Recorded Future

CYBER THREAT ANALYSIS

Pavlov's Digital House: Russia Focuses Inward for Vulnerability Analysis

By Priscilla Moriuchi and Dr. Bill Ladd

Recorded Future

Scope Note: Over the course of the past year, Recorded Future has examined the publication speeds, missions, and utility of the national vulnerability databases (NVDs) of two countries: China and the United States. We decided to apply the same analytic techniques to Russia's vulnerability database to see what we could learn. This report includes a detailed analysis of vulnerabilities published by the Federal Service for Technical and Export Control of Russia (FSTEC), official Russian government documents, Recorded Future data, and open source intelligence (OSINT). The data analyzed for this report was compiled on March 30, 2018.

Executive Summary

Russia's vulnerability database is highly focused. However, it is incomplete, slow, and likely intended to support the control of the Russian state over technology companies and users. Generally, Russia publishes only 10 percent of known vulnerabilities, is on average 83 days slower than China's National Vulnerability Database (NVD), 50 days slower than the U.S. NVD, and incomplete in the few technologies it does cover.

Key Judgements

- Russia's vulnerability database is run by the Federal Service for Technical and Export Control of Russia (FSTEC). FSTEC is the military organization responsible for protecting state secrets and supporting counterintelligence and counterespionage operations.
- FSTEC's vulnerability database is also known as the BDU (Банк данных угроз безопасности информации). The BDU has published only 11,036 vulnerabilities of the 107,901 CVEs reported by NVD (approximately 10 percent).
- FSTEC has published 61 percent of vulnerabilities exploited by Russian state-sponsored threat groups. This is substantially above the norm of 10 percent; however, the data is insufficient to determine the influence of Russian intelligence services on FSTEC publication.
- FSTEC populates the BDU database with vulnerabilities that primarily present a threat to Russian state information systems. This gives researchers information on which technologies, hardware, and software are used on Russian government networks.

Background

The Federal Service for Technical and Export Control of Russia (FSTEC) was established in 2004 and is subordinate to the Ministry of Defense (MOD). FSTEC has a central office in Moscow, seven regional "headquarters," and an information security research and testing

institute known as the State Science and Research Experimental Institute of Technical Information Protection Problems of FSTEC, or the GNIII PTZI FSTEC.

FSTEC headquarters in Moscow, located at 105066, Moscow, ul. Staraya Basmannaya, 17.

The prime minister's official website describes FSTEC as "a federal executive body responsible for implementing government policy, organizing interdepartmental cooperation and interaction, and exercising special and control functions in the area of state security."

According to further official documentation released in 2016, FSTEC implements state policy, organizes interdepartmental cooperation, and exercises special functions of state security in the fields of:

- Information systems security
- Countering foreign technical threats to Russia
- Security of state secrets
- Export control

As intimated in the organization's title, the first three areas fall squarely under the technical control mission. According to our extensive review of FSTEC documentation, export control likely assumes a much smaller share of FSTEC resources than all of the tasks and functions

under technical control. The technical control mission covers internal control, state information systems, and foreign technology sold in Russia.

While subordinate to the MOD, FSTEC has a much longer and more extensive list of authorities, particularly in the realms of technical control and security of state secrets. According to documentation listed on FSTEC's website, the organization also regulates commerce surrounding materials that could be used in chemical and nuclear weapons, counters technical intelligence, issues opinions on the use of Russian territory for foreign scientific research, and finances research on the study of radiation emitted from different types of systems and devices.

FSTEC also has a board of senior government officials appointed by position. This board includes the First Deputy Chief of the General Staff Department of the Russian Military, Deputy Minister of Internal Affairs, Head of the Economic Security Service under the Federal Security Service (FSB), and the Deputy Director of the SVR, among others. The primary function of the board is setting and administering the FSTEC budget, as well as coordinating interdepartmental functions.

Among the myriad responsibilities under the four primary FSTEC functions, the organization also works with the FSB in protecting state secrets, supports technical counterintelligence and counterespionage,[1] and is empowered to monitor the communications of government officials who work with state secrets.

FSTEC is currently run by Director Vladimir Selin, who has been in that position since May 2011. Selin is supported by one First Deputy Director, Sergey Yakimov, and four Deputy Directors. In addition to his position as Director of FSTEC, Selin is also a member of the Defense Ministry Board, and Deputy Chairman of the Commission on State Secrets (on which he sits with Chief of the General Staff of the Russian Military General Valery Gerasimov).

According to official state documents, in 2015 FSTEC was assigned a total of 1,111 employees, not including security, protection, or maintenance personnel. Of the 1,111 employees, 225 are located in the Moscow headquarters, and the remaining 886 are spread out over FSTEC's seven regional offices.

