보증 부인: 본 문서에 포함된 정보는 어떠한 보증 없이 "있는 그대로" 제공됩니다(정확성 관련 사항을 포함하되 이에 국한되지 않음). 본 문서는 정보 목적으로만 제공됩니다. Anomali Incorporated는 해당 정보의 사용과 관련하여 어떠한 종류의 책임도 지지 않습니다.

코로나바이러스(코로나19) 글로벌 대유행으로 인한 사이버 공격의 급증

개요

2020년 1월 이후, 사이버 공격자들이 2019년 신종 코로나바이러스(코로나19) 글로벌 대유행을 둘러싼 미디어의 이목을 이용하여 선량한 사용자에게 맬웨어를 배포하도록 설계된 피싱 캠페인을 시도하기 시작했습니다. 현재 게시일 시점으로 당사 연구진에서는 6,000여 개가 넘는 침해지표(IOC)와 11개 사이버 공격자 또는 단체가 배포한 39개의 다양한 맬웨어군과 80개의 다양한 마이터 어택(MITRE ATT&CK) 기술과 연관된 최소 15개의 뚜렷한 캠페인을 포착했습니다. 관련 맬웨어군 목록에는 AgentTesla, AZORult, 아기상어(BabyShark), Cerberus, 코로나바이러스 랜섬웨어, CovidLock Android 맬웨어, Crimson RAT, Emotet, GuLoader, Kpot Infostealer, Lokibot, Nanocore RAT, NetWalker 랜섬웨어, Parallax RAT, Redline Stealer, Remcos, Trickbot 등이 포함되며 이에 국한되지 않습니다. 또한 중국, 북한, 파키스탄, 러시아와 연관된 일부 사이버 공격자 및 단체가 코로나19를 주제로 한 악성 활동에 참여하고 있는 것으로 확인되고 있습니다.

이 백서에서는 이러한 사이버 이벤트에 대한 몇 가지 주요 사안을 다루고 있으나, 현재 진행 중인 모든 캠페인의 전체 목록을 나타내지는 않습니다. 또한 이 백서는 오늘자로 게시된 코로나19 관련 침해지표(IOC)의 대규모 리포지토리와 관련된 모든 연구를 다루고 있지 않습니다. 해당 리포지토리는 2020년 3월 15일부터 2020년 3월 22일까지 관측된 공개 IOC만 나타냅니다. 기존 Anomali 고객은 Anomali ThreatStream 및 Anomali Match를 통해서 당사 연구 기관의 전체 업데이트 현황을 확인할 수 있습니다.

세부 정보

코로나19를 주제로 한 악성 사이버 공격은 2019년 12월 중국 우한에서 전대미문의 코로나19 바이러스가 발생했다고 발표된 후 몇 주 만에 등장했습니다. 코로나19

발생이 보고된 지 3개월 만에, Anomali 연구진은 코로나 대유행 상황을 악용하여 수익을 확보하기 위해 사이버 범죄 및 테러지원국 공격자의 피싱을 통한 맬웨어 배포가 급증한 것을 관측했습니다.

