이스트시큐리티

보안 동향 보고서

No.121 2019.10

No.121 2019.10

이스트시큐리티 보안 동향 보고서

CONTENTS

01
악성코드 통계 및 분석

악성코드 동향

알약 악성코드 탐지 통계

랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

1. 악성코드 동향

2019 년 9 월은 8 월에 이어, Sodinokibi 랜섬웨어가 많이 유포되었으나, Sodinokibi 랜섬웨어 외에도 Nemty 랜섬웨어의 유포가 급증했던 달이었습니다.

Nemty 랜섬웨어는 8 월말에 모습을 드러낸 후 9 월 한달동안 유포가 급증하여 9 월 한달간 탐지된 랜섬웨어 중에서 Top3 에 포함될 정도로 활발한 활동을 보였습니다. Nemty 는 비너스락커 조직이 입사지원서를 위장한 메일로 주로 유포를 시도했으며, 특히 9 월은 국내 여러 기업들의 하반기 공개 채용 및 서류접수가 시작된 시즌인만큼 더더욱 유포가 성행한 것으로 추정되고 있습니다.

해외에서는 국내와는 조금 다른 양상을 보였습니다. 물론 Sodinokibi 가 간혹 발견되긴 하지만, 해외는 Exim 익스플로잇을 통해 서버와 웹사이트를 공격하는 Lilocked 랜섬웨어, 외부에 노출된 RDP(원격데스크톱서비스)를 노려서 기업내부환경을 노리는 Tflower 랜섬웨어, 미국에서는 라디오방송사와 병원이 알려지지 않은 랜섬웨어의 공격에 큰 피해를 겪었습니다. 이처럼 해외에서는 특정 랜섬웨어가 주로 공격에 활용된 것이 아닌 다양한 랜섬웨어가 공격에 활용되는 것이 국내와는 조금 다른 모습입니다.

랜섬웨어 외에도, 9 월에는 국내 유명 포털서비스 로그인 페이지를 사칭한 개인정보 탈취 피싱 사이트도 여러 차례 확인되었습니다. 이들은 주로 불특정 다수에게 견적서 혹은 송장 형태의 htm 파일을 첨부하고 검토 후 연락달라는 메시지를 보내 첨부파일을 열어보도록 유도하며, 첨부파일을 열 때, 국내 유명 포털서비스 로그인 페이지와 동일하게 보이는 피싱 페이지로 이동시켜 사용자로 하여금 로그인 정보를 입력하게 유도합니다. 이러한 피싱 캠페인 공격은 꾸준하게 발생하는 공격이지만 악성코드에 의한 공격이라기보다는 사용자의 정보 입력을 통해 피해가 발생하게 되므로 반드시 이러한 류의 공격에 대해 주의를 기울이고, 로그인 페이지에서 로그인 정보를 입력할 경우 반드시 주소창에 자물쇠 아이콘을 클릭하여 사이트 정보나 인증서 상태를 확인해보는 습관을 지니도록 권고 드립니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

감염 악성코드 Top 15 는 사용자 PC 에서 탐지된 악성코드를 기반으로 산출한 통계다.

2019 년 9 월의 감염 악성코드 Top 15 리스트에서는 지난 2019 년 8 월에 각각 1,2 위를 차지했었던 Misc.HackTool.AutoKMS 과 Trojan.Agent.gen 이 9 월에 자리를 바꿨으며, 전반적으로 감염통계 10 위권내의 악성코드들은 대동소이했다.

10 위권 밖에서는 기존에 자주 Top15 리스트에 오르던 BitCoinMiner 와 Neshta 등이 순위에 재진입하였다.

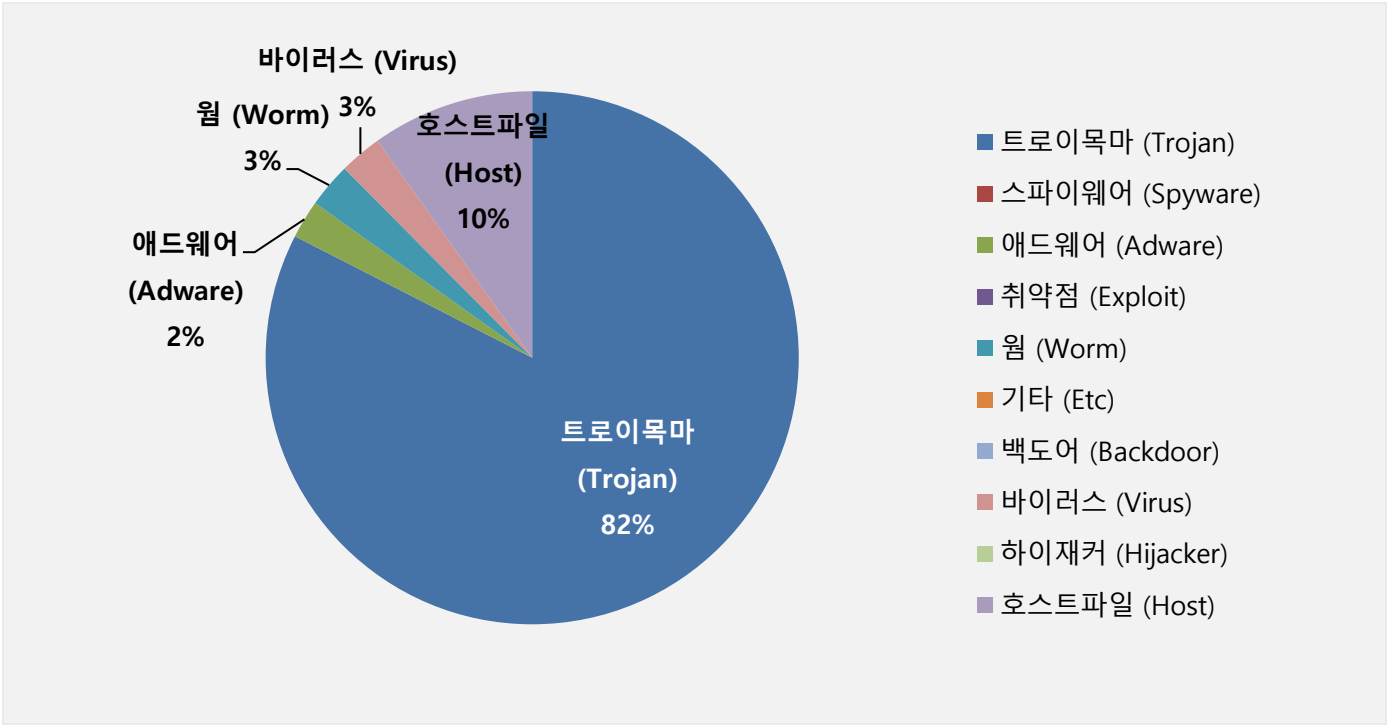
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	↑ 1	Trojan.Agent.gen	Trojan	780,767
2	↓ 1	Misc.HackTool.AutoKMS	Trojan	726,264
3	↑ 1	Trojan.HTML.Ramnit.A	Trojan	560,483
4	↑ 2	Hosts.media.opencandy.com	Host	489,949
5	-	Trojan.ShadowBrokers.A	Trojan	449,233
6	↑ 1	Misc.HackTool.KMSActivator	Trojan	357,699
7	New	Heur.BZC.YAX.Linx.15.029FCD3C	Trojan	300,728
8	↑ 1	Misc.Keygen	Trojan	263,600
9	↑ 4	Misc.Riskware.TunMirror	Trojan	203,093
10	↓ 2	Trojan.LNK.Gen	Trojan	188,628
11	New	Misc.Riskware.BitCoinMiner	Trojan	144,412
12	New	Worm.ACAD.Bursted	Worm	134,083
13	New	Win32.Neshta.A	Virus	128,111
14	-	Gen:Variant.Razy.348484	Trojan	126,294
15	New	Adware.SearchSuite	Adware	115,804

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2019 년 09 월 01 일 ~ 2019 년 09 월 30 일

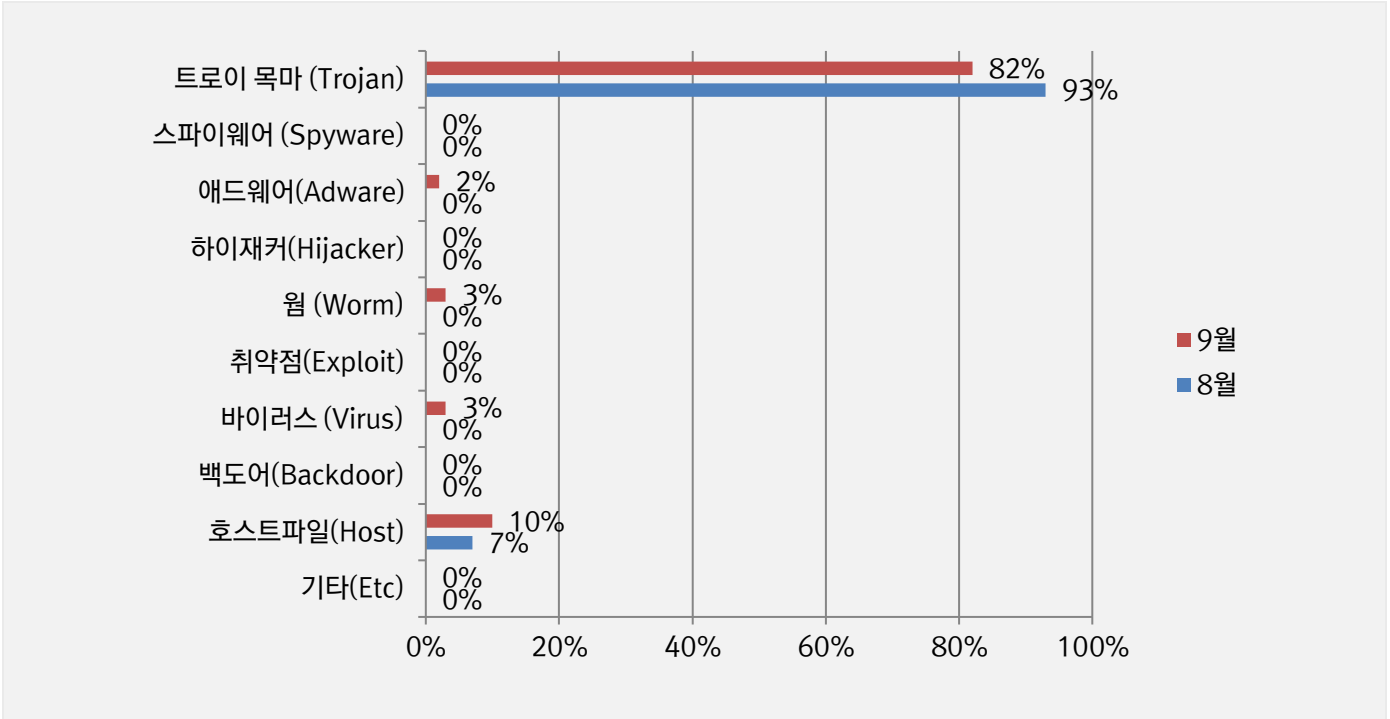
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 82%를 차지했으며 호스트파일(Host) 유형이 10%로 그 뒤를 이었다. 전반적으로 8 월에 비해 전체 감염건수는 5.5% 감소했다.