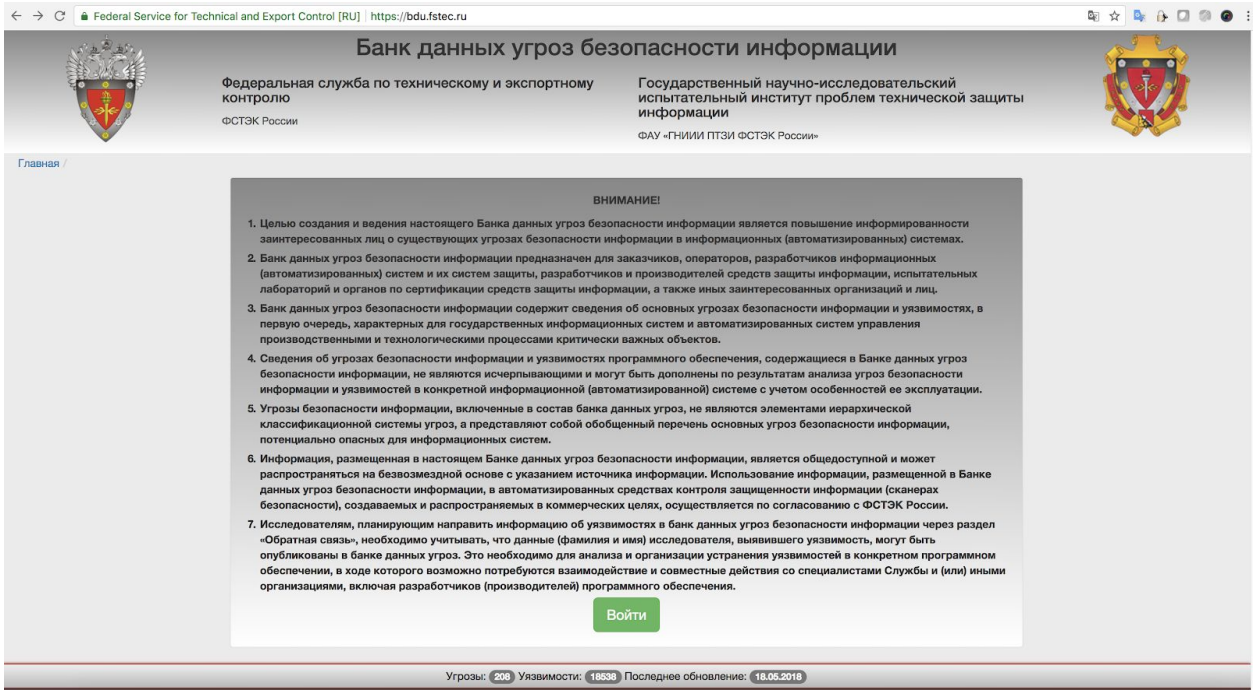
[1] According to the National Counterintelligence and Security Center's (NCSC) Counterintelligence Terms Glossary, counterespionage (CE) is a unique subset of counterintelligence and is the "offensive, or aggressive, side of counterintelligence." "CE is an offensive operation, a means of obtaining intelligence about the opposition by using — or, more usually, attempting to use — the opposition's operations."

Given the mission focus on technical control, it is likely that the majority of these 1,111 employees work on issues related to this mandate, while a much smaller minority support FSTEC's export control work.

FSTEC's Vulnerability Publication Process

FSTEC also runs a vulnerability publication database, to which it provides public access via the website bdu.fstec.ru/vul. The homepage states that the purpose of the database is to "increase the awareness of interested persons in existing threats to information security systems" and that it is designed for a wide range of customers, operators, developers, information security professionals, testing laboratories, and certification bodies.

FSTEC also states that the database "contains information about the main threats to information security and vulnerabilities, primarily those characteristic of state information systems and automated systems for managing production and technological processes of critical facilities.[2]"



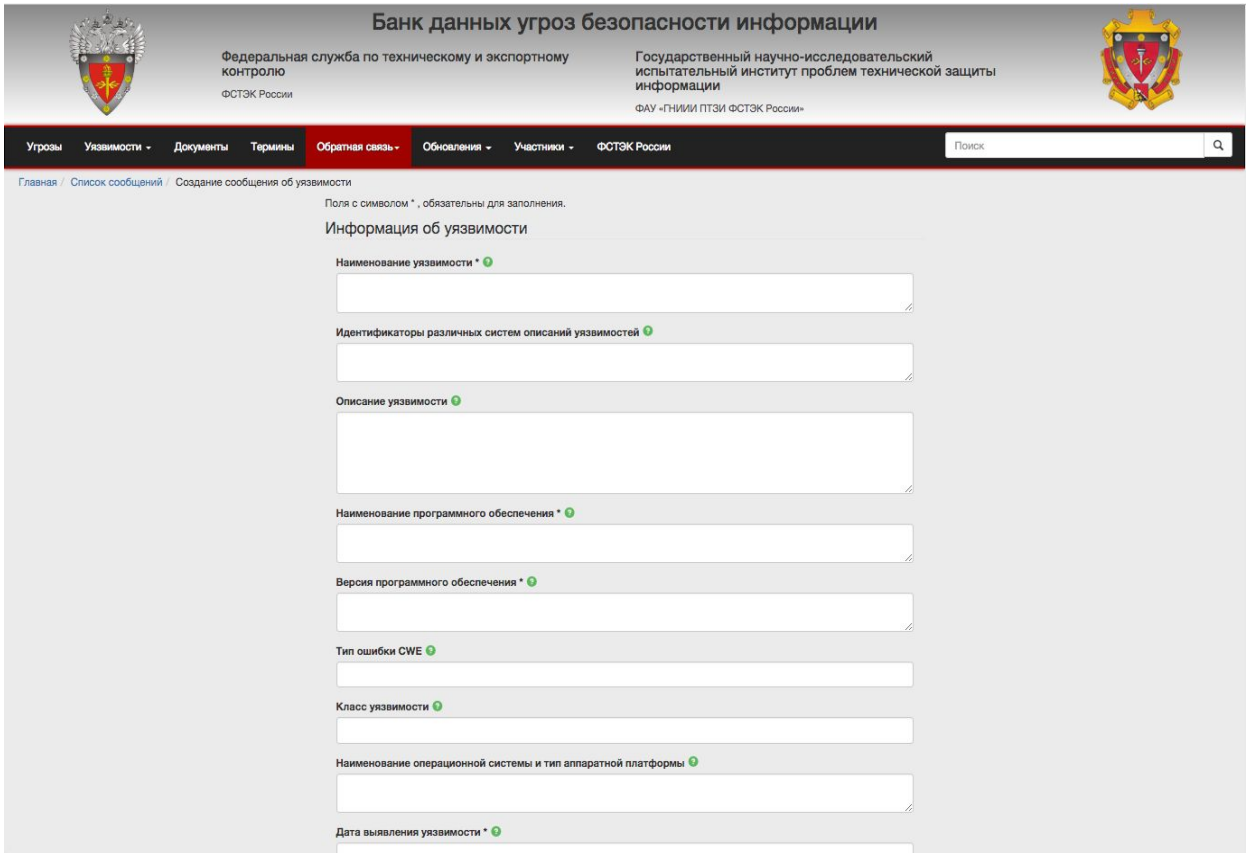
Homepage of FSTEC's Security Threats Database, which lists the purpose and intended audience for the data.

