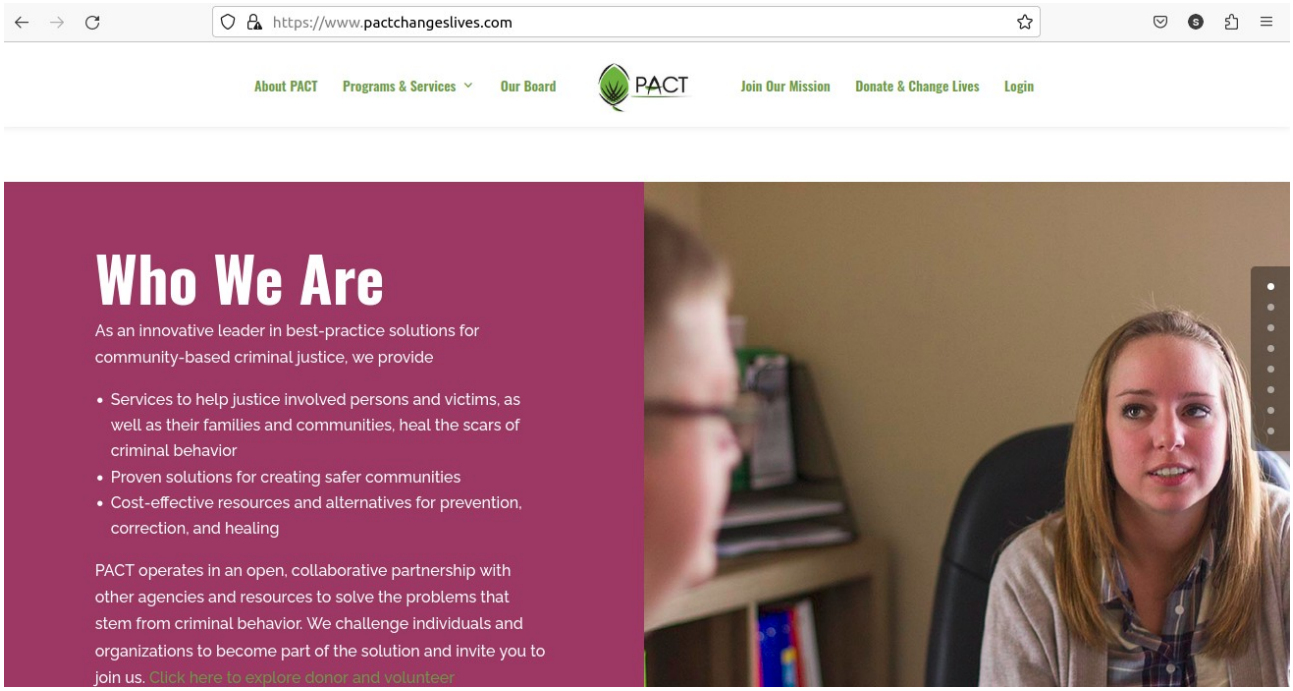
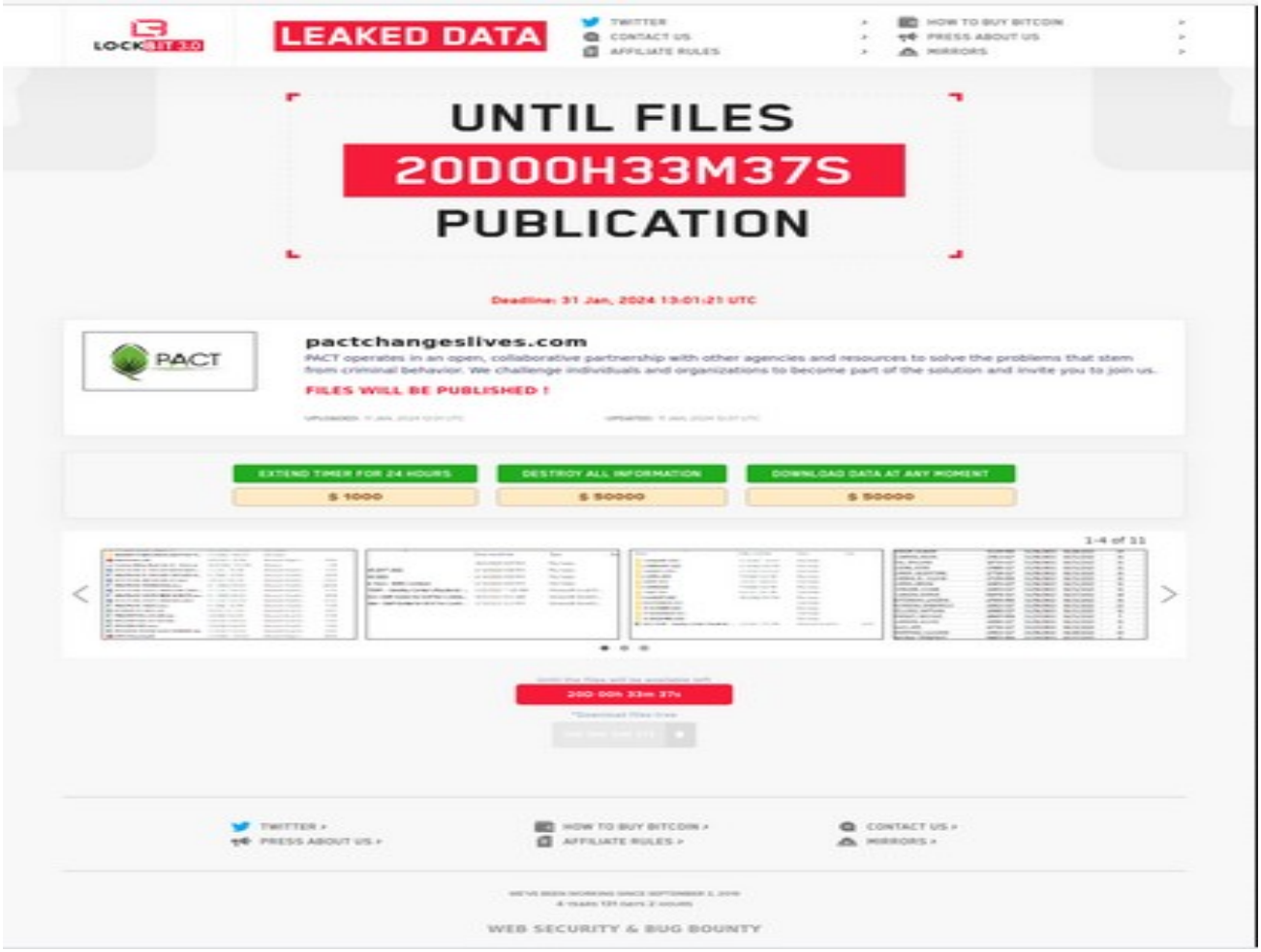
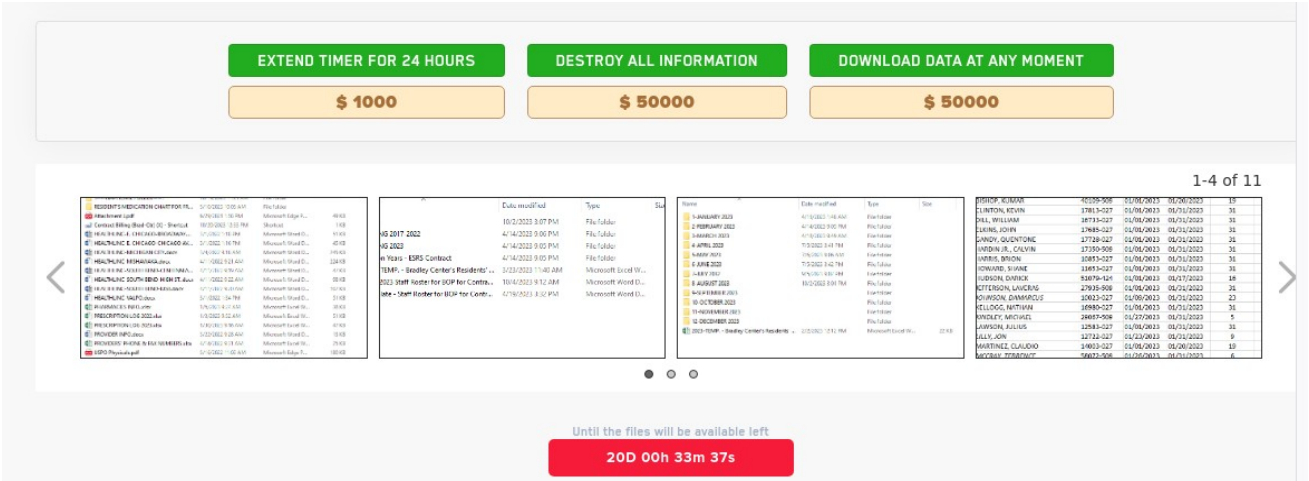
Ransomware attack on 'pactchangeslives.com' was done by Lockbit group on 11 january 2024 PACT operates in an open, collaborative partnership with other agencies and resources to solve the problems that stem from criminal behavior.