카테고리별 악성코드 비율 전월 비교

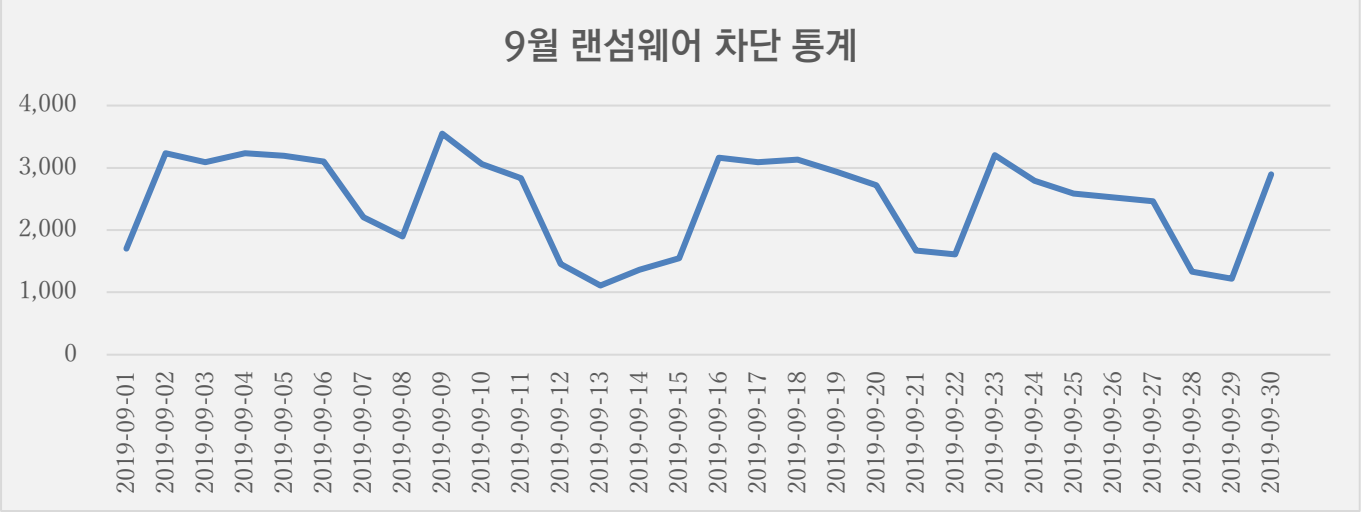
9 월에는 8 월과 비교하여 트로이목마(Trojan) 악성코드 감염 카테고리 비율이 대폭 감소했으며, 호스트파일(Host) 유형 악성코드 비율은 소폭 증가했다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

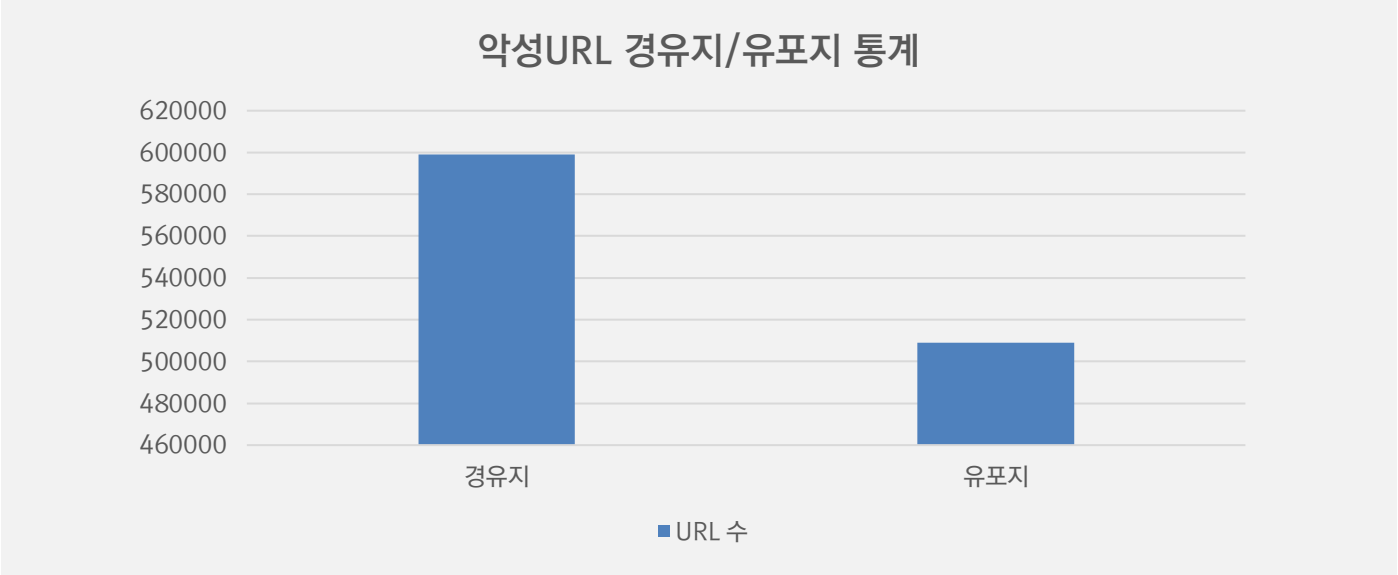
9 월 랜섬웨어 차단 통계

해당 통계는 통합백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간통계로써, DB 에 의한 시그니쳐 탐지횟수는 통계에 포함되지 않는다. 9 월 1 일부터 9 월 30 일까지 총 73,958 건의 랜섬웨어 공격시도가 차단되었다. 8 월에 비해 랜섬웨어 공격건수는 5.8% 가량 감소하였다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 9 월 한달간 총 1,117,976 건의 악성코드 경유지/유포지 URL 이 확인되었다. 이 수치는 8 월 한달간 확인되었던 188,700 건의 악성코드 유포지/경유지 건수에 비해 약 580% 가량 크게 증가한 수치다. 악성코드 경유지/유포지 URL 의 경우 항상 고정적인 URL 만 모니터링하는 것이 아닌, 계속적으로 모니터링 대상을 확대하고 있기 때문에 월별로 증가세와 감소세를 비교하는 부분은 참고로만 봐주시기 바란다.



02

전문가 보안 기고

1. 엔드포인트 위협 대응의 새로운 대안, 알약 EDR

2. 2019 년 3 분기, 알약 랜섬웨어 공격 행위차단 건수: 229,564 건!

1. 엔드포인트 위협 대응의 새로운 대안, 알약 EDR

보안 인식 변화와 함께 등장한 EDR

사이버 보안의 대상에 대한 인식이 변화했습니다. 신, 변종 악성코드, 랜섬웨어와 지능형 지속위협(APT) 공격의 범람과 함께, 공격자의 최종 목표인 엔드포인트의 보안 강화에 대한 요구가 많아졌습니다. 그 과정에서 전통적인 보안 솔루션의 한계를 극복하고 고도화된 엔드포인트 위협을 예측-예방-대응-탐지하는 'EDR(Endpoint Detection and Response)'이라는 개념이 등장했습니다.

EDR, 그러나 왜 아직인가?

하지만 이미 시장에 많은 EDR 제품이 출시되어있음에도 기대했던 만큼 보안 이슈들이 해결되지는 않고 있어, 사용자들은 제품 선택에 애로사항을 겪고 있습니다.
기존 EDR 제품들은 △ 평판 분석의 한계, △ 드라이버 문제, △ 에이전트, 관리콘솔 중복, △ 과도한 관리 리소스 등 크게 4 가지 한계점을 가지고 있기 때문입니다.

1. 평판 분석의 한계

2018 년도 AV-TEST 통계를 살펴보면, 전체 악성코드 중 알려진 위협은 84%, 알려지지 않은 위협은 16%로 나타납니다. 물론 알려지지 않은 위협을 탐지, 차단하는 것도 중요하지만 알려진 위협을 차단하는 것은 기본이 되어야 합니다. 현재 시장에 나와있는 독립형(Standalone) EDR 솔루션은 알려진 위협을 차단할 엔진이 없거나, 안티바이러스 제품을 병행해 사용해야 합니다. 평판 조회 서비스를 별도로 이용하더라도, 실시간 악성코드 샘플이 존재하지 않는 경우가 다반사이며, 탐지 결과 확인을 위해서는 원본 샘플을 등록해 공개적으로 공유해야하는 일이 빈번합니다.

2. 드라이버 문제

커널 레벨이 아닌 유저 레벨만 지원하는 독립형 EDR 제품들은 위협 모니터링과 복구를 위해 별도 드라이버를 설치해야 하기 때문에, 드라이버 충돌 및 중복에 대한 이슈가 계속해서 존재합니다.

3. 에이전트, 관리콘솔의 중복

알려진 위협의 차단에는 안티바이러스 기능이 필수적으로 필요합니다. 하지만 안티바이러스 제품과 완벽히 연동되지 않는 EDR 제품은 사용자 PC 단에 설치되는 에이전트도 2 개, 보안 관리자가 모니터링해야하는 관리콘솔도 2 개가 될 수 밖에 없습니다. 즉 보안 관리자의 리소스 문제가 따라오게 되어 비효율적인 자원 낭비가 발생하게 됩니다.

