Use of Initial Access Brokers by Ransomware Groups

Use of Initial Access Brokers by Ransomware Groups

28.Jun.2021

Beatriz Pimenta and Lidia López, Blueliv labs, an Outpost24 company

Threat Intelligence

Initial Access Brokers (IABs) are financially motivated threat actors that profit through the sale of remote access to corporate networks in underground forums, like Exploit, XSS, or Raidforums. The type of accesses offered are mostly Remote Desktop Protocol (RDP), Virtual Private Network (VPN), web shells, and remote access software tools offered by companies such Citrix, Pulse Secure, Zoho, or VMware. However, threat actors are also selling information and tools to perform intrusions into companies through SQL injections, remote code execution (RCE) exploits, and other vulnerabilities.

Access brokers can either find vulnerable systems massively scanning networks for known vulnerabilities on remote systems, or purchase access to compromised accounts on stores like the infamous Genesis Market and then, resell them on underground forums. Since 2020, there has been a huge increase in the sale of network accesses likely driven by two factors: the situation of forced remote workforce caused by the COVID-19 pandemic, and the rise of ransomware attacks.

The rise of Ransomware-as-a-Service (RaaS) groups and trends like double-extorsion –threatening the company publishing confidential data – have made network accesses a key valuable asset. In fact, researchers detected that ransomware groups like Ragnarok, DoppelPaymer, Nefilim, Maze, and Sodinokibi have leveraged different vulnerabilities, for instance the Citrix Application Delivery Controller (ADC) vulnerability (CVE-2019-19781), to gain initial access to networks.

Furthermore, “darksupp”, the representative of the Darkside Group on underground forums, posted that was looking for partners who could give it access to U.S. businesses with annual revenue of at least $400 million. The DarkSide Group is known for constantly acquiring access to their targets’ network from prominent cybercriminal underground threat actors who act as initial access brokers. This article will focus on different active Initial Access Brokers (IABs) and their relationships with Ransomware Groups. This existent interaction shows how easy threat actors can purchase an initial access just looking at underground forums.

Sheriff and REvil gang

“Sheriff” is a threat actor quite active in the cybercriminal underground. The threat actor is an IAB who sells access to networks that they acquire using brute-forcing techniques and credential-stealing malware. Sheriff has a prolific relation with the REvil gang, selling access to victims' networks to the ransomware gang who then proceeds with ransomware attacks by encrypting and exfiltrating data. This relationship between the two threat actors dangerously amplifies the capabilities of the ransomware gang, while, at the same time, it also incentivizes the active search for vulnerabilities and other access modalities by Sheriff.

