이스트시큐리티

보안 동향 보고서

No.94 2017.07

ESTsecurity Copyright © 2017 ESTsecurity Corp. All rights reserved.

No.94 2017.07

이스트시큐리티 보안 동향 보고서
CONTENTS

01
악성코드 통계 및 분석

악성코드 동향

알약 악성코드 탐지 통계

허니팟/트래픽 분석

알약 M 스미싱 분석

ESTsecurity Copyright © 2017 ESTsecurity Corp. All rights reserved.

1. 악성코드 동향

6 월에 발생했던 주요 보안이슈는 역시 랜섬웨어였으며, 그 중 특정 웹호스팅 업체에서 운영중인 리눅스 서버를 공격한 Erebus 랜섬웨어 이슈와, MBR 영역을 감염시켜 시스템을 사용할 수 없게 만드는 Petya 랜섬웨어 이슈가 가장 큰 화제였습니다. 이 중에서 국내에서 거의 피해가 없었던 Petya 랜섬웨어(정확하게는 암호화된 데이터의 복호화가 불가능하여 wiper 악성코드라고 불림)보다는 국내에서 굉장히 큰 이슈가 되었던 Erebus 랜섬웨어 위주로 말씀드리고자 합니다.

Erebus 랜섬웨어 이슈는 공격자가 Erebus 랜섬웨어를 이용해 국내 특정 웹호스팅 업체의 서버를 공격하여 해당 업체의 웹호스팅을 이용하는 다수의 웹사이트에서 장애가 발생하였으며, 공격자는 서버에 저장되어 있는 원본 데이터 및 백업 데이터를 모두 암호화시키고 업체에게 암호화된 데이터를 복구하기 위한 몇 십 억원 대의 복구비용을 요구한 이슈입니다.

이번 Erebus 랜섬웨어 이슈의 경우 기존의 랜섬웨어와 비교하여 랜섬웨어 자체로는 큰 특징은 없었지만, 공격자는 오랜 시간 동안 특정 웹호스팅 업체에 백도어를 설치하고, 전체 관리자 계정 정보와 권한을 탈취한 뒤 각 서버에 Erebus 랜섬웨어를 심어 특정 시간에 동시다발적으로 동작하게 세팅했다는 점에서, 단순 랜섬웨어 공격이 아닌 APT 공격과 랜섬웨어가 결합된 공격으로 간주가 되고 있기도 합니다. 중요데이터에 대한 별도 매체 백업과 주요 권한을 가진 계정으로의 접근 통제에 대한 중요성이 다시 한번 회자되고 있는 이 시기에, 각자 관리중인 계정 정보와 주요 데이터에 대한 관리실태를 점검해 보는 것은 어떨까 싶습니다.

이번 케이스에서 보셨다시피, 랜섬웨어는 점차 APT 공격과 결합되고 있는 형태를 보이고 있으며, 돈을 회수할 수 있는 가능성이 높지 않은 개인 대상의 공격에서 점차 기업 대상의 공격으로 확대되고 있습니다. 특히 기업이 보관하는 데이터를 공격하는 경우 피해 기업은 비즈니스 연속성을 위해 큰 비용을 지불하고서라도 복호화 비용을 지불할 가능성이 높다고 공격자들이 판단하기 시작해, 앞으로도 기업 대상의 랜섬웨어 공격은 더욱 교묘해지고 빈번해질 것이라 예상됩니다.

기업 업무환경에서의 중요 데이터를 안전하게 보호하는 백업 정책, 적절한 백업 솔루션과 더불어 주기적인 사내 임직원들을 대상으로 하는 보안인식교육이 필요한 시기입니다.

 Copyright © 2017 ESTsecurity Corp. All rights reserved.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

2017 년 6 월의 감염 악성코드 Top 15 리스트에서는 지난 5 월에 1,2 위를 차지했던 두 악성코드들이 서로 자리를 바꾸었으며, 3 위를 차지했던 Misc.Riskware.BitCoinMiner 는 지난 달과 동일한 순위를 차지했다. 전반적으로 이번 달의 악성코드 감염 수치는 5 월에 비해 크게 감소하였다.

순위	등락	악성코드 진단명	카테고리	합계(감염자수)
1	↑ 1	Adware.SearchSuite	Adware	1,633,577
2	↓ 1	Trojan.HTML.Ramnit.A	Trojan	1,120,245
3	-	Misc.Riskware.BitCoinMiner	Trojan	743,387
4	↑ 7	Gen:Variant.Razy.107843	Trojan	536,757
5	New	Worm.IM-VB.as	Worm	519,491
6	↓ 2	Trojan.LNK.Gen	Trojan	410,693
7	↑ 1	Win32.Ramnit	Trojan	358,318
8	↓ 1	Misc.Keygen	Trojan	289,224
9	-	Worm.ACAD.Bursted.doc.B	Worm	270,957
10	↓ 4	Worm.ACAD.Kenilfe	Trojan	216,311
11	New	Virus.IFrame.jL	Virus	202,368
12	New	Win32.Neshta.A	Trojan	166,077
13	↓ 3	Trojan.BAT.Poweliks.Gen	Trojan	139,347
14	New	Trojan.LNK-Bondat.Gen.1	Trojan	137,986
15	New	Win32.Ramnit.N	Trojan	133,367

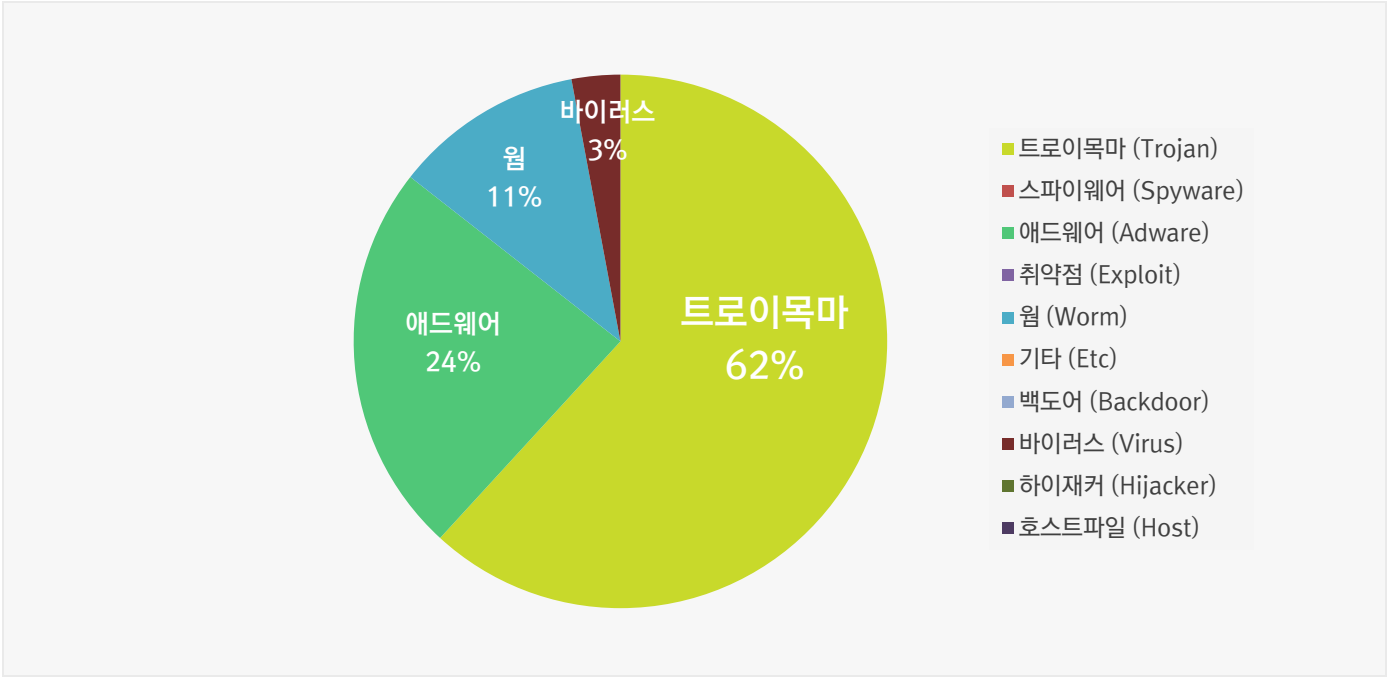
*자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

2017 년 06 월 01 일 ~ 2017 년 06 월 30 일

ESTsecurity Copyright © 2017 ESTsecurity Corp. All rights reserved.

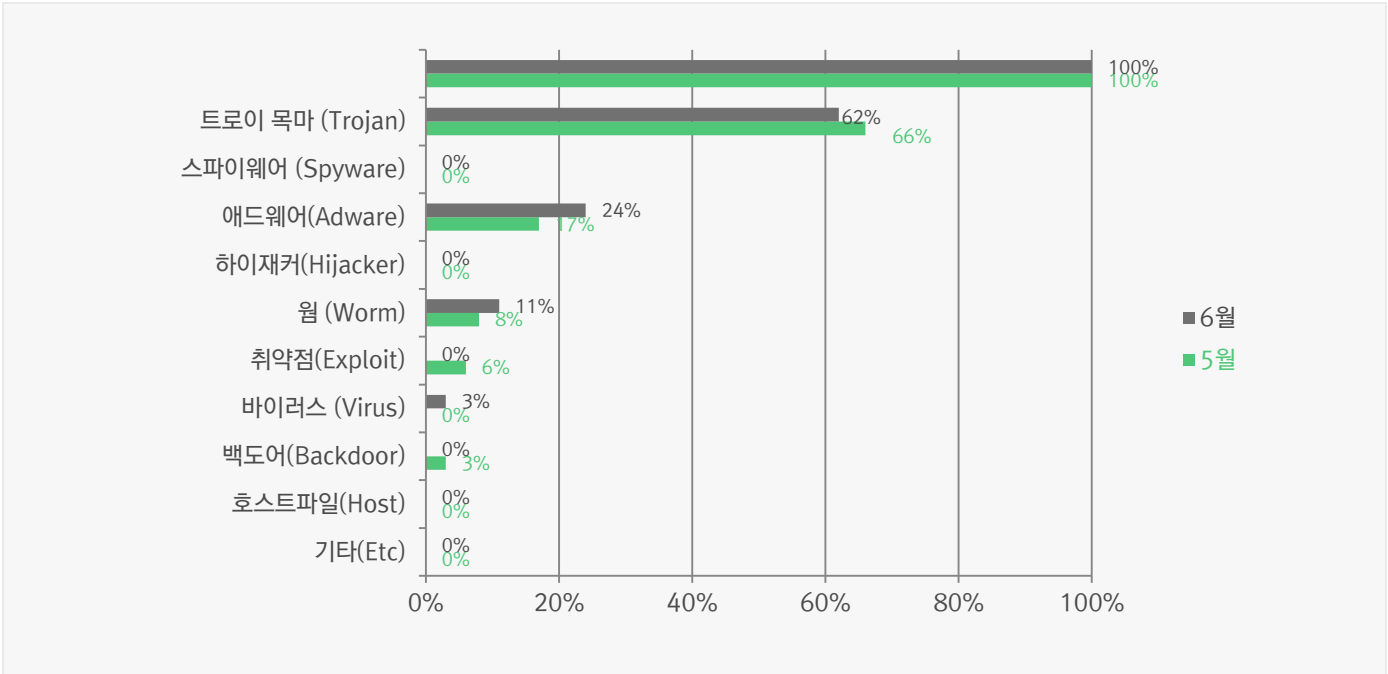
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 62%를 차지했으며, 애드웨어(Adware) 유형이 24%로 그 뒤를 이었다.



카테고리별 악성코드 비율 전월 비교

6 월에는 5 월에 비해 트로이목마 유형의 악성코드 비율이 소폭 감소하였으며, 전체적인 감염 수치는 약 37% 가량 크게 감소하였다.

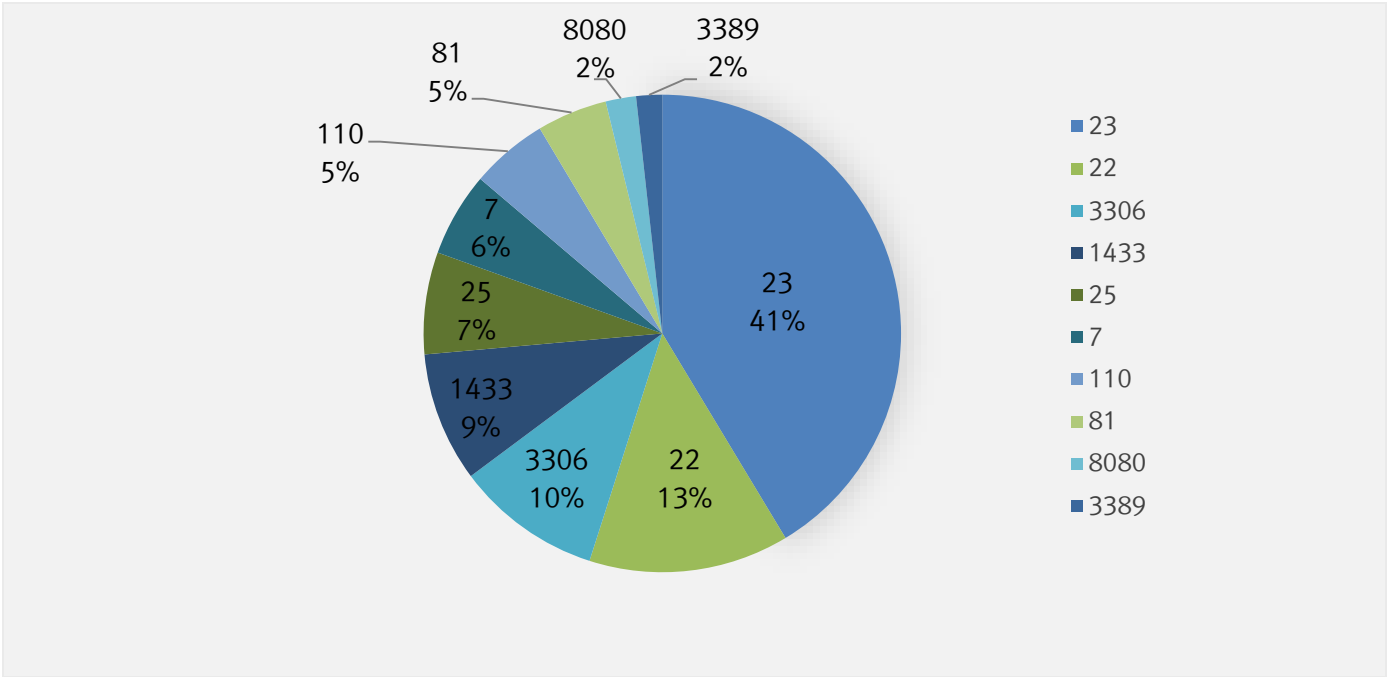


 Copyright © 2017 ESTsecurity Corp. All rights reserved.

