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

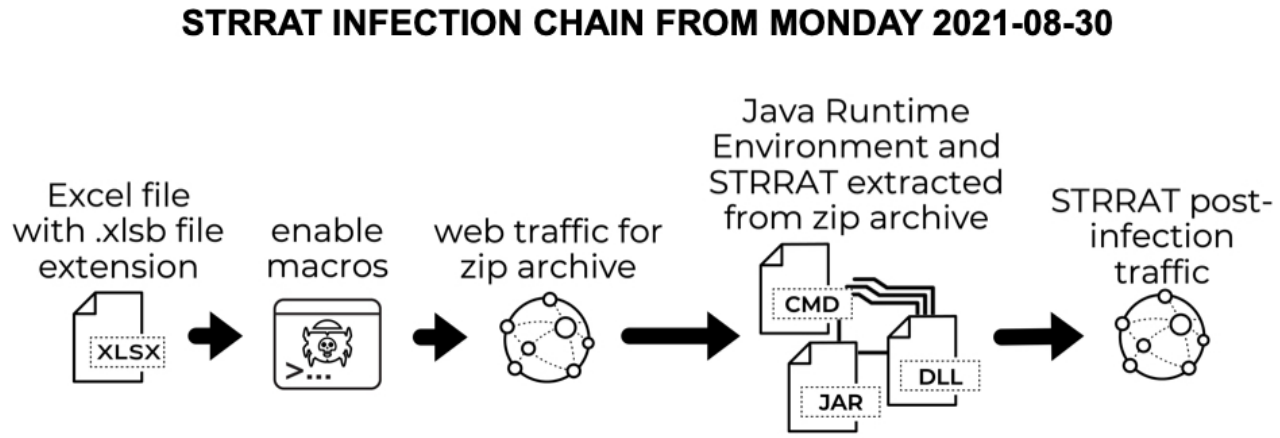
STRRAT: a Java-based RAT that doesn't care if you have Java

Published: 2021-09-01
Last Updated: 2021-09-01 00:15:49 UTC
by Brad Duncan (Version: 1)
0 comment(s)

Introduction

STRRAT was discovered earlier this year as a Java-based Remote Access Tool (RAT) that does not require a preinstalled Java Runtime Environment (JRE). It has been distributed through malicious spam (malspam) during 2021. Today's diary reviews an infection generated using an Excel spreadsheet discovered on Monday, 2021-08-30.

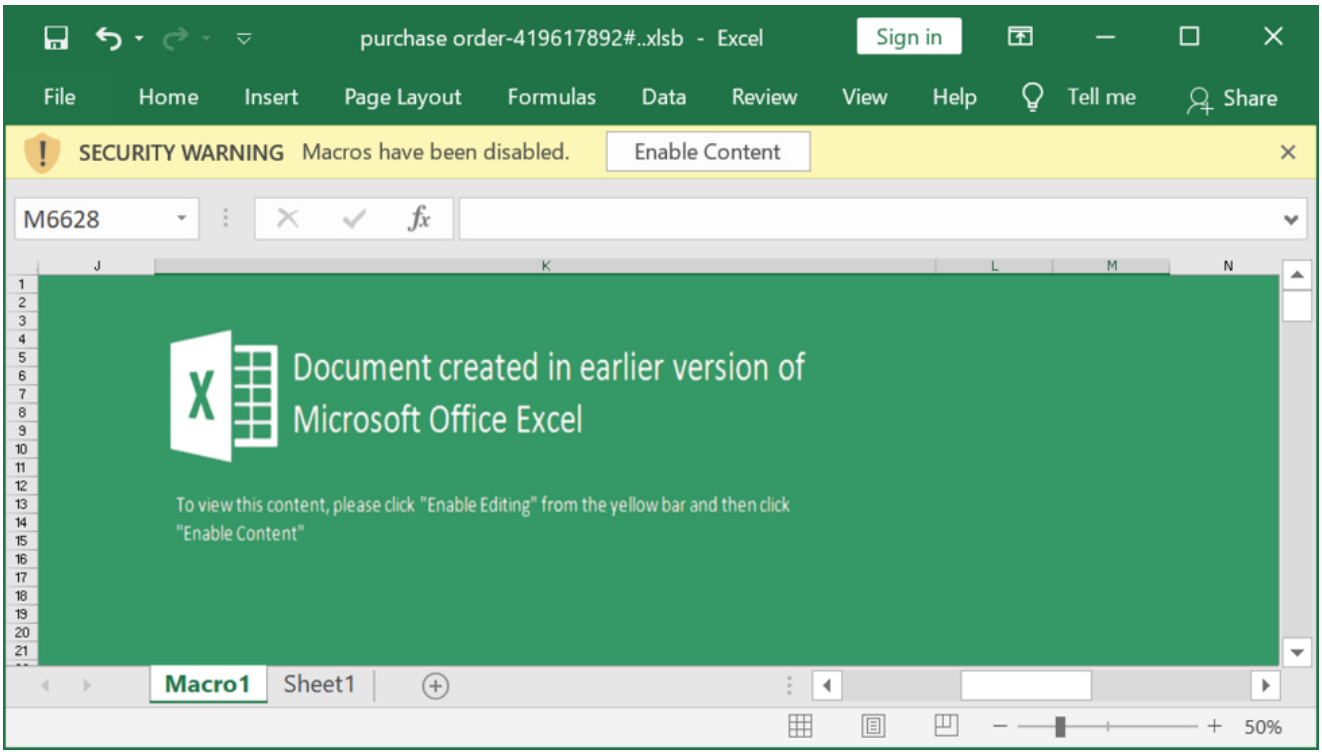
During this infection, STRRAT was installed with its own JRE environment. It was part of a zip archive that contained JRE version 8 update 261, a .jar file for STRRAT, and a command script to run STRRAT using JRE from the zip archive.



