Adventures in Contacting the Russian FSB

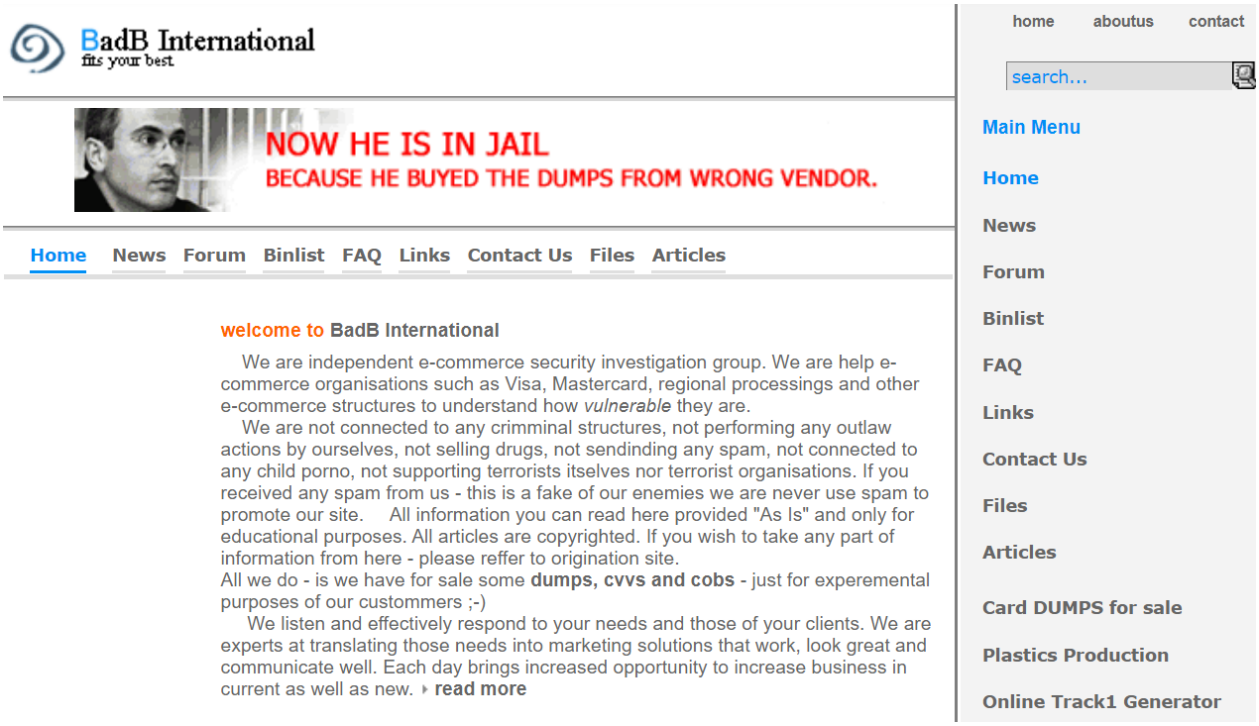
krebsonsecurity.com/2021/06/adventures-in-contacting-the-russian-fsb/

KrebsOnSecurity recently had occasion to contact the **Russian Federal Security Service** (FSB), the Russian equivalent of the **U.S. Federal Bureau of Investigation** (FBI). In the process of doing so, I encountered a small snag: The FSB's website said in order to communicate with them securely, I needed to download and install an encryption and virtual private networking (VPN) appliance that is flagged by at least 20 antivirus products as malware.

The FSB headquarters at Lubyanka Square, Moscow. Image: Wikipedia.

The reason I contacted the FSB — one of the successor agencies to the Russian KGB — ironically enough had to do with security concerns raised by an infamous Russian hacker about the FSB's own preferred method of being contacted.

KrebsOnSecurity was seeking comment from the FSB about a blog post published by Vladislav "BadB" Horohorin, a former international stolen credit card trafficker who served seven years in U.S. federal prison for his role in the theft of $9 million from RBS WorldPay in 2009. Horohorin, a citizen of Russia, Israel and Ukraine, is now back where he grew up in Ukraine, running a cybersecurity consulting business.



