Chae$ Chronicles: Version 4.1 Dedicated to Morphisec Researchers

blog.morphisec.com/chaes-chronicles

Arnold Osipov

- Tweet
-

In ongoing efforts to monitor and analyze emerging cyber threats, Morphisec Threat Labs has recently turned its focus to Chae$ 4.1, an update to the Chaes malware Infostealer series. This version introduces key updates, including an improved Chronod module, and features a unique aspect: a direct message to the Morphisec team within the source code.

Introduction

This blog post will briefly touch upon the updates in Chae$ 4.1 and mention Morphisec's initial interaction with the hackers. It will also cover several previously unknown details of the delivery chain.

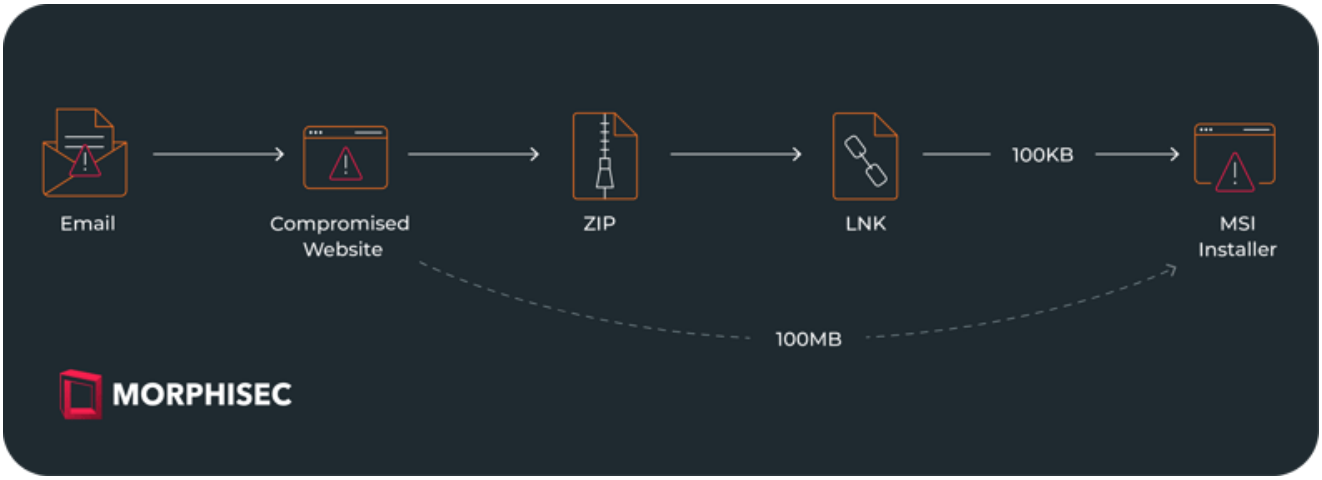
For those interested in an in-depth technical analysis, we have prepared a comprehensive report on Chae$ 4.1, available for download.

Download the full Chae$ 4.1 technical analysis containing exclusive details.

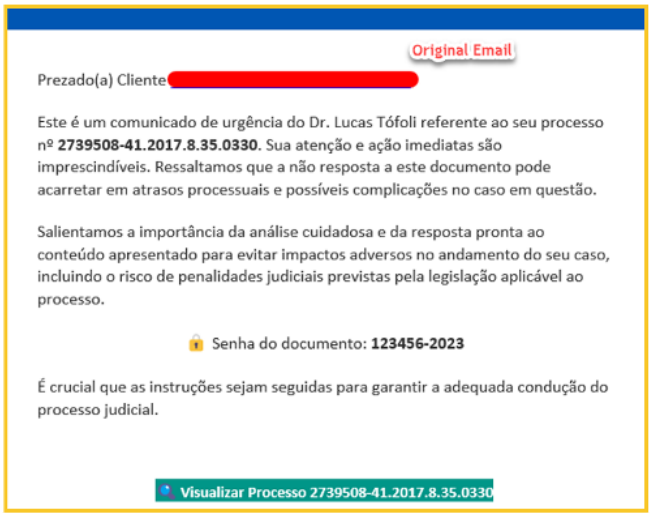
```
print('Dear, Mr. Arnold Osipov:')
print('')
print('We sincerely hope our efforts meet your expectations.')
print('If you write a detailed analysis about our software, we will')
print('write better code based on these analysis.')
print('')
```

The Chae$ authors dedicated parts of their source code to the Morphisec researchers

Infection Chain



The infection chain starts with an email written in Portuguese, which purports to be an urgent communication request from a lawyer regarding a legal case. The email pressured the victim with an urgent call for “prompt response”, or risk highly adverse legal repercussions. The email includes a link and a password to access the document from that link.


