The Evolution of the FIN7 JSSLoader

By Arnold Osipov

Archived: 2026-04-06 02:04:37 UTC

This report has been updated with assistance from the cybersecurity community.

Introduction

Morphisec Labs has been tracking FIN7 (Carbanak Group) activity for the past several years. Morphisec's ability to collect rich forensic data from memory has provided unique visibility into multiple FIN7 campaigns that our researchers were proud to share with MITRE and the InfoSec community at large. Fin7 is a well-funded financially motivated cybercrime group. Their advanced techniques and tactics were even emulated in the third round of the MITRE ATT&CK evaluations.

This report presents an attack chain that was intercepted and prevented within a customer's network in December 2020, then will focus on a component from a typical FIN7 attack chain – **JSSLoader**. Though JSSLoader is well known as a minimized .NET RAT, not many details have been publicly available with respect to various capabilities such as exfiltration, persistence, auto-update, malware downloading, and more. Furthermore, in the many occasions where JSSLoader is mentioned, there are few details on the complete attack chain. The following provides a never before seen technical analysis of this infamous group's JSSLoader as part of an end to end attack.

FIN7 JSSLoader Technical Analysis

Below is an example of a typical phishing campaign that may lead to a FIN7 JSSLoader compromise as well as to other malwares such as QBOT; the traffic is then redirected through BlackTDS traffic distribution system. In this example an email is being sent from "Natural Health Sherpa" with an invoice to pay from Quickbooks.

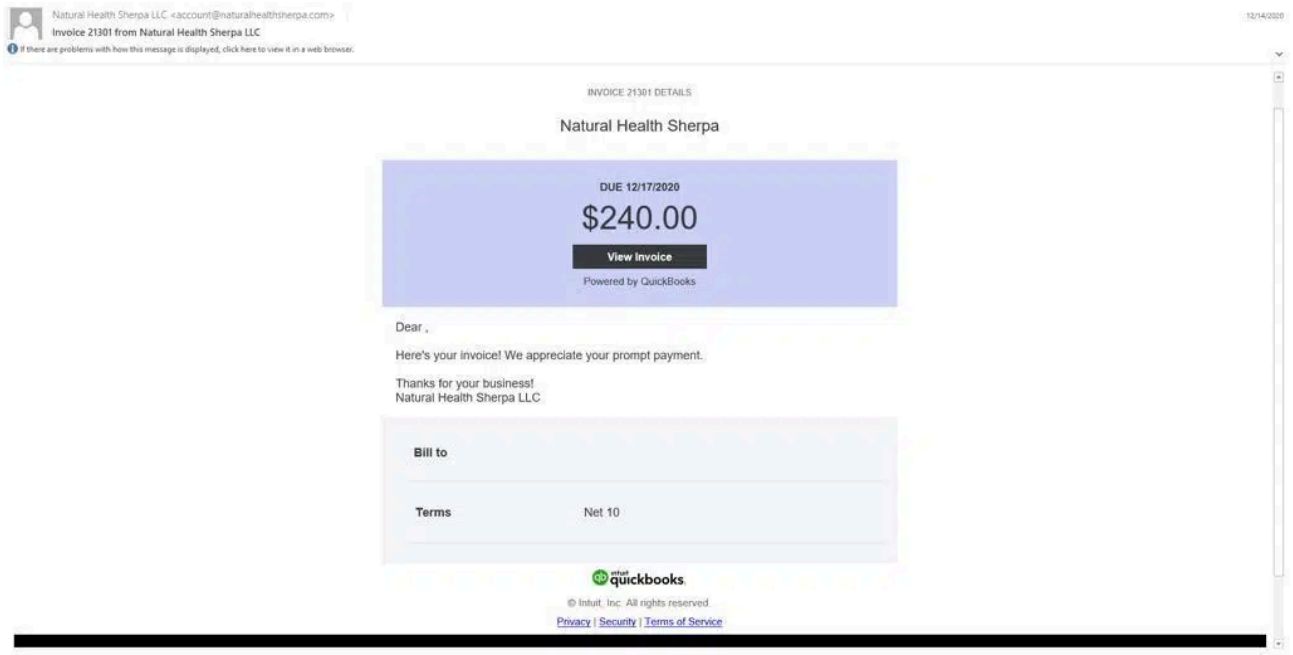


Figure 1: A typical phishing campaign

Clicking the invoice link leads to a private Sharepoint directory that stores an archive file containing a VBScript (later changed to WSF-Windows Script File).

