

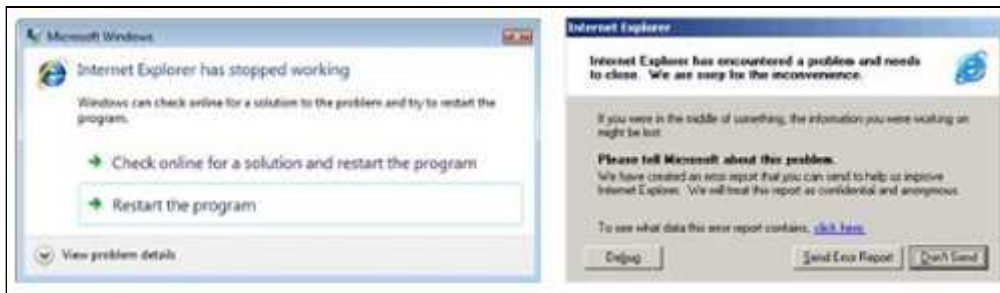
보안뉴스 미디어

‘오류 보고 메시지’, 해커의 정보 획득 수단?

2014-01-10

윈도우 보고 메시지의 사용자 정보 유출 가능성 제기

[보안뉴스 김경애] 운영체제가 시스템 오류 발생, 하드웨어 변경 등의 상황을 마이크로소프트 서버로 전송하기 위해 생성하는 윈도우 보고 메시지가 악의적 목적을 가진 공격자의 정보 획득 수단이 될 수 있다는 가능성이 제기돼 주목되고 있다.



인터넷침해대응센터는 10일 윈도우 오류 발생 시 생성되는 오류 보고 메시지에는 사용자의 하드웨어 및 운영체제 정보 등의 사용자 정보가 포함되어 있다고 밝혔다.

윈도우 오류 보고는 시스템 충돌 발생 시 자동으로 생성되며, 사용자 동의하에 인터넷을 통해 해당 보고서를 마이크로소프트 서버로 전송할 수 있도록 구성된다. 보고서 내용에는 PC 모델명, PC ID, OS 버전, 문제를 유발시킨 프로그램명 등이 있다.

Event	Application crash report
IP Address	XXX.XXX.XXX.XXX
Application	Firefox.exe
Application version	21.0.0.4879
Crash location	518ec3cc
App library	Xul.dll
App library version	21.0.0.4879
Library crash location	518ec306
Crash reason	0xC0000005 (Access Violation)
App crash offset	001c9789
PC Info	Acer Aspire 1930 – Mid Tower running Windows 7 SP2
PC Windows Version #	6.1.7601.2.00010300.1.0.3.17514 (SP2)
PC Machine ID	0513D3D-CBA4-2339-9ABC-ABCDEFABCDEF
〈오류 보고서에 담기는 사용자 정보〉	

또한 새로운 USB 접속 등의 오류가 아닌 하드웨어 변경 시에도 해당 내용을 담은 보고서가 생성돼 전송된다. 이는 새로운 USB 장치, 모바일 단말 등을 PC로 연결해 새로운 드라이버가 설치된 일반적인 상황에서도 운영체제는 마이크로소프트 서버로 해당 정보를 담은 보고서를 전송한다는 것이다. 보고서에는 장치 제조사, 모델명, 접속 시간 등의 정보가 포함돼 있다.

Example: Standard outbound Proxy log

6/30/13 - 3:44:17.000 PM
1372632257 cloud-proxy.example.com XXX.XXX.XXX.XXX 80
http://watson.microsoft.com/StageOne/Generic/PPGenericDriverFound/x64/USB_VID_05AC_PID_1208_P
EV_ISIO_MI_00.htm?LCID=1033&OS=6.1.7600.2.00010300.0.0.3.16385&SM=Sony%20Corporation&Pn=VPCEC3DFX&SV
=R1090YB&MRK=104D_Sony_VPCEC3DFX&MID=B293628E-B713-4AE8-1735-ABCDEFABCODEF microsoft.com

Event	USB device insert notification
IP Address	XXX.XXX.XXX.XXX
Date	06/30/2013 - 3:44:17 PM PST
Hardware Bus	USB
Device Vendor	Apple
Device ID	iPhone 5 (US Version)
PC Vendor	Sony Corporation
PC Version	VPCEC3DFX
PC BIOS Version	R1090YB
PC Machine ID	B293628E-B713-4AE8-1735-ABCDEFABCODEF
PC Windows Version	Windows 7 or Server 2008 R2
PC Windows Version #	6.1.7600.2.00010300 (SP1)

<iPhone 5를 USB로 연결 시 발생하는 메시지>

따라서 보고 메시지는 암호화되지 않은 채로 전송되기 때문에, 도·감청을 통한 정보 유출 가능성이 존재한다는 것이다. 또한 오류 보고 프로그램은 윈도우 XP에서부터 시작됐으며, 80%에 가까운 윈도우 PC들이 윈도우 오류 보고 프로그램에 참여하고 있다고 덧붙였다.

이와 관련 마이크로소프트 측에서는 성능 문제 때문에 해당 메시지에 대한 암호화를 수행하지 않고 있으나, 윈도우 8 이후 버전에서는 자동으로 TLS 암호화를 수행하고 있다고 밝혔다.

이미 미국 국방부 소속이자 전세계적인 정보 수집·암호 해독 등의 첩보 활동을 수행하는 정 부기관 NSA(National Security Agency)에서는 해킹 및 정보 수집을 담당하는 팀 TAO에서 자체 개발한 XKeyscore 툴을 통해 2008년부터 네트워크상에서 전송되는 오류 보고서를 수 집, 분석하고 있음이 밝혀진 바 있다.

[김경애 기자(boan3@boannews.com)]

<저작권자: 보안뉴스(<http://www.boannews.com/>) 무단전재-재배포금지>