Russian hackers hunt hi-tech secrets, exploiting US weakness

February 7 2018, by Jeff Donn, Desmond Butler And Raphael Satter

This combination of photos shows an Air Force F-22 Raptor stealth fighter jet, left, an MQ-9 Reaper/"Predator B" drone, right, and an X-37B unmanned spacecraft, bottom. Data supplied by the cybersecurity firm Secureworks shows Fancy Bear's hacking targets included defense contractor employees at Lockheed Martin, General Atomics, and Boeing, involved in the development of these systems. (AP Photo/Steve Helber, Heather Ainsworth, U.S. Air Force via AP)

Russian cyberspies pursuing the secrets of military drones and other

sensitive U.S. defense technology tricked key contract workers into exposing their email to theft, an Associated Press investigation has found.

What ultimately may have been stolen is uncertain, but the hackers clearly exploited a national vulnerability in cybersecurity: poorly protected email and barely any direct notification to victims.

The hackers known as Fancy Bear, who also intruded in the U.S. election, went after at least 87 people working on militarized drones, missiles, rockets, stealth fighter jets, cloud-computing platforms or other sensitive activities, the AP found.

Employees at both small companies and defense giants like Lockheed Martin Corp., Raytheon Co., Boeing Co., Airbus Group and General Atomics were targeted by the hackers. A handful of people in Fancy Bear's sights also worked for trade groups, contractors in U.S.-allied countries or on corporate boards.

"The programs that they appear to target and the people who work on those programs are some of the most forward-leaning, advanced technologies," said Charles Sowell, a former senior adviser to the U.S. Office of the Director of National Intelligence, who reviewed the list of names for the AP. "And if those programs are compromised in any way, then our competitive advantage and our defense is compromised."

"That's what's really scary," added Sowell, who was one of the hacking targets.

The AP identified the defense and security targets from about 19,000 lines of email phishing data created by hackers and collected by the U.S.-based cybersecurity company Secureworks, which calls the hackers Iron Twilight. The data is partial and extends only from March 2015 to

May 2016. Of 87 scientists, engineers, managers and others, 31 agreed to be interviewed by the AP.

Most of the targets' work was classified. Yet as many as 40 percent of them clicked on the hackers' phishing links, the AP analysis indicates. That was the first step in potentially opening their personal email accounts or computer files to data theft by the digital spies.

Keven Gambold, CEO of Unmanned Experts, demonstrates how to fly a drone at the Searchlight airport in Searchlight, Nev., on Wednesday, Jan. 17, 2018. Gambold, a hacking target, said the Russians might be counting on espionage to catch up with the Americans. "This would allow them to leapfrog years of hard-won experience," he said. (AP Photo/Isaac Brekken)

James Poss, who ran a partnership doing drone research for the Federal Aviation Administration, was about to catch a taxi to the 2015 Paris Air

Show when what appeared to be a Google security alert materialized in his inbox. Distracted, he moved his cursor to the blue prompt on his laptop.

"I clicked on it and instantly knew that I had been had," the retired Air Force major general said. Poss says he realized his mistake before entering his credentials, which would have exposed his email to the hackers.

Hackers predominantly targeted personal Gmail, with a few corporate accounts mixed in.

Personal accounts can convey snippets of classified information, whether through carelessness or expediency. They also can lead to other more valuable targets or carry embarrassing personal details that can be used for blackmail or to recruit spies.

Drone consultant Keven Gambold, a hacking target himself, said the espionage could help Russia catch up with the Americans. "This would allow them to leapfrog years of hard-won experience," he said.

He said his own company is so worried about hacking that "we've almost gone back in time to use stand-alone systems if we're processing client proprietary data—we're FedEx'ing hard drives around."

The AP has previously reported on Fancy Bear's attempts to break into the Gmail accounts of Hillary Clinton's presidential campaign, American national security officials, journalists, and Kremlin critics and adversaries around the world. U.S. intelligence agencies have concluded the hackers worked for the Kremlin and stole U.S. campaign email to tilt the 2016 election toward Donald Trump—all of which Russian leader Vladimir Putin has denied.

