The blurry boundaries between nation-state actors and the cybercrime underground

intel471.com/blog/the-blurry-boundaries-between-nation-state-actors-and-the-cybercrime-underground

When it comes to attributing malicious cyber activity, there are two buckets by which actors generally fall in: "financially-motivated" or "nation-state." The former is ultimately interested in money, while the latter is more concerned with obtaining or exploiting sensitive information to gain an advantage over a government or commercial entity. For the past decade, defenders could generally discern whether attackers fit into each of the previously mentioned buckets by examining tools, infrastructure, techniques and/or processes. Now, as cybercriminal work becomes increasingly lucrative due to the amount of money or information that could be acquired, the border between those buckets is eroding. The lines between nation-state objectives and financially-motivated cybercrime have continued to blur as the relationship between profit and espionage has grown, particularly within the cybercrime underground.

Whether nation-state threat actors were seen "moonlighting" in financially-motivated cybercrime or nation-states co-opted financially-motivated cybercriminals to do their bidding, Intel 471 has seen a slow and steady change in behavior where nation-states are incorporating the cybercrime underground to achieve their goals more than ever before.

An Opportunity Seized

One of the first instances of this behavior was formed in the heart of the cybercrime underground: Russia. In 2014, the ZeuS trojan was one the most prolific pieces of malware, described by security researchers as "smooth, effective and versatile" in its capabilities.

During that year, law enforcement discovered a variant of ZeuS, known as GameOver, being leveraged to obtain credentials belonging to Georgian intelligence officers or leaders of elite Turkish police units in order to access classified Ukrainian secrets, material linked to the Syrian conflict, and information on Russian arms dealing. Over the course of an investigation, it appeared that the malware's author, Yevgeniy Bogachev, was aware GameOver was being used as an intelligence tool, despite the fact that it was primarily used for financial crime. Upon reflection of the operations, it's likely that when Russian law enforcement had been monitoring Bogachev's actions (the malware had been in use since 2006) intelligence officers saw an opportunity to leverage GameOver for state objectives in exchange for looking the other way on ZeuS's role in financial crimes. There are indications that Russian security services were well aware of the significance of Bogachev and his ZeuS malware around the time of Operation Trident Breach in 2010.

In a similar turn of events, a prolific Iranian-linked actor who first surfaced in the cybercrime underground in 2016 eventually carried out various actions that were linked in Iranian state actions. Operating under the handle bc.monster (though tied to several different monikers), this actor was known for being sophisticated and highly experienced. The actor was likely behind several major data breaches, including the compromise of the Citrix Systems corporate network in late 2018.

Despite making money on the cybercrime underground, Intel 471 discovered that a lot of bc.monster's methods mimic those used by actors that have been linked to the Mabna Institute, an Iranian-based organization that has ties to the country's Islamic Revolutionary Guard Corps. While Intel 471 did not find any evidence that directly linked bc.monster to the Mabna Institute, we found a number of tactics, techniques and procedures (TTPs) that were common to the actor and the Mabna Institute. This included selling a Global Access List (GAL) from Exchange servers of various organisations, as well as the ability to perform password spraying attacks against multi-factor authentication (MFA) implemented accounts. Notably, the alleged dates of compromise mentioned by the actor, such as Visa (Jan. 2018), the National Bank of Canada (Feb. 2018), Saudi Aramco (Feb. 2018), were right before the publication of an FBI Flash Alert dated March 23, 2018 that detailed information on actors tied to the Mabna Institute.

Since bc.monster's work could be tied to both financial cybercrime and nation-state cyber operations, Intel 471 cannot rule out the possibility that the actor possibly worked for the Irainian government "by day" and engaged in financially motivated cybercrime after hours. However, despite the ties we've uncovered, that assessment remains uncorroborated at the time for this report.

Room For Growth

Over the past few years, the nation-states that are known to be aggressive actors have found ways to co-opt the cybercrime underground into their efforts. What was first looked at as serendipity is now considered standard operating procedure. Nation-states now often look to the know-how contained in the cybercrime underground as means to an end when it comes to their missions.

Iran

Bc.monster is only one example of Iran leaning on underground actors to carry out attacks. In early 2020, Intel 471 observed the actor hidehacker, a vendor of compromised access and data, specifically claiming to be based in Iran; working for the Iranian government as a member of the APT34 hacking group. Also known as Helix, Helix Kitten, or OilRig, APT34 likely worked on behalf of Iranian state interests and specialized in cyber-espionage. Evidence that Hidehacker is a government-worker-by-day, criminal-actor-by-night came when he stated in a form that the Iranian government did not provide a satisfactory income, so the actor was going to sell some of the information obtained during his government-linked work. Hidehacker also disclosed that most of the databases listed for sale were targets set by the Iranian government.

