**IN THE UNITED STATES DISTRICT COURT**

**FOR THE DISTRICT OF COLUMBIA**

**UNITED STATES OF AMERICA,**

**-v-** **1:22-cr-00354-RCL-1 and 2**

**RICHARD SLAUGHTER &**

**CADEN GOTTFRIED,**

**Defendants.**

**NOTICE THAT THE UNITED STATES HAS ATTEMPTED TO PLANT TROJAN MALWARE ON DEFENSE COMPUTERS TO GAIN REMOTE ACCESS**

**AND**

**MOTION FOR INVESTIGATION, EVIDENTIARY HEARING, CONTINUANCE AND OTHER SANCTIONS**

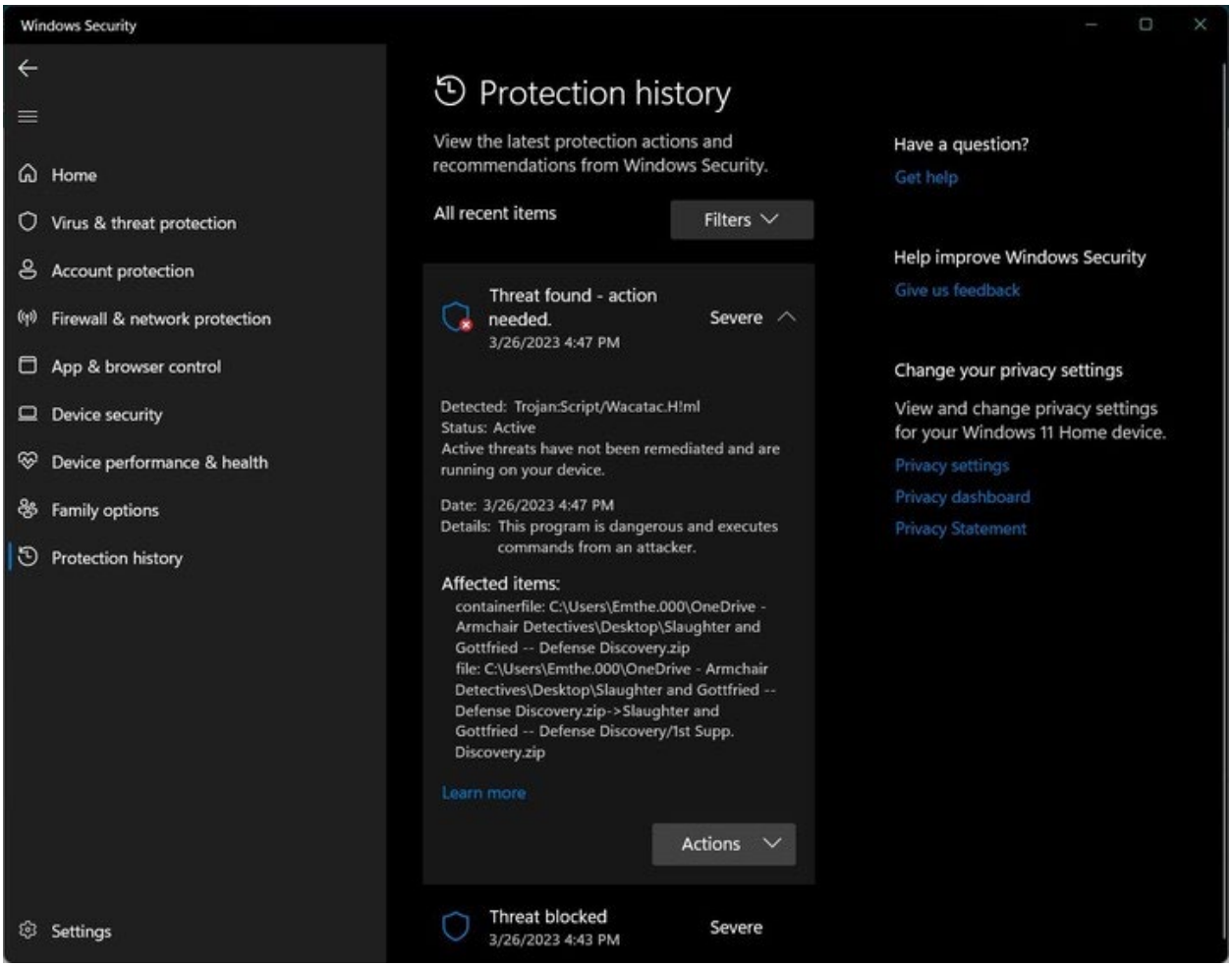
COMES NOW Defendants Rick Slaughter and Caden Gottfried, by and through undersigned counsel John Pierce, with this notice to the court of serious structural violations of the 4th, 5th, and 6th, and Amendments by the prosecution.

