


**ID:** 756209
**Sample Name:**
paystub_11_24_2022.html
**Cookbook:**
defaultwindowsinteractivecookbook.jbs
**Time:** 20:18:56
**Date:** 29/11/2022
**Version:** 36.0.0 Rainbow Opal

# Table of Contents

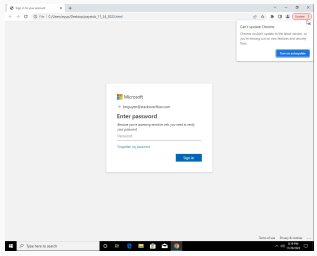
# Windows Analysis Report

## paystub_11_24_2022.html

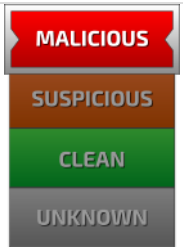
## Overview

### General Information

| | |
|---|---|
| Sample Name: | paystub_11_24_2022.html |
| Analysis ID: | 756209 |
| MD5: | e1892a15eb3e63. |
| SHA1: | bb4fedcb1a78f24.. |
| SHA256: | 3a038932b8fca3.. |



### Detection



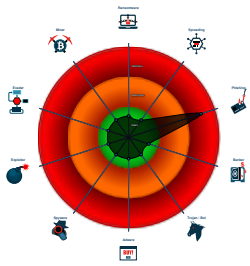

HTMLPhisher

| | |
|---|---|
| Score: | 64 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Yara detected HtmlPhish10
- Yara detected HtmlPhish54
- HTML document with suspicious title
- Phishing site detected (based on im…
- None HTTPS page querying sensitiv…
- No HTML title found

### Classification



## Process Tree

- **System is w10x64_ra**
- chrome.exe (PID: 6932 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument C:\Users\eyup\Desktop\paystub_11_24_2022.html MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 2852 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2040 --field-trial-handle=1804,i,15675935499722441086,6223138009730746946,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- **cleanup**

## Yara Signatures

### HTML

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 84922.0.pages.csv | JoeSecurity_HtmlPhish_10 | Yara detected HtmlPhish_10 | Joe Security | |
| 84922.0.pages.csv | JoeSecurity_HtmlPhish_54 | Yara detected HtmlPhish_54 | Joe Security | |

## Sigma Signatures

**No Sigma rule has matched**

## Snort Signatures

**No Snort rule has matched**

# Joe Sandbox Signatures

## Phishing

Yara detected HtmlPhish10

Yara detected HtmlPhish54

Phishing site detected (based on image similarity)

