랜섬웨어 SMB포트 차단 방법

㈜이지스헬스케어



한국인터넷진흥원 권장사항

한국인터넷진흥원(http://www.kisa.or.kr)에서는 랜섬웨어를 방어하기 위해 OS를 **"윈도우 7"**이상으로 업그레이드 하고 **보안패치**를 적용하는 것을 권장하고 있습니다.

윈도우XP 이하 버전에서는 공식 <mark>보안패치가 종료</mark> 되었기 때문에 나날이 발전하는 **바이러스 공격에 취약**할 수 밖에 없습니다.



랜섬웨어는 데이터 백업이 중요!

가장 좋은 예방은 데이터 백업 입니다. 철저하게 준비를 해도 한 순간의 <mark>방심</mark>과 나날이 <mark>발전하는 공격방법</mark>으로 사용자의 PC는 언제든 감염 될 수 있습니다.

중요한 데이터는 PC가 아닌 인터넷 연결이 안된 <mark>외장하드 같은 저장매체에 백업</mark>을 해주시는 것이 가장 좋은 예방법입니다.





랜섬웨어는 SMB(Server Message Block) 파일 공유 서비스의 취약점을 통해 감염이 되는데 이를 윈도우 방화벽을 통해 차단하는 것을 뜻합니다.

하기 내용은 <mark>윈도우7이상</mark>부터 SMB포트 차단하는 방법에 대해 기술하고자 합니다.

윈도우XP 이하 사용자 분들은 윈도우7이상으로 업그레이드 및 보안 패치를 적용 후 진행해 주시는 것을 권장합니다.









5

① 바탕화면에 있는 윈도우 로고 (시작 버튼) 클릭 하여 "방화벽" 검색 후 해당 프로그램 실행

_									
-	고급 5	ደ안이	포함된 Windows	방화벽					
=	과일(F) 등작(A) 보기(V) 도용말(H)								
4									
	-	THE CO.		ALM O F	3.41		_	_	_
-		10C	그치 그치	인마운드	119	<u>^</u>	_	_	
	M 01-5		새 규칙(N)		1	그를	프로필	사용	작업
	93				HTTP Server		공용	og	거부
>	1 QL		쓰도 흔들 들다당()	K) >	HTTP Server		공용	예	거부
			상태로 필터링(S)	>	ive Disassembler (32-bit)		공용	ol i	허용
			그릏으로 필터링(G) >	ive Disassembler (32-bit)		공용	og	허용
			97100	,	ive Disassembler (64-bit)		공용	예	허용
			2-1(4)	· ·	ive Disassembler (64-bit)		공용	에	허용
			새로 고침(F)		DRMAgent For NoAX		38	ol	허용
			육록 내보내기(L).		DRMAgent For NoAX		공용	예	허용
			C B Dan				공용	예	허용
			定县 昆(H)]		공용	9	허용
				Alloyn	라우터(TCP-In)	Allloyn 라우터	도메인	9	허용
				Alloyn	라우터(UDP-In)	AllJoyn 라우터	도메인,	예	허용
				Branch	Cache 콘텐츠 검색(HTTP-In)	BranchCache - 콘텐츠 검색.	. 모두	아니요	허용

② 방화벽 내에 "인바운드 규칙" 오른쪽 버튼으로 클릭 후 "새규칙" 클릭



🔗 새 인바운드 근직 마법사		>
규칙 종류 안물리는 방화제 규칙 종류를 선택	2 UD.	
(1)제: # 규작 중류 # 프로토랑 및 포트 # 작업 # 프로당 # 다동	만들려는 규칙 용류는 무엇입니까? - 프로그램과 연결을 제이하는 규칙 문로그램의 연결을 제이하는 규칙 (* 목록(0) 다가 또는 UNP 포트의 연결을 제이하는 규칙 - 역격 철확적(0): - 생리 철확적(0): - 생리 책(0): 사용자 지장 규칙	< (斩政(图) 〇〇〇〇〇〇〇 - 英企