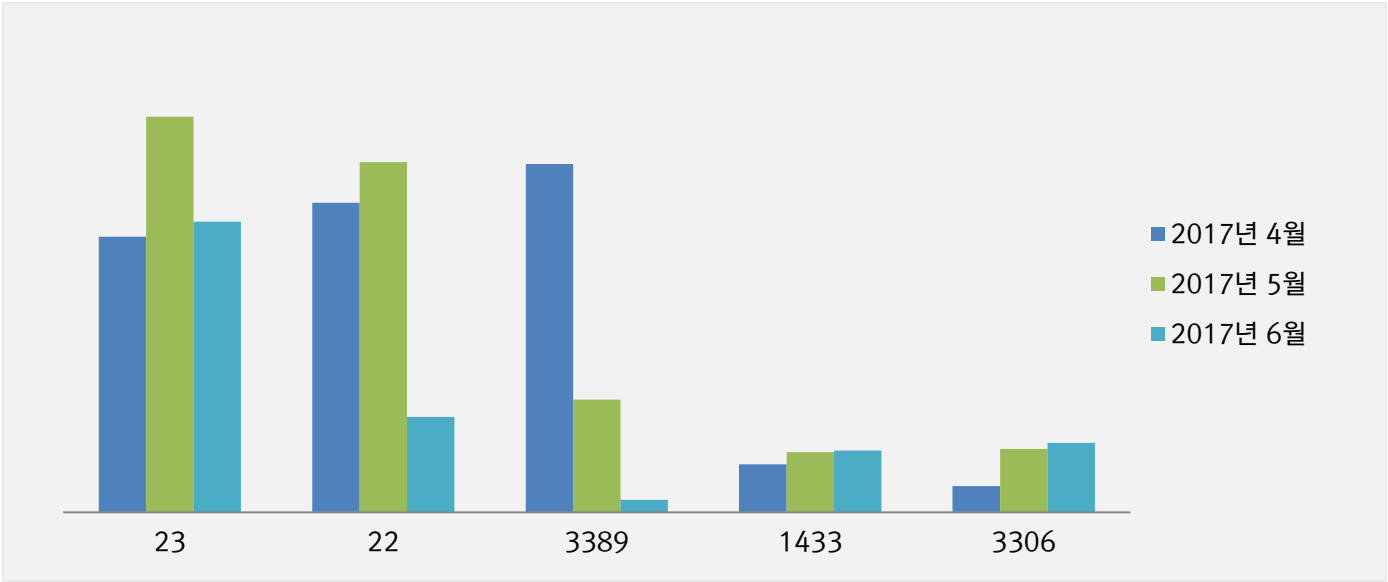
3. 허니팟/트래픽 분석

6 월의 상위 Top 10 포트

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



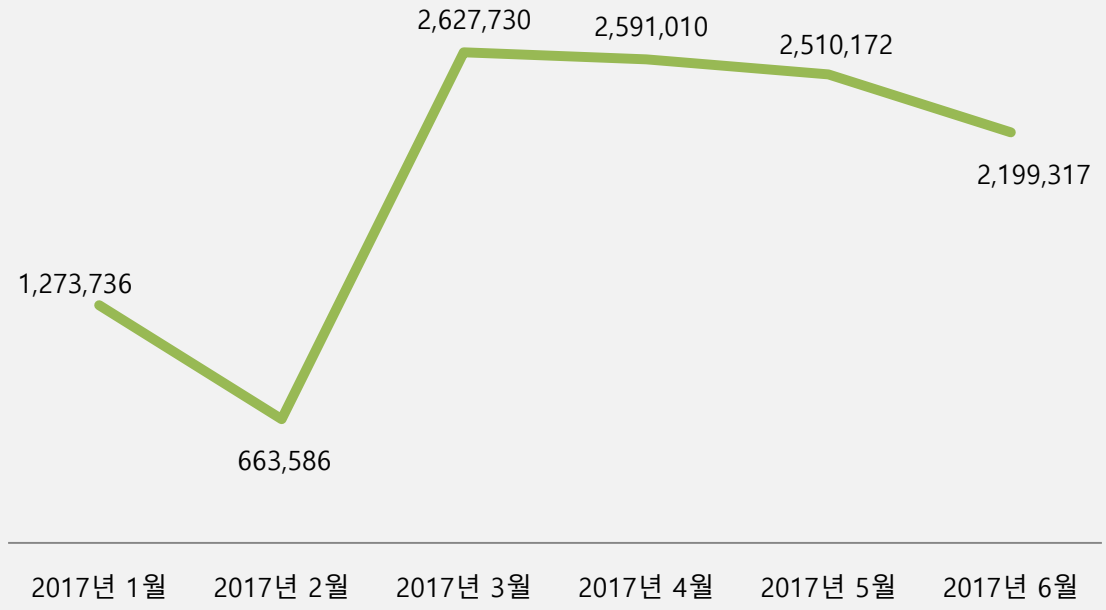
최근 3 개월간 상위 Top 5 포트 월별 추이



ESTsecurity Copyright © 2017 ESTsecurity Corp. All rights reserved.

악성 트래픽 유입 추이

외부로부터 유입되는 악의적으로 보이는 트래픽의 접속 시도가 감지된 수치



단위 : 악의적 트래픽 접속 시도 감지 건수

2017년 1월 ~ 2017년 06월

ESTsecurity Copyright © 2017 ESTsecurity Corp. All rights reserved.

4. 알약 M 스미싱 분석

알약 안드로이드를 통한 스미싱 신고 현황

기간	2017 년 06 월 01 일 ~ 2017 년 06 월 30 일
총 신고건수	3,086 건

키워드별 신고내역

키워드	신고 건수	비율
청첩장	97	3.14%
포토	32	1.04%
택배	24	0.78%
여행	11	0.36%
초대	10	0.32%
본인인증	8	0.26%
돌잔치	7	0.23%
동영상	5	0.16%
확인	2	0.06%
법원	1	0.03%

스미싱 신고추이

지난달 스미싱 신고 건수 1,982 건 대비 이번 달 3,086 건으로 알약 안드로이드 스미싱 신고 건수가 전월 대비 1,104 건 증가했다. 이번 달은 청첩장 관련 스미싱이 대부분을 차지했으며, 민사소송 관련 스미싱이 새로 등장했다.

ESTsecurity Copyright © 2017 ESTsecurity Corp. All rights reserved.

알약이 뽑은 6 월 주목할만한 스미싱

특이문자

순위	문자 내용
1	오래기다림속에저희하나되어결혼합니다 2017.7.16~ 한아름예식장
2	[Web 발신]새삶을출발하는저희에게해주신축복감사합니다 본식날포토보내드립니다
3	[법원] 민사소송 출석명령서입니다

다수문자

순위	문자 내용
1	오래기다림속에저희하나되어결혼합니다 2017.7.16~ 한아름예식장
2	[Web 발신]새삶을출발하는저희에게해주신축복감사합니다 본식날포토보내드립니다
3	[Web 발신] 대한통운 미확인 물품이 존재합니다 확인 부탁드립니다
4	l2 우 리(같 n 이 여행가요- 고고싱^~
5	[초대]\(^^꼭^0^와^^)/주세요~~(^.^)
6	[Web 발신]본인인증요망
7	저희 아기 돌잔치에참석해 주시어 감사합니다 돌잔치포토보내드립니다
8	$$^^ 여^기^에^ 너 ^이상한 동영상^ 있^는데 바로 삭제하세요
9	[Web 발신] 확인하세요
10	[법원] 민사소송 출석명령서입니다

ESTsecurity Copyright © 2017 ESTsecurity Corp. All rights reserved.

02

전문가 보안 기고

1. 취약점 악용 공격에 효과적인 방패, 패치관리 시스템이 필요하다

2. 스마트폰 랜섬웨어? 안드로이드 스마트폰을 안전하게 지키는 방법

ESTsecurity Copyright © 2017 ESTsecurity Corp. All rights reserved.

1. 취약점 악용 공격에 효과적인 방패, 패치관리 시스템이 필요하다

[Endpoint 개발팀 구기석 팀장]

마이크로소프트가 발표한 '2016 년 네트워크 보안트렌드' 보고서에 따르면, 공격자가 운영체제에 침입하기 위해 공격하는 주요 매체 경로를 '자바 취약점'에서 '어도비 플래시 플레이어 취약점'으로 옮겨간 것으로 분석됐다. 최근 발생하는 악성코드 공격의 대부분은 시스템과 어플리케이션의 취약점을 통해 이루어지고 있다.

효과적인 악성코드 유포 경로... 공격자는 '취약점'을 노린다

취약점이란 소프트웨어나 하드웨어의 버그나 설계상 결함을 의미한다. 공격자는 취약점을 통해 타겟 PC 의 제어 권한을 획득하거나 서비스 거부 공격 등을 시도할 수 있다. 취약점은 보통 알려진 취약점과 알려지지 않은 취약점으로 분류된다. 알려진 취약점들은 사용자 보안에 중대한 영향을 미치기 때문에 이를 보완하기 위한 패치들이 계속해서 생성되어 배포되고 있다. 하지만 수많은 공격자들은 이미 알려진 취약점이지만 사용자가 패치를 진행하지 않았거나, 알려지지 않은 취약점을 발빠르게 노린다. 패치가 공개되지 않은 취약점을 통해 이루어지는 '제로데이 공격'은 해마다 끊임없이 증가하고 있다.

시만텍의 '인터넷 보안 위협 보고서 21 호'에 따르면 2015 년 한 해 동안 발견된 제로데이 취약점은 2014 년 24 개에서 125% 늘어난 54 개로 집계되어 사상 최대치를 기록했다. 특히, 취약점을 노린 랜섬웨어 공격이 증가했다. 국내에서는 2015 년 이후 취약점 공격이 지속적으로 증가하여 정부기관 및 기업의 피해가 심각한 실정이다. 이에 정부기관과 보안 업체들은 시스템의 이상 행위나 의심스러운 행위를 사전에 차단할 수 있는 보안 솔루션을 계속해서 연구하고 있다.

'보안 패치'만 진행해도 취약점 대부분 대응... 기업 현황은?

문제는 공격자가 제로데이 취약점만 공격하는 것이 아니라, 이미 발견되어 보안 패치까지 제공된 원데이 취약점을 이용하기도 한다는 것이다. 이 공격 또한 상당한 비율을 차지하고 있다. 그러나 바꿔 말하자면, 이는 사용자가 보안 패치를 신속하게 진행하는 것만으로도 많은 공격을 예방할 수 있음을 의미한다.

 Copyright © 2017 ESTsecurity Corp. All rights reserved.

[그림 1. KISA 인터넷통계정보검색시스템 2016 년 정보보호 실태조사(기업부문) 결과 보고서]

미래창조과학부와 한국인터넷진흥원에서 발표한 2016 년 정보보호 실태조사(기업부문)에 따르면, 보안패치를 적용하고 있는 업체는 83.9%로 꽤 높은 비율을 차지하고 있다. 그러나 자동 업데이트를 설정한 기업은 50%정도이며, 수동 업데이트를 설정한 기업은 10%, 문제 발생 시에만 업데이트를 하거나 업데이트를 아예 진행하지 않는 경우가 40%에 달한다. 시스템이 안전한 상태로 유지되기 위해서는 지속적으로 업데이트를 진행해야만 한다. 업데이트를 하지 않은 나머지 40%는 보안에 매우 취약하다는 의미이다. 10 개의 기업 중 4 곳은 문제가 발생한 이후 업데이트를 하거나, 업데이트를 진행하지 않고 계속해서 보안 위협에 노출되어 있는 것이다. 이처럼, 많은 보안 전문가들이 보안패치의 중요성에 대해서 거듭 강조하고 있음에도 불구하고 보안패치를 철저히 적용하지 않는 이유는 무엇일까?

기관이나 기업의 경우, 전사에 보안 패치를 적용하는 것이 매우 어렵다. 임직원들이 사용하고 있는 소프트웨어는 천차만별이며, 임직원 모두가 동일한 소프트웨어를 사용해도 그 버전이 제각각인 경우가 많다. 특히, 폐쇄망 환경에서 업무를 진행하는 금융기관은 인터넷을 통해 보안 패치와 업데이트를 진행하는 것이 매우 까다롭다. 또한 해당 소프트웨어 관련 패치가 공개되어도 기관 및 기업이 이를 바로 적용하기까지는 많은 시간이 소요된다. 공격자는 바보가 아니다. 그들은 패치가 적용되지 않은 이 시기를 노리고 위협적인 공격을 시도한다.

꼼꼼한 패치 적용을 위해 필요한 패치관리 솔루션

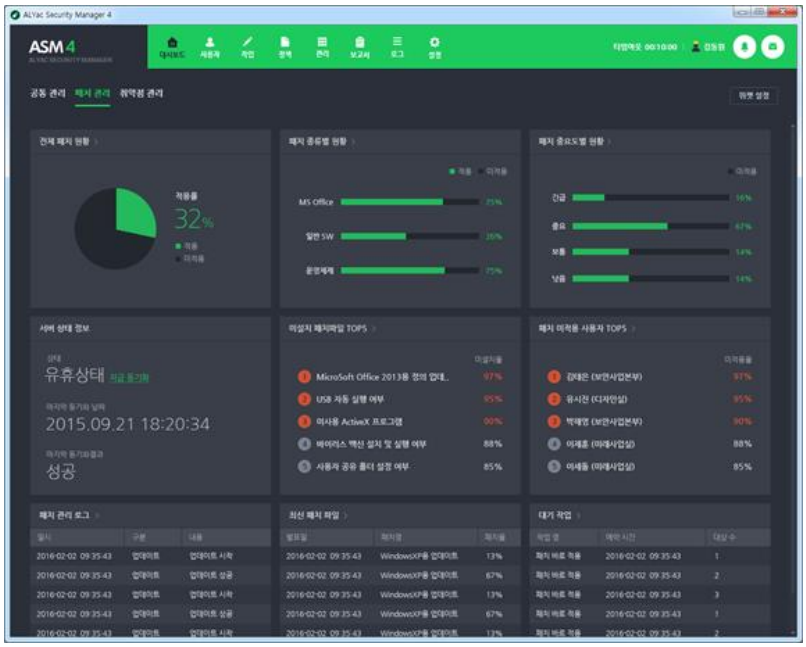
조직이 전사적으로 보안패치를 원활하게 적용할 수 있는 방법은 무엇일까? 전문가들은 별도의 패치 서버를 구축하거나, 전문 패치관리 솔루션의 도입을 권한다.

'패치관리 솔루션'이란, 보안 관리자가 기관 및 기업 내 PC 의 윈도우 업데이트나 주요 소프트웨어의 패치를 원활하게 관리할 수 있도록 돕는 솔루션이다. 이를 통해 관리자가 전사 PC 의 보안 상태를 간편하게 확인하고, 최신 보안 패치의 적용을 유지하여 안전한 보안 환경을 유지할 수 있다. 앞서 언급했듯이, 관리자가 별도의 서버나 시스템 없이 전사에 보안 패치를 적용하는 것은 매우 어렵다. 패치관리 솔루션을 도입하면 좀 더 꼼꼼한 패치 적용이 가능하기 때문에 많은 수의 보안 위협으로부터 벗어날 수 있다.

 Copyright © 2017 ESTsecurity Corp. All rights reserved.

02 전문가 보안 기고

이스트시큐리티가 출시한 알약 패치관리(PMS) 1.0 는 최소한의 운영 리소스와 비용으로 기관 및 기업이 안전한 보안 환경을 구축하는데 도움을 줄 수 있다. PMS 는 관리자가 전사 PC 의 패치를 일괄적으로 설치할 수 있게 지원하며, 원활한 패치관리를 통해 사내에 일관된 보안 정책을 유지할 수 있게 한다. 또한 사전 검수를 통해 검증된 패치를 제공하여, 고도화되는 보안 위협을 사전에 예방할 수 있다.



[그림 2. ASM(ALYac Security Manager) 대시보드]

특히, 관리자는 PMS 관리콘솔의 대시보드를 통해 실시간으로 관리 정보를 확인할 수 있다. 따라서 취약한 시스템에 대한 즉각적인 대응을 가능해진다. 이 외에도 PMS 는 패치 설치 상태 및 다양한 보안 위협 상황에 대한 실시간 알림 기능을 지원하고 있다. 이렇게 다양한 기능을 통해 조직은 최소한의 운영 리소스와 비용만으로 보안 취약점 공격에 효과적으로 대비할 수 있으며, 전사의 보안 수준을 향상시킬 수 있다.

공격자는 과거에 비해, 공격 수익성이 높은 기업이나 기관을 대상으로 교묘한 공격을 계속해서 시도하고 있다. 이러한 '창'은 앞으로도 계속해서 증가할 것이며, '방패' 또한 이를 막기 위해 쉬지 않고 대응해야 한다. 보안 취약점에 효과적인 방패는 무엇일까? 취약점을 점검하고, 신속하게 패치를 배포하는 등 다양한 취약점 관련 이슈를 관리할 수 있는 시스템 체계이다.

우리 속담에 '한 번 엎지른 물은 다시 주워 담지 못한다'는 말이 있다. 마찬가지로 시스템의 취약점을 통해 중요한 정보가 유출된 후에는 이를 되돌릴 수 없다. 또는 복구하더라도 막대한 비용과 노력이 수반되어야 할 것이다. 조직은 점점 더 고도화되는 보안 위협에 대응하기 위해, 더욱 능동적인 취약점 대응 체계 시나리오를 갖춰야 할 것이다.

ESTsecurity Copyright © 2017 ESTsecurity Corp. All rights reserved.