4. 과도한 관리 리소스

02 전문가 기고

독립형 EDR 의 경우 악성코드의 행위들을 차단하기보다 각각의 행위를 다른 이벤트로 탐지하면서, 모든 이벤트들을 하나씩 검토하고, 하나씩 차단 정책에 반영해야 하는 보안 관리자의 작업을 요구합니다. 게다가 의심행위를 차단하더라도 정확한 위협 판단 없이는 숙주파일을 탐지하지 못해 계속해서 보안 알림이 울려, 부득이하게 수백대의 PC 를 포맷한 사례도 있습니다. 결국 보안 관리자는 오탐/과탐의 문제를 떠안고, 위협 흐름도를 보고 의심되는 행위를 분석해서 대응해야 하는 반복적인 업무를 계속 할 수 밖에 없었습니다.

EDR 의 필수요소 – 위협 인텔리전스와 결합한 알약 EDR

모든 엔드포인트의 실질적인 보안 위협은 엔드포인트의 악성코드로부터 발생하기 때문에 각종 악성코드를 식별하고 분류하는 것이 차세대 엔드포인트 보안의 핵심이다. EDR 에 위협 인텔리전스가 필요한 이유입니다.

기존 EDR	2 세대 EDR
유지 레벨 드라이버	완벽한 커널 레벨 드라이버
평판 분석 의존	자체적인 탐지 엔진, DB
에이전트, 관리콘솔 중복	단일 에이전트., 단일 관리콘솔
과도한 관리 리소스	관리 리소스 최소화
단순한 대응 로직	위험도별 맞춤 대응 로직
대응 속도가 느림	신속하고 즉각적인 대응력

1. 알약 EDR 은 알려진 위협과 알려지지 않은 위협 모두를 탐지, 차단합니다.
자체 탐지 엔진인 '테라 엔진'을 기반으로 구동되기 때문에 과탐/오탐을 최소화하는 정책 운영이 가능하며, 추가적인 평판분석 정보를 제공하여 알려진 위협을 빈틈없이 탐지합니다.

2. 알약 EDR 은 안정적인 커널 레벨 드라이버를 사용합니다.
커널 레벨 기술을 통해 구현된 행위 기반 감시, 랜섬웨어 차단 기능으로 유저 레벨 및 훅 기반의 차단 기술보다 더 강력하고 효율적인 의심 행위 차단이 가능합니다. 또한 자체 행위 정보 수집 기술로 파일, 프로세스, 레지스트리, 네트워크 등의 위협 정보를 안정적으로 수집하여 엔드포인트 가시성을 제공합니다.

3. 알약 EDR 은 통합 에이전트, 통합 관리 콘솔을 지원합니다.
단일 에이전트를 기반으로 '알약', '알약 패치관리(PMS)', '알약 내 PC 지키미' 등 기존 알약 제품군과 통합 관리가 가능하기 때문에, 사용자 PC 의 리소스 최소화뿐만 아니라 보안 관리자의 효율적인 운영이 가능해집니다.

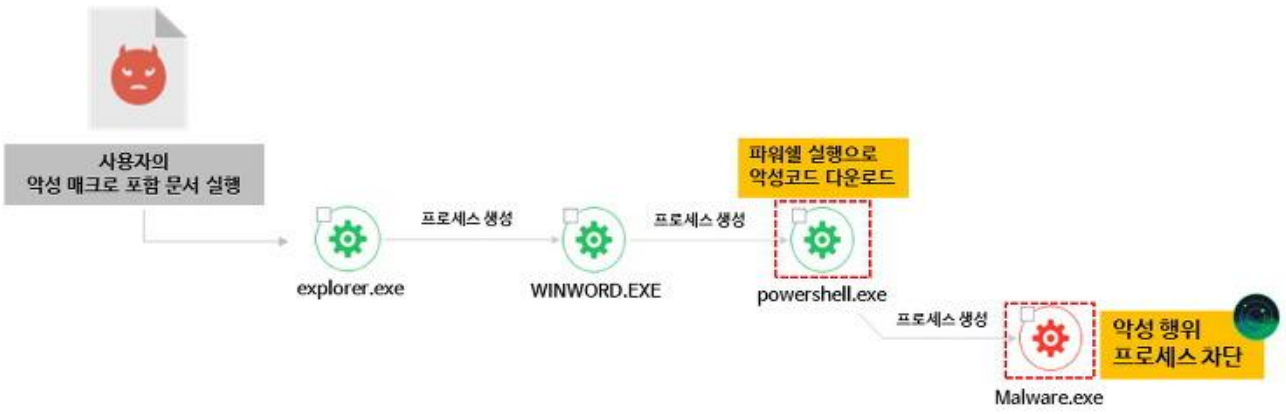
4. 알약 EDR 은 선조치-후보고로 관리 리소스를 최소화합니다.
알약 EDR 은 탐지되는 알려지지 않은 위협의 레벨을 악성-의심-주의로 세분화하여 차단 및 대응하고 있습니다. 주의 레벨의 일반적이지 않은 행위는 정책에 따라 차단 또는 허용하고, 의심 행위는 실행을 지연시킨 후 상세 분석 결과를

통해 판단이 가능하게끔 합니다. 기존 EDR 솔루션과 달리, 알약 EDR 은 확실한 악성 행위에 대해 사전 차단 후 리포트를 제공하여 보다 효율적인 대응이 가능합니다.

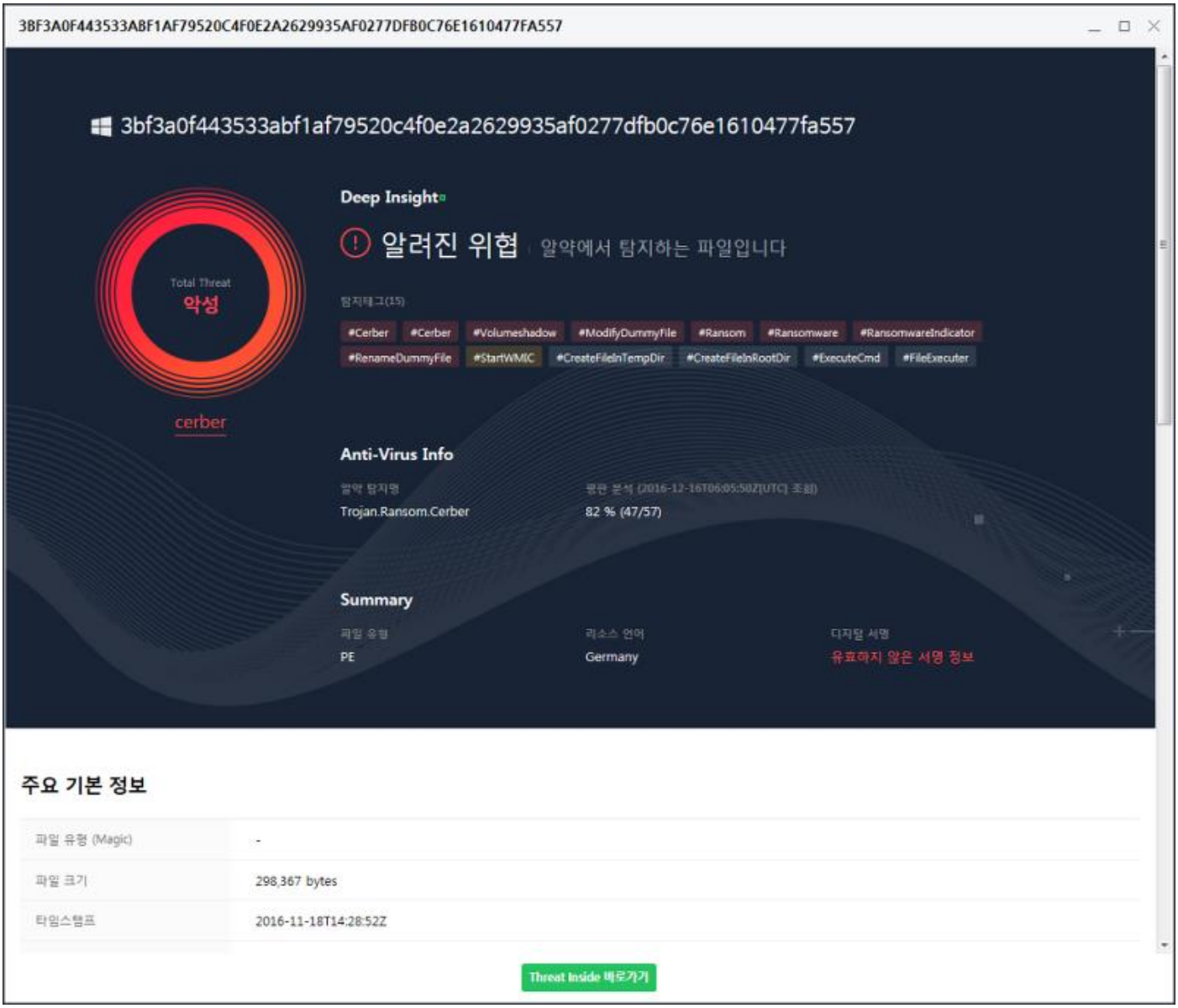
탐지방식	탐지 대상	위험 레벨	행위 / 로그 종류	차단 / 대응 절차
Non-Signature	알려지지 않은 파일	악성	다른 솔루션은 사전 차단하지 못함 확실한 악성 행위 (Exploit, 랜섬웨어 동작 등)	사전 차단
		의심	의심스러운 행위 (MBR변조, 파일 드랍 등)	실행 지연 후, 차단 / 허용 (상세 분석 결과에 따라 적용)
		주의	일반적이지 않은 행위 (호스트 변조, 매체접근, 쉘스크립트 등)	차단 / 허용 (관리자 정책에 따라)

알약 EDR 은 매니지먼트 콘솔, 자사의 인텔리전스 서비스인 '쓰렛인사이드(Threat Inside)'의 분석 체계가 유기적으로 결합되어 있습니다. 사용자 PC 에는 통합 에이전트가 설치되어 필요한 이벤트 로그를 전송하며, 의심 또는 악성 행위가 발생했을 때 해당 파일의 실행을 정책에 따라 지연 또는 차단합니다.