6

③ 새 인바운드 규칙 마법사에서 "포트"체크 후 "다음" 클릭

🔗 새 인바운도 규칙 다법사					×
프로토월 및 포트 이 규석을 적용할 프로토물과 프	토물 지장하십시오.				
971: - 구석 종류 - 조로도를 및 포트 - 조로도 - 조로도 - 진문	다 규칙은 TCPH 적용됩니다 ④ TCPHT) 〇 UDPHD 다 규칙은 오픈 운영 포함 이 규칙은 오픈 운영 포함(5) 다 규칙은 오픈 운영 포함(5) 이 규칙은 오픈 운영 포함(5)	8. UEP에 적용됩니다? 적용됩니다. 특징 로칠 포트에만 적용됩니 [135:445 북(180,443,5000-5650	< 2(800)	D800.2	网企

④ "TCP", "특정 포털 포트" 체크 후 "139, 445" 입력 후 "다음" 클릭



🖉 새 인바운도 규칙 다렵사	X
9 2	
구석에 지정된 조건과 연결이 일치	할 때 수영할 작업을 지장합니다.
274:	
규칙 중류	지정된 조건과 연결이 일치할 경우 여란 작업을 수명해야 합니까?
프로토콜 및 포트	ି ଅପ୍ଟ କଣ୍ଡ (A)
22	IPsec으로 보호되는 면결과 보호되지 않은 면결이 포합됩니다.
王建黎	○ 보안 연결한 취용(C) IPstec를 사용하여 연결한 모양된(LC), 연결 보안 규칙 노도의 IPstec 승성 및 규칙 성장을
015	사용하여 연물이 보호합니다.
	从意及 (12)
	 한글 차단0Q
	(4(症(3)) [16(00)] 利金

⑤ "연결 차단" 선택



⑥ **"도메인", "개인", "공용"** 체크 후 "다음" 클릭





# 새 인바운드 규칙 마법사 이 등 이 규칙의 이름과 설명을 지정합니	ID.		×	⑦ 이름을 "SMB 차단"으.
9 개: • 규석 중류 • 프로토랑 및 포트 • 작업	0800:			입력 후 "확인" 클릭
 ■ 225 ■ 016 	(5N6 74E) #B(8,2N0):]	
		< ឡ쥩(B)	[](台(F) 취소	

_						
1	새 언바운드 규칙 마법사					
ž	프로토콜 및 포트					
0	규칙을 적용할 프로토콜과 포트콜	지정하십시오.				
9	개: 규칙 용류 조건물 및 포트 작업 프로토 이름	이 규칙은 TCP에 적용됩니까, UC O TCP(T) ④ UDP(U) 이 규칙은 모든 로칠 포트에 적용[O 모든 로칠 포트(A) ④ 특정 로칠 포트(S):	우에 적용됩니까? 입니까, 특정 로칠 포트에만 적용됩니까? [137, 138] 예: 80, 443, 5000-5010		3	
				< ឡ星(8)	□ ₩0>	취소

⑧ 이와 같은 방법으로 동일하게 "UDP", "특정 로컬 포트" 내 137, 138 포트 차단



윈도우7 SMB포트 차단해제 방법

9

말 고급 보얀이 포함된 Windows 방 파일(F) 등작(A) 보기(V) 도용 ■ ➡ 2 1 1 금→ 2 1 1	방화벽 응말(H)						
로컬 컴퓨터의 고급 보안이 포함 300 인바운드 규칙 200 아우바운드 규칙	인바운드 규칙 이름	4	그룹 ^	프로필	사용	작업	다시 정! ^
Ng 연결 보안 규칙 Ng 모니터링	② AhnLab Safe Transaction ③ nProtect Online Security Starter ○ SMB 규칙 사용 안 함(!) ④ VMw		모두 모두	ମ ମ	허용 허용	아니요 아니요	
			도메인	<u>ମ</u> ମ ମ	거부 허용	아니요	
		을다다가(() 복사(C)		개인 도메인 개의	역 역 역	어풍 허용 지유	아니요
	vww atAl(D) vizw atAl(R)		모두	91 01	여용 허용 치용	아니요	
	Ø @[M	도응말(H)	@{Microsoft.Windows.Clou	도메인,	0I	허용	아니요

