3.3 DDoS Attack Report

(2011')

㈜ 하우리 보안대응센터

3.3 DDoS 공격 대응 Report

▣ 공격 배경 및 목적

3.3 DDoS 공격자와 배후세력은 파악되지 않았지만, 기존 DDoS 공격 수법 보다 더욱더 교묘하고 진화된 기술적 수법을 사용하여 사회적인 혼란과 피해를 유발하기 위해 제작되었다. 이를 위해 가장 접근이 쉽고, 관리가 소홀하며 일일 많은 회원들이 접속하여 자료를 다운받고, 업로드를 하는 웹하드 업체들을 그 타켓으로 선택하였다.

▣ 감염 경로

악성코드 제작자는 웹하드 업체인 쉐어박스, 슈퍼다운, 보보파일, 파일시티 4곳의 업데이트 모듈을 변조하여 업데이트가 진행되면 공격자의 명령에 따라 악성코드에 감염되어 좀비PC가 된다.

▣ 주요 증상

- 웹사이트 DDoS 공격(공공기관, 국가기관, 금융기관
- 특정 웹사이트 접속 차단(백신업체, 보호나라 등)
- 시스템 하드디스크 파괴(MBR 영역 파괴, Physical 하드정보 삭제)
  : 쉐어박스 유포 파일(감염시간 + 4일후) / 슈퍼다운 유포 파일(감염시간 + 7일후) 파괴시작
  : 5일(토) 접수된 악성코드는 감염 즉시 파괴
- 파일 파괴(특정 확장자의 파일은 0으로 지움)

▣ 좀비 PC 피해 통계

(YTN 보도자료)

날짜	공격 통계
4 일(금) 10 시	2 만 4,000 여대
4 일(금) 18 시 30 분	5 만 1,000 여대
5 일(토) 10 시 45 분	만 여대

▣ 디스크 파괴 피해 접수 현황

기준 : 3 월 6 일(일) 18 시

신고내역	KISA	Ahn	Hauri
상담전화	51 건	11 건	3 건 (메일 2 건/전화 1 건)

▣ 3.3 DDoS 공격 대응

날짜	상황 접수	대응 진행
3.3 (목)	오후 5시경 - 고객사로 부터 DDoS 징후 발생, 접수	- KISA 맞춤형 전용백신(54호) 제작 - 샘플 분석 및 패턴 작성, 보고서 작성
	오후 7시 30분	- 자사 전 제품 업데이트 완료.(2011-03-03.04)
3.4 (금)	오전 9시 30분 - 국정원으로부터 DDoS 샘플 접수	- 샘플 분석 및 패턴 작성, 보고서 작성- - 공격 대상 웹사이트 확인 - 공격 대상 웹사이트 모니터링 - 상황 파악, 상황 전파, - 상황 모니터링(SNS, 보도자료, 웹검색 등) - 홈페이지 긴급공지 게재
	오전 10시 - 공격 예상 시간	- 공격 대상 웹사이트 확인 - 공격 대상 웹사이트 모니터링 - 상황 모니터링(SNS, 보도자료, 웹검색 등)
	오전 11시 50분	- 하우리 긴급코드 3단계 발령(경계)
	오전 11시 57분	- DDoS 긴급공지 메일 발송
	오전 10시 19분	- KISA 맞춤형 전용백신(54호) 제작 // (3차 추가샘플적용)
	오후 12시 33분	- 자사 전 제품 업데이트 완료.(2011-03-04.02)
	오후 2시 41분	- 좀비 PC 하드 파괴 접수(메일 1건) - 고객이 임의로 시스템 날짜를 변경하여 피해 발생됨.
	오후 5시 27분	- KISA 맞춤형 전용백신(54호) 제작 // (4차 추가샘플적용)
	오후 6시 30분 - 공격 예상 시간	- 공격 대상 웹사이트 확인 - 공격 대상 웹사이트 모니터링 - 상황 모니터링(SNS, 보도자료, 웹검색 등)
	오후 7시 07분	- 홈페이지 3.3 DDoS 분석 Report 공지
	오후 8시 06분	- 보도자료 배포(3.3 DDoS 시스템 시간 변경시 PC 시스템 파괴 위험)
	오후 8시 22분	- 자사 전 제품 업데이트 완료.(2011-03-04.04)
3.5 (토)	오전 8시	- KISA 맞춤형 전용백신(54호) 제작 // (추가샘플적용) - 공격 대상 웹사이트 확인 - 공격 대상 웹사이트 모니터링 - 상황 모니터링(SNS, 보도자료, 웹검색 등)
3.5	오전 8시 20분	- KISA 맞춤형 전용백신(54호) 제작 // (5차 추가샘플적

