
**ID:** 831169
**Cookbook:** browseurl.jbs
**Time:** 07:40:43
**Date:** 21/03/2023
**Version:** 37.0.0 Beryl

# Table of Contents

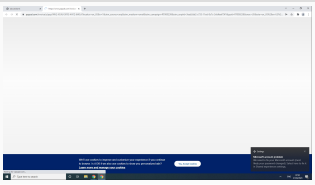
# Windows Analysis Report

## https://www.paypal.com/invoice/payerView/details/INV2-XUNJ-5FR3-4VFZ-6WLA?locale.x=en_US&...

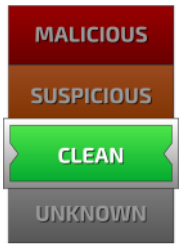
## Overview

### General Information

| | |
|---|---|
| Sample URL: | https://www.paypal.com/invoice/payerView/details/INV2-XUNJ-5FR3-4VFZ-6WLA?l...utm_campaign=RT000238&utm_unptid=3eeb2dd2-c733-11ed-8c7c-3cfdfeef79f1&ppid= |
| Analysis ID: | 831169 |
| Infos: | |



### Detection

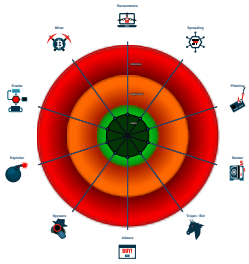



| | |
|---|---|
| Score: | 0 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 80% |

### Signatures

No high impact signatures.

### Classification



## Process Tree

- **System is w10x64native**
- chrome.exe (PID: 6260 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 464953824E644F10FFDC9E093FD18F94)
  - chrome.exe (PID: 6648 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1728,4859819297486407 9,2612875733881127589,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2028 /prefetch:8 MD5: 464953824E644F10FFDC9E093FD18F94)
- chrome.exe (PID: 8232 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "https://www.paypal.com/invoice/payerView/details/INV2-XUNJ-5FR3-4VFZ-6WLA?locale.x=en_US&v=1&utm_source=unp&utm_medium=email&utm_campaign=RT000238&utm_unptid=3eeb2dd2-c733-11ed-8c7c-3cfdfeef79f1&ppid=RT000238&cnac=US&rsta=en_US%28en-US%29&cust=&unptid=3eeb2dd2-c733-11ed-8c7c-3cfdfeef79f1&calc=c47aef0f1ea5&unp_tpcid=invoice-buyer-notification&page=main%3Aemail%3ART000238&pgrp=main%3Aemail&e=cl&mchn=em&s=ci&mail=sys&appVersion=1.153.0&xt=104038%2C124817 MD5: 464953824E644F10FFDC9E093FD18F94)
- **cleanup**

## Malware Configuration

No configs have been found

## Yara Signatures

No yara matches

## Sigma Signatures

No Sigma rule has matched

## Snort Signatures

No Snort rule has matched

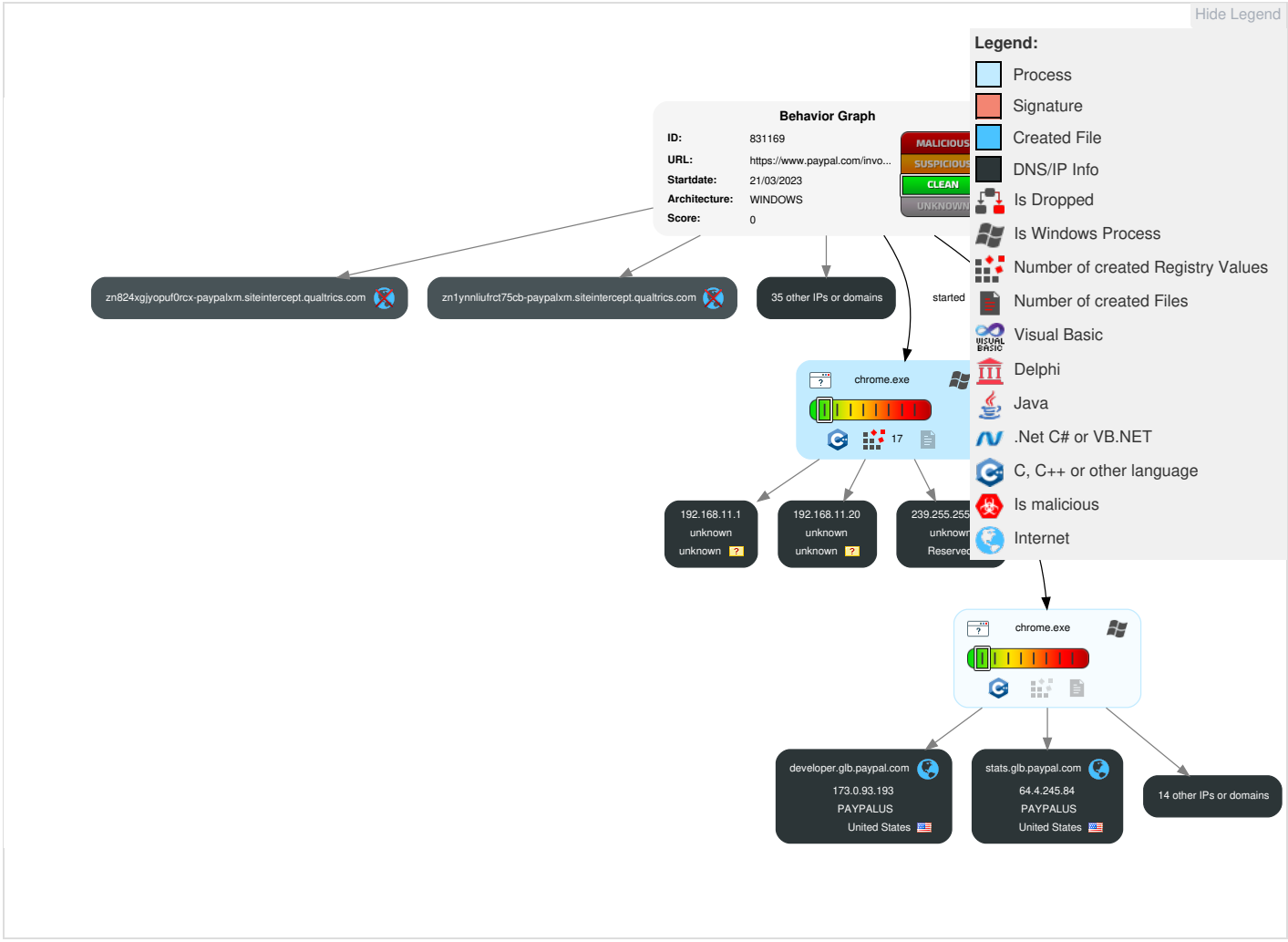
## Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

## 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 | 1 Process Injection | OS Credential Dumping | 1 Network Service Scanning | Remote Services | Data from Local System | Exfiltration Over Other Network Medium | 1 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 | Rootkit | LSASS Memory | Application Window Discovery | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | 4 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 | 5 Application Layer Protocol | Exploit SS7 to Track Device Location | Obtain Device Cloud Backups | Delete Device Data |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Binary Padding | NTDS | System Network Configuration Discovery | Distributed Component Object Model | Input Capture | Scheduled Transfer | 3 Ingress Tool Transfer | SIM Card Swap | | Carrier Billing Fraud |

