hj1003

보낸 사람: 황경상 <kshwang@hizeaero.com>
보낸 날짜: 2017년 5월 15일 월요일 오후 10:06
받는 사람: hj1003@nate.com
제목: [알림] WannaCrypt(워너크립프트) 랜섬웨어 대응 방법 안내

WannaCrypt(워너크립프트) 랜섬웨어 대응 방법 안내

Microsoft 보안 업데이트가 적용되지 않은 취약한 Windows 시스템을 겨냥한 'WannaCrypt(워너크라이프트) 랜섬웨어'의 공격이 전세계적으로 진행되고 있습니다.

랜섬웨어(Ransomware)란 컴퓨터 사용자의 파일을 인질로 금전을 요구하는 악성 프로그램으로 몸값을 뜻하는 랜섬(Ransom)과 소프트웨어(Software)의 합성어입니다.

WannaCrypt 랜섬웨어 감염 시 문서 파일, DB 파일 등을 암호화하며, 암호를 푸는 대가로 비트 코인을 요구합니다.

WannaCrypt 랜섬웨어는 Microsoft 보안 업데이트를 적용하지 않은 환경의 Windows 취약점을 악용한 것으로, 2017 년 3 월
발표된 Microsoft 보안 업데이트 [MS17-010 Microsoft Windows SMB 서버용 보안 업데이트(4013389)]에서 이미 해당 취약점이 해결되었습니다. MS17-010 보안 업데이트 적용하여 공격을 예방할 수 있으며, 또한 해당 업데이트가 이미 적용된 Windows 시스템은 이번 공격에서 안전합니다.

이번 랜섬웨어 감염으로 인한 피해를 줄이기 위해 아래의 대응방법을 적용하시기 바랍니다.

WannaCrypt 랜섬웨어 대응 방법

조치 방법

① 사용하고 있는 백신 소프트웨어를 최신으로 업데이트하고 시스템을 검사합니다.

만일 설치된 백신 소프트웨어가 없다면 Microsoft 백신 소프트웨어를 이용하십시오.
Windows Defender 와 Microsoft Anti-Malware 제품의 최신 엔진 버전 1.243.290.0 에서 Ransom:Win32/WannaCrypt 로 해당 맬웨어가 차단됩니다.

- Windows 8.1 및 Windows 10 : Windows Defender 이용
- Windows 7, Windows Vista: Microsoft Security Essentials 이용
- Microsoft 무료 PC 보안 검사 : Microsoft Safety Scanner 이용

② Windows Update 또는 WSUS 등을 이용하여 시스템을 최신으로 보안 업데이트 합니다.
WU 을 사용할 수 없는 경우, Microsoft 보안 업데이트 MS17-010 를 수동 설치합니다.
OS 별 설치 경로는 아래와 같습니다.

Microsoft 보안 공지 MS17-010 ? 긴급 Microsoft Windows SMB 서버용 보안 업데이트(4013389)
https://technet.microsoft.com/ko-kr/library/security/ms17-010.aspx

제품명	패치 발표일	MS17-010 보안 업데이트 다운로드 링크
Windows XP		
Windows XP SP3 용 보안 업데이트 (KB4012598) - 한국어	5/13/2017	https://www.microsoft.com/ko-KR/download/details.aspx?id=55245
Security Update for Windows XP SP3 (KB4012598) - 영어	5/13/2017	http://download.windowsupdate.com/d/csa/csa/secu/2017/02/windowsxp-kb4012598-x86-custom-enu_eceb7d5023bbb23c0dc633e46b9c2f14fa6ee9dd.exe
Security Update for Windows XP SP2 for x64-based Systems (KB4012598) - 영어	5/13/2017	https://www.microsoft.com/en-us/download/details.aspx?id=55250
Windows Server 2003		
Windows Server 2003 용 보안 업데이트(KB4012598) - 한국어	5/13/2017	https://www.microsoft.com/ko-KR/download/details.aspx?id=55248
Security Update for Windows Server 2003 for x64-based Systems (KB4012598) - 영어	5/13/2017	http://download.windowsupdate.com/d/csa/csa/secu/2017/02/windowsserver2003-kb4012598-x64-custom-enu_f24d8723f246145524b9030e4752c96430981211.exe
x64 기반 시스템용 Windows Server 2003 보안 업데이트(KB4012598) - 한국어	5/13/2017	https://www.microsoft.com/ko-KR/download/details.aspx?id=55244
Security Update for Windows Server 2003 (KB4012598) - 영어	5/13/2017	http://download.windowsupdate.com/c/csa/csa/secu/2017/02/windowsserver2003-kb4012598-x86-custom-enu_f617caf6e7ee6f43abe4b386cb1d26b3318693cf.exe
* Windows XP 와 Windows Server 2003 은 각 언어별 패치가 다릅니다. 다른 언어에 대한 패치가 필요한 경우 위 다운로드 링크에서 [언어 선택]을 변경하시면 됩니다.		