Shown above: Chain of events for the STRRAT infection on Monday 2021-08-30.

The Excel spreadsheet

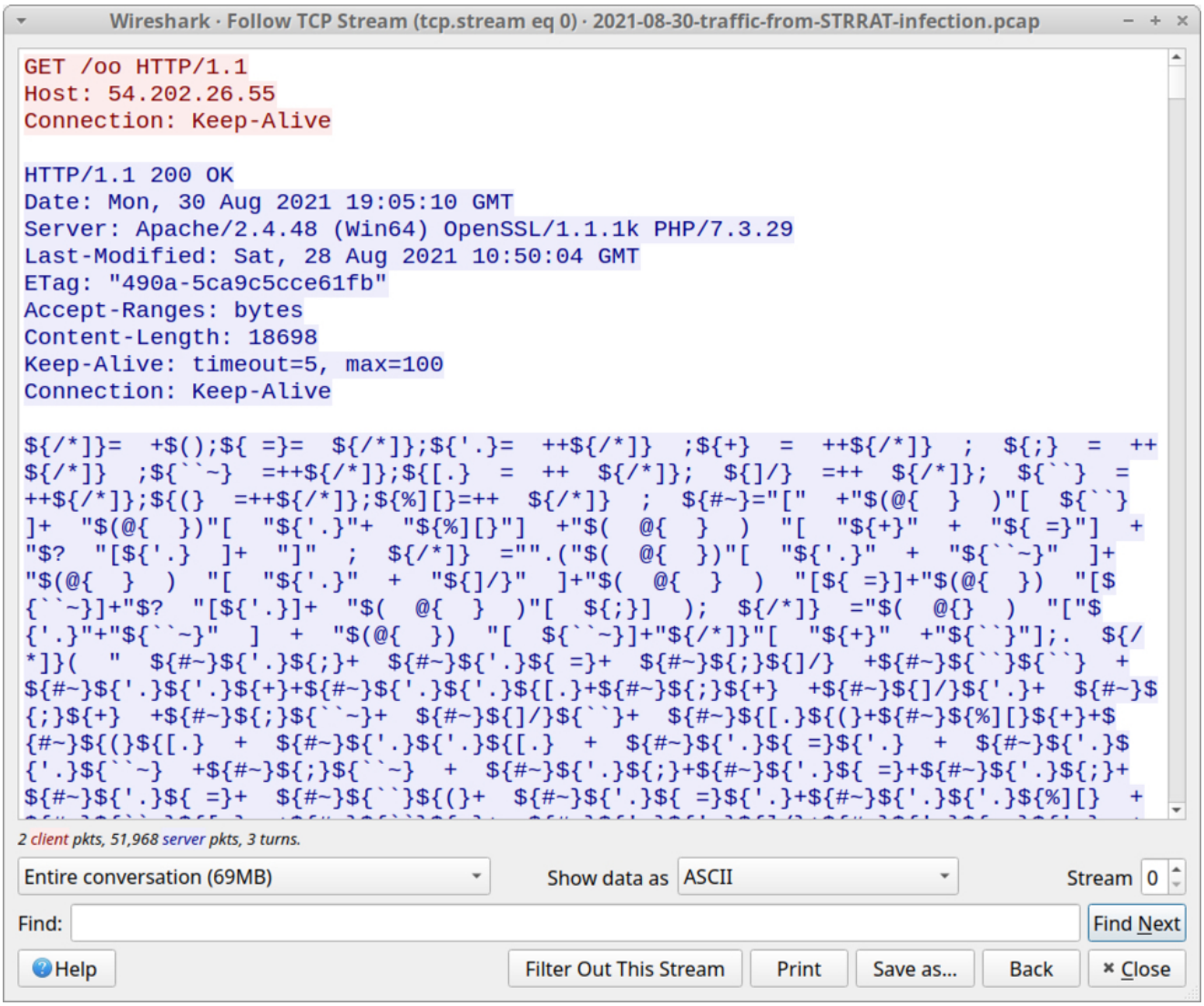
This Excel spreadsheet was submitted to bazaar.abuse.ch on Monday 2021-08-30. It likely was distributed through email, since previously-documented examples like this one were distributed through email.