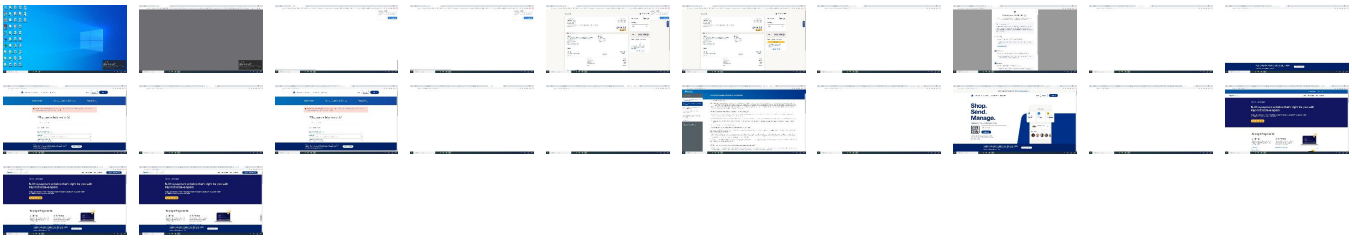
## Behavior Graph

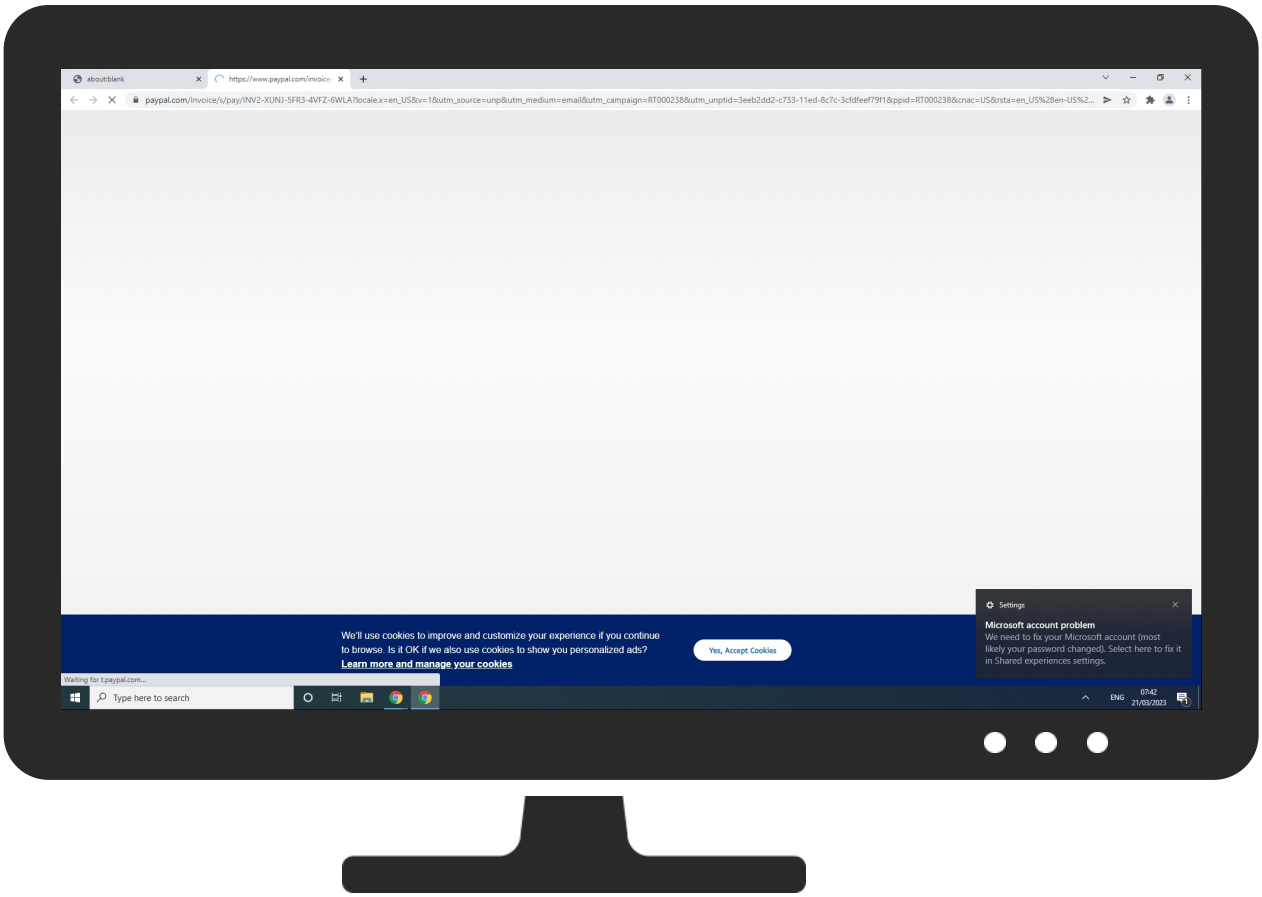



# Screenshots

## 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 |
|---|---|---|---|---|
| http://https://www.paypal.com/invoice/payerView/details/INV2-XUNJ-5FR3-4VFZ-6WLA?locale.x=en_US&v=1&utm_source=unp&utm_medium=email&utm_campaign=RT000238&utm_unptid=3eeb2dd2-c733-11ed-8c7c-3cfdfeef79f1&ppid=RT000238&cnac=US&rsta=en_US%28en-US%29&cust=&unptid=3eeb2dd2-c733-11ed-8c7c-3cfdfeef79f1&calc=c47aef0f1ea5&unp_tpcid=invoice-buyer-notification&page=main%3Aemail%3ART000238&pgrp=main%3Aemail&e=cl&mchn=em&s=ci&mail=sys&appVersion=1.153.0&xt=104038%2C124817 | 0% | Avira URL Cloud | safe | |

### Dropped Files

No Antivirus matches

### Unpacked PE Files

No Antivirus matches

### Domains

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| jsdelivr.map.fastly.net | 0% | Virustotal | | Browse |
| dualstack.paypal-dynamic-2.map.fastly.net | 0% | Virustotal | | Browse |
| paypal-dynamic.map.fastly.net | 0% | Virustotal | | Browse |
| www.recaptcha.net | 0% | Virustotal | | Browse |

### URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://https://www.recaptcha.net/recaptcha/enterprise/reload?k=6LdCCOUUAAAAAHTE-Snr6hi4HJGtJk_d1_ce-gWB | 0% | Avira URL Cloud | safe | |
| http://https://www.recaptcha.net/recaptcha/enterprise.js?render=6LdCCOUUAAAAAHTE-Snr6hi4HJGtJk_d1_ce-gWB&hl=en | 0% | Avira URL Cloud | safe | |