이스트시큐리티 알약 EDR 은 이스트시큐리티가 10 년 이상 엔드포인트 보안 사업을 전개하며 키워온 보안 노하우를 집약시킨 제품으로, 1,600 만 사용자를 확보하고 있는 국민 백신 알약이 탐지한 연간 약 1 억 건 이상의 악성코드와 분기별 130 만 건이상의 랜섬웨어 샘플를 통해 축적해온 악성코드 데이터베이스와 위협 대응 전문 노하우를 기반으로 개발되었습니다. 특히 경보 피로 및 신뢰할 만한 위협 인텔리전스 부족 등 기존 EDR 제품의 한계를 자사 위협 인텔리전스 서비스 '쓰렛인사이드(Threat Inside)'와 완벽히 연동해 해결하고, 기업에 보다 실효적인 보안 대응 가이드를 제시하는데 초점을 맞춘 제품입니다.



[그림 1] 알약 EDR '위협 흐름도' 및 '악성 행위 프로세스 차단'



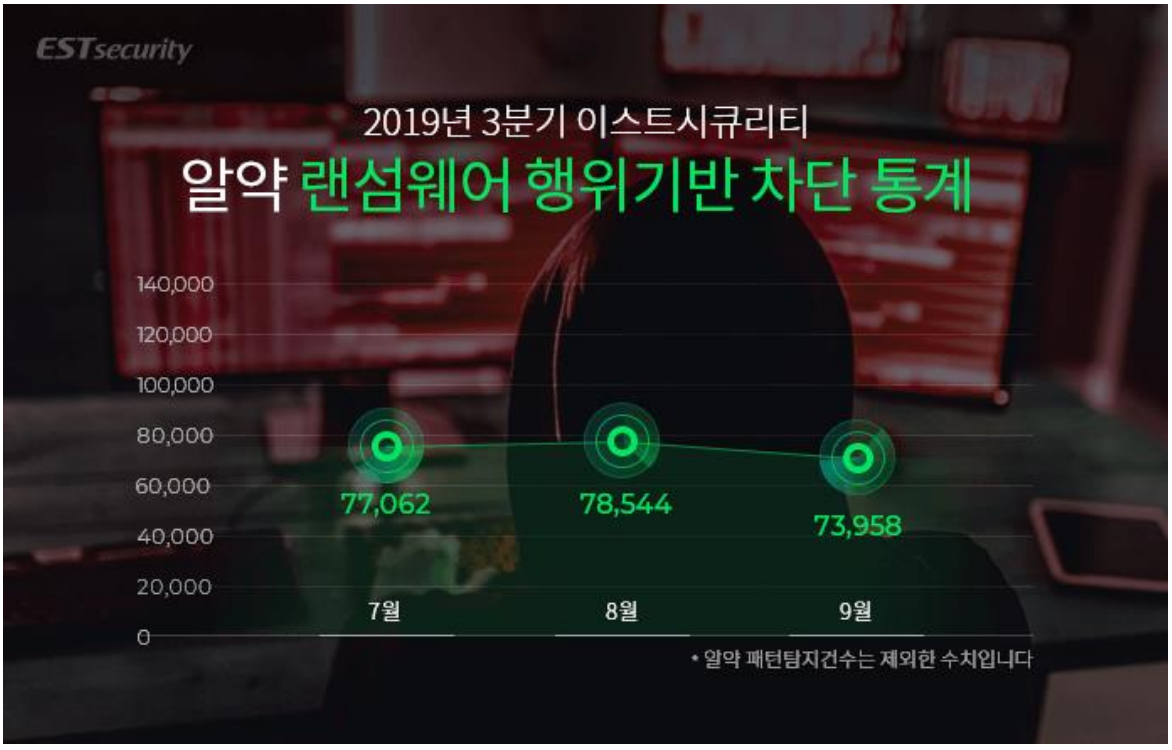
[그림 2] 알약 EDR에 연동된 쓰렛인사이드 위협 식별 결과 화면

2. 2019 년 3 분기, 알약 랜섬웨어 공격 행위차단 건수: 229,564 건!

2019 년 3 분기, 알약을 통해 총 22 만 9564 건의 랜섬웨어 공격이 차단된 것으로 확인되었습니다.

이번 통계는 일반 사용자를 대상으로 제공하는 공개용 알약의 '랜섬웨어 행위기반 차단 기능'을 통해 차단된 공격만을 집계한 결과로, 패턴 기반 공격까지 포함하면 전체 공격은 더욱 많은 것으로 예상됩니다.

통계에 따르면 2019 년 3 분기에 알약을 통해 차단된 랜섬웨어 공격은 총 22 만 9564 건으로, 이를 일간 기준으로 환산하면 일평균 약 2,496 건의 랜섬웨어 공격이 차단된 것으로 볼 수 있습니다.



[그림 1] '알약 랜섬웨어 행위기반 차단 기능'을 통해 차단된 2019 년 3 분기 랜섬웨어 공격 건수

시큐리티대응센터(이하 ESRC)는 이번 3 분기 주요 랜섬웨어 공격동향으로 3 가지를 꼽았습니다.

먼저 2019 년 2 분기에 첫 등장했던 소디노키비(Sodinokibi) 랜섬웨어가 현재 국내에서 가장 큰 랜섬웨어 위협으로 자리 잡으며, 지난 2 분기부터 운영 중단돼 유포가 급감한 갠드크랩(GandCrab) 랜섬웨어의 빈자리를 차지했습니다.

이어 지난 8 월 말부터 새롭게 등장한 넴티(Nemty) 랜섬웨어 유포가 9 월 들어 급격히 증가했으며, 이에 반해 2017 년 5 월 등장해 꾸준히 상위를 유지하던 워너크라이(WannaCry) 랜섬웨어 감염은 3 분기에 진입하며 점차 감소한 것으로 나타났습니다.

02 전문가 기고

실제로 ESRC 의 모니터링 분석 결과, 2019 년 3 분기 알약의 랜섬웨어 공격 차단 통계는 지난 2 분기와 비교해 약 7.33%가량 감소한 것으로 나타났습니다. 이는 소디노키비 랜섬웨어의 유포는 증가했지만, 네트워크를 타고 취약한 시스템을 감염시키는 워너크라이 랜섬웨어의 특성상 오랜 시간 일정 수치 이상의 감염 건수를 유지하다 최근 그 수치가 감소한 영향인 것으로 파악됩니다.

ESRC 센터장 문종현 이사는 “소디노키비 랜섬웨어를 유포하는 공격 조직이 기존에는 주로 갠드크랩 랜섬웨어를 활용했던 것과 달리, 최근 소디노키비와 함께 넴티나 스캐럽(Scarab) 등 다양한 랜섬웨어를 공격에 활용하고 있는 정황이 발견되고 있다”라며, “공격 조직의 활동을 지속적으로 모니터링 및 추적할 계획”이라고 덧붙였습니다.

이 밖에 ESRC 에서 밝힌 2019 년 3 분기에 새로 발견되었거나 주목할 만한 랜섬웨어는 다음과 같습니다.

랜섬웨어명	특징
Nemty	파일 암호화 시, nemty 문자열이 포함된 확장자로 변경하는 랜섬웨어. 감염된 PC 가 부여받은 사용자 ID 파일에 따라 복호화 비용과 월렛 주소가 개별적으로 할당되며, 동일 PC 에서 감염 행위가 발생할 때 마다 ID 파일값이 변경됨. 감염된 PC 의 IP, 국가정보, PC 명, 사용자명, OS 정보, PC ID 정보를 수집하여 공격자에게 전송하며, 데이터 복구를 위한 쉐도우 복사본을 삭제함.
GermanWiper	독일어 사용 지역에 주로 확산되었던 악성코드로 악성스팸 메일을 통해 주로 유포됨. 랜섬웨어의 형태를 띠고 있지만, 데이터를 암호화하는 대신 '0'으로 덮어쓰기 하는 와이퍼 악성코드 형태로 확인됨. 단순히 데이터를 삭제하는 형태로 데이터를 복구할 수 없는 악성코드임에도 불구하고, 감염 피해자들에게 암호화된 파일을 복호화하는 비용으로 비트코인을 요구하는 랜섬노트 메시지를 보여줌.
Tflower	외부에 노출된 원격 데스크톱 서비스를 통해 기업 네트워크에 진입한 공격자가 Tflower 랜섬웨어를 설치. 이때 Tflower 가 로컬머신을 감염시키고 특정 툴을 통해 기업 네트워크 탐색을 시도함. 워드프레스로 구축된 사이트를 C&C 서버로 사용하고 있었으며, 감염 시 복구를 막기 위해 쉐도우 볼륨 복사본 삭제 및 윈도 10 복구 환경 비활성화 명령을 실행함. 파일 암호화할 때, 확장자에 무엇인가를 추가하지는 않지만 *tflower 표시를 암호화된 파일의 맨 앞에 붙임.
Lilocked	리눅스 기반 서버를 노리는 랜섬웨어로 서버 데이터를 암호화하고 ".lilocked" 문자열을 확장자에 추가함. 랜섬노트에는 피해자가 랜섬머니를 지불하기 위해서는 공격자의 Tor 지불 사이트를 방문해야 한다고 요구함. Exim Exploit 을 통해 서버 접근 권한을 획득한다고 알려져 있으나 정확한 방식은 아직 밝혀지지 않았음.
Ech0raix	리눅스 기반의 NAS 장비를 노리는 랜섬웨어. SSH 크리덴셜을 이용한 브루트포싱 공격 또는 알려진 취약점을 이용하여 보안이 취약한 QNAP NAS 장비를 노림. 다만 NAS 장비가 벨라루스, 우크라이나, 러시아에 위치할 경우, 아무런 악성 행위를 하지 않음.

