Bobax.C 워시바이러스 분석 보고서

2004. 5. 20
인터넷침해사고대응지원센터 (KISC)

※ 본 보고서의 전부나 일부를 인용시 반드시 [자료: 한국정보보호진흥원(KISA)]을 명시하여 주시기 바랍니다.
□ 개 요

Bobax.C 의 특성을 분석하고 원의 감염 전파력 및 네트워크 영향력을 파악하여, 취합사고 예방 및 피해확산 방지를 기하고자 함

○ 국내 이상징후 트래픽 국내유입 일시 : 2004년 5월 16일
  < 최근 TCP 5000 트래픽 증감 변화 추이 (자체 분석 자료) >

![Network Monitoring - TCP SERVICE] Frame

※ 위 TCP 5000의 포트 트래픽이 반드시 Bobax 월관 트래픽이라고 몰수는 없음

○ 원 파일명 및 크기
  W32/Bobax.C 22,528 Byte

○ 확산 방법 및 특징

<table>
<thead>
<tr>
<th>원 이름</th>
<th>확산 경로</th>
<th>확산 관련 포트</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bobax.C</td>
<td>취약점</td>
<td>TCP 135, 445, 5000</td>
</tr>
<tr>
<td></td>
<td>메일</td>
<td></td>
</tr>
<tr>
<td></td>
<td>공유폴더</td>
<td></td>
</tr>
<tr>
<td></td>
<td>P2P</td>
<td></td>
</tr>
</tbody>
</table>

□ 감염 시스템 및 이용 취약점

○ 대상 OS: Windows 2000, XP

○ 이용 취약점:
  LSASS 버퍼 오버린 취약점(MS04-011)
  DCOM RPC 인터페이스 버퍼오버런 취약점(MS03-026,03-039)
□ 주요 공격 및 진파 기법

○ 공격 기법 특성

- LSASS 및 RPC DCOM 네트워크 서비스 취약점을 통하여 진파가 되는 웹으로써 특정 웹서버로부터 수행할 명령을 전송 받은 후, 공격을 실시(RPC 취약점 및 UPnP 스캔, LSASS 취약점 공격 등) 하는 것으로 판단됨
- LSASS 공격시에 먼저 UPnP 서비스 스캔 실시하여, 공격 성공률을 높임

※ UPnP는 WinXP에서만 제공하는 서비스로 스캔 공격을 통하여 OS 식별이 가능하며 스캔후에는 XP에 해당하는 Overflow Offset 값을 전송(LSASS공격)

○ 공격 절차
웹 제작자는 특정 웹서버에 명령어를 올려 놓아 웹 활동을 조성하며 감염된 웹은 특정 웹서버에 접속하여 명령 전달 받음

① 웹은 감염에 성공 후 특정 웹서버(cheese.dns4biz.org, butter.dns4biz.org, kwill.hopto.org)에 접속 함

② 웹은 웹서버에서 수행할 명령을 다운로드 하기 위하여 HTTP GET 전송

웹서버는 웹 제작자가 올려 놓은 웹 활동 명령 전송

③ 다운로드된 명령어의 내용에 따라 웹이 동작되며, 웹 전파시에는 RPC 취약점 및 LSASS 서비스 취약점 이용.

※ 5/20 06시 현재까지 발견된 명령이 전달 웹서버 목록

cheese.dns4biz.org
butter.dns4biz.org
kwill.hopto.org

감염공격 실탐을 위한 명령전달 외에도 웹 업그레이드 및 스파이킹 등 기타 여러가지 명령어 전달이 가능할 것이라고 판단됨

※ 단계별 분석

① 특정 웹 서버 접속

웹이 공격 명령을 전송 받기 위하여 특정 웹서버에 접속하여 Get 요청

GET /reg?u=057AA5E6&v=117&s=106496
② 특정 웹 서버로부터 명령 전달

웹서버로부터 공격 명령 전달 받은 후 해당 명령 (Scan) 수행
전달 명령: 06BB2343 scn

※ 웹브라우저를 통하여 해당 URL에 직접 쿼리 해 본 결과, 아래와 같은 명령어가 확인됨

http://67.15.16.39/reg?u=0577a5e5&v=117&s=1-6406 - Microsoft Internet Explorer
■ OS 변경 사항 및 감염 후 증상
  ○ 감염 후 시스템 변경
    - 파일 추가:
      * 시스템 폴더에 잔당파일 명으로 자산을 복사
    <파일 생성 확인>

      ![표현] (Table Icon)

      1. [Imophealex]
      2. 파일 원본: 유행 프로그램
      3. 설명: [Imophealex]
      4. 위치: C:\Windows\system32
      5. 크기: 22.0KB (22,528 байт)
      6. 디스크 혈당 크기: 24.0KB (24,576 бай트)
      7. 만든 날짜: 2004년 3월 29일 화요일, 오전 6:00:31

    - 부팅시 지정 실행 되도록 레지스트리 추가
      * HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\run 에 추가
    <레지스트리 변경 확인>

    ![표현] (Table Icon)

    1. [Imophealex.exe]