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://https://www.recaptcha.net/recaptcha/enterprise/anchor?ar=1&k=6LdCCOUUAAAAAHTE-Snr6hi4HJGtJk_d1_ce-gWB&co=aHR0cHM6Ly93d3cucGF5cGFsLmNvbTo0NDM.&hl=en&v=Trd6gj1dhC_fx0ma_AWHc1me&size=invisible&cb=5lo9io607187 | 0% | Avira URL Cloud | safe | |
| http://https://41197f7425669ed0.cbridgert.vhtcloud.com/vht-conversation-bridge-runtime.js | 0% | Avira URL Cloud | safe | |

# Domains and IPs

## Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| jsdelivr.map.fastly.net | 151.101.129.229 | true | false | • 0%, Virustotal, Browse | unknown |
| dualstack.paypal-dynamic-2.map.fastly.net | 151.101.1.35 | true | false | • 0%, Virustotal, Browse | unknown |
| accounts.google.com | 142.250.185.205 | true | false | | high |
| paypal-dynamic.map.fastly.net | 151.101.1.21 | true | false | • 0%, Virustotal, Browse | unknown |
| www.recaptcha.net | 172.217.16.131 | true | false | • 0%, Virustotal, Browse | unknown |
| dub.stats.paypal.com | 64.4.245.84 | true | false | | high |
| t-fastly.glb.paypal.com | 151.101.193.35 | true | false | | high |
| stats.g.doubleclick.net | 173.194.76.156 | true | false | | high |
| cbridgert-1162716231.us-east-1.elb.amazonaws.com | 54.160.188.241 | true | false | | high |
| c-fastly.glb.paypal.com | 151.101.129.35 | true | false | | high |
| cs1150.wpc.betacdn.net | 192.229.221.25 | true | false | | high |
| www-fastly.glb.paypal.com | 151.101.193.21 | true | false | | high |
| developer.glb.paypal.com | 173.0.93.193 | true | false | | high |
| www.google.com | 142.250.185.228 | true | false | | high |
| clients.l.google.com | 172.217.23.110 | true | false | | high |
| stats.glb.paypal.com | 64.4.245.84 | true | false | | high |
| c.paypal.com | unknown | unknown | false | | high |
| c6.paypal.com | unknown | unknown | false | | high |
| b.stats.paypal.com | unknown | unknown | false | | high |
| zn1ynnliufrct75cb-paypalxm.siteintercept.qualtrics.com | unknown | unknown | false | | high |
| cdn.jsdelivr.net | unknown | unknown | false | | high |
| 41197f7425669ed0.cbridgert.vhtcloud.com | unknown | unknown | false | | unknown |
| sjc1.qualtrics.com | unknown | unknown | false | | high |
| www.paypal.com | unknown | unknown | false | | high |
| clients2.google.com | unknown | unknown | false | | high |
| developer.paypal.com | unknown | unknown | false | | high |
| zn824xgjyopuf0rcx-paypalxm.siteintercept.qualtrics.com | unknown | unknown | false | | high |
| www.sandbox.paypal.com | unknown | unknown | false | | high |
| t.paypal.com | unknown | unknown | false | | high |
| www.paypalobjects.com | unknown | unknown | false | | high |

## Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://https://www.paypalobjects.com/ppdevdocs/v1/webpack-runtime-d7cf04c595556fc40df2.js | false | | high |
| http://https://www.paypalobjects.com/ppdevdocs/v1/d4d9defc-8b64dd61e59e55174123.js | false | | high |
| http://https://www.paypal.com/smartchat/open/chat-meta?app=loggedOut | false | | high |
| http://https://t.paypal.com/ts?v=1.7.6&t=1679384603103&g=0&pgrp=main%3Aconsappdownload%3A&page=main%3Aconsappdownload%3Axsell%3A%3A%3APRE_LOGIN_BANNER&pgst=1679381001946&calc=f6031034b1c6c&nsid=Hp5AaqckxR_BLIyp4sEJR5qyJFZEP9aY&rsta=en_US&pgtf=Nodejs&env=live&s=ci&ccpg=US&csci=dfcbd18bc93d4fd590d39cab6fc34c2f&comp=smarthelpnodeweb&tsrce=smarthelpnodeweb&cu=0&ef_policy=ccpa&c_prefs=P%3D1%2CF%3D1%2Ctype%3Dimplicit&link=main%3Ahelp%3Asmart%3A%3Acontact-us%3A%3A%3A%3A&pglk=main%3Ahelp%3Asmart%3A%3Acontact-us%3A%3A%3A%3A&pgln=main%3Ahelp%3Asmart%3A%3Acontact-us%3A%3A%3A%3A&lgin=out&e=im&displayPage=main%3Ahelp%3Asmart%3A%3Acontact-us&bannerType=app_download_sticky_banner&card_type=top&devc_type=DESKTOP&client_os=Windows%2010&pt=PayPal%20Contact%20Us&cd=24&sw=1920&sh=1080&dw=1920&dh=1080&bw=1920&bh=969&ce=1 | false | | high |

