Agent Tesla Updates SMTP Data Exfiltration Technique

By SANS Internet Storm Center

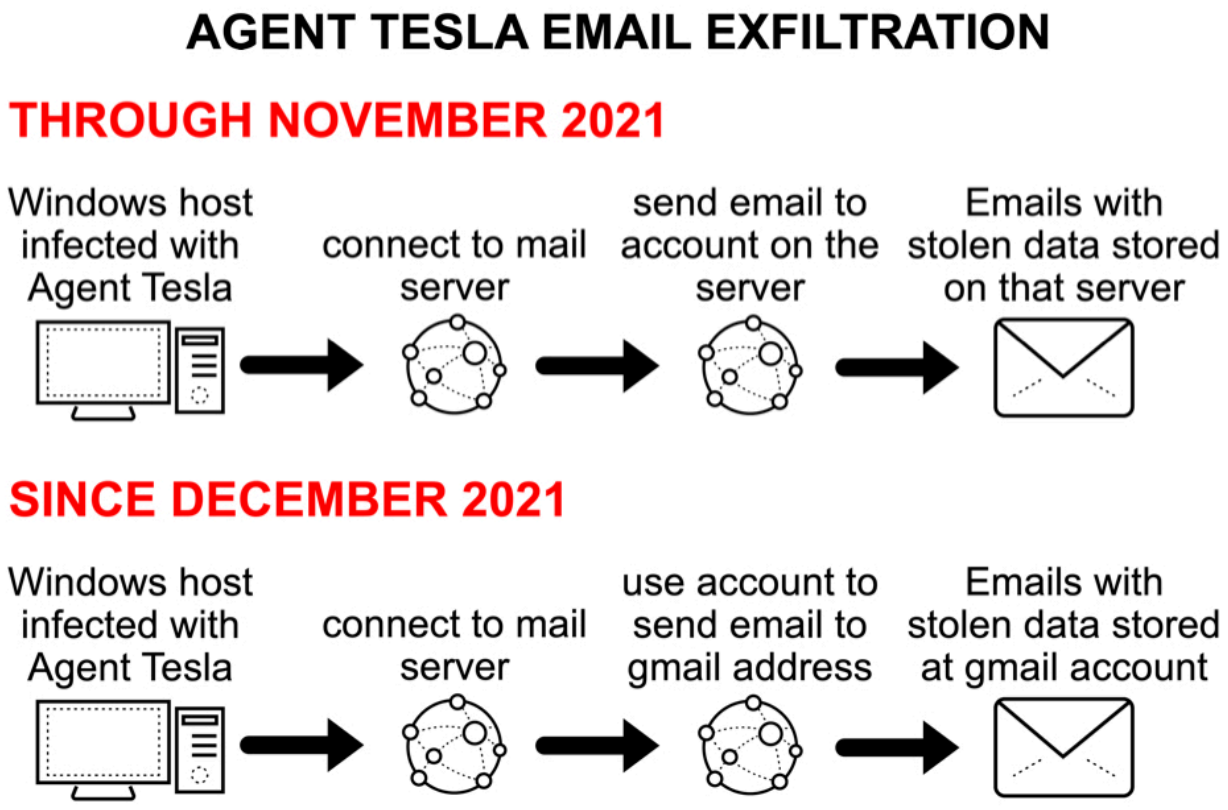
Archived: 2026-04-05 23:11:26 UTC

Introduction

Agent Tesla is a Windows-based keylogger and RAT that commonly uses SMTP or FTP to exfiltrate stolen data. This malware has been around since 2014, and SMTP is its most common method for data exfiltration.

Earlier today, I reviewed post-infection traffic from a recent sample of Agent Tesla. This activity revealed a change in Agent Tesla's SMTP data exfiltration technique.

Through November 2021 Agent Tesla samples sent their emails to compromised or possibly fraudulent email accounts on mail servers established through hosting providers. Since December 2021, Agent Tesla now uses those compromised email accounts to send stolen data to Gmail addresses.



Shown above: Flow chart of recent change in Agent Tesla SMTP data exfiltration.

SMTP exfiltration before the change

Agent Tesla is typically distributed through email, and the following sample was likely an attachment from malicious spam (malspam) sent on 2021-11-28.

