Advisory report on Vaccine Internet Survey Malspam

Date: 31st May, 2021
Problem ID & Name: Vaccine Internet Survey Malspam
Severity: Medium - High

Executive Summary

The ICEDID malware, first appeared in cyberspace as banking trojan in 2017 has now evolved into a infamous point of entry for threat actors motivated to target financial institutions for credential theft and data exfiltration.

During the earlier phase of ICEDID, it was deployed to primarily target banking credentials, credit card info etc. In the year of 2020 it was observed that ICEDID had evolved and was now able to perform common post-exploitation techniques and provide access to the threat actor and ultimately become severe ransomware. The main use of malware had now diverted towards post-exploitation techniques rather than credentials theft and data exfiltration.

Description

ICEDID is propagated via malspam emails that usually contain Office file attachments. These files are created with the use of microsoft macros. Macros are a feature of Microsoft office suite that can allow run commands or make changes to the system. Thus employing this technique the ICEDID malware fetches and runs the malicious payload. In February 2020 campaigns, maldocs were spread via spam and first dropped a malware called OStap malware which later in turn dropped the ICEDID malware. The ICEDID malware seems to have a connection with the Emotet gang.
The spread of ICEDID maldoc via spam has been consistent since it emerged. It has a main focus on the financial sector e-commerce and social media platforms. The ICEDID malware targets business users and business banking services.

The ICEDID malware that arose in 2021 was veiled as COVID Vaccine Survey and incited clients to empower macros to "decrypt" the record. This phishing style of the malware isn’t something however camouflaging as COVID Vaccine Survey is another received method.
Once the macros are enabled the malware downloads the malicious payload and runs it on the system. This malicious payload allows threat actors to steal information from the system. The domain on which the command and control server was hosted on was registered on 22nd March of 2021 thus this wave malspam must have started after then and observing the ip patterns and style of attack used in malware campaigns, the malware must have originated in Russia or Eastern Europe. The threat actors behind the campaign are likely to conduct these kinds of attacks in future. Thus deploying suitable measures and defences can stop you from being low hanging fruits for threat actors.

**Indicators of Compromise**

While analysing the IOC as given below came across some information such as:

**Md5:** 64e68e164ce33048d946ee797b59138f  
**Sha1:** d4cda4985f8b8c104dc96d4f14367c89aa1475c0  
**SHA-256:** 71e76bc250307330ae3c7f6a3dab344304f4a1fe8e4d91097ebbe4de5523a295  
**Vhash:** d3de453bab61b94b0e6ea2b66bb328a0  
**SSDeep:** 3072:hP4IUQsxT2sa1fJjVeeJyUwaCR+6r9U2bg3SyvN:K3dxohyZRR+T2bg3SyvN  
**TLSH:** T196C3126AA201CB9E4706B9DB1F7CFD402510DE7124D2944EF9FA8B470B4F6E191987B8  
**File type:** ZIP
MD5: 64e68e164ce33048d946ee797b59138f
SHA1: d4cda4985f8b8c104dc96d4f14367c89aa1475c0
Sha256: 71e76bc250307330ae3c7f6a3dab344304f4a1fe8e4d91097ebbe4de5523a295
Vhash: d3de453bab61b94b0e6ea2b66bb328a0
SSDeep: 3072:hp4IUQsxT2sa1f1jVeeJyUwaCR+6r9U2bg3SyvN:K3dxohyZRR+T2bg3SyvN

Detailed Static Analysis

Analysis of Contract_1720581471.xlsm

File identification

MD5: af5d5a7a7d1d5e1a27a81a6eaa2c071b
SHA1: 9f35820fb5187b3fb98dd9e8cf08b94f579abf06
Sha256: 71d51851078cd16a46ed93fa6fb95a5fbb15514560d3698c727ccf027d141274
Sha512: 3715e0f2fe1be-baa2829b2429073de65c93461c91793f34227d2389703594673044e121de38f082f8d66d80e6f9c908ba02ef1a1b5a15340abb66d50454b01d