But the hackers clearly had broader aims. Fifteen of the targets identified by the AP worked on drones—the single largest group of weapons specialists.

Jessica Balik, left, and Keven Gambold, right, CEO of Unmanned Experts, prepare a drone for a demonstration at the Searchlight airport in Searchlight, Nev., on Wednesday, Jan. 17, 2018. Gambold, a hacking target, said his own company is so worried about hacking that "we've almost gone back in time to use stand-alone systems if we're processing client proprietary data—we're FedEx'ing hard drives around." (AP Photo/Isaac Brekken)

Countries like Russia are racing to make better drones as the remote-control aircraft have moved to the forefront of modern warfare. They can fire missiles, hunt down adversaries, or secretly monitor targets for days—all while keeping human pilots safely behind computer controls.

The U.S. Air Force now needs more pilots for drones than for any other single type of aircraft, a training official said last year. Drones will lead growth in the aerospace industry over the next decade, with military uses driving the boom, the Teal Group predicted in November. Production was expected to balloon from $4.2 billion to $10.3 billion.

So far, though, Russia has nothing that compares with the new-generation U.S. Reaper, which has been called "the most feared" U.S. drone. General Atomics' 5,000-pound mega-drone can fly more than 1,000 miles (1,600 kilometers) to deliver Hellfire missiles and smart bombs. It has seen action in Afghanistan, Iraq and Syria.

The hackers went after General Atomics, targeting a drone sensor specialist. He did not respond to requests for comment.

They also made a run at the Gmail account of Michael Buet, an electronics engineer who has worked on ultra-durable batteries and high-altitude drones for SunCondor, a small South Carolina company owned by Star Technology and Research. Such machines could be a useful surveillance tool for a country like Russia, with its global military engagements and vast domestic border frontier.

"This bird is quite unique," said Buet. "It can fly at 62,000 feet (18,600 meters) and doesn't land for five years."

The Russians also appeared eager to catch up in space, once an arena for Cold War competition in the race for the moon. They seemed to be carefully eyeing the X-37B, an American unmanned space plane that looks like a miniature shuttle but is shrouded in secrecy.

In a reference to an X-37B flight in May 2015, Russian Deputy Prime Minister Dmitry Rogozin invoked the vehicle as evidence that his country's space program was faltering. "The United States is pushing

ahead," he warned Russian lawmakers.

Retired Air Force Maj. Gen. James Poss, speaks about a hacking attempt on him, and the danger of such attacks in general, in his home office in Ocean Springs, Miss., on Jan. 17, 2018. An expert with three decades of experience in the military, Poss now consults on drones and intelligence. (AP Photo/Rogelio V. Solis)

Less than two weeks later, Fancy Bear tried to penetrate the Gmail account of a senior engineer on the X-37B project at Boeing.

Fancy Bear has also tried to hack into the emails of several members of the Arlington, Virginia-based Aerospace Industries Association, including its president, former Army Secretary Eric Fanning. It went after Lt. Gen. Mark Shackelford, who has served in the military and aerospace industry as a corporate board member. He has been involved

with major weapons and space programs like SpaceX, the reusable orbital rocket company founded by billionaire tech entrepreneur Elon Musk.

Along another path, the hackers chased people who work on cloud-based services, the off-site computer networks that enable collaborators to easily access and juggle data.

In 2013, the CIA signed a $600 million deal with web giant Amazon to build a system to share secure data across the U.S. intelligence community. Other spy services followed, and the government cleared them last year to move classified data to the cloud at the "secret" level—a step below the nation's most sensitive information.

Fancy Bear's target list suggests the Russians have noticed these developments.

The hackers tried to get into the Gmail accounts of a cloud compliance officer at Palantir and a manager of cloud platform operations at SAP National Security Services, two companies that do extensive government work. Another target was at Mellanox Federal Systems, which helps the government with high-speed storage networks, data analysis and cloud computing. Its clients include the FBI and other intelligence agencies.