FSTEC does not claim that this database is exhaustive. Instead, it focuses on publishing vulnerabilities for information systems used by the state and in "critical facilities." This mission is also exhibited in the responsibilities and activities of FSTEC's seven regional

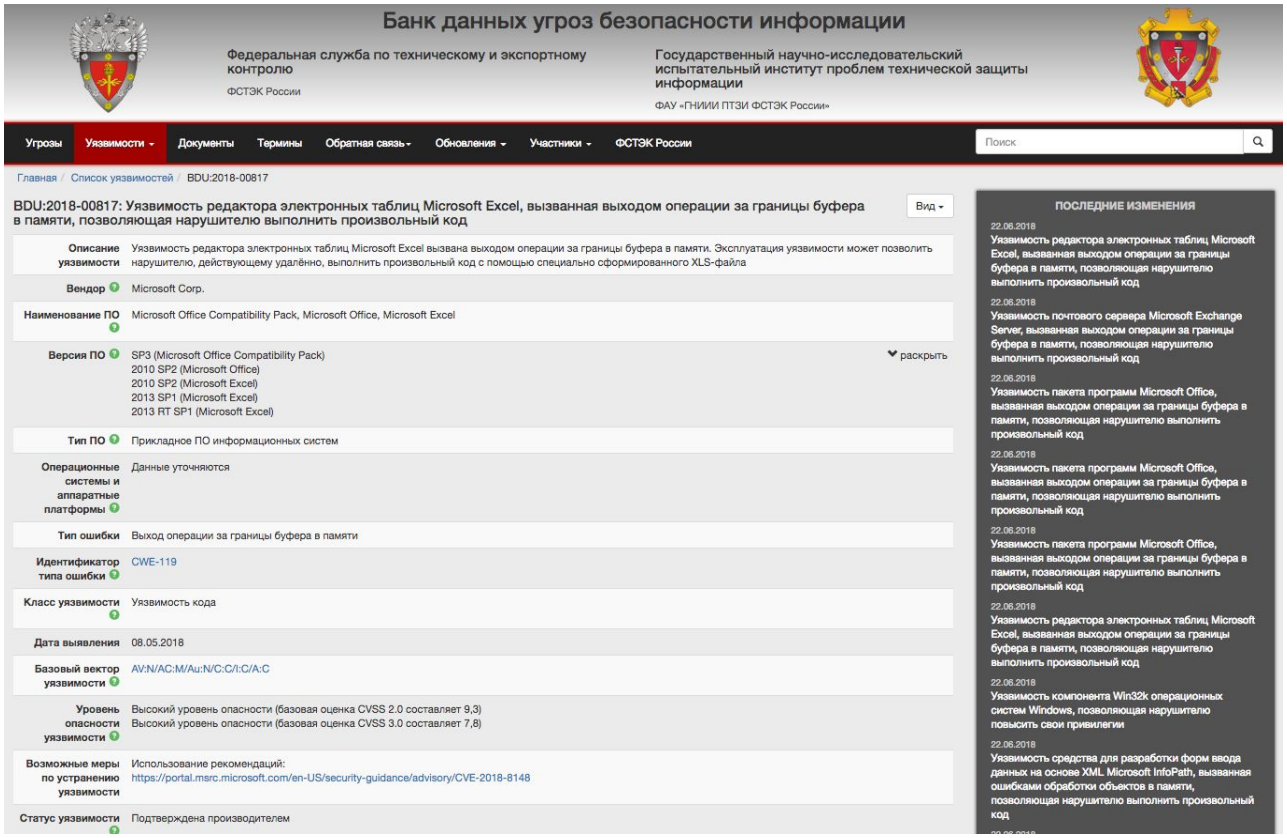
[2] This content was machine translated using Google Translate.

departments. The majority of tasks levied upon each of the regional headquarters are overwhelmingly centered around countering foreign technical intelligence and protecting state information systems and data within each district. Of the 10 or 11 tasks levied upon each of the regional headquarters, the top seven all concern countering foreign technical intelligence collection and protecting state information systems, while the remaining relate to export control.

Reporting a threat or vulnerability to the database (known as the BDU) is relatively simple. FSTEC provides a form for submission which closely matches the vulnerability entries themselves.



FSTEC vulnerability submission form.