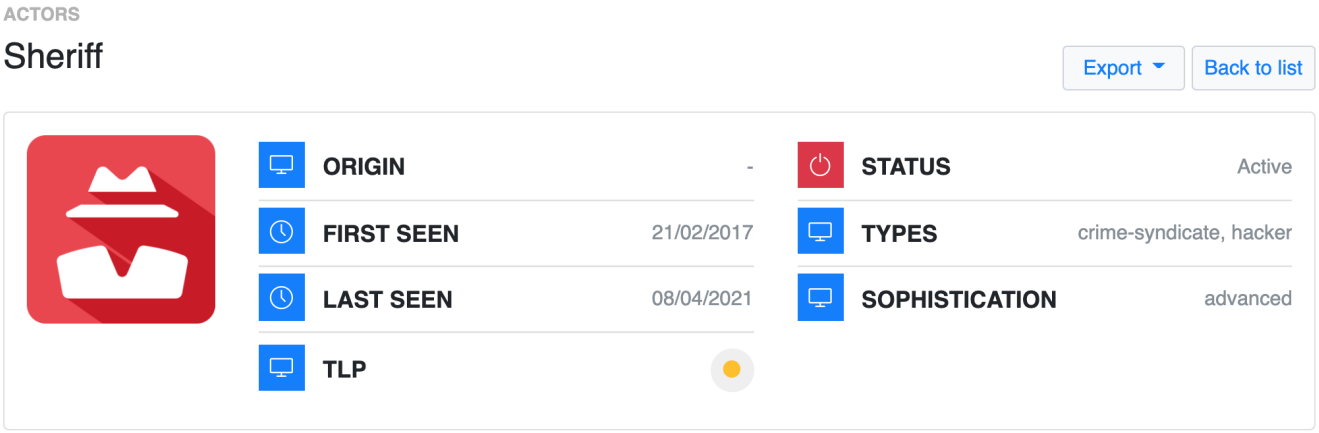

Image 1. “Sheriff” Threat Actor profile available in the Blueliv Threat Context module.

Mid-2020, Sheriff actively exploited Citrix vulnerabilities and acquired access to numerous high-profile entities. Sheriff’s targets include companies from a wide range of sectors in North America, Western Europe, and Australia; yet, U.S. financial institutions are by far their most preferred and recurrent target.

drumrlu/3lv4n and Thanos RaaS

"drumrlu" (aka 3lv4n) is an initial access broker and database seller active in underground forums since at least May 2020. drumrlu has sold domain access to organizations in Australia, the United States, Thailand, Pakistan, France, Italy, Switzerland, United Arab Emirates, Jordan, Egypt, Saudi Arabia across education, utility, insurance, healthcare, cryptocurrency, gaming, and government industries. On October 21, 2020, the threat actor started to sell VMware ESXi software root accesses with prices ranging between $250 and $500.

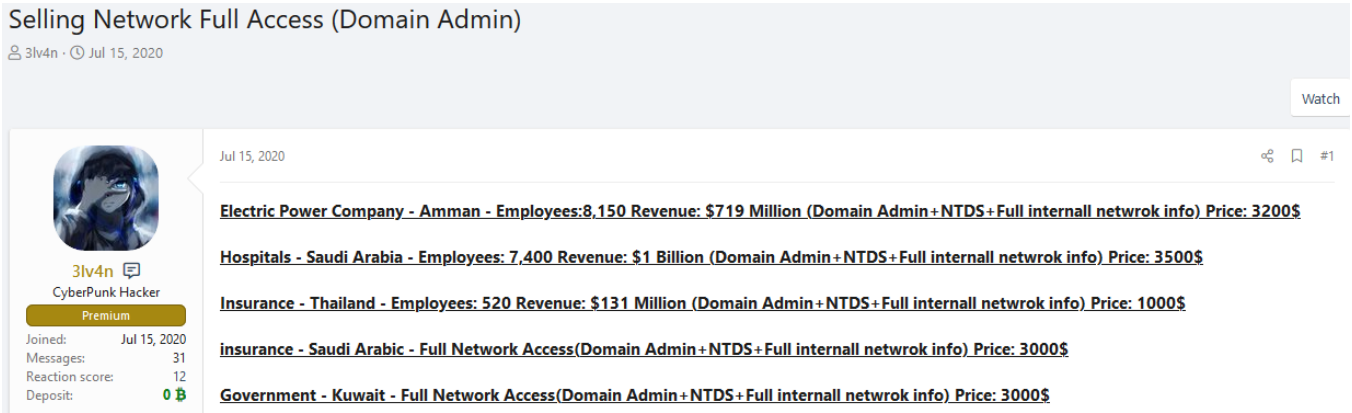

Image 2. “drumrlu” posts in their thread “Selling Network Full Access (Domain Admin)” on the XSS forum.

