**{documentName}**

{date}

{%imageTag}

This document was written and delivered for the internal use only of **{companyName}** (hereinafter: ‘the customer’) and is a classified confidential document. It is strictly forbidden to deliver this document or parts thereof to any person outside the recipient, including the absolute prohibition to copy or photocopy it by any means or method and/or to make any external use thereof. All rights are reserved for White-Hat Ltd. It is strictly forbidden to copy, photocopy, distribute, quote or duplicate this document or any part thereof by any means, whether mechanical or electronic or optical. This document is the intellectual property of White-Hat copyrights, and all rights are reserved

Table of Content

[About White-Hat - *True Resilience Built on an Attacker’s Perspective* 3](#_Toc129771960)

[What Differentiates Us - *A Proactive Hands-On Approach* 3](#_Toc129771961)

[“Eye of the enemy” - about 4](#_Toc129771962)

[Executive Summary 6](#_Toc129771963)

[Attack Emulation 7](#_Toc129771964)

[Scenario 1 – Defense Evasion and Domain Reconnaissance with SharpHound 7](#_Toc129771965)

[**Proof of Concept** 7](#_Toc129771966)

[**Security Recommendations** 10](#_Toc129771967)

[Scenario 2 - Initial Access & Command Execution using Python Reverse Shell 11](#_Toc129771968)

[**Proof of Concept** 11](#_Toc129771969)

[**Security Recommendations** 14](#_Toc129771970)

# **About White-Hat -** *True Resilience Built on an Attacker’s Perspective*

Based in Israel, with a team of 70 experts, many of them veterans of elite cyber units in the Israeli military, we focus on proactive cyber defense customized to our customers’ needs.   
Since 2013, we have handled some of the most sophisticated attacks in the world, and continue to do so daily for governmental, banking, insurance, aerospace and energy organizations worldwide.   
White-Hat harnesses its unique Cyber perspective and methodologies to protect our customers with effective, swift and practical solutions. Always one step ahead of our adversaries, we provide our customers with solutions that block the threats of today and counter the threats of tomorrow.

# **What Differentiates Us - *A Proactive Hands-On Approach***

* **An Attacker’s Mindset**

Our team brings together a group of hackers, who are active members in live hacker communities. This positions us on the attacker’s end, with an attacker’s perspective, understanding and mindset, and makes all the difference in the world. The enormous gap between the defender and the attacker is the key facilitator for most successful attacks.

* **We Don’t Just Tell You What’s Wrong, We Fix It**

White-Hat provides customers with an end-to-end Cyber resilience solution, from recording an attack (payload/silver bullet) to exploiting vulnerabilities and blocking them. With our hands-on approach, we actually solve the problem and bring the customer back to a business-as-usual mode. We don’t just consult, or provide a list of forklift requirements, leaving the customer with a mission-impossible task – we act. No tasks left open – ours is a true game-over solution.

* **Experience with Challenges on a National Scale**

Our team comprises talents from Israel’s elite Cyber military units of the highest caliber, who have a wealth of experience with high-impact projects. The Israeli military uses superior technologies to counter formidable threats, with an intensity and sense of purpose that provides the most challenging Cyber training available.

* **Fueled by Current Cyber Trends**

Our team is always up-to-speed with the latest trends, attacks and events in the cyber ecosystem. Whenever a new breed of attack surfaces, we are immediately fueled by it, using it as inspiration for silver bullets, or focused simulated attacks. The cycles of cyber-attacks are extremely short, so in order to ensure our relevancy, we live and breathe the attacker community. While many large vendors find it challenging to keep up, our agility allows us to easily align with this swift pace. Our customers never have to ask – their defense is regularly updated with up-and-coming new tools on a regular basis.

* **Our Skills, Your In-House Tools**

Our offering is the hands-on services of our elite professionals. We don’t sell products, so our only focus is providing a practical, robust solution for our customers with their existing systems. With our services, you’ll receive exactly what you need – full Cyber resilience, without any requirements to replace company infrastructure. Providing custom services rather than products, we are not bound by any schedules, considerations or interests other than protecting our client, staying on top of the Cyber ecosystem, and creating counter measures for current attacks.

# “Eye of the enemy” - about

Increased spending does not always translate into greater security capability. The number of cyberattacks increases, takes more time to resolve, and the cost of cybercrime continues to rise

PROBLEM

Security leaders are accountable for maintaining security posture that fits in broader organization’s risk tolerance. However, products and point solutions do not always reduce the risk of a significant data breach due to constantly changing and evolving attack techniques

VALUE

**Proactive:** Test yourself before the attack reaches your organization

**Speed:** We deliver 24X7 research. Within hours you will get notification on new threats

**Risk-based:** You select the vector/payloads that are most valuable for your business

**Detection and Response:** Out threat intelligence is always on alert looking for new attacks

NEED

**Proactive:** CISOs today need to make sure that there is a bias toward being proactive with their security programs and architecture

**Speed:** Move with the speed of digital business

**Risk-based:** Shift to risk-based decision making and away from checkbox compliance

**Detection and Response:** Invest in detection and response, and stop trying to perfectly protect the organization assets

SOLUTION

EOTE platform imitates attackers' actions and workflows, from intelligence and reconnaissance to actual attacks simulation.

