이스트시큐리티

보안 동향 보고서

No.138 2021.03

No.137 2021.03

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 06-12

발주서 파일로 위장한 "NAVER WORKS" 피싱메일 주의!

사생활 녹화 영상으로 협박하는 hoax 메일 주의!

03 악성코드 분석 보고 13-15

04 글로벌 보안 동향 16-22

01
악성코드 통계 및 분석

악성코드 동향

알약 악성코드 탐지 통계

랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

1. 악성코드 동향

2021 년 2 월에도 신규 악성코드 및 랜섬웨어의 발견부터 탈륨(Thallium) 그룹의 지속적인 APT 공격까지 다양한 보안 위협이 발견되었습니다.

코로나 19 로 인한 정부 긴급 재난 지원금 등 국가 지원 사업이 꾸준히 펼쳐지는 가운데 탈륨 조직의 수행으로 추정되는 코로나 19 관련 소상공인 지원 종합 안내로 위장한 HWP 공격이 발견되었습니다. 이번 공격은 지난 1 월 발견됐던 2021 코로나 19 대응 기부증서 사칭 스피어피싱 공격의 연장선으로 볼 수 있습니다. HWP 문서 파일의 정상 공지 화면으로 위장된 악성 HWP 문서가 실행되면 마치 문서 내용이 올바르게 표시되지 않는 것처럼 OLE 이미지 파일로 만든 가짜 메시지 창을 보여주며 사용자가 OLE 공격에 노출되도록 유도합니다. 탈륨 그룹의 공격은 갈수록 치밀해지고 정교해지고 있어 사용자의 각별한 주의가 요구됩니다. 관련 피해를 예방하기 위해서는 국가 사업 안내 등의 제목을 가진 메일을 수신할 경우 첨부된 파일의 확인을 지양하고 필요한 내용은 정부가 운영하는 공식 웹사이트에서 확인하는 것이 가장 좋습니다.

2 월에 주목할 만한 보안 위협으로는 애플(Apple)의 최신 아키텍처인 M1 칩이 탑재된 macOS 기기를 노리는 애드웨어 악성코드가 2 가지 발견되었습니다. 각각 'GoSearch22'와 'Silver Sparrow'로 명명된 두 악성코드는 이미 수 만대의 mac 기기를 감염시킨 것으로 알려졌습니다. 뿐만 아니라 두 악성코드 모두 이번에 신규 탑재된 M1 칩뿐만 아니라 기존의 Intel 칩을 모두 공격할 수 있는 멀티 아키텍처 악성코드로 밝혀져 악성코드 개발자들이 꾸준히 새로운 기술에 대응하는 악성코드를 개발 중이며 향후 더 많은 악성 변종이 나타날 것으로 예상됩니다.

2 월 한 달 동안에도 많은 랜섬웨어 이슈가 발생했습니다. 그중 Ziggy 랜섬웨어가 지금까지의 운영을 중단하고 피해자들이 파일을 복구할 수 있는 복호화 키를 공개하기로 했습니다. Ziggy 랜섬웨어 운영자들은 최근 Emotet 과 Netwalker 랜섬웨어가 국제 수사 기관의 공조로 무력화된 것을 보고 랜섬웨어 운영을 중단하기로 결정한 것으로 알려졌습니다. 운영자는 피해자들의 복호화 키와 함께 복호화 툴을 공개했으며 랜섬웨어 전문가에게 복호화 툴의 소스코드를 전달해 보안 전문가들의 Ziggy 랜섬웨어 복호화 툴이 제작됐습니다. Ziggy 랜섬웨어 피해자들은 Emsisoft 의 홈페이지에서 무료 복호화 툴을 다운로드해 파일을 복호화할 수 있습니다.

최근 공격자들이 지속적으로 공격 기능을 고도화하고 공격 범위를 확대해 가는 모습을 보여주고 있습니다. 항상 공격자들은 공격 목표로 삼는 타깃이 어떤 부분에 관심을 가지고 있는지 집중합니다. 내가 평소에 관심을 가지고 있는 주제에 대한 내용이라고 할지라도 출처를 알 수 없는 메일을 열람하거나 신뢰할 수 없는 앱을 PC 나 스마트폰에 설치하는 것은 최대한 지양해야 하며 사용하는 PC 및 모바일 기기의 운영 체제에 맞는 백신을 통해 사용 환경을 항상 점검할 것을 권장합니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

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

2021 년 2 월의 감염 악성코드 Top 15 리스트에서는 지난달에 이어 Hosts.media.opencandy.com 와 Misc.HackTool.AutoKMS 이 각각 1 위와 2 위를 차지했으며 지난달 13 위를 차지했던 Trojan.Agnet.Gen 이 10 계단 급상승하여 3 위를 차지했다. 이번 달에는 Misc.Riskware.Segurazo 를 비롯한 5 건의 악성코드가 새롭게 Top 15 에 이름을 올렸다. 그 외에는 큰 순위 변동 없이 대체적으로 지난달과 유사한 순위 양상을 보였다.

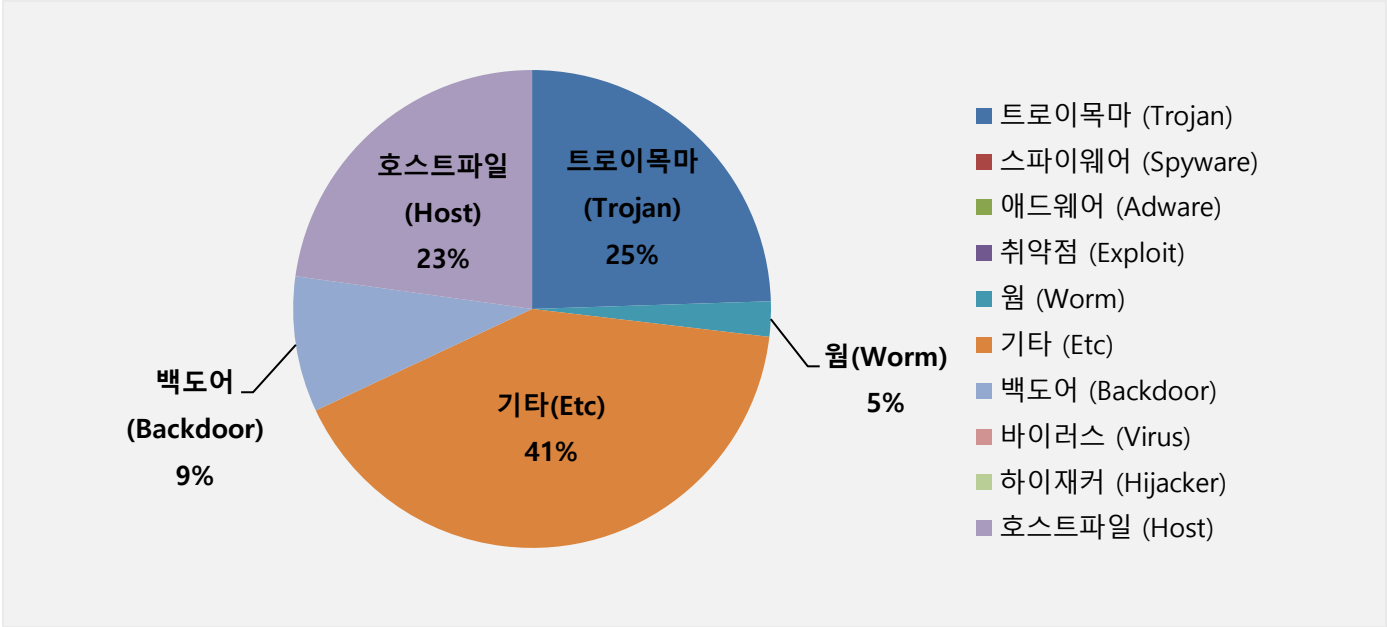
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	-	Hosts.media.opencandy.com	Host	550,517
2	-	Misc.HackTool.AutoKMS	ETC	345,948
3	↑ 10	Trojan.Agent.Gen	Trojan	295,745
4	↑ 3	Backdoor.Generic.792814	Backdoor	221,498
5	↓ 1	Trojan.ShadowBrokers.A	Trojan	167,249
6	↓ 3	Misc.HackTool.KMSActivator	ETC	166,029
7	↑ 2	Misc.Keygen	ETC	107,303
8	-	Misc.Riskware.TunMirror	ETC	90,119
9	New	Misc.Riskware.Segurazo	ETC	84,359
10	↑ 1	Gen:Trojan.Dropper.RQU.Ev1@aGUXIJfO	Trojan	74,047
11	↓ 5	Gen:Variant.Johnnie.248927	ETC	70,474
12	New	Misc.Riscware.BitCoinMiner	ETC	65,312
13	New	Gen:Variant.Mikey.118395	ETC	63,639
14	New	Worm.ACAD.Bursted.	Worm	57,482
15	New	Trojan.HTML.Ramnit.A	Trojan	53,951

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2021 년 02 월 01 일 ~ 2021 년 02 월 28 일