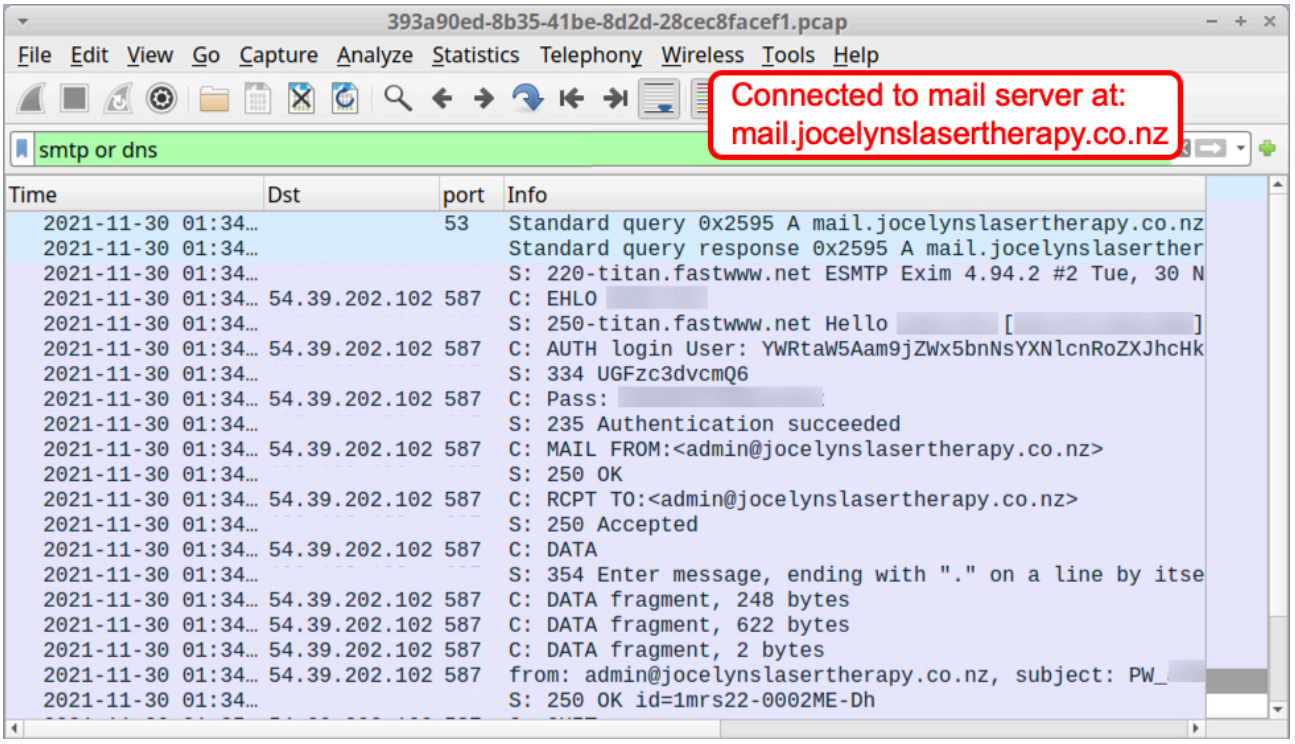
SHA256 hash: bdae21952c4e6367fe534a9e5a3b3eb30d045dcb93129c6ce0435c3f0c8d90d3

- File size: 523,919 bytes
- File name: Purchase Order Pending Quantity.zip
- Earliest Contents Modification: 2021-11-28 19:55:50 UTC

