Ransomware: LockBit 2.0 Borrows Ryuk and Egregor's Tricks

By Mathew J. Schwartz

Archived: 2026-04-06 15:16:41 UTC

Cybercrime , Fraud Management & Cybercrime , Malware as-a-Service

Rival Newcomer Hive's Ransomware-as-a-Service Operation Continues to Swarm Victims (euroinfosec) • August 20, 2021

Desktop wallpaper deployed by LockBit 2.0 on a system it's infected (Source: Trend Micro)

As ransomware-as-a-service operations continue to compete for affiliates, the operators behind LockBit have unveiled a new version of their crypto-locking malware boasting fresh features, some borrowed from rivals. Separately, a relatively unsophisticated newcomer called Hive has debuted.

See Also: Experts Offer Insights from Theoretical to the Realities of AI-enabled Cybercrime

Regardless of their sophistication, however, attackers wielding both types of ransomware continue to take down fresh victims.

Banner for the Hive ransomware-as-a-service operation's dedicated data leak site

Hive, for example, after less than two months of operation already lists on its data leak site more than two dozen victims who have so far refused to pay a ransom.

In the case of LockBit, the long list of victims has lately included the consultancy giant Accenture, which recently confirmed that it had suffered an attack and said it was restoring affected systems from backups, refusing to pay a ransom. LockBit then dumped allegedly stolen data via its dedicated data leak site, although Accenture has downplayed the value of what was stolen or leaked.

As with Hive, LockBit is run as a ransomware-as-a-service operation, meaning that operators maintain the malware and offer it as a service to affiliates, who use it to infect victims.

"The LockBit group provides a set of services - usually collecting the ransom, providing the infrastructure necessary to distribute and encrypt and apply the decryption tools and chat communications between the 'client' and the 'business,'" Matt Olney, director of threat intelligence at Cisco Talos, has told Information Security Media Group. "A cut of that final ransom ... goes to the affiliate and a cut is retained by the LockBit ransomware operators."

Security firm Emsisoft says LockBit and its affiliates have been extremely active in recent months.

Competition for Affiliates

Ransomware operators compete for affiliates, who may work with multiple operations at once. In June, LockBit's operators debuted LockBit 2.0. Experts and affiliates say that it continues to be one of the best-designed lockers on the market, with a focus on speed of encryption as well as functionality. For example, LockBit 2.0 enables

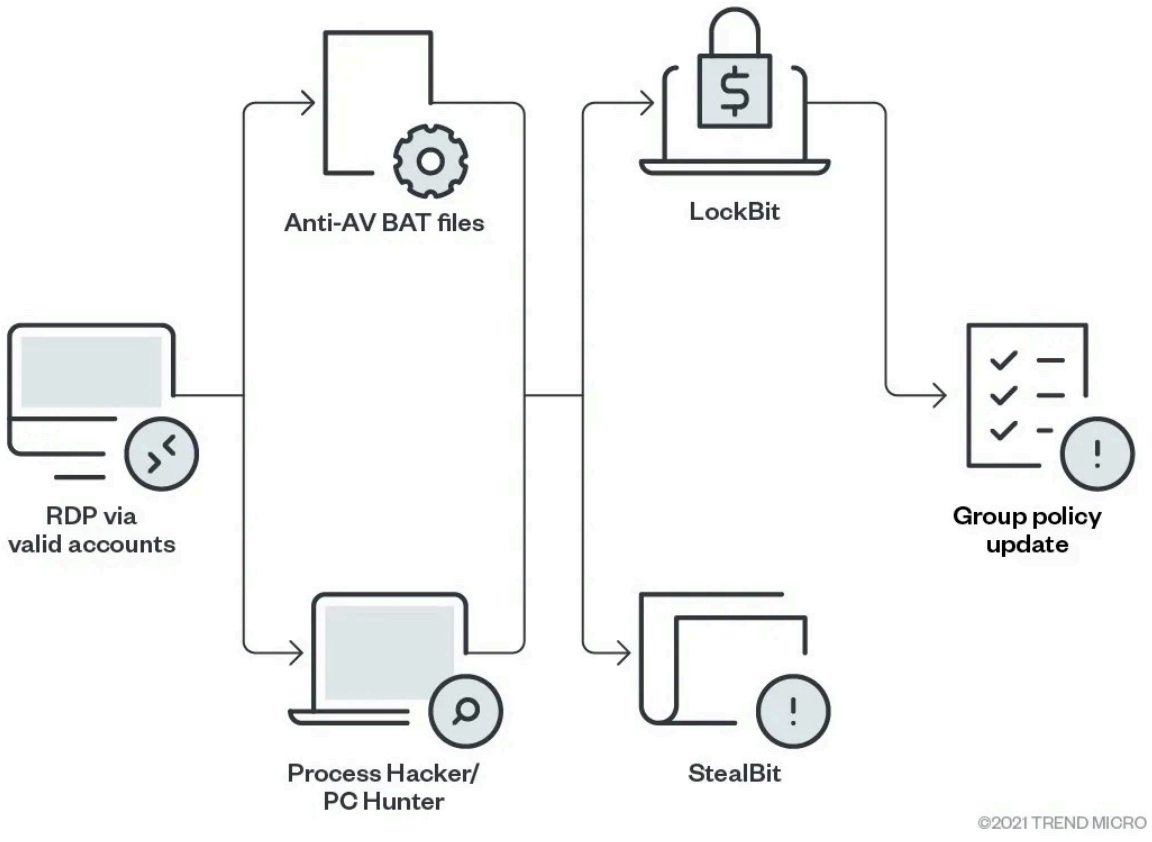
affiliates to use valid remote desktop protocol credentials - which remain easy to procure - to automatically access victims' networks, and also provides them with a Trojan called StealBit designed to automatically steal data from victims' networks, researchers at security firm Trend Micro say in a new report.