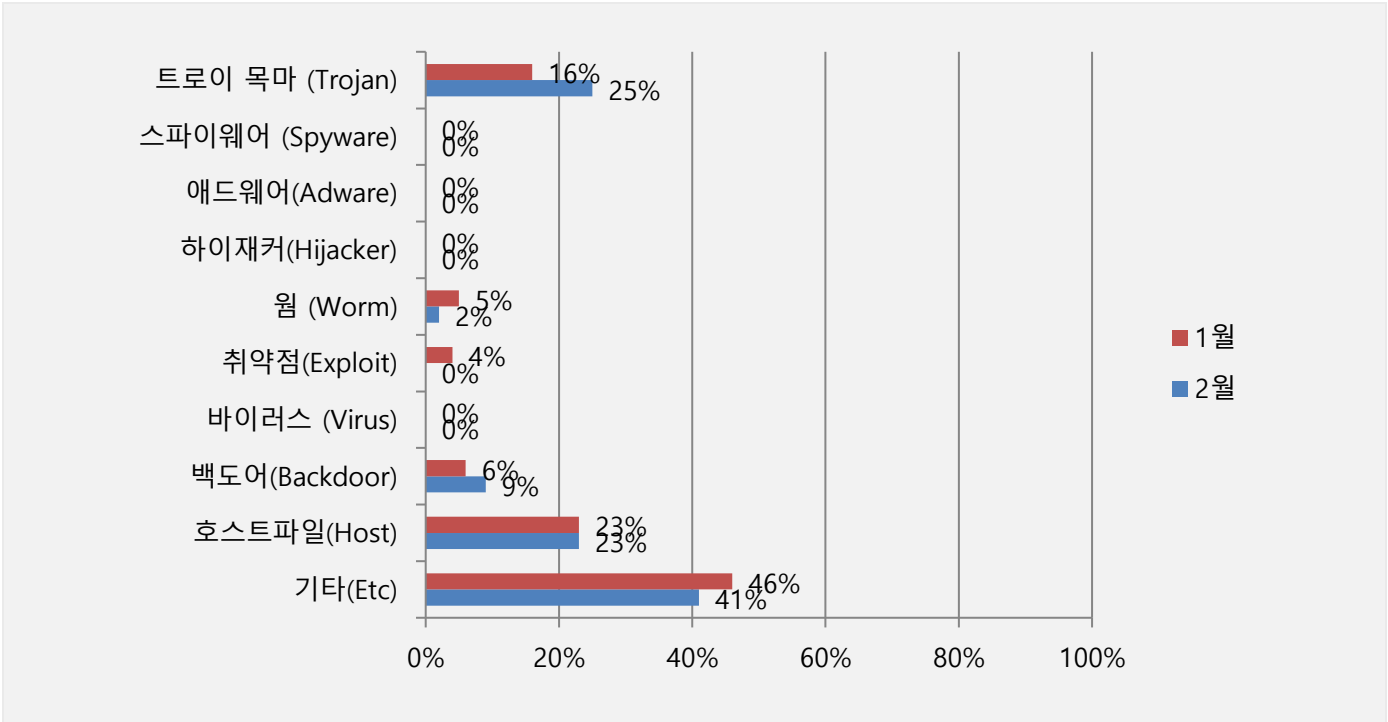
악성코드 유형별 비율

악성코드 유형별 비율에서 기타(ETC) 유형이 가장 많은 46%를 차지했으며 호스트파일(Host) 유형이 23%로 그 뒤를 이었다. 수 달간 두 번째로 많은 비중을 차지했던 트로이목마(Trojan) 유형이 16%로 소폭 감소했으며 지난달 미미한 수치를 보이던 취약점(Exploit) 유형의 비율이 4%로 상승했다. 2020 년 12 월과 비교하여 전체 감염 건수는 약 5.21% 증가하였다.



카테고리별 악성코드 비율 전월 비교

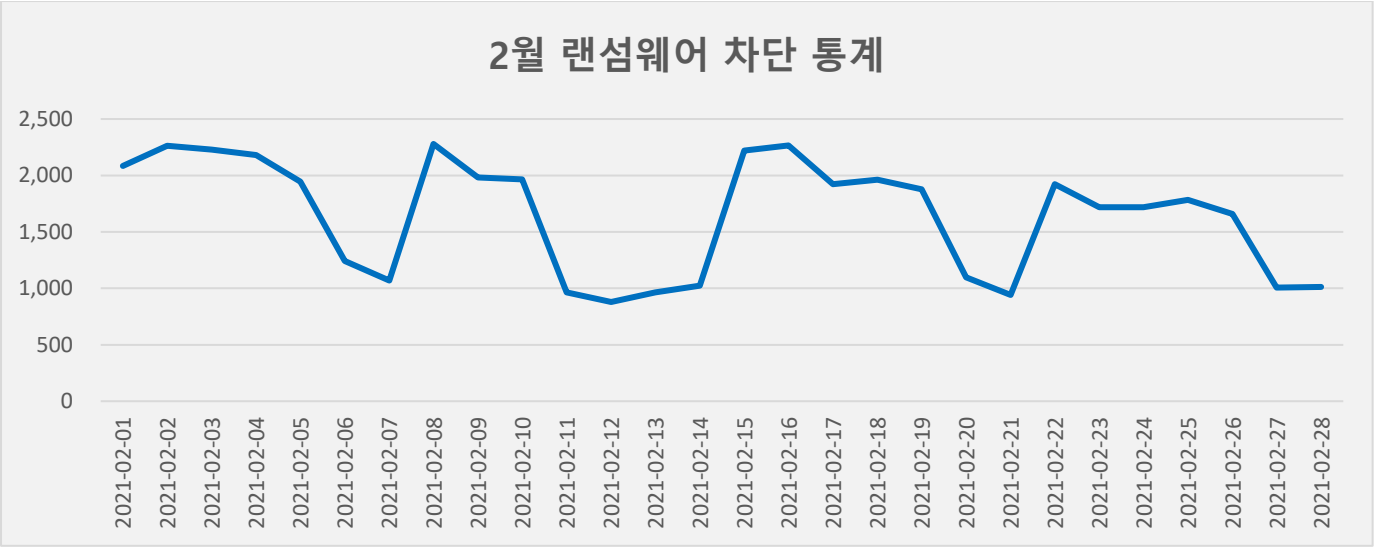
2 월에는 지난 1 월과 비교하여 트로이목마(Trojan) 유형이 9% 증가하였으며, 호스트파일(Host) 유형의 악성코드 감염 비율은 지난달과 동일하게 23%를 차지했다. 또한 지난달에는 적은 비율로 탐지됐던 웜(Worm) 유형과 취약점(Exploit) 유형의 수치가 감소하였으며 1 월에 6%를 차지했던 백도어(Backdoor) 유형이 소폭 증가하여 9%를 기록했다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

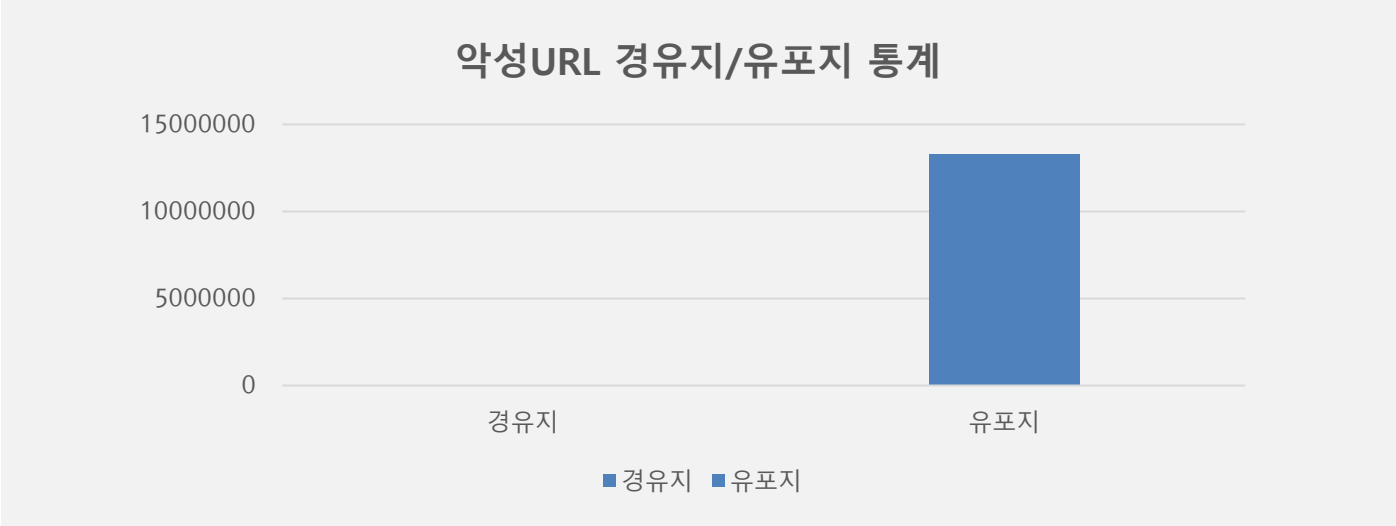
2 월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB 에 의한 시그니처 탐지 횟수는 통계에 포함되지 않는다. 2 월 1 일부터 2 월 28 일까지 총 46,182 건의 랜섬웨어 공격 시도가 차단되었다. 1 월에 비해 랜섬웨어 공격 건수는 약 15.19% 가량 감소하였다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 2 월 한 달간 총 13,338,133 건의 악성코드 경유지/유포지 URL 이 확인되었다. 이 수치는 1 월 한 달간 확인되었던 12,876,544 건의 악성코드 경유지/유포지 URL 수에 비해 약 3.58% 가량 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 보길 바란다.



02
전문가 보안 기고

1. 발주서 파일로 위장한 “NAVER WORKS” 피싱메일 주의!