Horohorin's BadB carding store, badb[.]biz, circa 2007. Image: Archive.org.

Visit the FSB's website and you might notice its web address starts with http:// instead of https://, meaning the site is not using an encryption certificate. In practical terms, any information shared between the visitor and the website is sent in plain text and will be visible to anyone who has access to that traffic.

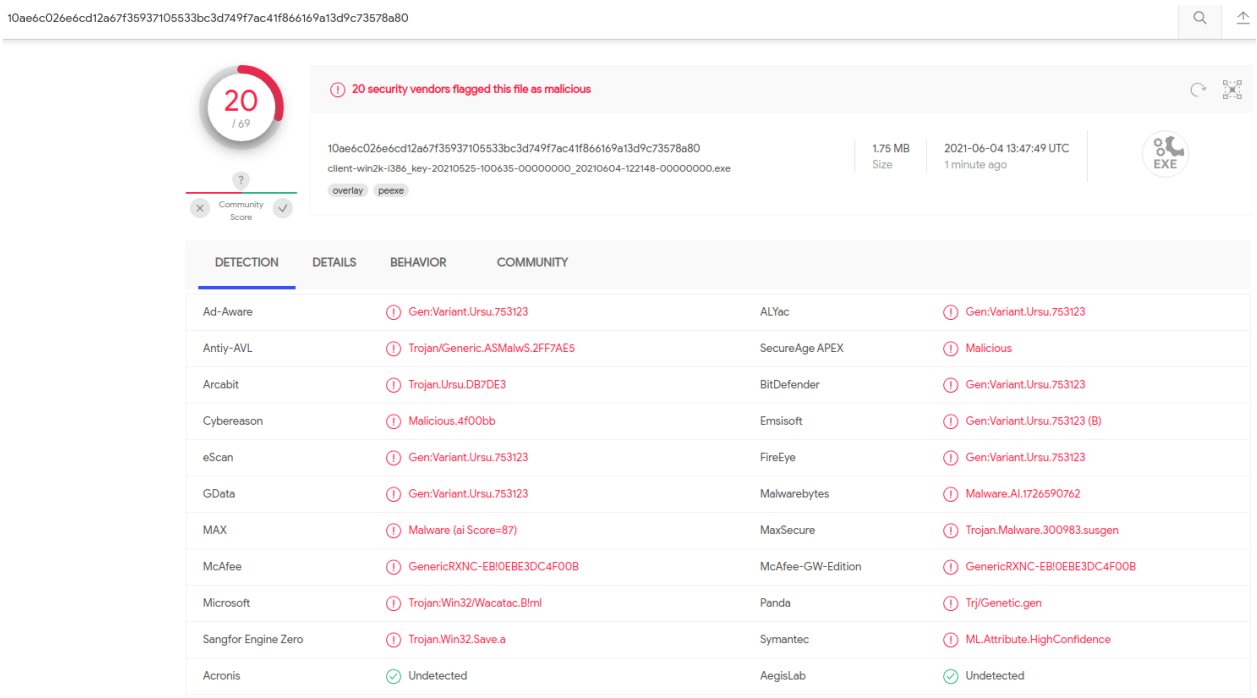
This appears to be the case regardless of which Russian government site you visit. According to Russian search giant Yandex, the laws of the Russian Federation demand that encrypted connections be installed according to the Russian GOST cryptographic algorithm.

That means those who have a reason to send encrypted communications to a Russian government organization — including ordinary things like making a payment for a government license or fine, or filing legal documents — need to first install **CryptoPro**, a Windows-only application that loads the GOST encryption libraries on a user's computer.

But if you want to talk directly to the FSB over an encrypted connection, you can just install their own client, which bundles the CryptoPro code. Visit the FSB's site and select the option to "transfer meaningful information to operational units," and you'll see a prompt to install a "random number generation" application that is needed before a specific contact form on the FSB's website will load properly.

