Lodestone

OCTOBER 2022

STATE OF CYBER

monthly newsletter

MORE RANSOMWARE REARS ITS UGLY HEAD

September proved to be another hectic month in an ongoing trend of increasing ransomware incidents. Lodestone saw a massive uptick in cases with what may be a record: nearly 50 victims posted in 24 hours.

The LockBit 3.0 ransomware group has been the primary player, accounting for over 30% of all the ransomware events Lodestone has recorded in 2022 so far. These groups are also enhancing their capabilities considerably; Lodestone has noted advancements in ransomware that, among other issues, make them more difficult to detect via off-the-shelf tools.

It's not all positive for these groups, however. Word on the web is that a massive, distributed denial-of-service (DDOS) attack has been ongoing against these groups. Lodestone has noticed a significant increase in the response times of ransomware groups over the past month, likely because of these attacks. In some instances, contact with these groups has completely stalled, with victims receiving no response from threat actors normally eager to start the negotiation process.

Lodestone continues to recommend that organizations take immediate action to ensure they are well-postured to defend against a ransomware event. Ensure that modern security appliances and controls are in place and up to date. In addition, regular ransomware readiness assessments or tabletop exercises can help ensure that organization's security personnel are ready for the real deal.

RANSOMWARE DATA THEFT TOOL MAY SHOW A SHIFT IN EXTORTION TACTICS

A recent analysis of a data exfiltration tool has alarming implications: threat actors may soon destroy data completely after exfiltration, leaving no room for data recovery outside of backups or paying the ransom.

LOCKBIT, ALPHV, AND OTHER RANSOMWARE GANG LEAK SITES HIT BY DDOS ATTACKS

Various ransomware groups have been the target of DDoS attacks from an unknown source.

LOCKBIT 3.0'S RANSOMWARE SURGE HIGHLIGHTS THAT THE CYBERCRIME EPIDEMIC IS FAR FROM OVER

LockBit 3.0 is on the rise, with over 40% of the cases in August tied to the group. This trend is expected to continue into September.

NEW PSEXEC SPINOFF LETS HACKERS BYPASS NETWORK SECURITY DEFENSES

Researchers have built a version of PsExec that works over port 135 exclusively. Lodestone recommends that organization review their mitigation strategies of remote management tools.