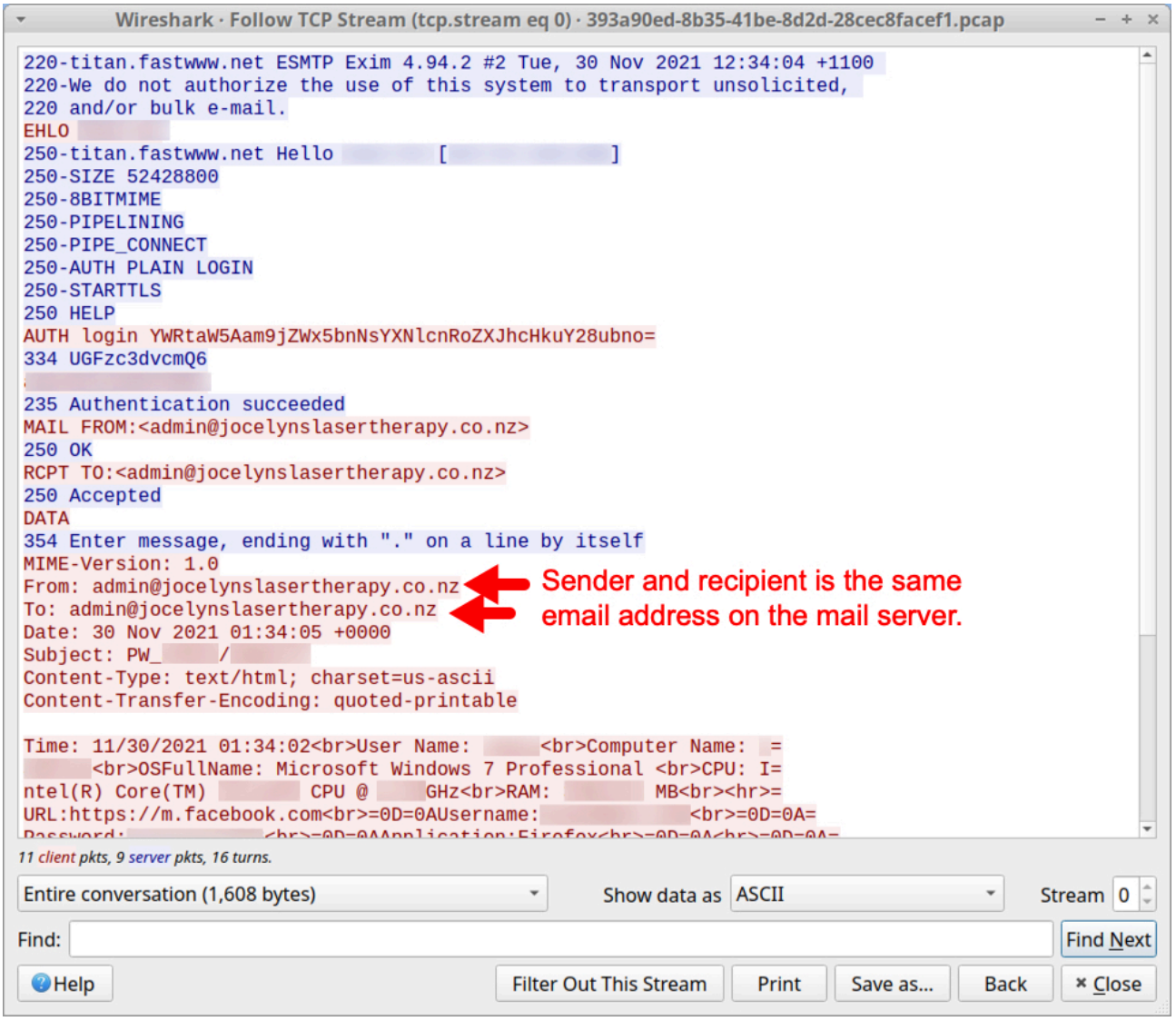
SHA256 hash: aa4ea361f1f084b054f9871a9845c89d68cde259070ea286babeadc604d6658c

- File size: 557,056 bytes
- File name: Purchase Order Pending Quantity.exe
- Any.Run analysis from 2021-11-29: link

The packet capture (pcap) from Any.Run's analysis shows a typical SMTP data exfiltration path. The infected Windows host sent a message with stolen data to an email address, and that address was on a mail server established through a hosting provider.



Shown above: Traffic from the Any.Run analysis filtered in Wireshark.



Shown above: TCP stream of SMTP traffic shows stolen data sent to the compromised email account.

Example after the change

The following Agent Tesla sample was likely an attachment from malspam sent on 2021-12-01.