그림 1. 코로나19를 주제로 한 사이버 활동에서 관측된 마이터 엔터프라이즈 어택(MITRE Enterprise ATT&CK) 기법

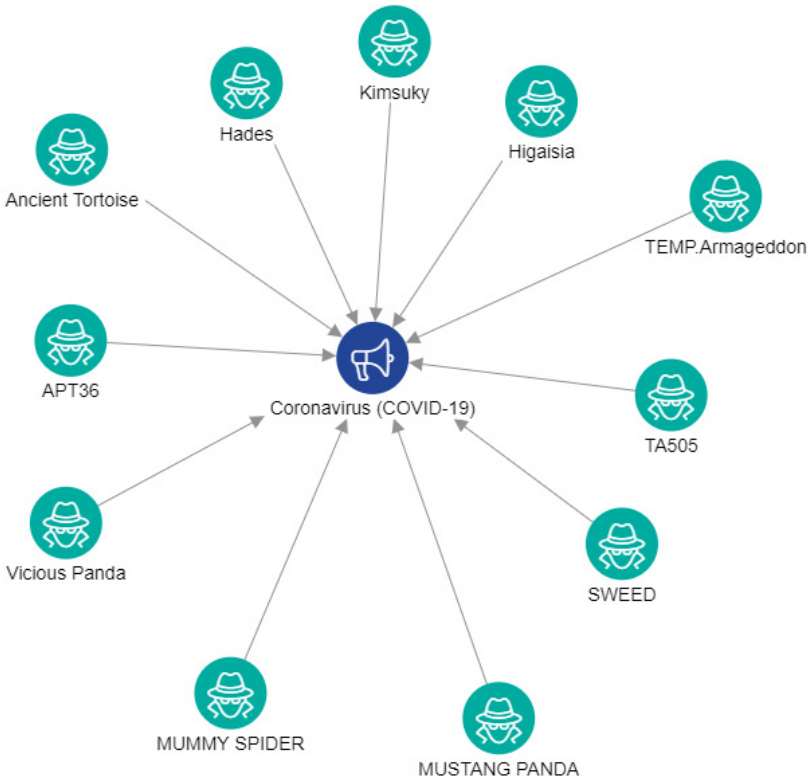

그림 2: 코로나19 피싱 캠페인 위협 공격자

코로나19를 주제로 한 사이버 활동 (2020년 1월에 확인)

코로나19 악용 사례로 보고된 초기 위협 단체 중 한 곳은 TA542(MUMMY SPIDER, Mealybug)로 Emotet(S0367)을 이용하며 별칭은 Geodo, Heodo입니다. 해당 단체는 장애인 복지사업단체 및 공공보건센터의 공식 알림으로 가장한 악성 이메일을 통해 2020년 1월 말 모습을 드러냈습니다. 해당 콘텐츠는 수신자에게 바이러스가 빠르게 확산되는 것을 경고하고 "예방 조치"가 포함된 첨부 공지문을 다운로드하도록 안내했습니다. 또한 해당 단체는 그레타 선버그를 주제로 한 피싱 이메일을 동시에 사용했다고 보고되고 있으며, 이 경우 캠페인 대상 선택에서 큰 차이를 보입니다. 코로나19 캠페인이 일본에 집중한 반면, 그레타 선버그 캠페인은 여러 국가를 대상으로 했습니다(그림 3).

Emotet 맬웨어에 감염된 컴퓨터는 랜섬웨어를 배포하거나 다른 유형의 맬웨어를 투입하여 사용자의 자격 증명, 브라우저 기록, 민감한 문서 등을 도용할 수 있다는 점에 주목해야 합니다. 수집된 데이터는 다른 이메일 계정으로 스팸을 보내는 데 사용되어 사이버 공격의 주기가 계속 증가하고 있습니다. 한편 두 번째 소규모 피싱 캠페인은 이와 동시에 정보 도용에 사용되는 Lokibot을 통해서 중요한 코로나19 예방 조치를 제공한다는 명목으로 인도네시아에서 확산되었습니다.

마이터 어택(MITRE ATT&CK) 기법: 스피어피싱 첨부(T1193) | PowerShell(T1086) | 스크립팅(T1064) | 레지스트리 실행 키/시작 폴더(T1060) | NTFS 파일 속성(T1096) | 파일 또는 정보 난독 처리 해제/디코딩(T1140) | 난독 처리된 파일 또는 정보(T1027) | 레지스트리 수정(T1112) | 시스템 네트워크 구성 탐색(T1016) | 프로세스 탐색(T1057) | 원격 파일 복사(T1105) | 표준 애플리케이션 계층 프로토콜(T1071)

코로나19를 주제로 한 사이버 활동 (2020년 2월에 확인)

2020년 2월 초순부터 중순까지, 현재까지도 출처가 밝혀지지 않은 코로나19 피싱 캠페인 두 건을 통해 원격 액세스 트로이 목마(RAT: Remote Access Trojans)인 Nanocore(S0336) 및 Parallax가 배포되었다고

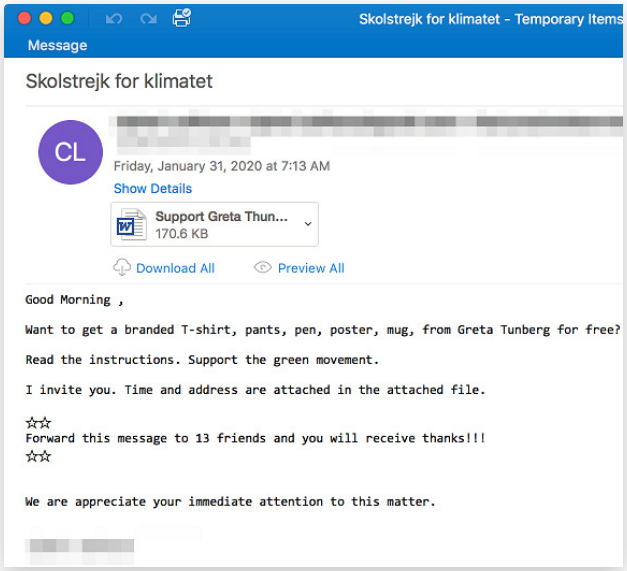

그림 3. Emotet 관련 피싱 캠페인(출처: Proofpoint)