Trend Micro says it's been seeing a large number of LockBit 2.0 attacks against victims in Chile as well as Italy, Taiwan and the U.K. Those results are based on the firm's own telemetry. Such a perspective varies by security firm, because it's based on the firm's own honeypots as well as any malware encountered by customers running its endpoint and server security software.

LockBit is one of a number of operations that continue to exfiltrate data as part of a double extortion tactic designed to increase the pressure on victims to pay. Many attackers now claim to have stolen data - although thieves do have a propensity to lie - and use dedicated data leak sites to first try to name and shame victims who won't pay, followed by leaking extracts of stolen data. For victims who still refuse to pay, many groups will typically dump all stolen data online as an example to any future victims who likewise decline to pay.

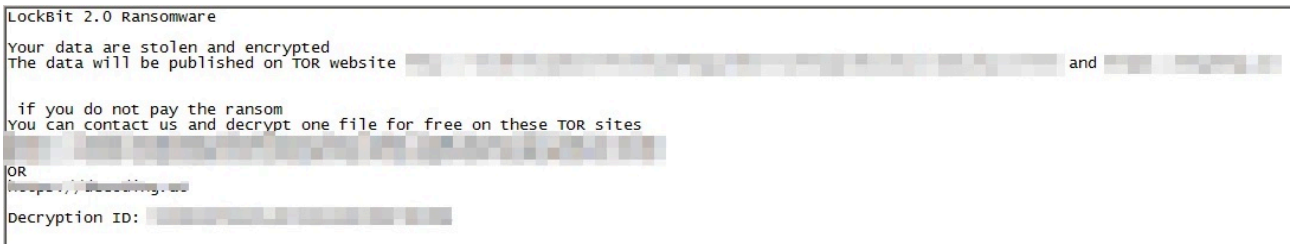
LockBit 2.0 Infection Chain

Once attackers gain access to a system and deploy LockBit 2.0, the malware "uses a network scanner to identify the network structure and to find the target domain controller," Trend Micro says. "It also uses multiple batch files that can be used to terminate processes, services and security tools. There are also batch files for enabling RDP connections on the infected machine."



LockBit 2.0's infection chain (Source: Trend Micro)

Ransomware attackers' main target is typically Active Directory's domain controller, because it enables them to operate as an administrator and push malware onto any endpoint - and Trend Micro says LockBit 2.0 is no different. "Once in the domain controller, the ransomware creates new group policies and sends them to every device on the network," it says. "These policies disable Windows Defender, and distribute and execute the ransomware binary to each Windows machine."



Ransom note - filename: Restore-My-Files.txt - dropped by LockBit into directories of files it has encrypted (Source: Trend Micro)

If LockBit 2.0 successfully crypto-locks a system, then, like many other types of ransomware, it will drop ransom notes into encrypted directories as well as change the desktop wallpaper, Trend Micro says. The wallpaper not only includes instructions for how victims can pay a ransom, but also advertises the group to potential affiliates, telling would-be recruits they can "earn millions of dollars" without ever sharing their real identity with the operation.

Learning From Maze, Ryuk and Egregor

Interpol says LockBit first partnered with the now-defunct Maze ransomware group in May 2020 before beginning to launch its own attacks several months later. Experts say LockBit appeared to recruit a number of former Maze affiliates by offering them a better cut of every ransom paid.