Shown above: Screenshot of the spreadsheet used for the STRRAT infection.

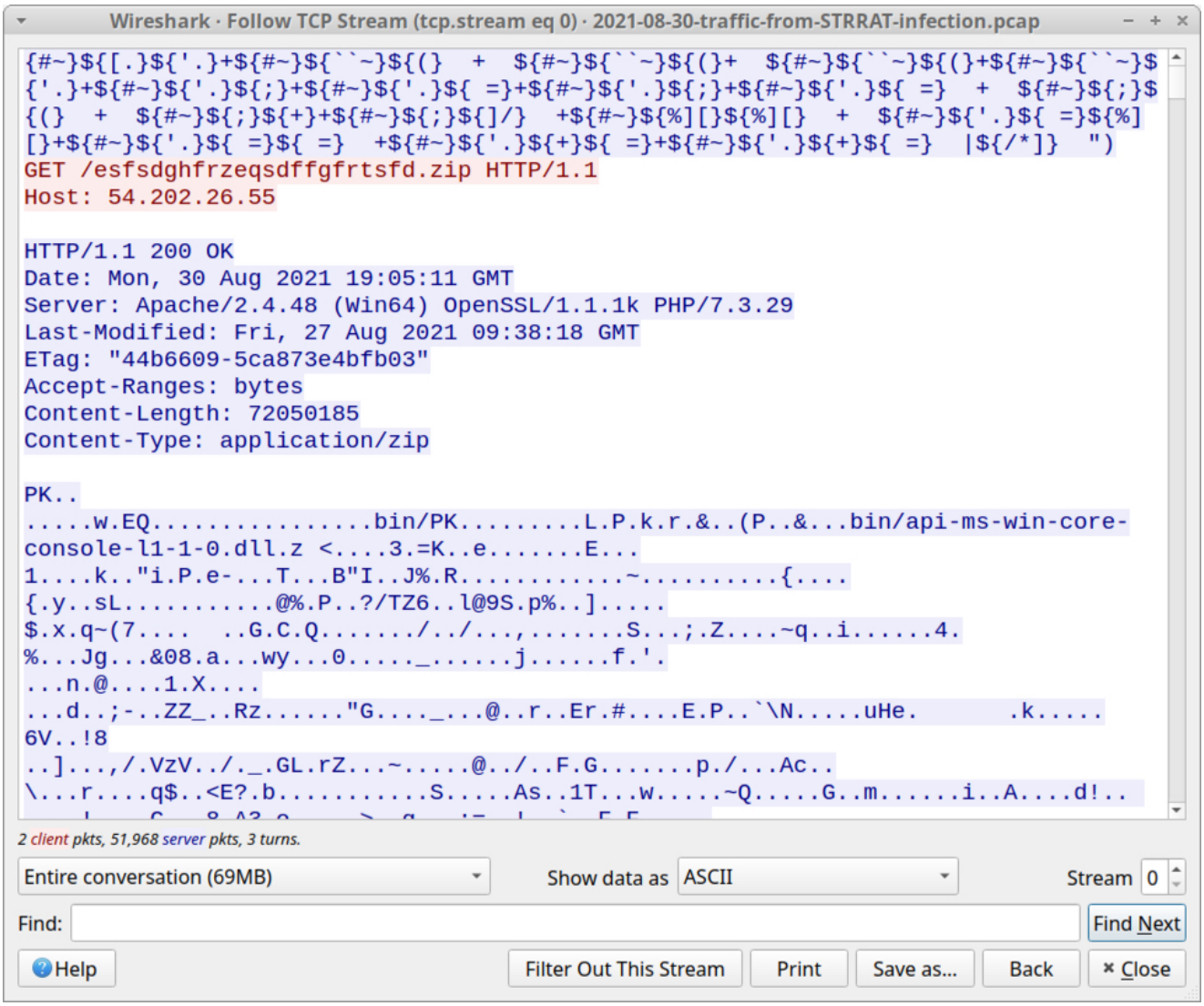
Initial infection activity

If a victim opens the spreadsheet and enables macros on a vulnerable Windows host, the macro code generates unencrypted HTTP traffic to ***54.202.26[.]55***. Testing the spreadsheet in a lab environment, we saw an HTTP GET request that returned approximately 18.7 kB of ASCII symbols with no letters or numbers.



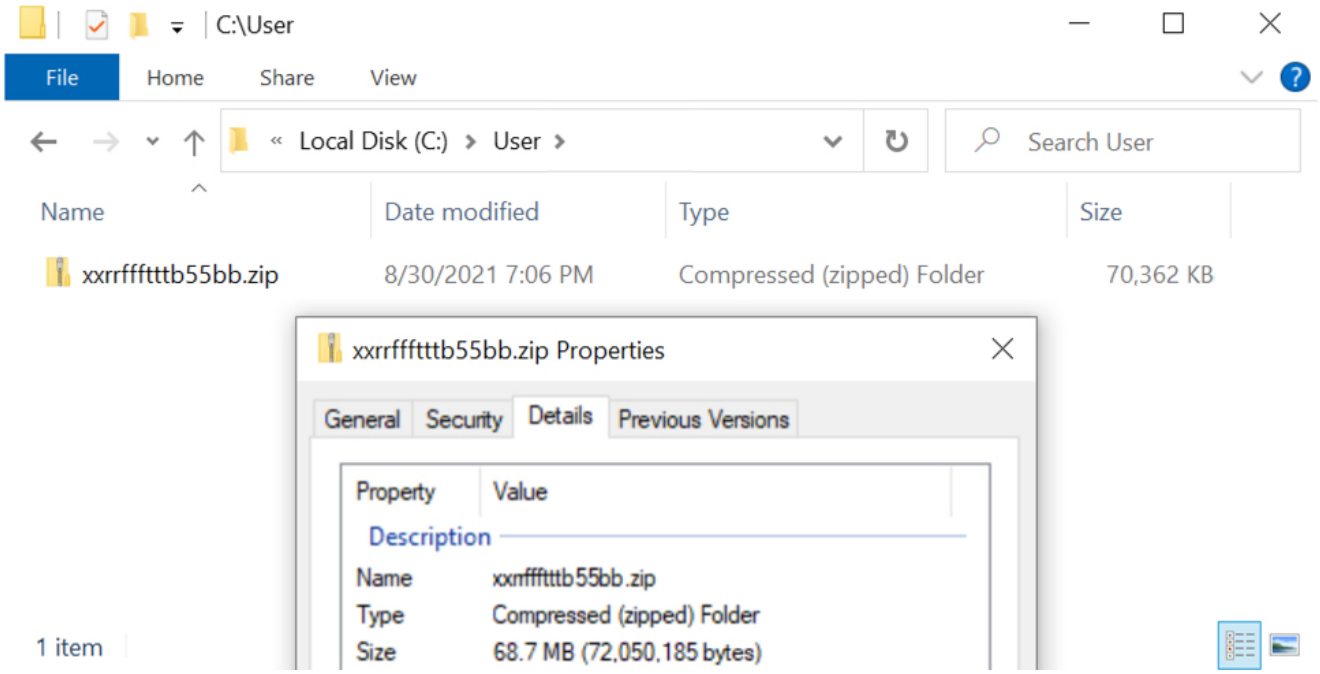
Shown above: First HTTP GET request and response caused by the Excel macro.

