From Dawn to "Silent Night": "DarkSide Ransomware" Initial Attack Vector Evolution

advanced-intel.com/post/from-dawn-to-silent-night-darkside-ransomware-initial-attack-vector-evolution

May 14, 2021

- May 14, 2021
-
- 5 min read

Disclaimer: This is a redacted excerpt of the report published by the subject matter expert team at Advanced Intelligence for the flagship product "Andariel".

DarkSide's affiliate group ascension to the top of the cybercrime food chain was determined by DarkSide's ability to build its initial attack arsenal, which included RDPs, infrastructural vulnerabilities, and, most importantly, a liaison with the Zloader aka "Silent Night" botnet sub-

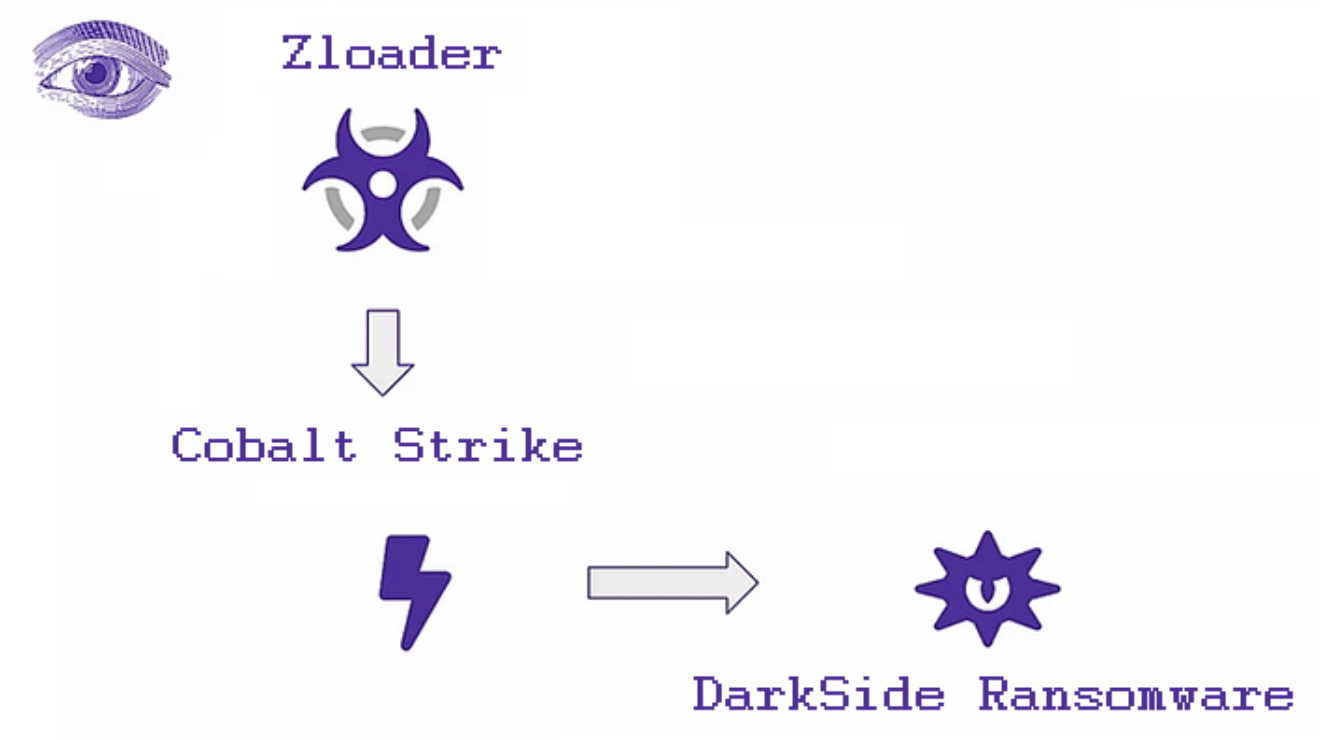
group operation.

DarkSide positioned itself as a unique group from the very beginning. Ironically, they started with a promise that they will not target healthcare and critical infrastructure. While many other ransomware-as-a-service (RaaS) affiliate groups preferred to target corporate networks with hopes of spotting vulnerable networks massively, DarkSide deliberately focused on long-planned attacks that took persistence and sophistication.

Moreover, based on multiple forensics and tailored intelligence matters, AdvIntel determined that the group diversified the initial attack points used during attacks according to our threat prevention product "*Andariel*."

This discovery and investigation were significant as we identified three crucial patterns for the DarkSide operation against the manufacturing, logistics, and infrastructure industry:

- **Use of supply-chain attacks**
- **Use of multiple attack vectors**
- **Alliance with Zloader aka “Silent Night” botnet group**



Evolution of DarkSide Methods

At the beginning of April, AdvIntel investigated a DarkSide breach of a major North American retailer. DarkSide was consistent in their victimology - the retailer network connected hardware producers and manufacturers. The data dumped by the DarkSide on the website included valuable corporate information likely extracted from the admin domain or other joint network that connects all the branches.