* 해당 서비스를 다시 사용해야 하는 경우

①번 과정을 다시 수행한 후, 방화벽 내에 "인바운드 규칙"에서 설정했던 규칙 **"우클릭"** -> **"삭제"**







① 바탕화면에 있는 윈도우 로고(시작 버튼) 클릭 하여 "<mark>제어판"</mark> 검색 후 해당 프로그램 실행



② [제어판] -> [시스템 및 보안] -> [Windows 방화벽] 선택





12

③ [Windows 방화벽] -> [고급 설정] 선택

🔄 🕘 = 🕆 🔗 · 제어판	▶ 시스템 및 보안 ▶ Windows 방좌벽	< ◇ ○ 제어판 참
제어판 홈	Windows 방화벽을 사용하여 PC 보호	
Windows 방화벽을 통해 앱 또 는 기능 허용	Windows 방화벽은 해커나 약성 소프트웨어가 인터넷 또는 네트워 줍니다. -	워크를 통해 PC에 액세스하는 것을 방지해
🚱 알림 설정 변경	🖉 🧭 개인 네트워크(R)	연결 안 됨 ⊙
Windows 방화벽 설정 또는 해 제	🕑 게스트 또는 공용 네트워크(P)	연결됨 🕥
🥵 기본값 복원 🕺 고근 성정	공항 또는 커피슬과 같은 공공장소의 네트워크입니다.	
네트워크 문제 해결	Windows 방좌백 상태: 켜짐	

🔗 고급 보	£안이	포함된 Windows 병	화벽					
파일(F)	동작(/	A) 보기(V) 도용	달(H)					
💠 🔿 👔		1 🕞 🛛 🖬						
🔗 로걸 컴	퓨터의	김 고급 보안이 포함	인바운드	규칙				
도 인비	10 0	그치			A			2 1.04
014 OF-5		새 규칙(N)		1	그들	프로필	사용	작업
L 012	_			HTTP Server		공용	01	거부
		프로필별 필터링(R) >	HTTP Server		공용	01	거부
) 🐄 ± .		상태로 필터링(S)	>	ve Disassembler (32-hit)		28	01	치용
				Disassembles (22 bit)		78	00	*10
		그렇으로 걸어 8(0	v 1	ive Disassembler (32-bit)		88	9	여왕
		¥7100	>	ive Disassembler (64-bit)		공용	예	허용
		- 107		ve Disassembler (64-bit)		공용	9	허용
		새로 고침(F)		DRMAgent For NoAX		공용	0	허용
		8.8. LEVIEZION		DRMAgent For NoAX		공용	01	허용
		ality ality of a large of a large of a		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		78	01	지유
		도용말(H)				78	00	大品
	_					00	~	18
			Alloyn	라우미(TCP-In)	Aluoyn 다꾸더	노메인,	og	어풍
🖸 AlUoyn			Alloyn	라우터(UDP-In)	AllJoyn 라우터	도메인,	01	허용
			Branch	Cache 콘텐츠 검색(HTTP-In)	BranchCache - 콘텐츠 검색	모두	아니요	허용

④ 방화벽 내에 "인바운드 규칙" 오른쪽 버튼으로 클릭 후 "새규칙" 클릭



🔗 새 인바운드 규칙 마법사	×
규칙 종류 안물리는 방화벽 규칙 종류를 선택	NULD.
1278: - 규석 종류 - 프로토출 및 포트 - 작업 - 프로토 - 이름	만물려는 규칙 용류는 무엇입니까? - 프로그램의 연결을 제0하는 규칙 - 프로그램의 연결을 제0하는 규칙 - 프로그램의 연결을 제0하는 규칙 - 전 또는 UOP 포트의 연결을 제0하는 규칙 - 사용작 지정(C) 사용자 지정 규칙