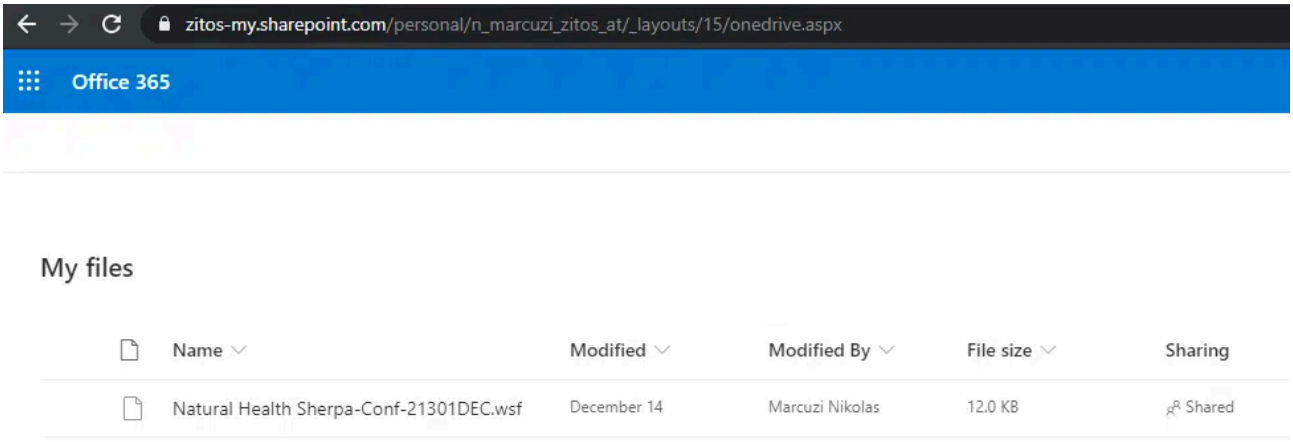


Figure 2: The private Sharepoint directory.

Shortly after this *phishing campaign "Natural Health Sherpa"* posted this on social media.