02 전문가 기고

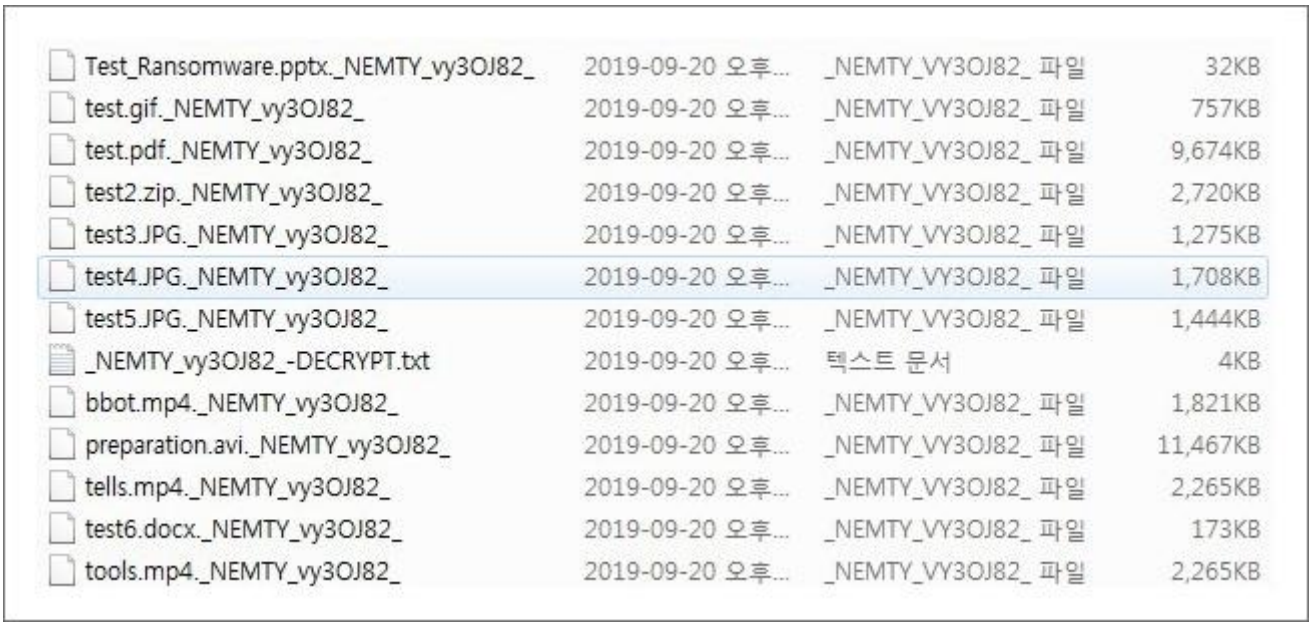
ESRC 센터장 문종현 이사는 “기존 기업환경을 노리는 클롭(Clop) 랜섬웨어 외에도, 외부에 노출된 기업의 원격 데스크톱 서비스를 노리는 티플라워(Tflower) 랜섬웨어, 리눅스 기반 서버를 노리는 리락드(Lilocked) 랜섬웨어 등 다양한 랜섬웨어들이 지속해서 기업 내부 네트워크와 시스템을 노리고 있다”라며, “사용 중인 시스템의 운영체제(OS)와 소프트웨어의 취약점을 점검 및 보완하고, 내부 임직원이 출처가 불분명한 이메일을 열람하지 않도록 하는 보안의식 교육도 강화해야 한다”라고 당부했습니다.

한편, 이스트시큐리티는 랜섬웨어 감염으로 인한 국내 사용자 피해를 미연에 방지하기 위해, 한국인터넷진흥원(KISA)과의 긴밀한 협력을 통해 랜섬웨어 정보 수집과 유기적인 대응 협력을 진행하고 있습니다.

03
악성코드 분석 보고

[Trojan.Ransom.Nemty] 악성코드 분석 보고서

최근 갠드크랩 4.1 버전에서 사용된 이미지를 동일하게 사용한 랜섬웨어가 발견되었다. 이 이미지는 다음과 같이 러시아 대통령과 러시아 문구가 삽입되어 있다. Nemty 랜섬웨어는 주로 입사 지원서를 위장한 메일로 유포되며, 파일명에 긴 공백을 넣어 PDF 파일인 것처럼 위장해 사용자를 속이는 것이 특징이다.



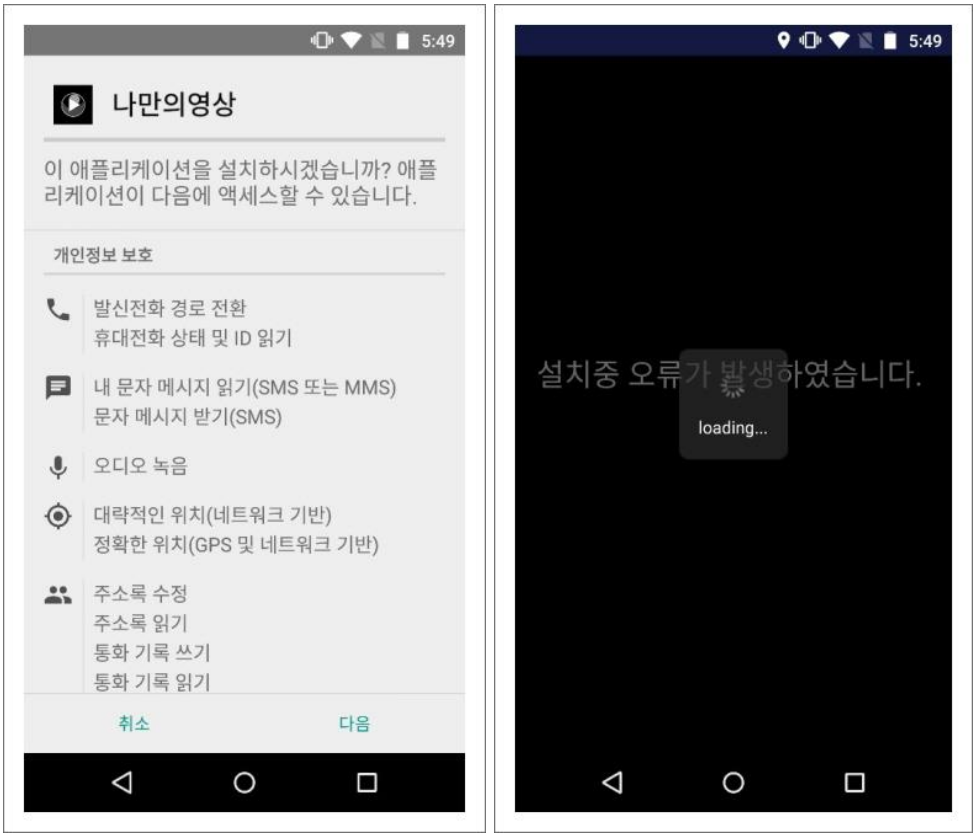
[그림] 암호화 완료 화면

현재 알약에서는 해당 악성 코드를 'Trojan.Ransom.Nemty' 탐지 명으로 진단하고 있으며, 관련 상세 분석보고서는 Threat Inside 웹서비스 구독을 통해 확인이 가능하다.

[Trojan.Android.InfoStealer] 악성코드 분석 보고서

한국에 몸캠 피싱앱이 등장하기 시작한 2013 년부터 최근까지 몸캠 피싱앱은 은밀하고 꾸준하게 유포되고 있다. 몸캠 피싱은 스마트폰 채팅 어플(랜덤채팅)을 통해 피해자를 찾으며 음란 화상 채팅을 유도하여 피해자의 음란 행위를 녹화한다. 그리고 피해자의 스마트폰에 악성앱 설치를 유도하여 지인의 연락처를 탈취한 후 음란행위 영상을 지인에게 유포하겠다는 협박을 통해 금전을 갈취한다. 이런 공격 과정은 체계적인 프로세스를 따르는 것으로 파악 되며 공격을 원할 하게 수행할 수 있도록 조직을 체계적으로 구성하여 역할에 따라 공격을 수행하고 있다.

공격자들이 조직까지 구성하며 꾸준하게 몸캠 피싱을 시도하는 이유는 결국 돈이 되기 때문일 것이다. 이렇게 조직적이며 치밀하게 이뤄지는 몸캠 피싱의 공격 대상은 누구라도 될 수 있으며 피해자는 금전적인 손실과 함께 사회적인 명성에도 피해를 입기에 여타의 다른 공격들 보다 문제의 심각성이 높다고 할 수 있다.



[그림 1] 악성앱 설치 및 실행 화면

[그림 2] 탈취된 피해자 SMS 내역

현재 알약 M 에서는 해당 악성 앱을 'Trojan.Android.InfoStealer' 탐지 명으로 진단하고 있으며, 관련 상세 분석보고서는 Threat Inside 웹서비스 구독을 통해 확인이 가능하다.

04
글로벌 보안 동향

iOS 와 안드로이드 앱스토어에서 도박 앱 발견 돼

Fake Apps Sneak Gambling Into iOS and Android App Stores

도박 앱들이 정책을 준수한 앱으로 위장하여 구글 플레이와 앱스토어의 심사를 통과했다. 검사를 우회한 후, 사용자들은 도박 기능을 사용할 수 있게 된다.
이 앱들은 지난 8 월 안드로이드 공식 스토어에 등록 되었다. iOS 에서는 앱들 중 일부가 10 만 건 이상 리뷰가 등록 되어 더욱 오래 살아남을 수 있었다.