1. Supply-Chain Attack

A supply-chain cyber-attack unites the seemingly ununitable - massive scale-based automated dissemination of ransomware and selectively targeted attacks requiring the persistent presence and protracted recognizance. Such a combination turns an already viable attack methodology into a far-more perilous attack foundation. At the same time, the affiliates of elite ransomware syndicates are keeping a close eye on the vulnerable periphery of larger targets to initiate an APT-style joint operation against a defense contractor, an investment fund, or, in this case - a major retailer.

2. Further Advancement - Multi-Vector Attack

However, utilization of the supply-chain attack methodology was not the only findings we had. Upon defining the likely attack strategy employed in the case, AdvIntel reconstructed the attack approach. For this purpose, we have performed a vulnerability analysis for the initial attack points using our unique visibility into the adversarial datasets. Three types of potential initial points were found for the victim's domains within the timing that matched DarkSide's TTPs and the attack timelines - exposed Microsoft Exchange Server endpoints, botnet infection indicators, Palo Alto vulnerability CVE indicators.

The methodology of exploiting Palo Alto CVE vulnerability by ransomware groups may be similar to the ones practiced by them against Pulse VPN and Fortigate endpoints. The exploitation of such CVEs implies remote code execution (as in the case of Palo Alto CVE-2019-1579), privilege elevation, or credential-stealing. The exposure remained present the day when the files of the victim were dumped. One of the possible scenarios is that the vulnerability was used at the final step of the attack, before the payload deployment. It is possible that DarkSide engaged in a multi-vector attack in which different initial attack points were used for various purposes - CVEs for maintaining persistence and/or auxiliary network investigations and access privilege elevation.

3. Peak - Zloader aka “Silent Night” Botnet

However, the most valuable finding was that we detected Zloader infection in relation to the victim's domain, prior to the attack. Zloader - a prolific botnet also known as “Silent Night” immediately became our primary investigation vector.

This was not the first time when we investigated a “Zloader-DarkSide” deployment. In the week of February 22, 2021, AdvIntel identified and reported a Zloader botnet infection of one of the largest insurance brokerages in the United States. The botnet operators noted host count, indicating that they had access to that many devices in the company network. In March 2021, the offering of the victim's data appeared on the "name-and-shame" blog of DarkSide.

According to AdvIntel's advanced HUMINT operations, the Zloader operators classified the access as the one that can be developed for a re-sell or share with ransomware collective and for the further attack conducted via a ransomware payload deployment orchestrated through the Zloader-established intrusion.

Not only is this botnet known for being one of the main attack vectors for DarkSide and working in a liaison with this group, but the infection present on the victim's domain may have supported the initial version with a supply-chain attack. This domain identified in relation to Zloader infection was likely related to a vendor, customer, third-party, or peripheral domain through which the initial attack began with DarkSide meticulously paving its way to a core domain.

Therefore, considering the timing and the indicators, Zloader infection of a peripheral domain eventually led to a core domain intrusion by DarkSide. The syndicate may have used the information, credentials, and system info collected by Zloader for conscience and intel purposes, and/or they may have used Zloader as a payload dropper.

The Finale - Colonial Pipeline

On May 8, 2021, top U.S. fuel pipeline operator Colonial Pipeline shut its entire network, the source of nearly half of the U.S. East Coast's fuel supply, after a cyberattack that industry sources said was caused by ransomware.

This attack included all of the methods which were signatures for DarkSide. For instance - multiple attack vectors. AdvIntel has identified an adversarially-targeted Microsoft Exchange server exposure for March 21, 2021.

date_collect	March 21st 2021, 00:02:35.000
t	domain	colpipe.com
t	geoip.city_name	
t	geoip.continent_code	NA
t	geoip.country_code2	US
t	isp	Colonial Pipeline Company
t	source	Adversary Feed of OWA Servers - Microsoft Exchange

Moreover, AdvIntel identified that Colonial Pipeline has been targeted by botnets in 2020.

On May 10, 2021, the US Federal Government confirmed that the ransomware variant Darkside had infected a critical infrastructure company in the United States, namely, the disruption of the operations of the Colonial Pipeline.

Conclusion

The DarkSide group attempted to become a new step in ransomware development. In order to decrease the attention to the RaaS business created by REvil, they chose to use a more quiet and diligent approach to attacks relying on long-term recognizance, supply chain infiltrations, and the use of Zloader malware for recon and delivery. Ironically, this approach led to an opposite result - ideas that were brought to rejuvenile the ransomware game, instead of culminating into the Colonial Pipeline incident with detrimental consequences to all RaaS groups.

It is still unclear what was happening behind the scenes when the Colonial Pipeline attack was in development. A possible scenario is that the affiliate(s) who were responsible for the malware operation liaison - a critical link in the entire Colonial Pipeline attack, started to act independently, understanding the power and capabilities they possessed by the DarkSide-Zloader liaison. This can lead to further negative dynamics, as even after the ransomware group declared a shutdown, the partnerships built with Zloader will not vanish.

The criminal alliance which resulted in the significant cyberattacks in the last decade is powerful and successful to simply vanish into the darkness without an international takedown or criminal arrest.