Mind you, I'm not suggesting anyone go do that: Horohorin pointed out that this random number generator was flagged by 20 different antivirus and security products as malicious.

"Think well before contacting the FSB for any questions or dealing with them, and if you nevertheless decide to do this, it is better to use a virtual machine," Horohorin wrote. "And a spacesuit. And, preferably, while in another country."



Antivirus product detections on the FSB's VPN software. Image: VirusTotal.

It's probably worth mentioning that the FSB is the same agency that's been sanctioned for malicious cyber activity by the U.S. government on multiple occasions over the past five years. According to the most recent sanctions by the **U.S. Treasury Department**, the FSB is known for recruiting criminal hackers from underground forums and offering them legal cover for their actions.

"To bolster its malicious cyber operations, the FSB cultivates and co-opts criminal hackers, including the previously designated Evil Corp., enabling them to engage in disruptive ransomware attacks and phishing campaigns," reads a Treasury assessment from April 2021.

While Horohorin seems convinced the FSB is disseminating malware, it is not unusual for a large number of security tools used by VirusTotal or other similar malware "sandbox" services to incorrectly flag safe files as bad or suspicious — an all-too-common condition known as a "false positive."

Late last year I warned my followers on Twitter to put off installing updates for their **Dell** products until the company could explain why a bunch of its software drivers were being detected as malware by two dozen antivirus tools. Those all turned out to be false positives.

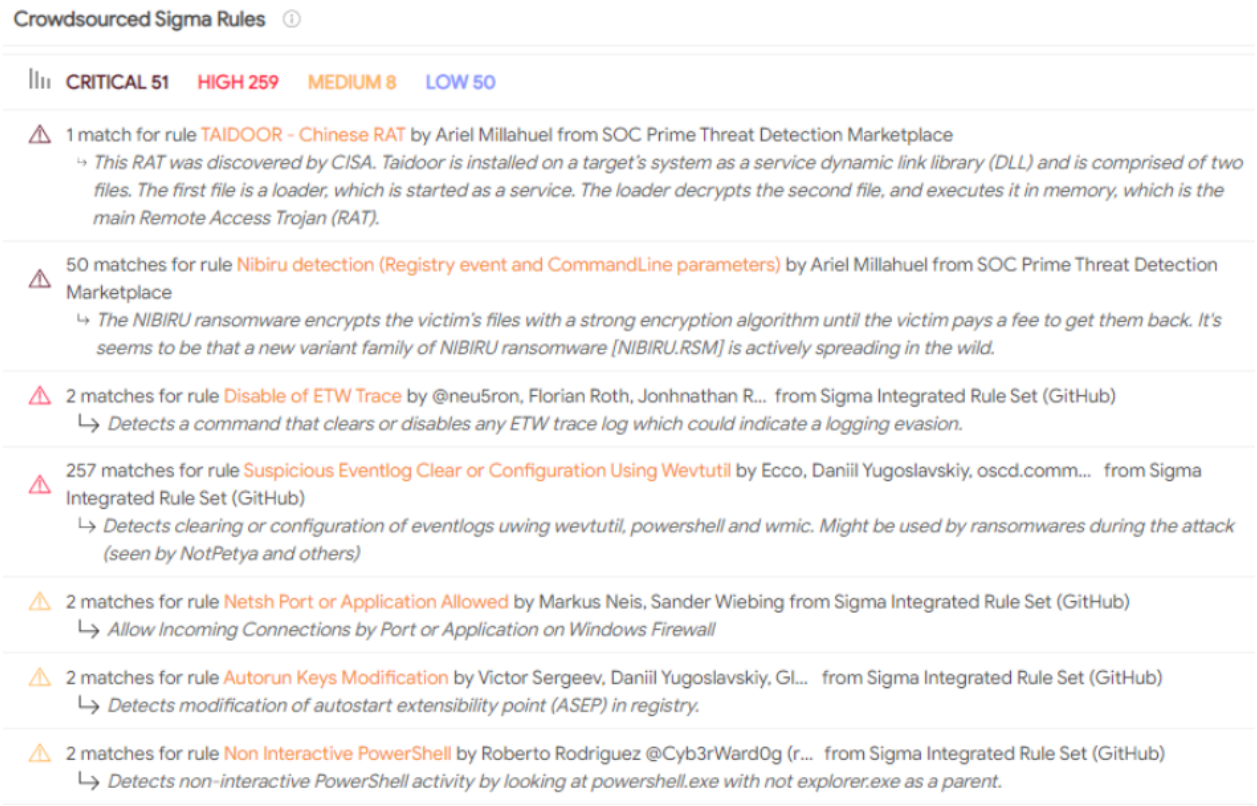
To really figure out what this FSB software was doing, I turned to **Lance James**, the founder of Unit221B, a New York City based cybersecurity firm. James said each download request generates a new executable program. That is because the uniqueness of the file itself is part of what makes the one-to-one encrypted connection possible.