⑤ 새 인바운드 규칙 마법사에서 **"포트"** 체크 후 "다음" 클릭

💣 새 인바운트 규칙 다볍사		>
프로토콜 몇 포트		
이 규석을 적용할 프로토클과 포트	L를 지정하십시오.	
이 규석을 적용할 프로토플과 포트 2371: * 프로토를 및 포트 * 각업 * 프로토 * (16)	1월 지정하십사오. 이 규칙은 TCP에 적용됩니까, UCP에 적용됩니까? ④ TCP(T) ● UDP(I) 이 규칙은 모든 로럴 포트에 적용됩니까, 특정 로럴 포트에만 적용됩니까? ● 모든 부럴 포트(A) ④ 특정 부럴 포트(S): 139,445 에: 80, 443, 5000-5510	
	< 5(값(B) [2(8(0)) >	취소

⑥ "TCP", "특정 포털 포트" 체크 후 "139, 445" 입력 후 "다음" 클릭



· 제 문비용도 근직 위험사	
약업 유석해 지정된 초건과 연결이 당	치할 때 수영할 취업을 지정합니다.
274 25 275 25 275 25 275 275 275 05	지정된 조건과 연결이 알지말 경우 아픈 작업을 수밖해야 합니까? 이 전철 제용(A) Proce으로 보호되는 연결과 보호되지 않은 연결이 포합됩니다. 이 전철 제용(A) Proce을 사람하여 연결과 보호되니다. 연결 보안 구석 노도의 Proce 속성 및 구석 물정을 사람하여 연결이 보호됩니다. 제품 지원(A) 환경 지원(A) 환경 지원(A)

⑦ "연결 차단" 선택

🔗 새 인바운드 규칙 마법사	
프로필 이 규칙을 적용할 프로토를 지장합니	ID.
971:	
• 규석 중류	이 규칙이 적용되는 시기는 안제입니까?
프로토콜 및 포트	
a 90	도 유해학(D) 합류터가 회사 도행인해 연결된 경우 적용됩니다.
• X28	2 attan
• 08	합류터가 개인 네트워크 위치(가정 또는 직장)에 연결된 경우 적용됩니다.
	금융09 합류터가 공용 네트워크 위치에 연결된 경우 적용됩니다.

⑧ **"도메인", "개인", "공용"** 체크 후 "다음" 클릭





① 이와 같은 방법으로 동일하게 "UDP", "특정 로컬 포트" 내 137, 138 포트 차단

💣 새 인바운트 규칙 마법사		×
프로토콜 및 포트 이 규칙을 적용할 프로토콜과 포트	를 지정하십시오.	
9 개: · 규칙 종류	이 규칙은 TCP에 적용됩니까, UDP에 적용됩니까?	
• 프로토콜 및 포트	O TCPYT) ⊛ UDPUJ	
 작업 프로탈 		
• 01 6	이 규칙은 모든 로칠 포트에 적용됩니까, 특당 로칠 포트에만 적용됩니까? ○ 모든 로칠 포트(A)	
	● 4/3 # 2 # #(S): [137, 139] [0]: 80, 443, 5000-5010	~ 7



16

말 고급 보안이 포함된 Windows 한 파일(F) 등작(A) 보기(V) 도용 ➡ ➡ 2 10 (2) 10	방화벽 응말(H)						
 로칠 컴퓨터의 고급 보안이 포] 21 인바운드 규칙 22 아웃바운드 규칙 23 연결 보안 규칙 24 모니터리 	인바운드 규칙 이름 ② AhnLab Safe Transac ③ nProtect Online Sect	ction urity Starter	그룹 ^	프로필 모두 모두	사용 예 예	작업 허용 허용	다시 정: ^ 아니요 아니요
	SMB 규칙 사용	용안함()		모두	9	거부	아니요
	 ♥ VMW ♥ VMw ♥ VMw ♥ VMw ♥ VMw 	m		도메인 개인 도메인	ମ ମ ମ	여용 허용 허용	아니요 아니요
	♥ VMw 삭제(D)			개인	예	허용	아니요
	♥ Wizw ♥ Wizw 속성(R)			모두	예	어용 허용	아니요
	☑ @{M 도움말(H)	10	@{Microsoft.Windows.Clou	도메인,	q	허용	아니요