2. 스마트폰 랜섬웨어? 안드로이드 스마트폰을 안전하게 지키는 방법

[알약 M 개발팀 곽승권 책임]

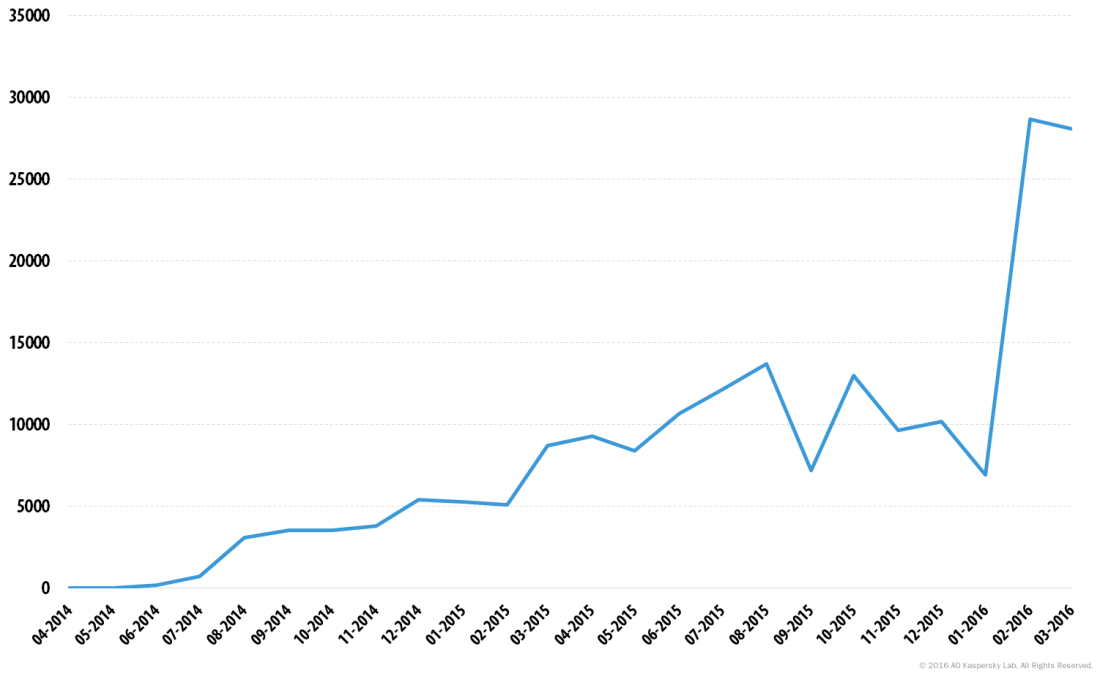
> You need to pay for us, otherwise we will sell portion of your personal information on black market every 30 minutes. WE GIVE 100% GUARANTEE THAT ALL FILES WILL RESTORE AFTER WE RECEIVE PAYMENT. WE WILL UNLOCK THE MOBILE DEVICE AND DELETE ALL YOUR DATA FROM OUR SERVER! TURNING OFF YOUR PHONE IS MEANINGLESS, ALL YOUR DATA IS ALREADY STORED ON OUR SERVERS! WE STILL CAN SELLING IT FOR SPAM, FAKE, BANK CRIME etc… We collect and download all of your personal data. All information about your social networks, Bank accounts, Credit Cards. We collect all data about your friends and family.

(출처 : 모바일 랜섬웨어의 위협 메시지 http://blog.checkpoint.com/2017/01/24/charger-malware/)

모바일 사용자 A 씨는 어느 날, 평소처럼 스마트폰을 사용하려고 했으나 이상한 점을 발견했다. 스마트폰을 켜도 위와 같은 메시지만 보여지고 잠금 설정에서 아무런 동작도 할 수 없게 된 것이다. A 씨는 모바일 랜섬웨어에 감염되어 스마트폰을 사용할 수 없을 뿐만 아니라, 개인정보까지 유출되는 피해를 입었다. 그는 스마트폰을 정상적으로 사용하기 위해 공격자에게 비용을 지불할까 고민했지만, 전문가들은 비용을 지불해도 피해를 복구할 수 없을 수 있다며 안타까움을 표했다.

이제 PC 뿐만 아니라, 모바일도 랜섬웨어의 위협에 노출되기 시작했다. 모바일 랜섬웨어는 2015 년부터 조금씩 증가하기 시작하여, 2016 년 2 월에는 5 배가 넘게 급증했다. 현재까지 한국에서 명확하게 보고된 사례는 없으나 최근 유럽이나 영어권 국가에서는 급증하고 있는 것으로 밝혀졌다.

ESTsecurity Copyright © 2017 ESTsecurity Corp. All rights reserved.



[그래프 1. 2014 년 4 월부터 2016 년 3 월까지 모바일 랜섬웨어를 한 번 이상 경험한 사용자 수 그래프, 출처: 카스퍼스키 랩 시큐어리스트]

랜섬웨어란 시스템을 감염시켜 접근을 제한하고 일종의 몸값을 요구하는 악성 소프트웨어의 한 종류이다. (출처: 위키피디아) 공격자들은 악성 소프트웨어를 무단으로 설치하거나 가짜 앱의 형태로 속여 사용자가 스스로 이를 설치하게끔 유도한다. 그 후, 사진이나 연락처, 금융정보와 같은 중요한 파일들을 암호화하여 인질로 잡고 금전적인 요구를 한다. 모바일 랜섬웨어의 경우, 공격자들은 잠금화면을 장악하고 사용자의 접근을 원천적으로 차단한다.

모바일 랜섬웨어, 어떻게 확산되는가?

모바일 랜섬웨어는 주로 공식적인 앱마켓이 아닌 비공식적인 경로를 통해 확산된다. 비공식적인 앱 마켓이나 모바일 기반 인터넷 환경에서 승인되지 않은 APK 파일을 설치했을 때, 사용자는 모바일 랜섬웨어를 포함한 각종 악성앱에 쉽게 감염될 수 있다. 무심코 다운로드한 악성 APK 파일은 이후 시스템앱 또는 인기있는 앱의 업데이트처럼 위장하여 사용자 스마트폰에 설치를 유도한다. 이후 개인정보 탈취 등 다양한 악성 행위를 할 수 있으니 각별히 주의해야 한다.

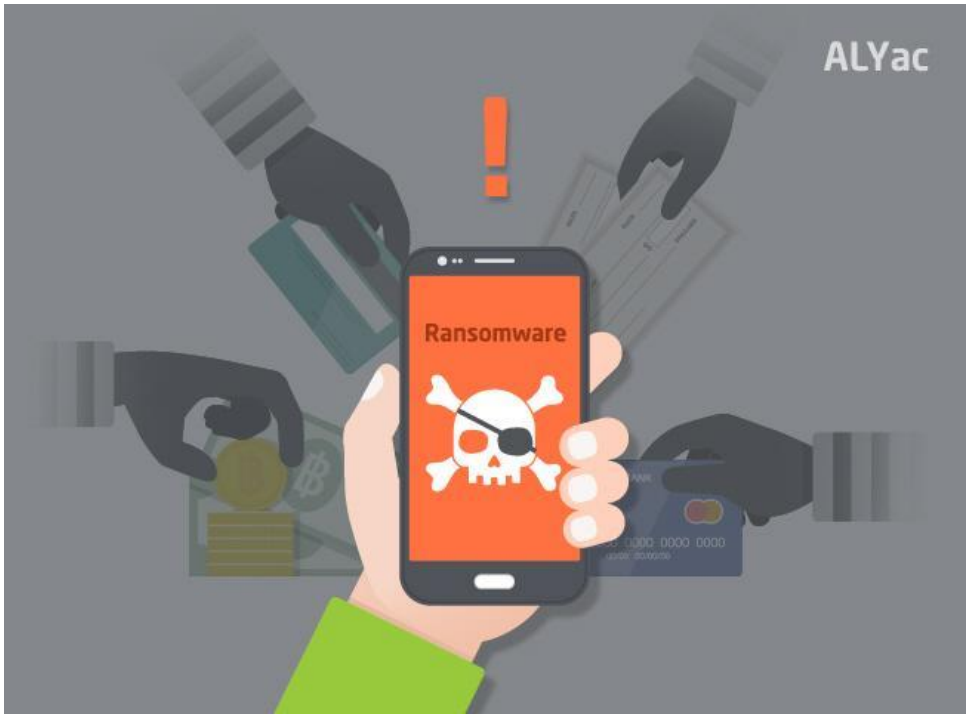
악성 APK 는 주로 블랙마켓을 통해 확산된다. 안드로이드에는 구글 스토어나 통신사가 제공하는 앱 스토어가 아닌, 블랙마켓이 존재한다. 블랙마켓 앱들은 보안성이 검증되지 않은 앱이 대부분이며, 공격자들의 악성앱 유포 경로로 자주 악용된다. 악성앱들은 정식 마켓에 등록된 정상앱의 아이콘과 이름을 사용하여 사용자를 속인다.

모바일 환경 특성상 악성 APK 파일은 링크(URL)를 통해 널리 퍼지기 쉽다. 이제 일반 사용자에게도 익숙한 스미싱(smishing) 공격이 바로 그것이다. 모바일 공격자는 문자메시지(SMS)에 링크(URL)를 삽입해 문자 수신자가 특정 페이지에 접속하여 악성앱을 내려받아 설치하도록(Fishing) 유도한다. 스미싱에는 주로 택배 도착 문자나 청첩장 문자 등 일반 사용자들의 생활과 밀접하게 연관된 문자가 악용되기 때문에 더욱 각별한 주의가 필요하다. 이스트시큐리티에 따르면, 최근까지도 스미싱 공격이 스마트폰 보안을 위협하고 있는 것으로 나타났다.

 Copyright © 2017 ESTsecurity Corp. All rights reserved.

(참고: 알약 블로그 http://blog.alyac.co.kr/1005)

스미싱과 유사한 방법으로, 메신저 또는 메일에 첨부된 링크를 통해서 악성앱을 감염시키기도 한다. 따라서 출처가 불분명한 발신처로부터 온 메일이나 메시지에 포함된 링크는 열어보기 전에 한 번 더 주의해서 확인하는 것이 좋다.



모바일 랜섬웨어에 감염되었을 때, 현명하게 대처하는 방법은...

랜섬웨어가 잠금화면을 장악했다면, 어떻게 해야 할까? 공격자가 원하는 금전적인 요구를 들어준다고 해도, 잠금화면이 풀리고 암호화된 데이터가 복호화될 것이라는 확실한 보장은 없다. 그러니 섣불리 돈을 송금할 생각은 일단 멈추자. 만약 스마트폰의 데이터가 백업되어 있다면 공장 초기화를 진행하는 것도 좋은 방법이다. 그러나 데이터를 백업해두지 않았다면, 일단 악성앱을 삭제해야 할 것이다. 이 때, OS 의 '안전모드'를 이용해서 악성 앱을 삭제할 수 있다.

'안전모드'는 시스템이 일시적으로 불안하거나, 시스템에 영향을 미치는 앱이 있으면 사용하는 모드이다. 해당 모드에서는 써드파티 앱(기본으로 설치된 앱이 아닌 사용자가 직접 설치한 앱)이 실행되지 않는다. 안전 모드로 부팅하면 랜섬웨어 앱의 기기 관리자 권한을 해제하고 앱을 삭제할 수 있다. 그러나 정말 안타깝게도, 랜섬웨어가 이미 데이터를 암호화했다면 해당 앱을 삭제해도 암호화된 데이터가 복호화되지는 않는다.

일단 암호화되면 '벼랑 끝'... 랜섬웨어는 '예방'이 중요하다.

랜섬웨어 감염 위협을 사전에 예방하고, 좀 더 안전하게 모바일을 사용하는 방법은 없을까? 사실 방법은 그렇게 어렵지 않다. KISA 보호나라에서 제공하는 PC 랜섬웨어 피해 예방 5 대 수칙을 모바일 환경에 그대로 적용하면 된다.

 Copyright © 2017 ESTsecurity Corp. All rights reserved.

02 전문가 보안 기고

1. 사용하는 모든 소프트웨어를 최신 버전으로 유지하기

공격자는 보안에 취약한 낮은 버전의 OS 나 앱을 노리고 악성앱 공격을 시도할 수 있다. 이에 항상 대응하기 위해서는 안드로이드 OS 와 사용하는 앱을 최신버전으로 유지해야 한다.

2. 최신 버전의 백신 소프트웨어를 사용하고 주기적으로 검사하기

랜섬웨어를 비롯한 각종 악성앱으로부터 모바일을 보호하기 위해서 '모바일 백신 설치'는 기본이다. 백신을 설치한 후에는 신종 악성앱에 대응하기 위해 주기적인 DB 업데이트가 선행되어야 하며, 정기적으로 검사를 진행하는 것이 좋다. 매번 검사하기가 번거롭다면, 모바일 백신 알약 안드로이드에서 제공하는 클라우드 스캔 기능을 이용해보는 건 어떨까. '클라우드 스캔 기능'은 실시간으로 악성앱을 감시하고 차단하기 때문에 모바일 기기 보안을 더욱 강화할 수 있다.

3. 출처가 불명확한 문자/메신저/이메일 내 링크(URL) 주의하기

모바일 기기 사용량이 증가하면서 스미싱 문자, 메신저, 스팸 메일 등에 악성파일을 첨부하거나 랜섬웨어 다운로드로 연결되는 악성 링크를 삽입한 공격이 확산되고 있다. 따라서 출처가 불분명한 문자나 메일, 메시지는 바로 열지 않고 주의하는 습관이 필요하다. 또는 모바일 백신 알약 안드로이드, 스팸 차단 앱 후후 등의 도움을 받아, 스미싱으로 의심되는 문자 알림 서비스를 제공받는 방법도 있다.

4. P2P 사이트, 블랙마켓에서의 앱 다운로드 주의하기

P2P 나 블랙마켓은 공격자들이 즐겨찾는 악성코드 유포 경로이다. 안전한 모바일 환경을 위해 앱을 다운로드 받을 때에는 되도록 공식 앱 마켓을 이용하기를 당부 드린다. 혹시 불가피하게 공식 앱 마켓이 아닌 경로에서 앱을 내려 받아야 할 때에는 모바일 백신의 실시간 감시 기능을 이용하도록 하자.

5. 중요 자료는 정기적으로 백업하기

개인적으로 중요한 문서나 사진 등은 반드시 주기적으로 백업하는 것이 좋다. 외장하드나 USB 등 별도의 저장매체를 이용해 중요한 파일을 저장하고, 운영체제에서 제공하는 사용자 파일백업 및 복원기능을 이용해 이중으로 백업하는 것을 권장한다.

(참고: 랜섬웨어 예방수칙, 보호나라 http://www.boho.or.kr/ransomware/prevention.do)

랜섬웨어의 피해를 최소화할 수 있는 방법은 위와 같이 '모바일 보안 수칙'을 잘 준수하는 것이다. 그러나 증가하는 피해 사례에도 불구하고 랜섬웨어에 대한 사용자의 인지도는 아직까지도 매우 낮다. 사용자 스스로 소중한 데이터를 지키기 위해 백업을 습관화하고, 관련 보안 수칙을 준수하는 자세가 필요하다. 또한 정부 기관과 유관 기업도 사용자 보안 의식을 개선하기 위해 관련 제도를 정비하고 효과적인 캠페인을 펼치는 등 노력해야 할 것이다.

 Copyright © 2017 ESTsecurity Corp. All rights reserved.

02 전문가 보안 기고

갈수록 스마트해지는 모바일 기기처럼, 사용자 또한 스마트한 보안 의식을 갖추는 노력이 요구되는 시점이다. 고도화되는 모바일 랜섬웨어 위협에 똑 부러지게 대처할 수 있도록, 예방법을 다시금 확인하여 준수할 것을 간곡히 당부 드린다.

ESTsecurity Copyright © 2017 ESTsecurity Corp. All rights reserved.

03
악성코드 분석 보고

개요

악성코드 상세 분석

결론

 Copyright © 2017 ESTsecurity Corp. All rights reserved.

[Trojan.Ransom.Sage] 악성코드 분석 보고서

1. 개요

최근 워너크라이(WannaCry)를 비롯한 다양한 랜섬웨어들이 출현하고 있는 가운데 기존 sage2.0 랜섬웨어의 변종인 sage2.2 랜섬웨어가 지속적으로 발견되고 있다. sage2.2 랜섬웨어는 sage2.0 랜섬웨어와는 다르게 한글 안내페이지를 지원한다. 또한 spora 랜섬웨어와 같이 오프라인 암호화를 진행하고 Cerber 랜섬웨어와 같이 감염 시 음성을 지원하는 것이 특징이다.

sage2.2 랜섬웨어는 스팸 메일을 통한 유입이나 웹 사이트 방문 시 노출되는 취약점을 통해 감염이 이루어졌을 것으로 추정된다.

