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/27798

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 <u>Brad Duncan</u> (Version: 1) <u>0 comment(s)</u> Introduction

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

Java Runtime Environment and STRRAT extracted Excel file STRRAT postfrom zip archive with .xlsb file enable web traffic for infection extension macros zip archive traffic CMD XLSX DLL JAR

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

STRRAT INFECTION CHAIN FROM MONDAY 2021-08-30

The Excel spreadsheet

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

Wireshark · Follow TCP Stream (tcp.stream eq	0) · 2021-08-30-traffic-from-STRRAT-infection.pcap – + ×
GET /oo HTTP/1.1 Host: 54.202.26.55 Connection: Keep-Alive	▲
HTTP/1.1 200 OK Date: Mon, 30 Aug 2021 19:05:10 GMT Server: Apache/2.4.48 (Win64) OpenSSL/ Last-Modified: Sat, 28 Aug 2021 10:50: ETag: "490a-5ca9c5cce61fb" Accept-Ranges: bytes Content-Length: 18698 Keep-Alive: timeout=5, max=100	1.1.1k PHP/7.3.29 04 GMT
Connection: Keep-Alive \${/*]}= +\$();\${ =}= \${/*]};\${'.}= + \${/*]};\${`~} =++\${/*]};\${[.} = + ++\${/*]};\${(} =++\${/*]};\${%][}=++ \${]+ "\$(@{ })"["\${'.}"+ "\${%][}"] "\$? "[\${'.}]+ "]" ; \${/*1} ="".	+\${/*]};\${+} = ++\${/*]}; \${;} = ++ + \${/*]}; \${]/} =++ \${/*]}; \${``} = /*]}; \${#~}="[" +"\$(@{ })"[\${``} +"\$(@{ }) "["\${+}" + "\${ =}"] + ("\$(@{ })"["\${'.}" + "\${``~}"]+
"\$(@{ }) "["\${'.}" + "\${]/}" {``~}]+"\$? "[\${'.}]+ "\$(@{ }) "[{'.}"+"\${``~}"] + "\$(@{ }) "[\$ *]}(" \${#~}\${'.}\${;}+ \${#~}\${'.}\${ \${#~}\${'.}\${'.}\${{'.}}\${ {'.}\${+}+\${#~}\${'.}\${'.}\${ {'.}}\${'.}\${{'.}}{ {'.}}	<pre>('(''''''''''''''''''''''''''''''''''</pre>
<pre>{#~}\${(}\${[.} + \${#~}\${'.}\${'.}\${[.] {'.}\${``~} +\${#~}\${;}\${``~} + \${#~} \${#~}\${``} + \${#~}\${;}\${``~} + \${#~} \${#~}\${'.}\${ =} + \${#~}\${``}\${(}+ \${# 2 client pkts, 51,968 server pkts, 3 turns.</pre>	+ \${#~}\${'.}\${ =}\${'.} + \${#~}\${'.}\$ \${'.}\$\$ \${'.}\${;}+\${#~}\${'.}\${ =}+\${#~}\${'.}\${;}+ ~}\${'.}\${ =}\${'.}+\${#~}\${'.}\${'.}\${;}+
Entire conversation (69MB)	how data as ASCII - Stream 0 🗘
Find:	Find <u>N</u> ext
Help Filt	er Out This Stream Print Save as Back × <u>C</u> lose

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.

▼ Wireshark · Follow TCP Stream (tcp.stream eq 0) · 2021-08-30-traffic-from-STRRAT-infection.pcap - + ×
<pre>{#~}\${[.}\${'.}+\${#~}\${``~}\${(} + \${#~}\${``~}\${(}+\${#~}\${``~}\${(}+\${#~}\${``~}\$ {'.}+\${#~}\${'.}\${;}+\${#~}\${'.}\${ =} + \${#~}\${``~}\$ {'.}+\${#~}\${'.}\${ =} + \${#~}\${;}\$ {(} + \${#~}\${;}\${+}+\${#~}\${;}\${]/} +\${#~}\${{'.}}\${ =} + \${#~}\${;}\$ {(} + \${#~}\${;}\${+}+\${#~}\${;}\${]/} +\${#~}\${{'.}}\${ =} + \${#~}\${;}\$ {[}+\${#~}\${'.}\${ =} + \${#~}\${;}\${]]} {[}+\${#~}\${'.}\${ =} +\${#~}\${;}\${ =} +\${#~}\${{'.}}\${ =} +\${{'.}}{{'.}} GET /esfsdghfrzeqsdffgfrtsfd.zip HTTP/1.1 Host: 54.202.26.55</pre>
HTTP/1.1 200 OK Date: Mon, 30 Aug 2021 19:05:11 GMT Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/7.3.29 Last-Modified: Fri, 27 Aug 2021 09:38:18 GMT ETag: "44b6609-5ca873e4bfb03" Accept-Ranges: bytes Content-Length: 72050185 Content-Type: application/zip
<pre>PK w.EQbin/PKL.P.k.r.&.(P&bin/api-ms-win-core- console-l1-1-0.dll.z <3.=K.eE 1k."i.P.eTB"I.J%.R~</pre>
2 client pkts, 51,968 server pkts, 3 turns.
Entire conversation (69MB) Show data as ASCII Stream 0
Find: Find Next
Help Filter Out This Stream Print Save as Back × Close

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.