보고되었습니다. 이러한 RAT는 일반적으로 사이버 공격자에게 키 입력, 파일, 웹캠 피드, 파일 다운로드 및 실행을 위한 원격 액세스를 제공합니다.

마이터 어택(MITRE ATT&CK) 기법: 스피어피싱 첨부(T1193) | 예약 작업(T1053) | 레지스트리 실행 키/시작 폴더(T1060) | 가상화/샌드박스 회피(T1497) | 숨겨진 창(T1143) | 소프트웨어 패킹(T1045) | 시스템 시간 탐색(T1124) | 시스템 네트워크 연결 탐색(T1049) | 표준 애플리케이션 계층 프로토콜(T1071) | 비정상 사용 포트(T1065) | 그래픽 사용자 인터페이스(T1061) | 숨겨진 파일 및 디렉터리(T1158) | 프로세스 주입(T1055) | 위장(T1036) | 보안 도구 비활성화(T1089) | 난독 처리된 파일 또는 정보(T1027) | DLL 사이드로딩(T1073) | 입력 캡처(T1056) | 프로세스 탐색(T1057) | 애플리케이션 창 탐색(T1010) | 보안 소프트웨어 탐색(T1063) | 원격 시스템 탐색(T1018) | 데이터 암호화(T1022) | 표준 암호 프로토콜(T1032) | 원격 액세스 도구(T1219) | 표준 비애플리케이션 계층 프로토콜(T1095)

미국 질병통제예방센터(CDC)의 권고를 중심으로 확산된 네 번째 피싱 캠페인은 2020년 2월 초에 최초로 보고되었습니다. cdc-gov[.]org 및 cdcgov[.]org라는 URL을 활용한 해당 캠페인은 CDC가 "미국 국내 및 국제 공중보건 대응을 조정하기 위한 관리 시스템을 구축했다"고 주장하거나 수신자가 비트코인을 기부하도록 촉구하는 등 설득력이 강한 피싱 이메일을 사용했습니다(그림 4).

마이터 어택(MITRE ATT&CK) 기법: 스피어피싱 링크(T1063)

2020년 2월 중순에는 자격 증명 도용으로 잘 알려진 AZORult(S0344)를 확산하는 피싱 캠페인(T1193)이 운송 산업에 대한 우려를 주제로 삼았다고 보고되었습니다. 구체적인 사이버 공격자는 아직 밝혀지지 않았으나 러시아 또는 동유럽에서 비롯되었을 가능성이 높습니다. 또한 이와 동시에 AZORult를 활용하는 그 외 관련 캠페인에서는 세계보건기구(WHO), 호주의료협회, 미국 질병통제예방센터(CDC) 및 여러 민간 기업과 관련하여 코로나19에 관한 잘못된 정보 및 음모 이론을 확산하고 있었던 것으로 나타났습니다(그림 5).

마이터 어택(MITRE ATT&CK) 기법: 스피어피싱 첨부(T1193)

2월 말에는 우크라이나 공공보건센터를 사칭하여 무기화 파일이 첨부(T1193)된 **Коронав□русна □нфекц□я**

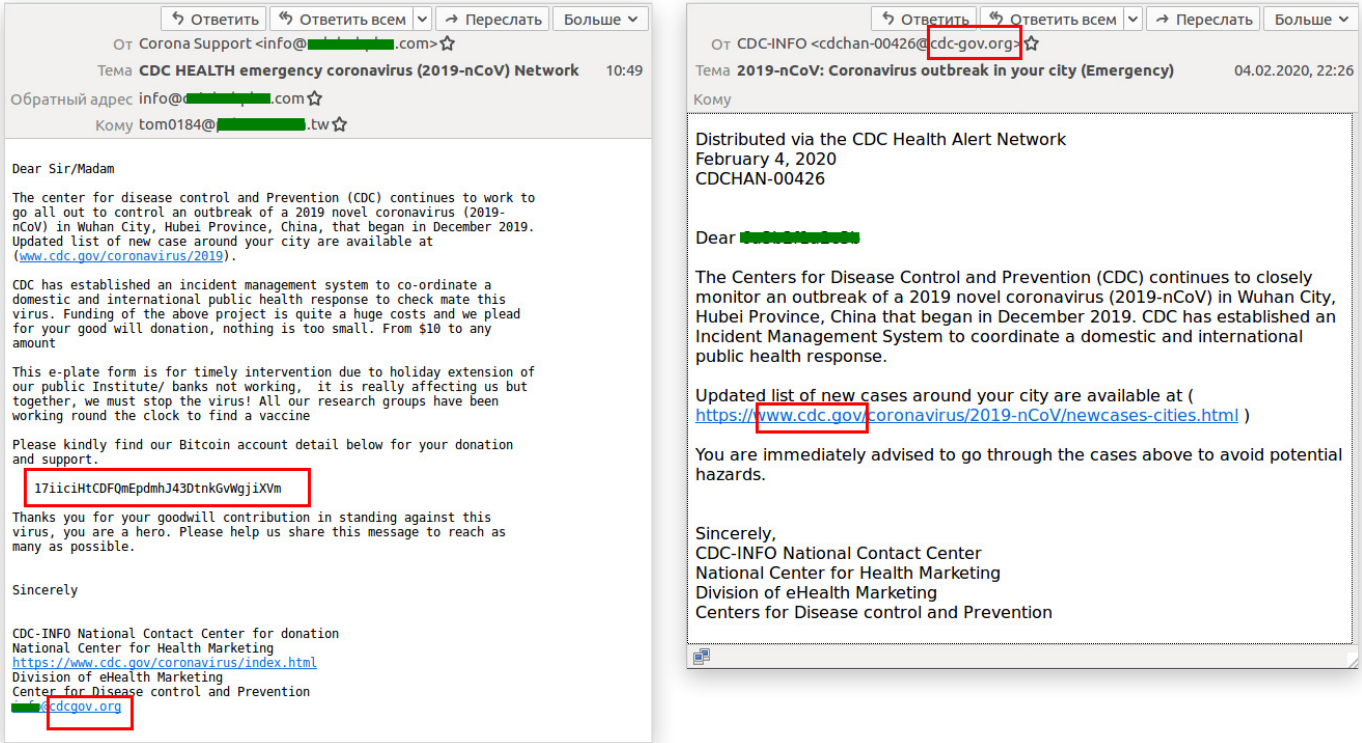

그림 4. CDC 관련 피싱(출처: Kaspersky)

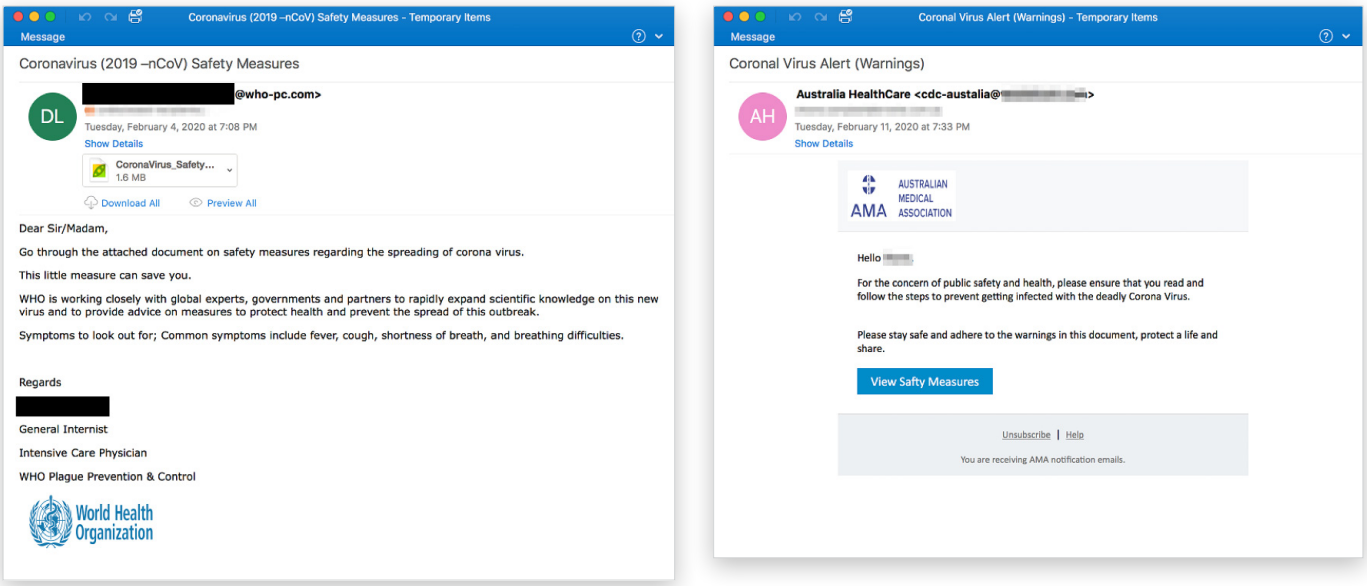

그림 5. AZORult 관련 피싱 이메일(출처: Proofpoint)

COVID-19.rar이라는 제목의 코로나19 관련 스피어피싱 이메일이 전송되었으며, Hades APT 또는 TEMP. Armageddon이라고 알려진 사이버 공격자와 연관된 것으로 보여지는 맬웨어 전송 방식을 활용했다고 합니다. 해당 단체는 출처가 모호하나 러시아의 국익을 지원하는 활동을 진행하는 것으로 추측되고 있습니다.

마이터 어택(MITRE ATT&CK) 기법: 스피어피싱 첨부(T1193) | 명령줄 인터페이스(T1059) | 쿼리 레지스트리(T1012) | 시스템 정보 탐색(T1082) | 동적 데이터 교환(T1173) | 난독 처리된 파일 또는 정보(T1027) | 스크립팅(T1064) | 프로세스 주입(T1055) | EWMI: Extra Window Memory Injection(T1181) | 레지스트리 수정(T1112)

지난 2월 27일 Anomali 연구진은 최초로 중국 기반 사이버 위협 단체인 Mustang Panda를 밝혀냈습니다. 해당 단체는 주로 DLL 사이드로딩(T1073) 및 Cobalt Strike(S0154) 전송을 위한 실행 파일(tencentsoso.exe)을 배포하도록 설계된 맬웨어로 대만 사용자를 공격합니다. Anomali에서 보고한 바 있는 Mustang Panda 활동에 대한 추가 정보는 여기에서 확인할 수 있습니다. 이와 거의 유사한 시점에, 위와는 무관한 북한의 국익과 관련된 맬웨어(아기상어)가 코로나19 대응과 관련된 대한민국 문서에 포함된 것이 밝혀졌습니다. 아기상어(S0414)는 비교적 단순한 Microsoft의 Visual Basic(VB) 스크립트 기반 맬웨어로, 2019년 11월부터 활동한 것으로 알려졌으며 북한 위협 단체 킴수키(Kimsuky)가 활용하고 있습니다.

마이터 어택(MITRE ATT&CK) 기법: 스피어피싱 첨부(T1193) | DLL 사이드로딩(T1073) | 템플릿 주입(T1221) | 동적 데이터 교환(T1173) | 원격 파일 복사(T1105) | 일반 사용 포트(T1043) | 클라이언트 실행 악용(T1203)

코로나19를 주제로 한 사이버 활동(2020년 3월에 확인)

3월 초, 사이버 보안 기업 Checkpoint는 코로나19를 주제로 한 도메인 등록이 다른 기타 주제와 비교했을 때 사기 가능성이 50% 더 높다고 보고했습니다. 이는 코로나19를 주제로 한 피싱 및 잠재적 악용 가능성과 관련된 위협이 증가하고 있다는 것을 시사합니다. 같은 기간에 Proofpoint는 질병 연구를 위한 분산형 컴퓨팅 프로젝트인 Folding@home 브랜드가 피싱 캠페인(T1192)의 일환으로 Redline Stealer라는 이름의 새로운 맬웨어군을 배포하는 데 악용되었다고 보고했습니다. 캠페인의 일환으로 주로 미국 기반 의료 및 제조 조직을 대상으로 삼은 이 맬웨어는 현재 구독 시 매월 약 100 달러를 지불하는 러시아 범죄 조직 지하 포럼에서 사용되고 있습니다. RedLine Stealer는 피해자의 브라우저에서 로그인, 자동 완성, 비밀번호 및 신용카드 정보를 캡처하며 최근에는 암호화폐 콜드월렛 도용 기능도 추가되었습니다.

또한 3월 초에는 중국 위협 단체 Mustang Panda가 대만 및 베트남을 대상으로 코로나19와 관련된 유인 문서에서 Cobalt Strike 및 PlugX RAT를 페이로드로 활용하고 있는 것으로 관찰되었습니다.

마이터 어택(MITRE ATT&CK) 기법: 스피어피싱 링크 (T1192) | 명령줄 인터페이스(T1059) | API를 통한 실행 (T1106) | 루트 인증서 설치(T1130) | 레지스트리 수정 (T1112) | 파일 자격 증명(T1081) | 자격 증명 덤핑(T1003) | 쿼리 레지스트리(T1012) | 시스템 정보 탐색(T1082) | 이메일 수집(T1114) | 비정상 사용 포트(T1065)

3월 중순, 보안 연구진은 존스홉킨스대학의 코로나바이러스 맵을 모방하여 사용자가 최신 정보 업데이트를 받기 위해 Windows 애플리케이션을 다운로드하고 실행하도록 유도하는 복제 웹 사이트를 발견했습니다. 사용자가 애플리케이션을 설치하면 시스템이 개인정보와 비밀번호 및 신용카드 정보와 같은 민감한 정보 도용 목적의 AZOrult 맬웨어에 감염됩니다. 결과적으로, 사이버 공격자는 맬웨어를 사용해 추가 맬웨어를 설치하고 숨겨진 백도어를 만들어 피해자의 시스템에 대한 추가 액세스를 확보할 수 있습니다. 또한 3월 중순 Anomali는 그 외 알려진 APT 단체와 유사한 감염 체인을 사용한 악성 .lnk 파일을 파악하고 한국 기반 위협 단체 히개사(Higaisa)와의 연관 가능성을 확인했습니다. 해당 공격 프로세스에는 PlugX 페이로드가 포함된 WHO의 PDF 문서 전송이 포함되었습니다.

마이터 어택(MITRE ATT&CK) 기법: 드라이브바이 침해 (T1189) | 명령줄 인터페이스(T1059) | API를 통한 실행 (T1106) | 예약 작업(T1053) | 숨겨진 파일 및 디렉터리 (T1158) | 파일 권한 수정(T1222) | 루트 인증서 설치 (T1130) | 파일 자격 증명(T1081) | 자격 증명 덤핑(T1003) | 쿼리 레지스트리(T1012) | 이메일 수집(T1114)

그 후, 얼마 되지 않아 몽골의 공공 부문이 코로나19를 주제로 한 피싱 이메일로 인해 피해를 보았으며 그 배후에는 Vicious Panda라는 사이버 공격자가 "Royal Road" Rich Text Format(RTF) 무기화를 활용한 것으로 나타났습니다 (그림 6). Royal Road는 이전부터 여러 중국 기반 위협 단체로 추정되어 왔으며, 최근 몽골을 대상으로 한 시도가 있기 전에 벨라루스, 러시아, 우크라이나를 대상으로 한 공격이 있었던 것으로 알려져 있습니다. 중국 위협 단체의 Royal Road RTF 무기화 활용에 대해 자세히 알아보려면 Anomali 블로그로 이동하여 여기 및 여기를 참조하십시오.

마이터 어택(MITRE ATT&CK) 기법: 스피어피싱 첨부 (T1193) | Office 애플리케이션 시작(T1137) | 쿼리 레지스트리(T1012) | 레지스트리 실행 키/시작 폴더 (T1060)

또한 3월 중순에는 미국에서의 코로나19 관련 보고 사례가 증가하고 있는 가운데 어배너 샘페인(일리노이주) 공공보건지구 역시 NetWalker(Mailto 또는 Kazakavkovkiz로도 알려져 있음)를 활용한 랜섬웨어

Original

МОНГОЛ УЛСААС БНХАУ-Д СУУГАА
ЭЛЧИН САЙДЫН ЯАМ

ШУУРХАЙ МЭДЭЭ

2020 оны 1 дүгээр сарын 22-ны өдөр | №ШМ072004 | Бээжин хот

Шинэ коронавирусын халдварын тархалтын тухай

БНХАУ-ын Төрийн эвлэлийн Хэвлэл мэдээллийн албанаас өнөөдрийн 10.00 цагт хийсэн хэвлэлийн бага хурлын үеэр Хятад улсад шинэ коронавирусын халдварт хатгалгаагаар өвчилсөн 440 хүн байгаа бөгөөд 9 нас барсан тохиолдол байгааг мэдээллэв.

Хятадын Үндэсний зөвлөл мэндийн хорооноос гаргасан статистик мэдээллээр өнөөдрийн байдлаар Хятад улсын өмнөд болон зүүн өмнөд хэсгийн 14 муж, хот мөн АНУ, Япон, Өмнөд Солонгос, Австрали (тус бүр 1), Сингапур (7), Тайланд (2) зэрэг улсад тархсан байна. Вирусын тархалтын явц хурдан байгаа бөгөөд дээрх 440 өвчтөний ойрын хүрээнийт 2197 хүнд тандалт хийж, 765 хүний халдваргүйг тогтоож, 1394 хүнийг үргэлжлүүлэн хянаж байна.

Шинэ коронавирусын халдварын талаарх шуурхай мэдээллийг үргэлжлүүлэн хүргэх болно.

Эх сурвалж: Хятадын Ардын өдрийн сонин цахим мэдээ

БОЛОВСРУУЛСАН: [redacted]

[redacted]

Translated (Automatically)

MONGOLIA FROM MONGOLIA TO CHINA
Ministry of Foreign Affairs

FAST NEWS

20 January 20 , 2004 No. SHM07 2004 Beijing

the 22nd day of the city

About the spread of new coronavirus infections

The State Council Media Service of the PRC informed at a press conference today at 10.00 a.m. that there are 440 people with the new coronary artery disease in China, and 9 have died.

According to statistics released by the National Health Committee of China, to date, it has spread to 14 provinces and cities in the southeast and southeast of China, as well as to the United States, Japan, South Korea, Australia (1), Singapore (7) and Thailand (2). The spread of the virus is rapid, with a total of 2197 surveys in the immediate vicinity of the 440 patients, 765 infected have been identified, and 1394 have been continuously monitored.

Instant updates on new coronavirus infections will continue to be provided.

Source: Chinese People's Day Newspaper

[redacted] / Temporary Provider /

[redacted]

그림 6. 몽골 공공 부문 대상(출처: Checkpoint)

공격으로 피해를 입었습니다. 이는 Microsoft Windows 10에서 실행되며 기업을 대상으로 하는 비교적 새로운 형태의 맬웨어입니다. 이틀 후에는 체코에서 코로나19 검사를 진행하는 브르노 대학병원이 불특정 랜섬웨어 공격으로 피해를 입었습니다. 이러한 랜섬웨어 공격이 현재 사이버 공격의 선봉에 서 있는 것처럼 보여 의료 조직과 시설에서는 급증하는 코로나19 의료 조치에 대응하면서 증가하는 랜섬웨어 공격에도 대비해야만 합니다.

마이터 어택(MITRE ATT&CK) 기법: 명령줄 인터페이스(T1059) | API를 통한 실행(T1106) | 모듈 로드를 통한 실행(T1129) | 예약 작업(T1053) | 사용자 실행(T1204) | 브라우저 확장(T1176) | 파일의 자격 증명(T1081) | 자격 증명 덤프(T1003) | 쿼리 레지스트리(T1012)| 시스템 정보 탐색(T1082) | 이메일 수집(T1114) | 비정상 사용 포트(T1065) | 대규모 공격을 위해 암호화된 데이터(T1486) | 시스템 복구 억제(T1490)

한편, 오랫동안 사이버 스파이 공격자로 활동하고 있는 APT36은 파키스탄의 군사 및 외교적 이익을 지원하기 위해 정보 수집을 수행하고 있으며, 인도 정부를 사칭한 가짜 코로나19 건강 권고를 수단으로 활용하여 Crimson RAT(S0115) 변종 맬웨어를 배포하고 있습니다.

마이터 어택(MITRE ATT&CK) 기법: 스피어피싱 첨부(T1193) | 스크립팅(T1064) | 시스템 정보 탐색(T1082) | 프로세스 탐색(T1057) | 파일 및 디렉터리 탐색(T1083) | 비정상 사용 포트(T1065) | 후킹(T1179)

마지막으로, 3월 16일 사이버 보안 기업 ESET은 2가지 종류의 맬웨어에 의한 감염 사례 2,500건이 모두 코로나19를 주제로 한 이메일에서 7시간 만에 발생했으며, 이는 스페인, 포르투갈, 체코, 말레이시아 및 독일을 겨냥한 코로나19 관련 활동이 크게 증가했다는 점을 시사한다고 밝혔습니다. 또 다른 사이버 보안 선두 기업인 Proofpoint는 잘 알려진 위협 공격자 TA505 및 TA564가 동일한 시점에 미국과 캐나다에 있는 사용자를 대상으로 벌인 활동이 크게 증가했음을 자체적으로 확인했다고 밝혔습니다. Proofpoint에 따르면 가장 큰 타격을 받은 산업은 의료, 제조 및 제약 산업이었습니다.

