DarkSide Ransomware Gang Quits After Servers, Bitcoin Stash Seized

The DarkSide ransomware affiliate program responsible for the six-day outage at Colonial Pipeline this week that led to fuel shortages and price spikes across the country is running for the hills. The crime gang 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.

Servers were seized (country not named), money of advertisers and founders was transferred to an unknown account, reads a message from a cybercrime forum reposted to the Russian OSINT Telegram channel.

What is DARKSIDE, the cybercriminal ransomware group that has the world on alert?

On May 7, 2021, a ransomware attack violated Colonial Pipeline, one of the most important oil pipeline companies in the United States, causing the interruption of the supply of naphtha, diesel and other refined products for a section of approximately 8,850 kilometers. According to the FBI, the person responsible for this attack is the DARKSIDE ransomware.

The ransomware economy and disruption of commerce, Third-party risk, Robocalls and a widespread vishing campaign.

[Ed: Blame shifting. Or how to blame those who exploit Microsoft holes, instead of Microsoft itself.]

[Ed: Shifting away attention from Microsoft, which enables these attacks]

[Ed: Why is Microsoft on this thing as "Expert" when Microsoft was the cause of the Colonial Pipeline meltdown?]
Last December was the Key Locker kernel patch series initially sent out as a request for comments. Intel Key Locker allows encrypting/decrypting data without the raw AES key but instead making use of a key handle that is in place until revoked by the system. The key when loaded is effectively sealed and then accessed by new Intel Key Locker instructions (AESENC128KL, AESENCWIDE128KL, AESDEC128KL, AESDECWIDE128KL, AESENC256KL, AESENCWIDE256KL, AESDEC256KL, and AESDECWIDE256KL) to reference the handle to a particular AES key. Intel Key Locker aims to protect AES keys by keeping the raw keys exposed for a minimal amount of time to reduce the chances they are compromised by rogue attackers. The Linux support for Key Locker is being implemented as a new "aeskl-intel" driver for the kernel's crypto subsystem.

Source URL: http://www.tuxmachines.org/node/151194

Links: