UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	
	:	
	:	
v.	:	**Crim No. 1:22-cr-00354-RCL**
	:	
	:	
RICHARD SLAUGHTER, and	:	
	:	
CADEN PAUL GOTTFRIED,	:	
	:	
Defendants.	:	

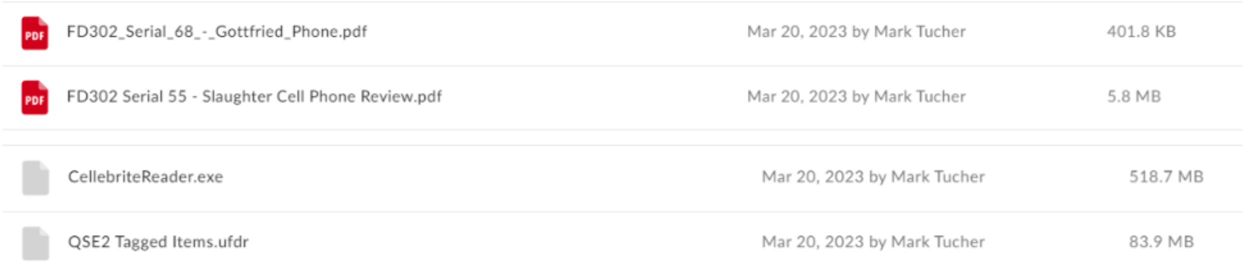
UNITED STATES' RESPONSE TO DEFENSE NOTICE THAT GOVERNMENT ATTEMPTED TO PLANT TROJAN MALWARE ON DEFENSE COMPUTERS

The United States of America (the "government") stands accused by defense counsel of attempting, through the discovery process, to plant trojan malware on counsel's computer systems. He claims, without evidence, this nefarious software is "designed to allow the sender to take over and remotely control the recipient's computer." Defendant's Brief at 2. Counsel then takes several leaps forward and surmises that the government's intent in planting malware was to "allow the government to invade and know all privileged and confidential contents and work product of defense team computers." Defendant's Brief at 3. He demands the Court "[i]nitiat[e] an investigation into this matter" to determine who created this malware, which agents are now tracking the computers of defense counsel, and other related relief, including sanctions on government counsel. Defendant's Brief at 7. In response, the undersigned states as follows:

1. Until recently and throughout the pendency of this case, defendants Slaughter and Gottfried were represented by Joseph R. Conte. On March 2, 2023, attorney John M. Pierce made his appearance in this case. Four days later, on March 6, 2023, Mr. Conte filed a motion to withdraw as counsel.

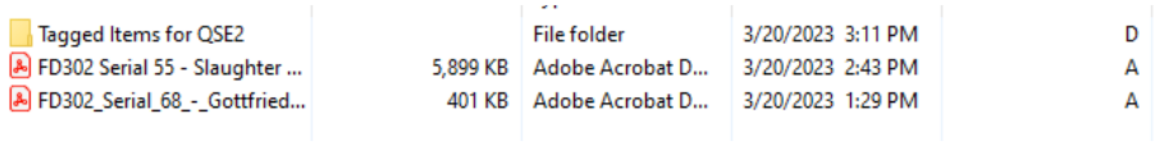
2. On March 20, 2023, the case agent informed the government that additional discovery had been produced in this case. Pursuant to a search warrant, the FBI had reviewed the contents of both Gottfried's and Slaughter's cell phones. The agent indicated that only Slaughter's phone contained any material related to the government's investigation.

3. Later that day, through USAfx[1], the case agent provided the government with four files: two FBI 302s summarizing the results of the cell phone searches, a Cellebrite report containing the scoped contents of Slaughter's phone as a .ufdr file, and the Cellebrite reader required to view the file:



FD302_Serial_68_-_Gottfried_Phone.pdf	Mar 20, 2023 by Mark Tucher	401.8 KB
FD302 Serial 55 - Slaughter Cell Phone Review.pdf	Mar 20, 2023 by Mark Tucher	5.8 MB
CellebriteReader.exe	Mar 20, 2023 by Mark Tucher	518.7 MB
QSE2 Tagged Items.ufdr	Mar 20, 2023 by Mark Tucher	83.9 MB

4. The government downloaded the files, reviewed them, and determined that the files could be produced to the defense. Less than two hours later, the undersigned took the four files, converted them to a .zip file, titled the file, "1st Supp. Discovery.zip," uploaded to USAfx, and shared with defense counsel.



Tagged Items for QSE2		File folder	3/20/2023 3:11 PM	D
FD302 Serial 55 - Slaughter ...	5,899 KB	Adobe Acrobat D...	3/20/2023 2:43 PM	A
FD302_Serial_68_-_Gottfried...	401 KB	Adobe Acrobat D...	3/20/2023 1:29 PM	A

The undersigned then invited Mr. Pierce and his associates to view the file at 4:42 p.m. on March 20, and the government's read receipt indicates that Mr. Pierce's co-counsel,

[1] USAfx is the government's secure, cloud-based file sharing platform. The platform is the near-exclusive means by which the government shares discovery for all January 6-related cases.

Roger Roots, accepted the invitation same day. The activity log from USAfx reflects that Mr. Roots downloaded the .zip file on Saturday, March 25, at 5:15 p.m.

5. On Sunday, March 26, the government learned for the first time that the defense team was having trouble opening the file, with defense stating that computer virus software was alerting them to malware within the file. The next morning, the government downloaded its own production from USAfx and successfully opened all four files without issue. It then created a new .zip file out of the four files previously produced, titled the file "1st Supp. Discovery – Resent 3.27.28.zip," re-uploaded to USAfx, and again shared the file with defense counsel. The government also sent an email to the defense team noting that the issue may have to do with the "Cellbrite.exe" file and that the government would "re-run the .zip file and send again."[2]

Undersigned counsel is an officer of the Court, and an attorney for the government with no specialized knowledge, training, or expertise in computer programming, hacking, computer espionage, or other methods of covert electronic surveillance. He lacks most administrative rights to his computer and has no access to the type of software defense counsel claims the government is attempting to infect him with. Despite the defendant's rhetoric, undersigned counsel nevertheless endeavored to see if there was an issue with the downloaded discovery, consistent with its representations to Court and Counsel.

[2] Defense notes in their filing that "the idea of 'rerunning' the file suggests [the government] ran the infected file previously." *See* Defense's Brief, ECF No. 39, at 6. To clarify, all the government did was convert the same four files into a separate .zip file and send to defense counsel a second time. Despite defense's statement at the status conference that he was not accusing the government's attorney of knowingly attempting to install spyware on his computer software, that is precisely what defense's pleading accuses the undersigned of doing.

Following defense counsel's pleading, the government conferred with a Senior Digital Investigative Analyst (the "analyst") with the DOJ's Computer Crime and Intellectual Property Section (CCIPS). This individual has 13 years of experience in digital forensics, four years' experience in the field of cybersecurity, and has participated in over 500 hours of training in digital forensics. The analyst's certifications include the following:

- GIAC Certified Forensic Analyst (GCFA);
- EnCase Certified Examiner;
- Nuix Investigation Specialist;
- Defense Cyber Crime Center Certified Digital Forensic Examiner;
- AccessData Certified Examiner;
- Cellebrite Certified Operator;
- Cellebrite Certified Physical Analyst; and
- Certified Information System Security Professional (CISSP).

The analyst downloaded the government's file marked "1st Supp. Discovery.zip" directly from the same USAfx file sharing account the government used to send the file to the defense. The analyst then computed the hash values[3] of the file, which were as follows:

- MD5: 95487d8cacd666168a9c2d5fd1452556
- SHA-1: 3ae5063fda6e79e15259d0581bb623e12a33b7af

The analyst scanned the file with Windows Defender (security intelligence version 1.385.1389.0, dated 3/28/2023 8:49 AM) and with Malwarebytes 4.5.25.256 (update package version 1.0.67276 and component package version 1.0.1957). No threats were found with either antivirus program.

[3] "A hash value is a numeric value of a fixed length that uniquely identifies data. Hash values represent large amounts of data as much smaller numeric values, so they are used with digital signatures. You can sign a hash value more efficiently than signing the larger value. Hash values are also useful for verifying the integrity of data sent through insecure channels. The hash value of received data can be compared to the hash value of data as it was sent to determine whether the data was altered." https://learn.microsoft.com/en-us/dotnet/standard/security/ensuring-data-integrity-with-hash-codes (last accessed April 10, 2023).

The analyst recommended reaching out to defense counsel to confirm the hash values of the file matched. According to the analyst, if the hash values matched, then the government could confirm the defense has an exact copy of the same .zip file uploaded to USAfx.

On April 10, 2023, the defense emailed the government and confirmed that the hash values of the file in question matched the hashes provided by the CCIPS analyst. Put another way: the government can confirm the CCIPS analyst reviewed the exact same file the defense claims was designed to take over their computers and "invade and know all privileged and confidential contents and work product of defense team computers." Defendant's Brief at 3. The analyst thus confirmed nothing is wrong with the file.

To summarize: defense counsel was sent discovery. His own computer systems were unable to open all the files, and his anti-virus software blocked the file. Instead of working to identify *why* the program would not open, defense counsel jumped, leaps and bounds, to the most logical, reasoned conclusion: the government took "newly invented" malware, which "allows the government to invade and know all privileged and confidential contents and work product of team defense computers," and used its discovery obligations as a subterfuge to hack into defense information technology systems. Defense further surmises that this software has possibly "been used before by the government and has succeeded in taking over other defense lawyers or legal teams." [4] This is false.

WHEREFORE, the United States, respectfully requests that this Court deny defense's request for investigation, evidentiary hearing, and sanctions. The government also respectfully

[4] As an aside, within minutes of his filing, Mr. Pierce's Notice and Motion was uploaded by his IT expert and "client advocate," Emily Lambert, to an online document sharing platform, where it was then immediately shared to Twitter. *See* Government's Exhibits 1 and 2.

requests the Court set a status conference to determine the state of plea negotiations or, in the alternative, to set a trial date.

Respectfully submitted,

MATTHEW M. GRAVES
United States Attorney
D.C. Bar Number 481052

By: ______________________________
Stephen J. Rancourt
Texas Bar No. 24079181
Assistant United States Attorney, Detailee
601 D Street, NW
Washington, D.C. 20530
(806) 472-7398
stephen.rancourt@usdoj.gov