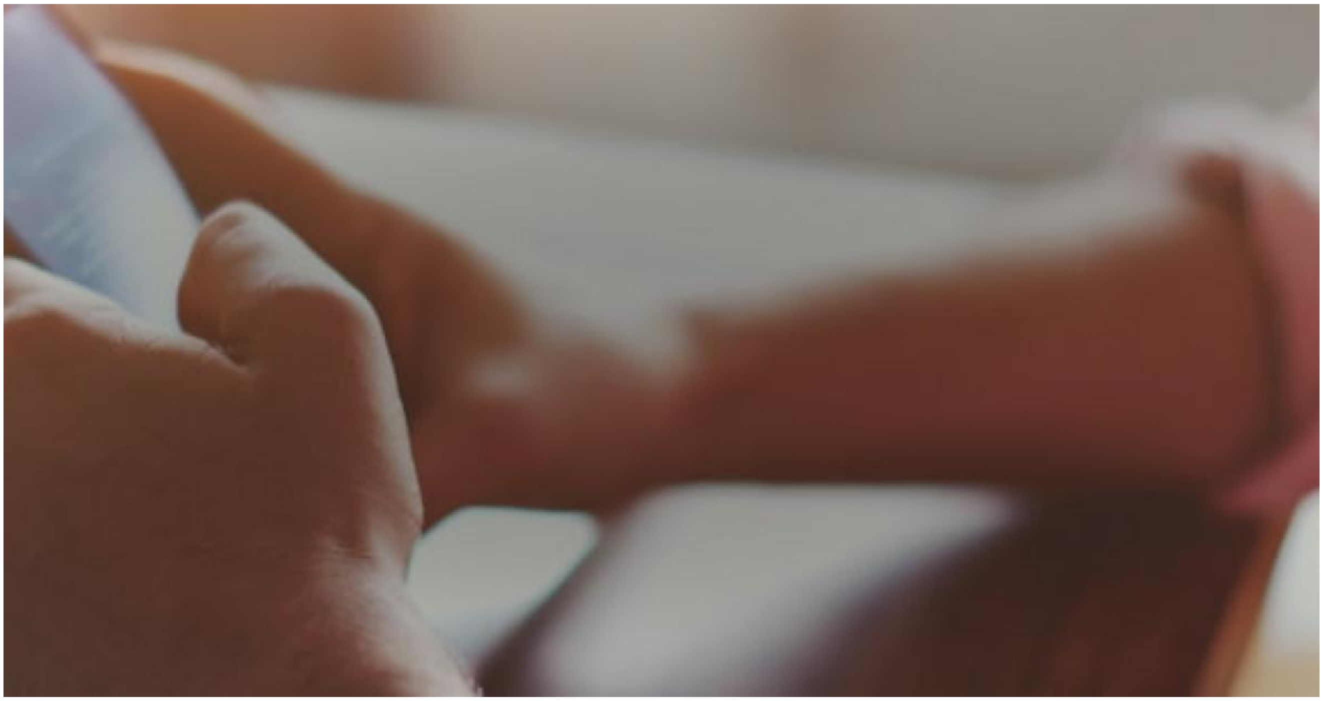
Threat Actors Repurpose Hupigon in Adult Dating Attacks Targeting US Universities

proofpoint.com/us/threat-insight/post/threat-actors-repurpose-hupigon-adult-dating-attacks-targeting-us-universities