On Monday, March 20, at 5:42 PM, the United States, through Assistant United States Attorney Stephen Rancourt, emailed defense counsel John Pierce and John Pierce Law partner Roger Roots, a discovery file entitled "Slaughter and Gottfried - 1st Supplemental Discovery."

John Pierce Law (JPL) Client Advocate Emily Lambert downloaded the file and unzipped the zipped file within.

Immediately upon unzipping the file, Lambert's computer froze, and the computer's Microsoft antivirus program gave the attached pop-up warning:

**"This program is dangerous and executes commands from an attacker."**

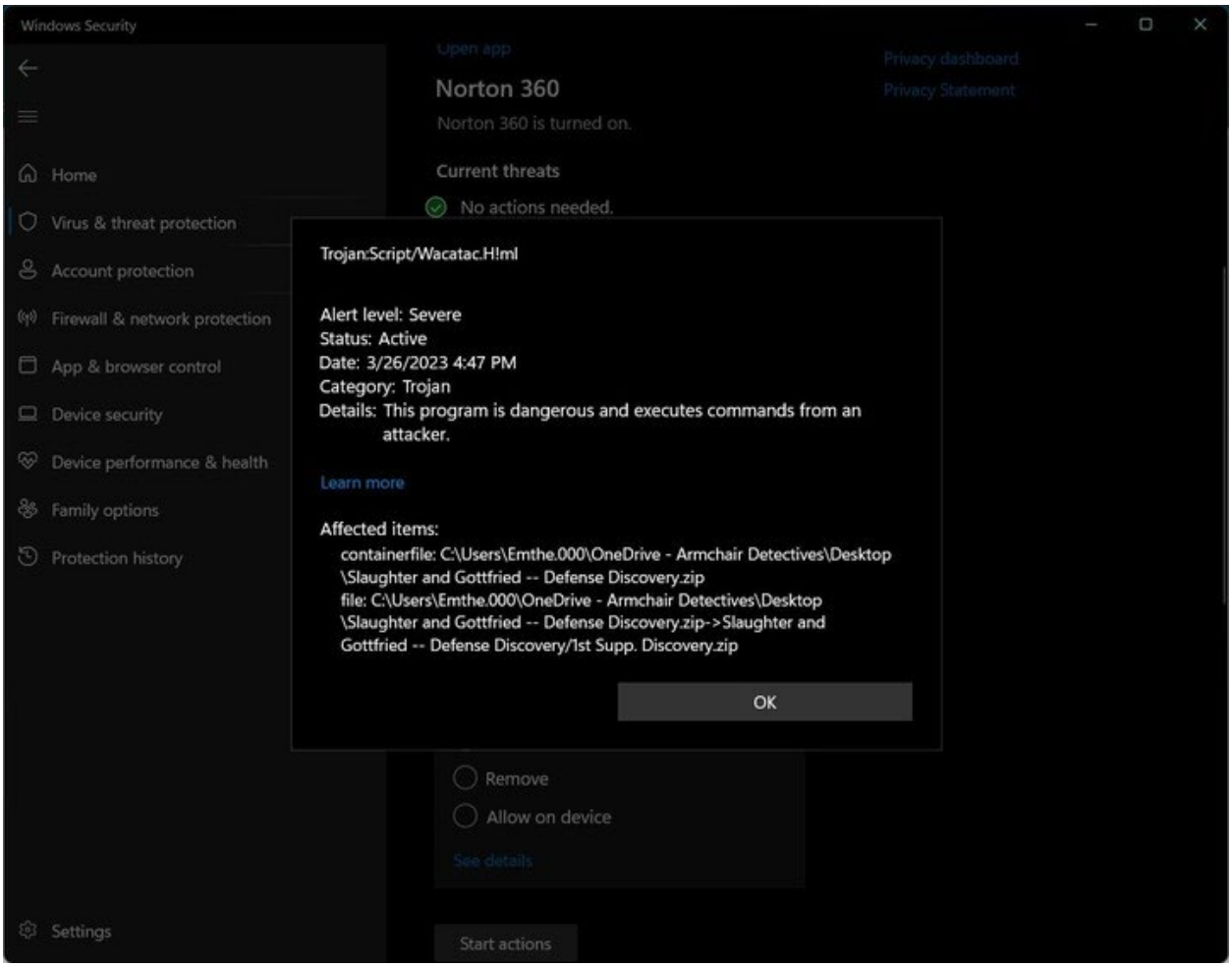



**The Government file contains newly invented Trojan Malware designed to allow the sender to take over and remotely control the recipient's computer.**

Ms. Lambert has certifications in forensics accounting and fraud investigations, OSINT (Open Source Intelligence), skip-tracing, cyber and social media intelligence, and anti-money laundering. She was previously tech support for a software company. It is significant that Ms. Lambert subscribes to three (3) antivirus programs, McAfee, Norton, and Microsoft. Only Microsoft's anti-virus software detected the government's Trojan malware attack. This means that (1) the malware is newly invented and designed (possibly by the government), and (2) it is possible that the government's malware attack has been used before by the government and has succeeded in

taking over other defense lawyers or legal teams whose antivirus software failed to detect the new spyware virus.

