

# Threat Spotlight: Machete Info-Stealer

---

[threatvector.cylance.com/en\\_us/home/threat-spotlight-machete-info-stealer.html](https://threatvector.cylance.com/en_us/home/threat-spotlight-machete-info-stealer.html)

Adam Martin



RESEARCH & INTELLIGENCE / 11.27.19 / Adam Martin

## Introduction

---

Machete is an info-stealing malware that can harvest user credentials, chat logs, screenshots, webcam pictures, geolocation, and perform keylogging. It can also copy files to a USB device and take control of the clipboard to exfiltrate information.

Machete is typically distributed via social engineering techniques and malicious websites. The user is enticed into opening the original executable under the premise that they are opening a PowerPoint presentation. This is in fact a Nullsoft installer SFX.

The Powerpoint can range from illicit images to cleverly crafted images that are meant to represent government/ military documentation. The most common names being: "Hermosa xxx,pps,rar", "Suntzu.rar", and "Hot brazilian XXX.rar". Based on language found within the file along with open source information the intended targets appear to be Spanish speaking nations across Latin America. The payload is typically packaged as part of a PowerPoint presentation with Nullsoft installer SFX. The executables within the SFX are compiled using Python.

## Technical Analysis

---

### Static Analysis Pre/Post SFX Extraction

---

The original executable is disguised as a document; however, it is an SFX Nullsoft installation file:



*Figure 1: Original SFX disguised as a document*

Once extracted, the following folders are opened in the working directory, which also contains NullSoft SFX files:



*Figure 2: Phase 2 of SFX*



*Figure 3: Phase 3 of SFX*

The fourth extraction creates a folder containing a PowerPoint presentation file and another SFX file disguised as a Java executable:



*Figure 4: Phase 4 of extraction, revealing two files*

The JavaAlq.exe file contains a multitude of java executables along with a series of Python libraries:



*Figure 5: JavaAlq.exe post-extraction*

Each of the Java executables contained within the original JavaAlq.exe is compiled with a Python script. Each one contains a large volume of Python libraries necessary for the executable to be compiled and run. These Java executables all contain a payload component:



*Figure 6: Python-script resource section found in each Java executable*

The raw script can be extracted from the executables using a Py2Exe Binary Editor:



*Figure 7: Java.exe PythonScript being dumped*

Once this Python script has been dumped it needs to be converted into a Python file using an open source Python script extractor:



*Figure 8: PythonScript extractor*

The final step involved in producing the malicious script is to decompile the Python script. This is done with Easy Python Decompiler:



*Figure 9: Decompiled PythonScript for Java.exe*

## Malicious Payloads

---

### Java.exe

---

The keylogging functionality contained within the payload of Java.exe is shown in Figure 10. The standard ascii keys are listed with their key IDs. The hook for the keyboard is also set within this script:



*Figure 10: Key IDs used to log keystrokes*



*Figure 11: Keyboard hook set*

Evidence of connection to the remote server contained within java.exe is shown in Figure 12:



*Figure 12: FTP connection to remote server 2*

### Document Type Check JavaUE.exe

---

Contained within the payload of JavaUE.exe is a document type check of a target directory:



*Figure 13: Checking for document extension types in the target directory*

### JavaK.exe Payload Script

---

Figure 14 illustrates the webcam information being sent to a remote server. Interestingly, it sets the resolution at which to capture information to a low resolution in order to expedite exfiltration of images:



*Figure 14: Webcam exfiltration*

### JavaTM.exe Payload Script

---

JavaS.exe is run as the last process. It terminates the rest of the spawned processes then deletes them from the victim machine:



*Figure 15: Deletion of Java files and termination of processes*

## Dynamic Analysis

---

When the script is executed, a series of files are created along with the Java labelled executables. A crypto.cipher.AES Python file is dropped which is used to encrypt the exfiltrated data sent to the FTP server. It is also used to assign an encrypted unique identifier to each victim machine. The other files installed are Python libraries necessary for the executable to run its payload. The system information text file is created to record data from the victim machine.

## Conclusion

---

Blackberry Cylance uses artificial intelligence-based agents trained for threat detection on millions of both safe and unsafe files. Our automated security agents block Machete based on countless file attributes and malicious behaviors instead of relying on a specific file signature.

Blackberry Cylance, which offers a predictive advantage over zero-day threats, is trained on and effective against both new and legacy cyberattacks. If you are a Blackberry Cylance customer using CylancePROTECT®, you are protected from Machete by our machine learning models.

For more information, visit <https://www.cylance.com>.

## APPENDIX

---

### Indicators of Compromise (IoCs)

---

Indicator	Type	Description
C:\Windows\system32\cmd.exe /c SCHEDULETASKS /create /ST 00:00:01 /SC MINUTE /MO 60 /TR "\"C:\Users\%USERNAME%\AppData\Roaming\MicroDes\JavaH.exe\"" /TN Microsoft_up, null".	Command-line	Scheduled task used to launch JavaH.exe as a service
C:\Users\%USERNAME%\AppData\Roaming\java	Path	Install folder
C:\Users\%USERNAME%\AppData\Roaming\Bin\Jre6\	Path	Install folder
C:\Users\%USERNAME%\AppData\Roaming\MicroDes	Path	Install folder
caso.txt	File	Present in install folder
Java.exe	File	Present in install folder
JavaD.exe	File	Present in install folder

---

JavaH.exe	File	Present in install folder
JavaK.exe	File	Present in install folder
JavaS.exe	File	Present in install folder
JavaTM.exe	File	Present in install folder
JavaUe.exe	File	Present in install folder
JavaAlq.exe	File	Present in install folder
Ujavap.exe	File	Present in install folder

---

## File Information

---

**SHA256**    **bf25b330975dc700be3f1f6b1b3362e34eb84b89725d4936d893cdd4f1499e69**

---

**Type**        Win32 EXE NullSoft SFX

---

**Size**         4830 KB


---

**Timestamp**   2008-08-16 20:26:10 (Time-stamped)

---

**ITW names**   Machete, Trojan/Spy.Python.Ragua

---

 Adam Martin

## About Adam Martin

---

Threat Researcher at BlackBerry Cylance

Adam Martin is currently working as a Threat Researcher in Cork, Ireland, having graduated from Cork Institute of Technology in summer 2019. Adam completed an internship with BlackBerry Cylance in his third year of college and was lucky enough to be kept on afterwards!

---

[Back](#)