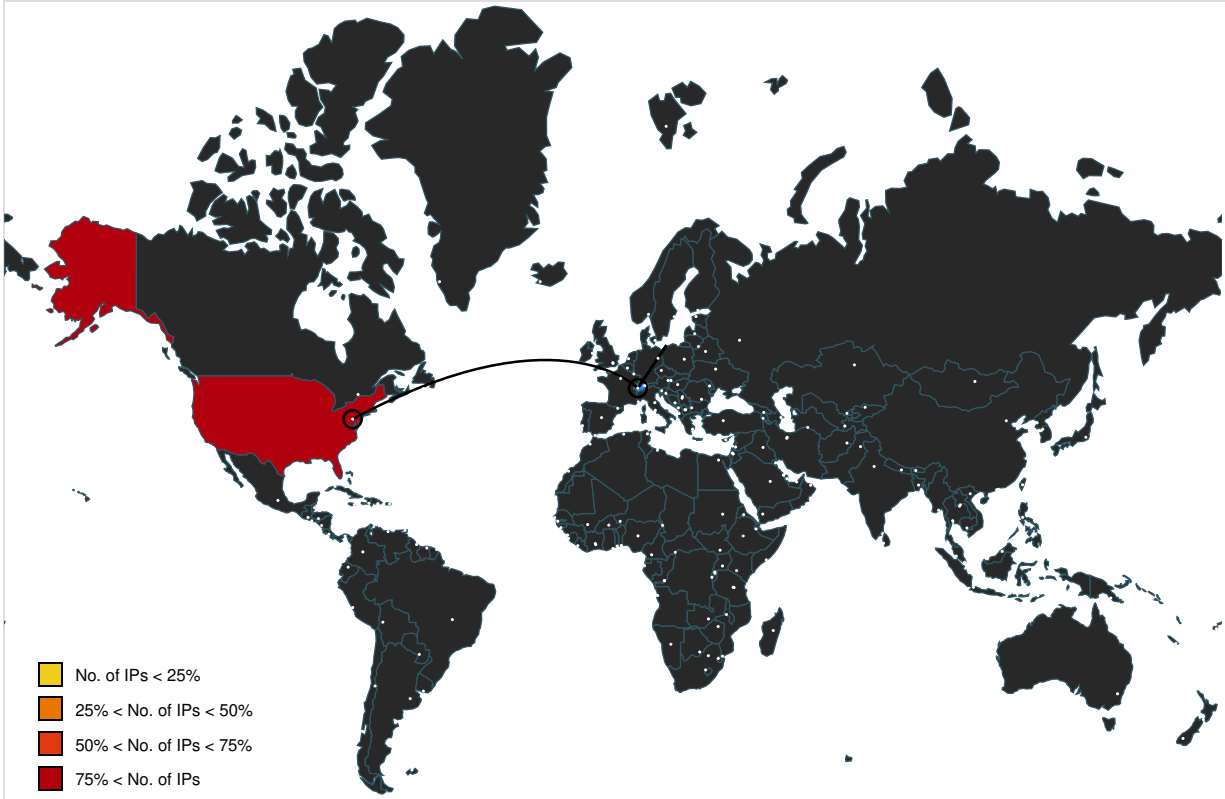
| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://https://www.paypalobjects.com/digitalassets/c/icons/status/18/newpage_18_white.svg | false | | high |
| http://https://www.paypalobjects.com/web/res/d33/6dfcf34262e820e9c7c3e466d635e/js/client/bundle.js | false | | high |
| http://https://www.paypalobjects.com/paypal-ui/logos/svg/paypal-mark-color.svg | false | | high |
| http://https://t.paypal.com/ts?v=1.7.6&t=1679384587928&g=0&pgrp=main%3Ahelp%3Asmart%3A%3Acontact-us&page=main%3Ahelp%3Asmart%3A%3Acritical-alert%3A%3A%3A&pgst=1679380984578&calc=f101737194789&nsid=Hp5AaqckxR_BLIyp4sEJR5qyJFZEP9aY&rsta=en_US&pgtf=Nodejs&env=live&s=ci&ccpg=US&csci=53c946f29e414632aa7bccbf8171d0df&comp=smarthelpnodeweb&tsrce=smarthelpnodeweb&cu=0&ef_policy=ccpa&c_prefs=P%3D1%2CF%3D1%2Ctype%3Dimplicit&link=smarthelp-critical-alert&pglk=main%3Ahelp%3Asmart%3A%3Acontact-us%7Csmarthelp-critical-alert&pgln=main%3Ahelp%3Asmart%3A%3Acritical-alert%3A%3A%3A%7Csmarthelp-critical-alert&lgin=out&e=ac&event_name=classic_help_critical_alert_in_contact_page_shown | false | | high |
| http://https://www.paypalobjects.com/web/res/e95/22d83c4b9d08440a724cba9e7c79f/js/apps/bundle.js | false | | high |
| http://https://www.paypalobjects.com/webstatic/mktg/2014design/font/PP-Sans/PayPalSansBig-Light.woff | false | | high |
| http://https://www.paypalobjects.com/ppdevdocs/v1/fa0a4f1ca647b7c9a5a90d2b5459c364088a3908-1b8b2e41aaac0262a41c.js | false | | high |
| http://https://www.paypalobjects.com/digitalassets/c/paypal-ui/logos/svg/paypal-color.svg | false | | high |
| http://https://www.paypal.com/smarthelp/getGriffinMetadata | false | | high |
| http://https://www.paypal.com/smarthelp/post-chat-bot-eligibility?intentId=contactUSpage&intentType=GENERIC&entryPoint=contact-us | false | | high |
| http://https://t.paypal.com/ts?v=1.7.6&t=1679384618297&g=0&pgrp=legalhub&page=cookie-full&pgst=1679381015068&calc=f692264404513&nsid=Hp5AaqckxR_BLIyp4sEJR5qyJFZEP9aY&rsta=en_US&pgtf=Nodejs&env=live&s=ci&ccpg=US&csci=e239f68345ed4b2ca0e27b675f25f812&comp=legalhubnodeweb&tsrce=authchallengenodeweb&cu=0&ef_policy=ccpa&c_prefs=P%3D1%2CF%3D1%2Ctype%3Dimplicit&e=im&imsrc=setup&view=%7B%22t10%22%3A1%2C%22t11%22%3A3849%2C%22tcp%22%3A3146%2C%22et%22%3A%224g%22%2C%22nt%22%3A%22navigate%22%2C%22bt%22%3A52%7D&pt=Statement%20on%20Cookies%20and%20Tracking%20Technologies&cd=24&sw=1920&sh=1080&dw=1920&dh=1080&bw=1920&bh=969&ce=1&t1=1&t1c=0&t1d=0&t1s=0&t2=408&t3=2509&t4d=0&t4=0&t4e=2&tt=3798&rdc=1&protocol=http%2F1.1&cdn=fastly&res=%7B%7D | false | | high |
| http://https://www.paypalobjects.com/ppdevdocs/v1/78db7eb9-f2a77a334bd99e9a5e47.js | false | | high |
| http://https://www.paypal.com/us/webapps/mpp/home | false | | high |
| http://https://www.paypalobjects.com/marketing/web/US/en/rebrand/pictograms/personal-app.svg | false | | high |
| http://https://www.paypalobjects.com/activation/js/marketingIntentsV2.js | false | | high |
| http://https://www.paypalobjects.com/marketing/web/US/en/rebrand/pictograms/business-start.svg | false | | high |
| http://https://www.paypalobjects.com/ppdevdocs/v1/0df6a05716ff351e4e1adb7cf212ed1eeadaa4f1-bdef5d61c748676261a7.js | false | | high |
| http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=94.0.4606.61&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1 | false | | high |
| http://https://www.paypal.com/us/smarthelp/contact-us | false | | high |
| http://https://www.paypalobjects.com/web/res/7e9/5f15b821f1247a286af2a3bcfd5b1/js/payerview.js | false | | high |
| http://https://www.paypalobjects.com/paypal-ui/fonts/PayPalSansBig-Regular.woff2 | false | | high |
| http://https://www.paypalobjects.com/ppdevdocs/v1/2cf658ad83971b66a20a515afce6186db6350b14-f969cecc5abd4319b0f2.js | false | | high |
| http://https://www.paypalobjects.com/pa/3pjs/qualtrics/1.64.1/17.0e47ac923c1fa85e46cf.chunk.js?Q_CLIENTVERSION=1.64.1&Q_CLIENTTYPE=hostedjs&Q_BRANDID=paypalxm | false | | high |
| http://https://www.paypal.com/smarthelp/active-users | false | | high |
| http://https://c.paypal.com/v1/r/d/b/p1 | false | | high |
| http://https://cdn.jsdelivr.net/npm/mutationobserver-shim/dist/mutationobserver.min.js | false | | high |
| http://https://www.recaptcha.net/recaptcha/enterprise/anchor?ar=1&k=6LdCCOUUAAAAAHTE-Snr6hi4HJGtJk_d1_ce-gWB&co=aHR0cHM6Ly93d3cucGF5cGFsLmNvbTo0NDM.&hl=en&v=Trd6gj1dhC_fx0ma_AWHc1me&size=invisible&cb=4s88in494qu | false | | unknown |
| http://https://c.paypal.com/v1/r/d/b/p2 | false | | high |
| http://https://c6.paypal.com/v1/r/d/b/p3?f=85252d8f49dc4538bf7cd0952c841415&s=invoicingnodeweb_s_pay | false | | high |
| http://https://www.paypalobjects.com/ppdevdocs/v1/7bc23de15ec3eb68df715500cb66b5dd0826c14d-35fd58c53936d17cb11d.js | false | | high |
| http://https://developer.paypal.com/apis/user | false | | high |
| http://https://www.paypalobjects.com/webstatic/mktg/2014design/font/PP-Sans/PayPalSansBig-Medium.woff | false | | high |
| http://https://www.paypal.com/smarthelp/topic-tree | false | | high |