Yet of the 31 targets reached by the AP, just one got any warning from U.S. officials.

"They said we have a Fancy Bear issue we need to talk about," said security consultant Bill Davidson. He said an Air Force cybersecurity investigator inspected his computer shortly after the 2015 phishing attempt but found no sign that it succeeded. He believes he was contacted because his name was recognized at the Air Force Office of Special Investigations, where he used to work.

Retired Air Force Maj. Gen. James Poss, speaks in his home office in Ocean Springs, Miss., on Jan. 17, 2018. Poss, whose Gmail was nearly compromised in a phishing attempt, said that military spying is now far easier than when somebody needed to carry blueprints or photographs out of office buildings. "You'd need maybe 2,000 spies to do in the real world what a small group of cyberspies can do," he says. (AP Photo/Rogelio V. Solis)

The FBI declined to give on-the-record details of its response to this Russian operation. Agency spokeswoman Jillian Stickels said the FBI does sometimes notify individual targets. "The FBI takes ... all potential threats to public and private sector systems very seriously," she said in an email.

However, three people familiar with the matter—including a current and a former government official—previously told the AP that the FBI knew

the details of Fancy Bear's phishing campaign for more than a year.

Pressed about notification in that case, a senior FBI official, who was not authorized to publicly discuss the hacking operation because of its sensitivity, said the bureau was overwhelmed by the sheer number of attempted hacks. "It's a matter of triaging to the best of our ability the volume of the targets who are out there," he said.

A Pentagon spokeswoman, Heather Babb, said she could release no details about any Defense Department response, citing "operational security reasons." But she said the department recognizes the evolving cyber threat and continues to update training and technology. "This extends to all of our workforce—military, civilian and contractor," she added.

The Defense Security Service, which protects classified U.S. technology and trains industry in computer security, focuses on safeguarding corporate computer networks. "We simply have no insight into or oversight of anyone's personal email accounts or how they are protected or notified when something is amiss," spokeswoman Cynthia McGovern said in an email.

Contacted by the AP, Lockheed Martin, Raytheon, Boeing, Airbus and General Atomics did not respond to requests for comment.

Jerome Pearson, a space system and drone developer, acknowledged that he has not focused on security training at his company, Star Technology, where Buet has consulted. "No, we really haven't done that," he said with a nervous laugh. "We may be a little bit remiss in that area." He said they may do training for future contracts.

Cybersecurity experts say it's no surprise that spies go after less secure personal email as an opening to more protected systems. "For a good

operator, it's like hammering a wedge," said Richard Ford, chief scientist at the Forcepoint cybersecurity company. "Private email is the soft target."

In this Monday, Jan. 11, 2016 file photo, Russian Deputy Prime Minister Dmitry Rogozin holds a model of an S-300 surface-to-air missile system at a news conference in Belgrade, Serbia. In May 2015, Rogozin invoked the X-37B unmanned space plane as evidence that his country's space program was faltering. "The United States is pushing ahead," he warned Russian lawmakers. Less than two weeks later, the hacking group Fancy Bear tried to penetrate the Gmail account of a senior engineer on the X-37B project at Boeing. (Marina Lopicic/Kurir via AP)

Some officials were particularly upset by the failure to notify employees of cloud computing companies that handle data for intelligence agencies. The cloud is a "huge target for foreign intelligence services in

general—they love to get into that shared environment," said Sowell, the former adviser to the Office of the Director of National Intelligence.

"At some point, wouldn't someone who's responsible for the defense contractor base be aware of this and try to reach out?" he asked.

Even successful hacks might not translate into new weapons for Russia, where the economy is weighed down by corruption and international sanctions.

However, experts say Russia, while still behind the U.S., has been making more advanced drones in recent years. Russian officials have recently been bragging as their increasingly sophisticated drones are spotted over war zones in Ukraine and Syria.

At a 2017 air show outside Moscow, plans were announced for a new generation of Russian combat drones.

Rogozin, the deputy prime minister, boasted that the technological gap between Russia and the United States "has been sharply reduced and will be completely eliminated in the near future."