LockBit has continued to significantly refine its malware, and with LockBit 2.0 in particular, it has added cutting-edge features previously seen in Ryuk and Egregor ransomware, Trend Micro says. Like Ryuk, LockBit 2.0 can now send a "magic packet" that executes a wake-on-LAN command, which wakes offline devices so they can be encrypted as well as enumerate printers and do a print-bombing run via the WritePrinter API, as Egregor has done. This allows the ransomware to print ransom notes on printers across a victim's organization.

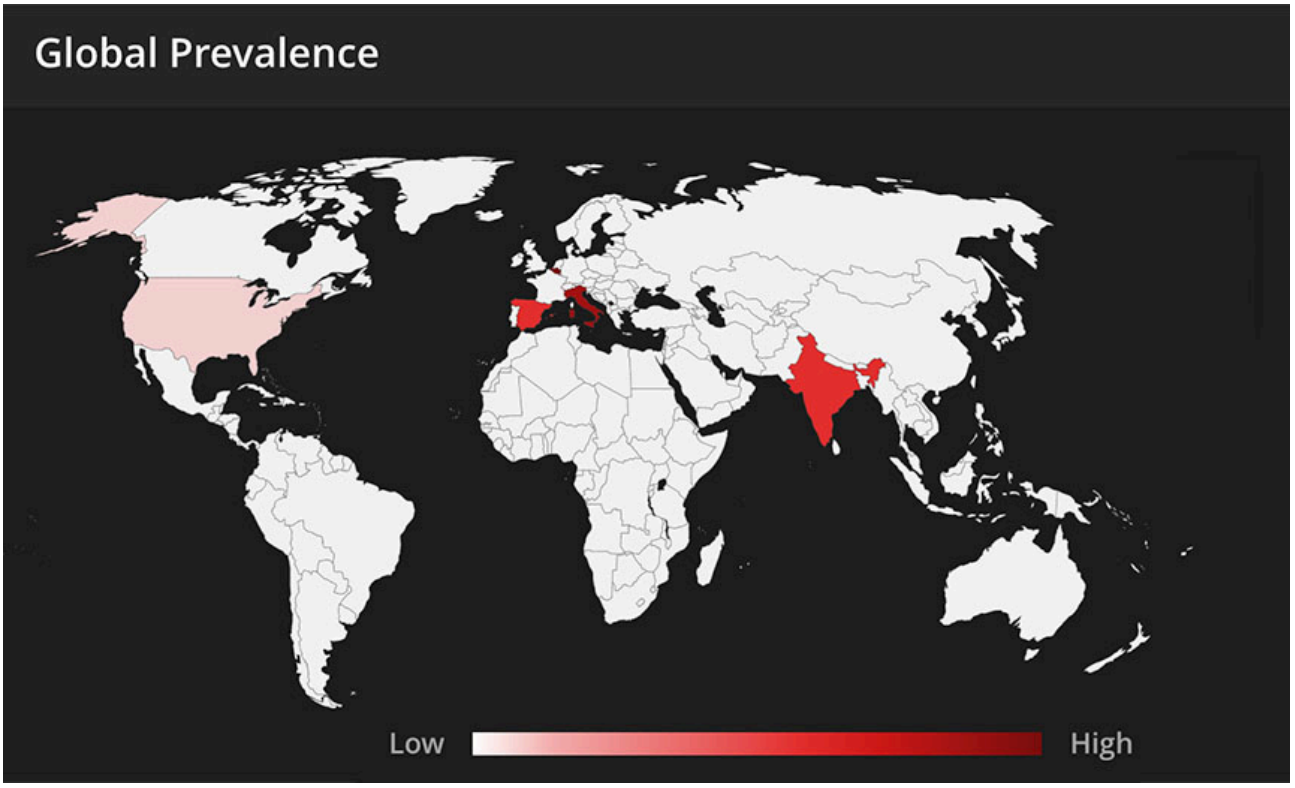
Hive Ransomware Swarms Victims

While LockBit operates at the more sophisticated end of the ransomware spectrum, new Hive ransomware is relatively unsophisticated, and yet it's still amassing victims, experts warn.

The emergence of Hive was first reported on June 26 by the self-described South Korea-based "ransomware hunter" behind the @fbgwls245 Twitter account, who spotted the malicious executable after it was uploaded to the VirusTotal malware-scanning service the prior day.

> .hive #Ransomware
> C3ACEB1E2EB3A6A3EC54E32EE620721E pic.twitter.com/HAJGyklnKu— dnwls0719 (@fbgwls245) June 26, 2021

Security firm McAfee says that based on its telemetry, the regions so far most hit by Hive affiliates are Belgium and Italy, followed by India, Spain and the United States.