April 23, 2020



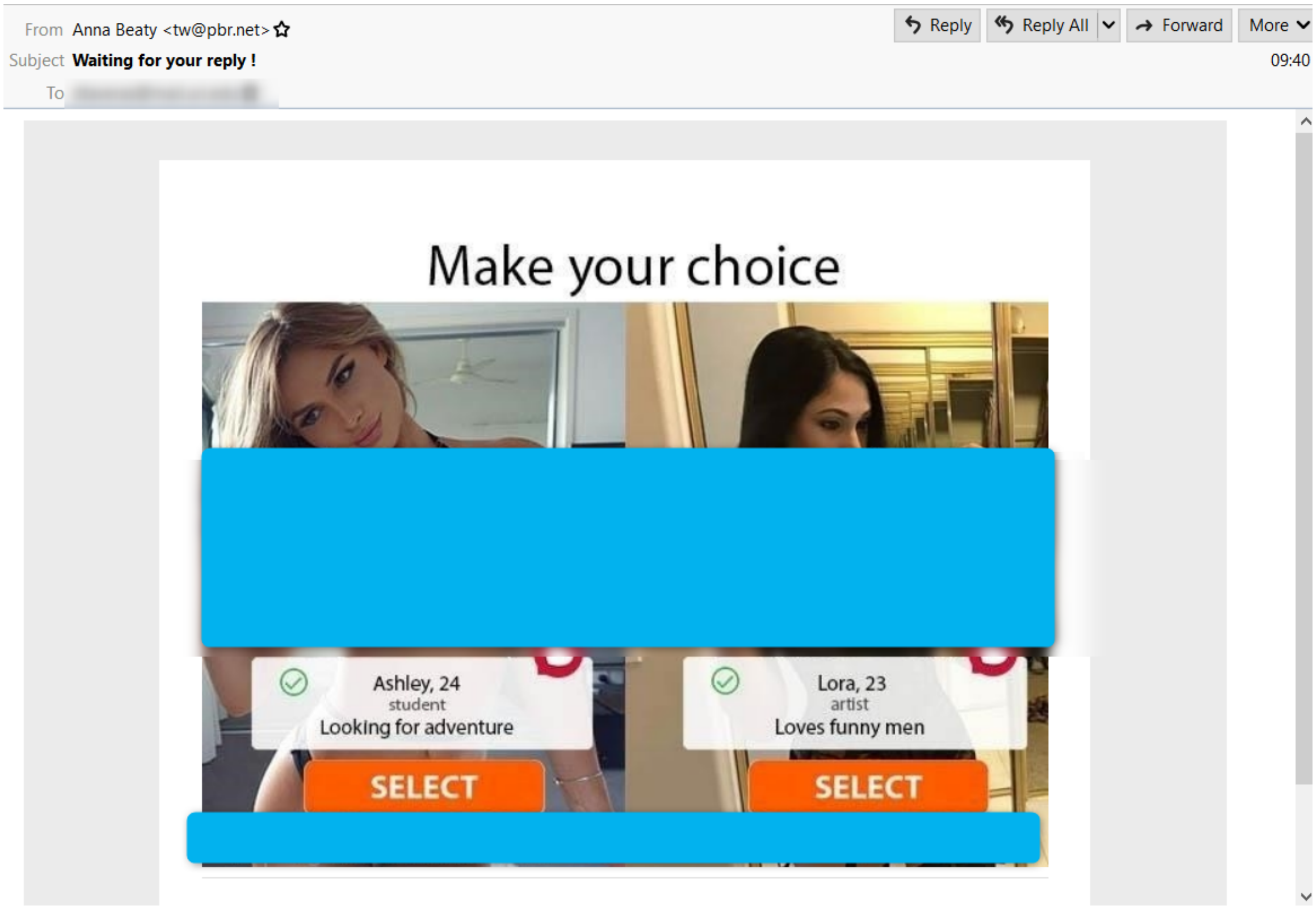
Blog
Threat Insight

Threat Actors Repurpose Hupigon in Adult Dating Attacks Targeting US Universities

April 23, 2020 Proofpoint Threat Research Team

Hupigon is a remote access Trojan (RAT) that has been around since at least 2006. Hupigon has been anecdotally associated with state-sponsored APT threat actors among others. Proofpoint researchers have recently discovered a large volume Hupigon campaign primarily targeting both faculty and students at United States colleges and universities.

Messages arrive obfuscated as adult dating lures requesting the user to choose between one of two pictures to connect with by clicking the link under their picture as shown in Figure 1.