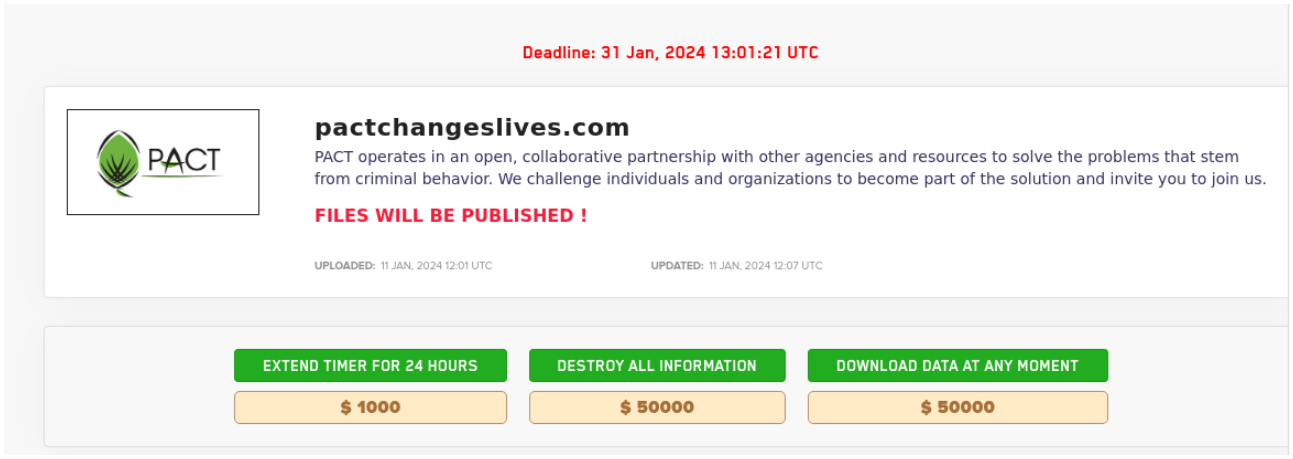


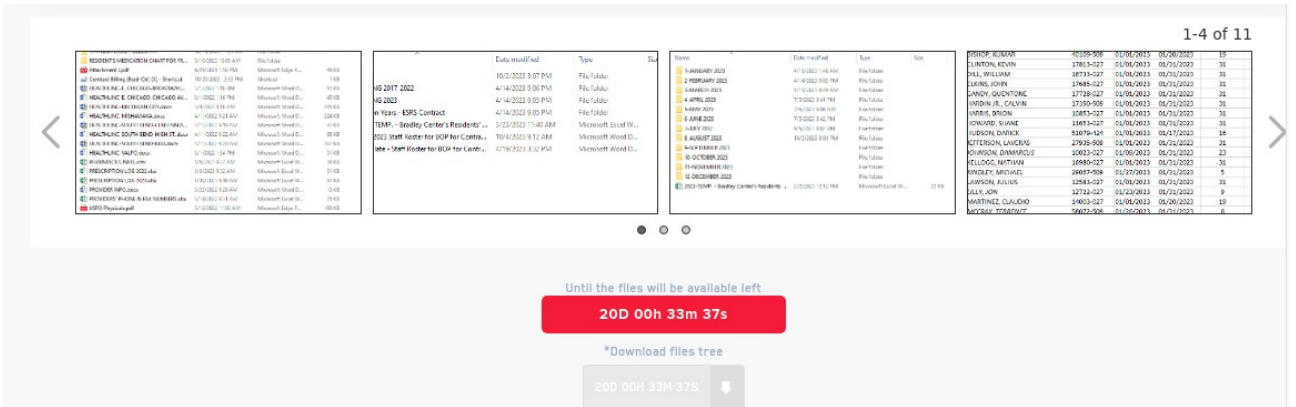
“pactchangeslives.com”



