# DarkSky Botnet

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.

Ma	y Version	December Version
DarkSky	0 0 1 1 1 0 0	●DatSy +Specializing No ●THE TIME & Dannel - alloy bin - Disput
Online 1	Offline	terit den 1 and and a second den and a second den a se
Total	Dead	Territoria Secondaria Second
ź	Page bots	Ching         d         4.2211         spin         5.2211         F. Balling         4. Ball
# HWID P	Country OS Username Status	Allow         D         Darme         D         Darme         D <thd< th="">         D         D         <t< th=""></t<></thd<>
#1 2225513067 82.1 #2 1647864855 178	Contractor Windows & Admin Contractor Mildraine Windows & Igars Office	Stringer         20         Classes         JACK         Classes         Body         D Fill         J Fill <thj fill<="" th=""></thj>
Timeset: Botton		D         D <thd< th=""> <thd< th=""> <thd< th=""> <thd< th=""></thd<></thd<></thd<></thd<>

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

DarkSky		≁ Open	Latest Log File	0	🛱 Control 👻 🝚 Pr	oxy Tools 👻 😃 Logo
Total: 253 Online: 14	Commands center					
Dead: 9 Offline: 239 Banned: 110	Select command: * HTTP Flood	во	t ¢	Commands	\$ Status	¢ x
Wi Main	Options command:* For example: http://domain.ru/index.php	# 1			0 0	
© Settings	Threads:* Timeout:* Request:* Country:	# 1			0	
Commands center	Потоков, наприм In miliseconds: 11 GET 🔹 Example: RU, UA	(AL # 2)			0	
↔ Crypt of utility	Target:				0	•
ø Black list	Only ID Bot Add					
⊘ Check Host						
🖿 File Manager	Command \$	Counts \$	Complete \$	Country \$	Target	¢
○ Update and other						•
						•
						•

#### 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:g=0.9,image/webp.image/apng,\*/\*;q=0.8 Referer: <referer from a list> Accept-Language: ru-RU.ru:g=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.

👄 DarkSky		✤ Open Latest Log	File 🕕	Control - Proxy Tools -	<mark>ပ်</mark> Logou
Total: 252 Online: 13	Commands center				
Dead: 9 Offline: 239 Banned: 110	Select command: * Download and Run v	Bot ¢	Commands	♦ Status ♦ <u>x</u>	Î
₩ Main	Options for command: * Ha npunep: http://domain.ru/file.exe			• •	
© Settings	Counts:* Country: Target:			• •	
Commands center  Crypt of utility	Example: ro, oo, Example: ro, on (vic every ro oon every			0	÷
ø Black list	Command ¢ C	Counts <b>\$</b> Comple	ete 🛊 Country	¢ Target ¢	
O Check Host					Û
🖿 File Manager					<b>T</b>
O Update and other					Û
					Û

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.

GET /activation.php? key=fSJCTTMyMDEiOiJtYXIIICwiIjo Content-Type: application/x-www-form- Cache-Control: no-cache User-Agent: 2zAz Host: Content-Length: 4 .*HTTP/1.0 404 Not Found Date: Mon, 29 Jan 2018 07:05:23 GMT	-urlencoded	
Server: Apacne/2.4.25 (DeDian) X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block Referrer-Policy: strict-origin-when-c Content-Length: 0 Connection: close Content-Type: text/html; charset=UTF-	cross-origin -8	
3 client pkts, 3 server pkts, 3 turns.		
Entire conversation (622 bytes)	✓ Show and save data as ASCII ✓	Stream 85
Find:		Find <u>N</u> ext
Help	Filter Out This Stream     Print     Save as     Back	Close

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

The GET request param value is base64 encrypted.

• Original obfuscated value:

fSJCTTc0MDIiOiJtYXIiICwiljoicHR0aClgLCliOil0cylgLCliOil1cylgLClwljoibmltZEEiLClxys8iOiJlb WFOcmVzVSIsIkZBMDFCRjQzIjoiZGl3aClsIjAyM2c3bjFXIjoibml3Ins=

```
    Decrypting the message using base64, translates to a reversed string:
}"BM7402":"mar","":"ptth","":"4s","":"5s"
,"0":"nimdA","1ÊÏ":"emaNresU","FA01BF53":"diwh","023g7n1W":"niw"{
```

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

{"win":"W1n7g320","hwid":"35FB10AF","UserName":"ÏÊ1","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

GET /activation.php? key=fSJCTTk5Ny16Im1hciIgLC1 HTTP/1.1 Content-Type: application/x-www-form-urlencoded Cache-Control: no-cache User-Agent: 2ZAZ Host: Content-Length: 4 HTTP/1.1 200 0K		
Date: Sun, 28 Jan 2018 11:31:56 GMT Server: Apache/2.4.25 (Debian) X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block Referrer-Policy: strict-origin-when-cross-origin Vary: Accept-Encoding Content-Length: 178 Content-Type: text/html; charset=UTF-8		
load:"http:///Bot.exe"	/Bot.exe"load:"http://u	
3 client pkts, 3 server pkts, 3 turns.		
Entire conversation (799 bytes)	Show and save data as ASCII -	Stream 0 🌲
Find:		Find <u>N</u> ext
	Filter Out This Stream     Print     Save as     Back     Close	Help

- 2. Vbox:
  - 1. VBoxService.exe
  - 2. VBoxHook.dll
- 3. Sandboxie
  - 1. SbieDII.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 <u>cloud DDoS protection</u> for real-time <u>DDoS</u> <u>attack prevention</u> 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 date for preemptive protection against currently active known attackers.

For further <u>network and application protection</u> 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 <u>DDoSWarriors.com</u>. Created by Radware's <u>Emergency Response Team (ERT)</u>, 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