WHITE-HAT's attack tools will bypass existing defenses. However, deploying the 'defense rules' developed by our team in the client’s defense systems will ensure the organization's safety. **WHITE HAT will provide you with the full circle - Offence & Defense**

IMPLICATING

**Eye of the Enemy** is a WHITE HAT platform imitating the attackers' actions and workflows, from intelligence and reconnaissance to actual attacks simulation.

WHITE-HAT's attack tools will bypass your defenses - that's guaranteed.

However, deploying the 'defense rules' developed by our team in your defense systems will ensure your organization's safety.

WHITE HAT will provide you with the full circle - Offence & defense.

Our platform allows our client to keep track of the payloads and defense rules executed and deployed, enabling him to have a clear view of where he stands.

A special notification window will alert our client when a new Payload/Defense rule is being added, keeping our client up to date with recent attacks happening

Being an offense-based solution Eye of the Enemy uses MITRE ATT&CK® framework.

Our payloads cover the following vectors:

* Initial Access
* A screenshot of a computer

  Description automatically generated with medium confidencePersistence
* Privilege escalation
* Data exfiltration
* Letteral movement
* Mail bypass
* System bypass
* Misconfiguration

**Going Proactive!**

# Executive Summary

On 08.03.2023, the client requested a security assessment to be conducted in order to determine whether an attacker can run Sharphound/Bloodhound on the organizational endpoints, and to identify the potential risks that may arise after an attacker gains initial access using a reverse shell.

The assessment was focused on identifying vulnerabilities in the organization's endpoint security, such as weaknesses in access controls, system configurations, and network segmentation. It also involved testing for the presence of common attack vectors that may be used by an attacker to gain access to the network, such as phishing attacks and malware infections. Once an attacker has gained access to the network using a reverse shell, the assessment will focus on identifying the extent of their ability to move laterally across the network and escalate their privileges. This will involve examining the organization's Active Directory (AD) configuration and access controls, as well as testing for any weaknesses in network segmentation.

The assessment will provide the client with a detailed report of the findings, including recommendations for mitigating identified vulnerabilities and improving the organization's security posture. By conducting this security assessment, the client can better understand their current security posture and take proactive measures to protect against potential attacks.

# Attack Emulation

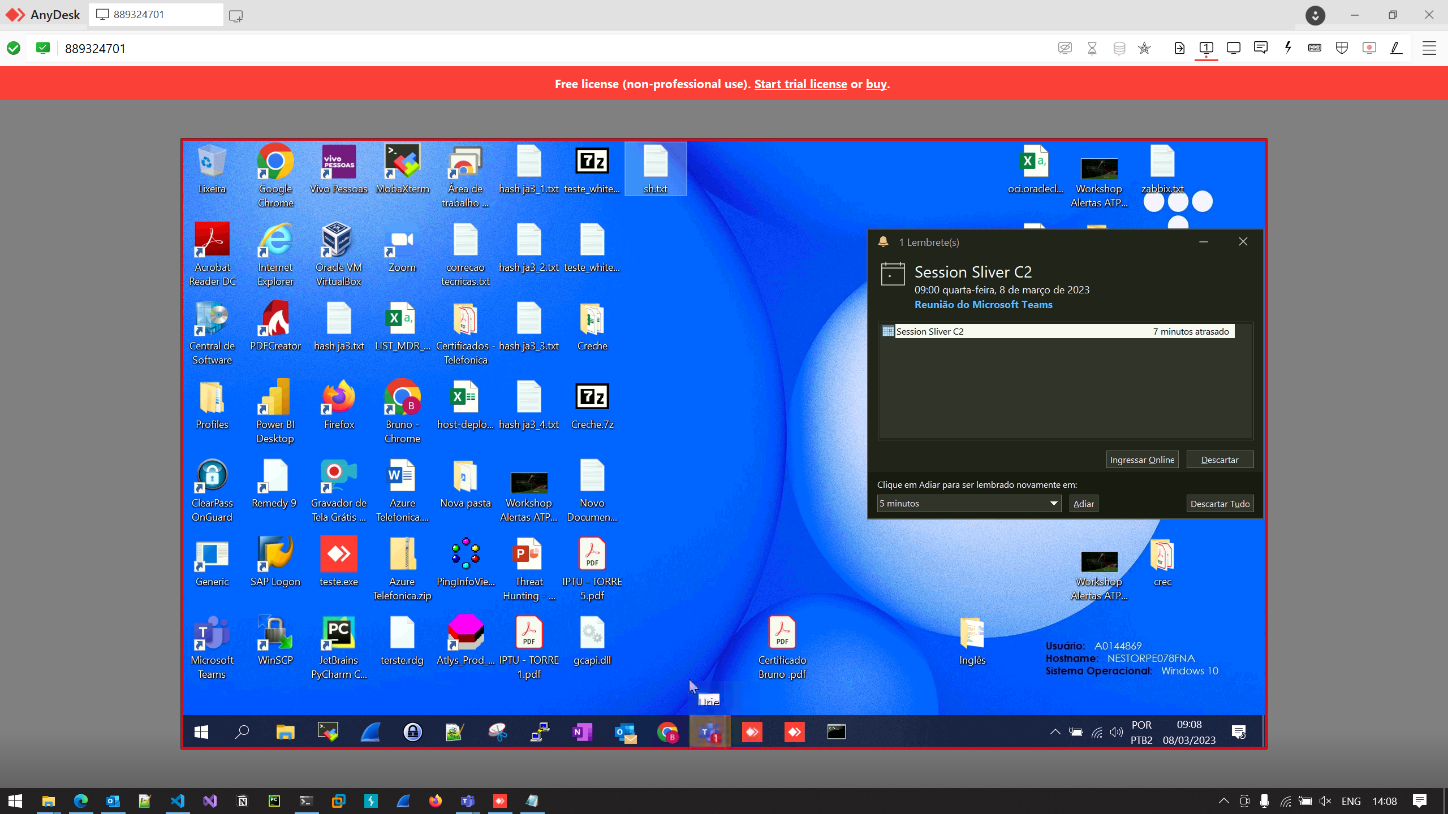
## **Scenario 1 – Defense Evasion and Domain Reconnaissance with SharpHound**