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://https://www.paypalobjects.com/ppdevdocs/v1/d580e957-6d915f64271996d2dc42.js | false | | high |
| http://https://www.paypalobjects.com/paypal-ui/fonts/PayPalOpen-Regular.woff2 | false | | high |
| http://https://b.stats.paypal.com/v2/counter.cgi?p=uid_4a37b78a6d_mdc6ndi6ndk&s=SMART_PAYMENT_BUTTONS | false | | high |
| http://https://www.paypalobjects.com/ppdevdocs/v1/a68e81b59c5cb95c03788356a4e9985f75616164-d63ed1bfc0b45611c81c.js | false | | high |
| http://https://www.paypalobjects.com/pa/3pjs/qualtrics/1.64.1/12.2e4d3453d92fa382c1f6.chunk.js?Q_CLIENTVERSION=1.64.1&Q_CLIENTTYPE=hostedjs&Q_BRANDID=paypalxm | false | | high |
| http://https://www.paypalobjects.com/marketing-resources/css/bb/4045be073bd1ebcd709ccbfc02c03fff52cbee.css | false | | high |
| http://https://www.paypalobjects.com/ppdevdocs/v1/styles-407fe62976dc5310c43e.js | false | | high |
| http://https://www.paypalobjects.com/ppdevdocs/v1/styles.22e87296f1d7b3b6e401.css | false | | high |
| http://https://www.paypalobjects.com/ppdevdocs/v1/component---src-pages-layout-js-235e0c4506b918fd0e60.js | false | | high |
| http://https://www.paypalobjects.com/web/res/d33/6dfcf34262e820e9c7c3e466d635e/js/client/main.css | false | | high |
| http://https://www.paypalobjects.com/ui-web/vx-icons/2-0-1/PayPalVXIcons-Regular.woff | false | | high |
| http://https://www.paypal.com/auth/createchallenge/733d68412256189e/recaptchav3.js?_sessionID=Hp5AaqckxR_BLIyp4sEJR5qyJFZEP9aY | false | | high |
| http://https://www.recaptcha.net/recaptcha/enterprise/anchor?ar=1&k=6LdCCOUUAAAAAHTE-Snr6hi4HJGtJk_d1_ce-gWB&co=aHR0cHM6Ly93d3cucGF5cGFsLmNvbTo0NDM.&hl=en&v=Trd6gj1dhC_fx0ma_AWHc1me&size=invisible&cb=sot1ocsh2x24 | false | | unknown |
| http://https://www.paypalobjects.com/ppdevdocs/v1/c7887393-3b17fb3ea74723c5fba6.js | false | | high |
| http://https://www.paypalobjects.com/paypal-ui/fonts/PayPalSansBig-Light.woff2 | false | | high |
| http://https://www.paypalobjects.com/ppdevdocs/v1/36a9dca1-fd4b9a03f3f1de973625.js | false | | high |
| http://https://www.paypalobjects.com/marketing-resources/vendors/emotion-react-11_9_0-bundle.js | false | | high |
| http://https://www.paypalobjects.com/messaging/messaging-chat/v58/messaging-chat.js | false | | high |
| http://https://t.paypal.com/ts?v=1.7.6&t=1679384636741&g=0&page=main%3Aprivacy%3Apolicy%3Accpa&pgrp=main%3Aprivacy%3Apolicy&comp=devdiscoverynodeweb&env=prod&xt=123956%2C123954%2C120840%2C119037%2C119038&xe=105410%2C105409%2C104759%2C104406%2C104407&displaypage=main%3Adeveloper%3Ahome&ppage=privacy_banner&bannertype=cookiebanner&ccpg=US&flag=ccpa&bannerversion=v3a&bannersource=ConsentNodeServ&eligibility_reason=false&is_native=false&cookie_disabled=false&e=ac | false | | high |
| http://https://www.paypalobjects.com/ppdevdocs/v1/308df44b-5a39602238ec14ba3082.js | false | | high |
| http://https://b.stats.paypal.com/v2/counter.cgi?p=85252d8f49dc4538bf7cd0952c841415&s=invoicingnodeweb_s_pay | false | | high |
| http://https://www.paypal.com/smartchat/open/eligibility?intent=SALESCHAT&page=/us/webapps/mpp/home | false | | high |
| http://https://dub.stats.paypal.com/v2/counter2.cgi?p=uid_4a37b78a6d_mdc6ndi6ndk&s=SMART_PAYMENT_BUTTONS | false | | high |
| http://https://developer.paypal.com/home/search.css | false | | high |
| http://https://www.paypalobjects.com/ui-web/paypal-sans-small/1-0-0/PayPalSansSmall-Bold.woff2 | false | | high |
| http://https://t.paypal.com/ts?v=1.7.6&t=1679384619300&g=0&pgrp=legalhub&page=cookie-full&pgst=1679381015068&calc=f692264404513&nsid=Hp5AaqckxR_BLIyp4sEJR5qyJFZEP9aY&rsta=en_US&pgtf=Nodejs&env=live&s=ci&ccpg=US&csci=e239f68345ed4b2ca0e27b675f25f812&comp=legalhubnodeweb&tsrce=authchallengenodeweb&cu=0&ef_policy=ccpa&c_prefs=P%3D1%2CF%3D1%2Ctype%3Dimplicit&event_name=t_paypal_cpl&t1=37&t1c=37&t1d=0&t1s=36&t2=182&t3=1&tt=220&protocol=http%2F1.1&cdn=fastly&tmpl=%2F%2Ft.paypal.&view=%7B%22t10%22%3A37%2C%22t11%22%3A220%2C%22nt%22%3A%22res%22%7D&e=pf | false | | high |
| http://https://www.paypalobjects.com/web/res/7e9/5f15b821f1247a286af2a3bcfd5b1/js/xhr-ads.min.js | false | | high |
| http://https://41197f7425669ed0.cbridgert.vhtcloud.com/vht-conversation-bridge-runtime.js | false | • Avira URL Cloud: safe | unknown |
| http://https://www.paypal.com/auth/createchallenge/5b44f4636fe6fc5d/recaptchav3.js?_sessionID=Hp5AaqckxR_BLIyp4sEJR5qyJFZEP9aY | false | | high |
| http://https://www.paypal.com/invoice/payerView/detailsInternal/INV2-XUNJ-5FR3-4VFZ-6WLA?isFreshPayment=false&isCcEmailParamSet=false&locale.x=en_US | false | | high |
| http://https://www.recaptcha.net/recaptcha/enterprise/anchor?ar=1&k=6LdCCOUUAAAAAHTE-Snr6hi4HJGtJk_d1_ce-gWB&co=aHR0cHM6Ly93d3cucGF5cGFsLmNvbTo0NDM.&hl=en&v=Trd6gj1dhC_fx0ma_AWHc1me&size=invisible&cb=5lo9io607187 | false | • Avira URL Cloud: safe | unknown |
| http://https://www.paypalobjects.com/ppdevdocs/v1/jscript/master-optimized.js | false | | high |
| http://https://www.paypalobjects.com/paypal-ui/fonts/PayPalSansBig-Medium.woff2 | false | | high |
| http://https://www.paypalobjects.com/ppdevdocs/v1/215156a9446f07201e71d42e2a778485480be15c-1e55f5887d628235b6dc.js | false | | high |

