Ransomware gangs add DDoS attacks to their extortion arsenal

By Lawrence Abrams

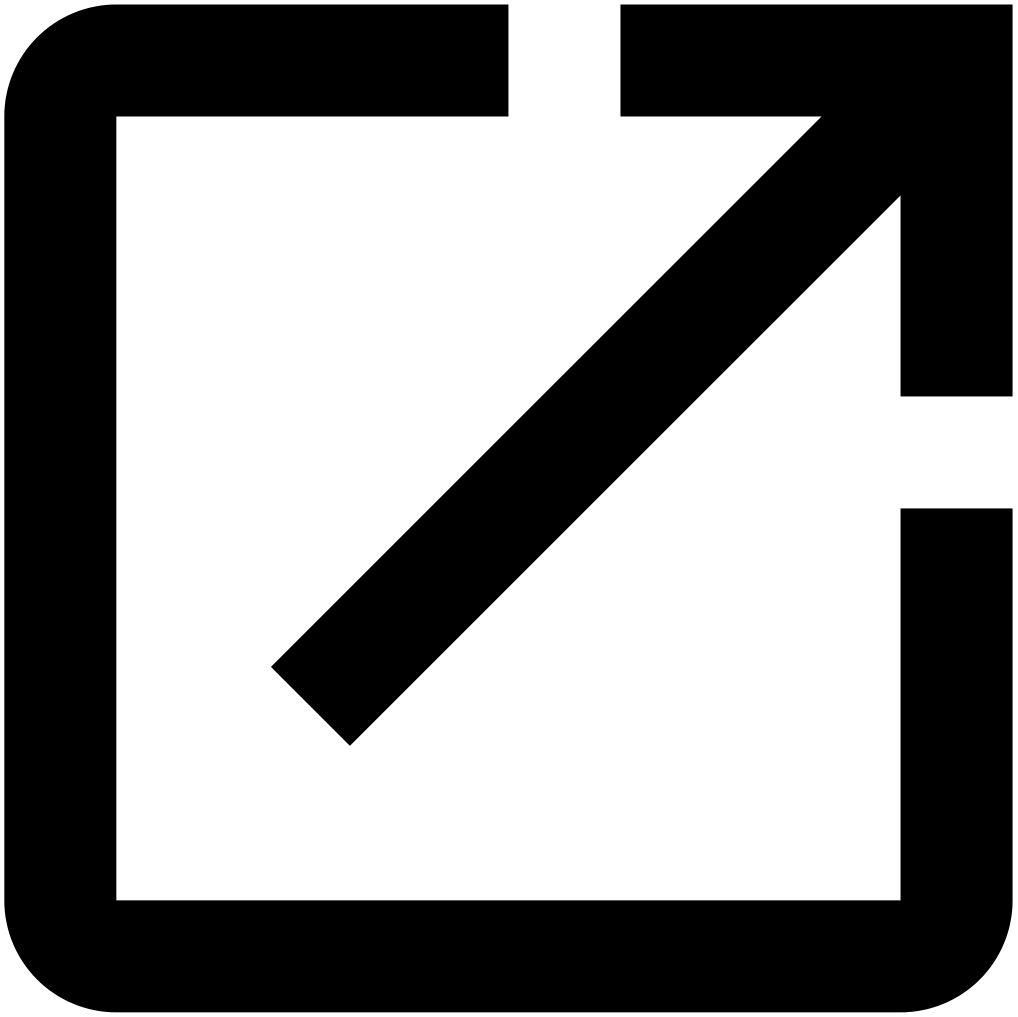
Published: 2020-10-01 · Archived: 2026-04-05 12:41:15 UTC

A ransomware operation has started to utilize a new tactic to extort their victims: DDoS a victim's website until they return to the negotiation table.

A distributed denial of service (DDoS) attack is when a threat actor floods a website or a network connection with a large volume of requests to make a service inaccessible.

After negotiations stalled in a recent ransomware attack, a SunCrypt ransomware affiliate DDoSed a victim's website.