SSDeep: 3072:CGJuulZ+jR5GccccccccccccccccjsgLzowOhb1jxILT+yw7h:CG-Js06ccccccccccccccccgUU/hUH+yw9,”malspam.xlm”

Size: 138195 B
First Seen: Tue, 13 Apr 2021 21:37:12 GMT

Virus Total:
https://www.virustotal.com/gui/file/71d51851078cd16a46ed93-fa6fb95a5fbb15514560d3698c727ccf027d141274/details

Inquest Labs:
https://labs.inquest.net/dfi/sha256/71d51851078cd16a46ed93-fa6fb95a5fbb15514560d3698c727ccf027d141274

Malicious File Summary

The malware uses a technique that employs the **NOW()** macro function to allow the download of files from certain time zones only. This malware could possibly be of the *icedID* family as it used a fairly similar technique.

The malware opens up like a phishing document and states that in order to “decrypt” the document you need to enable macros.

![The preview of the xlsx file](image-url)
The malware is macro based that uses rundll32.exe to load a malicious dll into the machine and then run a function called DllRegisterServer.

It registers **URLDownloadToFileA** API call from the Urlmon.dll with a custom name **Belandes** using the register function. It also concatenates strings using **CONCATENATE** function with 3 arguments:

1. Beginning of the urls (there are 3 IP in total)
2. Current date and time using **NOW()** macro function
3. The trailing extension “.dat”

Here the entire use of **NOW()** is that the sample wont download if the time isn’t correct. So I’m guessing this could be a method to implement the geo-fencing technique and affect only part of the world.
The URLs generated with the macro functions download the payload and save it as ..Hodas.vyur2, which is basically a dll that is later run with the help of rundll32. Pretty straight forward stuff.

Network Communication

The malware tries to download dll files from 3 different IP’s in total as follows:

- **188.127.254.156**
  - route: 188.127.254.0/24
  - descr: DHUB-CUST
  - origin: AS56694
  - inetnum: 188.127.254.0 - 188.127.254.255
  - country: Russia
  - address: Moscow, Starovatutinsky prospect, 17.
  - address: 1st floor, room 5
  - phone: +7 495 565 37 44
  - abuse-mailbox: @smartape.ru
  - nic-hdl: STFU1-RIPE

- **195.123.245.91**
  - route: 195.123.244.0/22
  - origin: AS204957
  - inetnum: 195.123.244.0 - 195.123.247.255
  - country: Czechia
  - geoloc: 50.069689 14.462943
  - org: ORG-GFL1-RIPE
  - organisation: ORG-GFL1-RIPE
  - org-name: Green Floid LLC
  - address: East Jefferson Street, 2707
  - address: Orlando, FL, 32803, USA
  - phone: +1 561 2500001
  - person: GREEN FLOOD EU Support Team
  - address: East Jefferson Street, 2707
  - address: Orlando, FL, 32803, USA
  - phone: +1 561 2500001
  - phone: +359 2 4925555
74.119.193.131
route: 74.119.193.0/24
origin: AS135330
inetnum: 74.119.193.0 - 74.119.193.255
country: Hong Kong
address: Republic of Moldova, Chisinau
address: str. Nicolae Dimo, 23/3, office 32
phone: +373 69979988
abuse-mailbox: abuse@pq.hosting

Further the files its downloaded are saved with the following names:

- ..\Hodas.vyur2
- ..\Hodas.vyur1
- ..\Hodas.vyur

Since the ips are down if you run the document now, this is the error that will pop up.