SHA256 hash: 6f85cd9df964afc56bd2aed7af28cbc965ea56e49ce84d4f4e91f4478d378f94

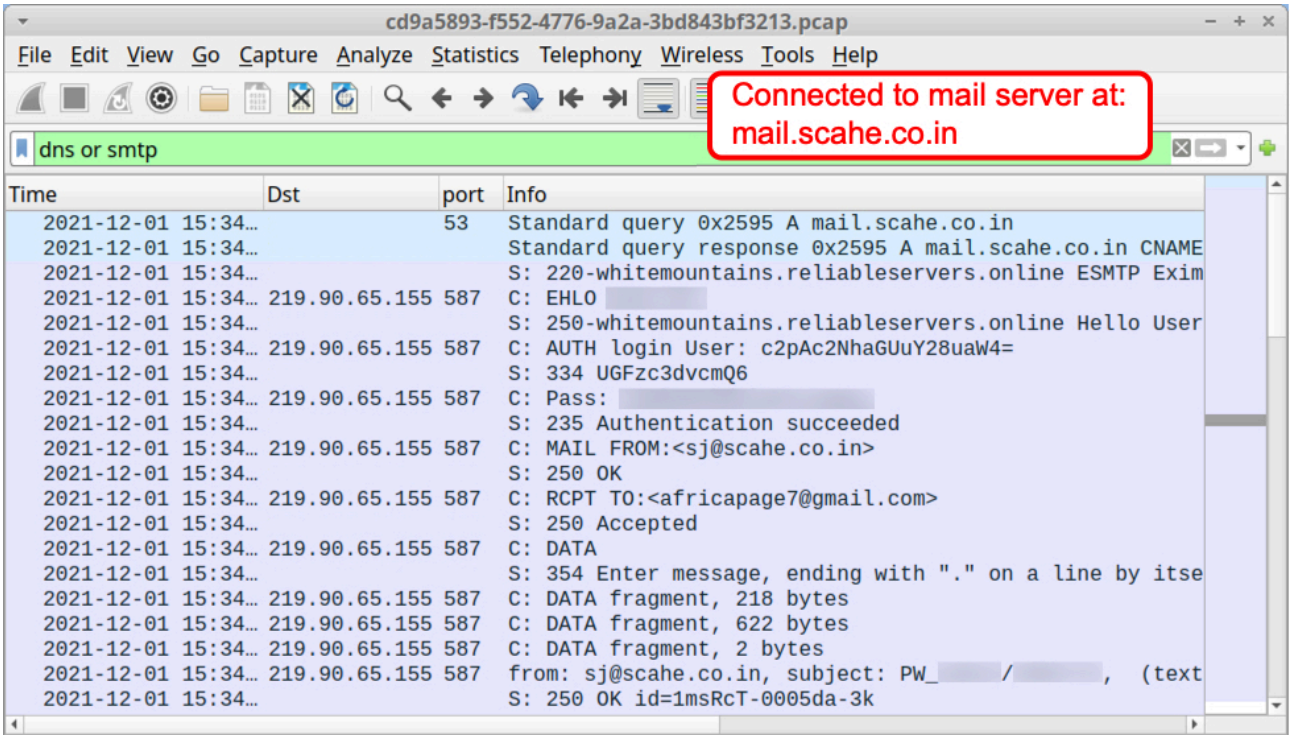
- File size: 375,734 bytes
- File name: unknown
- Earliest Contents Modification: 2021-12-01 05:02:06 UTC