Windows Vista		
Windows Vista 용 보안 업데이트 (KB4012598) - 한국어	3/14/2017	http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.0-kb4012598-x86_13e9b3d77ba5599764c296075a796c16a85c745c.msu
Security Update for Windows Vista (KB4012598) - Windows Vista - 영어	3/14/2017	http://download.windowsupdate.com/d/csa/csa/secu/2017/02/windowsxp-kb4012598-x86-custom-enu_eceb7d5023bbb23c0dc633e46b9c2f14fa6ee9dd.exe
x64 기반 시스템용 Windows Vista 보안 업데이트(KB4012598) - 한국어	3/14/2017	http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.0-kb4012598-x64_6a186ba2b2b98b2144b50f88baf33a5fa53b5d76.msu
Security Update for Windows Vista for x64-based Systems (KB4012598) - Windows Vista - 영어	3/14/2017	http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.0-kb4012598-x64_6a186ba2b2b98b2144b50f88baf33a5fa53b5d76.msu
Windows Server 2008		
Windows Server 2008 용 보안 업데이트(KB4012598) - 한국어	3/14/2017	http://download.windowsupdate.com/d/msdownload/update/software/secu/ 2017/02/windows6.0-kb4012598-x86_13e9b3d77ba5599764c296075a796c16a85c745c.msu
Security Update for Windows Server 2008 (KB4012598) - Windows Server 2008 - 영어	3/14/2017	http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.0-kb4012598-x86_13e9b3d77ba5599764c296075a796c16a85c745c.msu
x64 기반 시스템용 Windows Server 2008 보안 업데이트(KB4012598) - 한국어	3/14/2017	http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.0-kb4012598-x64_6a186ba2b2b98b2144b50f88baf33a5fa53b5d76.msu
Security Update for Windows Server 2008 for x64-based Systems (KB4012598) - Windows Server 2008 영어	3/14/2017	http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.0-kb4012598-x64_6a186ba2b2b98b2144b50f88baf33a5fa53b5d76.msu
Security Update for Windows Server 2008 for Itanium-based	3/14/2017	http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.0-kb4012598-ia64_83a6f5a70588b27623b11c42f1c8124a25d489de.msu

Systems (KB4012598) - Windows Server 2008 영어		
Windows 8		
Windows 8 용 보안 업데이트 (KB4012598) - 한국어	5/13/2017	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/05/windows8-rt-kb4012598-x86_a0f1c953a24dd042acc540c59b339f55fb18f594.msu
Security Update for Windows 8 (KB4012598) - 영어	5/13/2017	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/05/windows8-rt-kb4012598-x86_a0f1c953a24dd042acc540c59b339f55fb18f594.msu
x64 기반 시스템용 Windows 8 보안 업데이트(KB4012598) - 한국어	5/13/2017	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/05/windows8-rt-kb4012598-x64_f05841d2e94197c2dca4457f1b895e8f632b7f8e.msu
Security Update for Windows 8 for x64-based Systems (KB4012598) - 영어	5/13/2017	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/05/windows8-rt-kb4012598-x64_f05841d2e94197c2dca4457f1b895e8f632b7f8e.msu
Windows Embedded		
March, 2017 Security Only Quality Update for Windows Embedded 8 Standard (KB4012214)	3/14/2017	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/02/windows8-rt-kb4012214-x86_5e7e78f67d65838d198aa881a87a31345952d78e.msu
March, 2017 Security Only Quality Update for Windows Embedded 8 Standard for x64-based Systems (KB4012214)	3/14/2017	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/02/windows8-rt-kb4012214-x64_b14951d29cb4fd880948f5204d54721e64c9942b.msu
XPe 용 Windows XP SP3 에 대한 보안 업데이트(KB4012598) 사용자 지정 지원 - 한국어	5/13/2017	http://download.windowsupdate.com/c/csa/csa/secu/2017/02/windowsxp-kb4012598-x86-embedded-custom-kor_b603abee9e1c28e60104d061dde0cfcf03ebc27e.exe
Security Update for Windows XP SP3 for XP embedded (KB4012598) - 영어	5/13/2017	http://download.windowsupdate.com/c/csa/csa/secu/2017/02/windowsxp-kb4012598-x86-embedded-custom-enu_8f2c266f83a7e1b100ddb9acd4a6a3ab5ecd4059.exe