![Error message](image)

Error Stating dll not found in a malicious document
**DLL Analysis**

**Hodas.vyur Analysis (Malicious DLL)**

**File Info**

**Md5:** 0b00d514b6484a16d706d6098c336b44  
**Sha1:** 8e6b942430896c760eb54f87c8395b02284a4e24  
**Sha256:** 0bfbe59ac91d909de8ef5d3899409bf34dc7636972a6e65154cab44c85a8adee  
**SSDeep:** 1536:Vq8ByBeZnwLG+NoV1XjeNSazilz7Ja5j/Nj/Ix0Zcq+M6qacZZ-tr2wS+FJZLT:Q8+Kjv4RECZnrDSGZn

**Compilation Time (Taken for headers):** Thu 1 April 2021 12:10:19 UTC

By the time we got a malware sample the ip's hosting the malicious dll were already down. But since we know this malware belongs to the icelD family and does mostly the same thing as his other siblings, we can take a look at the dll with the same name found here.

[https://bazaar.abuse.ch/sample/0bf-be59ac91d909de8ef5d3899409bf34dc7636972a6e65154cab44c85a8adee/](https://bazaar.abuse.ch/sample/0bf-be59ac91d909de8ef5d3899409bf34dc7636972a6e65154cab44c85a8adee/)

Looking at the virtual size and raw size shows us that the dll was not packed.

![Size table of dll in CFF explorer](image)

**Exported Functions**

The excel macro was running the DllRegisterServer function from the dll. On analyzing it is found the dll contains one more export function called “**PluginInit**” that could have been used.

The malware seems to be written by a competent author as it has few tricks that make it hard to analyze and the encoding scheme used by the malware causes much trouble when reversing.
Exported Functions

Imported DLLs

Summary of the DLL Working

The dll once executed will try to contact the c2 framework located at the stoikoplot.xyz domain. The c2 must have been hosted on an aws instance that is why a dns query to the aws.amazon.com is made.
DNS requests captured for the domain in Wireshark

Once the IP is resolved, a request to the stoikoplot.xyz is made to verify the existence of the c2 framework. The dll follows a complex encryption scheme for all its strings and uses the method of dynamic allocation to load and call various dll during runtime.

Assembly code for Allocating and Writing to process

The purpose of dll is to collect data from the host, encrypt it and send it over the http protocol to the c2 server hosted at the stoikoplot.xyz domain. Thus if you notice huge amounts of http traffic being generated towards an aws host, it is very likely that you have been infiltrated.

Command And Control Server Information

**Name:** stoikoplot.xyz  
**Registry Domain ID:** D229431128-CNIC  
**Nameservers:** ns1.taco-salad.com  
ns2.taco-salad.comDates

---

CyberPeace Research
The domain on which the command and control was hosted on was registered on 22nd March of 2021 thus this wave malspam must have started after then and observing the ip patterns and style of attack used in malware campaigns, the malware must have origin in Russia or Eastern Europe. The threat actors behind the campaign are likely to conduct these kinds of attacks in future. Thus deploying suitable measures and defences can stop you from being low hanging fruits for threat actors.

Mitigation Strategy and techniques

This attack was based entirely on the phishing vector and social engineering. Thus As per recommendation and mitigation:

Specific Recommendations

Use The Following Yara Rule For Malicious Excel Document Detection

```python
import "hash"
rule covid_vaccine_malspam {
   meta:
      description = "Detects covid 19 vaccine malspam"
      organisation = "cyberpeace"
      date = "2021-05-21"

   strings:
      $magic = { 50 4b }
      $image = "xl/media/image1.jpeg"

      $macro1 = "xl/microsheets/sheet1.xmlPK"
      $macro2 = "xl/microsheets/sheet2.xmlPK"
      $macro3 = "xl/microsheets/sheet3.xmlPK"
      $macro4 = "xl/microsheets/sheet4.xmlPK"

   condition:
      ($magic and $macro1 and $macro2 and $macro3 and $macro4 and $image) or
      hash.sha256(0, filesize) == "71d51851078cd16a46ed93fa6fb95a5fbb15514560d3698c727ccf027d141274"
}
```
Block Outbound Connections to IP Mentioned in IOCs

A firewall rule that stops any computer inside the network to communicate with these IPs will stop the process of data exfiltration if the malware has already compromised the network. Thus creating such firewall rules will help in stopping the malware.