“Essentially it is like a temporary, one-time-use VPN, using a separate key for each download” James said. “The executable is the handshake with you to exchange keys, as it stores the key for that session in the exe. It’s a terrible approach. But it’s what it is.”

James said the FSB’s program does not appear to be malware, at least in terms of the actions it takes on a user’s computer.

“There’s no sign of actual trojan activity here except the fact it self deletes,” James said. “It uses GOST encryption, and [the antivirus products] may be thinking that those properties look like ransomware.”

James says he suspects the antivirus false-positives were triggered by certain behaviors which could be construed as malware-like. The screenshot below — from VirusTotal — says some of the file’s contents align with detection rules made to find instances of ransomware.



Some of the malware detection rules triggered by the FSB’s software. Source: VirusTotal.

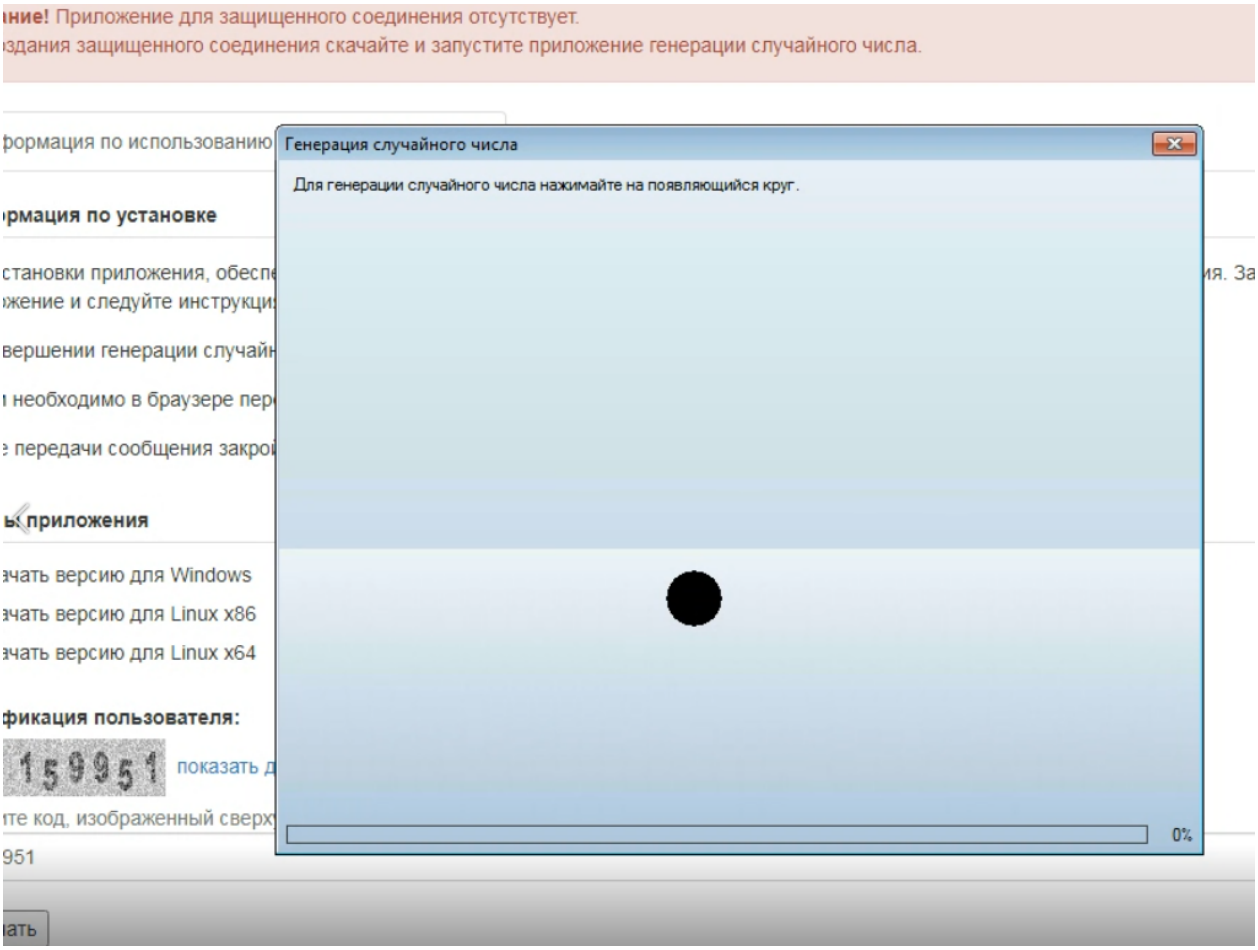
Other detection rules tripped by this file include program routines that erase event logs from the user’s system — a behavior often seen in malware that is trying to hide its tracks.

