Virus

  자가 복제 가능. 컴퓨터에 침투해서 숙주를 감염시킴. 파일을 통해 전파됨. 스스로 복제하여 파일들을 감염시키며 피해 범위를 확대하려 함. 컴퓨터의 비정상적인 동작을 유발.

- Trojan horse

  다른 적법한 프로그램인 척 위장하여 활동함. 자가 복제 안함. 파일 감염 없음.

- Backdoor

  시스템에 접근할 때 사용자 인증 등 정해진 절차를 거치지 않고 접근할 수 있도록 해줌.

- Bot

  컴퓨터를 공격자가 제어할 수 있도록 해줌. 제어를 위해서는 C&C 서버가 필요하고, 제3자에게 발각되지 않도록 하기 위해 특정 프로토콜을 사용함.

- Spyware

  사용자의 개인정보를 수집하여 공격자에게 전달.

- Ransomware

  파일을 암호화하거나 시스템 부팅을 못하게 해서 파일을 복구해주는 것을 빌미로 돈을 요구함.

IRC 웜

IRC란 전세계를 실시간으로 연결해 대화(채팅)를 나눌 수 있는 범세계적인 채팅 프로그램. 가까운 서버들끼리 직접·간접으로 연결되어 있어 IRC 서버 가운데 어느 한 서버에 연결하기만 하면 자동적으로 전세계 서버와 연결된다.

IRC웜은 IRC 네트워크를 통해 전파되는 웜. IRC 네트워크에 연결되어 있는 또 다른 호스트를 감염시킴. 피해자의 컴퓨터의 IRC 클라이언트 폴더에 스크립트를 떨굼. 피해자가 IRC 채널에 접속하면

스트립트가 자동으로 IRC 클라이언트로 하여금 웜 실행 파일을 채널에 참가한 사용자가에게 전송한다.

IRC 웜 중 하나인 Fagot은 IRC를 통해서 웹사이트 링크를 전송. 링크를 클릭할 경우 .jpg 확장자인 파일을 다운받게 함. 사진처럼 보이지만 실제로는 스크립트 코드를 포함한 html 페이지임. 열어볼 경우 스크립트가 실행됨. Window media player이 patch.exe 파일로 교체됨. 실행파일을 실행할 경우, 실행중이던 프로세스를 죽이고, 윈도우 시스템 폴더에 웜 복제 파일인 userinit32.exe와 dllhost32.exe를 생성하고 레지스트리에 등록하여 부팅 시 실행되도록 한다. 메모장, 시스템 파일 등 윈도우 기본 프로그램을 삭제하고 웜 파일로 대체. 레지스트리 트리 브런치 삭제. IRC 채널에 메시지 발송.

탐지 이벤트로는 레지스트리 등록, 삭제가 탐지될 것 같다.

레지스트리에서 userinit, dllhost32를 삭제하고 userinit32.exe, dllhost32.exe 파일을 삭제한다. 사진을 클릭할 경우 html 페이지로 연결되는데, 이 html 페이지를 차단하는 것도 가능할 것 같다.

https://www.f-secure.com/v-descs/irc-worm.shtml

https://www.f-secure.com/v-descs/fagot.shtml

Sasser 웜

MS04-011 (LSASS) 취약점 악용하는 웜. 웜이 임의의 IP로 접속을 시도하고, 상대가 응답이 있을 경우 이상 패킷을 전송한다. 상대 컴퓨터에 취약점이 존재한다면 감염됨. MS04-011 (LSASS) vulnerability는 원격 코드 실행할 수 있는 버퍼 오버런 취약점.

Avserve.exe을 생성하고 레지스트리에 등록해서 부팅 시 시작되게 함.

TCP 445 포트를 사용해 전파를 시도하면서 패킷이 증가함. 5554 포트 등 다른 TCP 포트를 오픈하기 때문에 후에는 CPU 점유율이 100%까지 올라간다고. 사용자가 정상적으로 컴퓨터를 사용할 수 없음.

탐지 이벤트로는 레지스터 등록과 TCP 445포트를 이용한 통신 시도 로그가 탐지될 거 같다.

MS04-011 취약점을 익스플로잇 하기 때문에 취약점 패치가 중요하다. sasser웜에 감염됐다면 패치를 적용하고 avserve.exe 프로세스를 죽인 후 해당 파일을 삭제한다. 방화벽으로 445 포트를 차단하는 것도 가능.

https://www.f-secure.com/v-descs/sasser.shtml

https://www.ahnlab.com/kr/site/securityinfo/asec/asecView.do?groupCode=VNI001&seq=5976

https://www.ahnlab.com/kr/site/securityinfo/asec/asecCodeView.do?tabGubun=1&virusSeq=1379

Welchia 웜

RPC DCOM(=rpc 인터페이스 버퍼 오버런으로 인한 코드 실행 가능 취약점), WebDAV 취약점(=ntdll.dll에 확인되지 않은 버퍼의 존재로 인한 서버 손상 가능성)을 악용. msblast.exe 파일이 실행되고 있다면 종료한 뒤 해당 파일을 삭제함. Microsoft에서 패치를 다운로드 해서 RPC DCOM 취약점을 패치함. 시스템 폴더에 dllhost.exe, svchost.exe 파일을 생성하고 레지스트리에 등록하여 부팅 시 실행되도록 한다.