Original Email

Prezado(a) Cliente [redacted]

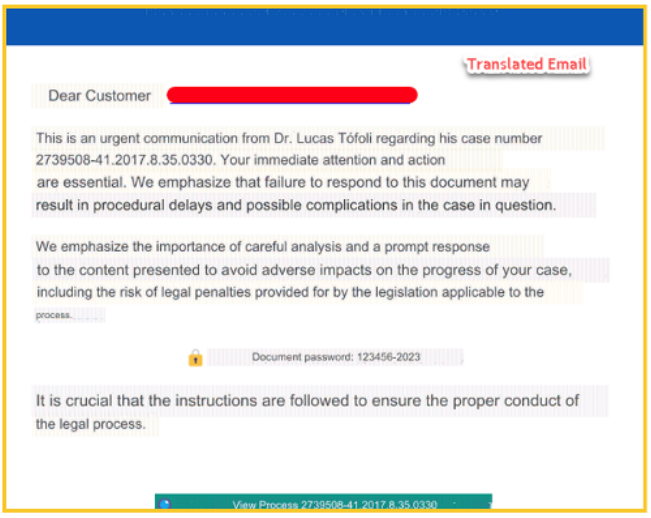
Este é um comunicado de urgência do Dr. Lucas Tófoli referente ao seu processo nº **2739508-41.2017.8.35.0330**. Sua atenção e ação imediatas são imprescindíveis. Ressaltamos que a não resposta a este documento pode acarretar em atrasos processuais e possíveis complicações no caso em questão.

Salientamos a importância da análise cuidadosa e da resposta pronta ao conteúdo apresentado para evitar impactos adversos no andamento do seu caso, incluindo o risco de penalidades judiciais previstas pela legislação aplicável ao processo.

Senha do documento: **123456-2023**

É crucial que as instruções sejam seguidas para garantir a adequada condução do processo judicial.

Visualizar Processo 2739508-41.2017.8.35.0330


Translated Email

Dear Customer [redacted]

This is an urgent communication from Dr. Lucas Tófoli regarding his case number 2739508-41.2017.8.35.0330. Your immediate attention and action are essential. We emphasize that failure to respond to this document may result in procedural delays and possible complications in the case in question.

We emphasize the importance of careful analysis and a prompt response to the content presented to avoid adverse impacts on the progress of your case, including the risk of legal penalties provided for by the legislation applicable to the process.

Document password: 123456-2023

It is crucial that the instructions are followed to ensure the proper conduct of the legal process.

View Process 2739508-41.2017.8.35.0330

Delivery via attacker Controlled Websites

Upon clicking the provided link, the victim will be redirected to https://totalavprotection[.]shop/abrirProcesso.php?email=<victims_email>. Then, the victim will be prompted to input the provided password to download the document, which is a ZIP file. This website https://totalavprotection[.]shop additionally functions as a deceptive website for TotalAV, directly delivering the MSI installer without the intermediary step of a ZIP file.

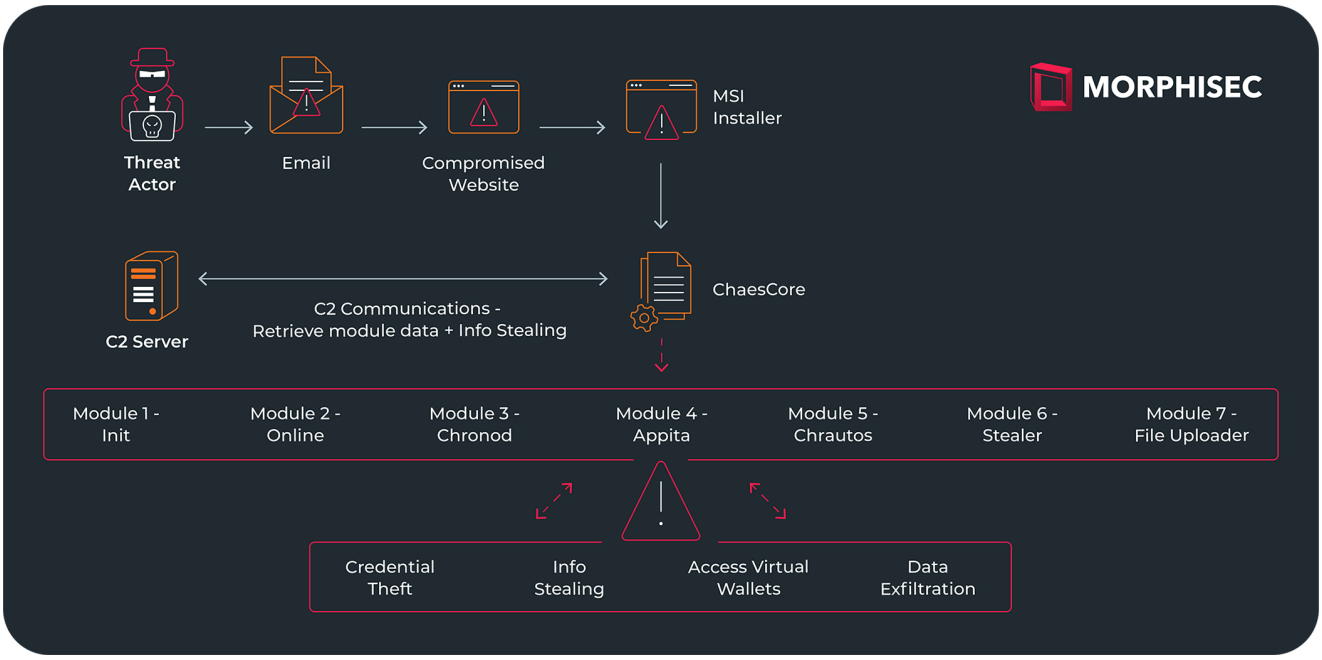
Yet another website delivers the malicious payload directly as an MSI installer. https://www.webcamcheck[.]online/ A website that allegedly scans the machine for risks and suggests updating the machine's driver after "scanning". After the victim clicks the BLOCK button (marked in red), a JavaScript is executed in the background. The script is designed to mimic the appearance of a legitimate system scan. During the simulated scan, a hardcoded list of files is presented, giving the illusion of a comprehensive analysis of the victim's computer.