심사 시스템 우회

앱 스토어는 실제 돈을 걸고 하는 게임 앱 (복권, 게임, 자선 단체, 디지털 상점)에 대한 제한을 더욱 강화했으며, 9 월 3 일을 시작으로 애플의 심사를 위해 해당 되는 모든 앱들은 이 기능에 대한 코드를 바이너리에 포함 시켜야 한다.
구글 또한 도박 앱이 합법적인 국가(영국, 프랑스, 아일랜드)의 안드로이드 스토어에서만 도박 앱을 허용한다.
하지만 이러한 제한에도 불구하고, 일부 개발자들은 이 두 스토어의 정책을 위반하는 컨텐츠를 포함하는 앱을 게시하는데 성공했다.
이들은 날씨 추적, 엔터테인먼트와 같은 스토어 요구사항을 준수하는 기능을 포함한 앱을 만들었다. 하지만 이는 불법 컨텐츠를 끄고 켤 수 있는 API 스위치 기능을 포함하고 있었다.
허가 된 컨텐츠는 앱이 사용자에게 노출 될 수 있을 때 까지만 유지 된다. 스토어에 등록 되면, 이 앱들은 웹뷰(WebView)에 '진짜' 컨텐츠를 로드한다. 이 진짜 컨텐츠는 웹뷰의 특정 URL 로부터 제공 받는다.
"이 앱은 특정 주소에 해당 앱 ID 를 포함한 쿼리를 보낼 것이다. 이에 대한 응답은 Base64 로 암호화 된다."
이 때 ID 가 유효할 경우에만 불법 컨텐츠가 로드 될 것이다. 유효하지 않을 경우 앱은 iOS 와 안드로이드 환경 모두에서 스토어가 승인한 기능만을 계속해서 제공한다.
스토어 리뷰 프로세스를 우회하는 작업은 여러 단계로 이루어진다. 먼저 초기 리뷰를 우회하기 위해 일반 앱을 등록하는 것으로 시작 된다. 스토어에 등록 되면, 개발자는 API 를 끄고 웹뷰 기능을 업데이트한다.
이로써 새로운 버전이 앱 스토어에 등록 되었을 때 이루어지는 리뷰를 통과할 수 있다. 그 후 개발자는 사용자가 도박 컨텐르를 볼 수 있도록 API 를 켤 수 있다.
문제 앱들 중 일부는 웹뷰 기능이 업데이트 되기 전 2 년 동안이나 사용이 가능했다.
연구원들은 이 앱들에서 웹뷰를 통해 도박 사이트를 로드하는 것 이외에 아직까지 어떠한 악성 기능도 발견할 수 없었다.
트렌드 마이크로는 이 앱의 개발자들이 앱의 순위를 높이기 위해 앱을 적극적으로 홍보했을 것이라 추측했다.
연구원들은 중국 마켓의 탑 100 목록에서 이 가짜 앱들을 찾아볼 수 있었다.
연구원들은 특정 키워드를 사용해 중국, 미국, 일본의 iOS 마켓에 위장한 앱들 수백 개를 발견했다. 도박이 불법인 중국에서만 대부분의 앱이(500 건 이상) 발견 되었다. 미국 마켓에서는 200 건이 조금 넘는 앱이 발견 되었다.
구글과 애플 모두 이 앱에 대한 신고를 받아 공식 스토어에서 제거한 상태이다.

[출처] https://www.bleepingcomputer.com/news/security/fake-apps-sneak-gambling-into-ios-and-android-app-stores/

https://blog.trendmicro.com/trendlabs-security-intelligence/gambling-apps-sneak-top-100-hundreds-fake-apps-spread-app-store-google-play/

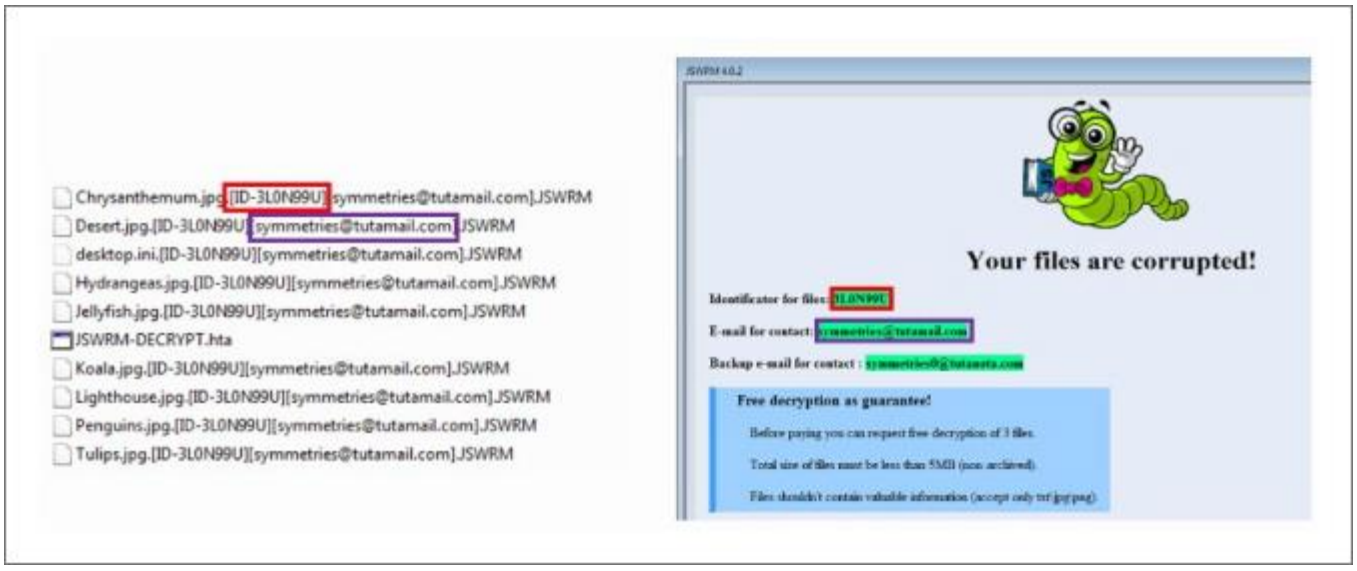
악명높은 JSWorm 랜섬웨어 4 번째 버전 발견 돼

JSWorm: The 4th Version of the Infamous Ransomware

악명 높은 JSWorm 랜섬웨어가 버전 4 로 업그레이드 되었다.
이름은 자바스크립트와 웜을 연상 시키지만, 이 악성 코드는 이 두 가지와는 관련이 없다.

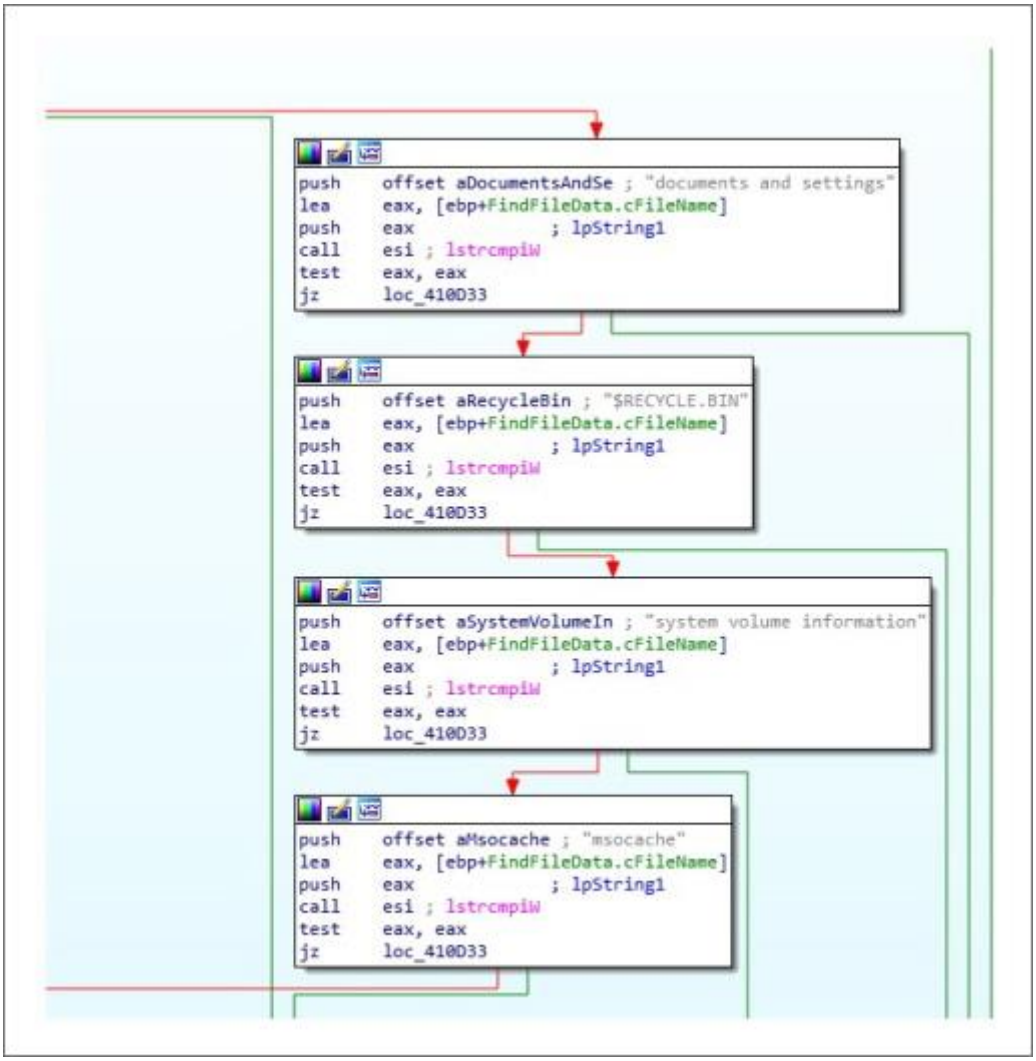
기술적 분석

JSWorm 은 모든 사용자 파일을 암호화 후 새로운 확장자를 붙인다. 다른 랜섬웨어들과 달리, 이 확장자는 많은 정보를 포함하고 있다. 파일이 암호화 되면 "파일명.[원래 확장자].[감염 ID][공격자 이메일].JSWRM"과 같은 형식으로 이름이 변경 된다.



[감염 ID 와 Email 연락처]

랜섬노트에는 블랙리스트에 추가 될 경우 사용할 수 있는 백업 이메일인 symmetries0@tutanota.com 또한 포함 되어 있다. 암호화 단계에서 이 랜섬웨어는 방문하는 모든 폴더에 HTML 어플리케이션인 "JSWRM-DECRYPT.hta"를 생성한다. 해당 HTA 파일은 위 그림 1 에서 확인할 수 있는 랜섬 창이다.
이 랜섬웨어는 시스템 기능은 정상 작동하도록 하기 위해 암호화 단계에서 Windows, Perflogs 와 같은 시스템 디렉토리 및 문서 및 설정, $RECYCLE.BIN, 시스템 볼륨 정보, MSOCache 와 같은 접점을 제외한다.