**Difficulty realizing the threat: Medium**

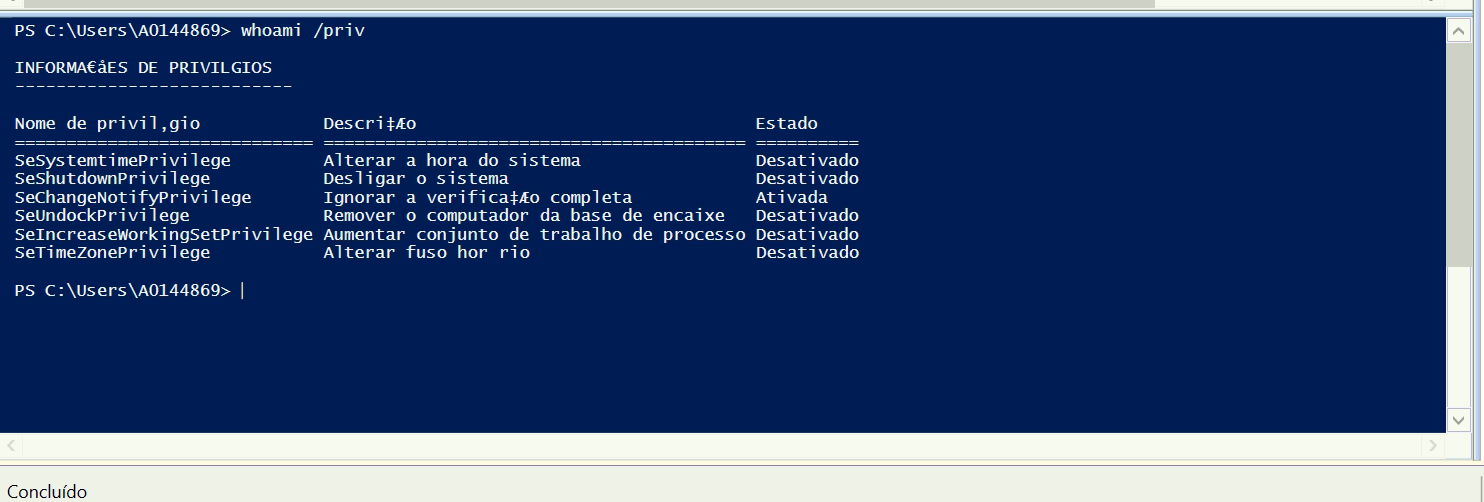
**Level of impact: High**

### **Proof of Concept**

First, White Hat gained a connection to two endpoints in the organizational network of Telefónica to conduct the Eye-of-the-Enemy assessment using the AnyDesk remote connection software:

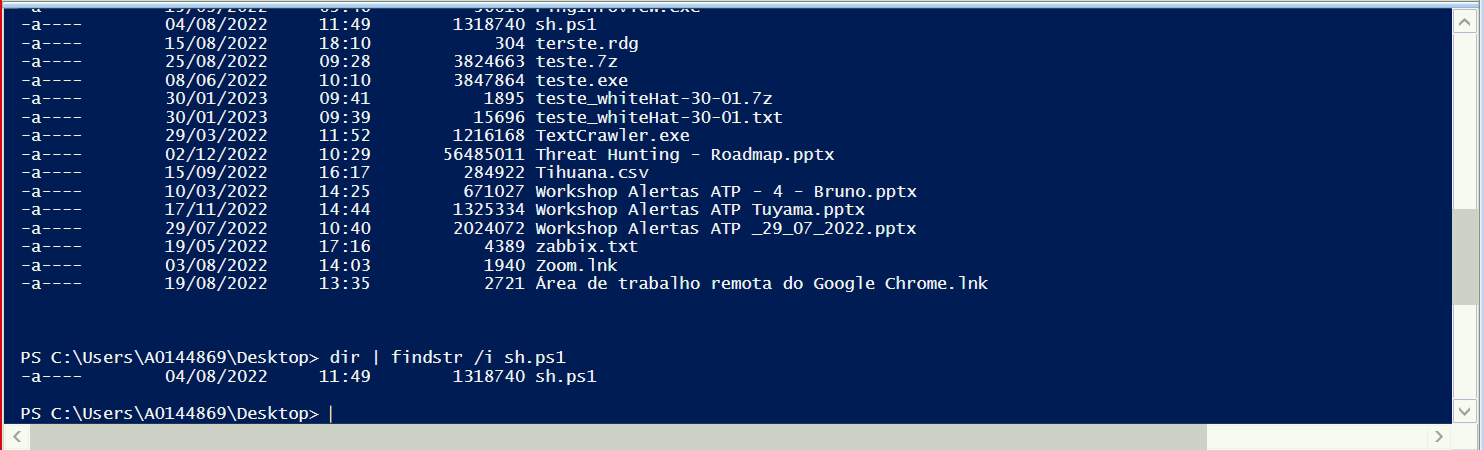


We proceed to start with our basic endpoint and domain reconnaissance / enumeration efforts. We checked and validated our user privileges as can be seen in the following screenshot:



In the above screenshot you can notice that we had regular user permissions without special administrative privileges.

Next, we tried to transfer PE-executable based files of SharpHouond.exe and it was detected and prevented immediately which is a sign of using **good security detections and practices**. Then we proceed to try and transfer other file types using different extensions like **PowerShell .ps1** files and we were succeed as can be seen in the following screenshot:

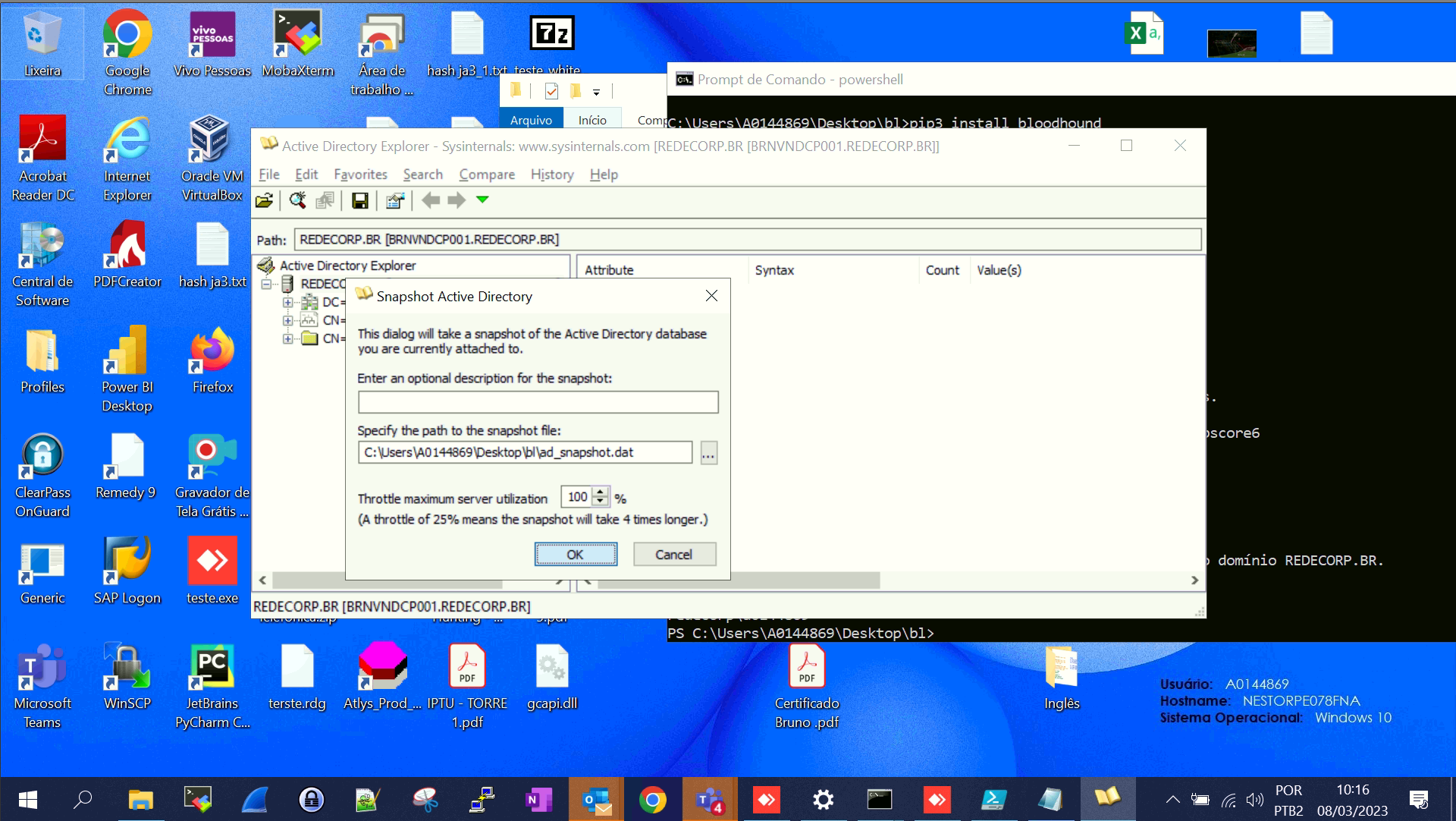


We tried to proceed and execute the PowerShell .ps1 version of SharpHound.ps1 and it was detected and prevented specifically because of the use of the **PowerShell / .NET Assembly.Reflection** method which is very common in offensive tools and is easily detected.