WES09 및 POSReady 2009 용 보안 업데이트(KB4012598) - 한국어	3/14/2017	http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windowsxp-kb4012598-x86-embedded-kor_4e62c3972598793f631af5f4f867c464c428b00a.exe
Security Update for WES09 and POSReady 2009 (KB4012598) - Windows XP Embedded - 영어	3/14/2017	ttp://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windowsxp-kb4012598-x86-embedded-enu_9515c11bc77e39695b83cb6f0e41119387580e30.exe
March, 2017 Security Only Quality Update for Windows Embedded Standard 7 (KB4012212)	3/14/2017	http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.1-kb4012212-x86_6bb04d3971bb58ae4bac44219e7169812914df3f.msu
March, 2017 Security Only Quality Update for Windows Embedded Standard 7 for x64-based Systems (KB4012212)	3/14/2017	http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.1-kb4012212-x64_2decefaa02e2058dcd965702509a992d8c4e92b3.msu
Windows 7		
2017 년 3 월, x64 기반 시스템용 Windows 7 에 대한 보안 전용 품질 업데이트(KB4012212)	3/14/2017	http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.1-kb4012212-x64_2decefaa02e2058dcd965702509a992d8c4e92b3.msu
2017 년 3 월 Windows 7 SP1 및 Windows Server 2008 R2 SP1 용 보안 전용 품질 업데이트 (KB4012212)	3/14/2017	http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.1-kb4012212-x86_6bb04d3971bb58ae4bac44219e7169812914df3f.msu
Windows Server 2008 R2		
2017 년 3 월, x64 기반 시스템용 Windows Server 2008 R2 에 대한 보안 전용 품질 업데이트(KB4012212)	3/14/2017	http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.1-kb4012212-x64_2decefaa02e2058dcd965702509a992d8c4e92b3.msu
March, 2017 Security Only Quality Update for Windows Server 2008 R2 for Itanium-based Systems (KB4012212)	3/14/2017	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/02/windows6.1-kb4012212-ia64_93a42b16dbea87fa04e2b527676a499f9fbba554.msu
Windows 8.1		

2017 년 3 월, Windows 8.1 에 대한 보안 전용 품질 업데이트(KB4012213)	3/14/2017	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/02/windows8.1-kb4012213-x86_e118939b397bc983971c88d9c9ecc8cbec471b05.msu
2017 년 3 월, x64 기반 시스템용 Windows 8.1 에 대한 보안 전용 품질 업데이트(KB4012213)	3/14/2017	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/02/windows8.1-kb4012213-x64_5b24b9ca5a123a844ed793e0f2be974148520349.msu
Windows Server 2012 R2		
2017 년 3 월, Windows Server 2012 R2 에 대한 보안 전용 품질 업데이트 (KB4012213)	3/14/2017	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/02/windows8.1-kb4012213-x64_5b24b9ca5a123a844ed793e0f2be974148520349.msu
Windows Server 2012		
2017 년 3 월, Windows Server 2012 에 대한 보안 전용 품질 업데이트 (KB4012214)	3/14/2017	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/02/windows8-rt-kb4012214-x64_b14951d29cb4fd880948f5204d54721e64c9942b.msu

최신의 Windows 10 누적 업데이트 - 2017 년 5 월

제품명	패치 발표일	MS17-010 보안 업데이트 다운로드 링크
Windows 10		
2017-05 Cumulative Update for Windows 10 for x64-based Systems (KB4019474)	5/9/2017	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/05/windows10.0-kb4019474-x64_4ed033d1c2af2daea1298d10da1fad15a482f726.msu
2017-05 Cumulative Update for Windows 10 for x86-based Systems (KB4019474)	5/9/2017	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/05/windows10.0-kb4019474-x86_259adeed4a4037f749afab211ff1bc6a771ff7f6.msu
Windows 10 Version 1511		
2017-05 Cumulative Update for Windows 10 Version 1511 (KB4019473)	5/9/2017	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/05/windows10.0-kb4019473-x86_5e2b7bce2f1b116288b4f1f78449c66ecc7c7a53.msu