ICMP 패킷을 전송하면서 살아있는 시스템을 탐색. 살아있는 시스템을 발견하면 TCP 135 포트의 RPC DCOM 취약점을 악용하여 공격한다. 공격에 성공하면 피해자 컴퓨터의 TCP 707번 포트를 오픈한다.

탐지 이벤트로는 레지스트리 등록, Microsoft를 통한 패치 다운로드 기록이 탐지될 것 같다.

https://www.ahnlab.com/kr/site/securityinfo/asec/asecCodeView.do?tabGubun=1&virusSeq=1206

https://www.giac.org/paper/gcih/517/welchia-worm/105720

NetSky 웜

Netsky 웜은 이메일의 첨부파일 형태로 전파됨. 이메일 메시지 안에 zip파일로 압축되어 있거나 실행파일로 첨부되어 있었음. 파일이 실행되면 service.exe 파일을 생성하고 레지스트리에 등록하여 부팅 시 실행되도록 함. + 레지스트리에 등록되어 있는 값을 삭제.

사용 가능한 모든 공유 폴더에 자가 복제하여 P2P 및 로컬 네트워크에 확산되도록 함.

웜이 share 폴더를 발견하면 해당 폴더에 정상 파일인 척 자신을 복제하여 전파. 인터넷에 연결이 되면 이메일을 통해서 웜을 확산함. 감염된 zip파일 또는 실행파일을 생성하여 이메일에 첨부해 발송. 이메일 발송 대상을 찾기 위해 웜은 CD-ROM 드라이브를 제외한 사용 가능한 모든 드라이브에서 주소를 탐색한다. 메일 수신자가 파일의 압축을 해체하고 실행하면 감염된다.

탐지 이벤트로는 이메일 첨부파일 다운, 메일 발송, 레지스트리 등록, 삭제가 탐지될 것 같다.

https://www.f-secure.com/v-descs/worm_w32_netsky.shtml

Mydoom 웜

이메일과 kazaa P2P 네트워크를 통해 확산. 웜은 윈도우 레지스트리 중 kazaa 공유 폴더를 탐색해서 정상적인 파일인 척 자신을 복제하여 P2P 방식으로 다른 컴퓨터를 감염. 웜은 피해자 컴퓨

터에서 이메일을 발송할 주소를 탐색하여 이메일을 발송한다.

Mydoom 웜이 실행되면 시스템 디렉토리에 taskmon.exe 파일을 복제하고 레지스트리에 등록해서 부팅 시 실행되도록 한다. taskmon.exe는 본문이 인코딩, UPX로 인코딩된 백도어 프로그램인 shimgapi.dll 파일을 생성한다. 이 파일은 TCP 3127 포트부터 3198 포트까지 순차적으로 오픈한다. 공격자가 원격으로 해당 포트에 연결하여 피해자 컴퓨터에 접근할 수 있다. Mydoom은 또한 DDoS 공격을 수행하기도 함.

탐지 이벤트로는 이메일 발송 기록, 레지스트리 등록, 백도어 프로그램을 통한 원격 접근이 탐지될 것 같다.

레지스트리에 등록된 taskmon과 taskmon.exe 파일을 삭제한다.

https://www.f-secure.com/v-descs/novarg.shtml

https://www.okta.com/identity-101/mydoom/

https://nordvpn.com/ko/blog/mydoom-virus/

Bagle 웜

메일을 통해 전파. 감염된 컴퓨터에서 메일 주소를 수집해 웜이 첨부된 메일을 전송. 감염된 시스템이 많을 경우 SMTP서버인 TCP 25번 포트의 네트워크 트래픽이 증가한다.

베이글 웜을 실행하면 시스템 디렉토리에 bbeagle.exe 실행 파일을 생성하고 레지스트리에 등록해 부팅 시 실행되도록 한다. 이 웜이 실행되면 미리 정의된 웹 서버에 연결하고 특정 매개변수와 함께 PHP 파일에 접근하려 한다. 백도어 프로그램이 오픈한 TCP 포트 번호도 이 매개변수 중 하나이다. Bagle 웜에는 백도어 프로그램이 포함되어 있는데, 이 프로그램이 실행되면 TCP 677 포트가 오픈되어 공격자가 피해자 컴퓨터에 원격으로 접근할 수 있다.

탐지 이벤트로는 이메일 발송 기록, 레지스트리 등록, 웹서버 접근 기록, 백도어 프로그램을 통한 원격 접근이 탐지될 것 같다.

레지스트리에 등록된 bbeagle과 bbeagle.exe 파일을 삭제한다. 웜이 실행되며 웹서버에 연결되는데, 이 웹서버를 차단. 677포트 차단.

https://www.ahnlab.com/kr/site/securityinfo/asec/asecCodeView.do?virusSeq=35250&tabGubun=1

https://www.f-secure.com/v-descs/bagle.shtml

관제 업무 중 악성코드 유포 탐지 시 대응 방안

위는 KISA에서 배포한 침해사고 대응 프로세스 중 악성코드 유포만 잘라낸 사진.

악성코드 유포가 탐지되면 유포지를 찾아내어 악성코드 링크, 파일 등 악성코드를 삭제하고 유포지를 차단한다.