# Sanctioned Firm Accused of Helping Russian Intelligence Was Part of Microsoft’s Early Vuln Access Program — MAPP

zetter.substack.com/p/sanctioned-firm-accused-of-helping

Kim Zetter

Share this post

Sanctioned Firm Accused of Helping Russian Intelligence Was Part of Microsoft’s Early Vuln Access Program — MAPP

zetter.substack.com

### A little-seen report issued last month by the Atlantic Council described in detail what a source confirms was the company’s alleged activities on behalf of the Russian government.

Kim Zetter
Apr 16, 2021

13

Share this post

Sanctioned Firm Accused of Helping Russian Intelligence Was Part of Microsoft’s Early Vuln Access Program — MAPP

zetter.substack.com

(Jordan Harrison/Unsplash)

A Moscow-based firm that the U.S. Treasury Department put on a sanctions list on Thursday for helping Russian intelligence agencies engage in offensive hacking operations, has long been a partner in a controversial Microsoft program that gives private security vendors advance access to information about vulnerabilities in Microsoft products.

The company, Positive Technologies, is part of the Microsoft Active Protections Program (MAPP), which includes nearly 100 software companies who receive advance information about software vulnerabilities that Microsoft is working to patch — before the information and patches are released to the general public. This information can include what's known as proof-of-concept code that demonstrates how the vulnerability can be exploited to hack systems. A leak of this critically sensitive information significantly shortens the time an adversary would need to develop their own exploit for the vulnerability.

Microsoft told the Associated Press, which first reported the link to MAPP, that it would be removing Positive Technologies from the program.

MAPP recently came under scrutiny after hackers linked to China began exploiting vulnerabilities in Microsoft Exchange servers before Microsoft went public with patches. Microsoft has reportedly been investigating whether a partner in MAPP may have leaked information Microsoft provided, inadvertently or intentionally, to actors who used it to exploit Exchange servers.

“Some of the tools used in the second wave of the attack [against Microsoft Exchange servers] … believed to have begun on Feb. 28, bear similarities to ‘proof of concept’ attack code that Microsoft distributed to antivirus companies and other security partners on Feb. 23,” the *Wall Street Journal* reported last month. Microsoft didn’t release a public patch to fix the vulnerabilities until March 2.

Microsoft has never confirmed the results of its investigation into a leak, nor has anyone suggested that Positive Technologies abused its privileged position in MAPP. But the government’s allegations that Positive Technologies assisted Russian intelligence agencies with their offensive hacking operations will likely draw more public criticism and scrutiny of MAPP.

Positive Technologies, in a statement posted to its web site on Friday, called the allegations behind the sanctions groundless.

“As a company, we deny the groundless accusations made by the U.S. Department of the Treasury,” the company wrote. “In the almost 20 years we have been operating there has been no evidence of the results of Positive Technologies’ research being used in violation of the principles of business transparency and the ethical exchange of information with professional information security community.”

The Treasury Department sanctioned six companies on Thursday for assisting Russian government hacking operations in various ways, including providing expertise and developing malicious hacking tools. Some of those firms allegedly have ties to the recent SolarWinds hacking campaign that hit U.S. government agencies and private companies, but the government didn’t identify which companies played a role in that operation.

Of the six, Positive Technologies, which says it earned $73 million last year, stands out for its respected role in the international security community. In addition to its partnership with Microsoft, it also lists HP and VMware as technology partners. [Notably, the government disclosed on Thursday that the Russian foreign intelligence service SVR, which was behind the recent SolarWinds campaign, was also exploiting a zero-day vulnerability in VMWare.]

The government sanctions announcement doesn’t provide a lot of details to back its claims about cooperation between Positive Technologies and Russian intelligence hackers. But a report published coincidentally by the Atlantic Council last month appears to offer a lot more detail about the activity behind these allegations.

The report doesn’t mention Positive Technologies at all. Instead it describes an unnamed Russian cybersecurity firm that has for years played a decisive role in Russian government hacking operations. The lengthy report only discusses the company on a few pages and uses a cryptonym or code name to refer to it: ENFER.

> **The source wouldn't say outright that ENFER and Positive Technologies are the same, but when asked if it would be incorrect to write that they are the same, the source said it would not be incorrect.**

But the concealment effort isn't very robust and almost immediately after the report came out, cybersecurity expert Ryan Naraine spotted language in it that was almost identical to language in a document on Positive Technologies' web site outlining the company's history.

The Atlantic report says that Russia's Ministry of Defense became one of ENFER's first clients within two years after the company was founded. It also says that over the past decade the company has strengthened its cooperation with Russian security services.

Positive Technologies states in its history document that the Russian Ministry of Defense became one of its first clients in 2004, two years after the company was founded. And in 2011, it began a cooperative relationship "with Russian law enforcement and security agencies."

Naraine made a cryptic reference to this finding on March 5 in a newsletter he publishes called Security Conversations. All he wrote was that the Atlantic report's description of ENFER was "particularly interesting." But he told Zero Day he was referring to the matching language in the Atlantic report and the Positive Technologies document.