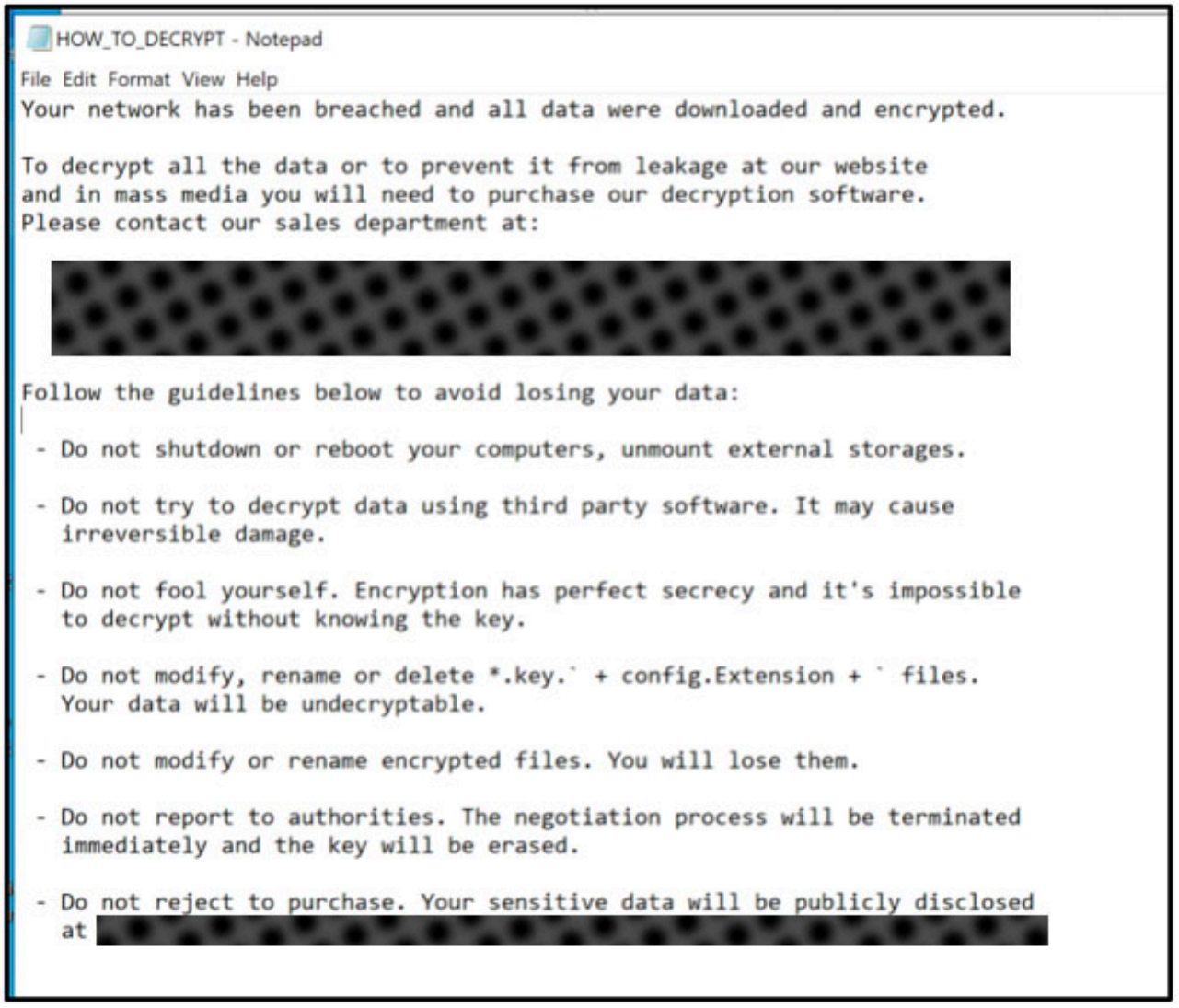


Location of Hive victims in recent days (Source: McAfee)

One apparent victim of Hive is the Memorial Health System in Ohio, Bleeping Computer reported earlier this week, based on "evidence" it's seen.

So far, however, Memorial Health System doesn't appear to have been added to the operation's dedicated data leak site, "Hive Leaks."