* 해당 서비스를 다시 사용해야 하는 경우

①번 과정을 다시 수행한 후, 방화벽 내에 "인바운드 규칙"에서 설정했던 규칙 **"우클릭"** -> **"삭제"**





Windows 10





① 바탕화면에 있는 윈도우 로고(시작 버튼) 클릭 하여 **"방화벽"** 검색 후 해당 프로그램 실행

② 방화벽 내에 "인바운드 규칙" 오른쪽 버튼으로 클릭 후 "새규칙" 클릭

1	고급	보안이	포함된 Windows 형	말화벽					
Ξ,	일(F)	동작(/	A) 보기(V) 도용	·달(H)					
٠		2	1 🔒 🛛 🗖						
2	토럽	컴퓨터의	의 고급 보안이 포	인바운드	규칙				
	20 0	s	새 규칙(N)		1	그를	프로필	사용	작업
	8 8	3			HTTP Server		공용	OII.	거부
>	1. 2	21	WEEE E18(0 >	HTTP Server		공용	예	거부
Ľ.,			상태로 필터링(S)	>	ive Disassembler (32-bit)			Of I	허용
			그릏으로 필터링((5) >	ive Disassembler (32-bit)		공용	OI .	허용
			H 7100		ive Disassembler (64-bit)		공용	q	허용
			±*((v)		ive Disassembler (64-bit)		공용	9	허용
			새로 고침(F)		DRMAgent For NoAX		38	0	허용
			육록 내보내기(L)		DRMAgent For NoAX		공용	Of I	허용
							공용	9	허용
			도용말(H)		1		공용	9	허용
		_		Alloyn	라우터(TCP-In)	Allioyn 라우터	도메인	og	허용
				Alloyn	라우터(UDP-In)	Alloyn 라우터	도메인,	Of I	허용
L				Branch	Cache 콘텐츠 검색(HTTP-In)	BranchCache - 몬텐츠 검색	모두	아니요	허용



🔗 새 인바운드 규칙 마법사			×
규칙 종류			
안들려는 방화벽 규칙 증류를 선택	박합니다.	×	
2월 22 월 24 위에 동유할 24 9 규칙 종류 4 관업 6 관업 6 프로또 6 이름	만물려는 규칙 용류는 무엇입니까? 프로그램(P) 프로그램의 연결을 제대하는 규칙 (* 프루(D) TCP 또는 UDP 포트의 연결을 제대하는 규칙 이 직접 정확(BC): Allion 근무터 Windows 관람의 연결을 제대하는 규칙 · 사용자 지정 규칙		
		(위로(B) 다음(N) > 취소	

19

③ 새 인바운드 규칙 마법사에서 **"포트"** 체크 후 "다음" 클릭

💣 새 인바운트 규칙 다볍사					×	() () () () () () () () () ()	
프로토콜 몇 포트							"
이 규칙을 적용할 프로토콜과 포트	E 지명하십시오.						
231: - 규석 응유 - 프로토용 및 포트 - 작업 - 프로토 - 이용	01 규칙은 TCP에 적용됩니까 ● TCP(T) ○ UOP(U) 01 규칙은 모든 료험 포트에 적 ○ 모든 포함 포트(A) ● 특징 포함 모트(S):	, UCP에 적용됩니까? 18됩니까, 특징 값할 포트에만 적용됩 [135,445 해: 80, 443, 5000-5510	11.1711?				<u>כ</u> יי
			< 9(星(B)	D800>	취소		

) **"TCP", "특정 포털 포트"** 체크 후 **"139, 445"** 입력 후 "다음" 클릭



작업 국칙에 지정된 조건과 연결이 일치	방 때 수영말 작업을 지장합니다.
2701:	
	지정위 조건과 연결이 일치할 것은 아파 작업을 수밖해야 합니까?
- HG 85	
프로토콜 및 포트	O 128 NB(A)
R2	Pset으로 보호되는 연결과 보호되지 않은 연결이 포함됩니다.
528	 ※2 232 利用G
0.0	만 <u>lec를 사용하여 인축된 연결</u> 만 포함됩니다. 연결 보안 규칙 노트의 Piec 속성 및 규칙 설명을
018	사용하여 전달이 포포됩니다.
	从他现为部门
	 한결 차단00