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://https://t.paypal.com/ts?v=1.7.6&t=1679384627948&g=0&pgrp=main%3Aprivacy%3Apolicy&page=main%3Aprivacy%3Apolicy%3Accpa&pgst=Unknown&calc=f9499510b352d&nsid=Hp5AaqckxR_BLIyp4sEJR5qyJFZEP9aY&rsta=en_US&pgtf=Nodejs&env=live&s=ci&ccpg=US&csci=57dcba35049e4133854642b71922ea59&comp=mppnodeweb&tsrce=legalhubnodeweb&cu=0&ef_policy=ccpa&c_prefs=P%3D1%2CF%3D1%2Ctype%3Dimplicit&xe=105410%2C105409%2C104759%2C104406%2C104407&xt=123956%2C123954%2C120840%2C119037%2C119038&mab_reward_104449=124068%3A0&mab_reward_104366=118892%3A0&pgld=Unknown&bzsr=main&bchn=mktg&pgsf=personal&lgin=out&page_type=ecm&shir=main_mktg_personal_homepage&pros=1&lgcook=0&event_props=cu%2Clgin%2Cpage%2Cxe%2Cxt&user_props=cu%2Cxe%2Cxt&page_segment=ppcom&displaypage=main%3Amktg%3Apersonal%3Ahomepage%3Ahome&ppage=privacy_banner&bannertype=cookiebanner&flag=ccpa&bannerversion=v3a&bannersource=ConsentNodeServ&eligibility_reason=false&is_native=false&cookie_disabled=false&e=ac | false | | high |
| http://https://www.paypal.com/invoice/payerView/details/INV2-XUNJ-5FR3-4VFZ-6WLA?locale.x=en_US&v=1&utm_source=unp&utm_medium=email&utm_campaign=RT000238&utm_unptid=3eeb2dd2-c733-11ed-8c7c-3cfdfeef79f1&ppid=RT000238&cnac=US&rsta=en_US%28en-US%29&cust=&unptid=3eeb2dd2-c733-11ed-8c7c-3cfdfeef79f1&calc=c47aef0f1ea5&unp_tpcid=invoice-buyer-notification&page=main%3Aemail%3ART000238&pgrp=main%3Aemail&e=cl&mchn=em&s=ci&mail=sys&appVersion=1.153.0&xt=104038%2C124817 | false | | high |
| http://https://www.paypalobjects.com/web/res/7e9/5f15b821f1247a286af2a3bcfd5b1/js/components/requirejs/require.js | false | | high |
| http://https://www.recaptcha.net/recaptcha/enterprise/anchor?ar=1&k=6LdCCOUUAAAAAHTE-Snr6hi4HJGtJk_d1_ce-gWB&co=aHR0cHM6Ly93d3cucGF5cGFsLmNvbTo0NDM.&hl=en&v=Trd6gj1dhC_fx0ma_AWHc1me&size=invisible&cb=sot1ocsh2x24 | false | | unknown |
| http://https://www.paypalobjects.com/marketing/web/US/en/rebrand/pictograms/personal-how-it-works.svg | false | | high |
| http://https://www.paypalobjects.com/paypal-ui/icons/v3/svg/phone.svg | false | | high |
| http://https://t.paypal.com/ts?v=1.7.6&t=1679384630213&g=0&pgrp=main%3Amktg%3Apersonal%3Ahomepage%3Ahome&page=main%3Amktg%3Apersonal%3Ahomepage%3Ahome%3A%3A%3A&pgst=Unknown&calc=f9499510b352d&nsid=Hp5AaqckxR_BLIyp4sEJR5qyJFZEP9aY&rsta=en_US&pgtf=Nodejs&env=live&s=ci&ccpg=us&csci=57dcba35049e4133854642b71922ea59&comp=mppnodeweb&tsrce=legalhubnodeweb&cu=0&ef_policy=ccpa&c_prefs=P%3D1%2CF%3D1%2Ctype%3Dimplicit&xe=104449%2C104366&xt=124068%2C118892&mab_reward_104449=124068%3A0&mab_reward_104366=118892%3A0&pgld=Unknown&bzsr=main&bchn=mktg&pgsf=personal&lgin=out&page_type=ecm&shir=main_mktg_personal_homepage&pros=1&lgcook=0&event_props=cu%2Clgin%2Cpage%2Cxe%2Cxt&user_props=cu%2Cxe%2Cxt&page_segment=ppcom&event_name=t_paypal_cpl&t1=38&t1c=38&t1d=0&t1s=36&t2=172&t3=2&tt=212&protocol=http%2F1.1&cdn=fastly&tmpl=%2F%2Ft.paypal.&view=%7B%22t10%22%3A38%2C%22t11%22%3A212%2C%22nt%22%3A%22res%22%7D&e=pf | false | | high |
| http://https://www.paypalobjects.com/marketing/web/US/en/rebrand/pictograms/business-pricing.svg | false | | high |
| http://https://www.paypalobjects.com/web/res/d33/6dfcf34262e820e9c7c3e466d635e/js/client/7.bundle.js | false | | high |
| http://https://www.paypal.com/invoice/payerView/details/INV2-XUNJ-5FR3-4VFZ-6WLA?locale.x=en_US&v=1&utm_source=unp&utm_medium=email&utm_campaign=RT000238&utm_unptid=3eeb2dd2-c733-11ed-8c7c-3cfdfeef79f1&ppid=RT000238&cnac=US&rsta=en_US%28en-US%29&cust=&unptid=3eeb2dd2-c733-11ed-8c7c-3cfdfeef79f1&calc=c47aef0f1ea5&unp_tpcid=invoice-buyer-notification&page=main%3Aemail%3ART000238&pgrp=main%3Aemail&e=cl&mchn=em&s=ci&mail=sys&appVersion=1.153.0&xt=104038%2C124817 | false | | high |
| http://https://www.paypalobjects.com/web/res/7e9/5f15b821f1247a286af2a3bcfd5b1/css/payerview.ltr.css | false | | high |
| http://https://www.paypalobjects.com/digitalassets/c/website/ua/img/print-icon-hover.svg | false | | high |
| http://https://www.paypalobjects.com/pa/mi/paypal/latmconf.js | false | | high |
| http://https://developer.paypal.com/home | false | | high |
| http://https://www.paypalobjects.com/pa/3pjs/qualtrics/1.64.1/1.1303dc17a61da0f506d3.chunk.js?Q_CLIENTVERSION=1.64.1&Q_CLIENTTYPE=hostedjs&Q_BRANDID=paypalxm | false | | high |
| http://https://www.recaptcha.net/recaptcha/enterprise/reload?k=6LdCCOUUAAAAAHTE-Snr6hi4HJGtJk_d1_ce-gWB | false | • Avira URL Cloud: safe | unknown |
| http://https://www.recaptcha.net/recaptcha/enterprise/anchor?ar=1&k=6LdCCOUUAAAAAHTE-Snr6hi4HJGtJk_d1_ce-gWB&co=aHR0cHM6Ly93d3cucGF5cGFsLmNvbTo0NDM.&hl=en&v=Trd6gj1dhC_fx0ma_AWHc1me&size=invisible&cb=xvre4mvlh5fm | false | | unknown |
| http://https://www.paypalobjects.com/pa/3pjs/qualtrics/1.64.1/CoreModule.js?Q_CLIENTVERSION=1.64.1&Q_CLIENTTYPE=hostedjs&Q_BRANDID=paypalxm | false | | high |
| http://https://www.paypal.com/xoplatform/logger/api/logger | false | | high |
| http://https://www.paypalobjects.com/pa/3pjs/qualtrics/1.64.1/OrchestratorMain.js | false | | high |
| http://https://c6.paypal.com/v1/r/d/b/p3?f=uid_4a37b78a6d_mdc6ndi6ndk&s=SMART_PAYMENT_BUTTONS | false | | high |
| http://https://t.paypal.com/ts?v=1.7.6&t=1679384636711&g=0&page=main%3Aprivacy%3Apolicy%3Accpa&pgrp=main%3Aprivacy%3Apolicy&comp=devdiscoverynodeweb&env=prod&xt=123956%2C123954%2C120840%2C119037%2C119038&xe=105410%2C105409%2C104759%2C104406%2C104407&displaypage=main%3Adeveloper%3Ahome&ppage=privacy_banner&bannertype=cookiebanner&ccpg=US&flag=ccpa&bannerversion=v3a&bannersource=ConsentNodeServ&eligibility_reason=false&is_native=false&cookie_disabled=false&e=ac | false | | high |