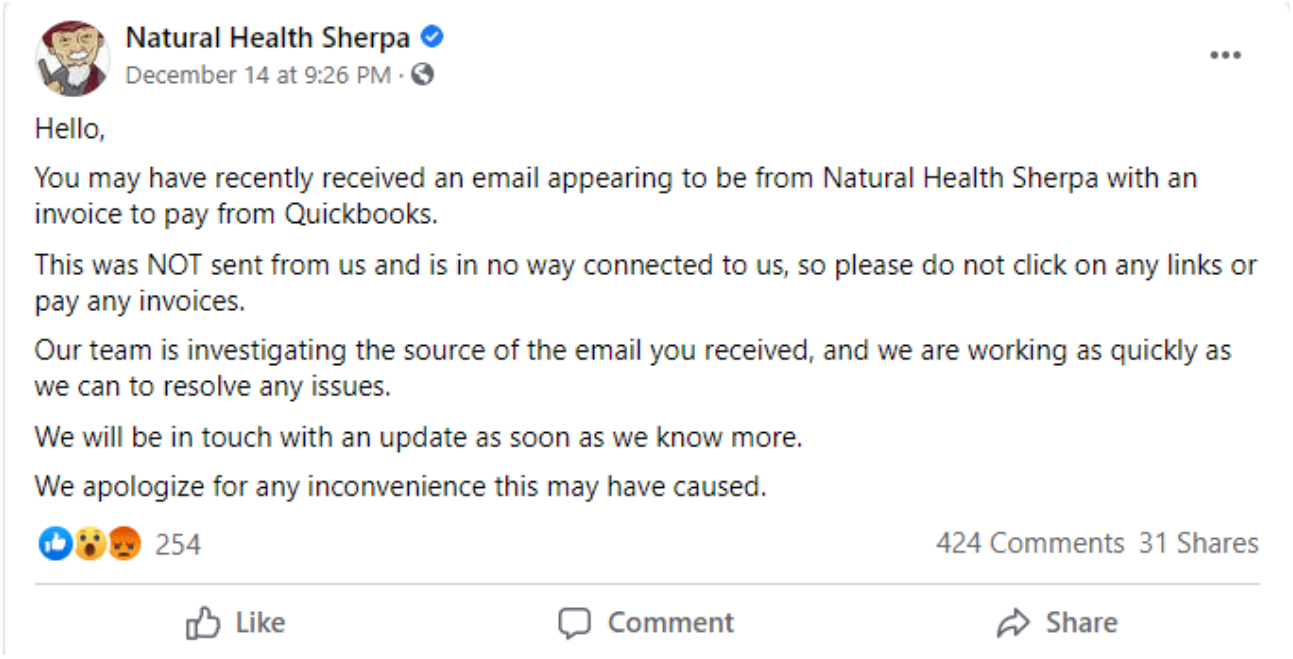


Figure 3: Natural Health Sherpa's message on social media.

This VBScript downloads and executes the next stage's VBScript in memory. This second stage was recently introduced. The in-memory script downloads and writes a .NET module (JSSLoader) on disk, then executes the module through a scheduled task with a newly introduced timeout delay to bypass attack chain monitoring.

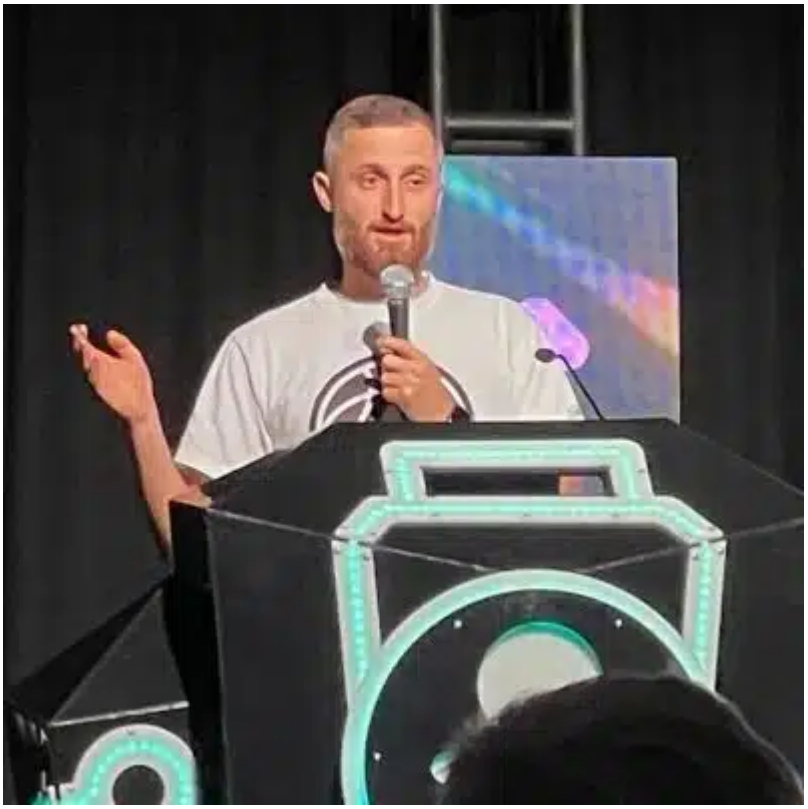
It is worth mentioning that the early versions of the VB scripts have a strong resemblance to the ongoing QBOT campaign that may lead to an Egregor compromise.

The *JSSLoader* is a RAT (Remote Access Trojan) with multiple capabilities that were introduced over time. These various capabilities are documented throughout this report. In the specific attack chain that was recently intercepted, the RAT typically executes a Takeout script which is responsible for the reflective loading and execution of a Carbanak.

Not surprisingly, the C2 hosting provider is a company named FranTech Solutions, which has been used before by the FIN7 group.

Note: Morphisec CTO Michael Gorelik contributed to this analysis.

About the author



Arnold Osipov

Malware Researcher

Arnold Osipov is a Malware Researcher at Morphisec, who has spoken at BlackHat and and been recognized by Microsoft Security for his contributions to malware research related to Microsoft Office. Prior to his arrival at Morphisec 6 years ago, Arnold was a Malware Analyst at Check Point.