Restrict The Command And Control Domain at Gateway Level

The malware has a specific domain to which it reaches out to in order to exfiltrate data and if that domain is unreachable the data is not exfiltrated. Thus blocking the mentioned domain will actually result in stopping the malware executing completely.

Scan For Malicious Files and Suspected DLL At Endpoint Device

Malware downloads files from the internet when it executes the macro. Thus scanning each system on your network for these files can help reduce the malware spread in the network.

Generic Recommendations

Utilize a Next-Generation Antivirus Solution for Your Enterprise

What makes Emotet malware so difficult to kill is the way that it was intended to dodge conventional record based antivirus discovery. Hence, you should introduce a more powerful piece of programming that can stay aware of and secure your association against developed dangers.

Continuously Apply Software Updates and Patches When Released

Weaknesses seem when fundamental programming gets out of date. This makes openings in the framework that can become points of passage for a wide range of awful dangers. Along these lines, introducing vital updates when they are conveyed is a significant advance in keeping up legitimate digital cleanliness in your business organization.

There are a couple of sensible practices that ought to be imparted in your association's working environment culture consistently, for example:

- not giving log-in certifications to dubious solicitations,
- trying not to open messages from new sources,
- distinguishing counterfeit marking in messages,
checking the objective of a connection prior to opening it, also, in every case twofold checking the legitimacy of different requests.

**Square File Attachments That Are Associated with Malware**

Another digital cleanliness practice that you can authorize for the online wellbeing of your business is to hinder email connections containing record augmentations that are most ordinarily connected with malware, to be specific .dll and .exe. Make it one stride further by obstructing augmentations that can’t be as expected filtered by your antivirus, for example, .zip. This can forestall an Emotet malware contamination, as the Trojan depends on Dynamic Link Libraries in its assaults.

**Appendix of Other Malicious Associated Domains**

Due to the COVID-19 pandemic, many cybercriminals are using malicious domains for spreading malware, and malicious email spam to make handsome money out of it. Suspiciously some domains were identified as

- A1covidtesting.com
- Apexfgplc[.]com
- Apexfgplc[.]com
- Capitalone[.]online
- Capitalonechecking[.]online
- Capitaloneonlinebank[.]us
- Citifinancialsv[.]com
- Cobgservices[.]com
- Csbnkgroups[.]online
- Diamonddpbplc[.]com
- Efficient-bk[.]com
- Enodataltd[.]com
- Financegrowth[.]com
- Garantibankonline[.]com
- Globaltechdeal[.]com
- My[.]santanderinvestment[.]com
- Secure[.]tescbk[.]online
- Secure[.]tsbk[.]online
- Secured[.]bcsbank[.]online
- secured[.]by fbonline[.]com
- Swiss[.]psiconline[.]com
- Zirexbanking[.]online
References

2. https://searchsecurity.techtarget.com/definition/credential-theft
11. https://heimdalsecurity.com/blog/banking-trojan/
14. https://labs.inquest.net/dfi/sha256/71d51851078cd16a46ed93-fa6fb95a5fbb15514560d3698c727ccf027d141274
15. https://www.virustotal.com/gui/file/71e76bc250307330ae3c7f6a3-dab344304f4a1fe8e4d91097ebe4de5523a295/relations
17. https://bazaar.abuse.ch/sample/0b-fe59ac91d909de8ef5d3899409bf34dc7636972a6e65154cab44c85a8adee/

Revision Note:

<table>
<thead>
<tr>
<th>VERSION</th>
<th>DESCRIPTION</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Initial Public Release</td>
<td>Final</td>
</tr>
</tbody>
</table>

Issued by

Research wing, CyberPeace Foundation
Research Wing, Autobot Infosec Private Ltd.