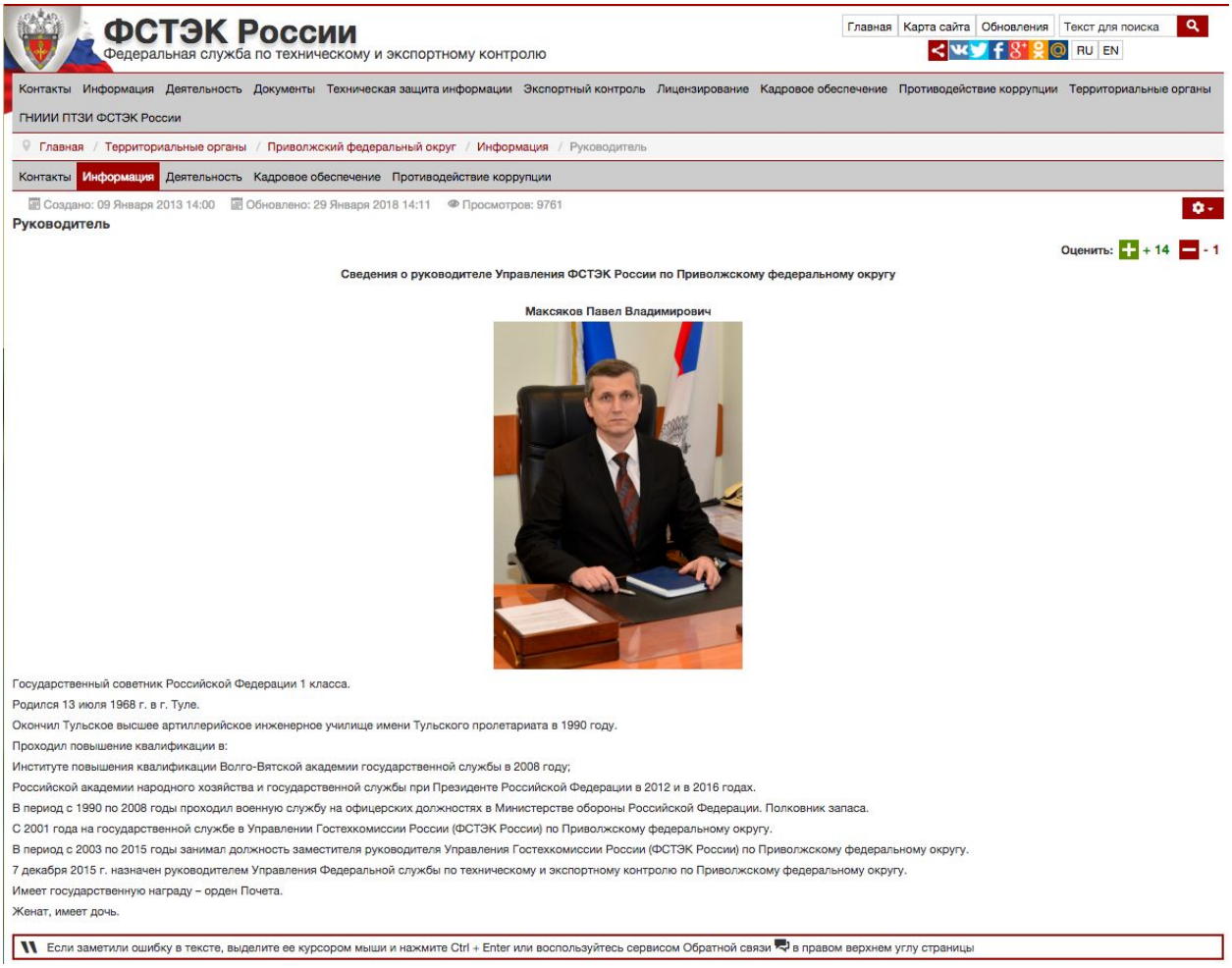
FSTEC BDU entry for [CVE-2018-8148](CVE-2018-8148).

FSTEC even provides simple download links to retrieve its entire database as either Excel or XML files. These downloads contain fields typical of other vulnerability databases including internal IDs, corresponding CVE identifiers, affected technologies, links to supporting documents, severity assessments, etc. What is not included in the publication is the date for when FSTEC first disclosed the vulnerability. We used proprietary techniques to establish these dates for vulnerabilities disclosed by FSTEC since January 1, 2017.

FSTEC Is Not a Public Service Organization

FSTEC is an organization subordinate to, run by, and administratively part of the Ministry of Defense (MOD). All current FSTEC senior leadership, including the director, deputy directors, and all heads of regional headquarters[3] are former military officers, many of whom also served concurrently in officer or reserve positions in previous roles within FSTEC.

[3] Biographies of each regional head can be found under the "Территориальные органы" tab at https://fstec.ru.



Screenshot of the biography of Pavel Maksyakov, head of the FSTEC Volga District office.

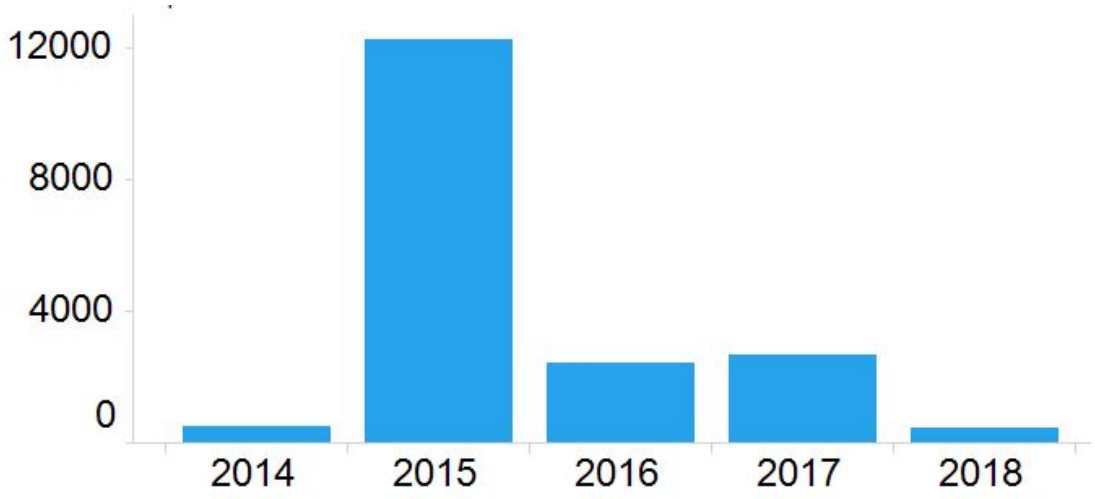
FSTEC's primary mission is explicit, documented, and repeated in law after law and order after order; state security is its overarching mandate. Unlike "sister" organizations in other countries, such as CNITSEC in China (which runs CNNVD), FSTEC does not claim to have a public service mission, but instead populates its vulnerability database (BDU) with vulnerabilities that primarily present a threat to state information systems. However, FSTEC is dissimilar to CNITSEC in that FSTEC is an overt military organization with an overt state secrecy mission.

A 2014 meeting between Chinese Premier Li Keqiang and Russian Prime Minister Dmitry Medvedev indicates that the Russian government views the Chinese Ministry of Commerce as the functional Chinese counterpart to FSTEC, not CNITSEC or the Ministry of State Security. This is probably because of FSTEC's primary focus on technical control of the domestic information and technology environment, which is a much broader mission than CNITSEC's.

Since FSTEC is an overt military organization, the questions about FSTEC's vulnerability database primarily center around why FSTEC even publishes the few vulnerabilities that it does. As documented below, the BDU is extremely slow and not comprehensive. The few vulnerabilities it does publish tell us more about FSTEC's mission and Russian state information systems than the intentions of the Russian military for offensive cyber operations.

