Researchers Say They Uncovered Uzbekistan Hacking Operations Due to Spectacularly Bad OPSEC

By Kim Zetter

Published: 2019-10-03 · Archived: 2026-04-06 01:32:45 UTC

Nation-state spy agencies are only as good as their operational security—the care they take to keep their digital spy operations from being discovered. But occasionally a government threat actor appears on the scene that gets it all wrong.

This is the case with a threat actor recently discovered by Kaspersky Lab that it's calling SandCat—believed to be Uzbekistan's repressive and much-feared intelligence agency, the State Security Service (SSS).

The group's lax operational security includes using the name of a military group with ties to the SSS to register a domain used in its attack infrastructure; installing Kaspersky's antivirus software on machines it uses to write new malware, allowing Kaspersky to detect and grab malicious code still in development before it's deployed; and embedding a screenshot of one of its developer's machines in a test file, exposing a major attack platform as it was in development. The group's mistakes led Kaspersky to discover four zero-day exploits SandCat had purchased from third-party brokers to target victim machines, effectively rendering those exploits ineffective. And the mistakes not only allowed Kaspersky to track the Uzbek spy agency's activity but also the activity of other nation-state groups in Saudi Arabia and the United Arab Emirates who were using some of the same exploits SandCat was using.

"These guys [Uzbekistan's intelligence agency] have been around for quite a long time and up until now I'd never heard of Uzbekistan having a cyber capability," said Brian Bartholomew, a researcher with Kaspersky's Global Research and Analysis Team who will present his findings about SandCat today in London at the VirusBulletin conference. "So it was kind of a shocker to me to know that they … were buying all of [these exploits] and targeting all these people and yet no one has ever written about them."

The SSS, previously known as the National Security Service, isn't new to the spy game: It emerged in 1991 with the collapse of the Soviet Union to succeed the KGB as Uzbekistan's national intelligence agency and secret police, adopting some of the KGB's surveillance technologies as well as its oppressive tactics. Known for its torture and human rights abuses, the SSS was revamped in early 2018 by the country's new president, who sought to reform its repressive ways. But earlier this year the new head of the spy agency was booted after a year on the job, reportedly amid allegations that the agency had turned its spying capabilities against the new president and his family.

The agency's interest in offensive hacking operations were first exposed in 2015 when a hacker named Phineas Fisher hacked the Hacking Team, an Italian firm that sells hacking tools to governments and law enforcement agencies, and published thousands of emails exposing the company's correspondence with customers, including the SSS. According to the emails, which cover the years 2011-2015, the SSS spent nearly a million dollars on Hacking Team tools. But its hacking operations have gone largely unnoticed until recently.

In October 2018, researchers at Kaspersky stumbled across SandCat after discovering an already known piece of malware called Chainshot on a victim's machine in the Middle East. Chainshot had been used by two other nation-state threat actors in the Middle East in the past—groups security researchers have attributed to the UAE and Saudi Arabia—but the malware in this case was using infrastructure not associated with either of these countries, suggesting it was a different group Kaspersky hadn't seen before. SandCat was also using a zero-day exploit to install Chainshot.

As Kaspersky analyzed machines infected with the exploit and Chainshot, and began to dig into the group's infrastructure that was tied to the infections, it ultimately led Kaspersky to discover three more zero days used by the same group each of which got essentially burned as the vulnerabilities they attacked got patched

"I'd call [SandCat] my zero-day Pez dispenser," Bartholomew told Motherboard, "because it seemed like every time we'd [find] another zero-day and patch it, they'd come up with another one. [T]hey're burning through them like nothing, which tells me one thing—that they have tons of money."

The discoveries didn't seem to affect SandCat. But as each zero-day got burned for SandCat, it also got burned for Saudi Arabia and the UAE.

When spy agencies purchase zero-day exploits from brokers, they often have two options: pay a premium rate for an exclusive right to use an exploit, or pay less for exploits that other customers of the broker also get to use. The latter option comes with a risk, though—if any customer using a shared exploit is careless or reckless, this can result in the exploit being caught, effectively burning it for anyone else who paid to use it.

"All it takes is one sloppy customer," Bartholomew said. "One customer who is bad at OPSEC ruins it for all the others."

Kaspersky believes SandCat purchased its exploits from two Israeli companies known as the NSO Group and Candiru but provided Motherboard with no evidence to support this. NSO Group is known for developing and selling some of the most powerful exploits for hacking mobile phones, including malware that has been used to spy on journalists and dissidents. Candiru is more of a full-service agency that provides, in addition to attack tools for computers, a platform for managing attack operations. A spokeswoman for the NSO Group wouldn't say whether the company has ever sold exploits to the SSS but told Motherboard the company "does not develop or license any products for PC-related interception such as 'Chainshot.'" Motherboard was unable to reach Candiru. A different Israeli company is known to have supplied surveillance equipment to Uzbekistan, suggesting strong ties between the latter and the Israeli surveillance industry.