이번 보고서에서는 sage2.2 랜섬웨어를 상세 분석하고자 한다.

ESTsecurity Copyright © 2017 ESTsecurity Corp. All rights reserved.

2. 악성코드 상세 분석

2.1 Rj3fNWF3.exe 상세 분석

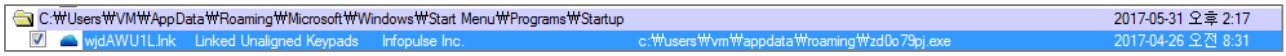
2.1.1 자가 복제 및 자동 실행 등록

윈도우 Vista 이상의 버전에서는 UAC(User Account Control)을 통해 컴퓨터 관리자 계정에서 응용 프로그램 실행을 제한하여 보안성을 높이고 있다. 따라서 랜섬웨어 제작자는 이러한 실행 제한을 우회하기 위해, 현재 실행된 프로세스가 관리자 권한으로 실행되지 않았을 경우, eventvwr.exe(이벤트 뷰어 프로그램)을 통하여 권한을 상승하여 실행한다.

```
v1 = RegCreateKeyA(HKEY_CURRENT_USER, "Software\\Classes\\mscfile\\shell\\open\\command", &v9);
v2 = -1;
if ( !v1 )
{
  v3 = lstrlenW(lpString);
  v4 = RegSetValueExW(v9, &ValueName, 0, 1u, lpString, 2 * v3);
  v2 = -2;
  if ( !v4 )
  {
    RegCloseKey(v9);
    GetEnvironmentVariableW("W", &v9, 0x104u);
    v19 = 0;
    v5 = MakeStr("%S\\System32\\eventvwr.exe", &v9);
    v12 = "o";
    v13 = v5;
    v16 = 0;
    v10 = 0x40;
    v9 = 0x3C;
    v11 = 0;
    v14 = 0;
    v15 = 0;
    v17 = 0;
    v6 = ShellExecuteExW(&v9);
```

[그림 1] 권한 상승 코드의 일부

부팅 시 자동 실행 되도록 시작프로그램 폴더에 자가 복제된 파일의 바로가기 파일을 생성한다.



[그림 2] 자동 실행 등록

2.1.2 감염 PC 정보 전송

무선 네트워크를 사용하고 있는 경우, 지역 정보를 수집하기 위해 감염 기기 주변의 무선 네트워크들의 맥 어드레스, SSID(무선 네트워크 이름) 정보를 구글맵스로 전송한다.

 Copyright © 2017 ESTsecurity Corp. All rights reserved.

다음은 UDP 방식으로 서버에 암호화된 데이터를 전송하는 코드이다. 전송되는 시스템 정보에는 컴퓨터 이름, 사용자 계정 이름, 어댑터, CPU 정보, 감염 기기의 로컬 언어, 관리자 권한 실행 여부, 종료 코드, 구글맵스 지리 정보가 포함된다.

```
v12 = (0x15A4E35 * v12 + 1) & 0x3FFFF;
if ( ((((v12 ^ 0x3F390) << 16) | *(&v14 + ((v12 ^ 0x3F390u) >> 16))) & 0xF0000000) != 0xF0000000 )
{
  *&to.sa_data[2] = ((v12 ^ 0x3F390) << 16) | *(&v14 + ((v12 ^ 0x3F390u) >> 16));
  if ( sendto(sock, buf, len, 0, &to, 16) == -1 )
  {
    v4 = WSAGetLastError();
    if ( v4 == WSAEHOSTUNREACH && ++v2 > 1000 )
      break;
    closesocket(sock);
    sock = socket(2, 2, 17);
```

[그림 3] 데이터 전송 코드

2.1.3 파일 암호화

① 감염 ID 발급 및 암호화에 사용된 키

파일 암호화에 앞서, %APPDATA%하위에 임의의 이름의 파일(*.tmp)을 드롭한다. 생성된 파일에는 감염 PC 의 식별을 위한 ID 와 암호화에 사용된 키가 포함된다. 감염 PC 의 ID 발급 시 CURVE25519 알고리즘으로 0x20 크기의 ID 값을 생성한다. 다음은 임의의 이름의 파일(*.tmp) 드롭 코드의 일부이다.

```
*(a1 + 64) = 1;
F_ComputeCURVE25519SecretKey(&SecretKey);
F_ComputePublicKey();
F_ComputeSharedSecret(&Shared, &SecretKey, HisPublicKey);
F_ComputeSecretKey_0(&Shared);
F_ComputePublicKey();
return 0;
```

[그림 4] 감염 ID 발급 코드의 일부

발급된 ID 는 추후 구글 맵스 전송 결과 값과 함께 Base64 로 인코딩되며, 비트코인 결제 안내를 위해 생성되는 랜섬노트 및 바탕화면에서 '감염 PC 식별 키'로 사용된다.

② 데이터 베이스 관련 프로세스 종료

데이터베이스와 연관된 프로세스를 탐색 및 종료한다. 종료하는 목적은 데이터 베이스(Database) 파일에 접근하여 암호화를 원활히 하기 위함으로 보인다. 다음은 종료되는 프로세스 목록이다.

msftesql.exe	synctime.exe	encsvc.exe
sqlagent.exe	mydesktopqos.exe	firefoxconfig.exe

 Copyright © 2017 ESTsecurity Corp. All rights reserved.

sqlbrowser.exe	agntsvc.exe	tbirdconfig.exe
sqlservr.exe	isqlplussvc.exe	ocomm.exe
sqlwriter.exe	xfssvccon.exe	mysqld.exe
oracle.exe	mydesktopservice.exe	mysqld-nt.exe
ocssd.exe	ocautoupds.exe	mysqld-opt.exe
dbsnmp.exe	agntsvc.exe	dbeng50.exe
		sqbcoreservice.exe

[표 1] 종료되는 프로세스 목록

③ 복구 기능 무력화

시스템 복구 기능을 무력화하여 암호화 이전 상태로 돌아가는 것을 방지한다. 이를 위해 다음과 같은 명령어로 '볼륨 섀도 카피본 삭제', 'Windows 오류 복구 알림창 표시 끄기', '복구 모드 사용 안함' 기능을 수행한다.

```
MOV DWORD PTR SS:[ESP+0x4],7Dk5n4hQ.00416094      UNICODE "delete shadows /all /quiet"
MOV DWORD PTR SS:[ESP+0x8],EAX
MOV DWORD PTR SS:[ESP],7Dk5n4hQ.004160CA          UNICODE "vssadmin.exe"
CALL <7Dk5n4hQ.ShellExec>
MOV DWORD PTR SS:[ESP+0x8],EBX
MOV DWORD PTR SS:[ESP+0x4],7Dk5n4hQ.004160E4      UNICODE "/set {default} recoveryenabled no"
MOV DWORD PTR SS:[ESP],7Dk5n4hQ.00416128          UNICODE "bcdedit.exe"
CALL <7Dk5n4hQ.ShellExec>
MOV DWORD PTR SS:[ESP+0x8],EBX
MOV DWORD PTR SS:[ESP+0x4],7Dk5n4hQ.00416140      UNICODE "/set {default} bootstatuspolicy ignoreallfailures"
MOV DWORD PTR SS:[ESP],7Dk5n4hQ.00416128          UNICODE "bcdedit.exe"
CALL <7Dk5n4hQ.ShellExec>
```

[그림 5] 추가 명령어 동작

④ 파일암호화

암호화 하기 이전, 제외 대상 PC 인지를 체크한다. 키보드 입력 환경이 벨라루스, 카자흐, 우크라이나, 우즈베키스탄, 사하 공화국, 러시아, 라트비아언어로 설정되어 있다면 해당 PC 는 암호화 대상에서 제외하고 위에서 언급한 감염 PC 의 정보만을 전송한 뒤 종료된다.

```
int result; // eax@2

if ( F_CheckLocale_0(0x23u)                    // Belarusian 벨라루스
  || F_CheckLocale_0(0x3Fu)                    // Kazakh 카자흐
  || F_CheckLocale_0(0x22u)                    // Ukrainian 우크라이나
  || F_CheckLocale_0(0x43u)                    // Uzbek 우즈베키스탄
  || F_CheckLocale_0(0x85u) )                  // Sakha 사하 공화국
{
  result = 1;
}
else
{
  result = F_CheckLocale_0(0x19u);             // Russian 러시아
  if ( result )
    result = F_CheckLocale_0(0x26u) == 0;      // Latvian 라트비아
}
return result;
```

[그림 6] 키보드 로컬 언어 확인

ESTsecurity Copyright © 2017 ESTsecurity Corp. All rights reserved.

위 국가어를 사용하지 않는 PC 의 경우, 암호화를 진행한다. 암호화 진행을 위해 암호화 조건에 부합되는 파일들을 검색 및 리스팅을 시작한다. 암호화 대상 확인 조건은 총 3 가지 암호화 대상 확장자, 암호화 제외 파일, 암호화 제외 문자열이 존재한다. 암호화 대상 확장자는 다음과 같다.

.wav .mp3 .m4u .m3u8 .m3u .flac .bmp .xlk .vhdx .tibs .tib .spi .spf .pvhd .pfi .pbf .pbd .paq .old .obk .npf .mrimg .gbp .gbm .ebk .cbu .c004 .c003 .c002 .c001 .c000 .bkf .bk2 .bjf .bif .bak5 .bak4 .bak3 .bak2 .bak1 .bak .backupdb .back .adi .010 .009 .008 .007 .006 .005 .004 .003 .002 .001 .xqx .xeq .xdi .xaa .wmf .wbk .wbcat .vyr .vyp .vdf .vc8 .vc7 .vc6 .vbpf .v30 .uot .uop .umv .u12 .u11 .u10 .u08 .trm .tmd .tkr .tfx .ta2 .str .stm .ssg .skg .seam .sbf .sbd .sbc .saj .rwl .rw2 .reb .ra .qxf .qwmo .quo .qpg .qmtf .qem .qdfx .qbz .qbmd .q43 .q09 .q08 .q07 .q06 .prpr .pp5 .pp4 .pls .pg .pd6 .pcif .op .oet .ocr .obi .nrg .nl2 .nd .nba .n43 .myox .mye .mx0 .ms11 .mrq .mql .mone .mnp .mne .mlc .meta .mem .mef .mds .mbsb .mac .m16 .m14 .m11 .m10 .log .lld .lhr .let .ldr .ldc .kmo .kd3 .kb7 .jsda .itf .iso .ipg .inx .int?.ini .indt .indl .idml .iban .i2b .i05 .i04 .i03 .i02 .i01 .hts .h12 .h11 .h10 .gsf .gsb .gpc .gnc .gem .fyc .fxw .fx1 .fx0 .ful .fef .fcr .fcpr .fcpa .fca .fa2 .fa1 .ets .etq .esv .esk .ert .eqb .epb .epa .ent .emd .efsl .efs .ec8 .ebq .ebd .ebc .dwf .dvd .dtau .defx .dat .dac .cur .cue .css .cso .cpw .cpbdf .cnt .cmd .ch .cgn .cfg .cfdi .cf9 .cf8 .cb .cat .btif .bpdx .bin .bd3 .bd2 .bc9 .bc8 .bat .b5i .awd .ati .arv .amj .afm .aepx .adp .acm .aci .acc .ac2 .aa ._vc .500 .4dd .3pe .3me .210 .13t .11t .10t .09t .09i .08i .07i .07g .00c .xhtm .wmv .wma .vob .rm .png .pdf .mpg .mpeg .mpe .mpa .mp4 .mp2 .mov .mkv .mhtm .m4v .m4a .m .jpg .jpeg .jp2 .html .gif .flv .djvu .djv .avi .asf .aac .3gp .3g2 .264 .wtv .jtv .iva .eye .dvr .camrec .fjp .vmxf .vmx .vmsd .vmdk .vhd .vdi .vbox .qed .qcow2qcow .hdd .zipx .zip .tgz .tar .s7z .rz .rar .lz .gz .cab .bz2 .arj .arc .ace .7z .wdseml .tbp .tbk .tbi .tbb .tab .slt .shlb .pst .p7z .p7s .ost .oab .msg .msf .msb .mozeml .mim .mflmbox .mar .mab .ldif .ldi .flx .eml .email .ebi .abd .xml .xlw .xltx .xltm .xlt .xlsx .xlsm .xlsb .xls .xlr .xlm .xll .xlc .xlam .xla .wps .wpd .wks .wk4 .wk3 .wk1 .wb2 .vcf .txt .text .sxw .sxm .sxi .sxd .sxc .stw .sti .std .stc .slk .sldx .sldm .shw .rtf .rss .pptx .pptm .pptf .ppt .ppsx .ppsm .pps .ppam .potx .potm .pot .per .ott .ots .otp .otg .odt .ods .odp .odm .odg .odc .mws .hwp .gfi .ess .eps .efx .dotx .dotm .dot .docx .docm .docb .doc .dif .csv .cntk .cht .cal .123 .vbs .vb .rb .py .pl .php .pas .lua .jsp .json .js .java .jar .hpp .h .fla .cs .cpp .class .cd .c .asx .asp .asm .as3 .as .yuv .xpm .xcf .x3f .wpg .wi .vsd .ttf .tpl .tiff .tif .tga .swf .svg .srf .sr2 .slp .set .ses .sct .sch .s12 .rpf .rif .raw .raf .r3d .pxa .pvc .ptx .psp .psd .ps .pm .prf .prel .ppj .ppf .por .pns .pmd .plt .plb .pic .pfb .pdd .pcx .pct .pcd .pat .p7m .orf .npc .nef .nap .mml .mmb .mid .met .mda .md .max .m15 .m12 .lin .ldf .lcd .lay6 .lay .kdc .jsd .jng .ipe .indd .imp .img .iff .ico .fpx .fon .fmv .ens .emp .dxf .dwg .dtl .dtd .dsf .dsb .ds4 .drw .dng .dip .dds .dcr .dch .d07 .csl .cpx .cpt .cmx .clk .cgm .cdx .cdt .cdr .brd .bay .asc .ai .aet .aep .aaf .3ds .3dm.$ac .zka .zix .zdb .wac .vnd .vmb .usa .txf .tt20 .tt19 .tt18 .tt17 .tt16 .tt15 .tt14 .tt13 .tt12 .tt11 .tt10 .tm .tom .tlg .tdr .tb2 .tax20 .tax2 .tax19 .tax18 .tax17 .tax16 .tax15 .tax14 .tax13 .tax12 .tax11 .tax10 .tax1 .tax0 .tax .ta9 .ta8 .ta6 .ta5 .ta4 .ta1 .t99 .t19 .t18 .t17 .t16 .t15 .t14 .t13 .t12 .t11 .t10 .t09 .t08 .t07 .t06 .t05 .t04 .t03 .t02 .t01 .t00 .sic .sdy .scd .sba .say .saf .rtp .resx .rec .rdy .rda .rcs .qwc .qw5 .quic .qtx .qst .qss .qsm .qsd .qpi .qph .qpd .qpb .qob .qnx .qmt .qml .qme .qix .qif .qfx .qfi .qel .qdt .qdf .qch .qby .qbx .qbw .qbr .qbp .qbo .qbmb .qbm .qbk .qbi .qbb .qba .qb2020 .qb2019 .qb2018 .qb2017 .qb2016 .qb2015 .qb2014 .qb2013 .qb2012 .qb2011 .qb2010 .qb1 .q98 .q01 .q00 .ptk .ptdb .ptb .pr5 .pr4 .pr3 .pr2 .pr1 .pr0 .pma .pfd .p08 .omf .ofx .ofc .nv2 .nv .mwi .mny .mn9 .mn8 .mn7 .mn6 .mn5 .mn4 .mn3 .mn2 .mn1 .mmw .m90 .m80 .m70 .m60 .m50 .m40 .m30 .m20 .lmr .lid .lgb .kmy .inv .intu .iif .hsr .hif .hbk .gto .fxr .fp9 .fp8 .fp7 .fp6 .fp5 .fp4 .fp3 .fp2 .fim .f91 .f90 .f81 .f80 .f71 .f70 .f61 .f60 .f51 .f50 .f41 .f40 .f31 .f30 .f21 .f20 .exp .dxi .dgc .des .ddd .cus .coa .chg .cfp .cdf .brw .bpw .bpf .bgt .aif .acr .ach .ab4 .2020 .2019 .2018 .2017 .2016 .2015 .2014 .2013 .2012 .2011 .2010 .1pe .1pa.#vc .nni .ml9 .ml2 .ffd .sqli .sql2 .sql1 .sql .sdf .sdb .pdb .odb .myi .myd .mlb .mdf .mdb .indb .ibd .gdb .frm .dbs .dbf .db3 .db .accdb .pfx .pem .p7c .p7b .p12 .lic .key .gpg .der .csr .crt .aes

[표 3] 암호화 대상 확장자 목록

다음은 암호화에서 제외되는 파일 목록이다.