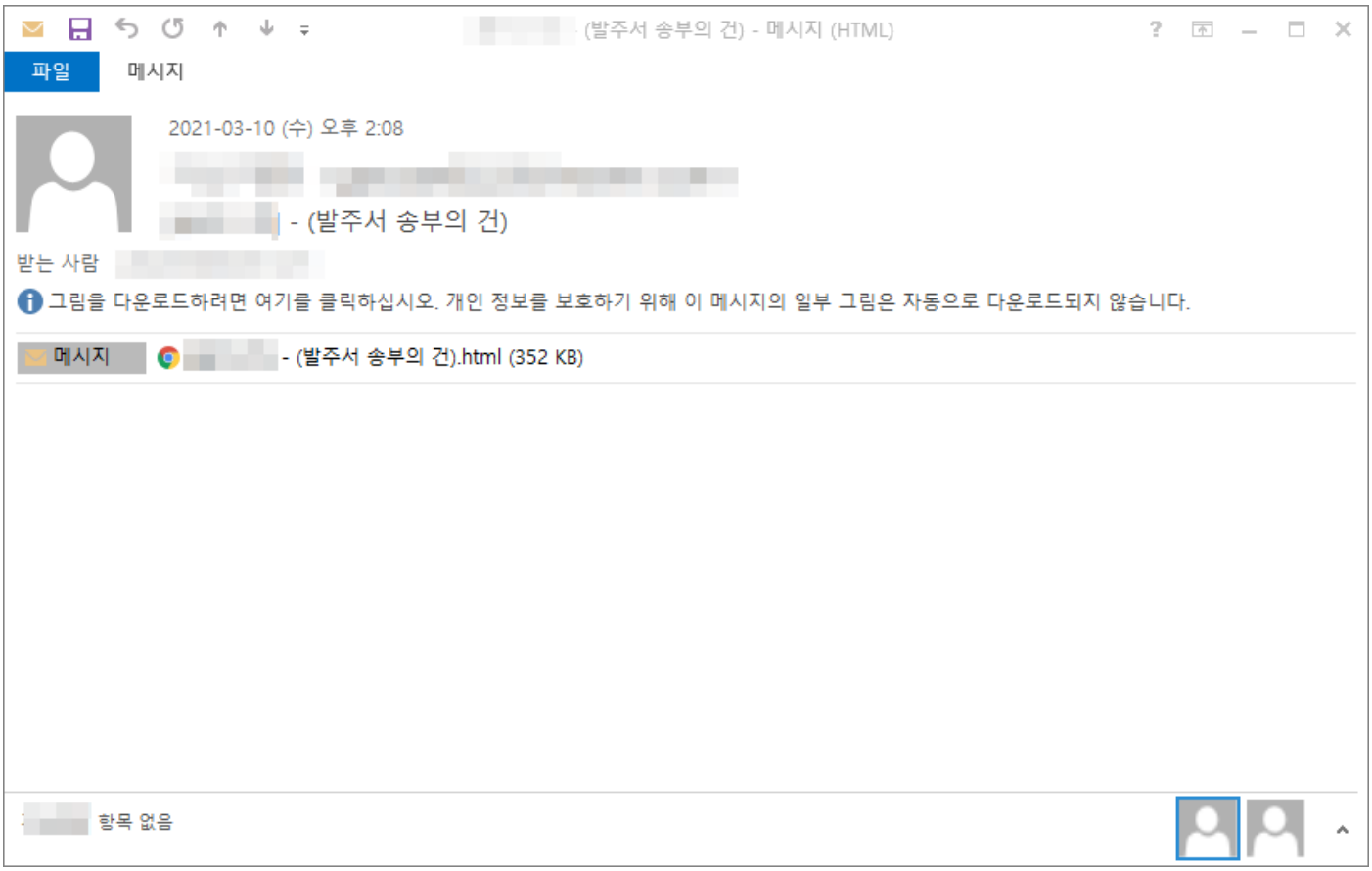
2. 사생활 녹화 영상으로 협박하는 hoax 메일 주의!

1. 발주서 파일로 위장한 "NAVER WORKS" 피싱메일 주의!

최근 발주서 파일로 위장하여 "NAVER WORKS(네이버 웍스)" 계정 탈취를 목적으로 발송되는 피싱 메일이 발견되어 사용자들의 주의가 필요합니다.

이번에 발견된 메일은 "[플***] – (발주서 송부의 건)"라는 제목으로 수신되었으며, 특정 업체명을 도용해 실제 기업에서 발송한 것처럼 위장했습니다.

사용자가 메일에 포함된 첨부파일을 실행하면 사용자 정보를 탈취하는 전형적인 '스피어 피싱' 방식입니다.

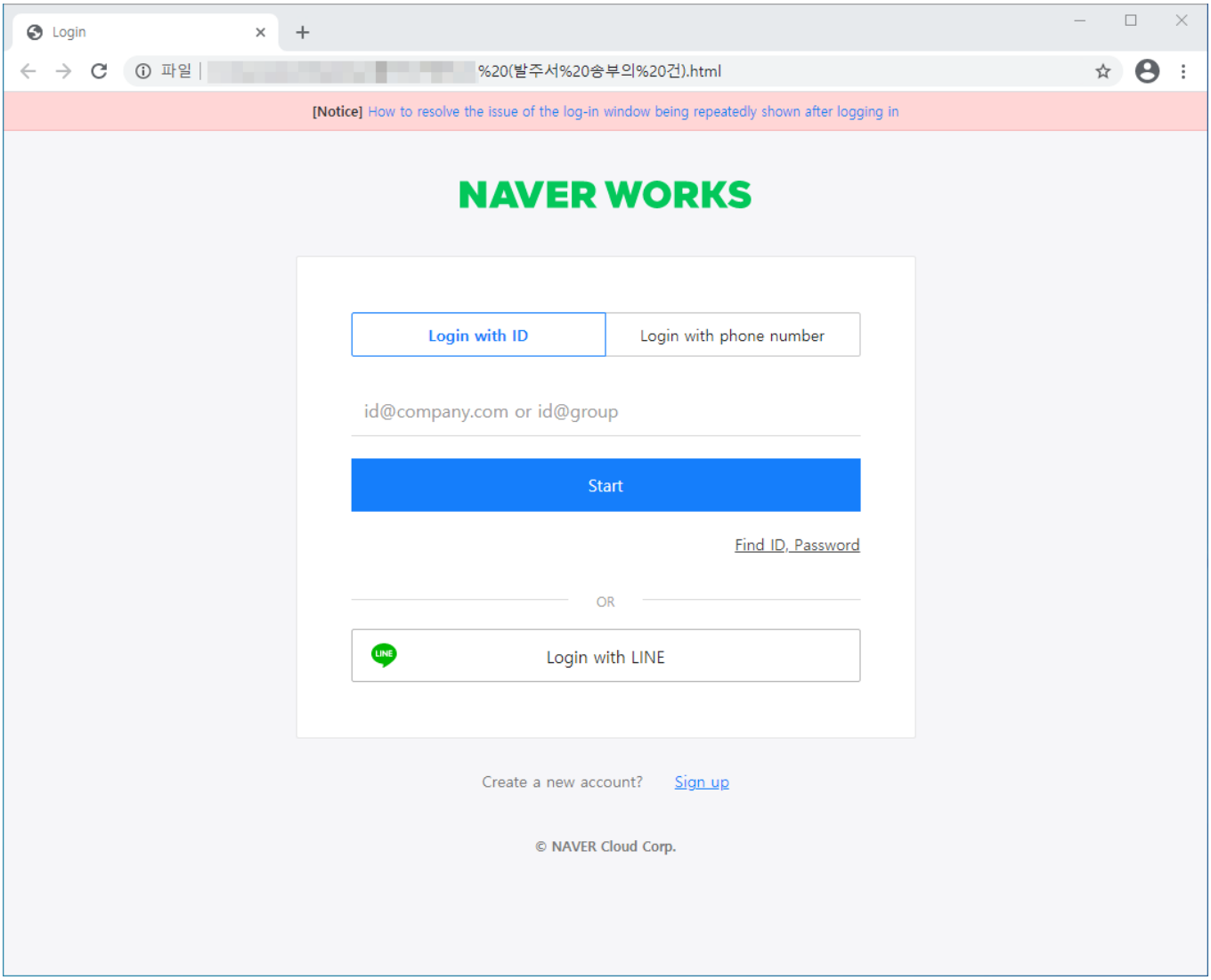


[그림 1] "NAVER WORKS" 계정탈취를 위한 피싱 공격 이메일 화면

사용자가 발주서 내용 확인을 위해 첨부된 파일을 다운로드하여 실행할 경우, 브라우저를 통해 "NAVER WORKS" 계정과 패스워드를 가로채기 위한 피싱 페이지로 연결됩니다.

첨부된 파일의 대한 정보는 다음과 같습니다.

