인터넷뱅킹 악성코드 감염 시 치료방법

최근들어 인터넷접속을 통해 PC에 악성코드가 감염되어, 인터넷뱅킹 거래가 정상적으로 이루어 지지 않은 사례가 발생하고 있습니다. 고객님의 PC에 다음과 같은 사례가 발생 될 경우, 악성 코드에 감염된 가능성이 많으므로, 당행 고객센터 신고(1577-8000) 및 악성코드 치료 후 거래하시기 바랍니다. 아래 방법으로 악성코드 치료 후에도 동일한 증상이 발생하면 PC A/S를 받아보시길 바랍니다.



번호

76

75

V3 GameHack Kill

Dropper/Agent. 429808

■ 거래 멈춤현상 등 신종 악성코드 감염 시 업무절차 (상기 ①②번 감염사례 경우)
- 결제를 위한 정보입력 후 멈춤 혹은 정보입력창이 특징임
① 이체완료 단계 인증서 암호입력 시 등 거래 도중 멈춤 현상 발생 (신종)
② 보안강화 등을 이유로 보안카드 일부 팝업창으로 입력요구 (신종)
-특히, <u>보안카드 번호 입력 진행까지 마친 경우</u> 즉시 고객센터(1577-8000) 연락하여
보안카드 분실신고 및 계좌 지급정지 신청하시기 바랍니다.
-이후 PC 악성코드 치료, 가까운 영업점을 방문하셔서 OTP 등 보안카드 재발급
인터넷뱅킹에서 전자금융사기예방서비스 가입(뱅킹보안센터 메뉴) 하시기 바랍니다.
▶ 악성코드 치료절차
- 전용 백신을 통해 정밀검사 (<u>http://www.ahnlab.com</u>)
1) 전용 백신 설치(다운로드 > 무료제공파일 > gamehackkill.exe)
시큐리티센터 보안정보 다운모드 고객지원 56668
제중관련 파일 30일 평가판 무료제공 파일 다운로드 아옹안내
전용백신 HOME > 다운로드 > 무료제공 피일 > 전용백신
전용백신 이용안내
1. 전용백신은 특정 악성코드 진단/치료를 위한 파일입니다. 2. 전용백신은 악성코드 예방 및 확산 방지를 위한 모든 사용자에게 무료로 제공됩니다.

이므로, 예방을 위한 시스템감시 기능은

제공일자

2013-08-01

2013-07-26

h 있을 경우, 이를 먼저 '일시중지' 이로 인해 데이터 또는 금전적 손실

> 전용백신 다운로드 🕞 gamehackkill.exe

😡 v3_integration.exe

2) 전용백신을 통한 악성코드 탐지 및 치료(검사 진행)

악성코드 명

3. 전용백신은 감염된 시스템을 치료하기 위한 용

4. 전용백신은 정기적인 업데이트를 제공하지 않습니다

5. V3의 시스템감시나 타사 백신의 실시간 감시가 실행되어 있 하신 후 전용백신을 실행하여 검사하시기 바랍니다.
6. 전용백신 실행 이후 컴퓨터 기능에 문제가 발생하거나 이뢰 이 발생하더라도 책임지지 않습니다.

제공되지 않습니다.

VINL	더	/s;c: :	₩Pro	gram Fi	les;C:₩E	Documer	nts and Se	ttings₩		검사		설제지료
일	명	:										
수:	0		J. i	감염 수	: 0	L.	시작 시간	:	11	경과 시간	:	00:00:00
님명	ļ		폴	더				진단명			상타	1
	일 수: 명	더 일 명 수: 0 실 명	더 : 일명 : 수: 0	더 : 일명: 수: 0 ;	더 : 일명 : 수:0 간염수 !명 풀 더	더 : 일명 : 수: 0 감염수: 0 ! 명 폴 더	더 : 일 명 : 수: 0 간 염 수: 0 ! 명 볼 더	G : 일 명 : 수: 0 감염수: 0 시작시간 ! 명 돌 더	G : 일 명 : 수: 0 감염수: 0 시작시간: ! 명 풀 더 진단명	대 : 일 명 : 수: 0 감염수: 0 시작시간: 상명 폴 더 진단명	더 : 일 명 : 수: 0 감염수: 0 시작시간: 경과시간 ! 명 폴 더 진단명	더 : 일 명 : 수: 0 감염수: 0 시작시간: 경과시간: ! 명 풀 더 진단명 전단명 상태