The government's Trojan Malware is designed to allow a sender (apparently the FBI or the U.S. Attorney's Office) to secretly and illegally take over and remotely control defense lawyers' computers. The spyware virus allows the government to invade and know all privileged and confidential contents and work product of defense team computers. This violates the 4th amendment freedom from unreasonable searches and seizures, the 5th amendment right to due process, the 5th amendment right not to be a witness against oneself and the 6th amendment rights to counsel and a fair trial.

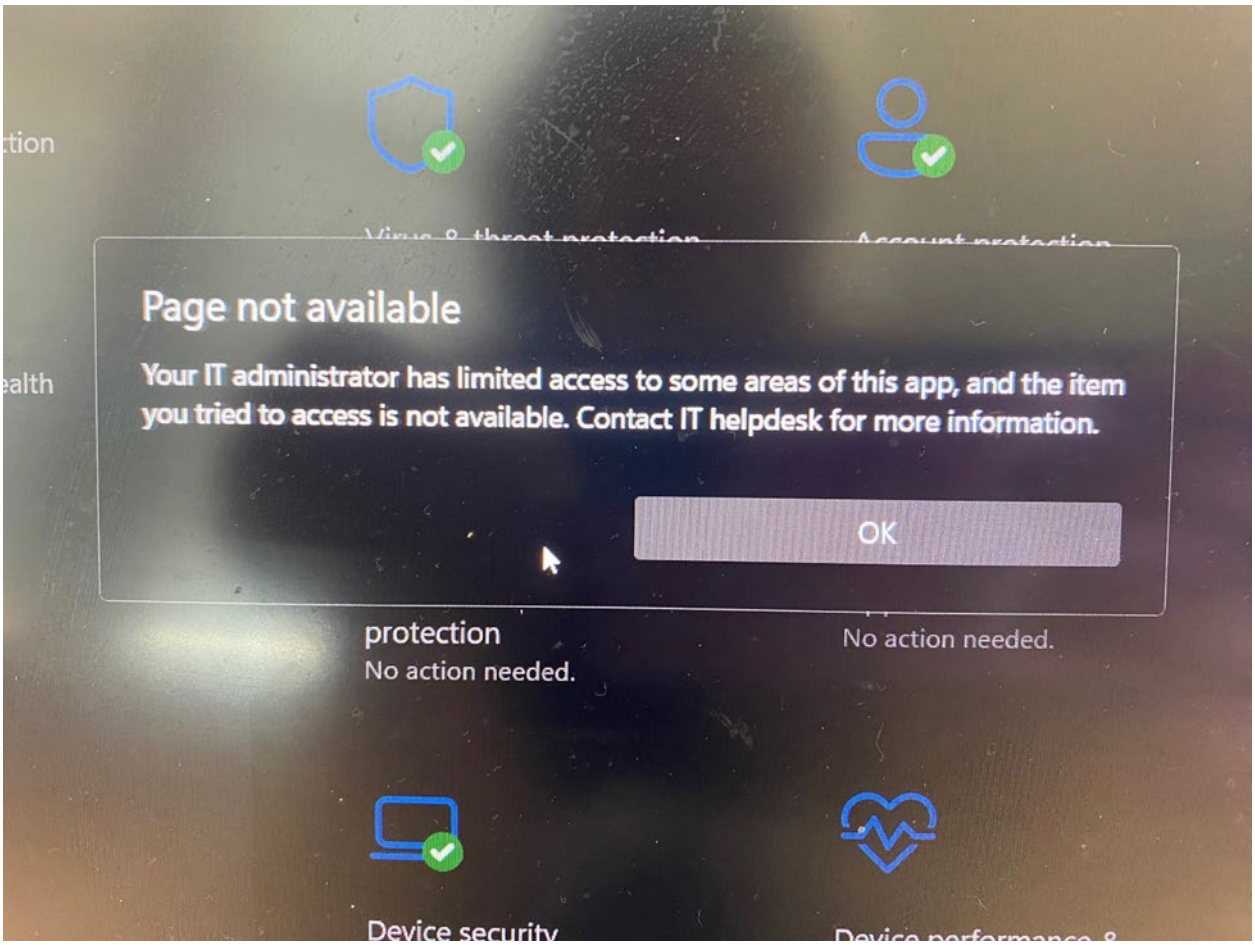


**Note that the U.S. government prosecutors have previously been caught doing the same thing in other high-profile cases.**