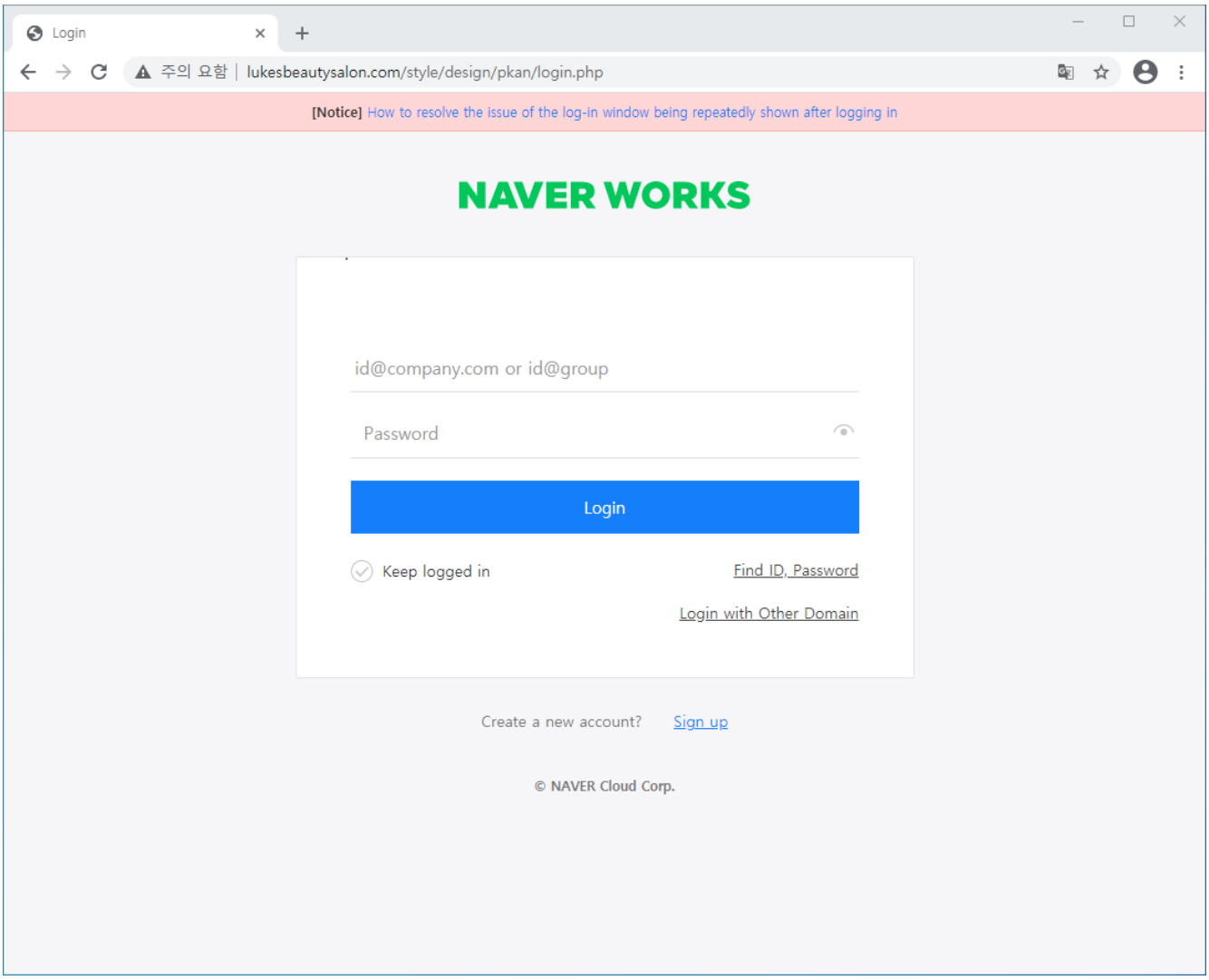
첨부 파일명	알약 탐지명
[플***] – (발주서 송부의 건).html	Trojan.HTML.Phish



[그림 2] 브라우저로 동작 된 피싱 페이지 화면

이메일을 통해 유포된 피싱 사이트의 이전 유형들의 경우, 첨부파일 실행 시 나타나는 피싱 사이트에 사용자가 정보를 입력하면 개인정보 수집 사이트로 바로 이동하는 방식이 대다수였습니다.

그러나 이번에 발견된 피싱 사이트는 사용자가 로그인을 위해 이메일을 등록하면 계정과 패스워드 정보 입력을 위한 실제 피싱 사이트로 사용자를 이동시키는 방식으로 두 단계에 걸쳐 진행됩니다.



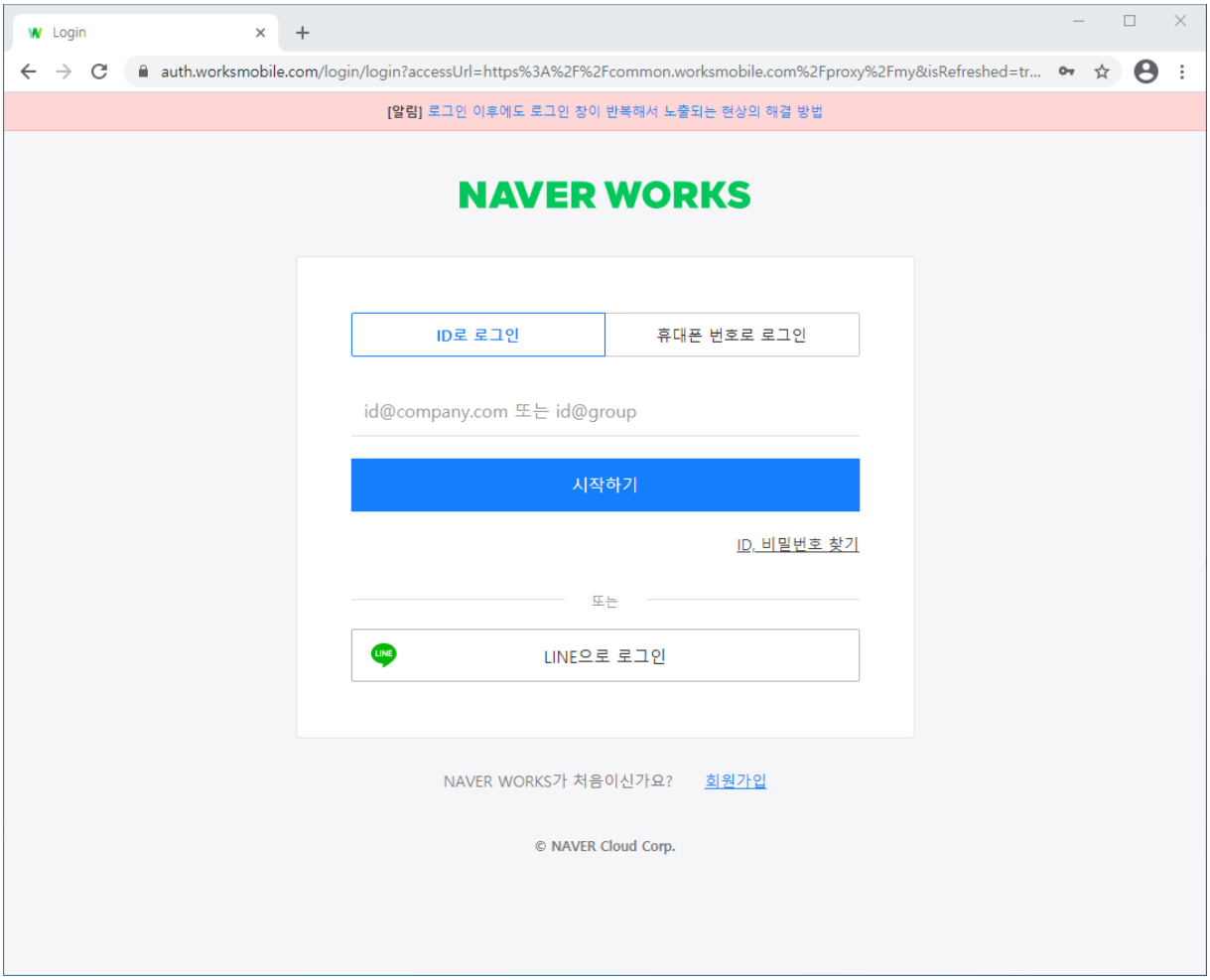
[그림 3] 웹을 통해 연결 된 피싱 사이트 화면

사용자가 입력한 NAVER WORKS 로그인 정보는 아래 공격자 서버로 전달됩니다.

- 개인 정보 수집 사이트
hxxps://lukesbeautysalon[.]com/style/design/pkan/login.php

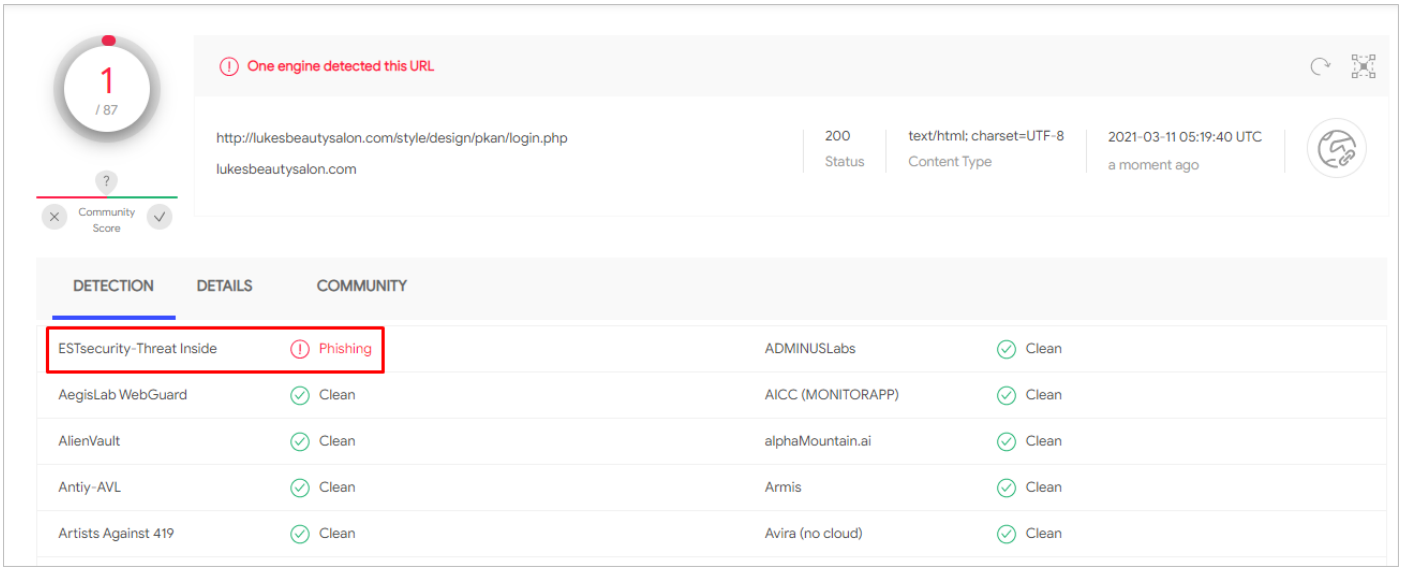
- 개인정보 전달 서버 IP
86.104.15.60

개인정보가 전달된 후에는 실제 "NAVER WORKS 로그인" 페이지로 리디렉션됩니다.