Following the scan, the victim is then shown with a crafted message: “Security Risk Detected” and urges the victim to download an updated driver to install the latest version and eliminate the risk.

Clicking the button triggers the execution of a script named download.js. Whose purpose is to smuggle the malicious installer by decoding a zipped base64 blob. Following the activation of the installer, Chae$ 4.1 is activated.

Chae$ 4.1 — Changes

From this point onward, the attack chain remains similar to Morphisec’s previous analysis, except for some adjustments in the Chae$ framework. It has advanced from version 4 to 4.1, primarily characterized by modifications in the Chronod module.

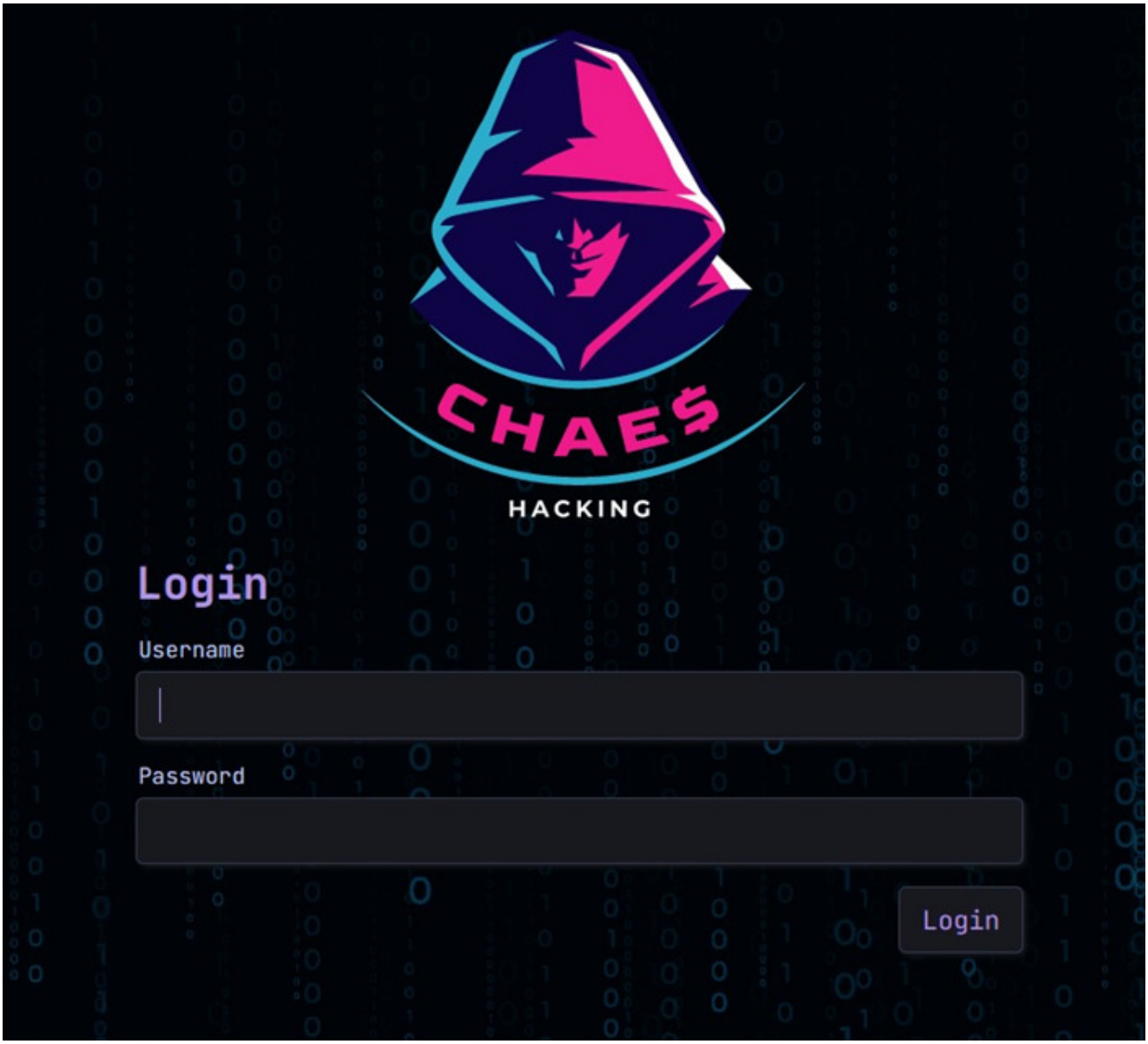


The full components of Chae$, as reviewed in the analysis of Chae$4

In fact, the advancement to Chae$ 4.1 is clearly shown in debug messages:


Oops!...I did it again

Following successful activation, exfiltrated data is delivered to the threat actor's C2. Examining the C2s employed throughout distinct phases of the framework unveils the presence of the Chae$ team panel login page.