Initially Kaspersky didn't know who SandCat was, but it didn't take a lot of work to tie it to Uzbekistan's SSS.

Kaspersky discovered that SandCat's developers had installed Kaspersky antivirus on their development machines—presumably to test whether malware they were developing inhouse could bypass the detection tool. But they're using it with the telemetry reporting feature of the antivirus tool enabled, which causes the antivirus software to grab a copy of any files on the machines that it suspects are malicious and sends them back to Kaspersky for analysis.

"[T]hat's how we caught a lot of this stuff … every time they would test it, our [software] would pull the binaries back," Bartholomew said.

Furthermore, any time SSS's suppliers sent SandCat new exploits for use, they arrived on a thumb drive. When SandCat developers inserted the drive into their machines, the Kaspersky software would automatically scan it for malware and grab files it deemed malicious.

"I think we got one of those exploits before they even were able to use it," Bartholomew said.

Having identified the systems SandCat used for development and testing, they discovered that these machines used IP addresses that resolved to the "itt.uz" domain. When Bartholomew looked up the registration information for itt.uz, it showed a 2008 registration to an entity in Tashkent, Uzbekistan called "Military Unit 02616." Military Unit 02616 is cited in an Uzbekistan court case for doing forensics on electronic devices seized from the defendant by an investigative unit of the SSS.

"Can it be this easy?" Bartholomew said he wondered. "I really wrestled hard with that for a long time thinking there's no way it's this easy. But every piece of data that we have links back to the same thing."

SSS's email domain resolved to the IP address 84.54.69.202, and the systems SandCat uses for developing and testing its malware use a nearly identical address 84.54.69.203. SandCat uses these same machines to upload test files to Virus Total. Virus Total is a website that aggregates numerous anti-virus programs so that anyone can upload suspicious files to the site to see if it's malicious. Attackers also sometimes upload their new malware to the site to test if it can successfully bypass antivirus detection, but Virus Total records the IP address from which every file is uploaded, which means that malicious files SandCat uploaded to the site for such testing can be traced back to SandCat's machines.

"As a developer you don't upload to Virus Total, [but] if you do, don't do it from the same IP addresses that you're conducting your operations from," Bartholomew said

In October 2018, during the time SandCat's zero-days were starting to be discovered and burned, the group began developing its own attack platform called Sharpa. Bartholomew thinks whoever supplied SSS with its zero-days and platform until then got fed up with so many of the tools being burned quickly, forcing SandCat to develop inhouse.

It's also possible the change was simply due to a natural progression, however—many spy agencies start out using a platform and malware purchased from others before developing internal capabilities to build their own. Or the move might have been brought on by budgetary constraints after the new president announced in 2017 he planned to rein in the powers of the SSS, reduce the number of dissidents being monitored on government blacklists, and transfer some SSS responsibilities to other agencies.

But if SandCat's mistakes did cause its suppliers to fire it as a customer, the group didn't reform its bad habits in developing its new platform.

In the process of conducting some tests, one of SandCat's developers took a screenshot of his desktop with a detailed image of the Sharpa interface open on it, and put it in a test file that he ran on a machine with the Kaspersky software on it. He wanted to be able to load Sharpa onto victim machines using a malicious Word file and for some reason used the screenshot of his desktop as part of the Word file. When Kaspersky's software grabbed the malicious file, the researchers learned about the new platform in development as well as other intel. The screenshot, for example, shows developer notes written in Uzbek, confirming the language of the developers,

and also shows the interface used to track and control Sharpa once it's on infected machines. It also shows the IP addresses for SandCat's test machines.

"This was really important, because … we didn't know about [these] addresses [before this]. So we were able to go back in our telemetry and find more installations of more stuff because this IP address showed up in the screenshot," Bartholomew said.

Bartholomew refers to SandCat as "trash actors" because of their reckless mistakes. But he thinks their OPSEC failures can be attributed to arrogance and inexperience.

"A lot of the [nation-state threat actors] in that region have the same bravado. They just don't care [about being stealth]. They adamantly deny everything. And if they get caught they get caught," he said. But he notes that SandCat is still in the infant stage of development, even though it's been active in spying a long time, and is bound to make rookie mistakes.

In publicly exposing the group's mistakes now, it's likely that SandCat will improve its OPSEC. But Bartholomew says exposing them will also increase the number of researchers tracking them, which could help uncover more of their current victims and provide them with protection.