 Copyright © 2017 ESTsecurity Corp. All rights reserved.

thumbs.db	ntuser.ini	boot.ini
desktop.ini	ntuser.dat.log	index.dat
ntuser.dat	autoexec.bat	BOOTSECT.BAK

[표 4] 암호화 제외 파일

다음은 암호화 제외 대상 문자열 목록이다.

tmp	Boot	Content.IE5
Temp	Windows	node_modules
winnt	WinSxS	All Users
Application Data	DriverStore	AppData
AppData	League of Legends	ApplicationData
ProgramData	steamapps	nvidia
Program Files (x86)	cache2	intel
Program Files	httpcache	Microsoft
$Recycle.Bin	GAC_MSIL	System32
$RECYCLE.BIN	GAC_32	Sample Music
Windows.old	GOG Games	Sample Pictures
$WINDOWS.~BT	Games	Sample Videos
DRIVER	My Games	Sample Media
DRIVERS	Cookies	Templates
System Volume Information	History.IE5	

[표 5] 암호화 제외 문자열

위와 같은 파일과 문자열이 존재할 경우, 암호화를 진행하지 않는다. 이는 시스템 동작에 필요한 폴더 및 암호화 진행 간 불필요한 폴더를 제외하여 시스템 오류 방지와 암호화 속도를 높이기 위함으로 보인다.

리스팅된 파일들은 스트림 암호화 방법 중 하나인 ChaCha20 알고리즘을 통해 최대 파일의 오프셋 0x20000 영역까지 암호화한다. 다음은 암호화 코드의 일부이다.

 Copyright © 2017 ESTsecurity Corp. All rights reserved.

```
F_ChaCha_Encrypt(&input, lpBuffer, lpBuffer, nNumberOfBytesToRead);
if ( a2 == a1 && !SetFilePointerEx(a2, __PAIR__(v10, v6), 0, 0) )
  goto LABEL_25;
if ( !WriteFile(a1, lpBuffer, nNumberOfBytesToRead, &NumberOfBytesWritten, 0)
  || nNumberOfBytesToRead != NumberOfBytesWritten )
{
  v7 = -5;
  goto LABEL_34;
}
v11 = (__PAIR__(v11, v7) - nNumberOfBytesToRead) >> 32;
v7 -= nNumberOfBytesToRead;
v10 += ~nNumberOfBytesToRead < v6;
v6 += nNumberOfBytesToRead;
```

[그림 7] 암호화 코드 일부

암호화된 파일은 확장자가 'sage'로 변경되며 암호화된 파일내부에는 시그니쳐, 감염 PC 발급 ID, 파일 암호화에 사용된 키, 원본파일크기, 암호화 option 이 담겨있다. 암호화 진행 시 파일 원본크기를 두 번 저장하는 특징이 있다. 다음은 암호화 파일의 구조를 나타낸다.

암호화 된 Data (0x0~0x20000) + 원본데이터
Signature (0x5A9EDEAD : 0x4)
감염PC발급 ID (0x20)
파일 암호화에 사용된 키(0x20)
원본파일의 크기(0x4)
원본파일의 크기(0x4)
Blank(0x8)
Crypt Algorithm Option(0x4)
Signature (0x5A9EBABE : 0x4)
Blank(0x4)

[그림 8] 암호화 파일 포맷

⑤ 결제 안내

Sage 랜섬웨어에 감염된 사실과 결제를 안내하기 위해 암호화된 파일의 경로와 공용 및 사용자 계정의 바탕화면, 문서 폴더 경로에 랜섬노트 파일을 생성과 vbs 를 통한 음성안내를 수행한다. 다음은 음성안내 vbs 코드의 일부이다.

```
Set f=CreateObject("Scripting.FileSystemObject")
f.DeleteFile Wscript.ScriptFullName,True
On Error Resume Next
Set v=CreateObject("sapi.spvoice")
v.Speak"Attention! Attention! This is not a test!"
WScript.Sleep(1500)
v.Speak"All you documents, data bases and other important files were encrypted and Windows can not restore them without special software"
v.Speak"User action is required as soon as possible to recover the files"
WScript.Sleep(2000)
```

[그림 9] 음성안내 스크립트

ESTsecurity Copyright © 2017 ESTsecurity Corp. All rights reserved.

다음은 랜섬노트파일을 드롭하는 코드이다.

```
PublicDesktopPath = F_GetPublicDesktopPath();
F_CreateRansomNote(PublicDesktopPath, &RansomNoteText, 0);
UserDesktopPath = F_GetUserDesktopPath();
F_CreateRansomNote(UserDesktopPath, &RansomNoteText, &RansomNotePath);
UserDocuments = F_GetUserDocumentsPath();
F_CreateRansomNote(UserDocuments, &RansomNoteText, 0);
PublicDocuments = F_GetPublicDocumentsPath();
F_CreateRansomNote(PublicDocuments, &RansomNoteText, 0);
```

[그림 10] 랜섬노트 드롭 일부 코드

또한 바탕화면을 임시 폴더(%Temp%)에 생성된 결제 안내 그림파일인 '[랜덤파일명].bmp' 파일로 변경한다.

```
RandName = F_RandFileName();
TempPath = F_GetTempPath();
DesktopBMPPath = MakeStr("%s\\%s.bmp", TempPath, RandName);
ScreenHeight = GetSystemMetrics(SM_CYSCREEN);
ScreenWidth = GetSystemMetrics(SM_CXSCREEN);
F_DesktopImage(DesktopBMPPath, RansomNoteText, ScreenWidth, ScreenHeight, "A", 14.0, 0xEE00, 0);
F_CreateKeyReg(HKEY_USERS, 0xF003Fu, 0, F_SetDesktopImageReg);
return SystemParametersInfoW(SPI_SETDESKWALLPAPER, 0, DesktopBMPPath, 3u);
```

[그림 11] 바탕화면 변경 코드의 일부

Sage 랜섬웨어는 타 랜섬웨어와는 다른 특이점이 있다. 이는 레지스트리에 아이콘을 등록하여 'sage' 및 'hta' 확장자의 아이콘을 각각 열쇠 및 자물쇠로 변경 및 새로고침한다. 이는 감염 사실을 알리기 위한 것으로 보인다.

```
result = RegCreateKeyExA(HKEY_CURRENT_USER, "Software\\Classes", 0, 0, 0, 0xF003Fu, 0, &phkResult, 0);
if ( !result )
{
  v3 = MakeStr("mshta.exe \"%s\" \"%1\"", a2);
  RegSetValueW(phkResult, L".sage", 1u, L"sage.notice", 0);
  RegSetValueW(phkResult, "s", 1u, L"%WinDir%\\system32\\shell32.dll,47", 0);
  RegSetValueW(phkResult, &word_416576, 1u, &word_416552, 0);
  RegSetValueW(phkResult, L"sage.notice\\shell\\open\\command", 1u, v3, 0);
  RegSetValueW(phkResult, "s", 1u, L"%WinDir%\\system32\\shell32.dll,47", 0);
  RegSetValueW(phkResult, L"htafile\\DefaultIcon", 1u, "%", 0);
  F_HeapFree(v3);
  result = RegCloseKey(phkResult);
}
return result;
```

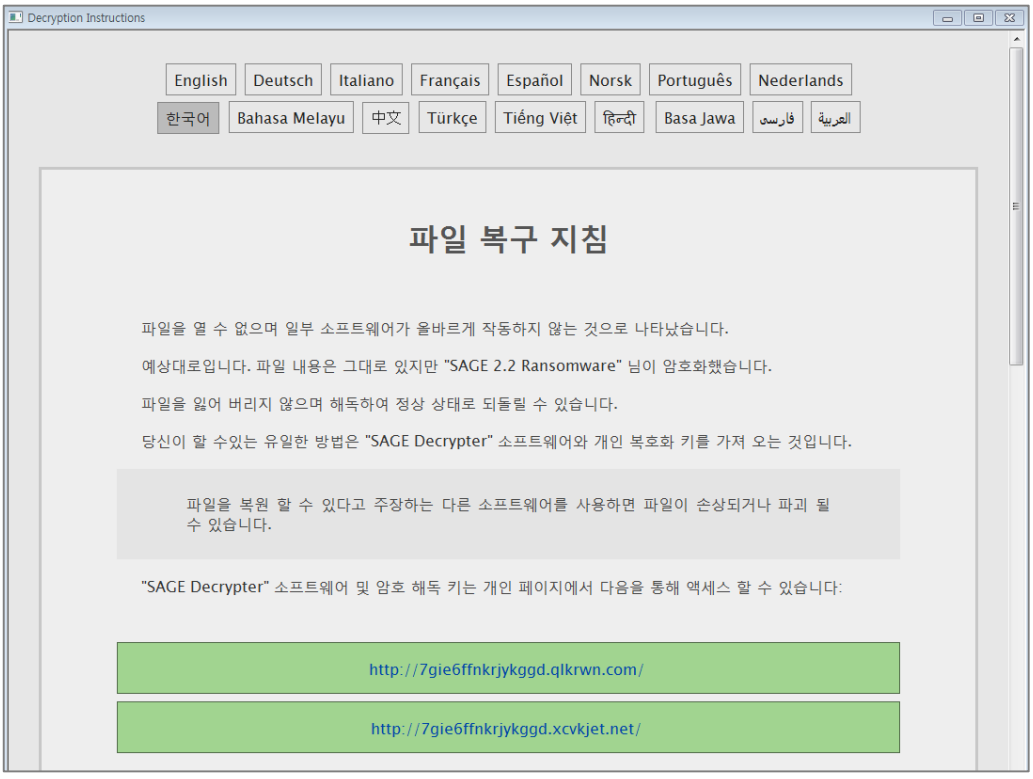
[그림 12] 아이콘 설정 코드

ESTsecurity Copyright © 2017 ESTsecurity Corp. All rights reserved.

다음은 변경되었을 때 아이콘이다.

[그림 13] 일부 확장자 암호화 확인

모든 암호화가 진행되고 바탕화면에 생성된 '!HELP_SOS.hta' 랜섬노트 파일을 실행하여 암호화 사실과 복호화를 위한 결제방법을 안내한다.



[그림 14] 파일 복구 지침 방법 안내

2.4 자가 삭제

모든 암호화가 진행된 이후 자가 복제한 파일, 시작 프로그램의 .lnk 파일을 삭제한다. 다음은 자가 삭제 코드의 일부이다.

 Copyright © 2017 ESTsecurity Corp. All rights reserved.

```
v4 = SHGetFolderPath();
v5 = sprintf("%sWW%s.lnk", v4, v3);
v6 = v5;
if ( a3 )
{
  result = DeleteFileW(v5);
}
```

[그림 15] 자가 삭제 코드

ESTsecurity Copyright © 2017 ESTsecurity Corp. All rights reserved.

3. 결론

이번에 다룬 sage2.2 악성코드는 사용자의 중요파일을 암호화 시킨 후 복구가 불가능하게 하며, 복구를 원할 시 복호화 비용으로 비트코인 결제를 요구하는 sage2.2 랜섬웨어이다. sage2.0 과는 다르게 sage2.2 에서는 한국어로 번역된 복호화 안내를 진행함으로써 국내 사용자들의 피해가 더 증가할 것으로 보인다.

또한 spora 랜섬웨어처럼 암호화에 필요한 key 를 주고받는 C&C 서버가 존재하지 않는다. 즉 오프라인에서도 감염될 위험성이 큰 만큼 폐쇄망을 사용하는 기업들의 대비가 필요하다.

따라서 지속적으로 변종이 등장하고 있는 만큼 사용자는 주기적으로 중요 파일을 백업하여야 하며, 패치 누락으로 인한 취약점이 발생하지 않도록 OS 와 소프트웨어는 최신 버전의 업데이트를 유지해야 한다. 메일로 첨부되는 파일에 대해서는 실행 시 주의해야 하고 백신을 최신 업데이트 상태로 유지하며 주기적인 검사를 실시하여야 한다.

ESTsecurity Copyright © 2017 ESTsecurity Corp. All rights reserved.

04
해외 보안 동향

영미권

중국

일본

ESTsecurity Copyright © 2017 ESTsecurity Corp. All rights reserved.

1. 영미권

새로운 Petya 는 랜섬웨어가 아니라 파괴적인 와이퍼(Wiper) 멀웨어로 밝혀져

Turns Out New Petya is Not a Ransomware, It's a Destructive Wiper Malware

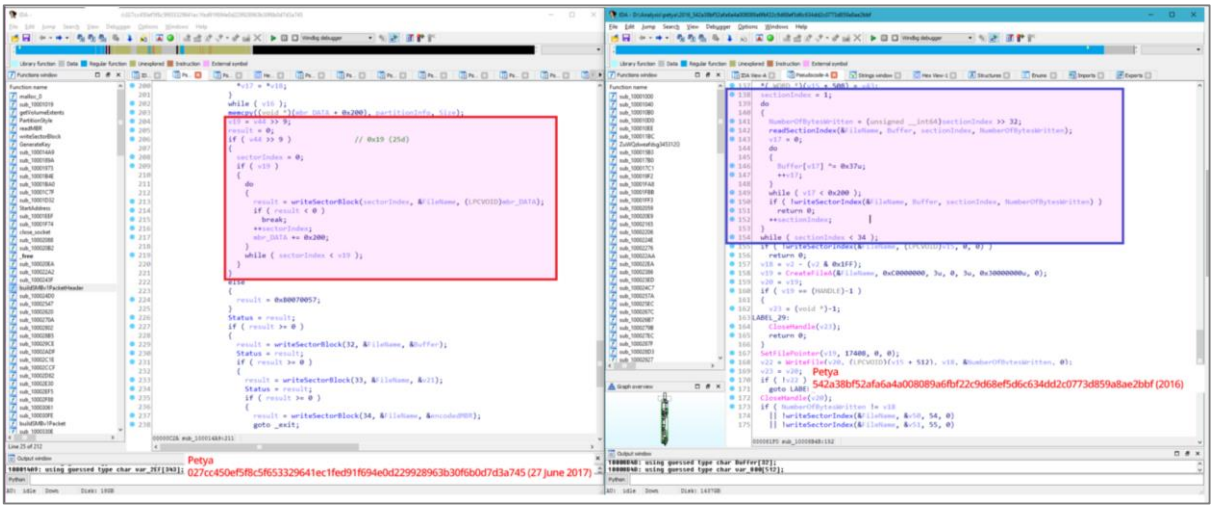
Petya 랜섬웨어가 요구하는 $300 의 랜섬머니는 컴퓨터를 복원해주는 의도가 전혀 아닌 것으로 밝혀졌다. Comae Technologies 의 설립자인 Matt Suiche 는 Petya 로 알려진 바이러스를 분석한 결과, 이는 랜섬웨어가 아닌 "와이퍼 멀웨어"라는 사실을 발견했다. 심지어, 보안 전문가들은 이 실제 공격이 국가가 주도한 우크라이나 공격에서, 멀웨어로 세계의 관심을 돌리기 위해 위장한 것이라 믿고 있다.

Petya 랜섬웨어의 실수인가, 아니면 과도하게 똑똑한 탓인가?

Petya 는 다른 일반적인 랜섬웨어와는 달리, 대상 시스템의 파일을 하나씩 암호화하지 않는다.

대신, Petya 는 피해자의 컴퓨터를 재부팅하고 하드 드라이브의 마스터 파일 테이블(MFT)을 암호화 하고 마스터 부트 레코드(MBR)을 사용할 수 없는 상태로 만들어서 파일의 이름, 크기, 물리적 디스크 내의 위치 등과 관련 된 정보를 점령해 전체 시스템에 대한 접근을 제한한다.