The second HTTP request to the same IP address returned a zip archive that was approximately 72.1 MB.

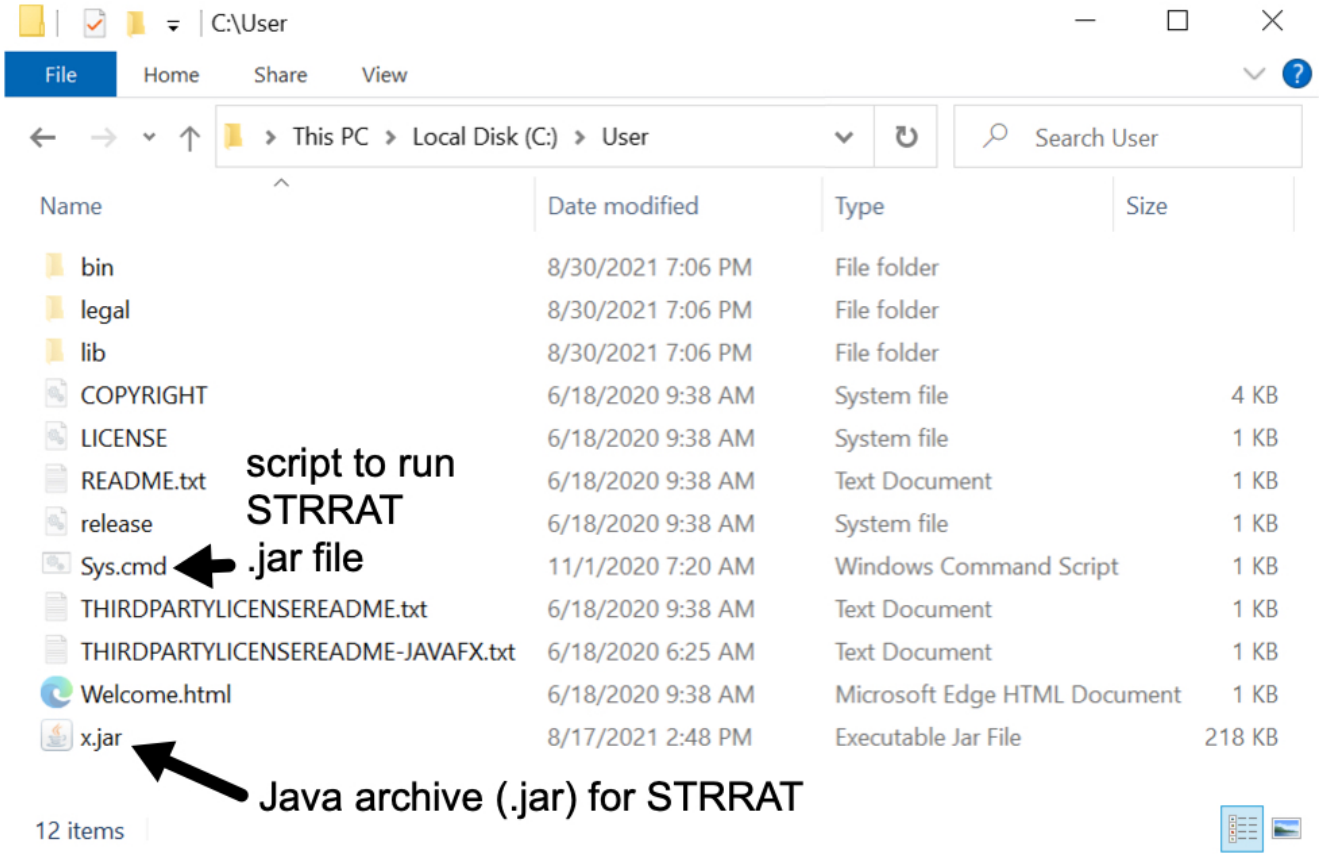


Shown above: The second HTTP GET request to 54.202.26[.]55 returned a 72.1 MB zip archive.

The zip was saved under a newly-created at ***C:\User*** (very close in spelling to ***C:\Users***), then the contents were extracted, and the saved zip archive was deleted.



Shown above: Location the zip archive was saved to on the infected host.



Shown above: Extracted contents of the zip archive include JRE, a .jar file for STRRAT, and a script to run STRRAT.