※ 검사 완료 후 '전체 치료' 클릭 시 '<u>재부팅 후 검사 재진행 메시지'가 나오면</u>
 '확인'을 누르고, <u>재부팅 및 재검사</u>를 통해 잔재하는 악성코드를 치료 바랍니다.
 (재부팅 전 저장 및 확인이 필요한 부분이 있으면 반드시 먼저 처리 바랍니다)

3) V3실행 → 엔진 업데이트 버튼 클릭 (우측 하단)



4) 고급설정 → Smart Defense 사용 (체크) → 진단수준 선택 : 높음



5) 정밀검사 버튼 클릭 (검사진행)



■ 보안카드번호 전체 입력요구 악성코드 감염 시 업무절차 (상기 ③④번 감염사례 경우)

'③ 보안카드 번호 전체, ④금융사기 안내 후 개인정보 입력유도'가 특징임
 -특히, <u>보안카드 번호 입력 진행까지 마친 경우</u> 즉시 고객센터(1577-8000) 연락하여
 보안카드 분실신고 및 계좌 지급정지 신청하시기 바랍니다.

- -이후 PC 악성코드 치료, 가까운 영업점을 방문하셔서 OTP 등 보안카드 재발급 인터넷뱅킹에서 전자금융사기예방서비스 가입(뱅킹보안센터 메뉴) 하시기 바랍니다.
- 악성코드 치료절차
- 개인용 무료 백신인 V3 Lite, 알약 등을 통해 정밀검사
- 1) V3실행 → 엔진 업데이트 버튼 클릭 (우측 하단)



2) 고급설정 → Smart Defense 사용 (체크) → 진단수준 선택 : 높음



3) 정밀검사 버튼 클릭 (검사진행)



- ▶ 만약, 악성코드로 인해 백신 프로그램이 실행되지 않는 경우 아래절차 진행 (선택조작) -인터넷뱅킹 홈페이지 AOS(Ahnlab Online Security) 를 통해서 검사진행
- 1) 인터넷 주소창에 http://59.7.252.100 입력 (신한은행 홈페이지)
- 2) 인터넷뱅킹 로그인 버튼 클릭

은 신한은행 개인범킹 [6p-xrib2_3] - Windows Internet Explor	er	
C C + K + K + K + K + K + K + K + K + K		
파일(E) 편집(E) 보기(V) 즐겨찾기(A) 도구(T) 도움말(H)		
🖕 즐겨찾기 🛛 🕥 신한은행 개인뱅킹 [6p-xrib2_3]		
	개인 기업 패밀리뱅킹 오픈뱅킹	스마트금융
🔇 신한은행	개인뱅킹 자산관리 예금 대출 펀드	외환 골!
Q	조회 이체 신규/해지 공과금/법원 골드뱅킹 금융서비스 사용자관리	뱅킹보안센터 7
	인터넷뱅킹 로그인 也 공인인증센터 ≽	
	조회 이체 공과금센터 지로납부 간변서비스	신한5뱅크

3) 아래 메시지가 표시될 경우 '예(Y)' 를 선택 → 보안프로그램 설치

증신한은행Ⅰ개인뱅킹[6p-xrib2_7]	 Windows Internet Explorer 		
😋 💿 🗢 🔇 http://59, 7, 252, 100,	/index.jsp	💌 🐓 🔀 🔂 Bing	<u></u>
파일(E) 편집(E) 보기(<u>V</u>) 즐겨	찾기(<u>A</u>) 도구(<u>T</u>) 도움말(b	Ð	
🖕 즐겨찾기 🛛 🏤 🔁 추천 사이트 🗸	🛛 🙋 Get more Add-ons ·		
⊖ 신한은행 개인병킹 [6p-xrib2_7]		🏠 👻 🗟 👻 📑 👼 👻 페이지(P) ·	• 안전(<u>S</u>)• 도구(<u>O</u>)• 😯
	고객님의 안전	한인터넷뱅킹 이용을 위하여 보안프로그램 설지 중 입니다.	
INISA	FE SFilter v7.2 Error		
	59,7,252,100은 인증서에	에 포함되지 않는 도메인으로 신뢰할 수 없습니다. RETA 아유 도메인 저너로 사리하지 않는 것이 다.	
	좋으며, 특히 해당 사이.	특되지 않은 노매인 정보로 전퇴될 수 없습니다. 따라지 더 미양 전쟁하지 않는 것이 트에서 이 경고를 처음 보는 것이라면 더욱 주의해야 합니다.	
	예 : 문시하고 계속 진행 마니오 : 중지하기	(하기) 도우막	
		예(쏘) 마니오(\\) 인쇄하기	
		Lt.	
	• Mac 이용 고객용 _ 년	IA 읽어모세요 INF ezPlus for Mac 나운도드	
	· · · · · · · · · · · · · · · · · · ·	MALELON # 1577 0000 1544 0000	
	00058 I MT	객센디컨네 1577-6000, 1544-6000	