Threat Analysis

FSTEC began publishing vulnerability data in 2014, roughly 15 years after the U.S. National Vulnerability Database (NVD) was established. As seen below, the FSTEC vulnerabilities published by year demonstrate an initial low volume of publications in 2014, a surge in 2015, and then a lower level of publications between 2016 and 2018.



Russian vulnerabilities published by year.

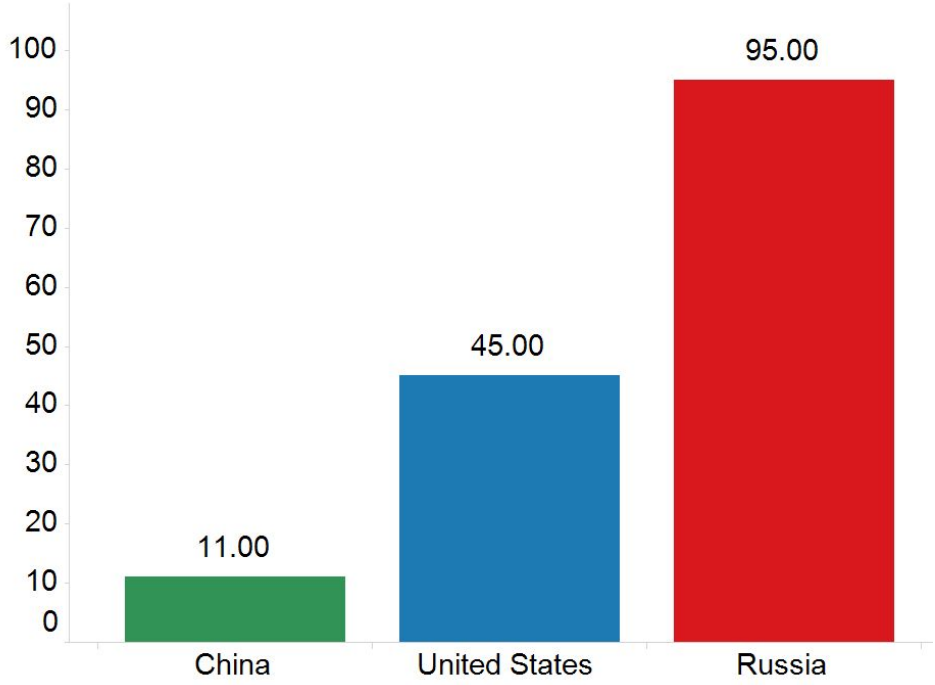
What Happened in 2015?

In examining the mapping of FSTEC's BDU identifiers to NVD's CVE identifiers, we observed that the mappings were not always one to one. FSTEC occasionally linked multiple CVEs into a single BDU vulnerability, and also occasionally created multiple BDU identifiers for different operating systems vulnerable to a single CVE. Russian BDUs cover 11,036 — or approximately 10 percent — of the 107,901 CVEs reported by NVD. This difference is not simply due to FSTEC starting later, as approximately 25 percent of CVEs covered by FSTEC were from years before FSTEC began operation.

Despite the non-linear correlation between BDU and CVE identifiers, it is clear that FSTEC published far more vulnerabilities in 2015 than any other year. This is probably because 2015 was an experimental year for the BDU database, in which FSTEC evaluated its functionality and utility. Although the 2015 FSTEC annual activity report (issued in March 2016) did not address the outcome of the BDU experiment, it is clear from the data that a decision was made to drastically reduce the scope and number of vulnerabilities published. A narrower scope is also in better alignment with the database's public mission, which is to report on vulnerabilities in information systems used by the state or in "critical facilities."

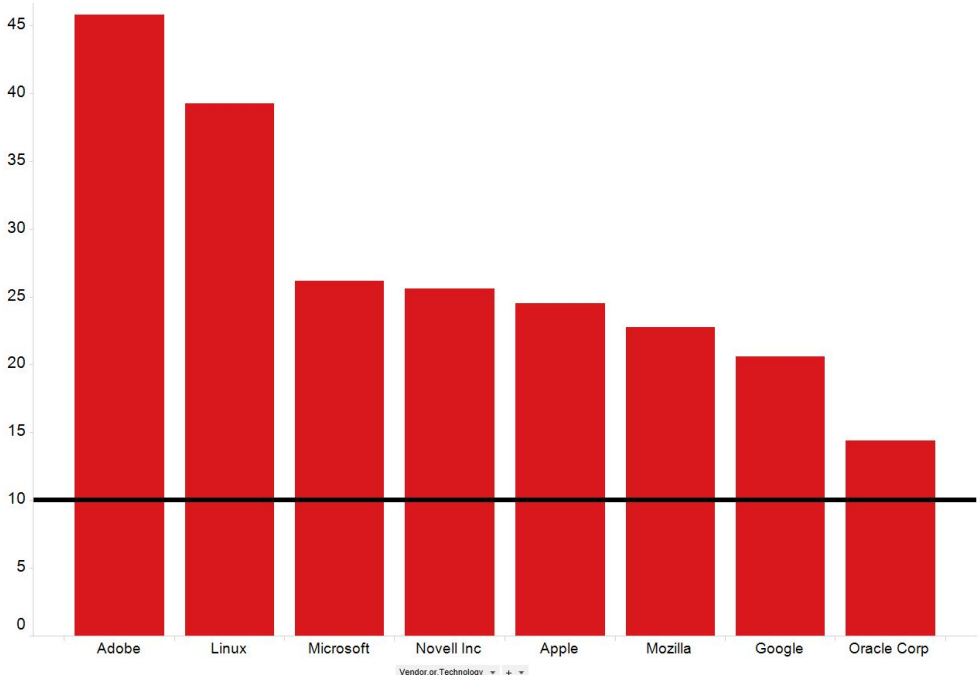
Furthermore, among the vulnerabilities that FSTEC published the fastest, 75 percent were vulnerabilities for browsers or industrial control-related software.