From Anna Beaty <tw@pbr.net>

Subject **Waiting for your reply !**

To [redacted]

09:40

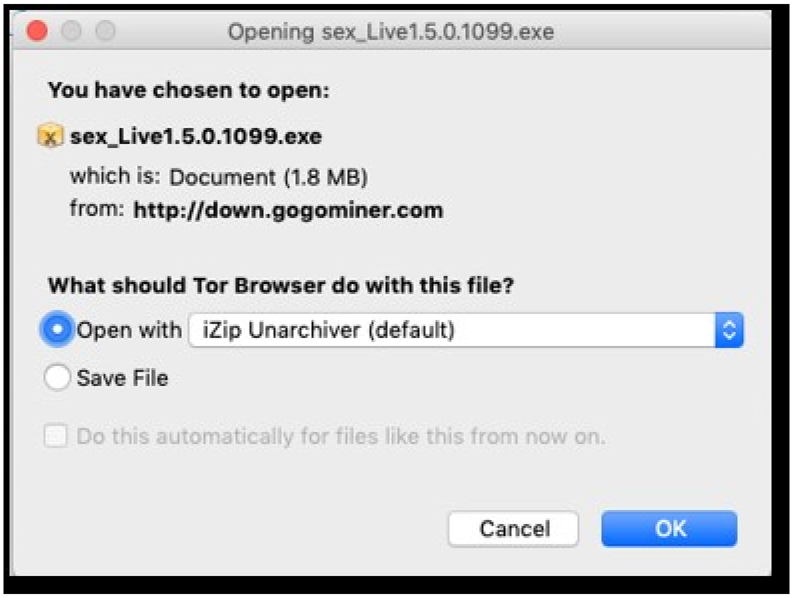
Make your choice

Ashley, 24
student
Looking for adventure

Lora, 23
artist
Loves funny men

Figure 1 Adult Dating Lure

If the recipient clicks either link, an executable download begins.



Opening sex_Live1.5.0.1099.exe

You have chosen to open:

sex_Live1.5.0.1099.exe

which is: Document (1.8 MB)

from: **http://down.gogominer.com**

What should Tor Browser do with this file?

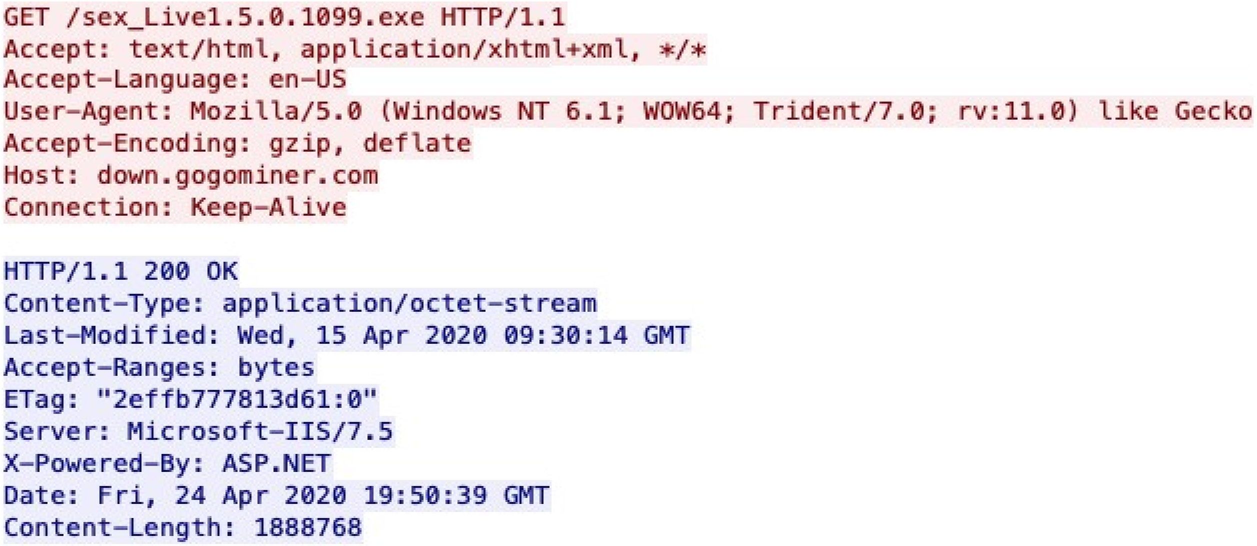
● Open with iZip Unarchiver (default)

○ Save File

□ Do this automatically for files like this from now on.

