KRNIC
한국인터넷정보센터

인터넷 주소자원 관련
동향 및 주요 이슈

-2015년 12월 3호-

리눅스 노린 XOR DDoS 공격

□ 개요

o Akamai의 리눅스를 노린 XOR DDoS공격 보고서

o DDoS 공격의 초점이 윈도우에서 리눅스로 변경

□ 주요 내용

o XOR DDoS 공격

- 리눅스 하이재킹용 트로이 목마 악성코드인 XOR DDoS 공격 대역폭이 한 자릿수에서 시작해 150Gbps 이상으로 진화
- 최대치 179Gbps에 달하는 공격이 발견, 가장 많은 공격을 받은 분야는 게임이고, 그 다음은 교육기관
- XOR DDoS에 감염된 봇넷은 하루 평균 20곳의 표적을 공격했고 전체 표적의 90%는 아시아에 집중

▪ XOR DDoS

1. 공격자가 원격으로 리눅스 시스템을 감염시켜 온디맨드(On-demand) DDoS 공격을 실시하도록 지시하는 트로이 목마
2. 공격자는 무차별 공격을 실행해 시큐어 쉘(Secure shell) 비밀번호를 알아냄
3. 루트 권한을 획득하여 bash 쉘 명령어로 악성코드를 다운로드한 후에 실행시킴

o 윈도우 시스템에서 리눅스 시스템으로 이동

- 과거 봇마스터가 가장 좋아했던 시스템은 윈도우 시스템이었으나 시대가 변화하면서 공격의 타깃도 변함
- 데이터센터에서 도입이 크게 확대된 리눅스 기반 네트워크가 주된 표적으로 변경
- 리눅스는 복원성이 뛰어나다는 통상적 이유로 운영, 유지관리에 있어 문제가 없다는 사고방식이 만연해 있었던 것도 이유 중 하나임

o 향후 전망

- 지난 1년간 XOR DDoS 봇넷은 대형 DDoS 공격을 감행할 정도로 성장, 앞으로는 윈도우를 겨냥한 DDoS 공격보다 더 자주 발생할 정도로 급증
- 지속적인 모니터링 및 악성코드 감염파일 식별, 메인 공격 프로세스를 지원하는 공격 프로세스 식별, 악성 프로세스 제거, 악성코드 감염 파일 제거 등 4단계 제거 기법을 권고

■ 4단계 제거 기법 예시

- 1단계 : 메인 PID와 /boot와 /etc/init.d로 드롭(drop)된 파일들을 식별함

```
root@ubuntu:/# ls -lha /boot ¦ egrep " [a-z]{10}$"
-rwxr-x--- 1 root root 606K Aug 19 11:42 utmhsahoca
root@ubuntu:/# ls -lha /etc/init.d/utmhsahoca
-rwxr-x--- 1 root root 28 Aug 19 11:42 /etc/init.d/utmhsahoca
root@ubuntu:/# find /proc/ -name exe 2> /dev/null ¦ xargs -I{} ls -l {} 2> /dev/null ¦egrep '/boot/[a-z]{10}$'
lrwxrwxrwx 1 root root 0 Aug 19 11:42 /proc/3746/exe -> /boot/utmhsahoca
```

- 2단계 : 메인 프로세스를 지속하게 해주는 supporting 프로세스 식별

```
root@ubuntu:/boot# ps -eaf -u root ¦ grep `date +%H:%M` ¦ egrep -v "ps¦grep"
root 8318 2868 0 12:04 ? 00:00:00 ps -ef
root 8321 2868 0 12:04 ? 00:00:00 cat resolv.conf
root 8324 2868 0 12:04 ? 00:00:00 ls -la
root 8326 2868 0 12:04 ? 00:00:00 id
root 8327 2868 0 12:04 ? 00:00:00 ls -la
```

- 3단계 : 메인 프로세스 "Kill"

```
root@ubuntu:/boot# ps -eaf ¦ grep ^root ¦ grep `date +%H:%M` ¦ egrep -v "ps¦grep" ¦ awK'{print $2}' ¦ xargs -I{} kill -9 {}; kill -9 3746
```

- 4단계 : 1단계에서 식별한 드롭(drop)된 파일을 /boot와 /etc/init.d에서 삭제

```
root@ubuntu:/boot# rm -f /boot/utmhsahoca && rm -f /etc/init.d/utmhsahoca && /lib/udev/udev
```

□ 출처

o 2015-threat-advisory-xor-ddos-attacks-linux-botnet-malware-removal-ddos-mitigation-yara-snort.pdf