In previous reporting, we assessed the differing rates of vulnerability disclosure publications between the Chinese and U.S. national vulnerability databases and learned that the Chinese are much faster at disclosure on average than the United States. We examined the set of vulnerabilities published in 2017 to 2018 that were in common among the three national vulnerability databases and observed that Russian vulnerability disclosure dramatically lags behind both U.S. and Chinese disclosure. Russian vulnerability disclosure is not only incomplete, but also extremely slow.

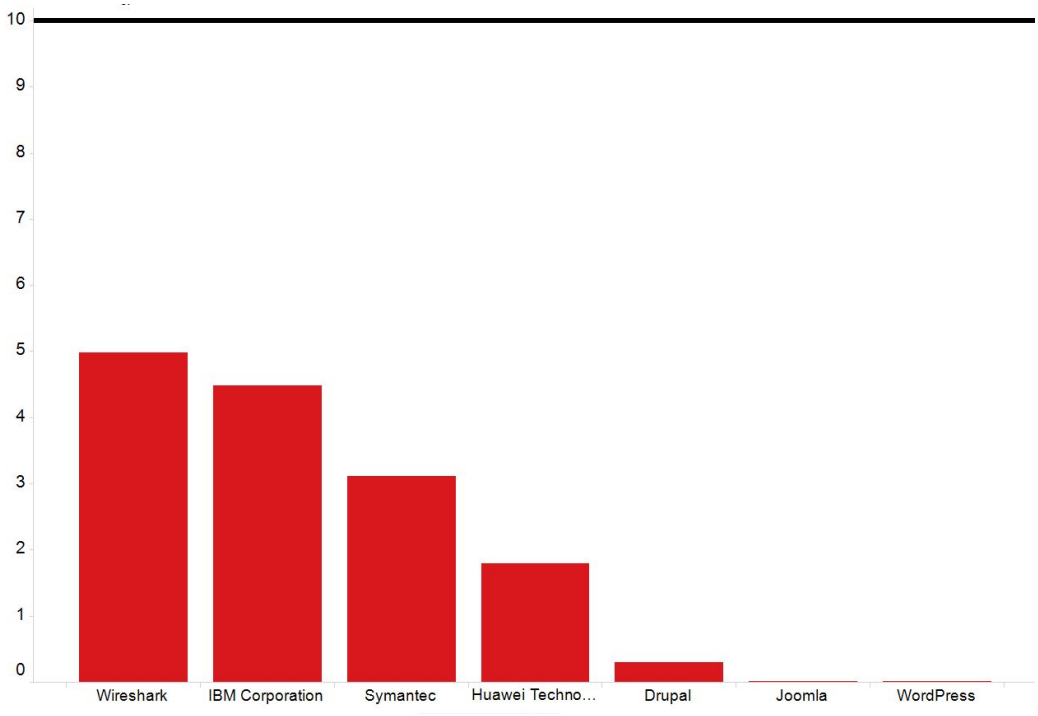


Days of vulnerability disclosure delay across different national vulnerability databases.

To better understand how FSTEC selected vulnerabilities to disclose, we examined the technology vendors that FSTEC covered at a higher rate than expected given its overall coverage level of 10 percent. The black line in the two charts below (at the value for 10) represents the 10 percent of all vulnerabilities that FSTEC publishes. All vendors with coverage under 10 percent are considered "under covered," and all vendors substantially over 10 percent are considered "over covered."



Percentage of vendor CVEs covered by FSTEC.



Percentage of vendor CVEs covered by FSTEC.

Similar analysis suggests that FSTEC significantly under covered content management systems (such Wordpress, Joomla, and Drupal), as well as IBM and Huawei compared to its baseline level of coverage across all technologies.

Coverage of Russian APT Vulnerabilities

In a 2016 Recorded Future publication, we provided an analysis of vulnerabilities used by Russian APTs, and in particular, which vendors were most widely represented.

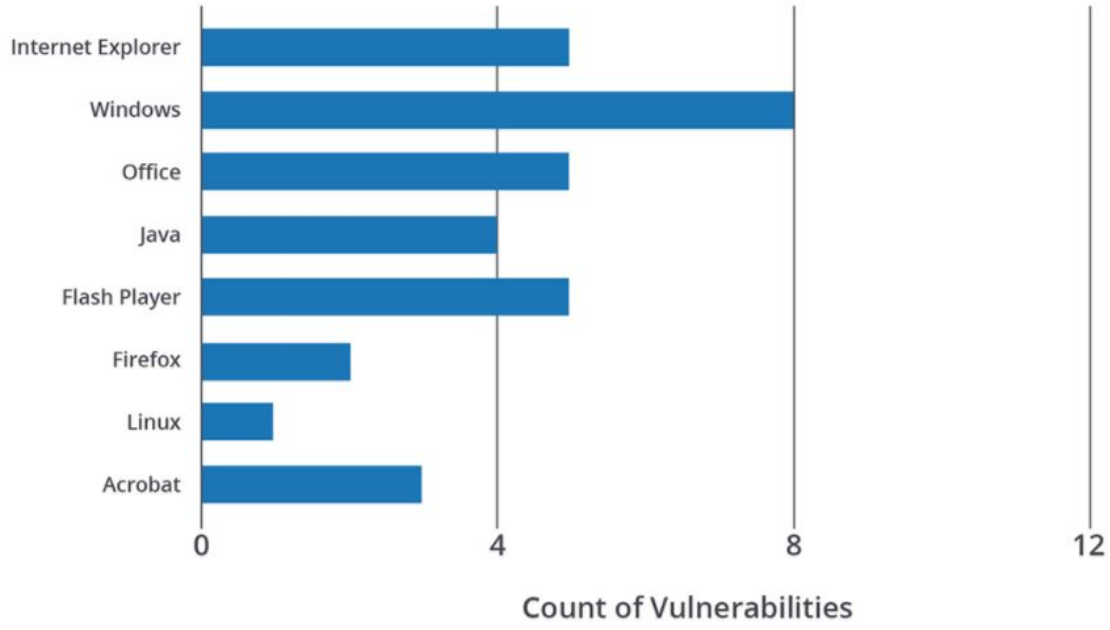


Image from a Recorded Future blog, "Running for Office: Russian APT Toolkits Revealed."