This is not the first time the federal government has sent trojan malware to invade defense teams in a high-profile case. In 2019, military prosecutors launched a similar illegal cyber-attack to invade the defense computers of Edward Gallagher, a highly decorated Navy SEAL platoon leader charged with war crimes.[1] The government's tracking malware attack in the Gallagher case *was far less significant* than the attack in this (the Slaughter) case. According to media sources, military prosecutors in the Gallagher case sent a "bit of digital artwork, embedded in an email message, contained hidden software that could track if anyone read or forwarded the email, and may have also been able to allow access to all communications and files on the recipients' computers."

Here, the government's malware actually took over Emily Lambert's computer. Below is a screenshot of Ms. Lambert's screen, notifying her that her "IT administrator" has limited her access to her own computer. It goes without saying that Ms. Lambert is supposed to be the actual administrator of her computer.

[1] Dave Philipps, Navy SEAL War Crimes Trial in Turmoil Over Claims Prosecutors Spied on Defense," New York Times, May 17, 2019. https://www.nytimes.com/2019/05/17/us/navy-seal-war-crimes-spying.html (accessed 3/28/20023).




The court in Gallagher suspended proceedings and ordered the prosecutors removed[2] and the defendant released from custody.[3] Slaughter and his son Gottfried ask for an investigation into the government's tracking malware.

[2] Howard Altman, "Lead Navy prosecutor in SEAL war crime case out over email spying," Navy Times, June 3, 2019 https://www.navytimes.com/news/2019/06/04/lead-navy-prosecutor-in-seal-war-crime-case-out-over-email-spying/ (accessed 3/27/2023) ("Navy Cmdr. Christopher Czaplak was ordered off the case against Special Warfare Operator Chief Edward "Eddie" Gallagher by the judge, Navy Capt. Aaron Rugh, on Monday after Czaplak admitted emailing 13 defense attorneys and paralegals, as well as Navy Times editor Carl Prine, a tracking beacon in an effort to find the source of leaks to the media.")

[3] Julie Watson, "Military judge frees Navy SEAL in advance of murder trial The Associated Press and Brian Melley, May 30, 2019 https://www.navytimes.com/news/your-military/2019/05/31/military-judge-frees-navy-seal-in-advance-of-murder-trial/ (accessed

**There are only three possible explanations for this Trojan malware attached to government discovery files, and the accidental explanations are the most serious.**

There are only three possibilities:

(1) Federal prosecutors knowingly sent Trojan malware to take over defense lawyers' computers;

(2) Federal prosecutors unintentionally forwarded discovery files containing malware from the FBI, without examining the files; or

(3) Federal prosecutors' computers and discovery files contain malware which allows **someone else** to control **US government computers**; and federal prosecutors are unaware that their computers are under the control of **someone else**.

For obvious reasons, each of these three possibilities is problematic. In fact it is difficult to rank which of the three possibilities are worse than others; because all three pose the most serious possible Constitutional, ethical and/or national security issues that can be imagined. If anything, the accidental explanations are the most serious.

Note that upon being questioned by email at 5:55 pm, AUSA Stephen Rancourt offered explanation #3 (some 18 hours later): "Well I'm certainly not trying to send you malware. It may have something to do with providing you the Cellbrite.exe. Let me re-run the .zip file and send again. (Note that the idea of "rerunning" the file suggests Rancourt ran the infected file previously.)

---

3/27/2023) (saying freeing Gallagher at this point would be a remedy for interference by prosecutors).

CONCLUSION

Defendants pray for an order by the Court:

1. Initiating an investigation into this matter;
2. Holding an evidentiary hearing regarding this matter;
3. Determining precisely which agency or agents created or originated the tracking malware virus;
4. Determining which agency or agents are now tracking and controlling defense lawyers' computers—or to what extent. (AUSA states that the case agent in this case is named Mark Tucher of Seattle.);
5. Determining whether the FBI or anyone else had a proper search warrant to search defense lawyers' computers in this case;
6. Determining the scope and scale of the FBI's (or other agencies') use of such tracking malware against other defense lawyers; and
7. Any other relief the Court deems proper, including dismissal of this case.

Dated: March 28, 2023

Respectfully Submitted,

*/s/ John M. Pierce*

John M. Pierce
21550 Oxnard Street
3rd Floor, PMB #172
Woodland Hills, CA 91367
Tel: (213) 400-0725
Email: jpierce@johnpiercelaw.com
Attorney for Defendant