  ○ 랜덤 Port가 open 됨 (원 전송 Port)
    <DOS에서 Netstat -an 명령으로 확인>

    ![표현] (Table Icon)
네트워크 영향력

공격 빈도 및 발생 트래픽

<table>
<thead>
<tr>
<th></th>
<th>TCP 135 (RPC_DCOM)</th>
<th>TCP 5000 (UPnP)</th>
<th>Total (TCP135+5000스캔)</th>
</tr>
</thead>
<tbody>
<tr>
<td>공격 빈도 / 분당</td>
<td>2,723 회</td>
<td>2,740 회</td>
<td>5,524회</td>
</tr>
<tr>
<td>발생 트래픽 / 분당</td>
<td>181,538 Byte</td>
<td>180,712 Byte</td>
<td>366,850 Byte</td>
</tr>
</tbody>
</table>

* 결과치는 확인에 따라 차이가 있을수 있음

<TCP/135 분당 공격 빈도, 발생 트래픽 샘플 >

<table>
<thead>
<tr>
<th></th>
<th>공격 빈도수</th>
<th>공격 트래픽 수</th>
<th>결과시간</th>
</tr>
</thead>
<tbody>
<tr>
<td>2717</td>
<td>IP-10.100</td>
<td>IP-192.168.8</td>
<td>5.248 IP-2701 IP-115 66</td>
</tr>
<tr>
<td>2718</td>
<td>IP-10.100</td>
<td>IP-192.168.8</td>
<td>6.60 IP-2703 IP-115 66</td>
</tr>
<tr>
<td>2719</td>
<td>IP-10.100</td>
<td>IP-192.168.8</td>
<td>4.8 IP-2706 IP-115 66</td>
</tr>
<tr>
<td>2720</td>
<td>IP-10.100</td>
<td>IP-192.168.8</td>
<td>3.214 IP-2707 IP-115 66</td>
</tr>
<tr>
<td>2721</td>
<td>IP-10.100</td>
<td>IP-192.168.8</td>
<td>9.107 IP-2709 IP-115 66</td>
</tr>
<tr>
<td>2722</td>
<td>IP-10.100</td>
<td>IP-192.168.8</td>
<td>0.8 IP-2711 IP-115 66</td>
</tr>
<tr>
<td>2723</td>
<td>IP-10.100</td>
<td>IP-192.168.8</td>
<td>0.233 IP-2713 IP-115 66</td>
</tr>
<tr>
<td>2724</td>
<td>IP-10.100</td>
<td>IP-192.168.8</td>
<td>0.174 IP-2715 IP-115 66</td>
</tr>
<tr>
<td>2725</td>
<td>IP-10.100</td>
<td>IP-192.168.8</td>
<td>0.121 IP-2717 IP-115 66</td>
</tr>
</tbody>
</table>

<TCP/5000 분당 공격 빈도, 발생 트래픽 샘플 >

<table>
<thead>
<tr>
<th></th>
<th>공격 빈도수</th>
<th>공격 트래픽 수</th>
<th>결과시간</th>
</tr>
</thead>
<tbody>
<tr>
<td>2731</td>
<td>IP-10.1</td>
<td>IP-151.1</td>
<td>1.112.17 IP-2594 IP-5000 66</td>
</tr>
<tr>
<td>2732</td>
<td>IP-10.1</td>
<td>IP-151.1</td>
<td>254.159 IP-2595 IP-5000 66</td>
</tr>
<tr>
<td>2733</td>
<td>IP-10.1</td>
<td>IP-151.1</td>
<td>61.237 IP-2598 IP-5000 66</td>
</tr>
<tr>
<td>2734</td>
<td>IP-10.1</td>
<td>IP-151.1</td>
<td>126.204 IP-2599 IP-5000 66</td>
</tr>
<tr>
<td>2735</td>
<td>IP-10.1</td>
<td>IP-151.1</td>
<td>139.251 IP-2702 IP-5000 66</td>
</tr>
<tr>
<td>2736</td>
<td>IP-10.1</td>
<td>IP-151.1</td>
<td>1.145.124 IP-2704 IP-5000 66</td>
</tr>
<tr>
<td>2737</td>
<td>IP-10.1</td>
<td>IP-151.1</td>
<td>1.64 IP-2705 IP-5000 66</td>
</tr>
<tr>
<td>2738</td>
<td>IP-10.1</td>
<td>IP-151.1</td>
<td>1.57 IP-2708 IP-5000 66</td>
</tr>
<tr>
<td>2739</td>
<td>IP-10.1</td>
<td>IP-151.1</td>
<td>70.236 IP-2710 IP-5000 66</td>
</tr>
<tr>
<td>2740</td>
<td>IP-10.1</td>
<td>IP-151.1</td>
<td>18.2 IP-2712 IP-5000 66</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IP-76.15.85.140</td>
<td>IP-2714</td>
<td>IP-5000 66</td>
</tr>
</tbody>
</table>
<Total(TCP/135, TCP/5300 스캔) 분당 공격 반도, 발생 트래픽 셀프>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>[2,400 pps]</td>
<td>[80,000 pps]</td>
<td>[1,000 pps]</td>
<td>[5,524 pps]</td>
<td></td>
</tr>
</tbody>
</table>