Additionally, Intel 471 also suspects that drumrlu, a vendor of compromised data and unauthorized access to high-profile organizations, has also done work on behalf of the Iranian government. In October 2020, we learned that drumrlu allegedly compromised and deployed ransomware against several companies. Our research into those attacks revealed that drumrlu's TTPs matched other open-source research into the TTPs of Iran-based state-sponsored group MuddyWater. While we cannot definitively say that drumrlu is associated with MuddyWater, we have determined that it is likely.

China

In July 2020, the U.S. Department of Justice released an indictment that alleged two Chinese residents hacked into the computer systems of hundreds of victim companies, governments, non-governmental organizations, and individual dissidents, clergy, and democratic and human rights activists all over the world, including Hong Kong and China. The release stated Li Xiaoyu (李啸宇) and Dong Jiazhi (董家志) conducted a hacking campaign where the two acted for their own personal financial gain in some instances, while also working at the direction of the Ministry of State Security (MSS) and other Chinese government agencies. Using a host of tools, techniques, and procedures — including the well-known "China Chopper" web shell program — The two stole information tied to technology designs, manufacturing processes, test mechanisms and results, source code, and chemical structures related to the pharmaceutical industry. After the indictment was announced, U.S. Assistant Attorney General John C. Demers declared that "China has now taken its place, alongside Russia, Iran and North Korea… providing a safe haven for cyber criminals in exchange for those criminals being 'on call' to work for the benefit of the state."

Russia

Of course the country with the biggest share of the cybercrime underground is going to find a way to leverage it for its government's objectives. Observers can examine the now-infamous SolarWinds hack to see the numerous ways Russian intelligence and the cybercrime underground have worked side-by-side.

Coming to light in December 2020, the SolarWinds incident will likely be used for decades as a prime example of the worst-case supply-chain-attack scenario. After months of speculation, on April 15, 2021, the U.S. government formally claimed the Russian Foreign Intelligence Service (SVR) was responsible for "the broad-scope cyber espionage campaign that exploited the SolarWinds Orion platform and other information technology infrastructures."

While only coming to light in 2020, actors on the cybercrime underground have been targeting SolarWinds for years prior to the discovered attack. Intel 471 observed an actor known as Fxmsp in October 2017 claim to have gained access to some SolarWinds-controlled assets. By November 2017, Fxmsp stated the access was no longer available because they were reserved for a "client." Additionally, Fxmsp reportedly had issues with the SolarWinds access, but claimed to be working to provide the client with what they were looking for. When pressed for more details on the issues, Fxmsp revealed the actor allegedly was working toward obtaining access to "the source codes and databases."

While there is no evidence of a connection between the 2017 actions and the SolarWinds hack, these two events show an overlap in targets of interest, as well as operational practices between sophisticated financially-motivated threat actors like Fxmsp and nation-state actors like Russia's SVR. On a deeper level, this exemplifies the level of access that a nation-state actor could obtain through the underground marketplace. Financially-motivated cybercriminals usually aim for the path of least resistance when it comes to making their personal profit. This usually means working with already established, "plug-and-chug" products and services like ransomware, rather than getting into the complicated matter of source code. Considering Fxmsp's mention of a private "client" who allegedly appeared to be interested in "source code," the possibility that state-actors like those within or related to Russia's SVR were the buyers of the SolarWinds access cannot be ruled out.

Another infamous, Russian-linked threat actor, Maksim Viktorovich Yakubets, was observed to be directly co-opted by Russia's Federal Security Service (FSB). Over time, Intel 471 tracked Yakubets, operating under the handle "Aqua," as the leader of the Russian hacking group Evil Corp, which was involved with the Dridex malware and botnet. Yakubets also purportedly supervised and managed the development, maintenance and distribution of, and cashout activity related to Dridex. In 2019, Intel 471 reported (alongside other open source reports) that Yakubets was actively collaborating with the FSB over a number of years. In April 2021, the U.S. government announced sanctions against the government of the Russian Federation, citing "aggressive and harmful activities." In a related press release from the U.S. Department of the Treasury, the U.S. claimed the FSB bolstered its cyber operations by co-opting criminal hackers, "including the previously designated Evil Corp." While Yakubets was not specifically named in the press release, it's likely that he was one of the many cybercriminals co-opted for Russian state objectives. As with Bogachev, there are strong indications that Russian security services were well aware of the significance of Yakubets and his operations around the time of Operation Trident Breach in 2010.

A Blurry Reality

The majority of actors on the cybercriminal underground are heavily motivated by profit. They come to the underground to make as much money as possible by illicit means. However, the notion that the underground is only an arena for financially-motivated cybercriminals is short-sighted. The instances discussed in this report, while far from definitive, show how the relationship between nation-states and the cybercriminal underground have grown as each side embraced the benefits of utilizing cybercrime to carry out their goals. As more countries lean on computer network exploitation as a means to their own geopolitical objectives, the outreach to the cybercriminal underground suggests that the buckets discussed in the beginning of the report may become one, murky mass where motives become increasingly difficult to decipher.