⑤ "연결 차단" 선택

ſ	🔐 새 인바운드 규칙 마법사		1
	프로 발 이 규칙을 적용할 프로탈을 지장합니다.		
ŀ	971:		
ŀ	- 34 8s	이 규칙이 적용되는 시기는 언제입니까?	
ŀ	- 프로토콜 및 포트		
ŀ	• RC	년 도백인(D) 컴퓨터가 회사 도행인해 연결된 경우 적용됩니다.	
ŀ	- <u>X</u> 28	2 7(2)(2)	
ŀ	• 0.6	법류터가 개인 네트워크 위치(가정 또는 직장)에 연결된 경우 적용됩니다.	
		공용00 합류터가 공용 네트워크 위치에 연결된 같은 적용됩니다.	

⑥ **"도메인", "개인", "공용"** 체크 후 "다음" 클릭





10.0			
11	18		
- 0	I 규칙의 이름과 설명을 지정합니(
Т			
	201:		
1			
ŀ	귀석 음류		
ŀ	프로토콜 및 포트		
ŀ	작업	0(800):	
ŀ	王张音	SMB AB	
ŀ	0166	설명(옵션)(0):	
1			
1			

⑦ 이름을 "SMB 차단"으로 입력 후 "확인" 클릭

📕 세 인마운드 뉴의 비밀사	
프로토콜 및 포트 이 규칙을 적용할 프로토콜과 포트	별 지정하십시오.
9개: * 규칙 중류 * 프로토물 및 포트 * 작업 * 프로탈 * 이호	이 규칙은 TCP에 적용됩니까, U0P에 적용됩니까? () TCP(T) ④ UDP(U) 이 규칙은 모든 로칠 포트에 적용됩니까, 특징 로칠 포트에만 적용됩니까? () 우든 호철 포트(A) ④ 특정 호철 포트(A) 제: 80, 443, 5000-5010

⑧ 이와 같은 방법으로 동일하게 "UDP", "특정 로컬 포트" 내 137, 138 포트 차단



윈도우10 SMB포트 차단해제 방법

22

말 고급 보안이 포함된 Windows 5 파일(F) 등작(A) 보기(V) 도용 ● ➡ 2 10 금 10 금 10 10 ■ 도접 컴퓨터의 고급 보안이 포함	방화벽 응말(H) 인바운드 규정	1					
조 인바운드 규칙 ▲ 아웃바운드 규칙 ▲ 연결 보안 규칙 목 모니터링	이름 ② AhnLab Sa ③ nProtect C	fe Transaction Inline Security Starter	그룹 ^	프로필 모두 모두	사용 예 예	작업 허용 허용	다시 정! ^ 아니요 아니요
	SMB	규칙 사용 안 함(I)		모두	9	거부	아니요
	VMw VMw VMw	잘라내기(T) 복사(C)		도메인 개인 도메인	ମ ମ ମ	어용 허용 허용	아니요 아니요 아니요
	🕑 VMw	삭제(D)		개인	예	허용	아니요
	Vizvi Wizvi	속성(R)		모두 모두	ମ ମ	허용 허용	아니요 아니요
	🖉 @{M	도움말(H)	. @{Microsoft.Window	ws.Clou 도메인,.	. 01	허용	아니요

* 해당 서비스를 다시 사용해야 하는 경우

①번 과정을 다시 수행한 후, 방화벽 내에 "인바운드 규칙"에서 설정했던 규칙 **"우클릭"** -> **"삭제"**





감사합니다!

랜섬웨어 같은 바이러스는 한번 **감염**이 되고 나면 되돌리기가 힘들기 때문에 **사전 예방이 최선**입니다. 사용자 분들의 **소중한 데이터**를 지켜내시길 바랍니다.

마치며...