Blueliv analysts have observed that “Nosophoros”, the threat actor behind Thanos Ransomware as a Service (RaaS), likely collaborates with drumrlu. On July 18, 2020, Nosophoros posted on Exploit “*drumrlu is a good vendor, I vouched for him before and I still do. Glad you are back”.*

drumrlu also left a review in Nosophoros profile stating "*Best RaaS, Best Programmer".* Another comment from the threat actor "peterveliki" supports the potential partnership between drumrlu and Nosophoros: "*I bought access from this seller - everything went smoothly. A very helpful dude. He also recommended using Thanos from Nosphorus; which turned out to be very helpful in this case. Good seller, I recommend".*

fooble

On March 28, 2021, "fooble" posted an auction of more than 200 compromised Citrix and VPN access credentials on the Exploit forum. The auction started at 20,000 (the currency was not specified, but sales are usually shown on U.S. dollars), with the possibility of a direct sale for 30,000. The list of affected entities mainly includes universities, government institutions, banks, and healthcare from Europe, Brazil, China, India, Australia, and Indonesia. A month later, the initial access broker posted an auction of 700 Citrix, VPN, and RDWeb compromised network accesses, but this time did not specify which organizations were affected. The auction started at 50,000, with the option of a direct sale for 70,000. This threat actor successfully compromised organizations worldwide, with no specific focus on any region, country or industry sector, as the following target map shows:

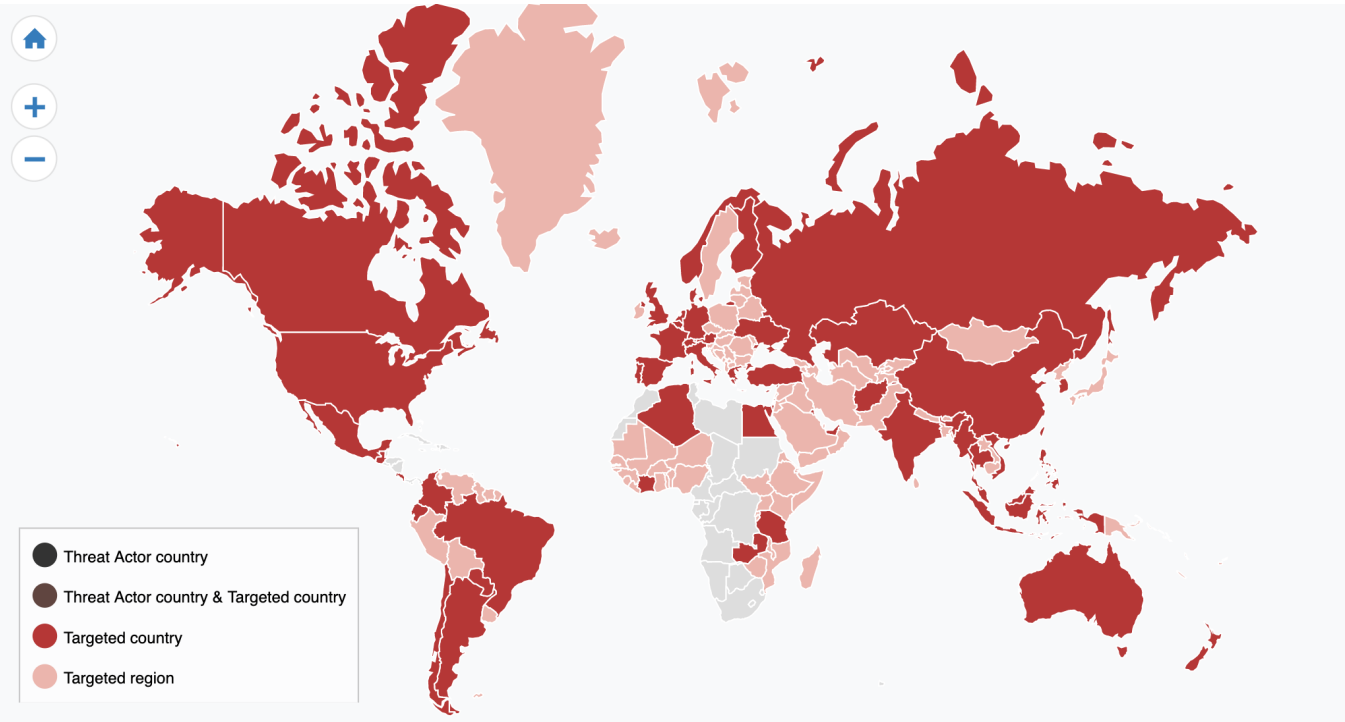

Image 3. Target Map showing "fooble" objectives in the Blueliv Threat Context module.