> **Most notably, the report says that ENFER reverse-engineers malicious code captured in the wild — particularly malware found infecting Russian government networks — and then redevelops it as new malware to be used by the Russian government and others.**

A story published on Thursday by *MIT Technology Review* reporter, Patrick Howell O'Neill, further bolsters the connection between ENFER and Positive Technologies.

In the article, which is about the Treasury Department sanctions against Positive Technologies, O'Neill reveals what he describes as "previously unreported US intelligence assessments" about Positive Technologies that sources provided him. He reveals that the company "is a major provider of offensive hacking tools, knowledge, and even operations to Russian spies." As an example of this, he notes that the company specifically developed exploits for the SS7 telecommunications protocol.

The SS7 protocol is used by telecommunications networks to route calls and text messages to users wherever they are. The security world has long known about vulnerabilities in SS7 that can allow malicious actors to trick telecom networks into sending phone calls and text messages through a system they control so they can intercept the communication. And O'Neill reports that although the company once gave a public demonstration to Forbes about the weaknesses in SS7 for purposes of warning users, privately the company "developed offensive hacking capabilities to exploit [these SS7 flaws] that were then used by Russian intelligence in cyber campaigns."

The Atlantic Council report describes the same about ENFER, but with much greater detail, noting that the company gained some of its knowledge while performing security defensive services for a prominent Russian telecommunication client. It then developed techniques to exploit SS7, which were used in the networks of other telecoms who were ENFER customers, as well as in networks in the Middle East — all “on behalf of other state services.” This appears to imply that SS7 hacking services were provided to the state services of Middle East nations. This included techniques for geolocating phone users, intercepting their communications and infecting older-generation Android phones with malware.

How does this connect ENFER to the story that O’Neill wrote about Positive Technologies? O’Neill is a co-author on the Atlantic Council report, though he doesn’t mention the report in his *MIT Technology Review* story. Asked if ENFER is Positive Technologies, O’Neill replied to Zero Day that the terms of his agreement with the Atlantic Council prevent him from discussing the report.

A source with knowledge about how the Atlantic Council report was created says O’Neill was brought in as a volunteer to help write up the research conducted by his co-authors. The source wouldn’t say outright that ENFER and Positive Technologies are the same, but when asked if it would be incorrect to write that they are the same, the source indicated that it would not be incorrect.

Based on this, the report would appear to provide a lot more information that may have served as the basis for the Treasury Department sanctions against Positive Technologies.

## Well-Connected Security Player

Positive Technologies was founded in 2002 with just six employees and a security scanning tool called XSpider, according to the document on its web site that outlines its history. By 2003, the tool had 300,000 downloads, and in 2004, Russia’s Ministry of Defense became one of the company’s first major clients, along with a Russian bank and steel and ironworks firm.

In 2008 the company created a pen-testing team to find vulnerabilities in customer networks by trying to hack them, and the next year launched a research center to uncover vulnerabilities in software products and report them to vendors for fixing.

In 2011, it began “cooperation” with Russian law enforcement “and security agencies.” It doesn’t state what that cooperation entailed but that same year it launched an annual conference called Positive Hack Days, and its staff jumped from 90 employees to 199. The next year, it had 331 employees and 1,000 corporate clients and opened offices in Italy, South Korea, Tunisia, U.S., and St. Petersburg, according to the history outline. But the Associated Press reports that although the company has claimed in news releases to have an office in Framingham, Massachusetts, it’s not listed in city or state records under that name.

In 2012, the company partnered with Siemens to secure its Simatic WinCC industrial control system and also became a partner in VMware's Technology Alliance Program. That same year the National Election Commission of South Korea began using one of its security products.

[The Siemens Simatic WinCC software is famous for having been targeted by the U.S. and Israel in their 2007-2010 Stuxnet attack against centrifuges at Iran's Natanz enrichment plant.]

Positive Technologies claims to have more than 1,100 employees and more than 2,000 customers across 30 countries, including ING and Societe Generale — two banking powerhouses in Europe — as well as Samsung, the British telecommunications giant BT, and SK Telecom of South Korea. The company makes a number of security products that are widely used and plays a prominent role in the computer security community by finding critical vulnerabilities in software and hardware and disclosing them to vendors for fixing. In 2018, it says it published data on 46 security flaws, "including 30 high-risk vulnerabilities discovered in products from Cisco, Hirschmann, SAP, Schneider Electric, Siemens, and other companies."

> **The company boasts that it "has earned the gratitude of such world names as Google, Adobe, Apple, Red Hat, and Siemens."**

The company boasts that it "has earned the gratitude of such world names as Google, Adobe, Apple, Red Hat, and Siemens."

Last year, its researchers discovered and disclosed a major unfixable flaw in Intel chips that could undermine the chips' built-in encryption and other security features.

"This vulnerability jeopardizes everything Intel has done to build the root of trust and lay a solid security foundation on the company's platforms," Mark Ermolov, a security researcher with Positive Technologies wrote in a blog post.

Riding on these successes, the company has recently been contemplating an initial public offering, according to a Russian newspaper.