[그림 4] 사용자 정보 수집 후 보여지는 NAVER WORKS 정상 로그인 사이트 화면

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

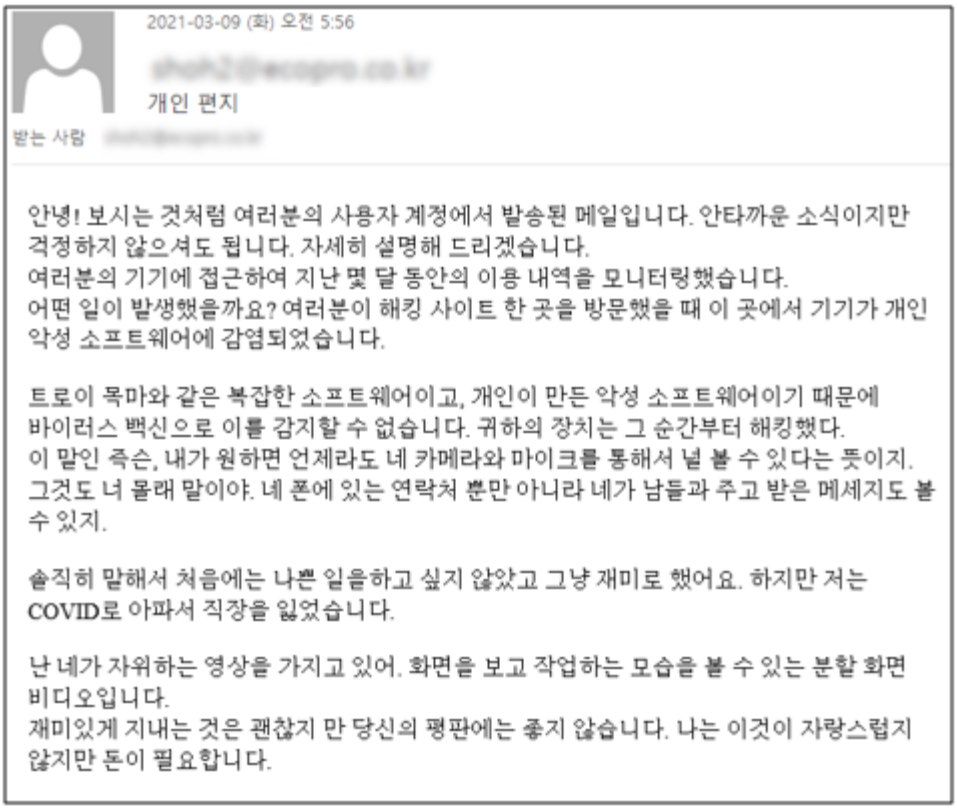


[그림 5] ESTSecurity-Threat Inside 개인정보 수집 사이트 탐지 화면

2. 사생활 녹화 영상으로 협박하는 hoax 메일 주의!

최근 환경 기술 관련 기업 내 사내 계정을 대상으로 Hoax 메일이 유포되고 있어 사용자들의 주의가 필요합니다.

이번에 발견된 피싱 메일은 "개인 편지"라는 제목으로 전파되었으며, 제목에서 추측할 수 있듯이 본문 내용은 매우 사적인 내용으로 수신자를 협박하고 있음을 알 수 있습니다.



2021-03-09 (화) 오전 5:56

[redacted]

개인 편지

받는 사람 [redacted]

안녕! 보시는 것처럼 여러분의 사용자 계정에서 발송된 메일입니다. 안타까운 소식이지만 걱정하지 않으셔도 됩니다. 자세히 설명해 드리겠습니다.
여러분의 기기에 접근하여 지난 몇 달 동안의 이용 내역을 모니터링했습니다.
어떤 일이 발생했을까요? 여러분이 해킹 사이트 한 곳을 방문했을 때 이 곳에서 기기가 개인 악성 소프트웨어에 감염되었습니다.

트로이 목마와 같은 복잡한 소프트웨어이고, 개인이 만든 악성 소프트웨어이기 때문에 바이러스 백신으로 이를 감지할 수 없습니다. 귀하의 장치는 그 순간부터 해킹했다.
이 말인 즉슨, 내가 원하면 언제라도 네 카메라와 마이크를 통해서 널 볼 수 있다는 뜻이지.
그것도 너 몰래 말이야. 네 폰에 있는 연락처 뿐만 아니라 네가 남들과 주고 받은 메세지도 볼 수 있지.

솔직히 말해서 처음에는 나쁜 일을하고 싶지 않았고 그냥 재미로 했어요. 하지만 저는 COVID로 아파서 직장을 잃었습니다.

난 네가 자위하는 영상을 가지고 있어. 화면을 보고 작업하는 모습을 볼 수 있는 분할 화면 비디오입니다.
재미있게 지내는 것은 괜찮지 만 당신의 평판에는 좋지 않습니다. 나는 이것이 자랑스럽지 않지만 돈이 필요합니다.

[그림 1] 기업 내 사내 계정으로 유포된 Hoax 메일 화면

해당 메일에는 번역기를 돌린듯한 어색한 말투가 사용되었으며, 이를 통해 공격자는 하나의 스크립트를 여러 언어로 번역하여 전 세계 불특정 다수에게 유포한 것으로 추측됩니다.

작성된 내용을 살펴보면, 수신자가 접속했던 성인 사이트에서 악성코드 감염이 발생했고, 이를 통해 사생활이 녹화된 동영상을 획득하였으니 이를 유포하기 전에 금전을 보내라는 식으로 수신자를 협박하고 있습니다.

해당 메일은 이전에도 꾸준히 발견되어 온 몸캠 피싱 유형으로 확인되나, 공격자가 코로나 19 여파로 인해 생활이 어려워졌음을 덧붙인 것으로 볼 때 비교적 최근에 작성된 것으로 보입니다.

02 전문가 기고

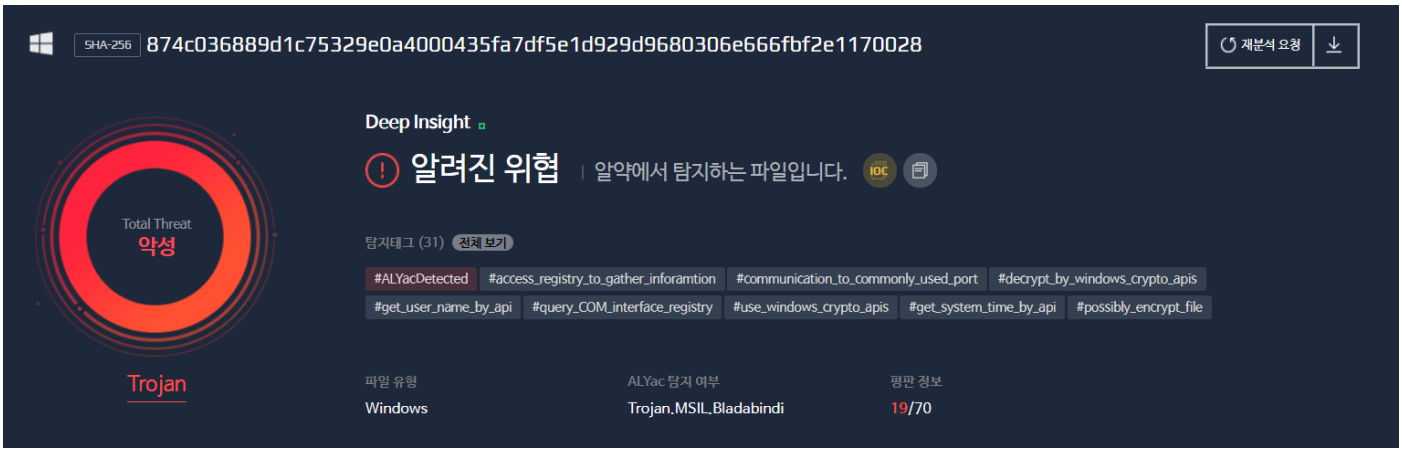
Hoax 메일의 전체 내용은 아래와 같습니다.

> 안녕! 보시는 것처럼 여러분의 사용자 계정에서 발송된 메일입니다. 안타까운 소식이지만 걱정하지 않으셔도 됩니다. 자세히 설명해 드리겠습니다.
> 여러분의 기기에 접근하여 지난 몇 달 동안의 이용 내용을 모니터링했습니다.
> 어떤 일이 발생했을까요? 여러분이 해킹 사이트 한 곳을 방문했을 때 이 곳에서 기기가 개인 악성 소프트웨어에 감염되었습니다.
>
> 트로이 목마와 같은 복잡한 소프트웨어이고, 개인이 만든 악성 소프트웨어이기 때문에 바이러스 백신으로 이를 감지할 수 없습니다. 귀하의 장치는 그 순간부터 해킹했다.
> 이 말인 즉슨, 내가 원하면 언제라도 네 카메라와 마이크를 통해서 널 볼 수 있다는 뜻이지.
> 그것도 너 몰래 말이야. 네 폰에 있는 연락처 뿐만 아니라 네가 남들과 주고 받은 메세지도 볼수 있지.
>
> 솔직히 말해서 처음에는 나쁜 일을하고 싶지 않았고 그냥 재미로 했어요. 하지만 저는 COVID 로 아파서 직장을 잃었습니다.
>
> 난 네가 자위하는 영상을 가지고 있어. 화면을 보고 작업하는 모습을 볼 수 있는 분할 화면 비디오입니다.
> 재미있게 지내는 것을 괜찮지 만 당신의 평판에는 좋지 않습니다. 나는 이것이 자랑스럽지 않지만 돈이 필요합니다.