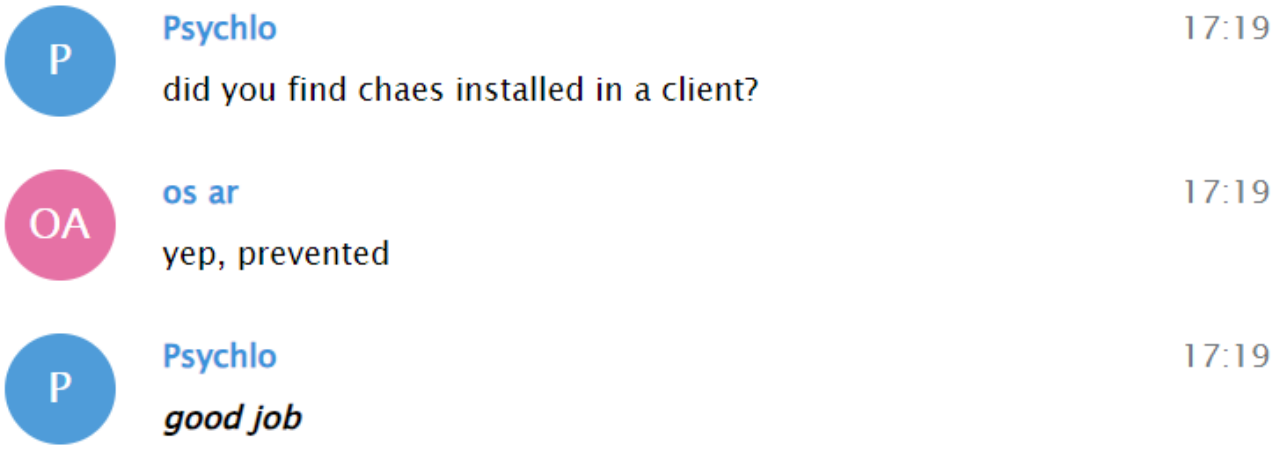
Full Technical Analysis of Chae$ 4.1

The attached report dives deeper into the new Chae$ variant. Read the full Chae$ 4.1 analysis to delve deeper into the mechanics of this evolved malware, its implications, and what businesses can do to safeguard themselves.

How Morphisec Helps

Morphisec's Automated Moving Target Defense (AMTD) technology uses a preventative approach to cybersecurity, using an ultra-lightweight agent to block unauthorized processes deterministically, rather than probabilistically. Protecting over 7,000 organizations and deployed at over nine million endpoints, Morphisec's AMTD technology prevents unauthorized code from executing, regardless of whether a recognizable signature or behavior pattern exists.

If you don't believe us, ask the Chae$ group:



Morphisec researchers were contacted by the threat actors, leading to an interesting exchange...

Schedule a demo to experience Morpisec's advanced anti-ransomware, endpoint protection and risk-based vulnerability prioritization. Reduce Risk Now.