Figure 2 Hupigon Download

Once the recipient runs the file in the download, Hupigon is then installed on their system. In Figure 3 you can see the traffic upon clicking the malicious link leading to the download of the compressed executable.



```
GET /sex_Live1.5.0.1099.exe HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: down.gogominer.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Content-Type: application/octet-stream
Last-Modified: Wed, 15 Apr 2020 09:30:14 GMT
Accept-Ranges: bytes
ETag: "2effb777813d61:0"
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
Date: Fri, 24 Apr 2020 19:50:39 GMT
Content-Length: 1888768
```

Figure 3 Downloading the Hupigon Executable

Figure 4 illustrates the volumes of this campaign unfolding between April 13, 2020 and April 17, 2020.

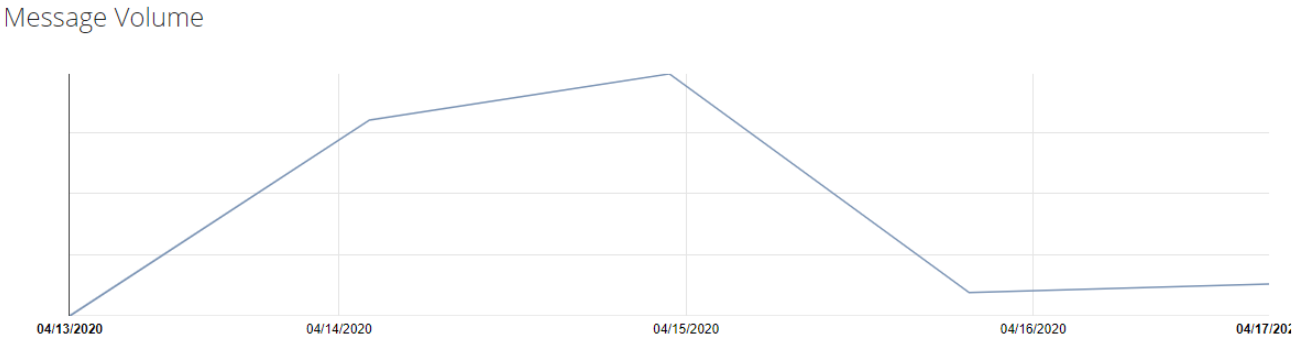


Figure 4 Hupigon Adult Dating Campaign Volume

Between the April 14, 2020 and April 15, 2020, message volumes reached approximately 80,000 messages, coinciding with an observed rotation in payload, exemplified below:

Date Used	SHA256
April 14, 2020	8e2f624f7bf79f35951fa8a434537caa7d82dfbdf0bcd97461f879c43eece7fa

April 15 2020	373c7986a56ee7b428757ac7862676a6b5bbaa1aee4122747fce5680ae024ff

This campaign delivered over 150,000 messages to over 60 different industries, with 45% focused on education, colleges, and universities.

Hupigon has many features and capabilities. It allows actors to access the infected machine, has rootkit functionality, webcam monitoring, and the ability to log keystrokes and steal passwords.

The payload makes a DNS request to eth[.]ceo located at 142.54.162[.]66 for the initial command and control communication. In addition, another domain was discovered on the IP address - **‘ooeth[.]com’.** Interesting to note the domain used for delivery ‘down.gogominer[.]com’ is hosted on the same address space as the C2 ‘142.54.162[.]67’.

Proofpoint associates Hupigon with historic APT campaigns based on the language of the builder, open source breach reporting, and multiple reports of similar APT actor behaviors between 2010 and 2012.

In this case, cybercriminals repurposed a nearly 15-year-old attack tool leveraged by state-sponsored threat actors among others. We believe this campaign is crimeware motivated. This judgment is based on the distribution methods and message volumes referenced in Figure 4 as well as other technical associations that we observed.

Indicators of Compromise

Payload	8e2f624f7bf79f35951fa8a434537caa7d82dfbdf0bcd97461f879c43eece7fa
Payload	373c7986a56ee7b428757ac7862676a6b5bbaa1aee4122747fce5680ae024ff
C2	142.54.162[.]66
C2	eth[.]ceo
DNS	ooeth[.]com
Delivery Domain	down.gogominer[.]com

Subscribe to the Proofpoint Blog