## Leading a Double Life

But according to the U.S. government, Positive Technologies has for years been leading a double life, secretly helping Russian intelligence agencies hack targets in the U.S. and elsewhere, providing expertise and developing tools and infrastructure. Positive Technologies also allegedly uses an annual security conference it hosts in Russia to recruit skilled hackers on behalf of Russia's Federal Security Service (FSB), Russia's Main Intelligence Directorate (GRU) and its Foreign Intelligence Service (SVR).

The Treasury Department didn’t identify the conference by name, but it appears to be Positive Hack Days (PHDays), which drew 8,000 attendees in 2019. This year’s event will be held in Moscow May 20-21.

A 2018 story in the *Daily Beast* called the conference “ground zero for Russia’s cyber spies.” Reporter Kevin Poulsen found among the conference’s online lists of past attendees the names of two GRU officers who have been charged in the U.S. with breaching the Democratic National Committee in 2016. The names of other attendees match Russian hackers who have been indicted for interfering in the 2016 presidential election in other ways.

It should be noted, though, that the conference isn’t much different than the annual DefCon hacker conference, held in Las Vegas, where researchers and hackers demonstrate hacks against critical infrastructure, banks, cars, and voting machines. U.S. and foreign intelligence agencies regularly attend DefCon to recruit skilled hackers and researchers.

To understand more the possible reasons behind the sanctions against Positive Technologies, we have to again turn to the Atlantic report about ENFER.

According to the report, ENFER, maintains a public and a secret face — publicly offering code-auditing services, penetration testing, vulnerability research and threat intelligence services to corporate and government clients, while providing weaponized exploits to the Russian spy agencies. The work is done “in response to direct tasking by officers of the FSB on specific projects involving offensive activities,” the report states. This includes “exploit discovery and weaponization, malware development, and infrastructure engineering” as well as the development of offensive tools for conducting system and network reconnaissance and exfiltrating documents.

Although ENFER, like Positive Technologies, is publicly considered a good corporate citizen by using the software vulnerabilities it finds only for penetration testing and other defensive security activities, the company gave the same capabilities to Russian government clients, the report alleges. The pen-testing ENFER does to test customer networks and the vulnerabilities it discloses to vendors to be patched are merely ways to provide “a veneer of legitimacy” and plausible deniability about the other work it does for the Russian government, the report alleges.

Most notably, the report says that ENFER reverse-engineers malicious code captured in the wild — particularly malware found infecting Russian government networks — and then redevelops it as new malware to be used by the Russian government and others.

> **The work is done “in response to direct tasking by officers of the FSB on specific projects involving offensive activities,” the report states.**

In at least one case, this allegedly involved a malware family that was found and which “Russian researchers” attributed to a hacking campaign conducted by a member of the Five Eyes spy alliance that got detected “between 2014 and 2015.” Evidently a zero-day exploit used by this actor was discovered and then allegedly “repurposed by ENFER for use in other intrusions.”

This appears to be referencing the U.S., which is a member of the Five Eyes spy alliance that includes the UK, Australia, New Zealand and Canada. The malware family likely refers to a suite of NSA hacking tools dubbed the Equation Group that the Moscow-based antivirus firm Kaspersky Lab says it discovered in 2014 and then publicly exposed in 2015. Kaspersky has said the first Equation Group component it discovered was found on a system in the Middle East that was also infected with several other families of malware from various nation-state actors.

The zero-day exploit that ENFER reverse-engineered for use in other intrusions sounds like Eternal Blue, an Equation Group tool that wasn’t discovered by Kaspersky, but was released publicly in August 2016 by a mysterious hacking group known as the Shadow Brokers who are believed to be from one of the Russian intelligence agencies. The repurposing of this exploit may refer to two incidents in which Eternal Blue was re-used in hacking operations. On May 12, 2017, it was used to spread the WannaCry ransomware worm to computers around the world. The next month it was also used to spread the NotPetya attack around the world, beginning with computers in Ukraine. The NotPetya worm has been attributed to Russia; WannaCry has been attributed to North Korea.

But ENFER didn’t just hand off tools to government hackers. The Atlantic report alleges that it was “directly involved” in command and control of operations — meaning it managed servers and tools used to communicate and send commands to malware planted on hijacked machines.

“The extent to which ENFER staff have been involved in the planning and management of operations remains unclear,” the report notes. It’s also possible that some of the activity ENFER conducted was done at the direction of a state but was essentially ENFER employees engaging in cybercriminal hacking for their own purposes or for other non-state partners.

It’s also not clear how much of ENFER’s activity is voluntary. The report notes that FSB oversight of ENFER includes “threats against individual staffers’ families” to keep them motivated to cooperate with the FSB.

[Author note: this story has been updated to identify where Kaspersky discovered the first Equation Group tool and to clarify that O’Neill worked on the report as an unpaid volunteer.]

Share

Comment

Share

Share this post

Sanctioned Firm Accused of Helping Russian Intelligence Was Part of Microsoft’s Early Vuln Access Program — MAPP

zetter.substack.com