Darkside Ransomware: Falcon Protects Customers

crowdstrike.com/blog/falcon-protects-from-darkside-ransomware/

Karan Sood - Shaun Hurley - Adrian-Liviu Arsene May 18, 2021

- The CrowdStrike Falcon® platform provides CrowdStrike clients with protection from DarkSide ransomware
- DarkSide is a ransomware as a service (RaaS) associated with an eCrime group tracked by CrowdStrike as CARBON SPIDER

Ransomware incidents such as the DarkSide attack that disrupted a major fuel pipeline — one that transports almost half of all fuel consumed on the East Coast of the United States — underscore the fragility of our critical infrastructure, and the magnitude of the problems faced by the public and private sector leaders who are charged with protecting it.

“The vulnerability of infrastructure is significant to our national security and the operations of this country,” said Shawn Henry, CrowdStrike CSO and President of CrowdStrike Services, in an interview for MSNBC. “These organized crime groups have been making billions of dollars by extorting U.S. companies and global companies that have not been able to protect themselves from this debilitating ransomware.”

Who Was Behind the Pipeline Attack?

DarkSide is associated with a criminal group tracked by CrowdStrike Intelligence as CARBON SPIDER. Security researchers, customers and anyone interested in learning more about the technical tradecraft, the targeted verticals and the origin of CARBON SPIDER can explore the CrowdStrike Adversary Universe for intelligence on all tracked adversaries. This information is consistently updated, and enterprises can use it to defend their organizations against some of the most persistent adversaries active now.

CARBON SPIDER first emerged in 2013 and is known to conduct several different financially motivated operations. In the summer of 2020, it began using ransomware and ultimately built and marketed its own ransomware as a service (RaaS), which it dubbed “DarkSide.”

DarkSide operators traditionally focused on Windows machines and have recently expanded to Linux, targeting enterprise environments running unpatched VMware ESXi hypervisors or stealing vCenter credentials to log in to management consoles directly, to encrypt virtual machine files. This tactic further increases the scope of affected systems, placing additional pressure on victims to give in to ransom demands.

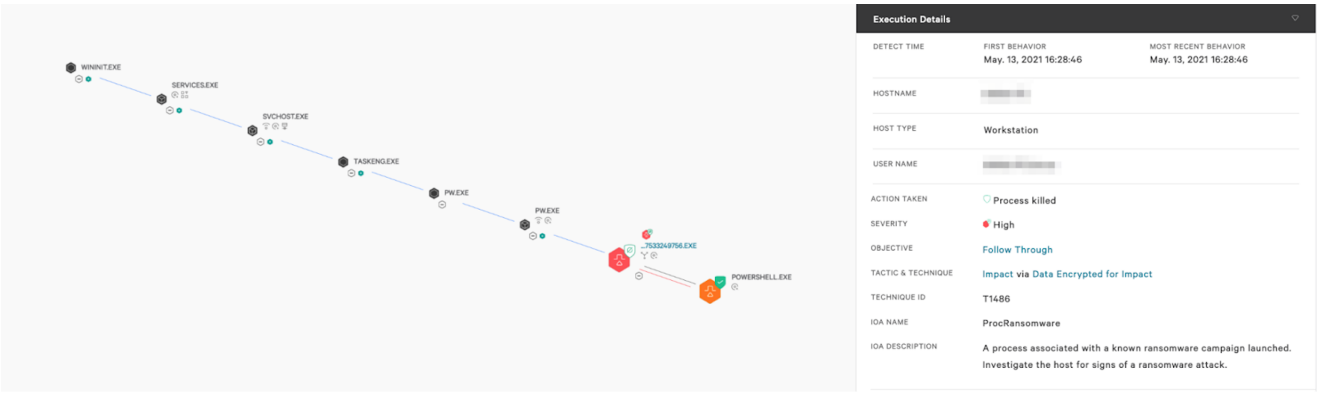
DarkSide operators seemed to pride themselves on their ability to vet affiliates that match a strictly defined set of criteria and adhere to their code of conduct. While the eCrime group claimed in the past that it will not target medical, educational or government institutions, it is clear that either its vetting process is not strict or some affiliates may not share their beliefs. DarkSide ransomware operators to whom this incident was attributed issued a statement claiming their goals are strictly financially motivated, with no political affiliation or intent to cause societal problems.

(According to Krebs on Security, the DarkSide ransomware affiliate program behind the pipeline attack later “announced it was closing up shop after its servers were seized and someone drained the cryptocurrency from an account the group uses to pay affiliates.”)

Falcon vs. DarkSide: How CrowdStrike Protects Customers

The CrowdStrike Falcon platform incorporates intelligence derived from continuous monitoring of the tactics, techniques and procedures of over 160 identified threat actors and numerous unnamed groups, enabling us to protect organizations from sophisticated attacks, including **DarkSide ransomware.**

CrowdStrike employs a layered approach when it comes to detecting malware, including machine learning as well as indicators of attack (IOAs). As the screenshot below shows, the Falcon sensor is able to kill the ransomware process as soon as the file encryption behavior is seen.



(Click to enlarge)

This video demonstrates how the DarkSide ransomware sample is immediately blocked and quarantined by Falcon upon execution. CrowdStrike's machine learning engine is part of the Falcon agent and can protect the system online or offline. In addition to machine learning, CrowdStrike Falcon's built-in behavioral detection also identifies the rapid encryption of files and blocks the ransomware execution to protect the system.

CrowdStrike takes layered security to the next level by integrating machine learning and behavioral detection within a single lightweight agent to protect those systems critical to our customers.

Recommendations

Organizations that are being hit with DarkSide or other ransomware risk a significant impact to their business operations for a protracted period of time. Companies have to protect themselves, making sure they have the right technology in place and the right visibility into their environments so that they can disrupt these operations through their security infrastructure.

The U.S. government, law enforcement and security companies understandably recommend that companies do not give in to ransomware and extortion demands. Unfortunately, public and private entities are sometimes stuck in a situation where they cannot reconstitute their environment, making an attack an existential threat to the organization.

Therefore, it's vitally important for companies to protect themselves before an incident occurs, especially as ransomware is a prolific business that adversaries will continue to invest in.

Protecting our customers against threats like DarkSide ransomware and sophisticated adversaries like CARBON SPIDER is something the CrowdStrike platform does every day. Organizations currently leveraging the Falcon platform can quickly and effectively detect and protect against DarkSide ransomware and other BGH attacks.

Independent third-party validation also supports the strength of our platform. CrowdStrike Falcon has recently been named a leader in the Gartner 2021 Magic Quadrant for Endpoint Protection Platforms (EPP) and The Forrester Wave™ Endpoint Security Software As A Service. In addition, CrowdStrike Falcon has consistently proven its detection and protection capabilities in tests performed by leading independent testing organizations, such as MITRE, SE Labs, AV-TEST and AV-Comparatives.

By deploying the Falcon platform and following the recommended "1-10-60" benchmark time (one minute to detect an incident, 10 minutes to investigate and one hour to remediate), organizations will have the best available protection for their operations and data from ransomware attacks like DarkSide.

Additional Resources

- *Learn about recent intrusion trends, adversary tactics and highlights of notable intrusions in the CrowdStrike 2021 Global Threat Report.*
- *Understand the trends and themes that we observed while responding to and remediating incidents around the globe in 2020 — download the latest CrowdStrike Services Cyber Front Lines Report.*
- *Learn more about the CrowdStrike Falcon® platform by visiting the product webpage.*
- *Test CrowdStrike next-gen AV for yourself. Start your free trial of Falcon Prevent™ today.*