📙 🔄 📜 🗧 🛛 C:\User		- 🗆	\times
File Home Share View			~ ?
\leftarrow \rightarrow \checkmark \uparrow] \blacktriangleright This PC \Rightarrow Local Disk (C:) \Rightarrow User		✓ V Search User ✓ Search User	
Name	Date modified	Type Size	
📕 bin	8/30/2021 7:06 PM	File folder	
📒 legal	8/30/2021 7:06 PM	File folder	
📕 lib	8/30/2021 7:06 PM	File folder	
COPYRIGHT	6/18/2020 9:38 AM	System file	4 KB
LICENSE	6/18/2020 9:38 AM	System file	1 KB
README.txt	6/18/2020 9:38 AM	Text Document	1 KB
SIRRAI	6/18/2020 9:38 AM	System file	1 KB
🖲 _{Sys.cmd} 🛖 .jar file	11/1/2020 7:20 AM	Windows Command Script	1 KB
THIRDPARTYLICENSEREADME.txt	6/18/2020 9:38 AM	Text Document	1 KB
THIRDPARTYLICENSEREADME-JAVAFX.txt	6/18/2020 6:25 AM	Text Document	1 KB
💽 Welcome.html	6/18/2020 9:38 AM	Microsoft Edge HTML Document	1 KB
🔬 x.jar	8/17/2021 2:48 PM	Executable Jar File	218 KB
Java archive (.jar) for STRRAT			

12 items

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

File Edit Format View Help			~
JAVA_VERSION="1.8.0_261" Version of JRE			~
OS_NAME="Windows"			
OS_VERSION="5.1"			
SOURCE=" .:148386d4b327 corba:7bba472d7452 deploy:3bc2e14623db hotspot:1a97f34cea08 hotspot/make/closed:e11b6693ad95 hotspot/src/closed:21fdb178e79d install:df9a079c476a jaxp:0741fb08db6d jaxws:62a7981fdbd8 jdk:cd33dd84ca12 jdk/make/closed:c0061afa7a2a jdk/src/closed:9fe66686fb70 langtools:dc513ee0a27c nashorn:be9a82e37fea" BUILD_TYPE="commercial"			
			\sim
	- file –		
Sys.cmd - Notepad script to run STRRAT is			×
Sys.cmd - Notepad script to run STRRAT .ja	ar file		×
Sys.cmd - Notepad File Edit Format View Help @echo off	ar file		×

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.git	hubusercontent.com Client Hello
2021-08-30 19:07:02	Standard query	0x1eda	a A str-master.pw	
2021-08-30 19:07:02	Standard query	respor	nse Ox1eda No such na	ame A str-master.pw
2021-08-30 19:07:02	Standard query	0x7571	L A idgerowner.duckd	ns.org
2021-08-30 19:07:02	Standard query	respor	ise 0x7571 A idgerow	ner.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.

 Wireshark · Follow TCP Stream (tcp.strea 	m eq 8) · 2021-08-30-traffic-from-STRRAT-infection.pcap – + ×
ping STRRAT 26D259F4 DESKTOP-USER1F Windows Defender UHJvZ3JhbSBNYW5hZ2 sec159	C user1 Microsoft Windows 10 Pro 64-bit Vy 1.5 US:United States Not Installed 1 min 1
ping STRRAT 26D259F4 DESKTOP-USER1F Windows Defender UHJvZ3JhbSBNYW5hZ2 sec160	C user1 Microsoft Windows 10 Pro 64-bit Vy 1.5 US:United States Not Installed 1 min 6
ping STRRAT 26D259F4 DESKTOP-USER1F Windows Defender UHJvZ3JhbSBNYW5hZ2 sec148	PC user1 Microsoft Windows 10 Pro 64-bit PVy 1.5 US:United States Not Installed 1 min 11
ping STRRAT 26D259F4 DESKTOP-USER1F Windows Defender VGhpcyBQQw== 1.5 U	C user1 Microsoft Windows 10 Pro 64-bit S:United States Not Installed Not Idle148
ping STRRAT 26D259F4 DESKTOP-USER1F Windows Defender RG9jdW1lbnRz 1.5 U	PC user1 Microsoft Windows 10 Pro 64-bit US:United States Not Installed Not Idle144
ping STRRAT 26D259F4 DESKTOP-USER1F Windows Defender U2VhcmNo 1.5 US:Ur	C user1 Microsoft Windows 10 Pro 64-bit hited States Not Installed Not Idle160
ping STRRAT 26D259F4 DESKTOP-USER1F Windows Defender VW50aXRsZWQgLSB0b3 Idle164	PC user1 Microsoft Windows 10 Pro 64-bit RlcGFk 1.5 US:United States Not Installed Not
ping STRRAT 26D259F4 DESKTOP-USER1F Windows Defender KlVudGl0bGVkIC0gTm Not Idle148	C user1 Microsoft Windows 10 Pro 64-bit 190ZXBhZA== 1.5 US:United States Not Installed
122 client pkts, 0 server pkts, 0 turns.	
Entire conversation (9,877 bytes)	 Show data as ASCII Stream 8 ²
Find:	Find <u>N</u> ext
😮 Help	Filter Out This Stream Print Save as Back × Close

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: <u>f148e9a2089039a66fa624e1ffff5ddc5ac5190ee9fdef35a0e973725b60fbc9</u>

- 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\xxrrffftttb55bb.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: <u>excel macros malware rat strrat</u> <u>0 comment(s)</u> Join us at SANS! <u>Attend with Brad Duncan in starting</u>

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

<u>Top of page</u>

×

Diary Archives