Vendors for all of these technologies were listed in the areas that FSTEC over focused on. This means that FSTEC published far more than 10 percent of the vulnerabilities discovered for each vendor. However, each of these vendors produces some of the most widely used software in the world and it would be reasonable to expect that Russian APT groups would target these technologies.

To explore this point more thoroughly, we also conducted an updated analysis of all vulnerabilities exploited by Russian APT groups in the last four years. Utilizing only vulnerabilities with a CVE number and those which were also published by U.S. NVD and CNNVD, we identified 49 vulnerabilities that had been utilized by Russian APT groups in that timeframe.

Thirty of those 49 vulnerabilities, or 61 percent, were published by FSTEC. This is substantially higher than FSTEC's average of 10 percent. Further, 18 of those 30 published vulnerabilities have been exploited by APT28 (Intelligence Card), which has been attributed to the Russian military's Main Intelligence Directorate (GRU). This amounts to FSTEC publishing 60 percent of vulnerabilities exploited by the Russian military. This is far outside FSTEC's statistical average of 10 percent.

Again, many of these vulnerabilities are for the most widely used software in the world. However, this abnormally high reporting rate for both the software vendors and vulnerabilities themselves raises two possibilities. First, since FSTEC's mission is to protect Russian government information systems, this indicates that Russian government systems utilize these programs and were themselves exposed to these vulnerabilities as well. This is further confirmation that examining FSTEC publications can yield insight into Russian government information systems.

Second, FSTEC is a military organization, has several military intelligence members on its board, and would regularly interact with military intelligence to protect classified systems. It is possible that military intelligence could be obligated to protect Russian state information systems with knowledge they possessed on vulnerabilities, or that Russian military hackers could be leveraging vulnerabilities published by FSTEC for their operations.

The public record and available data is not yet sufficient to determine the relationship between FSTEC and Russian state-sponsored cyber operations. However, it is clear that FSTEC's vulnerability database is utilized by Russian intelligence services in a different manner than CNNVD is by Chinese intelligence. In China, CNNVD delays or hides the publication of vulnerabilities being used by the intelligence services, while in Russia, it is possible that FSTEC publishes vulnerabilities being used by the intelligence services in order to protect against them.

The only high-coverage vendor covered by FSTEC but not listed above is Novell.

From our over-coverage analysis, we know FSTEC focuses on Adobe more than any other individual vendor by covering nearly half of all Adobe vulnerabilities. However, when we took a closer look at the Adobe vulnerabilities not covered by FSTEC, we observed that FSTEC has not published 386 Adobe vulnerabilities with a CVSS score of 10, or 871 Adobe vulnerabilities with a CVSS score greater than eight. FSTEC is not even comprehensive on vulnerability disclosure for the technology area in which the data clearly shows the most interest.

If FSTEC was a serious resource for vulnerability information, it would have to be faster and more comprehensive. Even FSTEC's corporate partners do not claim to exclusively use the BDU database. We examine three hypotheses for why FSTEC publishes so few vulnerabilities below.

Technology Licensing

A primary portion of FSTEC's technical control mission is to conduct product reviews and issue licenses to companies that want to sell their products in Russia. According to a June 2017 Reuters article, both the FSB and FSTEC conduct reviews of foreign technology including "source code for security products such as firewalls, antivirus applications, and software containing encryption before permitting the products to be imported and sold in the country." The FSB reportedly utilizes certified partner companies to conduct some of the reviews, including a company called Echelon, which is also a partner to FSTEC in administration of the BDU database.

According to Echelon and the websites of a number of other certified FSTEC partners,[4] the FSB is responsible for the reviews of cryptographic and encryption tools, while FSTEC issues licenses for the development or production and technical protection of "confidential information." FSTEC licenses are broadly required for the production and sale of software in Russia.

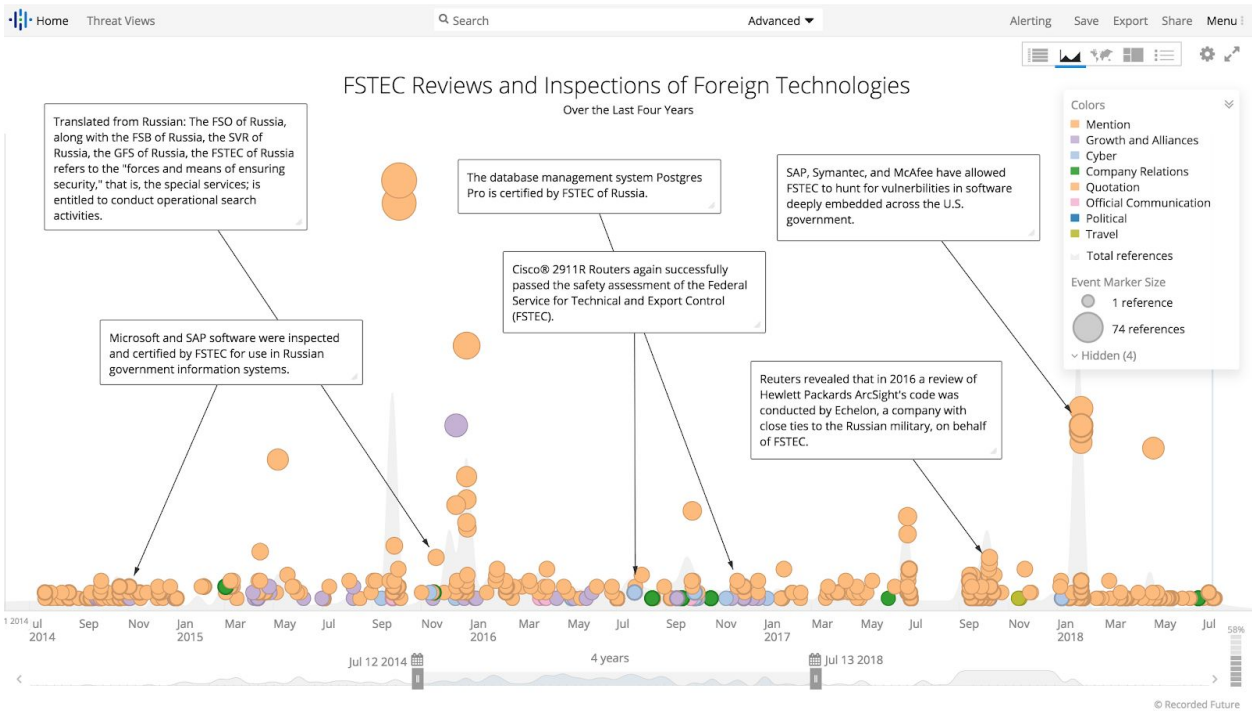
Among FSTEC's partners in administering the BDU, including Digital Security, Institute of System Programming of The V.P. Ivannikova Russian Academy of Science, Rusbitech, All-Tech-Soft, and Perspective Monitoring, only Echelon claims to be able to assist customers with FSTEC, FSB, and MOD reviews.