이번 Hoax 메일에는 기존 몸캠 피싱에서 흔히 사용되는 비트코인 주소와 같은 금전 지불 방법은 나와있지 않아서, 실제 공격을 수행하기 전 테스트 용도 또는 누군가의 단순 장난 목적으로 발송된 것으로 추정됩니다.

수신자의 사생활 동영상으로 협박하는 Hoax 메일은 지속적으로 발견되고 있습니다. 이러한 Hoax 메일은 거의 유사한 내용으로 유포되고 있기 때문에 기업 내에서 외부에 공개된 메일을 담당하고 있는 담당자나 개인 메일 사용자들은 이러한 형태의 Hoax 메일을 확인할 경우 바로 삭제해야 하며, 금전을 송금하거나 악성 사이트 링크를 클릭하지 않도록 각별한 주의를 기울여야 합니다.

현재 이스트시큐리티 '쓰렛 인사이드(Threat Inside)'에서는 발견된 eml 파일을 아래와 같이 '악성'으로 탐지하고 있습니다.



03
악성코드 분석 보고

[Spyware.Ursnif] 악성코드 분석 보고서

'Spyware.Ursnif'(이하 'Ursnif') 악성코드는 'Gozi,'Dreambot'라는 이름의 뱅킹 트로이목마로 알려져 있다. 해당 악성코드는 메일 내 첨부된 Microsoft Office 악성 문서 파일에서 유포되는 것으로 알려져 있다.

본 악성코드는 C&C 로 정보 전송 및 추가 페이로드 실행 기능이 있으며, 페이로드의 명령 제어 기능에 따라 OS 파괴, 추가 DLL 실행 등이 있어서 공격자 의도에 따라 이용자의 피해가 발생할 수 있다.

```
HIDWORD(Hinstance) = "R1";
LODWORD(Hinstance) = "F1";
LOBYTE(v0) = 1;
TResourceStream = TResourceStream_Create(Hinstance, VMT_415354_TResourceStream, v0, hInstance);// 리소스 영역(F1 R1) load
dwSize = (**TResourceStream)(TResourceStream);// GetSize
alloc = GetMem(dwSize);
TStream_ReadBuffer(TResourceStream, alloc, dwSize);
TObject_Free(TResourceStream);
dword_45BC50 = *alloc;
alloc += 4;
alloc_ = kernel32_VirtualAlloc_0(0, dwSize, MEM_COMMIT, PAGE_EXECUTE_READWRITE);
dword_45BC44 = alloc_ - 4;
dword_45BC70 = 0;
dword_45BC74 = 0;
FillMemory(alloc_, dwSize, 0);
while ( dword_45BC70 < dwSize )
{                                       // 4byte 이후 0x7b 만큼 move
  move_(alloc_ + dword_45BC74, (dword_45BC70 + alloc), size);
  dword_45BC74 += size;
  dword_45BC70 += size;
  dword_45BC70 += dword_45BC68;
}
for ( encrypt_data = 0; encrypt_data < dword_45BC50; alloc_ = alloc_ + 4 )
{                                       // 4byte 씩 xor 연산을 통해 디코딩
  *alloc_ += encrypt_data;
  v1 = user32_LoadIconA_0(0, 0x926) + ((encrypt_data + 0x1C8 + 0x8A58A) ^ *alloc_);
  *alloc_ = &v1[user32_LoadIconA_0(0, 0x926)];
  encrypt_data += 4;
}
dword_45BC5C = dword_45BC54 + dword_45BC44 - dword_45BC58 + 4;
__asm { jmp     edx }                   // decoded_data
```

[그림] 페이로드 디코딩 및 로드 코드 중 일부

만일 기업에서 이 악성코드에 감염될 경우, 추가 악성코드 다운로드나 사용자 정보 탈취 등에 의해 정보 유출 및 시스템 파괴로 이어지는 피해가 발생할 수 있어 주의가 필요하다.

특히나 본 악성코드는 과거에 'Ursnif/ISFB' 이름으로 소스코드가 공개되어, 많은 공격자들이 커스텀하여 사용할 수 있어 여러 변종이 나올 가능성이 높다.

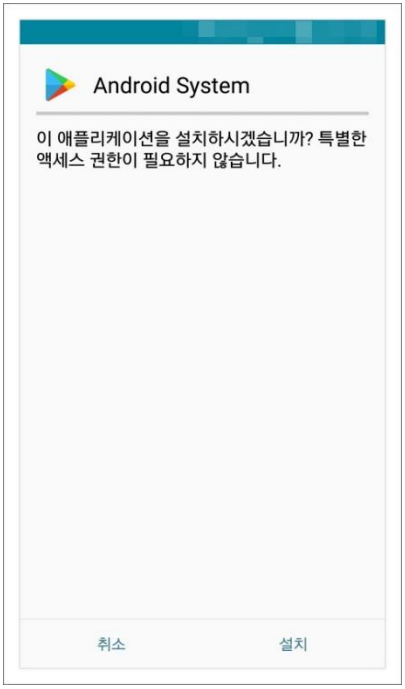
따라서, 이러한 악성코드 감염을 예방하기 위해서는 출처가 불분명한 메일에 있는 첨부파일에 대해 접근을 삼기는 보안 습관을 가져야 한다.

현재 알약에서는 해당 악성코드를 'Spyware.Ursnif' 탐지 명으로 진단하고 있으며, 관련 상세 분석보고서는 Threat Inside 웹서비스 구독을 통해 확인이 가능하다.

[Trojan.Android.Agent] 악성코드 분석 보고서

최근 해외에서 발견되는 악성 앱 중 피해자의 정보 탈취를 주요 목적으로 하는 악성 앱을 살펴보도록 하겠다. 이 악성 앱은 올해 최초 발견되었으며 다양한 악성 행위를 수행한다.

악성 앱은 안드로이드 OS 에서 제공하는 접근성 서비스를 활용하여 피해자를 감시하는 기능을 가지고 있으며 공격자가 지정한 특정 앱 실행 시 실행을 막은 후 공격자의 웹 페이지로 접속하는 브라우저를 실행한다. 공격자가 유도한 이런 페이지들은 피해자가 실행하려는 앱과 유사한 형태로 꾸며진 웹 페이지 일 것으로 추정되며 내용은 피해자 계정 등의 민감한 개인 정보를 탈취하는 내용 일 것으로 추측할 수 있다.



[그림] 설치 시 화면

'Trojan.Android.Agent'는 피해자의 민감 정보 탈취를 주요 목적으로 하고 있다. 탈취를 시도하는 개인 정보의 종류는 금융이나 암호화폐와 관련된 정보도 포함되기에 주의가 필요하다.

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

04

글로벌 보안 동향

Ziggy 랜섬웨어, 운영 중단 후 피해자 복호화 키 공개해

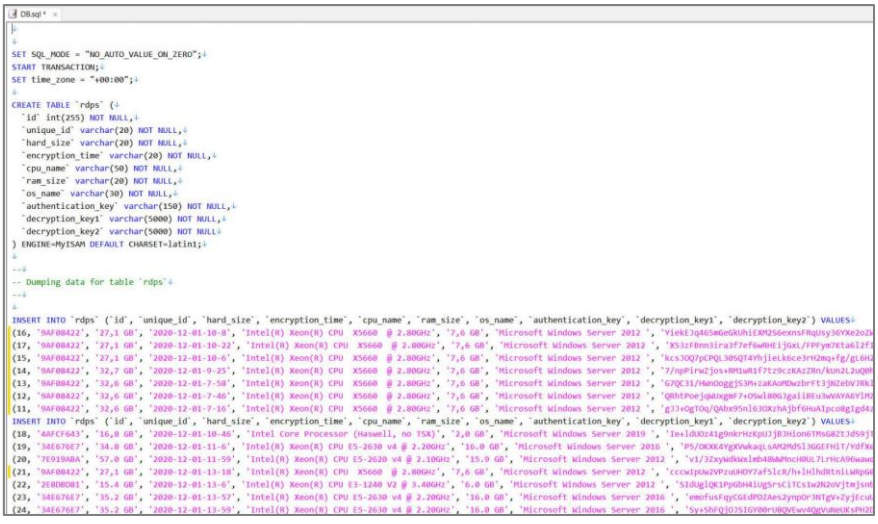
Ziggy ransomware shuts down and releases victims' decryption keys

Ziggy 랜섬웨어가 운영을 중단하고 피해자의 복호화 키를 공개했다. 이는 최근 법 집행부 활동에 대한 우려와 피해자를 암호화한 것에 대한 죄책감때문인 것으로 나타났다. 보안 연구원인 M. Shahpasandi 는 Bleeping Computer 에 Ziggy 랜섬웨어 관리자가 텔레그램에서 랜섬웨어 운영을 중단하고 암호 복호화 키를 공개하겠다고 말했다고 전했다.