2017-05 Cumulative Update for Windows 10 Version 1511 for x64-based Systems (KB4019473)	5/9/2017	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/05/windows10.0-kb4019473-x64_c23b6f55caf1b9d6c14161b66fe9c9dfb4ad475c.msu
Windows 10 Version 1607 & Windows Server 2016		
2017-05 Cumulative Update for Windows Server 2016 for x64-based Systems (KB4019472)	5/9/2017	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/05/windows10.0-kb4019472-x64_dda304140351259fcf15ca7b1f5b51cb60445a0a.msu
2017-05 Cumulative Update for Windows 10 Version 1607 for x64-based Systems (KB4019472)	5/9/2017	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/05/windows10.0-kb4019472-x64_dda304140351259fcf15ca7b1f5b51cb60445a0a.msu
2017-05 Cumulative Update for Windows 10 Version 1607 for x86-based Systems (KB4019472)	5/9/2017	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/05/windows10.0-kb4019472-x86_9bf106e898b57c20917cd98fd8b8d250333015a5.msu
Windows 10 Version 1703		
2017-05 Cumulative Update for Windows 10 Version 1703 for x64-based Systems (KB4016871) -Windows 10	5/9/2017	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/05/windows10.0-kb4016871-x64_27dfce9dbd92670711822de2f5f5ce0151551b7d.msu
2017-05 Cumulative Update for Windows 10 Version 1703 for x86-based Systems (KB4016871) -Windows 10	5/9/2017	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/05/windows10.0-kb4016871-x86_5901409e58d1c6c9440e420d99c42b08f227356e.msu

③ 보안 업데이트 MS17-010 을 적용할 수 없다면, **'Microsoft SMBv1 사용 안함'으로 설정합니다.**

WannaCrypt 랜섬웨어는 Microsoft SMBv1 원격 코드 실행 취약점(CVE-2017-0145)을 이용합니다. 패치를 설치하지 못하는 경우

SMBv1 사용을 해제하여 이 취약점 악용을 피할 수 있으나 가능한 빠른 시일 내에 패치를 적용할 것을 권장합니다.

[SMBv1 사용 안 함]

Windows Vista 이상을 실행하는 고객

Microsoft 기술 자료 문서 2696547 을 참조하십시오.

Windows 8.1 또는 Windows Server 2012 R2 이상을 실행하는 고객의 대안 방법

클라이언트 운영 체제:

1. **제어판을 열고 프로그램을 클릭한 후 Windows 기능 사용/사용 안 함**을 클릭합니다.

2. Windows 기능 창에서 **SMB1.0/CIFS 파일 공유 지원** 확인란의 선택을 해제하고 **확인**을 클릭해 창을 닫습니다.
3. 시스템을 다시 시작합니다.

서버 운영 체제:

4. **서버 관리자**를 열고 **관리** 메뉴를 클릭한 후 **역할 및 기능 제거**를 선택합니다.
5. 기능 창에서 **SMB1.0/CIFS 파일 공유 지원** 확인란의 선택을 해제하고 **확인**을 클릭해 창을 닫습니다.
6. 시스템을 다시 시작합니다.

해결 방법의 영향. 대상 시스템에서 SMBv1 프로토콜이 사용되지 않도록 설정됩니다.

해결 방법을 실행 취소하는 방법. 문제 해결 단계를 다시 수행하면서 SMB1.0/CIFS 파일 공유 지원 기능을 활성 상태로 복원합니다.