From here, we decided to proceed with a different technique of extracting the Active Directory database with all its necessary information to gain better understanding of the organizational network using the legitimate and Microsoft signed tool of **ADExplorer** which is part of the Sysinternals Microsoft suite:

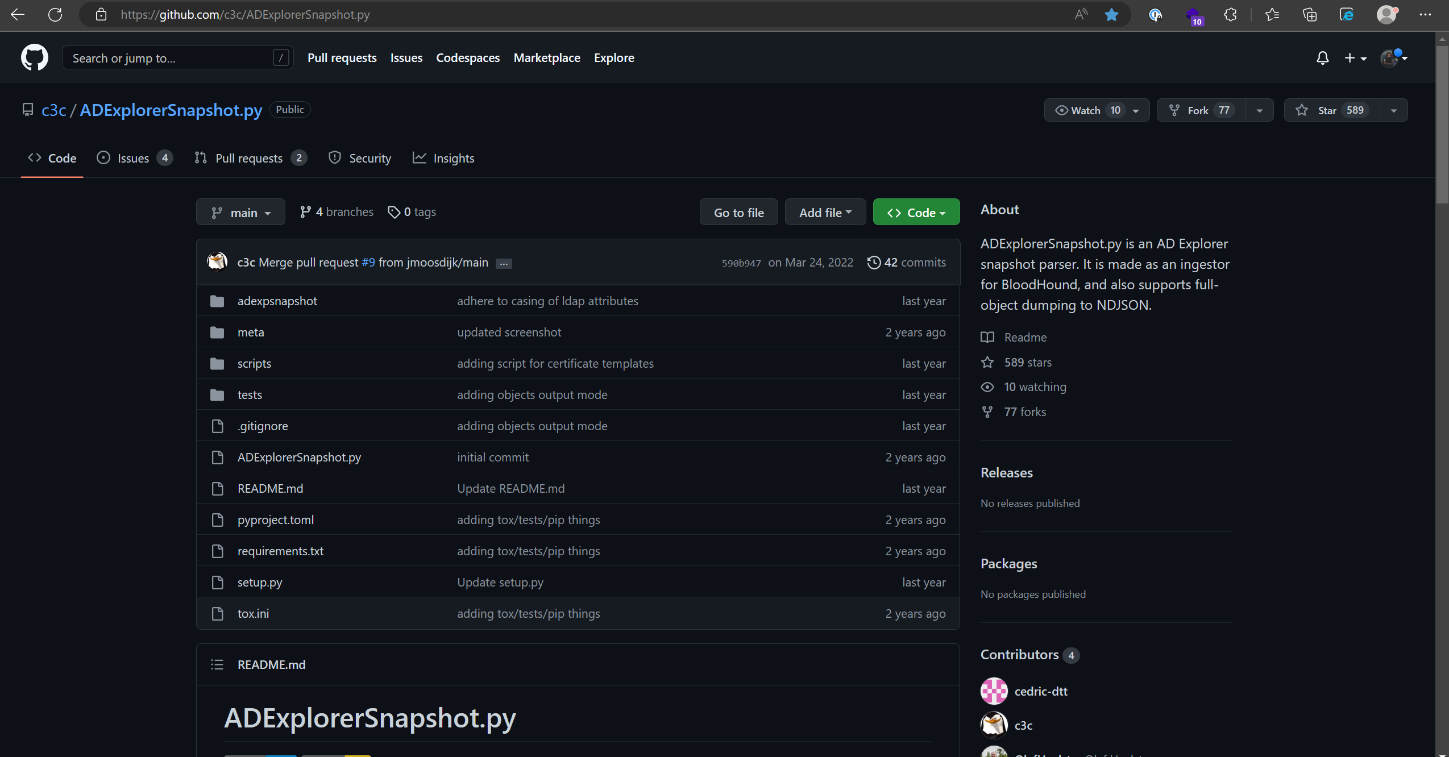
Graphical user interface, text, application, Word