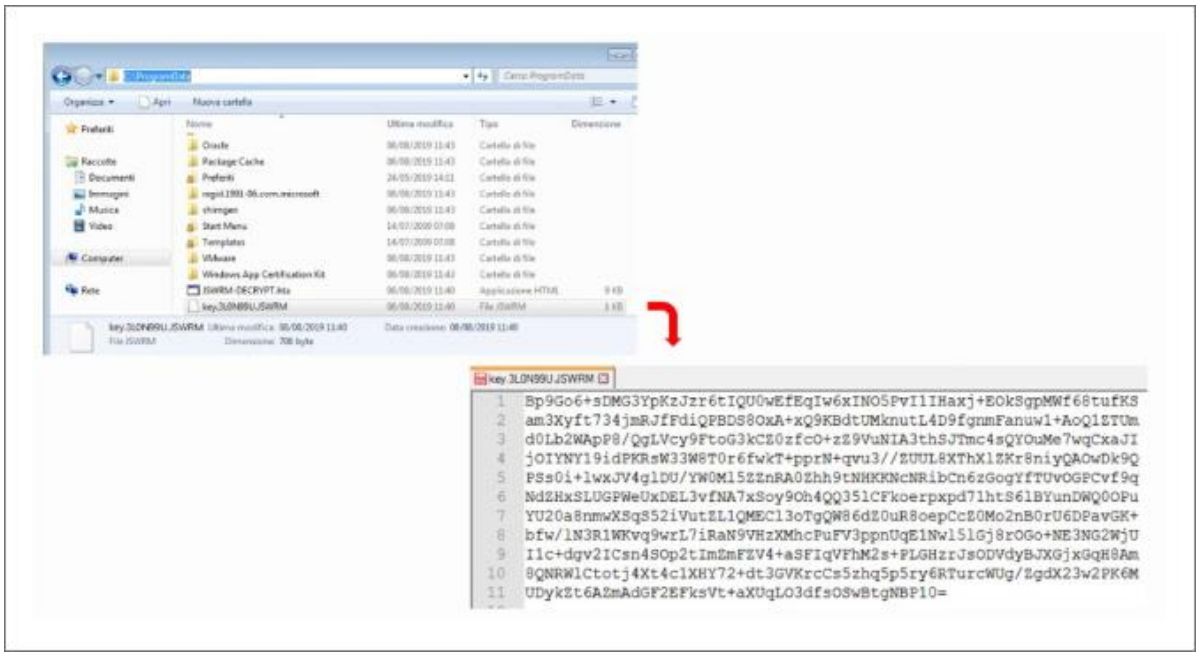
[제외된 경로들]

다른 랜섬웨어 대부분과는 다르게, JSWorm 은 암호화 할 파일 확장자 목록을 포함하지 않고 제외할 확장자 세트만을 포함한다. 이 악성코드는 리스트에 없는 확장자를 사용하는 모든 파일을 암호화 한다.

1025	11:00:01.360 AM	1	kernel32.dll	wcsrchr ("\.exe", '\')
1026	11:00:01.360 AM	1	kernel32.dll	wcsrchr ("\.exe", '\')
1027	11:00:01.360 AM	1	kernel32.dll	wcsrchr ("\.ade", '\')
1028	11:00:01.360 AM	1	kernel32.dll	wcsrchr ("\.ade", '\')
1029	11:00:01.360 AM	1	kernel32.dll	wcsrchr ("\.adp", '\')
1030	11:00:01.360 AM	1	kernel32.dll	wcsrchr ("\.adp", '\')
1031	11:00:01.360 AM	1	kernel32.dll	wcsrchr ("\.app", '\')
1032	11:00:01.360 AM	1	kernel32.dll	wcsrchr ("\.asp", '\')
1033	11:00:01.360 AM	1	kernel32.dll	wcsrchr ("\.asp", '\')
1034	11:00:01.360 AM	1	kernel32.dll	wcsrchr ("\.bas", '\')
1035	11:00:01.360 AM	1	kernel32.dll	wcsrchr ("\.bas", '\')
1036	11:00:01.360 AM	1	kernel32.dll	wcsrchr ("\.bat", '\')
1037	11:00:01.360 AM	1	kernel32.dll	wcsrchr ("\.bat", '\')
1038	11:00:01.360 AM	1	kernel32.dll	wcsrchr ("\.cer", '\')
1039	11:00:01.360 AM	1	kernel32.dll	wcsrchr ("\.cer", '\')
1040	11:00:01.360 AM	1	kernel32.dll	wcsrchr ("\.chm", '\')
1041	11:00:01.360 AM	1	kernel32.dll	wcsrchr ("\.chm", '\')
1042	11:00:01.360 AM	1	kernel32.dll	wcsrchr ("\.cmd", '\')
1043	11:00:01.360 AM	1	kernel32.dll	wcsrchr ("\.cmd", '\')
1044	11:00:01.360 AM	1	kernel32.dll	wcsrchr ("\.com", '\')
1045	11:00:01.360 AM	1	kernel32.dll	wcsrchr ("\.com", '\')
1046	11:00:01.360 AM	1	kernel32.dll	wcsrchr ("\.cpl", '\')
1047	11:00:01.360 AM	1	kernel32.dll	wcsrchr ("\.cpl", '\')
1048	11:00:01.360 AM	1	kernel32.dll	wcsrchr ("\.crt", '\')
1049	11:00:01.360 AM	1	kernel32.dll	wcsrchr ("\.crt", '\')
1050	11:00:01.360 AM	1	kernel32.dll	wcsrchr ("\.csh", '\')

[암호화 제외된 확장자들]

암호화 단계에서, JSWorm 은 “C:\ProgramData”에 “key.Infection_ID.JSWRM”라는 이름의 의심스러운 파일을 생성한다. 이는 파일을 암호화 하는데 사용 되는 AES 키를 포함하고 있다. 안타깝게도, 키는 저장 되기 전 추가적인 RSA 암호화 과정을 거친다. 아래 그림은 암호화 된 키의 한 예이다.



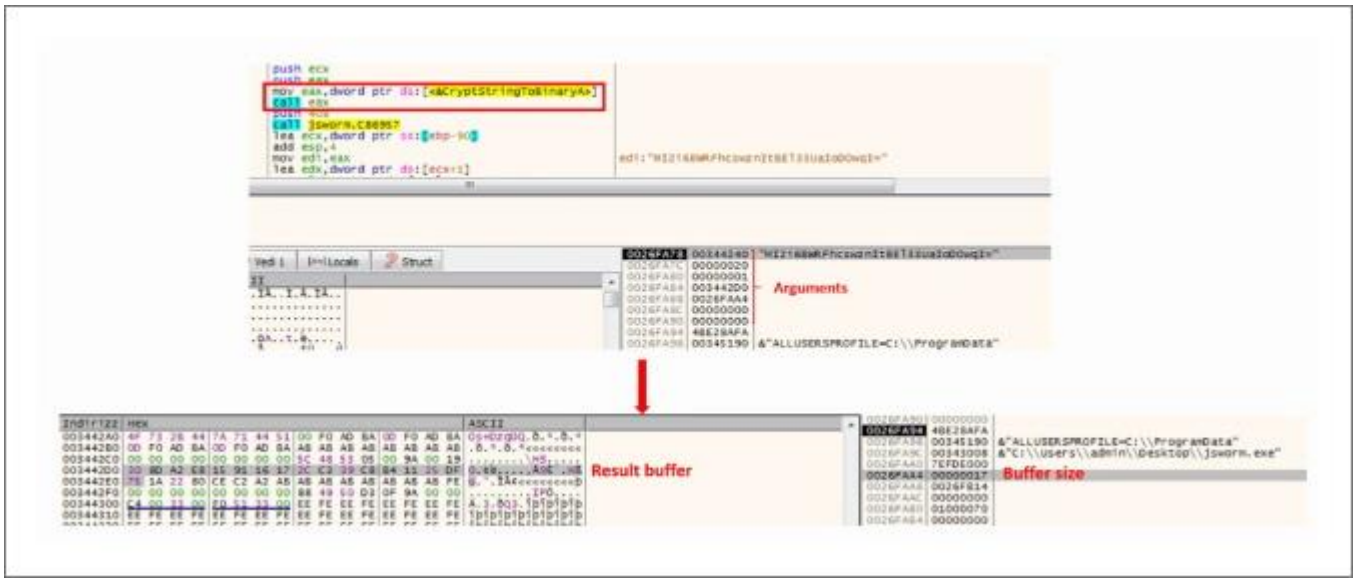
[“C:\ProgramData”내 “Key” 파일 내용]

또한 이 랜섬웨어는 암호화 작업이 미칠 수 있는 영향을 극대화 하기 위해 아래와 같은 작업을 실행합니다:

- 윈도우가 자동으로 생성한 섀도우 복사본 및 기타 시스템 복원 포인트 삭제
- SQL 서버 등 일반적인 프로그램이 사용 중인 파일을 암호화 하기 위해 관련 된 일부 프로세스 종료시킴
- 시스템 재부팅 후에 랜섬노트 창을 표시하기 위해 자동 실행 경로에 레지스트리 키 추가

암호화 체계

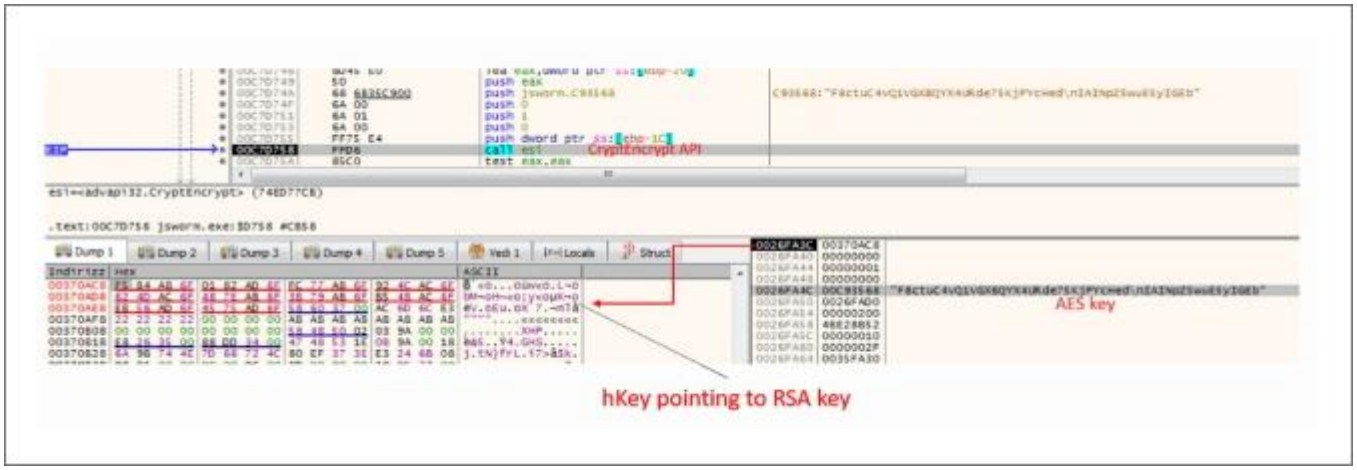
악성코드가 암호화 하는 AES 키는 내장 된 “MI2i6BWRFhcswznItBEl33UaloDOwqI=” base64 시드를 기반으로 생성 된다. 이는 저 수준 조작을 진행하기 전 CryptStringToBinaryA API 를 통해 바이트 배열로 변환된다.