마이터 어택(MITRE ATT&CK) 기법: 스피어피싱 첨부(T1193) | 스피어피싱 링크(T1192) | 모듈 로드를 통한 실행(T1129) | 쿼리 레지스트리(T1012)

코로나19 관련 사이버 위협 방어 대책

Anomali는 사이버 범죄 및 테러 지원국 공격자가 코로나19를 주제로 한 이메일을 토대로 계속 공격하여 수신자에게 트로이목마 첨부파일을 다운로드하도록 유도하거나, 재정 관련 또는 국익 관련 목표에 따라 악성 링크를 클릭하도록 유도할 것이라고 확신하고 있습니다. 악성 활동이 급증함에 따라, 많은 정부에서 사회적 거리두기를 장려하고 기업이 원격 업무를 수행하고 있기에 위협 공격자가 악용할 기회 역시 증가하여 사용자와 기업이 처한 전반적인 위험도 증가하고 있다고 판단됩니다. 이에 따라 피싱 공격으로 인한 피해를 방지할 수 있는 몇 가지 권장 사항을 알려드립니다.

- 신뢰할 수 없는 사용자로부터 받은 원치 않는 코로나19를 주제로 한 이메일 또는 SMS(문자) 메시지를 경계하고 합법적인 정부 기관 또는 조직을 가장하여 수신자가 즉시 동작을 취하도록 유도하는 메시지에 유의하십시오.
- 수신자가 개인 식별 정보 또는 기타 중요한 기밀 정보를 요청하는 의심스러운 사이트를 방문하도록 요청하는 경우 첨부 파일을 열거나 포함된 하이퍼링크를 클릭하지 마십시오. 웹 브라우저에 올바른 주소를 입력하여 합법적인 웹 사이트로 이동하는 것이 언제나 가장 안전합니다.
- 항상 합법적인 웹 사이트가 제대로 표시되는지 웹 사이트 주소를 확인하십시오. 대상 컴퓨터에서 요청된 사이트로 이동된 정보가 암호화된 것을 나타내는 주소 표시줄 왼쪽 상단에 있는 자물쇠를 보고 합법적인 웹 사이트라고 맹목적으로 신뢰해서는 안 됩니다.
- 운영 체제 및 애플리케이션은 항상 즉시 최신 패치로 업데이트하십시오.
- 바이러스 백신 및 방화벽 솔루션을 사용하고 최신 패치 및 바이러스 백신 서명을 항상 최신 상태로 유지하십시오.

- 기업은 지속적인 사용자 보안 인식 교육 및 커뮤니케이션을 통해 직원이 의심스러운 활동을 파악하고 이를 보고하는 방법을 알 수 있도록 해야 합니다.
- Anomali 주간 위협 브리핑 및 그 외 사이버 뉴스 기사와 블로그를 구독하여 최신 사이버 보안 위협 상황을 파악하는 것이 좋습니다.
- 가능한 경우 이러한 사이버 공격에 대한 경고를 받으면 ISAC(정보 공유 분석 센터) 또는 관련 보안 이해 단체 등의 보안 채널을 통해 신뢰할 수 있는 파트너 간에 침해지표(예: 보낸 사람 이메일 주소, 보낸 사람 IP 주소, 포함된 하이퍼링크, 악성 첨부파일 및 전술, 기법 및 절차)를 공유하십시오. 자세한 내용은 여기를 참조하십시오.

또한 다양한 정부 기관에서 제공하는 안전한 지침에 따라 코로나19 관련 사이버 위협을 방어하는 것이 좋습니다.

- 사이버 보안 및·인프라 보안기관(CISA)
  - 코로나19 사이버 사기 방어 대책
  - 신종 코로나바이러스 리스크 관리(코로나19)
- 국립사이버보안센터(NCSC)
  - 재택근무: 조직 및 직원 대처
- 호주신호정보국(ASD)의 호주사이버보안센터(ACSC)
  - 코로나19 대응의 핵심은 사이버 보안입니다