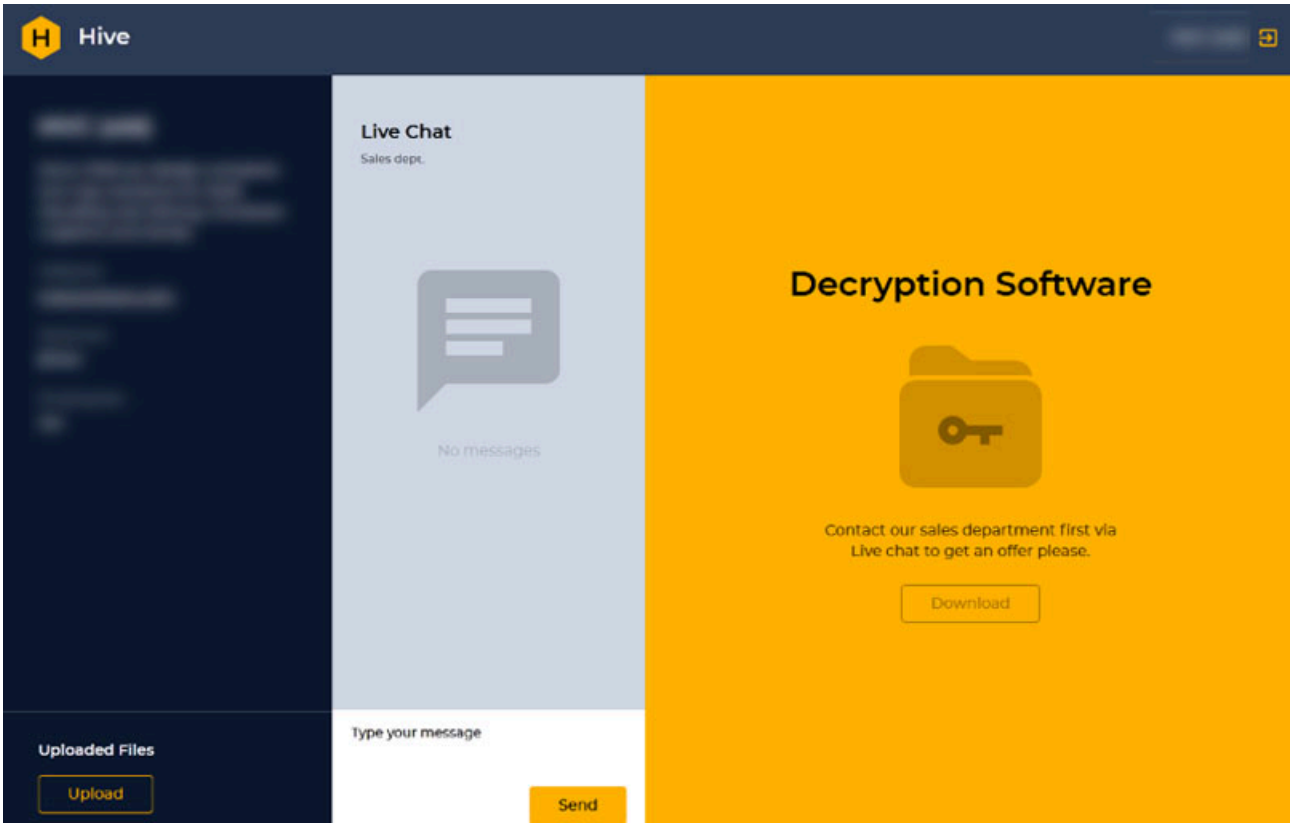
As of Friday, the leak site listed 28 victims, including a Florida-based industrial equipment manufacturer; a Florida-based, privately owned vendor of health information technology - including integrated electronic health record systems; a Chinese motor manufacturer; a Pennsylvania school district; and an Ohio-based turkey farm, among many others. The quantity of victims marked a sharp rise from July 22, when the research and intelligence team at BlackBerry counted seven victims being listed.



Hive ransom note (Source: BlackBerry)

Based on samples of Hive seen in the wild, the ransomware code appears to be "still under development," BlackBerry says.

All versions of the Hive executable seen so far have been written in the Go language. They've been seen targeting both 32-bit and 64-bit versions of Windows. "After compiling the samples, a packer - UPX - is used to obscure the code and make generic detection based on strings more difficult," McAfee says. "File sizes for Go language binaries can be very large; using UPX will make the file-size smaller."



Hive's "customer service" portal (Source: BlackBerry)

Whoever developed Hive doesn't appear to be bringing advanced coding skills to bear.

"Hive uses an idiotic and amateurish cryptographic scheme in which 100 RSA keys of varying bit size are used to encrypt files," Brett Callow, a threat analyst at security firm Emsisoft, tells Information Security Media Group.

The result for any organization that pays to obtain a decryptor will be extremely slow recovery efforts, compounded by all of the other "usual bugs and annoyances that are pretty much standard in threat actors' tools," he says. "Combined, these factors make for a very slow recovery process in cases where the demand needs to be paid."