DIE LINKE.
0:00

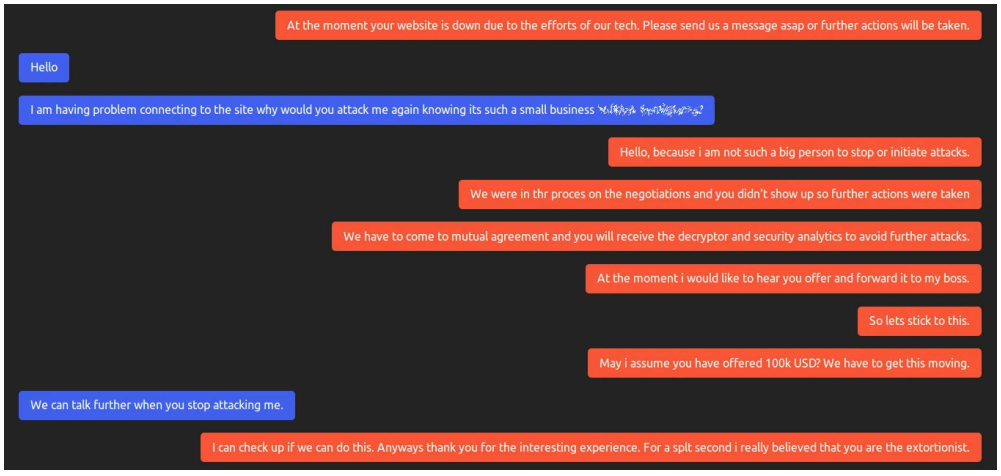


When the victim logged back into the ransomware's Tor payment site, they were greeted by a message stating that SunCrypt was responsible for the DDoS and will continue the attack if negotiations do not continue.

"At the moment your website is down due to the efforts of our tech. Please send us a message asap or further actions will be taken," the SunCrypt ransomware operator warned a victim.

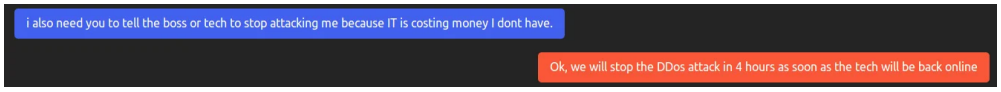
When the victim asked why they were taking their website down, the ransomware operators stated that it was to force negotiations.

"We were in thr [sic] process on the negotiations and you didn't show up so further actions were taken," the threat actors stated.



SunCrypt telling victim they are DDoSing the website
Click for larger version

After the victim began ransom negotiations again, the ransomware operator agreed to have the "tech" turn off the DDoS attack.



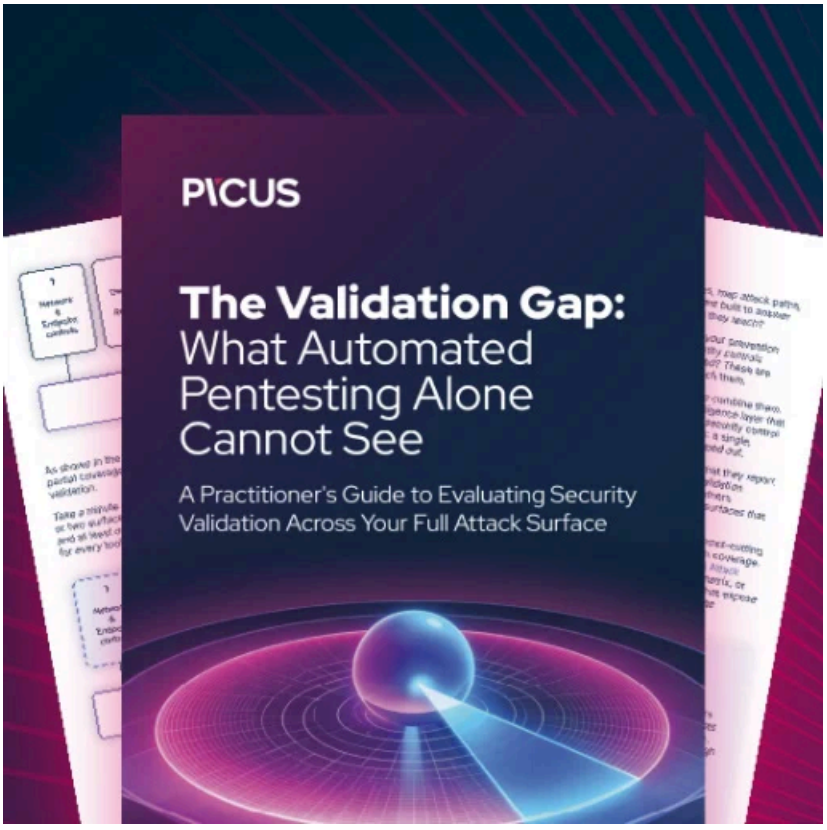
SunCrypt agreed to terminate the DDoS attack

MalwareHunterTeam, who shared the chat with BleepingComputer, told us that this tactic ultimately led to the victim paying the ransom.

This tactic was particularly effective against this victim as they were a smaller organization that was already greatly affected by the ransomware attack.

By combining data theft, the threat of a data breach, lack of access to encrypted files, and now a DDoS attack, a smaller victim could have their operation completely shut down.

This is another example of ransomware gangs updating their tactics to increase pressure on their victims so that they feel there is no choice but to pay the ransom.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/ransomware-gangs-add-ddos-attacks-to-their-extortion-arsenal/