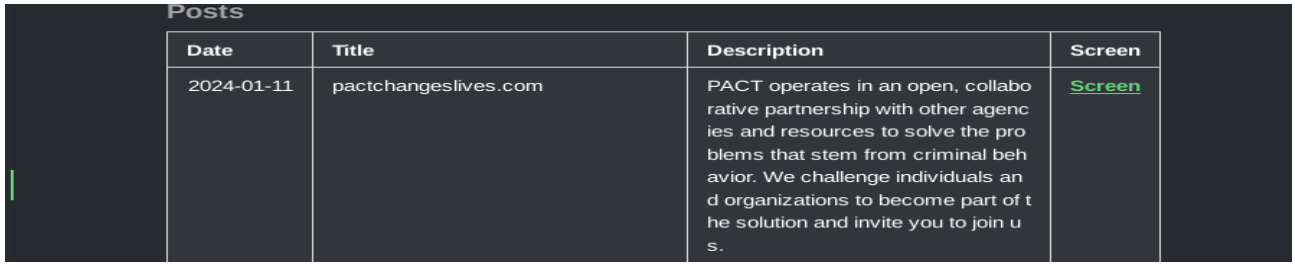


The attck was done 11-01-2024 by Lockbit3 group and they posted it on Darkweb forum with dates and also shared the screen and the dead line is given of 31 Januray to pay the rensom