이후 MBR 의 암호화 된 복사본을 가져가고, 이를 랜섬노트를 표시하는 악성 코드로 바꿔버려 컴퓨터들을 부팅할 수 없는 상태로 만든다.



〈왼쪽: 와이퍼 코드가 포함 된 새로운 Petya 변종, 오른쪽: 기존의 Petya 랜섬웨어〉

〈원본 이미지 출처: https://blog.comae.io/petya-2017-is-a-wiper-not-a-ransomware-9ea1d8961d3b〉

 Copyright © 2017 ESTsecurity Corp. All rights reserved.

하지만 이 새로운 Petya 의 변종은 실수로, 또는 의도적으로 바꿔치기 된 MBR 의 복사본을 보관하지 않기 때문에, 피해자가 복호화 키를 얻더라도 감염 된 컴퓨터를 부팅할 수 없게 된 것이다.
또한 Petya 는 한대의 컴퓨터를 감염시킨 후 로컬 네트워크를 탐색하고 EternalBlue SMB 익스플로잇, WMIC, PSEXEC 툴을 이용해 재빠르게 동일한 네트워크 상의 다른 모든 장비들(심지어는 모두 패치 된 장비들까지)을 감염시킨다.

랜섬 머니를 지불하지말라; 파일을 복구할 수 없을 것이다
지금까지 총 45 명의 희생양이 $10,500 상당의 비트코인을 지불한 상태로 파일을 복구 받기를 기다리고 있겠지만, 안타깝게도 복구 받을 수 없을 것이다. 독일의 이메일 서비스 업체가 공격자와 피해자가 연락을 주고받고 복호화 키를 받는데 사용하는 이메일 주소의 사용을 중지 시켰기 때문이다. 이는 피해자들이 랜섬머니를 지불하더라도, 절대 파일을 복구 받을 수 없다는 것을 의미한다.

Kaspersky 의 연구원들도 "분석 결과 피해자가 데이터를 복구할 수 있다는 희망은 아주 희박한 것을 알 수 있었다. 우리는 암호화 루틴의 상위 레벨 코드를 분석했으며, 제작자가 디스크 암호화 후 피해자의 디스크를 복호화 할 수 없다는 사실을 발견했다. 피해자의 디스크를 복구하기 위해서, 제작자들은 설치 ID 가 필요하다.
Petya/Mischa/GoldenEye 와 같은 이전 버전의 '유사한' 랜섬웨어들에서는 이 설치 ID 내에 키 복구에 필요한 정보들이 포함되어 있었다."고 밝혔다.

새로운 Petya 변종이 전 세계의 서비스를 중지시키고 방해하도록 설계 된 파괴적인 멀웨어라는 연구원들의 주장이 사실이라면, 이 멀웨어의 임무는 성공적이었다고 볼 수 있겠다. 하지만, 여전히 추측이긴 하나 이 바이러스는 우크라이나의 지하철, Kiev 의 Boryspil 공항, 전기 공급 업체, 중앙 은행 및 국영 통신회사를 포함 주로 우크라이나의 기관들을 대상으로 공격을 수행했다. Petya 에 감염 된 다른 국가들은 러시아, 프랑스, 스페인, 인도, 중국, 미국, 브라질, 칠레, 아르헨티나, 터키, 대한민국 등이다.

Petya 는 어떻게 컴퓨터들에 침투할 수 있었나?
Talos Intelligence 의 연구에 따르면, 우크라이나의 MeDoc 이라는 회사가 주된 원인인 가능성이 높다.
연구원들은 우크라이나의 세금 계산 시스템인 MeDoc 의 악성 소프트웨어 업데이트를 통해 바이러스가 퍼졌다고 밝혔다. 하지만 MeDoc 은 페이스북을 통해 이를 부인하였다.
하지만, 몇몇 보안 연구원들과 심지어는 마이크로소프트도 Talos 의 연구결과에 동의하며 MeDoc 이 해킹 되었으며 바이러스가 업데이트를 통해 퍼진 것으로 보인다고 밝혔다.

[출처] http://thehackernews.com/2017/06/petya-ransomware-wiper-malware.html

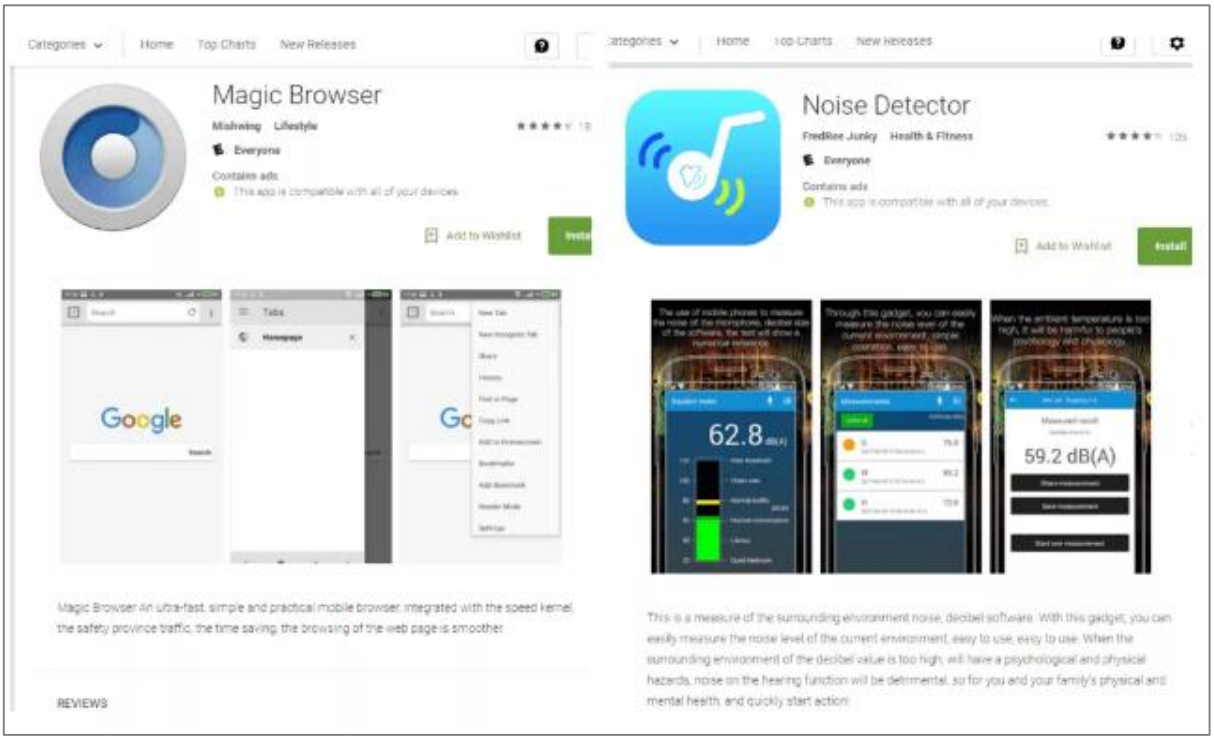
 Copyright © 2017 ESTsecurity Corp. All rights reserved.

Ztorg 트로이목마 2 개, 구글 플레이 스토어에서 제거 돼

Two Ztorg Trojans Removed from Google Play Store Are Definitely Better

한달 만에 2 번째로, 구글이 공격자들이 타겟 기기를 루팅하는데 사용할 수 있는 Ztorg 트로이목마에 감염 된 악성 앱들을 제거했다.

소프트웨어 개발자들 대부분은 취약점 패치 및 새로운 기능 추가를 위해 앱을 업데이트한다. 하지만 이 소프트웨어가 멀웨어일 경우, 업데이트는 최악의 작업일 수 있다. 구글 플레이스토어는 항상 사용자들이 멀웨어를 다운로드하는 것을 예방하기 위해 노력하고 있으며, 최근 Ztorg 멀웨어가 포함 된 앱 2 개를 제거했다. 이 두개의 앱은 "Magic Browser"와 "Noise Detector"이며, 원래 플레이 스토어에 업로드 되었을 때는 정상적인 앱이었으나 시간이 지날수록 멀웨어 툴킷을 사용하는 악성 소프트웨어로 업데이트 되었다.



Ztorg 멀웨어 툴킷은 카스퍼스키랩이 2016 년 9 월 "Guide for Pokemon Go"앱에 포함된 것을 처음 발견했다. 당시 이 앱은 50 만회 이상 다운로드 되었으며, 연구원들에 따르면 그중 6 천 건이 성공적으로 감염 되었다. 이후 Ztorg 가 포함 된 수십개의 앱들이 구글 스토어를 통해 배포되었으며 결국 삭제되었다.

일단 초기 앱이 설치 되면, 이는 광범위한 고급 기술들을 사용해 탐지를 피하며 C&C 인프라로부터 업데이트를 받아 기기에서 Root 접근 권한을 얻으려 시도한다. Fortinet 연구원들에 따르면:
많은 에뮬레이터 탐지 기능을 구현한다. 이는 안드로이드 SDK 에뮬레이터, Genymotion, Bluestacks 및 BuilDroid 의

 Copyright © 2017 ESTsecurity Corp. All rights reserved.

에뮬레이터들을 탐지한다. 또한 오염 된 환경도 탐지한다. 이들의 점검 사항들 중 몇 개는 우회하기 어렵다.
XOR 기반의 강력한 문자열 난독화를 사용한다.
DES-CBC 암호화를 사용해 원격 서버와 통신한다.
원격서버에서 안드로이드 어플리케이션을 다운로드, 설치 및 실행한다.

스마트폰이 Ztorg 트로이목마에 감염 되면 무슨 일이 일어나는가?

다른 대부분의 멀웨어들처럼, 범죄자들의 궁극적인 목적은 돈을 버는 것이다. 초기 Ztorg 트로이목마는 정식 광고 네트워크를 통해 수익을 창출하는 AdWare 를 사용했다. 사용 된 기술들 중 일부는 웹 페이지 리디렉팅, 검색 결과 조작, 사용자가 방문하는 사이트 정보 수집 등이 있다. 범죄자들이 모든 수익을 가져가며, 사용자의 기기는 성능이 저하되어 불안정하게 되거나 사용할 수 없게 될지도 모른다.

최근 구글 플레이스토어에서 제거 된 앱인 "Magic Browser"와 "Noise Detector"는 불법적으로 돈을 벌 수 있는 새로운 기술들을 포함해, Ztorg 트로이목마의 기능이 진화했다는 것을 보여준다. 사용자의 기기로 특정 문자 메시지를 보내 요금이 청구 되도록 하는 '유료 SMS 보내기'가 주요 비즈니스 모델이다. 예를 들면, 사용자는 문자로 금액을 보내기만 하면 재난 구호 자금을 기부할 수 있다. 최신 Ztorg 트로이목마는 이러한 유료 SMS 시스템을 악용해 수익을 발생시킨다. 다른 Ztorg 시스템들과 마찬가지로, 이들도 수익을 극대화 하고 탐지를 피하기 위한 정교한 기술들을 사용한다.

일단 감염 되면, 트로이목마는 10 분간 휴면 상태에 들어간다. 이로써 사용자가 뭔가 이상함을 느끼더라도, 설치 된 앱과 연결시킬 확률을 줄인다. 휴면 후, 이 트로이목마는 기기의 IMSI 의 처음 5 자리를 C&C 서버로 전송한다. 이 부분은 기기가 연결 된 네트워크 및 국가를 식별한다. 이 정보를 이용해 C&C 는 어떤 유료 SMS 서비스가 가능한지 파악한 후 요금을 마구 청구하기 시작한다. 대부분의 유료 SMS 서비스들은 이후 텍스트 메시지로 영수증이나 알림을 보내지만, Ztorg 트로이목마가 들어오는 SMS 메시지들을 삭제해버린다.

보안 연구원들은 "보안 장치들을 우회하고 많은 기기들을 감염시키기 위한 새로운 트릭으로 무장한 Ztorg 트로이목마가 지속적으로 구글 플레이 스토어에 나타나고 있다. 피해자들이 정상적인 앱을 다운로드 할지라도, 시간이 지난 후에도 이 앱이 여전히 깨끗할거라는 보장은 없다. 사용자들, 구글, 그리고 보안 연구원들은 항상 이를 경계해야하며, 적극적으로 대응해야 할 것이다."고 밝혔다.

[출처] http://securityaffairs.co/wordpress/60272/malware/ztorg-trojans-google-play-store.html

 Copyright © 2017 ESTsecurity Corp. All rights reserved.

리눅스와 BSD 시스템의 Stack Clash 취약점, 루트 접근 허용해

STACK CLASH VULNERABILITY IN LINUX, BSD SYSTEMS ENABLES ROOT ACCESS

Linux, BSD, Solaris 와 기타 오픈 소스 시스템들이 공격자들이 루트에서 코드를 실행시킬 수 있도록 허용하는 로컬 권한 상승 취약점인 Stack Clash 에 취약한 것으로 나타났다. 주요 리눅스 및 오픈소스 배포자들은 금일 패치를 발표했다. 리눅스, OpenBSD, NetBSD, FreeBSD 또는 i386 이나 amd64 하드웨어에서 Solaris 를 사용중인 시스템들은 신속히 업데이트 해야한다.

이 결함(CVE-2017-1000364)으로 인한 위험은 특히 공격자가 취약한 시스템에 이미 존재하고 있을 경우 상승한다. 이 취약점을 발견한 Qualys 의 연구원들은 공격자들이 이 취약점을 최근 수정 된 Sudo 취약점을 포함한 다른 치명적인 문제들과 연쇄적으로 적용할 수 있게 되었으며, 가장 높은 권한으로 임의의 코드를 실행할 수 있다고 밝혔다.
이 취약점은 시스템의 메모리 관리 영역인 스택에서 발견 되었다. 이 공격은 리눅스가 2010 년 도입한 스택의 가드페이지 완화 장치를 우회한다.
이 스택 메모리 영역은 프로그램이 더 많은 스택 메모리를 필요로 할 때 확장시키는 메커니즘을 포함하도록 설계 되어있다. 하지만, 이는 보안 위협이 될 수 있다.

Qualys 는 “포인터의 스택 포인터가 페이지 오류를 일으키지 않고 공격으로부터 (공격이 시작하는 곳에서 정확히 끝나는) 다른 메모리 영역으로 이동될 수 있다면, 이 프로세스는 다른 메모리 영역을 스택의 확장 영역인 것처럼 사용할 수 있다.”고 밝혔다. 공격자는 이 확장된 스택에 쓸 수 있고(write) 인접한 메모리 영역을 충돌시키거나, 다른 메모리 영역에 쓰고(write) 확장된 스택을 충돌시킬 수 있다.

또한 Qualys 는 이 취약점이 원격으로 악용 될 가능성을 완전히 배제하지 않았다.
Qualys 는 그들이 작성한 7 개의 PoC 익스플로잇들이 모든 과정이 완료되기 전 까지 free 되어서는 안되는 메모리를 할당하는 4 단계의 순차적 절차를 밟는다고 밝혔다. 이 4 단계는 스택을 다른 메모리 영역과 충돌 시키는 것, 스택 포인터를 스택의 시작부분에서 실행하는 것, 스택 가드 페이지를 건너뛰는 것, 그리고 스택 또는 다른 메모리 영역을 충돌시키는 것이다.

Qualys 는 업데이트가 적용되기 전 까지, 임시 방편으로 스택 가드페이지의 사이즈를 최소 1MB 로 늘리는 것을 권고하였다. 또한 모든 유저랜드 코드를 –fstack-check 옵션으로 리컴파일링 하기를 추천하였다. 이는 스택 포인터가 다른 메모리 영역으로 이동하는 것을 방지할 것이다. Qualys 는 이는 비용이 많이 드는 해결책이지만, –fstack-check 옵션에 알려지지 않은 취약점이 있는 것이 아닌 이상 아주 좋은 해결책이라 밝혔다.

[출처] https://threatpost.com/stack-clash-vulnerability-in-linux-bsd-systems-enables-root-access/126355/

 Copyright © 2017 ESTsecurity Corp. All rights reserved.