Although Blueliv analysts did not find any proof of ransomware groups using accesses sold by fooble, due to the popularity and the number of targets of the threat actor, it is quite likely that one of these targeted ransomware gangs might use fooble as an IAB for their operations.

pshmm

"pshmm" is an initial access broker that sells access to networks from companies using Remote Monitoring & Management (RMM) software. pshmm registered to Exploit on March 31, 2020, but did not start to sell access to networks until July 2020. They also joined RaidForums on January 10, 2021, and ever since they have only one thread, which is constantly updated. The threat actor has a thread with the title "sell network access to company" that they frequently update it with network accesses for sale. pshmm does not seem to target specific industries or regions, but a high number of victims were businesses from the United States, United Kingdom, China, Canada, Spain, Switzerland, Brazil, and Portugal from technology, government, education, construction, manufacturing, and healthcare sectors. Furthermore, the threat actor has occasionally published threads selling RDP accesses and compromised Mega cloud service accounts.

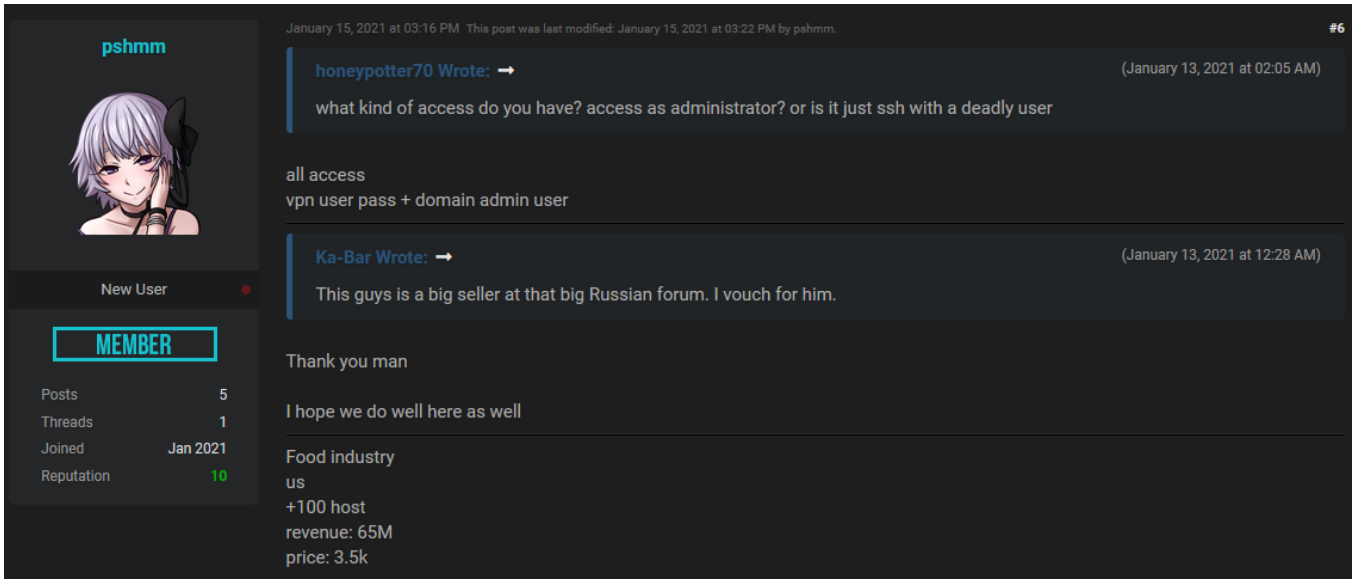

Image 4. "pshmm" updates their thread concerning network accesses at RaidForums.