Description automatically generated

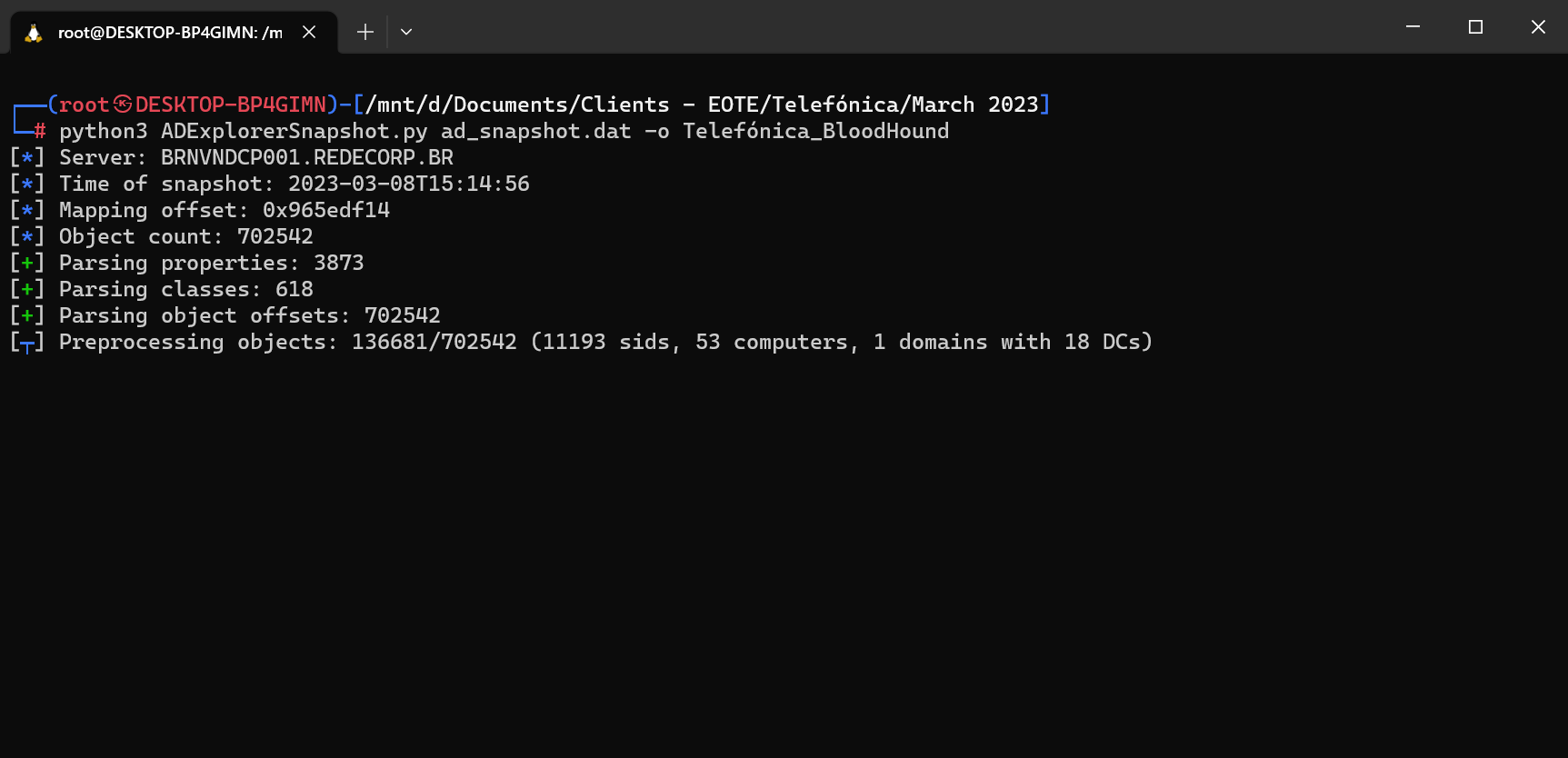


This attempt of dumping the Active Directory database using ADExplorer was successfully conducted with no detection and prevention taking place.

The following tool of ADExplorerSmapshot.py is used to convert the ADExplorer dump file:



The following screenshot demonstrates the usage of the tool which parses and converts ADExplorer’s .dat output file to a format to be used by the BloodHound tool:



### **Security Recommendations**

Although the current security practices are good, the following can be applied to enhance security:

* Block the usage of **ADExplorer.exe** and **ADExplorer64.exe** using AppLocker and other security controls like AV/EDR security solutions.
* Limit the use of domain reconnaissance / enumeration Windows-built-in net.exe and net1.exe commands (net user, group), nbtstat.exe.

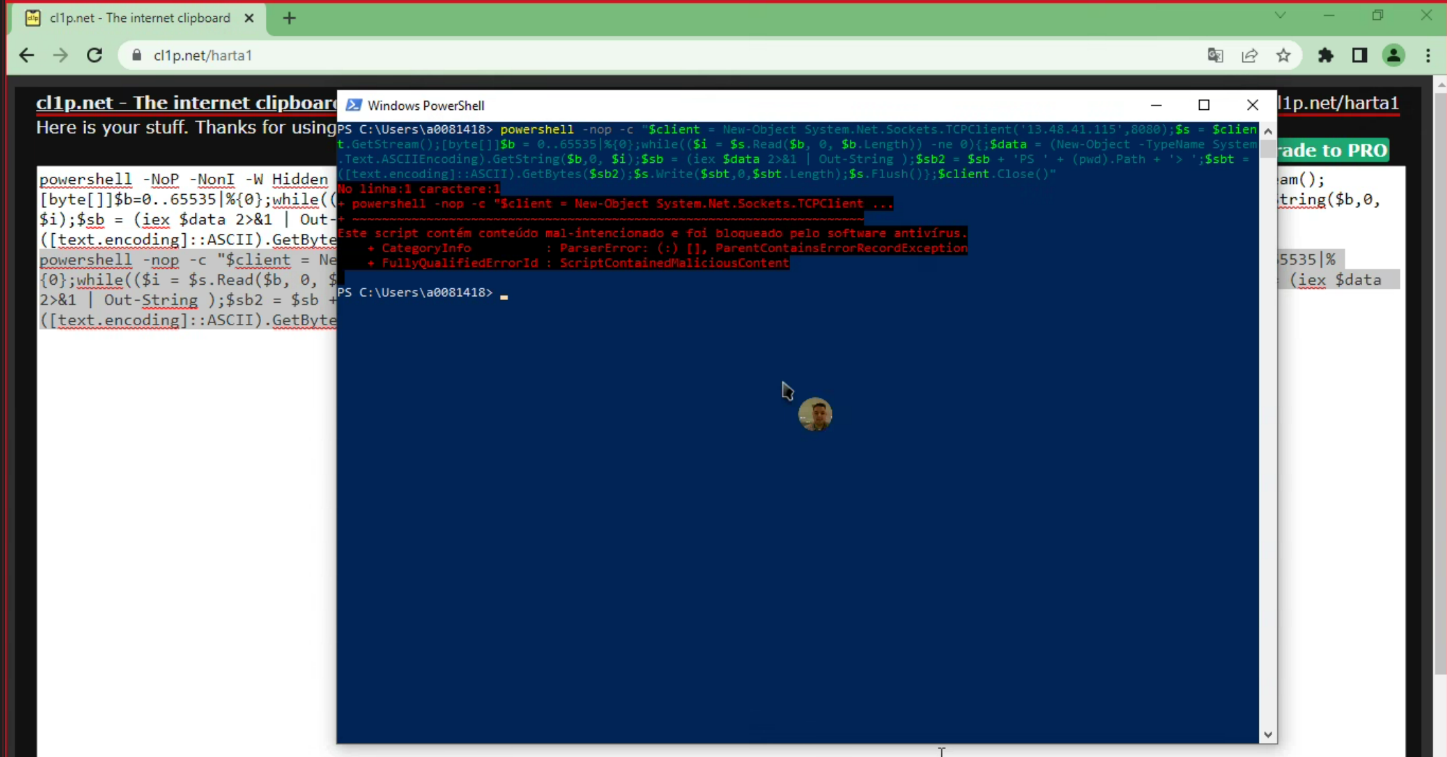
## **Scenario 2 - Initial Access & Command Execution using Python Reverse Shell**