2. 중국

중국 사이버 보안법, 6 월 1 일부터 시행

《网络安全法》今日起施行 与你息息相关

6 월 1 일부터, 〈중국인민공화국사이버보안법(이하 사이버보안법)〉이 정식으로 시행된다. 이 사이버보안법은 중국 사이버보안업계의 향후 발전방향, 새로운 사업 및 사이버보안의 발전과 이익에 중요한 조치가 될 것으로 보인다.

〈사이버보안법〉은 총 7 장 29 조로 이루어져 있으며, 총칙, 사이버보안 촉진, 네트워크운영보안, 사이버정보 보안, 감사경보 및 긴급조치, 법률책임 및 부칙들로 구성되어 있다. 법률책임 및 부칙 외, 그 대상에 따라 각 조례는 크게

- 국가의 책임과 의무
- 유관부문 및 각 정부부처의 역할 분담
- 인터넷서비스 운영업자들의 책임과 의무
- 인터넷제품 및 서비스 제공자들의 책임과 의무
- 중요정보를 기반으로하는 인터넷보안관련 조례
- 기타

총 6 개의 분류로 나눌 수 있다.

이 중, 다음 3 가지 부분은 중국사용자들의 안전한 인터넷 생활을 할 수 있도록 보호막이 될 것으로 보인다.

해당 법률은 다음과 같이 규정되어 있다. 인터넷서비스 운영업자들은 서비스와 무관한 개인정보를 수집 및 제공할 수 없으며, 행정법에 규정되어 있고 사용자와 사업자 서로 동의한 개인정보에 대해서만 수집 및 사용할 수 있다. 또한 법률에 명시되어 있는 규정을 통하고, 사용자에 동의가 있어야만 사용자의 개인정보를 처리 및 보관할 수 있다. 만약, 개인 사용자가 인터넷서비스 운영자가 법률을 위반하거나 사용자의 동의없이 개인정보 수집을 발견하였다면, 인터넷서비스 운영자에게 자신의 개인정보를 삭제할 권리가 있다.

또한 국가는 미성년자의 건강한 인터넷 생활에 도움을 주기 위해 인터넷을 통해 미성년자의 심신건강에 위협이 되는 서비스를 제공하는 자는 법률에 따라 처벌하여, 미성년자들에게 안전하고 건장한 인터넷환경을 제공해 주도록 명시되어 있다. 모든 개인과 조직은 인터넷보안을 위협하는 행위를 발견할 시 China Telecom, NCF Group, 공안국 등 관련부처에 신고를 할 권리가 있다. 이는 미성년자 인터넷보안이 법률의 보호를 받을 수 있도록 한 조치다.

 Copyright © 2017 ESTsecurity Corp. All rights reserved.

법률에는 모든 개인과 조직은 비합법적인 방법으로 타인의 인터넷을 침범하고, 타인의 정상적인 인터넷 생활을 방해하고, 데이터를 탈취하는 등 인터넷 보안에 위협이 되는 행위들을 금지한다고 명시하였다. 또한 다른 사용자 인터넷 환경에 침입하거나, 정상적인 인터넷 환경과 보호조치를 방해하고, 사용자들의 데이터를 탈취할 수 있는 등의 프로그램이나 툴을 판매해서도 안된다고 명시하였다. 뿐만 아니라, 태인의 안전한 인터넷 생활을 위협할 수 있는 기술적 지원, 서비스 및 광고 유포 등의 도움도 철저히 금지한다고 명시되어 있다.

중국 국가통계국이 2017 년 2 월 28 일에 발표한 〈중화인민공화국 2016 년 국민경제 및 사회발전통계보고서〉에 따르면, 2016 년 중국 인터넷사용자수는 7.31 억명, 그 중 모바일을 이용한 인터넷사용자 수는 6.95 억명, 인터넷보급률은 53.2%에 달하며, 그 중 농촌지역에 인터넷 보급률은 33.1%라고 확인되었다.

〈사이버보안법〉의 등장은, 중국의 첫번째 사이버 보안에 대해 전문적으로 종합적인 내용을 담은 입법안으로 매우 중요한 의미가 있다. 미래에, 이 사이버보안법을 근거로, 법률의 보호 아래서 중국의 인터넷 환경이 더 안전하고 좋게 발전할 것이 기대된다.

[출처] http://news.mydrivers.com/1/534/534589.htm

 Copyright © 2017 ESTsecurity Corp. All rights reserved.

중국에서 개발된 "Fireball" 악성코드 분석

国产流氓软件“火球”分析与溯源

6 월 1 일, CheckPoint 는 중국 기업에서 개발된 "Fireball" 악성코드를 발견하였다고 발표하였다.

Fireball 악성코드 사건은, huorong 보안연구원들이 Mustang, DealWifi 등을 위장한 8 개의 악성코드를 발견하면서 시작되었다. 이 악성코드들은 사용자 PC 를 감염시킨 후 Chrome 브라우저 시작 페이지, TAB 페이지를 임의의 검색페이지로 변경시킨 후 사용자들이 다시 변경할 수 없도록 한다. 변경하는 페이지들은 각각 다르지만, 검색페이지에서 모두 야후와 구글의 데이터를 크롤링 하는 것으로 보아 악성코드 제작자들이 야후와 구글의 광고를 통해 수익을 얻는 것이 아닐까 추측하고 있다.

악성코드는 사용자 PC 에 설치될 때 사용자 PC 에 크롬브라우저가 있는지 확인하는데, 만약 크롬브라우저가 없다면 아무일도 발생하지 않지만, 만약 크롬브라우저를 사용하고 있다면 플러그인 설치하지 않으면 프로그램을 설치할 수 없다는 창을 띄우며 사용자의 설치를 유도한다.

이 프로그램들은 卿烨科技, 百盛达科技등 여러 기업들을 통해 제공되었지만, Huorong 보안연구원들이 추적해본 결과, 모두 동일한 “baoyu430@gmail.com”계정을 가진 제작자에 의해 제작된 것으로 확인되었다. 제작자는 각기 다른 홈페이지에서 대량의 악성코드를 제작한 것이다.

이 악성코드는 크롬브라우저만을 타깃으로 하고 있지만, 크롬브라우저가 전 세계 적으로 많이 사용되고 있는 만큼, Fireball 악성코드의 파급력은 매우 클 것으로 예상되고 있다. 사용자는 해당 악성코드를 제거함으로서 크롬 브라우저 설정을 복구할 수 있다.

이번 Fireball 사건은 비록 해외에서 발견되었지만, 그 공격 수법은 이미 중국에서도 흔히 볼 수 있는 방법이다. 이는 즉 중국 내 해킹조직들의 공격수법이 전 세계적으로 퍼져나가고 있다고 볼 수 있다.

사건 분석

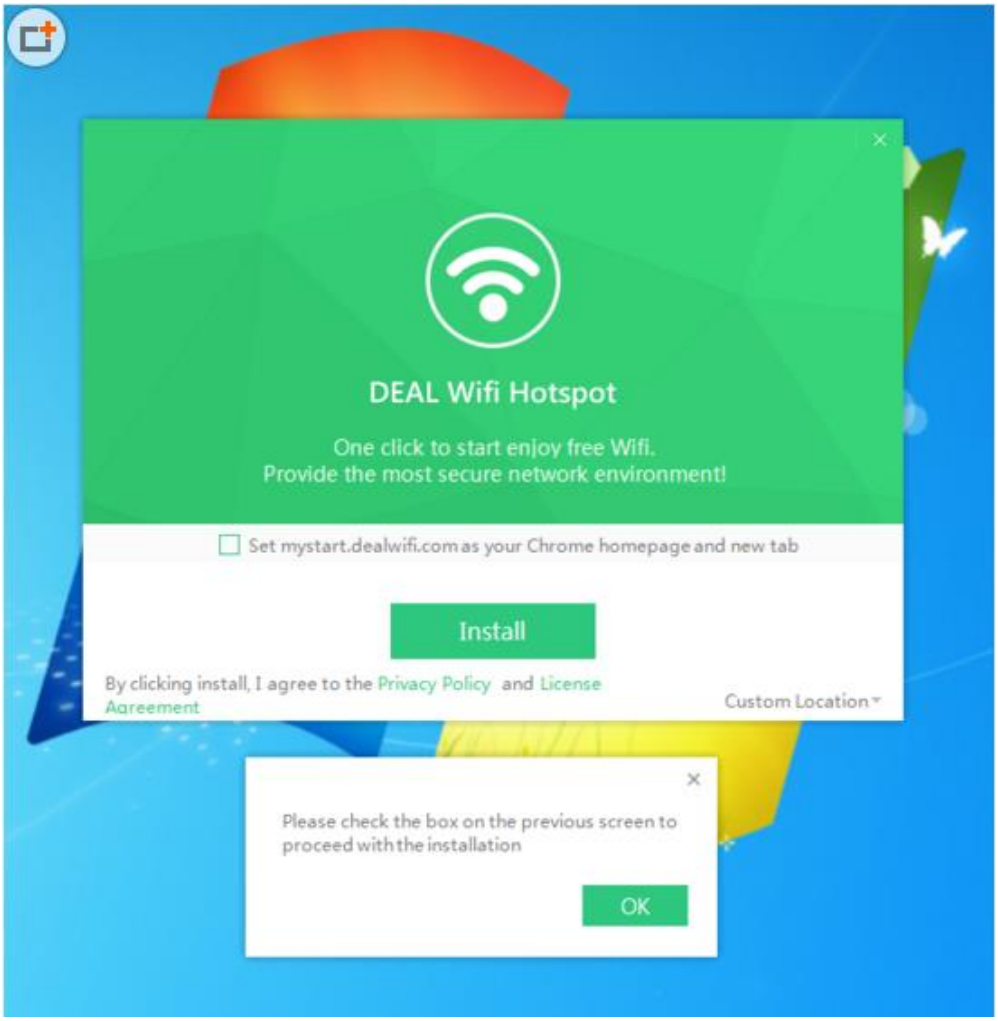
최근 Fireball 악성코드를 발견한 후 조사를 한 결과, 해당 사건과 관련된 더 다양한 악성코드들을 발견할 수 있었다.

 Copyright © 2017 ESTsecurity Corp. All rights reserved.

软件名称	软件首页	数字签名
Mustang Browser	http://mustang-browser.com	RAFO TECHNOLOGY INC.
Deal WiFi	http://dealwifi.com	RAFO TECHNOLOGY INC.
FVP Imageviewer	https://www.fvpimageviewer.com	Beijing Baijianqi Touzi Guanli Youxiangongsi
Soso Desktop	https://sosodesktop.com	BYSENDA TECHNOLOGY LIMITED
Holainput 输入法	http://holainput.com	Hongkong zoekyu Technology Limited
OZIP	http://ozipcompression.com	Hongkong zoekyu Technology Limited
Siviewer	http://siviewer.com	EVANGEL TECHNOLOGY (HK) LIMITED
Winzippers	http://www.winzippers.com	(软件未下载成功)

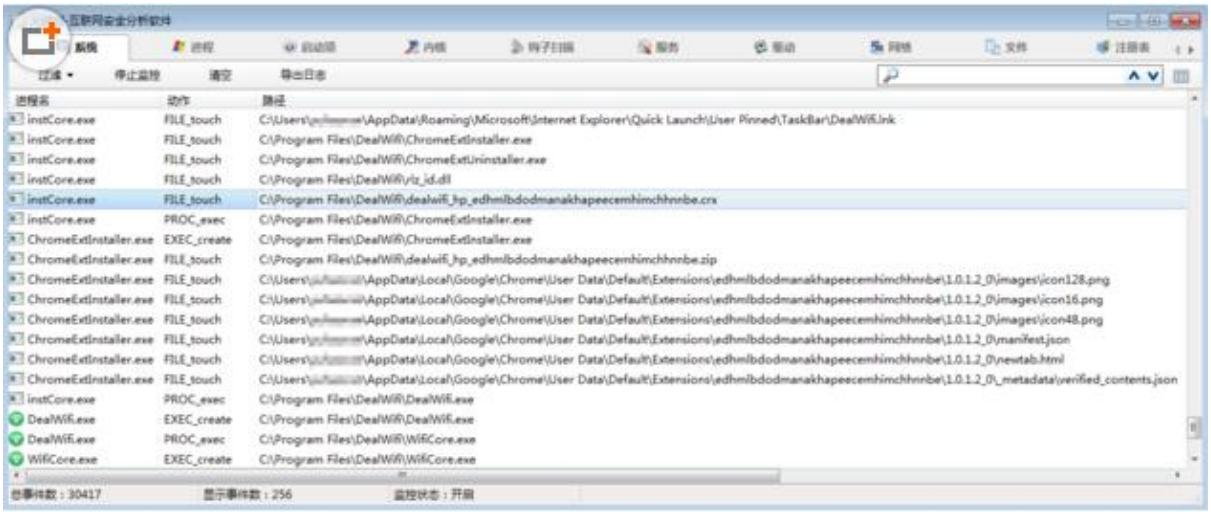
DealWiFi 프로그램을 예로 들어보겠다.

해당 프로그램이 설치 될 때 다음과 같은 화면이 보이게 되는데, 만약 사용자가 “Setmystart.dealwifi.comasyourchromehomepageandnewtab” 선택을 하지 않는다면 프로그램 설치가 불가하게 된다.



해당 옵션을 선택한 후 설치를 하면, 다음과 같이 크롬 플러그인을 설치한다.

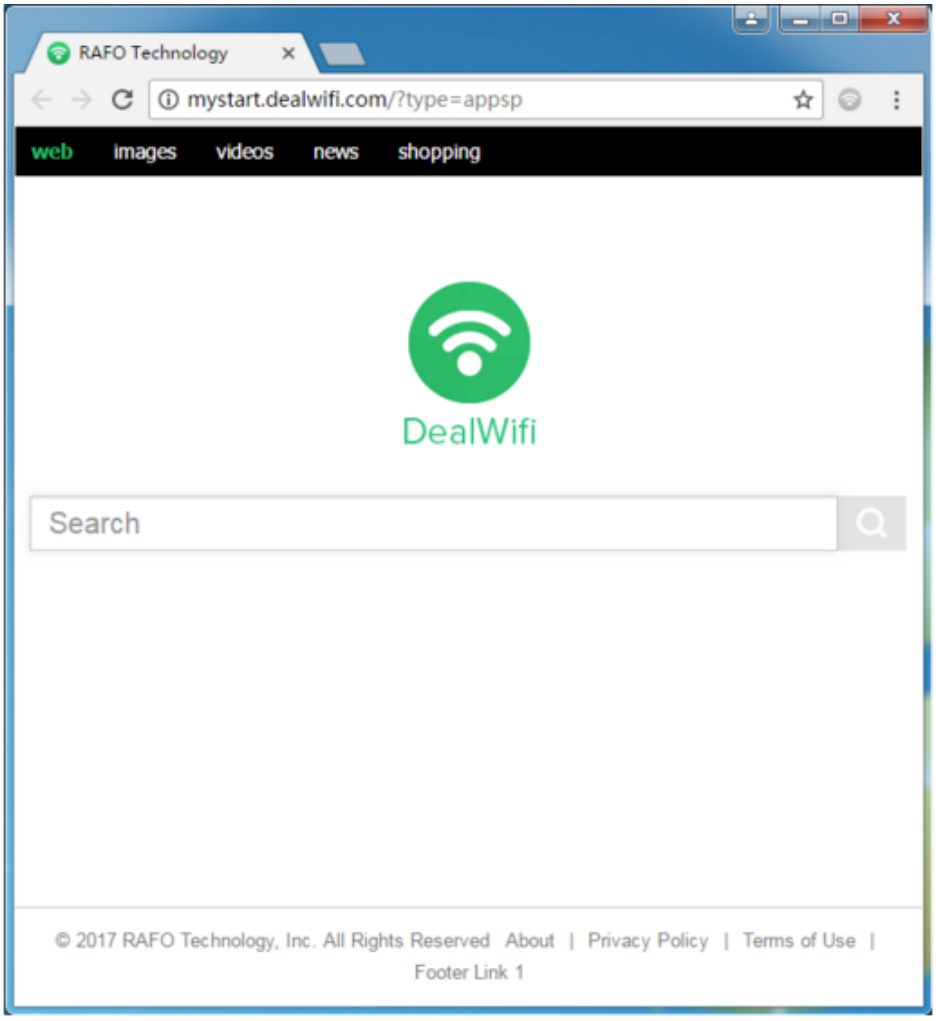
 Copyright © 2017 ESTsecurity Corp. All rights reserved.



