The Introduction of the Jupyter InfoStealer/Backdoor

blog.morphisec.com/jupyter-infostealer-backdoor-introduction

- Tweet

An **Infostealer** is a trojan that is designed to gather and exfiltrate private and sensitive information from a target system. There is a large variety of info stealers active in the wild, some are independent and some act as a modular part of a larger task such as a Banking Trojan (Trickbot) or a RAT.

Infostealers are usually lightweight and stealthy payloads that do not have persistence or propagation (get-in and get-out) capabilities. This type of trojan is particularly difficult to detect as it leaves an extremely small footprint.

During what began as a routine incident response process, Morphisec has identified (and prevented) a new .NET infostealer variant called **Jupyter.** Morphisec discovered this variant as part of assisting a higher education customer in the U.S. with their incident response.

Jupyter is an infostealer that primarily targets Chromium, Firefox, and Chrome browser data. However, its attack chain, delivery, and loader demonstrate additional capabilities for full backdoor functionality. These include:

- a C2 client
- download and execute malware
- execution of PowerShell scripts and commands
- hollowing shellcode into legitimate windows configuration applications.

Jupyter's attack chain typically starts with a downloaded zip file that contains an installer, an executable that usually impersonates legitimate software such as Docx2Rtf. Some of these installers have maintained **0** detections in VirusTotal over the last 6 months, making it exceptional at bypassing most endpoint security scanning controls.

Upon execution of the installer, a .NET C2 client (**Jupyter Loader**) is injected into a memory. This client has a well defined communication protocol, versioning matrix, and has recently included persistence modules.

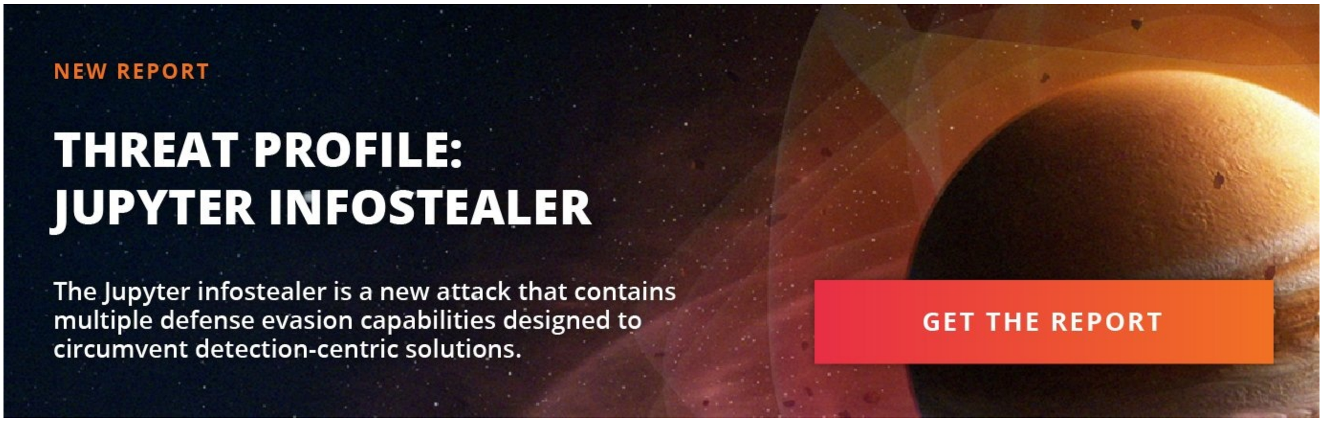
The client then downloads the next stage, a PowerShell command that executes the in-memory **Jupyter** .NET module. Both of the .Net components have similar code structures, obfuscation, and unique UID implementation. These commonalities indicate the development of an end to end framework for implementing the Info stealer.

Morphisec has monitored a steady stream of forensic data to trace multiple versions of **Jupyter** starting in May 2020. While many of the C2s are no longer active, they consistently mapped to Russia when we were able to identify them.

This is not the only piece of evidence that this attack is likely Russian in origin. First, there is the noticeable Russian to English misspelling of the planet name. Additionally, Morphisec researchers ran a reverse Google Image search of the C2 admin panel image and were not surprised to find the exact image on Russian-language forums.

Download the complete report for details on the changes and evolution of the Jupyter infostealer as well as its backdoor component.

Note: Morphisec CTO Michael Gorelik contributed to this analysis.



NEW REPORT

THREAT PROFILE:
JUPYTER INFOSTEALER

The Jupyter infostealer is a new attack that contains multiple defense evasion capabilities designed to circumvent detection-centric solutions.

Contact SalesInquire via Azure