**Difficulty realizing the threat: Medium**

**Level of impact: High**

### **Proof of Concept**

In this stage of the security assessment we continued to the reverse shell initial access vector. We first tried to execute a PowerShell inline script to gain a reverse shell on the victim machine and we it got detected and prevented successfully:

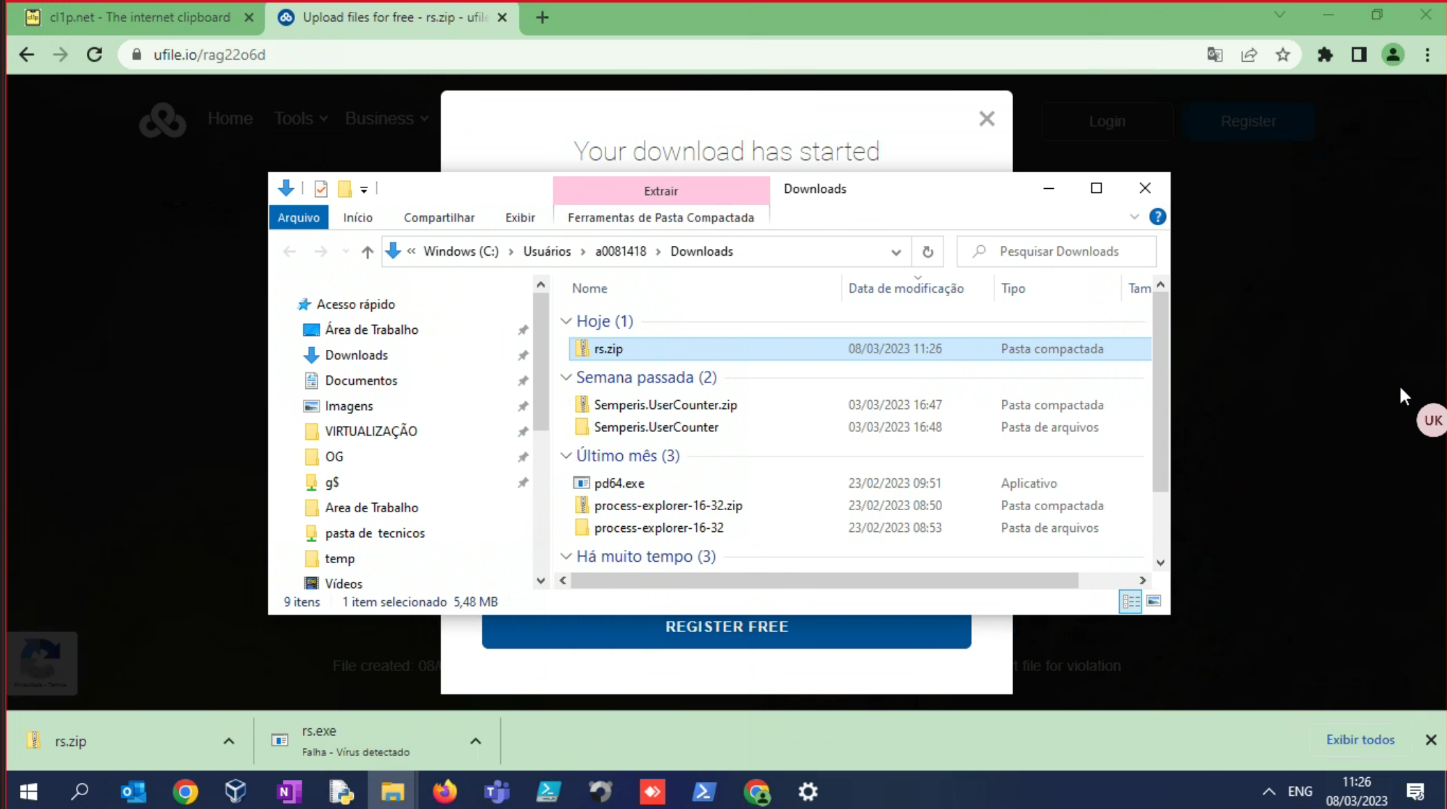


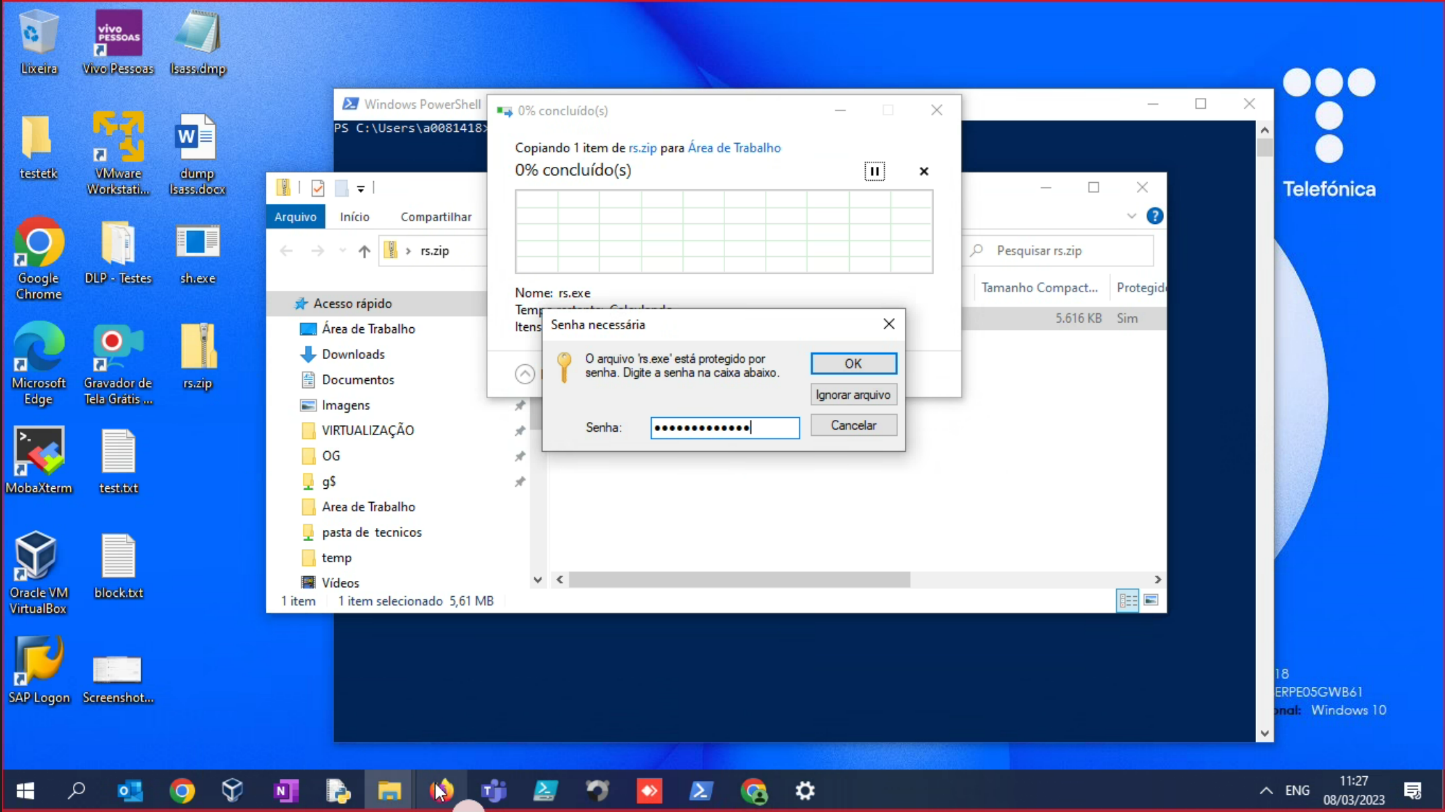
Then we proceed to running a Python based reverse shell with the following code written:

Graphical user interface, text, application, email

Description automatically generated

We tried to infiltrate a Python based script executable which was compiled/transformed to a PE-executable file using PyInsatller. In order to infiltrate the PE-executable file we used a ZIP file protected with password and we succeeded with this attempt as can be seen in the following screenshots:





And we succeeded to bypass three endpoint security AV/EDRs of: McAfee, Panda, and Defender ATP and to gain reverse shell to our attacker C2 server:

Text

Description automatically generated

From here we continued to assess and emulate specific techniques that most attackers use when gaining their first reverse shell foothold.

First we gained information regarding the main synchronized DC that the endpoint we gained reverse shell on is connected to:

Graphical user interface, text

Description automatically generated with medium confidence

Afterwards, we gleaned more information about running process for situational awareness purposes and to be aware of which AV/EDR/EPP products are deployed on this endpoint:

Text

Description automatically generated

From this point out we can continue to do the things we need as attackers to escalate privileges, laterally move in the network and gain more sensitive information from critical organizational assets.

### **Security Recommendations**

Although the current security practices are good, the following can be applied to enhance security:

* Do not install Python in network endpoints where it is not necessary.
* Use Group Policy, AppLocker, and other security controls like AV/EDR security solutions, if possible, to block the following processes:
  + cmd.exe (both x86 and x64).
  + powershell.exe (both x86 and x64).
  + powershell\_ise.exe (both x86 and x64).
* Apply network segmentation to ensure that only authorized network traffic can communicate between different segments. This can help prevent attackers from moving laterally within your network using reverse shells.
* Ensure that your firewall is properly configured to block all inbound and outbound traffic except for authorized traffic. This will help prevent attackers from establishing a reverse shell to a command and control server.
* Apply continuous monitoring of your network and systems to detect any suspicious activity or unauthorized access attempts. This can include monitoring for unusual network traffic or changes in system configurations.
* Disable any unused services and ports on your systems (Windows, Linux, etc.) to reduce the attack surface available to attackers. This can help prevent attackers from exploiting vulnerabilities in unused services to execute a reverse shell.