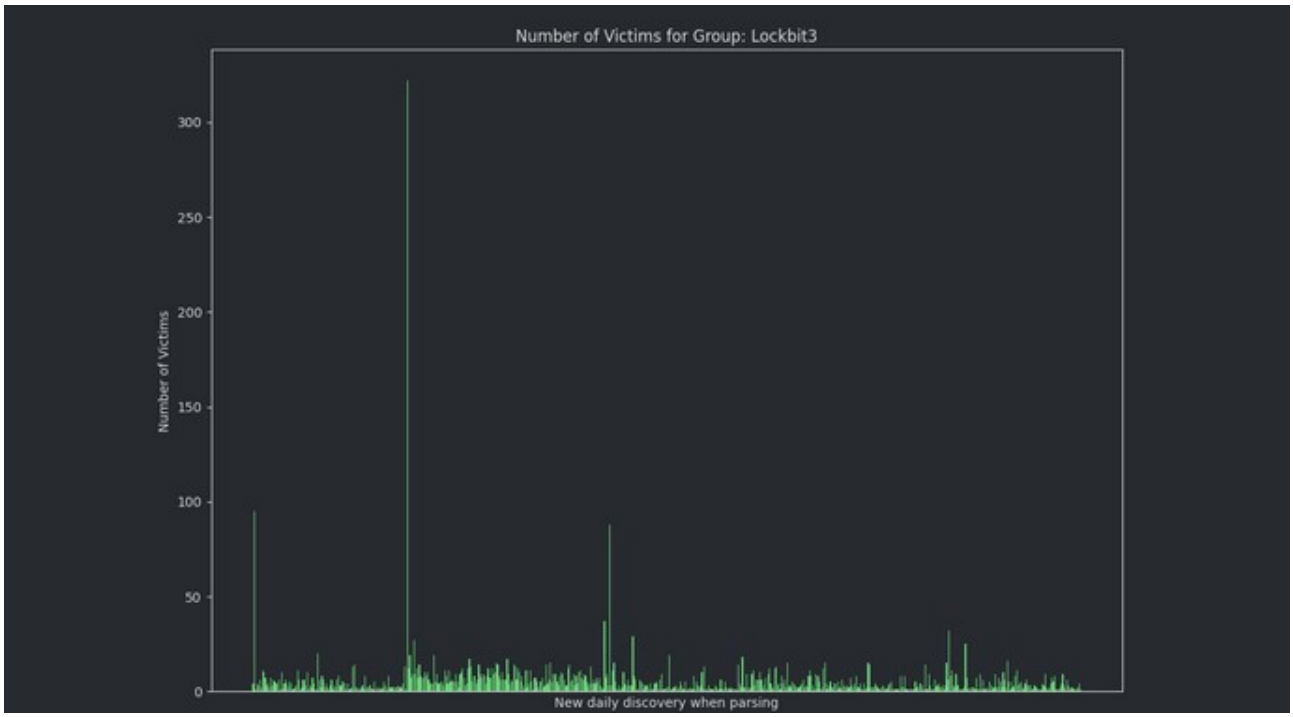
Lockbit3



Posts

Date	Title	Description	Screen
2024-01-11	pactchangeslives.com	PACT operates in an open, collaborative partnership with other agencies and resources to solve the problems that stem from criminal behavior. We challenge individuals and organizations to become part of the solution and invite you to join us.	Screen

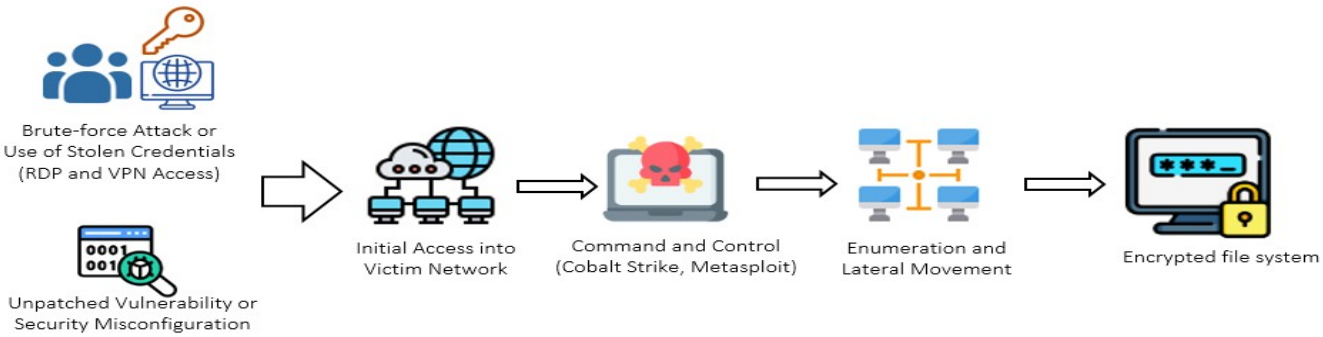
LockBit 3.0 is a Ransomware-as-a-service(RaaS) group that continues the legacy of LockBit and LockBit 2.0. From January 2020, LockBit adopted an **affiliate-based ransomware** approach, where its affiliates use various tactics to target a wide range of businesses and critical infrastructure organizations. LockBit has been highly active in deploying models such as double extortion, ,initial access broker affiliates, and advertising on hacker forums. They have even been known to recruit insiders and make contests in forums for recruiting skilled hackers; such expansionist policies have attracted numerous affiliates, have victimized thousands of entities, and continue their malicious acts.



“Attack graph of Lockbit3 ”

LockBit 3.0 affiliates exfiltrate sensitive company data files before encryption using **Stealbit**, rclone, -exfiltration tools that LockBit commonly uses- and public file-sharing services. Their affiliates also use other public file-sharing services to exfiltrate data. LockBit threat actors use various tools such as **ProDump** and **SoftPerfect Network Scanner** to collect information about hostnames, network services, and remote access protocols. They also use remote desktop software, popular file transfer tools, and PuTTY Link to move between hosts and transfer files between compromised hosts and their command and control servers.

LockBit ransomware deletes log files, files in the recycle bin, and volume shadow copies after encrypting the victim's files. The group also employs a hybrid encryption approach using AES and RSA encryption algorithms.



An overview of a typical LockBit operation. (Source: Australian Cyber Security Center)