[그림] Ziggy 관리자의 운영 중단 공지

[이미지 출처] https://www.bleepingcomputer.com/news/security/ziggy-ransomware-shuts-down-and-releases-victims-decryption-keys/

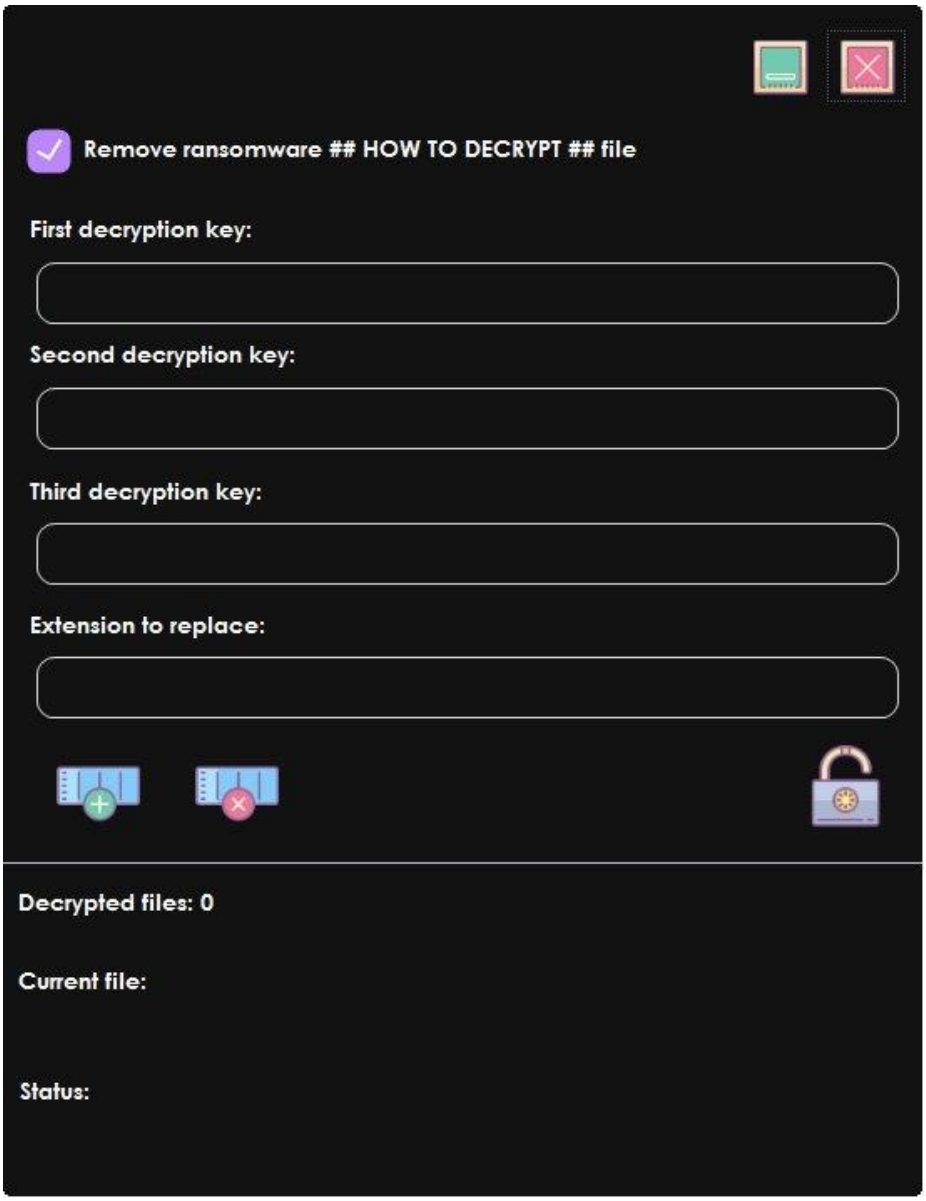
Bleeping Computer 와의 인터뷰에서, 랜섬웨어 관리자는 "제 3 세계 국가"에 거주하면서 돈을 벌어들이기 위해 랜섬웨어를 만들었다고 밝혔다. 그의 행동에 죄책감을 느끼고, 최근 법 집행부에서 Emotet 과 Netwalker 랜섬웨어를 단속한 것에 대한 우려로 인해 관리자는 랜섬웨어 운영을 중단하고 모든 키를 공개하겠다고 밝혔다. 그리고 마침내 Ziggy 랜섬웨어 관리자는 파일이 암호화된 피해자를 위한 복호화 키 922 건을 포함한 SQL 파일을 공개했다.



[그림] Ziggy 복호화 키를 포함한 SQL 파일

[이미지 출처] https://www.bleepingcomputer.com/news/security/ziggy-ransomware-shuts-down-and-releases-victims-decryption-keys/

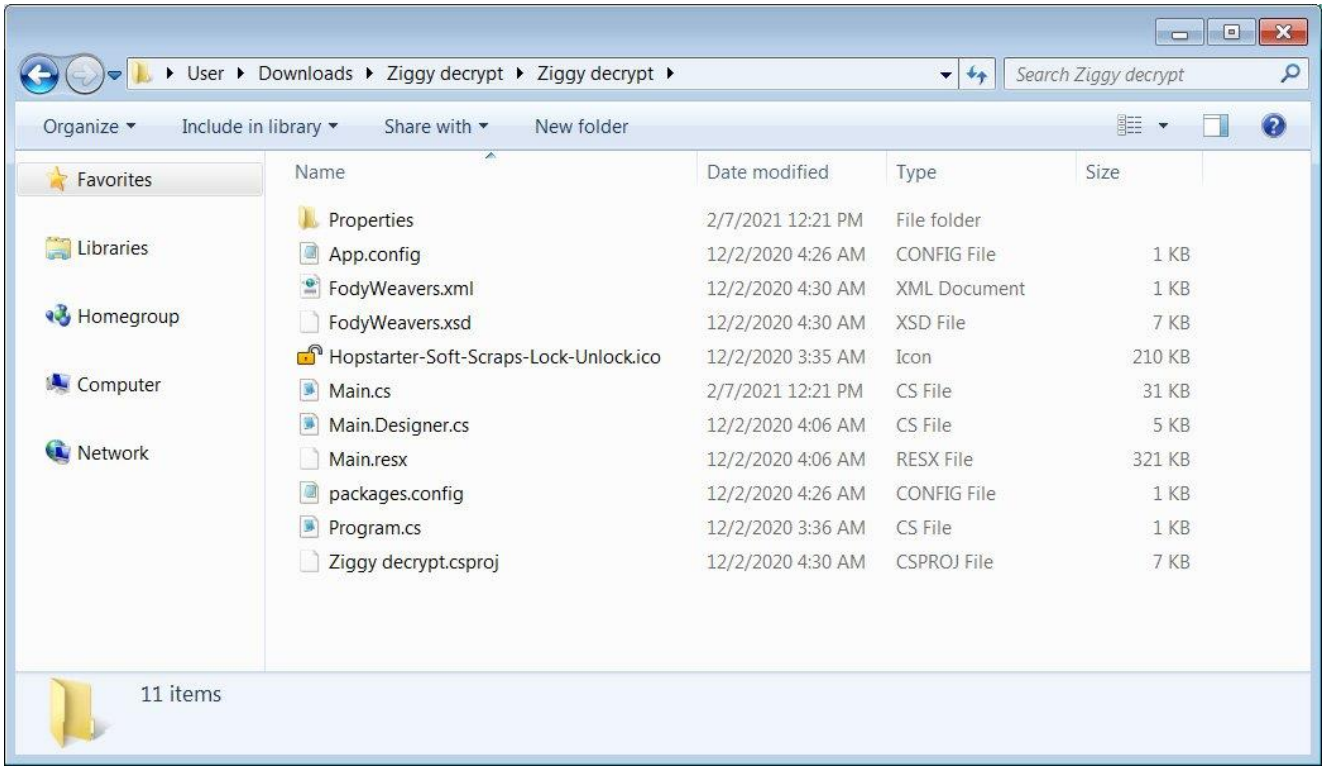
해당 랜섬웨어의 관리자는 피해자가 SQL 파일 내 포함된 키를 사용할 수 있는 복호화 툴 또한 공개했다.



[그림] Ziggy 랜섬웨어 복호화 툴

[이미지 출처] https://www.bleepingcomputer.com/news/security/ziggy-ransomware-shuts-down-and-releases-victims-decryption-keys/

복호화 툴과 SQL 파일 이외에도, 랜섬웨어 관리자는 오프라인 복호화 키를 포함하는 또 다른 복호화 툴의 소스코드를 Bleeping Computer 와 공개했다. 랜섬웨어는 인터넷에 연결되지 않은 상태 또는 C2 서버가 응답하지 않은 상태일 경우 오프라인 복호화 키를 사용하여 사용자의 암호화된 파일을 복호화 한다.



[그림] 또 다른 Ziggy 랜섬웨어 복호화 툴의 소스코드

[이미지 출처] https://www.bleepingcomputer.com/news/security/ziggy-ransomware-shuts-down-and-releases-victims-decryption-keys/

이 랜섬웨어의 관리자는 이 파일을 랜섬웨어 전문가인 Michael Gillespie 에게도 공유했으며, 그는 Emsisoft 에서 곧 복호화 툴을 공개하겠다고 밝혔다.

Emsisoft 의 Brett Callow 는 아래와 같이 밝혔다.

"자발적이든 비 자발적이든, 키를 공개하는 것이 최선의 결과라 볼 수 있다. 이로써 피해자가 랜섬머니를 지불하거나 백도어 또는 취약점을 포함할 가능성이 있는 개발자의 복호화 툴을 사용하지 않고도 데이터를 복구할 수 있게 된다. 또한 걱정해야 할 랜섬웨어 그룹이 하나 적어진다는 의미이기도 하다. 또한 최근 Emotet 및 Netwalker 관련자가 체포됨에 따라, 다른 공격자들 또한 불안할 수 있다. 따라서 더 많은 랜섬웨어 그룹이 키를 공개하기를 바란다."