- 중 신한은핵 | 개인뱅킹 [6p-xr/b2_7] Windows Inte 중 ⓒ ⓒ ♡ ◎ 🐼 http://59.7.252.100/index.jsp 8 × 💌 😽 🐹 📴 Bing 파일(E) 편집(E) 보기(Y) 즐겨찾기(A) 도구(I) 도움말(H) 🍃 즐겨찾기 🛛 🚑 💽 추천 사이트 - 🖉 Get more Add-on 🚱 신한은행 | 개인병킹 [6p-xrib2_7] 🐴 • 📾 - 🖃 🚔 • 페이지(P) • 안전(S) • 도구(Q) • 개인 기업 패밀리뱅킹 오픈뱅킹 스마트금융센터 금융서비스 신한멤버스 고객센터 은행소개 LANGUAGE 신한은행 미션플러스 Q, 조회 이체 신규/해지 공과금/법원 골드뱅킹 금융서비스 사용자관리 뱅킹보안센터 카드/증권 TOTAL MENU + 💦 은행을 사칭한 전화금융사기 및 피싱/파밍사이 인터넷뱅킹 로그인 🕛 ※ 신한은행은 보안승급, 보안강화를 위해 주민등록번호 계좌 비밀번호, 보안카드 번호 전체를 요구하지 않습니 절대로 비밀번호와 보안카드 번호 전체를 입력하지 마습 공인인증센터 > 최근 은행을 사칭한 금융사기 범죄가 빈번히 발생하고 있어 사례를 피해가 발생되지 않도록 주의를 당부드립니다. "고객정보유출로 보안강화 서비스 신청하기 신한은행과 유사한 사이트로 접속을 유도한 번호 및 비밀번호를 입력하게 하는 사례 피싱/파밍사이트 피싱사이트 주의 안내 0 \mathbf{x} G (Ë 은행 또는 공공기관을 사칭하여 개인정보, 유출 또는 자금이체를 요구하는 사례 전화금융사기 전화 금융사기예방안내 전자금융사기 예방서비스 🂦 은행 또는 대출 상담사를 사칭한 대출 주의 안니 은행을 사칭하여 '대출기능여부 또는 한도 확인 하세요' 등의 전화 발생하고 있습니다. 신한은행은 대출 승인, 한도 추가등을 조건으로 등 금풍을 고객에게 요구하거나 재직증명서등의 서류를 팩스, 유선 입습니다. (G출시기 피해유원 및 - [공지] 신한은행을 사칭한 피싱사이트 주의 안내 > 인터넷 뱅킹 이용시 유의사할 스마트펀드센터 355 everyday 신규서비스 출시 2011년 2월 1일부터 [금융IC카드 전용사용] 시법문영... 인쇄프로그램 재설치 안내
 보안프로그램 재설치 방법 대출사기 피해유형 및 파상 사이트 발견시 신한은행 고객센터 (1577-8000), 인터넷: 대출 전화/문자신고 신한은행 고객센터 (1577-8000), 경찰서 전화금융사기 피해 |방 안내 👂 रेतर -외환센터 오픈기념 인터넷환전 댓글 달기 이벤트 인터넷환전 댓글 달고 환율우대 10% 데!! 1 비근 공공기관을 사칭한 전희금등 보이스파싱, 메신져파싱) 주의 일주일동 A 🥐 시작 🗍 🏈 동안물고... ∫ 🔊 비 ロレ ... 🧑 カイさき ...) 🚱 신むきせ ... 🦢 248 To...) 🚱 사용 자 ...) 🚱 化容 とう...) 👰 化한 은 ... 🗋 에 신 차수... | 🔤 전 감수 🖓 😭 🖓 😭 🖓 😭 🖓 😭
- 4) 악성코드 검사 (Ahnlab Online Security) 아이콘 클릭 (우측 하단에 있음, 공모양)

5) PC검사 메뉴 선택



6) 정밀검사 클릭



7) 모든파일 선택 → 검사하기

Lab Online Security	?	-
□ □ ●<		
 검사대상 선택 ● 모든 파일 ● 감염되기 쉬운 파일(상행 파일, 태크로 파일, 스크립트 파일) 		
김사대상 선택 ⓒ 모든 파일 ⓒ 감영되기 쉬운 파일(상행 파일, 배크로 파일, 스크립트 파일) ☞ 약성코드 자동 치료		