SHA256 hash: ff34c1fd26b699489cb814f93a2801ea4c32cc33faf30f32165b23425b0780c7

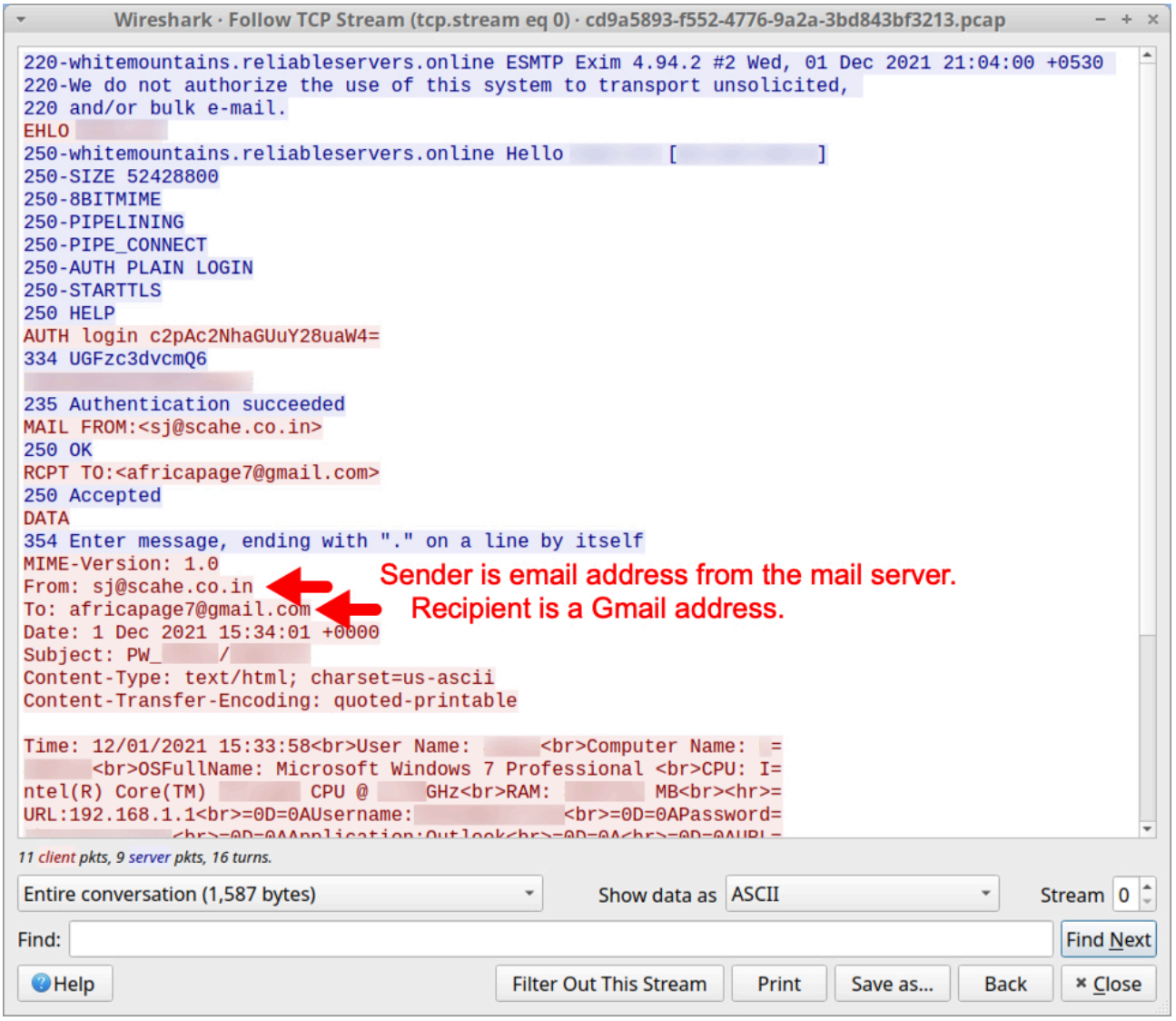
- File size: 537,397 bytes
- File name: Partial Shipment.exe
- Any.Run analysis from 2021-12-01: link

The pcap from Any.Run's analysis of this malware sample shows a new data exfiltration path. The infected Windows host sent a message with stolen data to a Gmail address using a compromised email account from a mail

server established through a hosting provider.



Shown above: Traffic from the Any.Run analysis filtered in Wireshark.



Shown above: TCP stream shows stolen data sent to Gmail address using the compromised email account.

Final words

The basic tactics of Agent Tesla have not changed. However, post-infection traffic from samples since 2021-12-01 indicates Agent Tesla using STMP for data exfiltration now sends to Gmail addresses. Based on the names of these addresses, I believe they are fraudulent Gmail accounts, or they were specifically established to receive data from Agent Tesla.

Brad Duncan
brad [at] malware-traffic-analysis.net