[AES 키를 생성하는데 사용된 내장된 초기 문자열]

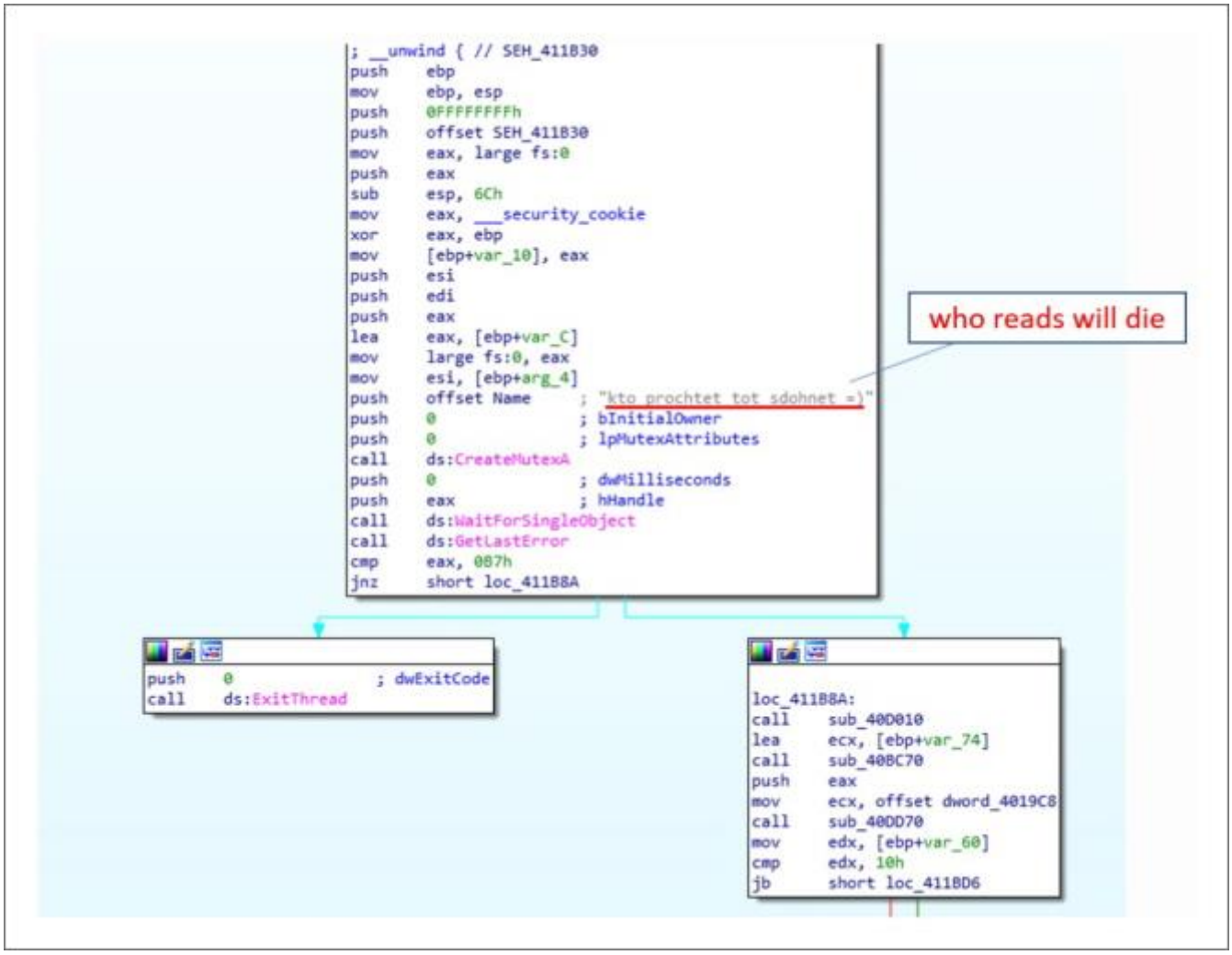
이 문자열은 랜덤한 문자열과 조합 되어 각 감염마다 다른 파생 AES 키를 만들어냅니다. 악성코드 제작자조차도 파일을 해독할 수 있는 최종 AES 키를 알지 못하기 때문에, 파일 복구를 요청하고자 하는 사용자는 “C:\ProgramData”에 저장된 키 파일을 보내야한다. 공격자는 파일을 받은 후 그가 가진 개인 RSA 키로 내용을 해독 후 사용자 파일을 해독하는데 사용할 AES 키를 추출해야 한다.

마지막 단계는 암호화 루틴으로, 아래 그림에서 볼 수 있듯 “CryptEncrypt” 함수를 사용한다.



[CryptEncrypt 함수용 파라미터]

이 악성코드의 새로운 뮤텍스를 인스턴스하는 부분에는 “kto prochtet tot sdohnet =)”라는 러시아 문장이 포함되어 있었다. 이는 “읽는 사람은 죽는다 =)”로 해석 된다.



[뮤텍스 생성]

결론

위에서 분석 된 이 랜섬웨어는 대부분의 랜섬웨어와 동일하게 암호화 체계, 섀도우 복사본 삭제 기능, 지속성 등을 가지고 있다. 이 랜섬웨어는 암호화 체계로 CryptStringToBinaryA API 를 통해 바이트 문자열로 변환 될 내장 된 Base64 시드를 사용하여 생성 되는 AES 키를 사용한다. 랜섬웨어에서 안정성과 개발 시간 단축을 위해 암호화 작업에 이 라이브러리(CryptoAPI)를 사용하는 것은 매우 일반적이다.

또 다른 흥미로운 부분은 러시아어로 “kto prochtet tot sdohnet =)”라는 문자열이 포함 된 뮤텍스가 존재한다는 것이다. 이로써 악성코드의 제작자가 러시아어를 사용한다고 추측해볼 수 있다. 물론 잘못 된 단서일 수 있지만, 러시아 언더그라운드는 이러한 사이버 범죄 활동에 자주 연루되어 왔다.

[출처] https://blog.yoroi.company/research/jsworm-the-4th-version-of-the-infamous-ransomware/

은밀히 데이터를 추출하기 위해 윈도우 BITS 서비스를 사용하는 악성 코드 발견

New Malware Uses Windows BITS Service to Stealthy Exfiltrate Data

사이버 보안 연구원들이 정부 지원을 받는 사이버 간첩 그룹인 Stealth Falcon 과 관련 된 새로운 컴퓨터 바이러스를 발견했다. 이 악성코드는 훔친 데이터를 공격자가 제어하는 서버로 은밀히 추출해 내기 위해 마이크로소프트 윈도우 IOS 의 내장 컴포넌트를 악용한다.

2012 년부터 활동해온 Stealth Falcon 은 주로 중동의 언론인, 활동가, 반체제 운동가들을 노려 스파이웨어를 설치하는 것으로 알려진 수준 높은 해킹 그룹이다.

Win32/StealthFalcon 이라 명명 된 이 악성코드는 원격 C&C 서버와 통신하고 BITS(Windows Background Intelligent Transfer Service)를 통해 수집 된 데이터를 보낸다.

BITS 는 사용하지 않는 네트워크 대역폭을 사용하여 네트워크 활동에 영향을 주지 않으면서 포그라운드 또는 백그라운드에서 기기간에 파일을 비동기식으로 우선순위화 하여 제한적으로 전송하는 윈도우의 통신 프로토콜이다. BITS 는 소프트웨어 업데이터에서 흔히 사용 된다. 윈도우 10, 메신저 및 백그라운드에서 동작하도록 설계 된 기타 어플리케이션의 업데이트를 설치하기 위해 마이크로소프트 서버 또는 피어로부터 파일을 다운로드 할 때도 사용 된다.

사이버 보안 회사인 ESET 의 보안 연구원들에 따르면, BITS 태스크는 호스트 기반 방화벽에서 허용 될 가능성이 높으며 기능을 통해 자동으로 데이터 전송 속도를 조정하기 때문에 악성 코드가 위험 신호를 발생시키지 않은 채 은밀하게 백그라운드에서 실행될 수 있게 된다.

“API 기능을 통한 기존 통신과 비교했을 때, BITS 메커니즘은 COM 인터페이스를 통해 노출 되기 때문에 보안 제품이 탐지하기가 어려워진다.”

“네트워크 정전, 사용자 로그아웃, 시스템 재부팅 등의 이유로 전송이 중단 된 후에도 자동으로 재개된다.”

또한 이 악성코드는 수집한 데이터를 평문 상태로 가져가는 대신 암호화 된 복사본을 생성하고 BITS 프로토콜을 통해 해당 복사본을 C&C 서버로 업로드한다.

훔친 데이터를 성공적으로 이동시키면, 악성코드는 포렌식 분석 및 삭제 된 데이터 복구를 막기 위해 랜덤 데이터로 덮어쓰기하여 모든 로그 및 수집한 파일을 삭제한다.

보고서에 설명 된 대로, Win32/StealthFalcon 백도어는 해킹 된 시스템에서 데이터를 훔치고 공격자가 C&C 서버를 통해 명령을 보내 더 많은 악성 툴을 설치하고 해당 구성을 업데이트할 수 있도록 설계 되었다.

“Win32/StealthFalcon 백도어는 2015 년 생성 된 것으로 보이며, 공격자가 해킹 된 컴퓨터를 원격으로 제어할 수 있도록 한다. UAE, 사우디아라비아, 태국, 네덜란드에서 적은 수의 타깃이 발견 되었다. 후자의 경우 중동 국가의 외교 공관을 노린 것이었다.”

연구원들은 새로이 발견 된 이 악성코드는 C&C 서버와 코드 베이스를 Stealth Falcon 그룹의 PowerShell 기반 백도어와 공유하고 있다고 밝혔다.

[출처] https://thehackernews.com/2019/09/stealthfalcon-virus-windows-bits.html

https://www.welivesecurity.com/2019/09/09/backdoor-stealth-falcon-group/

(주)이스트시큐리티

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