해당 플러그인은 크롬의 설정에서 기본 페이지를 강제로 변경한다.

 Copyright © 2017 ESTsecurity Corp. All rights reserved.

설정이 변경된 크롬 브라우저의 시작 페이지 화면은 다음과 같다.



이런 악성코드들은 강제로 설치한 프로그램과 동일한 이름을 가진 크롬 플러그인을 강제로 설치한다. 이 플러그인들의 기능은 모두 시작페이지를 고정하며, “SosoDesktop”이라는 명칭을 가진 악성코드는 강제로 기본 검색엔진을 변경하기도 한다.

软件名称	锁定首页
Deal WiFi	hxxps://mystart.dealwifi.com/?type=apps
OZIP	hxxp://search.ozipcompression.com/?r=sp
Siviewer	hxxp://start.siviewer.com/?r=sp
SOSO DESK	hxxp://search.sosodesktop.com/?so=sp
FVP Imageviewer	hxxp://search.fvpimageviewer.com/
Holainput	hxxp://search.holainput.com/?r=b

분석결과, Holainput 프로그램이 변경하는 시작 검색 페이지의 검색결과는 최종적으로 Google 로 가지만, 나머지 검색페이지들은 야후의 검색결과와 동일한 것으로 보아 최종적으로 야후로 넘어가는 것으로 추측할 수 있었다. 하지만

 Copyright © 2017 ESTsecurity Corp. All rights reserved.

구글이든 야후든, 결과적으로 사용자의 검색 기록을 모두 공격자 서버에 저장하기 때문에 검색 키워드를 통한 추가적인 정보들이 유출될 가능성도 있다.

조사 결과에 따르면, 위에 언급된 악성프로그램들은 모두 baoyu430@gmail.com 메일로 등록이 되어있었다. 卿烨科技 회사 정보를 검색해본 결과, 卿烨科技라는 이름을 가진 회사들은 총 5 곳이 있었으며, 그 중 해당 악성코드와 직접적으로 연관이 있는 회사는 총 3(北京卿烨, 海卿烨北京分公司, 上海卿烨)곳으로 확인되었다.

Check Point 보고서에 따르면, 중국에서 개발된 이 악성코드는 전 세계를 강타하고 있으며, 인도, 브라질, 멕시코, 인도네시아, 미국 순으로 많이 감염되었다고 밝혔다. 하지만 중국에서의 감염률은 그렇게 많지 않은 것으로 나타났다.

그 이유는 무엇일까?

그 이유는 중국에서는 살아남기가 매우 힘들어서 일 것이라고 추측했다. 중국에서는 이러한 수법을 사용하는 악성코드는 결코 새로운 것이 아니기 때문일 것이다.

그리고 중국의 일각에서는 Fireball 을 악성코드라고 보기도 힘들다는 견해도 있다. 그 이유는 중국에서 뜻하는 악성코드는 보안프로그램이 정당한 이유로 제거할 수 있는 프로그램(웜, 트로이목마, 다운로더 등)을 뜻하는데 Fireball 은 설치과정에 명백히 사용자의 동의를 받는 영역이 있으며, 제어판에서 직접적으로 삭제할 수도 있기 때문에 사기 프로그램(Rogue software)으로 보는 것이 더 맞다는 견해도 있다.

현재 알약에서는 해당 악성코드에 대하여 Misc.Riskware.Elex, Trojan.Agent.153600C, Misc.Riskware.Mutabaha 로 탐지하고 있다.

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

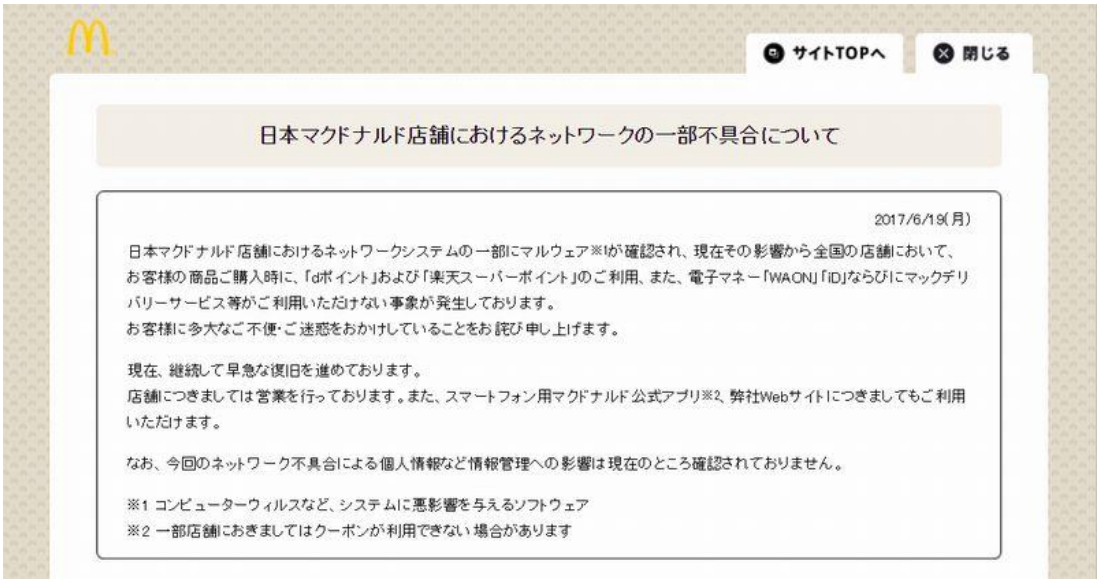
 Copyright © 2017 ESTsecurity Corp. All rights reserved.

3. 일본

맥도날드 시스템 장애는 악성코드가 원인, 대량 패킷으로 통신 차단

マックのシステム障害はマルウエアが原因、大量パケットで通信が遮断

일본 맥도날드의 점포시스템에서 일어나고 있는 장애에 대해 맥도날드는 2017 년 6 월 19 일, 이 시스템이 악성코드에 감염되어 있었다고 발표했다. 복수 점포시스템의 컴퓨터가 악성코드에 감염되어 외부로 대량 패킷을 발신하고 통신에 부담을 주어, 상품구입 시의 포인트서비스를 이용할 수 없게 된 것이라고 한다. 이 회사에서는 새롭게 전자화폐나 택배서비스 등도 이용할 수 없게 된 사건이 일어나고 있다는 것도 밝혀졌다.



일본 맥도날드 점포에서의 네트워크의 일부 문제에 대해서

일본 맥도날드 점포에서의 네트워크시스템의 일부에 악성코드가 확인되어 현재 그 영향에서 전국 점포에서 고객의 상품 구입 시에 'd 포인트' 및 '라쿠텐 수퍼 포인트'의 이용,

또 전자화폐 'WAON', 'iD' 및 맥딜리버리 서비스 등을 이용할 수 없는 사건이 발생하고 있습니다. 고객님께 큰 불편을 끼쳐드린 점 사죄 드립니다.

현재 계속해서 조속히 복구를 진행하고 있습니다.

점포에서는 영업을 하고 있습니다. 또 스마트폰용 맥도날드 공식 어플, 저희 회사 Web 사이트에서도 이용하실 수 있습니다.

그리고 이번 네트워크 문제에 의한 개인정보 등 정보관리에 대한 영향은 현재 확인되지 않고 있습니다.

시스템장애를 알리는 일본 맥도날드 Web 사이트 (출처:일본 맥도날드)

회사는 악성코드의 종류에 대해서 '조사 중'이라며 명백히 밝히지 않았다. 올해 5 월에 세계적으로 발생한 랜섬웨어

 Copyright © 2017 ESTsecurity Corp. All rights reserved.

'WannaCry(워너크라이)'의 가능성도 있다고 했다. 다만, 네트워크 경유로 자기 증식하여 감염을 확산시키는 웜의 동작은 하고 있지 않다고 한다. 이 회사 앱 등록자의 데이터를 비롯한 기밀데이터의 사외유출은 '확인되지 않고 있다'고 한다.

악성코드에 감염된 것은 점포에 설치하여 판매관리 등을 담당하는 시스템 컴퓨터로, 복수 점포에서 감염을 확인했다. 감염된 컴퓨터가 대량의 패킷을 발신하여 이 회사 네트워크 및 정상적인 패킷에 과부하를 일으키거나, 포인트서비스 시스템과의 통신이 타임아웃하여 시스템장애를 일으켰다고 한다.
이용할 수 없는 서비스는 'd 포인트', '라쿠텐수퍼포인트', 전자화폐 'WAON', 'iD' 그리고 회사 배달서비스 '맥딜리버리'이다.

[출처] http://itpro.nikkeibp.co.jp/atcl/news/17/061901699/?ST=security&itp_list_theme

 Copyright © 2017 ESTsecurity Corp. All rights reserved.

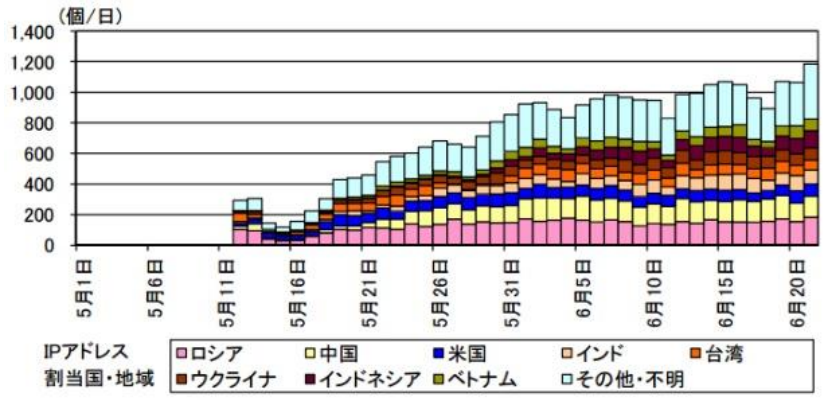
랜섬웨어 공격하지 않는 'WannaCrypt' 변종이 확산 – 잠복 주의

ランサム攻撃発動しない「WannaCrypt」亜種が拡散 - 潜伏にご注意

악성코드 'WannaCrypt'에 감염된 단말을 발신원으로 한 패킷이 계속 발견되고 있다. 6 월 이후에는 랜섬웨어 공격을 하지 않는 새로운 변종이 확산을 보이고 있다고 한다.

관측시스템을 운영하는 경찰청이 'WannaCrypt'이나 이 악성코드 변종에 감염된 단말을 발신원으로 한 TCP 445 번 포트 접속에 대해서 관측 상황을 정리했다. 이 악성코드는 'WannaCryptor', 'WanaCrypt0r', 'Wanna Decryptor', 'WannaCry', 'WCry'로도 알려진 랜섬웨어다. 이미 알려진 Windows 에 관한 취약성 'MS17-010'을 악용하여 감염을 확산시키는 웜의 성질을 가지고 5 월 13 일 전후부터 전세계로 감염이 확대되었다.

경찰청에서도 5 월 12 일부터 이 악성코드에 의한 감염활동으로 보이는 패킷을 관측했다. 14 일부터 수일간에 걸쳐 일시적으로 패킷량의 감소도 볼 수 있었으나, 그 후는 패킷량이 증가했다. 러시아나 중국, 미국, 인도, 대만, 인도네시아 등을 발신국으로 한 이 악성코드에 의한 패킷이 계속해서 관측되고 있다.



경찰청 시스템에 패킷을 송신한 'WannaCrypt' 감염단말의 IP 주소 수의 추이 (그래프 : 경찰청)

등장 초기의 단계에서 보안기관의 공지나 특정 도메인에 접속을 할 수 있는 경우에 활동을 정지하는 이른바 '킬 스위치' 기능이 밝혀지는 등 이 악성코드에 대한 대책이 진행되었으나, 그 한편으로 '킬 스위치'가 활동하지 않는 새로운 변종이 유통되었다.

게다가 랜섬웨어의 주요기능인 '암호화 기능'을 발동하지 않는 변종이 등장했다. 경찰청에 따르면 6 월 초순 이후에 감염된 단말은 이러한 변종에 감염되었다는 사실이 밝혀지고 있다고 한다.

 Copyright © 2017 ESTsecurity Corp. All rights reserved.

경찰청에서는 당초의 'WannaCrypt'와 달리 변종은 랜섬웨어의 모습을 볼 수 없는 만큼 감염에 대해 눈치채기 힘들고, 네트워크를 통해 감염이 확대될 우려가 있다고 지적한다. 네트워크의 문제를 일으키거나 감염원인이 된 취약성이 방치되고 있다는 사실을 눈치채지 못하고 다른 악성코드의 감염을 일으킬 가능성도 있어 주의를 호소하고 있다.

[출처] http://www.security-next.com/083070

ESTsecurity Copyright © 2017 ESTsecurity Corp. All rights reserved.

메루카리가 개인정보 유출에서 얻은 새로운 정보, 실제는 '유효기한 0 초 캐시'

メルカリが個人情報流出で新情報、実際は「有効期限0秒のキャッシュ」

메루카리는 2017 년 6 월 27 일, 메루카리 Web 버전의 개인정보 유출에 관해서 새로운 정보를 이 회사의 기술 블로그에서 공개했다. CDN 의 캐시 동작에 대해서 CDN 프로바이더와 사양에 대해서 확인하고 검증한 결과라고 한다. 6 월 26 일까지의 설명과는 일부 다른 점이 있어서, 블로그 엔트리를 수정했다.

CDN 교체작업에서의 Web 판 메루카리의 개인정보유출의 원인에 대해서

오늘 기업 사이트에서 공지한 바와 같이 Web 버전의 메루카리에서 일부 고객님의 개인정보가 타인에게 열람될 수 있는 상태가 있었다는 사실이 판명되었습니다. 원인인 이미 판명되어 수정이 완료되었습니다. 또한 개인정보를 열람 당했을 가능성이 있는 고객들에게는 메루카리사무국에서 메루카리 내의 개별 메시지로 연락을 하였습니다. 고객님의 소중한 개인정보를 맡겨주셨는데 이와 같은 사태가 벌어져 깊은 사죄 말씀을 드립니다.

본 엔트리에서는 기술적 관점에서 상세한 내용을 전해 드리겠습니다.

2017 년 6 월 27 일 CDN 의 캐시동작에 대해서 CDN 제공업체와 사양에 대해서 확인하고 검증을 했습니다. 그 결과 일부 기술에 실제와 다른 부분이 있어 수정했습니다.

메루카리의 기술블로그

메루카리는 당초, 'Expires 헤더(header)가 과거의 날짜라고 해도 Cache-Control 헤더가 존재하고 있을 경우, Expires 헤더(header)의 정보는 고려되지 않는 사양이 되어 있었다'고 설명하고 있다. 그러나 이 내용이 정확하지 않았다. 정확하게는 Expires 헤더(header)는 Cache-Control 헤더에 max-age(캐시 유효기한을 설정하는 키) 또는 s-maxage(공유 캐시의 유효기한을 설정하는 키)가 없을 때에 기능하고 있었다. 다만 Expires 헤더에 과거의 날짜가

 Copyright © 2017 ESTsecurity Corp. All rights reserved.

지정되어 있었던 경우에는 이 CDN 제공업체에서는 캐시의 유효기한이 0 초로 취급되고 있었다고 한다. 즉 메루카리의 경우에는 '유효기한이 0 초인 캐시'가 존재하고 있었다는 것이 된다.

캐시의 유효기한이 0 초가 되어 있으면, CDN 에서 Web 서버에 대한 리퀘스트 처리를 실시하고 있는 사이에 같은 URL 에 대해 리퀘스트가 발생하면 Web 서버에서의 최초의 응답을 가지고 두 번째 이후의 리퀘스트에 대해서도 같은 응답을 받는 사양이 되어 있었다.

덧붙여 어떤 유저가 Web 버전 메루카리에 접속하여 메루카리의 Web 서버가 응답을 구축하고 있는 도중에 다른 유저가 같은 URL 에 접속한 경우, 어느 유저 정보를 포함한 콘텐츠가 다른 유저에 보이게 되었다고 밝혔다.

[출처] http://itpro.nikkeibp.co.jp/atcl/news/17/062701776/?ST=security&itp_list_theme

ESTsecurity Copyright © 2017 ESTsecurity Corp. All rights reserved.

(주)이스트시큐리티

(우) 06711
서울시 서초구 반포대로 3 이스트빌딩
02.583.4616
www.estsecurity.com