However, unlike the FSB, FSTEC does not use partners or intermediaries to conduct its reviews. In October 2016, FSTEC issued a clarification on its website, stating that FSTEC does not interact with "intermediaries" and does not work with any private organizations in the "provision of government services for licensing."

FSTEC publishes a registry of licensees for each certification it issues. Fourteen licenses have been issued in 2018 for the development and production registry, while 66 technical protection licenses have been issued this year (as of July 9, 2018). This is in contrast to the 140 development and production licenses and 293 technical protection licenses issued in 2017.

Many well-known international companies have received these certifications, including Honeywell, Alcatel-Lucent, Kaspersky, Huawei, Hewlett-Packard, Bombardier, Atos, and Symantec.

[4] See http://rusbitech.ru/about/certificate/, https://www.ntcsiz.ru/site/view?id=1, and https://www.altx-soft.ru/license.htm.



Timeline of foreign technology inspections conducted by FSTEC.

The criteria for obtaining an FSTEC license are so broad that it is difficult to assess which information from a software company would be deemed unnecessary to the approval process. Further, despite the different certification regimes and credentials, the information a company must share with FSTEC is very similar to that required by the FSB for its licensure. This includes extensive data on personnel, facilities, products, software production and testing, and more.

Outlook

Why Does FSTEC Publish so Few Vulnerabilities?

As the research above demonstrates, FSTEC broadly publishes only about 10 percent of known vulnerabilities. The larger question is, "Why?" Why waste resources on a vulnerability disclosure database that does not address 90 percent of vulnerabilities for its users?

There are three likely hypotheses:

1. FSTEC is vastly under resourced and can only focus on key technologies for Russian users and key vulnerabilities of these technologies.

2. FSTEC is a military organization and is publishing "just enough" content to be credible as a national vulnerability database. The Russian government needs vulnerability research as a baseline for FSTEC's other technical control responsibilities, such as requiring reviews of foreign software.
3. FSTEC has a dual offensive and information security mission and publishes based on the competing needs. This would be similar to how China's NVD (CNNVD) functions.

In prior research, we disclosed that the NIST Information Technology Laboratory (ITL) employs about 400 scientific and technological staff and possesses a budget of roughly $120 million annually. The ITL is comprised of seven divisions and runs numerous databases and systems, including the U.S. NVD. In comparison, Russia's FSTEC has 1,111 employees, not including security, protection, or maintenance personnel, and a roughly comparable (if not slightly larger) bureaucratic structure and mission scope. While NIST ITL and FSTEC are not analogous organizations, this loose comparison does demonstrate that FSTEC is not vastly under resourced for its mission and that reporting only 10 percent of published vulnerabilities is a function of choice and not due to resource constraints.

Further, FSTEC does not even provide adequate coverage of the technology it focuses on most. As shown in our example above, FSTEC has published about half of all Adobe vulnerabilities; however, it is still missing over 1,000 Adobe vulnerabilities with a CVSS of "critical" or "high." If Adobe truly were that important to it, then FSTEC would not omit the publication of these vulnerabilities with the highest possible severity scores. This leads to the conclusion that FSTEC does not determine the need for publication simply by focusing on several key technologies. This also rules out hypothesis number one, that FSTEC is hugely under resourced and does not have the personnel or capital to keep up with NVD.

Second, we find no evidence to support hypothesis number three, that FSTEC is following CNNVD's model in trying to balance public disclosure and offensive cyber missions. FSTEC is not a public service organization — its database is not comprehensive or timely and does not publish enough vulnerabilities to support a broadly protective mission. FSTEC's mission, instead, is very focused and specific: to protect Russian state and critical infrastructure systems and support counterintelligence efforts.

Additionally, FSTEC over reports on vulnerabilities that have been exploited by Russian state-sponsored threat groups, while CNNVD delays or hides the publication of vulnerabilities that have been utilized by Chinese intelligence. If anything, FSTEC might be a little too focused in its support of Russian state information systems, as the few vulnerabilities it does publish yield insight into Russian government priorities and software.

Finally, we assess with high confidence that hypothesis number two accurately describes

the mission and intent of Russia's NVD. This intent is that FSTEC's vulnerability database provides a baseline for state information systems and legitimate cover for foreign technology reviews. According to February 2017 amendments to FSTEC documentation regarding inspection and requirements for state information systems, vulnerabilities in the BDU database are intended to provide a baseline of security — not a comprehensive vulnerability listing — for state information systems. This is further demonstrated by the surge in vulnerability publication during 2015, which was an experimental year for the database's future functionality and led to subsequent publication declines. Our research and data indicate that the BDU database is not intended to be comprehensive, but is simply a baseline for government information systems security and software inspections.

It is also possible that given the functional, managerial, and informal overlaps between FSTEC and the FSB, some of the BDU database's focus on the exact technologies Russian APT groups are known to favor could be derivative of FSB knowledge about its own operations and the exploitability of these technologies. There is minimal evidence to support this theory, aside from the overlap between the vulnerabilities that FSTEC over covers and those most used by Russian APT groups.

To this end, the vulnerabilities that FSTEC does publish convey more information about the hardware and software Russian government organizations use on their networks than which vulnerabilities they will target in offensive cyber operations.