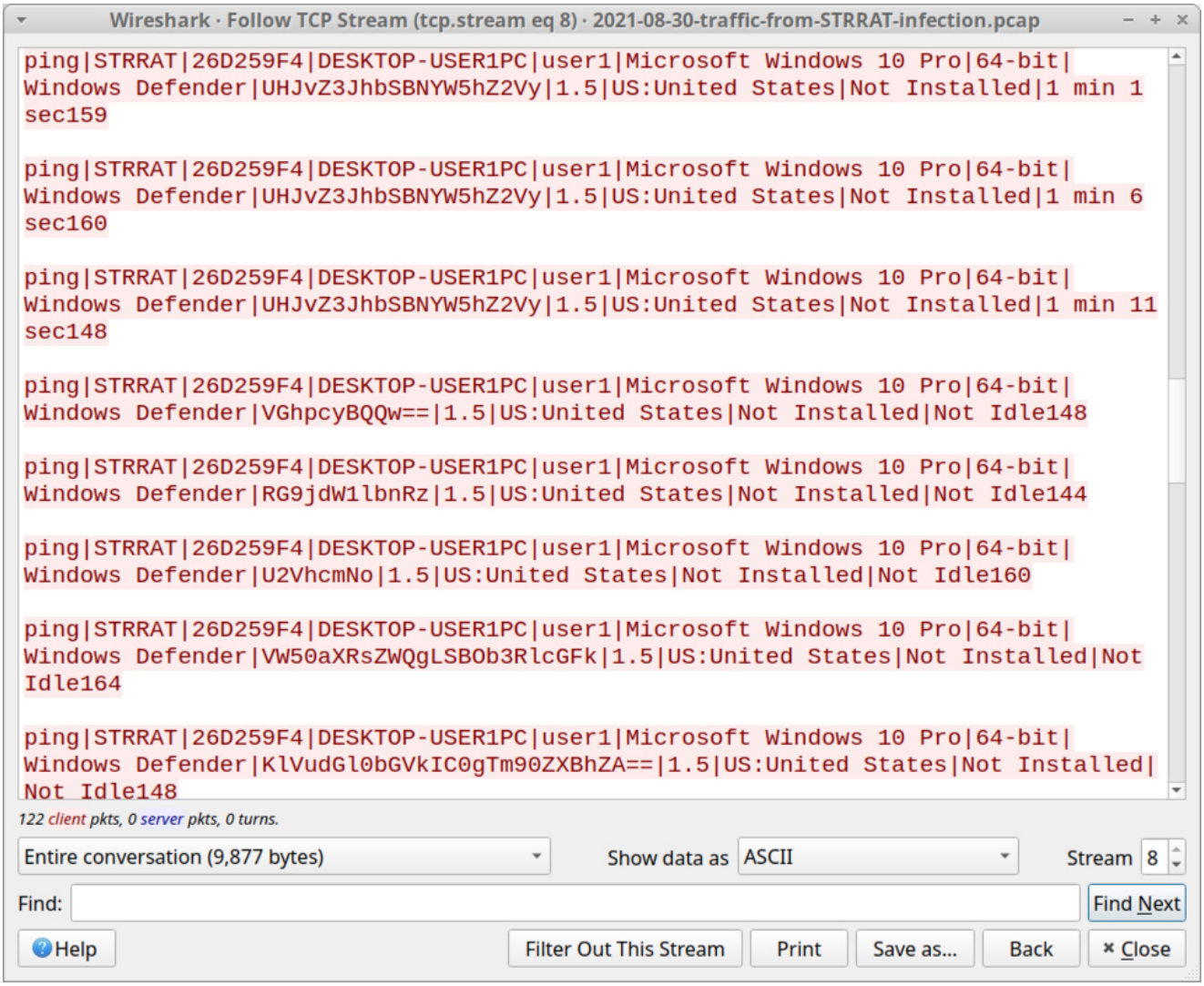
Shown above: Version file shows JRE version 8 update 261), and sys.cmd contains script to run the STRRAT .jar file.

Infection traffic

RAT-based post-infection traffic is often easy to spot, since many RATs use non-web-based TCP ports. Furthermore, traffic for the initial zip archive was over unencrypted HTTP. Finally, we saw HTTPS traffic to legitimate domains from ***Github*** and ***maven.org*** that appeared to be caused by the infection process.