PC의 hosts 파일 복구조치
 -사기 홈페이지 악성코드는 윈도우 hosts 파일을 변조하므로, 이 파일을 원상복구 조치

1) 이메일을 통해 사기사이트 IP 차단 신고 (선택사항이나 가능한 처리 부탁)

-신고내용 : 추가 피해확산을 방지하기 위해 사기사이트 차단신고

-신고방법 : pc의 hosts파일을 <u>shbcert@shinhan.com</u> e-mail 주소로 첨부하여 발송함

디렉토리 위치 c:₩windows₩system32₩drivers₩etc 첨부파일 : hosts 파일

🚔 C : \WINDO \S \System 32\Wdrivers \Wetc						
파일(E) 편집(E) 보기(⊻) 즐겨찾기(<u>A</u>) 도구(<u>T</u>) 도움말(<u>H</u>)						
🔆 뒤로 - 🕞 - 🎓 🔎 검색 🎼 풀더 💷 ·						
주소(D) 🗁 C:₩WINDOWS₩system32₩drivers₩etc						
좋더	×	01 = (1 EC	종류	수정한 날짜	
C sustem		🖬 hosts	31K	3 파일	2013-02-15 오전	
System 32	-1	🚖 hosts	21K	3 문서로 바로 가기	2005-05-17 오후	
📇 🛄 Systemse		🖬 hosts, 2011	8K	3 2011 파일	2011-03-09 오후	
1025		📷 hosts, 2012	8K	3 2012 파일	2011-03-09 오후	
1028		📷 hosts, 5001	26K	3 5001 파일	2007-10-22 오후	
1031		📷 hosts, 9999	8K	3 9999 파일	2011-03-09 오후	
1033		📩 hosts, old	7K	B OLD 파일	2011-05-31 오후	
1037		📑 hosts, org	26K	B ORG 파일	2006-11-29 오전	
1041		nosts_tmp	31K	5 파일	2012-08-10 오후	
1042		🔄 Imhosts sam	4K	3 SAM 파일	2006-08-04 오후	
1054		networks	IK	5 파일	2006-08-04 오후	
2052		protocol	IK	5 파일 - 파이	2006-08-04 오후	
3076		services	51	5 ILB	2004-03-02 또신	
🛅 ADSpider, exe						
🗉 🚞 apprograt						
🚞 bits						
🗉 🧰 CatRoot						
🗉 🧰 CatRoot2						
🛅 Com						
표 🚞 config						
🛅 ctvmon32, exe						
🛅 dgtnmres, dll						
i dgtstart, exe						
ancp						
DigitalNamesStart, exe						
DirectX						
i alsan						
C BIC						

2) 인터넷 주소창에 http://support.microsoft.com/kb/972034/ko 입력

-Microsoft사 hosts 파일 초기화 사이트 접속하여 처리함 hosts파일이 초기화 되므로, 별도 설정한 값이 있을 경우 주의 (전문가용 PC 등)

3) 마우스를 아래로 내려서 hosts 파일 복구 프로그램 다운로드 (Fix it 버튼)



4) 다운받은 프로그램을 실행 → ⑤ 종료 후 PC를 재부팅 함



5) 신한은행 인터넷뱅킹 정상 사이트 접속 확인 (banking.shinhan.com)



▶ 인터넷뱅킹 접속 후 보안승급 강화이유로 개인정보 상세 입력이나 보안카드번호 전체 요구 등 화면이 더 이상 나오지 않아야 합니다.

▶ 인터넷뱅킹 악성코드 감염 예방법

- 백신 프로그램의 자동 업데이트를 설정
- 잘 모르는 웹사이트는 접속하지 않음
- 정품 소프트웨어를 사용
- 출처가 불분명한 파일은 다운로드하지 않음
- 이메일 첨부파일 열기 전, 인터넷뱅킹 이용 전 악성코드 검사 (V3나 알약 등)
- 이메일을 통해 전달된 링크는 직접 클릭하지 말고 주소창에 직접입력해서 확인

▶ 인터넷뱅킹 금융사기 방지안내

- 은행에서는 절대 보안승급을 요청하지 않음. 계좌번호, 비밀번호, 보안카드 번호 전체를 요구하면 바로 고객센터에 신고함
- 서비스 이용 시 의심스러운 부분이 있으면 고객센터에 확인
- 만약 개인 금융정보가 유출되었다면 즉시 고객센터에 계좌 지급정지, 보안카드 분실신고