7h0rf1nn

"7h0rf1nn" is an initial access broker active since at least September 2020. 7h0rf1nn attempts to gain network access to vulnerable organizations with the aim of selling that access to other threat actors. The threat actor advertises their services on popular underground forums like Raidforums, Exploit, and XSS. 7h0rf1nn has targeted insurance, financial services, education, telecommunication, and defense sectors. The access types offered for sale by 7h0rf1nn are Remote Code Execution (RCE) and webshell accesses. Blueliv researchers have observed prices range between $450 and $10,000 USD depending on the targets.

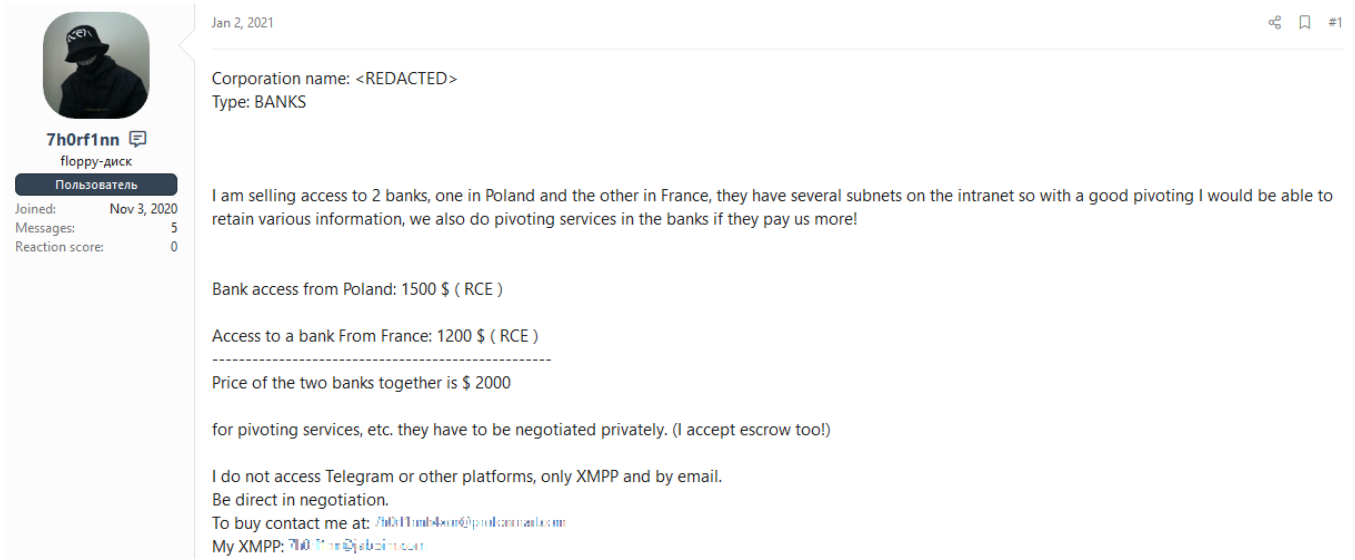

Image 5. "7h0rf1nn" offers network accesses at the XSS forum.

BadMonkey and Nefilim ransomware

"BadMonkey" is a threat actor active in underground forums since at least 2019. BadMonkey does not have a consistent set of activities, as they engage in different forum posts about malware, hacking, leaked data, etc. But the threat actor seems to be especially interested in the network accesses market, as they quite often engage in other forum members' posts selling different types of access. Yet, from their own forum posts, it is possible to verify that they are not particularly active in their sales. Still, on January 08, 2021, BadMonkey posted both on Exploit and XSS forums an offer for 225 VPN accesses obtained using a Pulse Secure VPN vulnerability, as seen in the following screenshot:

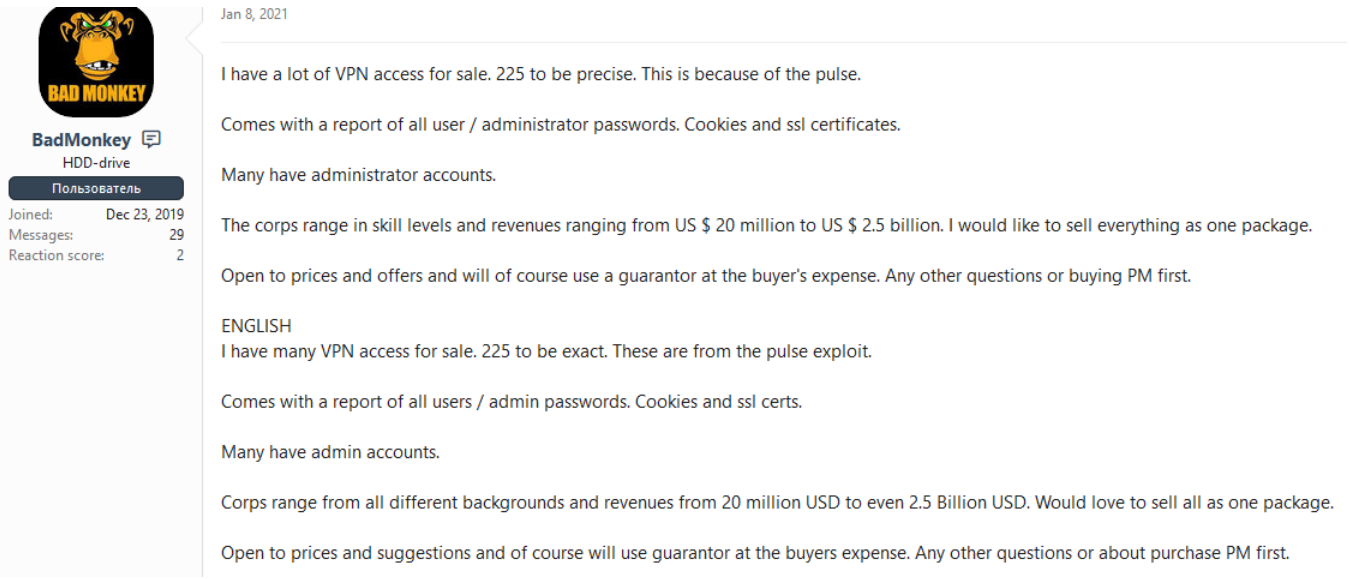

Image 6. "BadMonkey" posts on XSS forum an offer for 225 VPN network accesses.

On Exploit, one threat actor responded to BadMonkey's post: "Jingo" (aka "farnetwork"). Jingo is a known threat actor in underground forums who is believed to be related to the Nefilim ransomware group since the initial phases of that ransomware development, back when it was Nemty ransomware. Jingo responded to the aforementioned post telling BadMonkey to contact them on Jabber, to which BadMonkey answered saying that they already added Jingo on the messaging platform.

Conclusions

The usage of Initial Access Brokers by ransomware groups as a starting point to perform an intrusion into an organization has greatly increased in the past months. The use of credential shops to obtain some sort of access to targeted companies has been popular for years, but IABs have fueled and simplified this task for attackers who just need to pay for a confirmed access to a given target. The use of access brokers by ransomware gangs has shown this market interest in underground forums, serving as a stimulus for cybercriminals to look for vulnerabilities and accesses in order to sell them to the best buyer.

At the same time, this relationship between IABs and ransomware groups shows how industry sectors and the location of the victims are unimportant to attackers, as long as they have money to pay for the ransom. The adversaries look for targets by revenue instead of by sector or country, making this a global and widespread threat.

Nowadays, companies must defend against their targeted attackers plus the adversaries who can target any company, like ransomware gangs. In any case, knowledge about how threat actors behave and attack is crucial for an effective and rapid defense. The Blueliv Threat Intelligence solution gives insights about these relationships, offering additional information like MITRE ATT&CK techniques, IOCs, targets, and much more.