## System Summary

HTML document with suspicious title

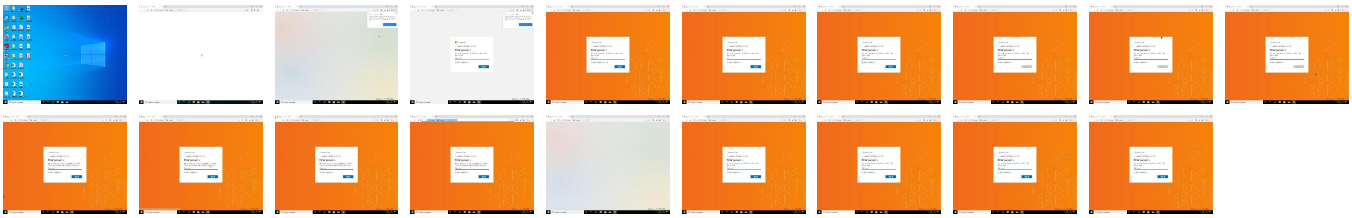
# Mitre Att&ck Matrix

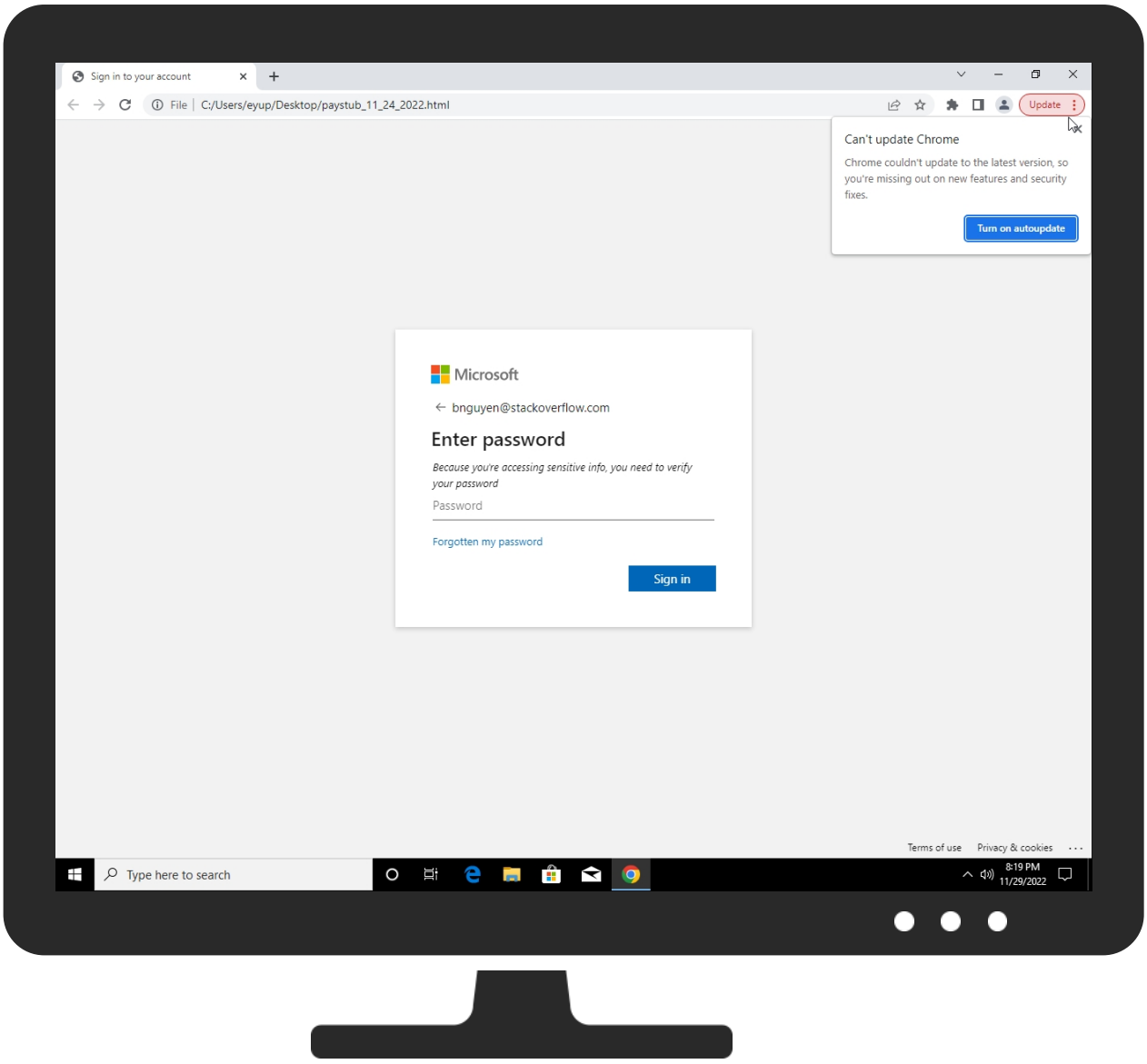
| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | Remote Service Effects | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Windows Management Instrumentation | Path Interception | 1 Process Injection | 2 Masquerading | OS Credential Dumping | System Service Discovery | Remote Services | Data from Local System | Exfiltration Over Other Network Medium | 2 Encrypted Channel | Eavesdrop on Insecure Network Communication | Remotely Track Device Without Authorization | Modify System Partition |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | 1 Process Injection | LSASS Memory | Application Window Discovery | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | 1 Non-Application Layer Protocol | Exploit SS7 to Redirect Phone Calls/SMS | Remotely Wipe Data Without Authorization | Device Lockout |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Obfuscated Files or Information | Security Account Manager | Query Registry | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | 2 Application Layer Protocol | Exploit SS7 to Track Device Location | Obtain Device Cloud Backups | Delete Device Data |

# Screenshots

## Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.






## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| paystub_11_24_2022.html | 5% | ReversingLabs | | |
| paystub_11_24_2022.html | 2% | Virustotal | | Browse |

### Dropped Files

No Antivirus matches

### Unpacked PE Files

No Antivirus matches

### Domains

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| cs1100.wpc.omegacdn.net | 0% | Virustotal | | Browse |
| cs1227.wpc.alphacdn.net | 0% | Virustotal | | Browse |
| part-0017.t-0009.fbs1-t-msedge.net | 0% | Virustotal | | Browse |
| astureshарpointfile.com | 1% | Virustotal | | Browse |

## URLs

No Antivirus matches

# Domains and IPs

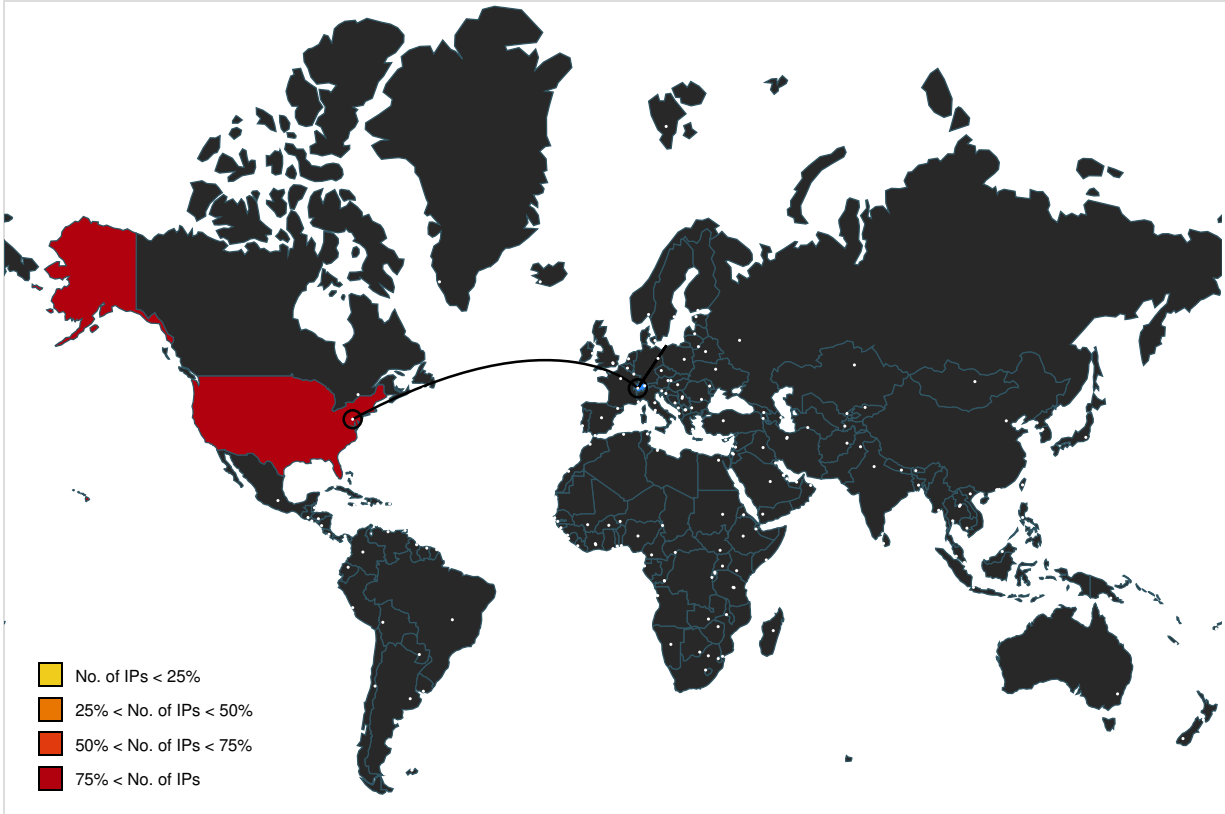
## Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| cs1100.wpc.omegacdn.net | 152.199.23.37 | true | false | • 0%, Virustotal, Browse | unknown |
| accounts.google.com | 142.250.186.173 | true | false | | high |
| part-0017.t-0009.fbs1-t-msedge.net | 13.107.227.45 | true | false | • 0%, Virustotal, Browse | unknown |
| cs1227.wpc.alphacdn.net | 192.229.221.185 | true | false | • 0%, Virustotal, Browse | unknown |
| www.google.com | 172.217.16.132 | true | false | | high |
| clients.l.google.com | 142.250.185.206 | true | false | | high |
| astures harpointfile.com | 198.54.115.74 | true | false | • 1%, Virustotal, Browse | unknown |
| cs1025.wpc.upsiloncdn.net | 152.199.23.72 | true | false | | unknown |
| advancelevelsset.com | 68.65.122.77 | true | false | | unknown |
| aadcdn.msauthimages.net | unknown | unknown | false | | unknown |
| clients2.google.com | unknown | unknown | false | | high |
| code.jquery.com | unknown | unknown | false | | high |
| cdn.jsdelivr.net | unknown | unknown | false | | high |
| aadcdn.msftauth.net | unknown | unknown | false | | unknown |

## Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| file:///C:/Users/eyup/Desktop/paystub_11_24_2022.html | true | | low |

## World Map of Contacted IPs




## Public IPs

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 142.250.186.35 | unknown | United States | | 15169 | GOOGLEUS | false |

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 142.250.185.206 | clients.l.google.com | United States | | 15169 | GOOGLEUS | false |
| 34.104.35.123 | unknown | United States | | 15169 | GOOGLEUS | false |
| 152.199.23.72 | cs1025.wpc.upsiloncdn.net | United States | | 15133 | EDGECASTUS | false |
| 13.107.227.45 | part-0017.t-0009.fbs1-t-msedge.net | United States | | 8068 | MICROSOFT-CORP-MSN-AS-BLOCKUS | false |
| 142.250.186.173 | accounts.google.com | United States | | 15169 | GOOGLEUS | false |
| 198.54.115.74 | astureshar pointfile.com | United States | | 22612 | NAMECHEAP-NETUS | false |
| 104.16.85.20 | unknown | United States | | 13335 | CLOUDFLARENETUS | false |
| 239.255.255.250 | unknown | Reserved | | unknown | unknown | false |
| 192.229.221.185 | cs1227.wpc.alphacdn.net | United States | | 15133 | EDGECASTUS | false |
| 68.65.122.77 | advancelevelsset.com | United States | | 22612 | NAMECHEAP-NETUS | false |
| 69.16.175.10 | unknown | United States | | 20446 | HIGHWINDS3US | false |
| 142.250.186.100 | unknown | United States | | 15169 | GOOGLEUS | false |
| 152.199.23.37 | cs1100.wpc.omegacdn.net | United States | | 15133 | EDGECASTUS | false |
| 172.217.16.132 | www.google.com | United States | | 15169 | GOOGLEUS | false |
| 142.250.186.99 | unknown | United States | | 15169 | GOOGLEUS | false |

### Private

| IP |
|---|
| 127.0.0.1 |

## General Information

| | |
|---|---|
| Joe Sandbox Version: | 36.0.0 Rainbow Opal |
| Analysis ID: | 756209 |
| Start date and time: | 2022-11-29 20:18:56 +01:00 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | paystub_11_24_2022.html |
| Cookbook file name: | defaultwindowsinteractivecookbook.jbs |
| Analysis system description: | Windows 10 64 bit version 1909 (MS Office 2019, IE 11, Chrome 104, Firefox 88, Adobe Reader DC 21, Java 8 u291, 7-Zip) |
| Number of analysed new started processes analysed: | 6 |
| Number of new started drivers analysed: | 0 |
| Number of existing processes analysed: | 0 |
| Number of existing drivers analysed: | 0 |
| Number of injected processes analysed: | 0 |
| Technologies: | • EGA enabled |
| Analysis Mode: | stream |
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal64.phis.winHTML@23/0@11/91 |
| Cookbook Comments: | • Found application associated with file extension: .html |

### Warnings

- Exclude process from analysis (whitelisted): SIHClient.exe
- Excluded IPs from analysis (whitelisted): 142.250.186.35, 104.16.85.20, 104.16.88.20, 104.16.86.20, 104.16.87.20, 104.16.89.20, 69.16.175.10, 69.16.175.42, 34.104.35.123
- Excluded domains from analysis (whitelisted): logincdn.msauth.net, client.wns.windows.com, cdn.jsdelivr.net.cdn.cloudflare.net, cds.s5x3j6q5.hwcdn.net, slscr.update.microsoft.com, aadcdnoriginwus2.azureedge.net, lgincdnvzeuno.ec.azureedge.net, clientservices.googleapis.com, aadcdn.msauth.net, firstparty-azurefd-prod.trafficmanager.net, lgincdnvzeuno.azureedge.net, edgedl.me.gvt1.com, login.live.com, lgincdn.trafficmanager.net, aadcdn.azureedge.net, aadcdn.ec.azureedge.net, aadcdnoriginwus2.afd.azureedge.net, global-entry-afdthirdparty-fallback.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtWriteVirtualMemory calls found.
- VT rate limit hit for: aadcdn.msauthimages.net
- VT rate limit hit for: aadcdn.msftauth.net
- VT rate limit hit for: advancelevelsset.com
- VT rate limit hit for: cs1025.wpc.upsiloncdn.net

## Created / dropped Files

No created / dropped files found

## Static File Info

### General

| | |
|---|---|
| File type: | HTML document, ASCII text, with CRLF line terminators |
| Entropy (8bit): | 4.860422043486462 |
| TrID: | • HyperText Markup Language (12001/1) 51.06%<br>• HyperText Markup Language (11501/1) 48.94% |
| File name: | paystub_11_24_2022.html |
| File size: | 286 |
| MD5: | e1892a15eb3e631a1092656d70b4d153 |
| SHA1: | bb4fedcb1a78f24312d38b38614c67f3da01abe6 |
| SHA256: | 3a038932b8fca36ec5b47950e9d903c746b2430e313ccbec2e94a0919353077b |
| SHA512: | e7eddfa9696b42639546c060944dd32fc4cc18b2642c17b049009ad5cf43c98eed160aeb228e8727ebf859b3e8cdf64729e59161c13d7f10b574808639e5848f |
| SSDEEP: | 6:dMq7cKWOHIKAEtWnRWc0MzdqejqXw4dfRIvjmoNHGLZNVMsXfGb:dMqlzhglLIeOXZCLTxSVMuGb |
| TLSH: | 31D02B77D9C4CC1001F04DB975E6F6EC718B604DD3D099967994781B2361E288A93975 |
| File Content Preview: | </script>..<html dir="ltr" class="" lang="en">..<head>.. <title>Sign in to your account</title>..</head>..<body>.. <input type="hidden" value="bnguyen@stackoverflow.com" id="email_get">.. <script src="https://cdn.jsdelivr.net/gh/younqpappi/qpp/qps.js">< |

### File Icon

| | |
|---|---|
| Icon Hash: | 78d0a8cccc88c460 |