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://https://www.recaptcha.net/recaptcha/enterprise.js?render=6LdCCOUUAAAAAHTE-Snr6hi4HJGtJk_d1_ce-gWB&hl=en | false | • Avira URL Cloud: safe | unknown |
| http://https://t.paypal.com/ts?v=1.7.6&t=1679384603104&g=0&pgrp=main%3Aprivacy%3Apolicy&page=main%3Aprivacy%3Apolicy%3Accpa&pgst=1679381001946&calc=f6031034b1c6c&nsid=Hp5AaqckxR_BLIyp4sEJR5qyJFZEP9aY&rsta=en_US&pgtf=Nodejs&env=live&s=ci&ccpg=US&csci=dfcbd18bc93d4fd590d39cab6fc34c2f&comp=smarthelpnodeweb&tsrce=smarthelpnodeweb&cu=0&ef_policy=ccpa&c_prefs=P%3D1%2CF%3D1%2Ctype%3Dimplicit&link=main%3Ahelp%3Asmart%3A%3Acontact-us%3A%3A%3A&pglk=main%3Ahelp%3Asmart%3A%3Acontact-us%3A%3A%3A&pgln=main%3Ahelp%3Asmart%3A%3Acontact-us%3A%3A%3A&lgin=out&displaypage=main%3Ahelp%3Asmart%3A%3Acontact-us&ppage=privacy_banner&bannertype=cookiebanner&flag=ccpa&bannerversion=v3a&bannersource=ConsentNodeServ&xe=105410%2C105409%2C104759%2C104406%2C104407&xt=123956%2C123954%2C120840%2C119037%2C119038&eligibility_reason=false&is_native=false&cookie_disabled=false&e=ac | false | | high |
| http://https://www.paypalobjects.com/ppdevdocs/v1/8c13cb77-f4d0979d75167c67a7df.js | false | | high |
| http://https://www.paypalobjects.com/paypal-ui/web/fonts-and-normalize/1-1-0/fonts-and-normalize.min.css | false | | high |
| http://https://www.paypal.com/us/legalhub/cookie-full | false | | high |
| http://https://www.paypal.com/auth/recaptcha/grcenterprise_v3.html | false | | high |
| http://https://www.paypal.com/invoice/wr-metadata | false | | high |

## World Map of Contacted IPs




## Public IPs

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 173.194.76.156 | stats.g.doubleclick.net | United States | | 15169 | GOOGLEUS | false |
| 151.101.193.35 | t-fastly.glb.paypal.com | United States | | 54113 | FASTLYUS | false |
| 142.250.185.228 | www.google.com | United States | | 15169 | GOOGLEUS | false |
| 151.101.129.229 | jsdelivr.map.fastly.net | United States | | 54113 | FASTLYUS | false |
| 151.101.1.35 | dualstack.paypal-dynamic-2.map.fastly.net | United States | | 54113 | FASTLYUS | false |
| 142.250.185.205 | accounts.google.com | United States | | 15169 | GOOGLEUS | false |
| 172.217.23.110 | clients.l.google.com | United States | | 15169 | GOOGLEUS | false |
| 192.229.221.25 | cs1150.wpc.betacdn.net | United States | | 15133 | EDGECASTUS | false |
| 151.101.129.35 | c-fastly.glb.paypal.com | United States | | 54113 | FASTLYUS | false |
| 64.4.245.84 | dub.stats.paypal.com | United States | | 17012 | PAYPALUS | false |
| 151.101.193.21 | www-fastly.glb.paypal.com | United States | | 54113 | FASTLYUS | false |
| 173.0.93.193 | developer.glb.paypal.com | United States | | 17012 | PAYPALUS | false |

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 151.101.1.21 | paypal-dynamic.map.fastly.net | United States | | 54113 | FASTLYUS | false |
| 54.160.188.241 | cbridgert-1162716231.us-east-1.elb.amazonaws.com | United States | | 14618 | AMAZON-AESUS | false |
| 239.255.255.250 | unknown | Reserved | | unknown | unknown | false |
| 172.217.16.131 | www.recaptcha.net | United States | | 15169 | GOOGLEUS | false |

