Here's what we know about DarkSide ransomware

intel471.com/blog/darkside-ransomware-colonial-pipeline-attack

With the ransomware incident that shut down a major fuel pipeline in the United States, another well-known variant on the cybercrime underground has been thrust into the international spotlight.

On May 10, 2021, the U.S. Federal Bureau of Investigation announced the attack on Colonial Pipeline was caused by the DarkSide ransomware variant, which forced the company to halt the pipeline's operations so Colonial could carry out a full investigation into the event. While the general public may be hearing DarkSide's name for the first time, Intel 471 has been tracking those associated with the variant since they first announced their products to the cybercrime underground last year.

The following is an examination of how DarkSide rose to prominence among cybercriminals — which Intel 471 has been tracking since they emerged in the underground — in an ecosystem that is teeming with actors looking for new ways to extort businesses out of their money.

While spotted in the wild as far back as August 2020, DarkSide's developer "debuted" the ransomware on the popular Russian-language hacker forum XSS in November 2020, advertising that he was looking for partners in an attempt to adopt an affiliate "as-a-service" model. Soon after, the ransomware was spotted to be behind numerous attacks, including several incidents targeting manufacturers and law firms in Europe and the United States.

In March 2021, the developer rolled out a number of new features in an effort to attract new affiliates. These included versions for targeting Microsoft Windows and Linux based systems, enhanced encryption settings, a full-fledged and integrated feature built directly into the management panel that enabled affiliates to arrange calls meant to pressure victims into paying ransoms, and a way to launch a distributed denial-of-service (DDoS).

With respect to DarkSide's affiliates, there is overlap in how the ransomware was delivered, including affiliates gaining initial network access by exploiting vulnerable software like Citrix, Remote Desktop Web (RDWeb), or remote desktop protocol (RDP), performing lateral movement, and exfiltrating sensitive data before ultimately deploying ransomware.

For initial access to networks, actors usually purchased access credentials on underground forums, conducted brute-force attacks, used spam campaigns to spread malware loaders and/or bought access to popular botnets such as Dridex, TrickBot and ZLoader. As for post-

exploitation tools, the arsenal usually included Cobalt Strike and Metasploit frameworks, Mimikatz and BloodHound.

Some of the tactics, techniques and procedures that Intel 471 has observed from DarkSide affiliates:

- One prominent actor partnered with network access brokers to source initial access credentials, used the Mega.nz file-sharing service to exfiltrate data from victims, leveraged a PowerShell backdoor for reconnaissance and persistence within corporate networks, and also operating the KPOT information-stealing malware in conjunction with deploying DarkSide.
- Another actor recruited penetration testers to use VPNs in conjunctions already-obtained network access, allowing attackers to move laterally within the network, exfiltrate sensitive data and deploy ransomware.

DarkSide operators did not take responsibility for the Colonial Pipeline attack or publicly dump any data belonging to the company at the time of this report. However, on May 10, 2021, the group released an announcement alluding to its possible involvement in the attack. The operators pledged in the announcement that they will introduce “moderation” in the future by carefully checking each company DarkSide affiliates want to encrypt “to avoid social consequences in the future.” Operators also claimed that the group is strictly motivated by money, and not affiliated with any government apparatus.

This is not the first time DarkSide operators have tried to put PR spin on their actions. In October, the group announced on its blog that it would donate a portion of the collected ransoms to Children International, non-profit child sponsorship organization dedicated to fighting poverty, and The Water Project, a non-profit aiming to provide clean water to countries in sub-Saharan Africa.

"We think it's fair that some of the money they've paid will go to charity,” the entry on the blog site read. “No matter how bad you think our work is, we are pleased to know that we helped change someone's life."

It is unknown if DarkSide continued to fund the charities outside of their initial donation.

The popularity and increasing maturity of the ransomware-as-a-service model combined with the aging systems that control energy systems is a compounding problem. As threat actors continue to observe ransomware’s operational success, more cybercriminals likely will want to get in on the action due to its thriving sub-industries (i.e. access brokers, credential shops, and bulletproof hosting) and higher returns when compared other crimes (i.e. targeting bank accounts). It’s imperative that companies responsible for critical infrastructure understand that insecure systems present a juicy ransomware target to the cybercriminal underground, and proactive defenses will go a long way in preventing future incidents like what happened with Colonial Pipeline.