Time	Dst	port	Host	Info
2021-08-30 19:05:10	54.202.26.55	80	54.202.26.55	GET /oo HTTP/1.1
2021-08-30 19:05:11	54.202.26.55	80	54.202.26.55	GET /esfsdghfrzeqsdffgfrtsfd.zip
2021-08-30 19:06:43	151.101.48.209	443	repo1.maven.org	Client Hello
2021-08-30 19:06:43	140.82.114.4	443	github.com	Client Hello
2021-08-30 19:06:43	151.101.48.209	443	repo1.maven.org	Client Hello
2021-08-30 19:06:43	151.101.48.209	443	repo1.maven.org	Client Hello
2021-08-30 19:06:44	185.199.111.154	443	github-releases.githubusercontent.com	Client Hello
2021-08-30 19:07:02	Standard query 0x1eda A str-master.pw			
2021-08-30 19:07:02	Standard query response 0x1eda No such name A str-master.pw			
2021-08-30 19:07:02	Standard query 0x7571 A idgerowner.duckdns.org			
2021-08-30 19:07:02	Standard query response 0x7571 A idgerowner.duckdns.org A 105.109.211.84			
2021-08-30 19:07:02	105.109.211.84	1990		65400 → 1990 [SYN] Seq=0 Win=6424
2021-08-30 19:07:03	208.95.112.1	80	ip-api.com	GET /json/ HTTP/1.1
2021-08-30 19:07:40	105.109.211.84	1990		65405 → 1990 [SYN] Seq=0 Win=6424

Shown above: Traffic from the infection filtered in Wireshark.



Shown above: TCP stream of post-infection traffic generated by STRRAT.

Indicators of Compromise (IOCs)

The following malware was retrieved from an infected Windows host:

SHA256 hash: f148e9a2089039a66fa624e1ffff5ddc5ac5190ee9fdef35a0e973725b60fbc9

- File size: 71,350 bytes
- File name: purchase order-419617892#..xlsb
- File description: Excel spreadsheet with macro for STRRAT

SHA256 hash:
cd6f28682f90302520ca88ce639c42671a73dc3e6656738e20d2558260c02533

- File size: 72,050,185 bytes
- File location: hxxp://54.202.26[.]55/esfsdghfrzeqsdffgfrtsfd.zip
- File location: C:\User\xxrrffffttb55bb.zip
- File description: zip archive retrieved by macro from Excel spreadsheet

- Note: This package contains Java Runtime Environment (JRE) verion 8 update 261 and a .jar file for STRRAT

SHA256 hash:
685549196c77e82e6273752a6fe522ee18da8076f0029ad8232c6e0d36853675

- File size: 222,711 bytes
- File location: C:\User\x.jar
- File description: STRRAT .jar file from the above zip archive
- Run method: CMD.EXE /C C:\User\bin\java.exe -jar C:\User\x.jar

The following traffic occured on an infected Windows host:

- 54.202.26[.]55 port 80 - ***54.202.26[.]55*** - GET /oo
- 54.202.26[.]55 port 80 - ***54.202.26[.]55*** - GET /esfsdghfrzeqsdffgfrtsfd.zip
- port 443 - ***repo1.maven.org*** - HTTPS traffic *(not inherently malicious)*
- port 443 - ***github.com*** - HTTPS traffic *(not inherently malicious)*
- port 443 - ***github-releases.githubusercontent.com*** - HTTPS traffic *(not inherently malicious)*
- DNS query for ***str-master[.]pw*** - response: No such name
- 105.109.211[.]84 port 1990 - ***idgerowner.duckdns[.]org*** - TCP traffic generated by STRRAT
- port 80 - ***ip-api.com*** - GET /json/ *(not inherently malicious)*

Final words

This specific STRRAT infection was notable because it included JRE version 8 update 261 as part of the infection package. Including JRE allows this Java-based RAT to run on vulnerable Windows hosts whether or not they have Java installed.

The host I used for testing had a more recent version of Java, but this sample didn't care. It sent its own version of JRE anyway.

Fortunately, default security settings in Windows 10 and Microsoft Office should prevent this particular STRRAT infection chain.

Mass-distribution methods like malspam remain cheap and profitable for cyber criminals, so we expect to see STRRAT and other types of commonly-distributed malware in the coming months.

A pcap of the infection traffic and malware from the infected host can be found here.

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

Keywords: excel macros malware rat strrat

0 comment(s)

Join us at SANS! Attend with Brad Duncan in starting

Top of page

×

Diary Archives