### Private

| IP |
|---|
| 192.168.11.1 |
| 192.168.11.20 |
| 127.0.0.1 |

## General Information

| | |
|---|---|
| Joe Sandbox Version: | 37.0.0 Beryl |
| Analysis ID: | 831169 |
| Start date and time: | 2023-03-21 07:40:43 +01:00 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 6m 12s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Cookbook file name: | browseurl.jbs |
| Sample URL: | http://https://www.paypal.com/invoice/payerView/details/INV2-XUNJ-5FR3-4VFZ-6WLA?locale.x=en_US&v=1&utm_source=unp&utm_medium=email&utm_campaign=RT000238&utm_unptid=3eeb2dd2-c733-11ed-8c7c-3cfdfeef79f1&ppid=RT000238&cnac=US&rsta=en_US(en-US)&cust=&unptid=3eeb2dd2-c733-11ed-8c7c-3cfdfeef79f1&calc=c47aef0f1ea5&unp_tpcid=invoice-buyer-notification&page=main%3Aemail%3ART000238&pgrp=main%3Aemail&e=cl&mchn=em&s=ci&mail=sys&appVersion=1.153.0&xt=104038%2C124817 |
| Analysis system description: | Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301 |
| Number of analysed new started processes analysed: | 7 |
| 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: | • HCA enabled<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | CLEAN |
| Classification: | clean0.win@43/0@21/19 |
| EGA Information: | Failed |
| HDC Information: | Failed |
| HCA Information: | • Successful, ratio: 100%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Browse: https://www.paypal.com/myaccount/privacy/cookiePrefs?locale=en_US<br>• Browse: https://www.paypal.com/smarthelp/contact-us<br>• Browse: https://www.paypal.com/smarthelp/contact-us<br>• Browse: https://www.paypal.com/US/webapps/mpp/ua/cookie-full<br>• Browse: https://www.paypal.com/us/webapps/mpp/home<br>• Browse: https://developer.paypal.com/home |

### Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, CompPkgSrv.exe, backgroundTaskHost.exe
- Excluded IPs from analysis (whitelisted): 142.250.184.195, 34.104.35.123, 104.17.208.240, 104.17.209.240, 216.58.212.131, 142.250.186.138, 142.250.185.74, 142.250.185.138, 172.217.18.106, 142.250.185.202, 142.250.185.106, 216.58.212.138, 172.217.23.106, 142.250.74.202, 142.250.186.106, 142.250.181.234, 142.250.185.234, 142.250.186.42, 142.250.184.202, 142.250.186.74, 142.250.185.170, 142.250.185.131, 172.217.16.206, 172.217.18.10, 142.250.184.234, 142.250.186.170, 172.217.16.202, 2.18.232.194, 52.242.101.226, 95.100.53.90, 184.30.21.171, 23.211.8.217

- Excluded domains from analysis (whitelisted): definitionupdates.microsoft.com.edgekey.net, slscr.update.microsoft.com, e13678.dscb.akamaiedge.net, clientservices.googleapis.com, www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net, e11290.dspg.akamaiedge.net, www.microsoft.com-c-3.edgekey.net, go.microsoft.com, login.live.com, update.googleapis.com, sls.update.microsoft.com, cloudenhanced.qualtrics.com.edgekey.net, www.gstatic.com, e12671.g.akamaiedge.net, www.google-analytics.com, glb.sls.prod.dcat.dsp.trafficmanager.net, definitionupdates.microsoft.com, client.wns.windows.com, content-autofill.googleapis.com, e12398.b.akamaiedge.net, wdcp.microsoft.com, wdcpalt.microsoft.com, edgedl.me.gvt1.com, prodlb.siteintercept.qualtrics.com.cdn.cloudflare.net, go.microsoft.com.edgekey.net, www.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing network information.
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

## Simulations

### Behavior and APIs

No simulations

## Joe Sandbox View / Context

### IPs

No context

### Domains

No context

### ASNs

No context

### JA3 Fingerprints

No context

### Dropped Files

No context

## Created / dropped Files

No created / dropped files found

## Static File Info

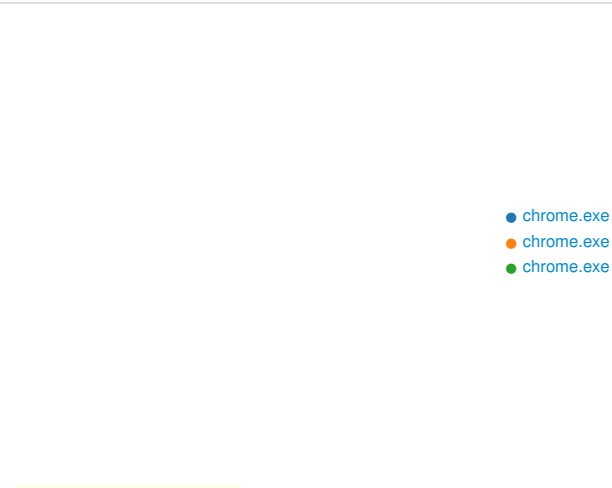
No static file info

## Network Behavior

**Report size exceeds maximum size, go to the download page of this report and download PCAP to see all network behavior.**

# Statistics

## Behavior




# System Behavior

## Analysis Process: chrome.exe PID: 6260, Parent PID: 7668

### General

| | |
|---|---|
| Target ID: | 0 |
| Start time: | 07:42:38 |
| Start date: | 21/03/2023 |
| Path: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank |
| Imagebase: | 0x7ff642c70000 |
| File size: | 2509656 bytes |
| MD5 hash: | 464953824E644F10FFDC9E093FD18F94 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | low |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|

| Old File Path | New File Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|

### Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| Key Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|

| Key Path | Name | Type | Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

| Key Path | Name | Type | Old Data | New Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|

## Analysis Process: chrome.exe PID: **6648**, Parent PID: **6260**

### General

| | |
|---|---|
| Target ID: | 2 |
| Start time: | 07:42:38 |
| Start date: | 21/03/2023 |
| Path: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| Wow64 process (32bit): | false |
| Commandline: | "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1728,48598192974864079,2612875733881127589,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2028 /prefetch:8 |
| Imagebase: | 0x7ff642c70000 |
| File size: | 2509656 bytes |
| MD5 hash: | 464953824E644F10FFDC9E093FD18F94 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | low |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|

| Old File Path | New File Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|

## Analysis Process: chrome.exe PID: **8232**, Parent PID: **7668**

### General

| | |
|---|---|
| Target ID: | 4 |
| Start time: | 07:42:39 |
| Start date: | 21/03/2023 |
| Path: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Program Files\Google\Chrome\Application\chrome.exe" "https://www.paypal.com/invoice/payerView/details/INV2-XUNJ-5FR3-4VFZ-6WLA?locale.x=en_US&v=1&utm_source=unp&utm_medium=email&utm_campaign=RT000238&utm_unptid=3eeb2dd2-c733-11ed-8c7c-3cfdfeef79f1&ppid=RT000238&cnac=US&rsta=en_US%28en-US%29&cust=&unptid=3eeb2dd2-c733-11ed-8c7c-3cfdfeef79f1&calc=c47aef0f1ea5&unp_tpcid=invoice-buyer-notification&page=main%3Aemail%3ART000238&pgrp=main%3Aemail&e=cl&mchn=em&s=ci&mail=sys&appVersion=1.153.0&xt=104038%2C124817 |
| Imagebase: | 0x7ff642c70000 |
| File size: | 2509656 bytes |
| MD5 hash: | 464953824E644F10FFDC9E093FD18F94 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | low |

### Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| Key Path | Name | Type | Old Data | New Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|

# Disassembly

No disassembly