(토)		용)
	오전 10시 30분 - 공격 예상 시간	- KISA 맞춤형 전용백신(54호) 제작 // (추가샘플적용) - 공격 대상 웹사이트 확인 - 공격 대상 웹사이트 모니터링 - 상황 모니터링(SNS, 보도자료, 웹검색 등)
	오전 11시 04분	- 좀비 PC 하드 파괴 접수(메일 1건) // 총 2건 - 고객이 임의로 시스템 날짜를 변경하여 피해 발생됨
	오전 11시 54분	- 자사 전 제품 업데이트 완료.(2011-03-05.02)
	오후 12시 10분	- KISA 맞춤형 전용백신(54호) 제작 // (6차 추가샘플적용)
	오후 10시 56분	- KISA 맞춤형 전용백신(54호) 제작 // (7차 추가샘플적용) - 감염 즉시 하드디스크 파괴시키는 샘플 접수 - 샘플 분석 및 패턴 작성, 보고서 작성
	오후 11시 20분	- 감염 즉시 하드디스크 파괴 증상 확인
3.6	오전 6시 04분	- 자사 전 제품 업데이트 완료.(2011-03-06.00)
(일)	오후 5시 01분	- 홈페이지 안전모드 점검 가이드 업로드 완료

▣ 3.3 DDoS 추후 대응

C&C 서버의 명령이 변경되면 변형 공격이 가능함으로 주기적인 상황 모니터링과 하드디스크 파괴 증상의 피해를 최소화 하기 위해 정부기관과 함께 DDoS의 위험성을 대대적으로 홍보하고 백신 프로그램의 설치의 의무화를 강조하고 3.3 DDoS 전용백신으로 시스템 점검을 권장하도록 한다.

▣ 3.3 DDoS 샘플 세부 진단내역

공격 내용	공격 대상	내 용	업데이트 진단명
1차 공격 발생 (3.3 오후 5시경)	29여곳	고객사로 부터 최초 공격을 신고 및 보고 받았으며, KISA 측으로부터 샘플을 접수 받아 KISA 맞춤형 전용백신 및 바이로봇 업데이트 완료. (2011-03-03.04)	// Hosts was Modified by Malware SBUpdate.exe (Trojan.Win32.S.Downloader.10240.AF) SBUpdate.exe (Trojan.Win32.S.Downloader.11776.Y) soetsvc.dll (Trojan.Win32.S.Generic.46432) wtcesvc.dll (Trojan.Win32.S.Obfuscated.40960) ntds50.dll (Trojan.Win32.S.QHost.118784) mopxsvc.dll (Trojan.Win32.S.Generic.71008)
2차 공격 발생 (3.4 오전 10시)	40여곳	(2011-03-04.02)	setup_bobofile.exe (Trojan.Win32.Downloader.11776.MH) setup_filecity.exe (Trojan.Win32.Downloader.20480.ALQ) rtdrvupr.exe (Trojan.Win32.Qhost.16384.G) ntgg55.dll (Trojan.Win32.Qhost.126976) wricsvc.dll (Trojan.Win32.Generic.42320) ssaxsvc.dll (Trojan.Win32.Generic.46416) mdomsvc.dll (Trojan.Win32.Generic.71008)
3차 공격 발생 (3.4 오후 18시 30분)	29여곳	국정원, 외교통상부, 주한미군, 외환은행, 농협, 키움 증권 일시적인 접속 장애 발생 확인 되었음. (2011-03-04.04)	SBUpdate.exe(원본 파일명 추정) (Trojan.Win32.Agent.10240.DP) (원본 파일명 알수없음) (Trojan.Win32.Generic.24576.I)
4차 공격 발생 (3.5 오전 8시)	29여곳	청와대, 디시인사이드 접속 장애 발생 확인	setup.exe (Trojan.Win32.Generic.13312.B)

		되었음. (2011-03-05.02)	newsetup2.exe (Trojan.Win32.Generic.27648) wtvtsvc.dll (Trojan.Win32.Generic.36864.I) messsvc.dll (Trojan.Win32.Generic.71000) svki65.dll (Trojan.Win32.Generic.77824.L) dasrrvm.dat (Bin.S.Agent.8) doqmcru.dat (Bin.S.Agent.616) faultrep.dat (Bin.S.Agent.112)
5차 공격 발생 (3.5 오전 10시 45분)	29여곳		(접수된 변종 샘플 없음)
6차 공격 발생 (3.5 오후 18시 30분)	29여곳	해커로부터 C&C 지령이 변경되어 감염 즉시 하드 파괴 악성코드 다운로드 및 실행됨. (2011-03-06.00)	(원본 파일명 알수없음) (Trojan.Win32.Generic.57948) srsjproc.dll (Trojan.Win32.Generic.24576.J) TYEI08.DEP (Bin.S.Agent.16) muropc.dll (Bin.S.Agent.4674) (원본 파일명 알수없음) (Trojan.Win32.Generic.16384.B) tljoqgv.dat (Bin.S.Agent.616.A) jzsltpcy.exe (Trojan.Win32.Qhost.16384.H)

<안전모드 점검 가이드>

http://www.hauri.co.kr/updata/SafeModeGuide.pdf