On a hunch that just including the GOST encryption routine in a test program might be enough to trigger false positives in VirusTotal, James wrote and compiled a short program in C++ that invoked the GOST cipher but otherwise had no networking components. He then uploaded the file for scanning at VirusTotal.

Even though James' test program did nothing untoward or malicious, it was flagged by six antivirus engines as potentially hostile. Symantec's machine learning engine seemed particularly certain that James' file might be bad, awarding it the threat name "ML.Attribute.HighConfidence" — the same designation it assigned to the FSB's program.

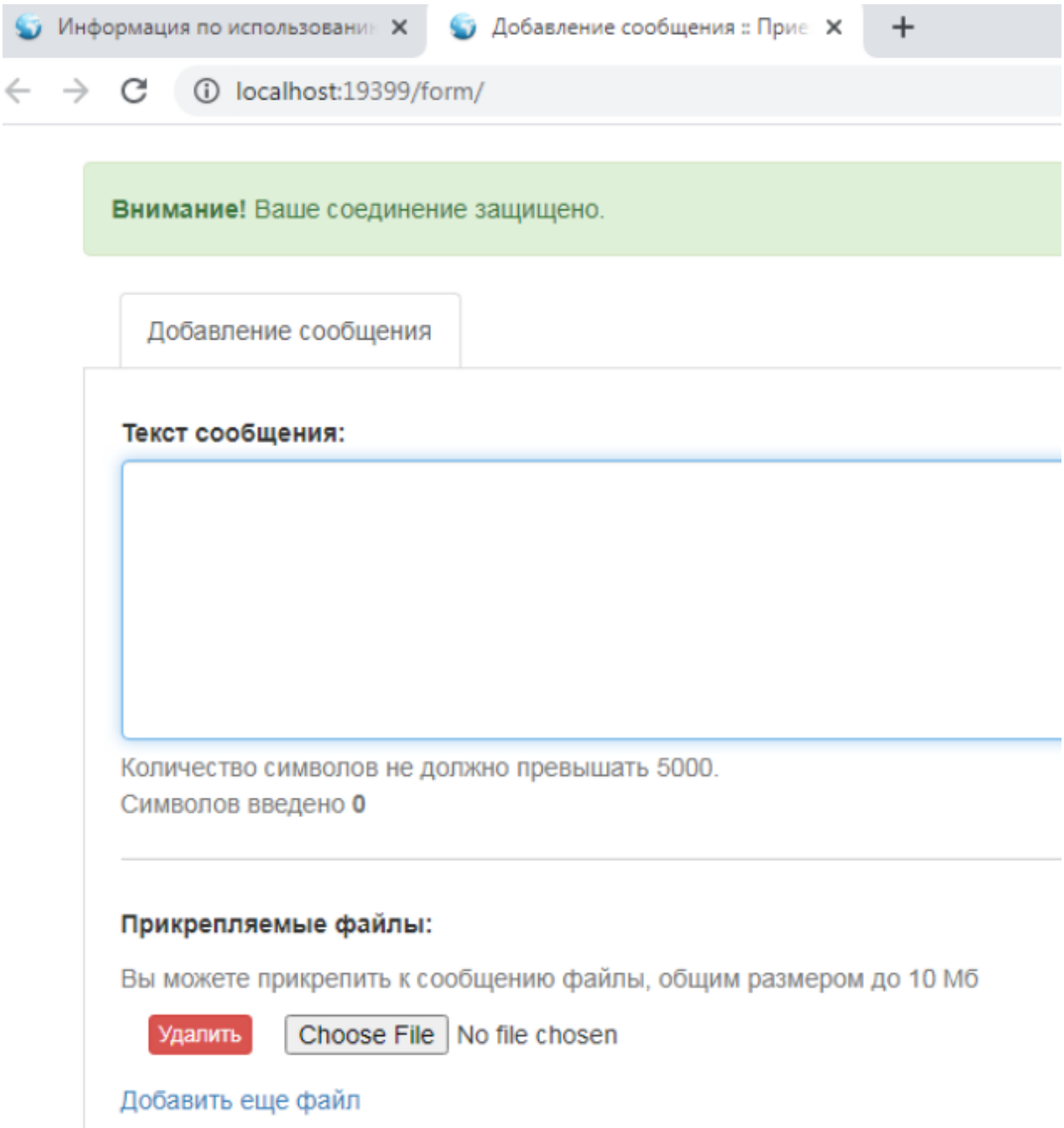
KrebsOnSecurity installed the FSB's software on a test computer using a separate VPN, and straight away it connected to an Internet address currently assigned to the FSB (213.24.76.xxx).

The program prompted me to click on various parts of the screen to generate randomness for an encryption key, and when that was done it left a small window which explained in Russian that the connection was established and that I should visit a specific link on the FSB's site.



The FSB's random number generator in action.

Doing so opened up a page where I could leave a message for the FSB. I asked them if they had any response to their program being broadly flagged as malware.



The contact form that ultimately appeared after installing the FSB's software and clicking a specific link at fsb[.]ru.

After all the effort, I'm disappointed to report that I have not yet received a reply. Nor did I hear back from S-Terra CSP, the company that makes the VPN software offered by the FSB.

