The Washington Post

National Security

Powerful NSA hacking tools have been revealed online

By Ellen Nakashima August 16 at 6:52 PM

Some of the most powerful espionage tools created by the National Security Agency's elite group of hackers have been revealed in recent days, a development that could pose severe consequences for the spy agency's operations and the security of government and corporate computers.

A cache of hacking tools with code names such as Epicbanana, Buzzdirection and Egregiousblunder appeared mysteriously online over the weekend, setting the security world abuzz with speculation over whether the material was legitimate.

The file appeared to be real, according to former NSA personnel who worked in the agency's hacking division, known as Tailored Access Operations (TAO).

"Without a doubt, they're the keys to the kingdom," said one former TAO employee, who spoke on the condition of anonymity to discuss sensitive internal operations. "The stuff you're talking about would undermine the security of a lot of major government and corporate networks both here and abroad."

Said a second former TAO hacker who saw the file: "From what I saw, there was no doubt in my mind that it was legitimate."

The file contained 300 megabytes of information, including several "exploits," or tools for taking control of firewalls in order to control a network, and a number of implants that might, for instance, exfiltrate or modify information.

The exploits are not run-of-the-mill tools to target everyday individuals. They are expensive software used to take over firewalls, such as Cisco and Fortinet, that are used "in the largest and most critical commercial, educational and government agencies around the world," said Blake Darche, another former TAO operator and now head of security research at Area 1 Security.

The software apparently dates back to 2013 and appears to have been taken then, experts said, citing file creation dates, among other things.

"What's clear is that these are highly sophisticated and authentic hacking tools," said Oren Falkowitz, chief executive of Area 1 Security and another former TAO employee.

Several of the exploits were pieces of computer code that took advantage of "zero-day" or previously unknown flaws or vulnerabilities in firewalls, which appear to be unfixed to this day, said one of the former hackers.

The disclosure of the file means that at least one other party — possibly another country's spy agency — has had access to the same hacking tools used by the NSA and could deploy them against organizations that are using vulnerable routers and firewalls. It might also see what the NSA is targeting and spying on. And now that the tools are public, as long as the flaws remain unpatched, other hackers can take advantage of them, too.

The NSA did not respond to requests for comment.

"Faking this information would be monumentally difficult, there is just such a sheer volume of meaningful stuff," Nicholas Weaver, a computer security researcher at the University of California at Berkeley, said in an interview. "Much of this code should never leave the NSA."

The tools were posted by a group calling itself the Shadow Brokers using file-sharing sites such as BitTorrent and DropBox.

As is typical in such cases, the true identity of whoever put the tools online remains hidden. Attached to the cache was an "auction" note that purported to be selling a second set of tools to the highest bidder: "!!! Attention government sponsors of cyber warfare and those who profit from it !!!! How much you pay for enemies cyber weapons?"

The group also said that if the auction raised 1 million bitcoins — equivalent to roughly $500 million — it would release the second file to the world.

The auction "is a joke," Weaver said. "It's designed to distract. It's total nonsense." He said that "bitcoin is so traceable that a Doctor Evil scheme of laundering $1 million, let alone $500 million, is frankly lunacy."

One of the former TAO operators said he suspected that whoever found the tools doesn't have everything. "The stuff they have there is super-duper interesting, but it is by far not the most interesting stuff in the tool set," he said. "If you had the rest of it, you'd be leading off with that, because you'd be commanding a much higher rate."

TAO, a secretive unit that helped craft the digital weapon known as Stuxnet, has grown in the past decade or so from several hundred to more than 2,000 personnel at the NSA's Fort Meade, Md., headquarters. The group dates to the early 1990s. Its moniker, Tailored Access Organization, suggests a precision of technique that some officials have likened to brain surgery. Its name also reflects how coding whizzes create exquisite tools from scratch, in the same way a fine tailor takes a bolt of wool and fashions a bespoke suit — only the computer geeks more often work in jeans and T-shirts and "have epic Nerf gun fights," as one former hacker said.

Some former agency employees suspect that the leak was the result of a mistake by an NSA operator, rather than a successful hack by a foreign government of the agency's infrastructure.

When NSA personnel hack foreign computers, they don't move directly from their own covert systems to the targets', fearing that the attack would be too easy to trace. They use a form of proxy server called a "redirector" that masks the hackers' origin. They use one or more such servers to make it difficult to trace a hack.

“NSA is often lurking undetected for years on the . . . [proxy hops] of state hackers,” former agency contractor Edward Snowden tweeted Tuesday. “This is how we follow their operations.”

At the same time, other spy services, like Russia’s, are doing the same thing to the United States.

It is not unprecedented for a TAO operator to accidentally upload a large file of tools to a redirector, one of the former employees said. “What’s unprecedented is to not realize you made a mistake,” he said. “You would recognize, ‘Oops, I uploaded that set’ and delete it.”

Critics of the NSA have suspected that the agency, when it discovers a software vulnerability, frequently does not disclose it, thereby putting at risk the cybersecurity of anyone using that product. The file disclosure shows why it’s important to tell software-makers when flaws are detected, rather than keeping them secret, one of the former agency employees said, because now the information is public, available for anyone to employ to hack widely used Internet infrastructure.

Snowden, Weaver and some of the former NSA hackers say they suspect Russian involvement in the release of the cache, though no one has offered hard evidence. They say the timing — in the wake of high-profile disclosures of Russian government hacking of the Democratic National Committee and the Democratic Congressional Campaign Committee — is notable.

The Russians are also suspected of involvement in the release of hacked DNC emails and of the private email addresses and personal cellphone numbers of Democratic lawmakers that were taken from DCCC computers. Those moves have caused great consternation among party officials and dread that more is to come.

Tweeted Snowden: “Circumstantial evidence and conventional wisdom indicates Russian responsibility.” He said that the disclosure “is likely a warning that someone can prove U.S. responsibility for any attacks that originated from this” redirector or malware server by linking it to the NSA.

“This could have significant foreign policy consequences,” he said in another tweet. “Particularly if any of those operations targeted U.S. allies” or their elections.

“Accordingly,” he tweeted, “this may be an effort to influence the calculus of decision-makers wondering how sharply to respond to the DNC hacks.”

In other words, he tweeted, it looks like “somebody sending a message” that retaliating against Russia for its hacks of the political organizations “could get messy fast.”

Ellen Nakashima is a national security reporter for The Washington Post. She focuses on issues relating to intelligence, technology and civil liberties. Follow @nakashimae

The Post Recommends

A Playboy Playmate found this normal woman’s naked body gross. So she posted it online.

Los Angeles police are investigating.

Paul Ryan just summed up Republicans’ Donald Trump problem in three lines

The news cycle belongs to the Republicans. They probably wish it didn't.

From Trump to Clinton to Russia: These political cartoons go for the Olympic gold

Nothing stokes the creative flame quite like juicing these election-year cartoons with Olympic themes. Here's the tale at the political tape.