④ 네트워크 방화벽 및 Windows 방화벽을 이용하여 SMB 관련 포트 차단

- SMB 관련 포트 : 137(UDP), 138(UDP), 139(TCP), 445(TCP)
  ※ SMB 서비스 포트 차단 시 공유 및 기타 관련 서비스가 중지될 수 있으니 적용 전 반드시 영향이 없는지 점검하신 후 적용하시기 바랍니다.
- 관련 문서 : KB 3185535 - 특정 방화벽 포트를 차단하여 SMB 트래픽이 회사 환경을 빠져나가지 못하도록 하기 위한 지침

WannaCrypt 랜섬웨어 감염 증상

.WNCRY 파일이 추가되며, 다음과 같은 파일이 표시됩니다.

r.wnry , s.wnry, t.wnry , taskdl.exe , taskse.exe , 00000000.eky , 00000000.res , 00000000.pky , @WanaDecryptor@.exe , @Please_Read_Me@.txtm.vbs , @WanaDecryptor@.exe.lnk

다음과 같은 메시지가 화면에 표시됩니다.

아래 파일 확장자를 가진 파일들을 암호화 합니다.

.123	.jpeg	.rb	.accdb	.m3u	.sln	.avi	.mov	.stw
.602	.jpg	.rtf	.aes	.m4u	.snt	.backup	.mp3	.suo
.doc	.js	.sch	.ai	.max	.sql	.bak	.mp4	.svg
.3dm	.jsp	.sh	.ARC	.mdb	.sqlite3	.bat	.mpeg	.swf
.3ds	.key	.sldm	.asc	.mdf	.sqlitedb	.bmp	.mpg	.sxc
.3g2	.lay	.sldm	.asf	.mid	.stc	.brd	.msg	.sxd
.7z	.ldf	.slk	.asp	.mml	.sti	.c	.myi	.sxm
.cgm	.nef	.sxw	.cmd	.odg	.tbk	.cs	.odt	.tiff
.class	.odb	.tar	.cpp	.odp	.tgz	.csr	.onetoc2	.txt
.dbf	.otp	.vb	.crt	.ods	.tif	.csv	.ost	.uop
.dch	.ots	.vbs	.dip	.PAQ	.vmdk	.db	.otg	.uot
.der	.ott	.vcd	.djvu	.pas	.vmx	.docm	.pem	.vsd

.dif	.p12	.vdi	.docb	.pdf	.vob	.docx	.pfx	.vsdx
.dot	.php	.wav	.flv	.pps	.xlm	.ibd	.psd	.xltx
.dotm	.pl	.wb2	.frm	.ppsm	.xls	.iso	.pst	.xlw
.dotx	.png	.wk1	.gif	.ppsx	.xlsb	.jar	.rar	.zip
.dwg	.pot	.wks	.gpg	.ppt	.xlsm	.edb	.potm	.wma
.gz	.pptm	.xlsx	.eml	.potx	.wmv	.h	.pptx	.xlt
.fla	.ppam	.xlc	.hwp	.ps1	.xltm	.java	.raw	

추가 정보

- **Microsoft Security Response Center Blog, Customer Guidance for WannaCrypt attacks**: https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
- **Microsoft Malware Protection Center Blog, WannaCrypt ransomware worm targets out-of-date systems**: https://blogs.technet.microsoft.com/mmpc/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/

문의 사항

이와 관련하여 문의 사항이 있으신 경우 아래로 연락 주십시오.

- **Microsoft 고객 지원 센터 : 1577-9700**
- 프리미어 기술 지원을 받고 있는 고객께서는 담당 TAM(기술 담당 관리자)로 문의주시기 바랍니다.

Microsoft

마이크로소프트는 고객님의 프라이버시를 존중합니다. 자세한 내용은 당사의 온라인 개인정보취급방침 및 청소년보호정책을 참조하세요.

향후 마이크로소프트에서 발송하는 홍보성 이메일 수신을 원하지 않으시면 여기를 클릭하세요. 수신거부를 하셔도 고객님께서 요청한 뉴스레터 또는 특정 마이크로소프트 서비스에 대한 필수 정보를 수신하시는데 영향을 끼치지 않습니다. 다른 마이크로소프트 메세지에 대한 수신 설정을 변경하시려면 여기 를 클릭하세요.

If you would prefer not to receive future promotional emails from Microsoft Corporation please click here. These settings will not affect any newsletters you've requested or any mandatory service communications that are considered part of certain Microsoft services. To set your contact preferences for other Microsoft Communications, click here

주소: 서울특별시 종로구 종로 1 길 50 더 케이트윈타워 A 동 12 층 한국마이크로소프트(유) (우편번호 110-150)

사용권에 대한 고지 사항| 개인정보취급방침 및 청소년보호정책| 문의처