○ 트래픽 발생률 비교

- 웹치아.B
- AgcBot441344
- Sasser.A
- Bobax.C

* 결과치는 환경에 따라 차이가 있을 수 있음

○ 공격 대상 주소 생성 분석

- 자신의 수소정보 일부를 이용하여 공격대상 수소 생성
- 자신의 주소 A,B,C,D 중
  - A → 고정, B,C,D → 랜덤 인 경우: 약 30 ~ 40%
  - A,B → 고정 C,D → 랜덤 인 경우: 약 20~30%
  - A,B,C,D 모두 랜덤 인 경우 : 약 30~40%
- 보컬 공격보다 원거리 공격 반도가 매우 높음
□ 위험 요소 예측

○ LAN 및 WAN 위험 요소
  - TCP/135, TCP/445와 다르게, TCP/5000 포트는 Edge 네트워크 단에서 대부분 Filter가 미적용 되어 있으리라 판단되기에는, 월 확산과 비례하여 TCP/5000 Scan 패킷 수의 큰 증가가 예상됨
  - 내부지역 네트워크로의 공격빈도 보다도 외부 네트워크로의 빈도가 큰 것으로 관찰됨. 월이 확산되어, 내부에서 외부로 나가는 SYN 패킷수가 폭증할 경우에는 방화벽 메모리(Stateful Inspection 방화벽의 경우) 및 CPU부하 증가 현상 발생주의. L3 Switch 단 서브넷별 ACL적용 권장

○ 개인 이용자 단 피해 발생 가능성
  - 웹서버를 이용한 웹 동제 통한 개인 정보 유출 가능성
  - 개인 PC가 Spam Relay로 악용될 가능성

□ 향후 전망

○ 예전 Sasser 월 감염시, 재부팅 현상이 발생하였으므로, 많은 취약 OS들의 재설치 및 패치가 이미 이루어졌을 것이라 판단되나, 방화벽이 설치된 기관 내부에서는 Sasser 월의 피해 발생이 상대적으로 매우 적었으므로, 아직 LSASS 미패치된 OS가 다수일 것으로 추측됨.
  ADSL 및 기타 방법으로 기관내부에 월 점투시 피해발생이 가능하므로 LSASS 취약점에 대한 신속한 패치 실시 필요.

○ 웹서버를 통하여 밍령어를 전달하므로 DDoS등 예상치 않은 피해 발생 가능성 존재. 명령전달 웹사이트에 대한, 신속한 조치가 필요
ो UPnP서비스 스캔과 LSASS 취약점 공격을 병행하는 다른 신중 퀵 출현이 예상되므로 신속히 폐지 실시
ो 웹서버를 통한 웹 Upgrade 실시가 예상되고, 기능 강화된 변증 퀵 출현 가능성이 높다고 판단됨.

□ 예방 및 대응 방안
ो 웹 명령 진달 웹사이트 신속 차단 및 변송 출현 수시
※ 2004.5.20 03시 현재 기준
   cheese.dns4biz.org, butter.dns4biz.org
   해당 사이트는 국외 사이트인 것으로 파악되었고, 조치를 요청하였음
   kwil.hopto.org
   ※ 현재 조치가 완료되어 접근이 불가
ो MS04-011,MS03-026,03-039 취약점 신속한 폐지 실시
ो 스위치 및 라우터에서 세그먼트 별 TCP445,135,5000 포드에 대한 차단.
   ※ 최소 관문 라우터에서는 필터 적용 권고
оБ업내 방화벽 설치 및 정책 적용
оЊ 백신 업데이트 및 주기적 점검 실시

□ 참고 (명령전달 웹사이트 차단 시 예방효과 테스트)
o 웹 명령 진달 웹사이트에 대한 접근을 차단한 후, 웹 활동 현상 을 관찰.
미치던 상태에서 웹을 감시했을 경우, 다 시스템으로의 전파 공격발생이 관찰되었지만, 웹에 공격 명령이 전달되지 않도록 명령전달 웹사이트와의 통신을 차단하고 김연식인 경우에는 스캔공격이 발생하지 않는 것으로 관찰되어 명령 전달 사이트에 대한 차단 조치시 큰 효과가 예상됨.
<감염 후 공격 패킷 발생률 샘플>
▶ 명령전달 사이트 미치단 상태에서
PC 감염 후 pps 관찰
▶ 명령 전달 사이트 차단 상태에서
PC 감염 후 pps 관찰

◆ Microsoft 취약점 패치 정보
☞ 자동 패치
http://v4.windowsupdate.microsoft.com/ko/default.asp
☞ 개별 패치
* RPC DCOM 취약점
  .MS03-026
  http://www.microsoft.com/korea/technet/security/bulletin/MS03-026.asp
  .MS03-039
  http://www.microsoft.com/korea/technet/security/bulletin/MS03-039.asp
* LSASS 취약점
  .MS04-011
* UPnP 취약점
  .MS01-059
  http://www.microsoft.com/korea/technet/security/bulletin/MS01-059.asp