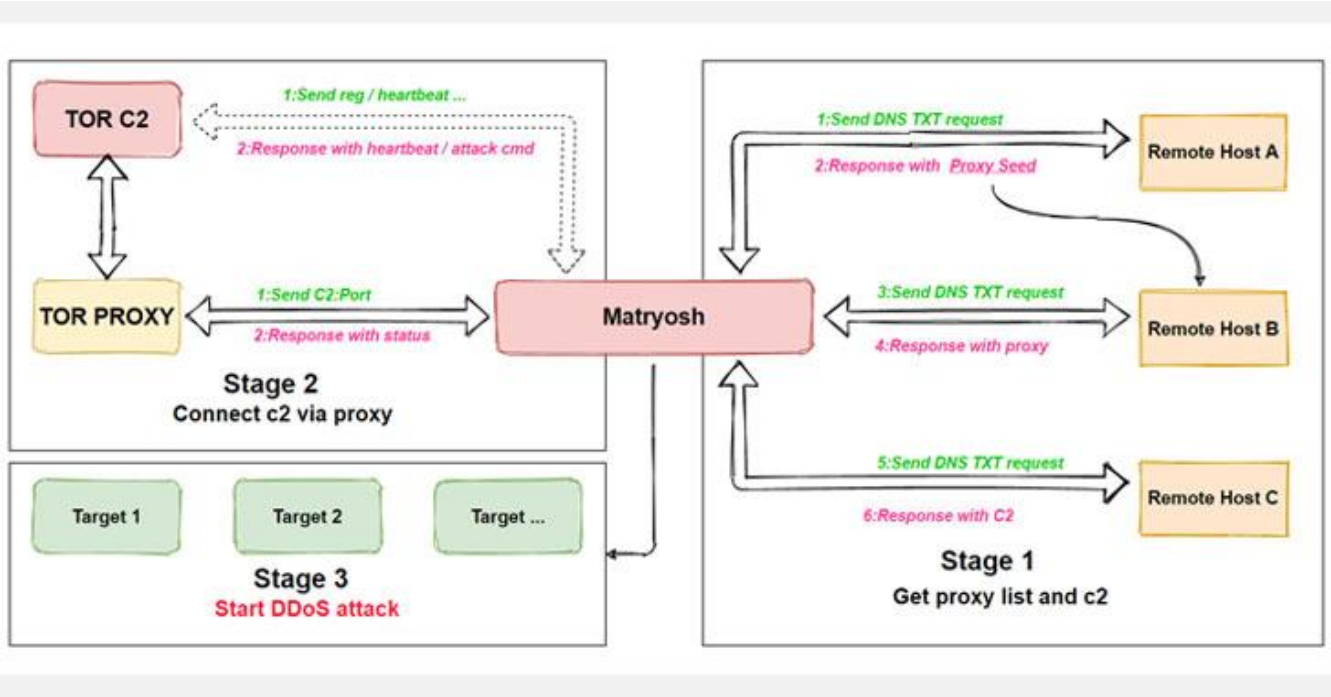
랜섬웨어 관리자가 정직하게 운영을 종료하고 키를 공개했지만, Bleeping Computer 는 항상 공격자가 제공한 복호화 툴보다는 보안 회사에서 개발한 복호화 툴을 사용하는 것이 좋다고 밝혔다. Emsisoft 는 Ziggy 랜섬웨어에 대한 무료 복호화 툴을 공개했다.

[출처] https://www.bleepingcomputer.com/news/security/ziggy-ransomware-shuts-down-and-releases-victims-decryption-keys/
https://www.emsisoft.com/ransomware-decryption-tools/ziggy

새로운 Matryosh DDoS 봇넷, 안드로이드 기반 기기 노려

Beware: New Matryosh DDoS Botnet Targeting Android-Based Devices

초기 악성코드 캠페인이 안드로이드 기기를 봇넷에 추가하고 있는 것으로 나타났다. 이 캠페인의 주된 목적은 DDoS 공격을 수행하는 것이었다.



[이미지 출처] https://blog.netlab.360.com/matryosh-botnet-is-spreading-en/

Qihoo 360 Netlab 의 연구원들이 "Matryosh"라 명명한 이 최신 공격은 Mirai 봇넷 프레임워크를 재사용했으며, 노출된 ADB(Android Debug Bridge) 인터페이스를 통해 안드로이드 기기를 감염시키고, 이를 공격자의 네트워크에 종속시킨다. ADB 는 커뮤니케이션을 처리하고 개발자가 안드로이드 기기에 앱을 설치 및 디버깅 할 수 있도록 하는 안드로이드 SDK 의 커맨드라인 툴이다. 해당 옵션은 대부분의 안드로이드 스마트폰 및 태블릿에서 기본적으로 꺼져있는 상태이지만, 일부 공급 업체는 이 기능이 활성화된 상태로 출시하기 때문에 인증되지 않은 공격자가 5555TCP 포트를 통해 기기에 원격으로 연결하여 장치를 직접 오픈해 악용이 가능하다.

봇넷이 ADB를 활용하여 취약한 기기를 감염시킨 것은 이번이 처음은 아니다. 2018년 7월, ADB 포트는 Fbot을 포함한 Satori 봇넷 변종 다수를 확산시키는데 사용되었으며, 이로부터 1 년 후 새로운 가상화폐 마이닝 봇넷 악성코드가 발견되었으며 동일한 인터페이스를 통해 한국, 대만, 홍콩, 중국의 안드로이드 사용자들을 노렸다.

하지만 Matryosh 의 특이점은 악성 행위를 숨기고 네트워크를 통해 공격자가 제어하는 서버에서 명령을 받아온다는 것이다. Netlab 의 연구원들은 "C2 를 얻어내는 과정은 마트료시카 인형처럼 여러 층으로 둘러싸여 있다"라고 밝혔다. Matryosh 는 원격 호스트네임을 복호화하고 DNS TXT 요청(리소스 기록 유형)을 통해 TOR C2 및 TOR 프록시를 얻어낸다. 그런 다음 TOR 프록시와의 연결을 설정하고 프록시를 통해 TOR C2 서버와 통신하고, 서버의 추가 지시를 기다린다. 연구원들은 이 봇넷의 명령 형식과 TOR C2 를 사용한다는 점이 Moobot 그룹이 개발한 LeetHozer 라는 다른

봇넷과 매우 유사하다고 밝혔다. 연구원들은 “이러한 내용을 고려해볼 때 Matryosh 가 이 그룹의 새로운 작업일 것으로 추측한다”고 밝혔다.

[출처] https://thehackernews.com/2021/02/beware-new-matryosh-ddos-botnet.html
https://blog.netlab.360.com/matryosh-botnet-is-spreading-en/

Apple M1 칩용으로 설계된 첫 번째 악성코드, 실제 공격에서 발견돼

First Malware Designed for Apple M1 Chip Discovered in the Wild

애플의 M1 칩에서 실행되도록 맞춤형 설계된 최초의 악성코드 샘플 중 하나가 발견되었다. 이는 악성 공격자가 자체 프로세서를 사용하는 최신 Mac 을 공격하기 위한 악성 소프트웨어를 채택하기 시작했음을 나타낸다. 애플 실리콘으로 전환됨에 따라, 개발자들은 더 나은 성능 및 호환성을 위해 새로운 버전의 앱을 빌드해야 한다. macOS 보안 연구원인 Patric Wardle 은 공격자들이 악성코드가 애플의 새로운 M1 시스템에서 실행할 수 있는 악성코드를 빌드하기 위해 유사한 단계를 밟고 있다고 밝혔다.

Wardle 은 처음에는 인텔 x86 칩에서 실행되도록 작성되었으나 후에 ARM 기반 M1 칩에서도 실행되도록 포팅된 사파리 애드웨어 확장 프로그램인 GoSearch22 에 대해 자세히 설명했다. 12 월 27 일 VirusTotal 에 업로드된 샘플에 따르면, Pirrit 광고 악성코드의 변종인 이 악성 확장 프로그램은 2020 년 11 월 23 일 실제 공격에서 처음 목격되었다.

M1 Mac 은 동적 바이너리 변환기인 Rosetta 의 도움으로 x86 소프트웨어를 실행할 수 있지만, 네이티브 서포트를 통해 효율성이 개선될 뿐만 아니라 사용자의 관심을 끌지 않고 감시망 아래에 숨어있을 수 있는 가능성이 증가한다.

[이미지 출처] https://objective-see.com/blog/blog_0x62.html

04 글로벌 보안 동향

2016 년 처음으로 문서화된 Pirrit 는 지속적인 Mac 악성코드 패밀리로 공격적인 광고를 사용자에게 푸시하는 것으로 악명이 높으며, 광고를 클릭할 경우 정보 수집 기능이 포함된 원치 않는 앱을 다운로드 및 설치한다. 높은 강도로 난독화된 GoSearch22 애드웨어는 자신을 정식 사파리 브라우저 확장 프로그램으로 위장한다. 하지만 사실 이는 브라우징 데이터를 수집하고, 추가 악성코드를 배포하는 악성 사이트로 연결되는 링크를 포함한 배너 및 팝업과 같은 많은 광고를 제공한다.

Wardle 은 해당 확장 프로그램이 악성 콘텐츠를 숨기기 위해 지난 11 월 애플 개발자 ID "hongsheng_yan"으로 서명했지만, 해당 인증서는 현재 폐기된 상태이기 때문이 해당 애플리케이션은 또 다른 인증서로 다시 서명하지 않는 이상 macOS 에서 실행되지 않을 것이다. Wardle 은 "(정적) 분석 툴이나 안티바이러스 엔진은 arm64 바이너리를 다룰 때 어려움이 있을 것이다"고 밝혔다. GoSearch22 의 악성 기능은 완전히 새롭거나 위험하지 않을 수는 있지만, 이것이 요점은 아닙니다. 새로운 M1 호환 악성코드가 출현했다는 것은 이제 시작일 뿐이며, 앞으로 더 많은 변종이 나타날 가능성이 높다.

[출처] https://thehackernews.com/2021/02/first-malware-designed-for-apple-m1.html
https://objective-see.com/blog/blog_0x62.html

(주)이스트시큐리티

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