James said that given their position, he could see why many antivirus products might think it's malware.

"Since they won't use our crypto and we won't use theirs," James said. "It's a great explanation on political weirdness with crypto."

Still, James said, a number of things just don't make sense about the way the FSB has chosen to deploy its one-time VPN software.

“The way they have set this up to suddenly trust a dynamically changing exe is still very concerning. Also, why would you send me a 256 random number generator seed in an exe when the computer has a perfectly valid and tested random number generator built in? You’re sending an exe to me with a key you decide over a non-secure environment. Why the fuck if you’re a top intelligence agency would you do that?”

Why indeed. I wonder how many people would share information about federal crimes with the FBI if the agency required everyone to install an executable file first — to say nothing of one that looks a lot like ransomware to antivirus firms?

After doing this research, I learned the FSB recently launched a website that is only reachable via Tor, software that protects users’ anonymity by bouncing their traffic between different servers and encrypting the traffic at every step of the way. Unlike the FSB’s clear web site, the agency’s Tor site does not ask visitors to download some dodgy software before contacting them.

“The application is running for a limited time to ensure your safety,” the instructions for the FSB’s random number generator assure, with just a gentle nudge of urgency. “Do not forget to close the application when finished.”

Yes, don’t forget that. Also, do not forget to incinerate your computer when finished.