Ransomware gang urges victims' customers to demand a ransom payment

bleepingcomputer.com/news/security/ransomware-gang-urges-victims-customers-to-demand-a-ransom-payment/

Lawrence Abrams

By
Lawrence Abrams

- March 26, 2021
- 03:42 PM
- 0

A ransomware operation known as 'Clop' is applying maximum pressure on victims by emailing their customers and asking them to demand a ransom payment to protect their privacy.

A common tactic used by ransomware operations is to steal unencrypted data before encrypting a victim's network. This data is then used in a double-extortion tactic where they threaten to release the data if a ransom is not paid.

When data is published, it can be damaging to the victim and their customers, as the stolen data could contain personal information, credit cards, social security numbers, and even government-issued identification.

Clop warns customers of impending data leaks

After the Clop gang stole data from jet maker Bombardier in an Accellion hack, they leaked a small amount on their ransomware data leak site. A week later, the threat actors began emailing journalists to let them know that further data would be released.

As Bombardier had already disclosed the data breach, this tactic did not work as hoped by the threat actors.

However, Clop has now taken it a step further and directly emailed victims' customers found in files or database dumps stolen during the ransomware attack.

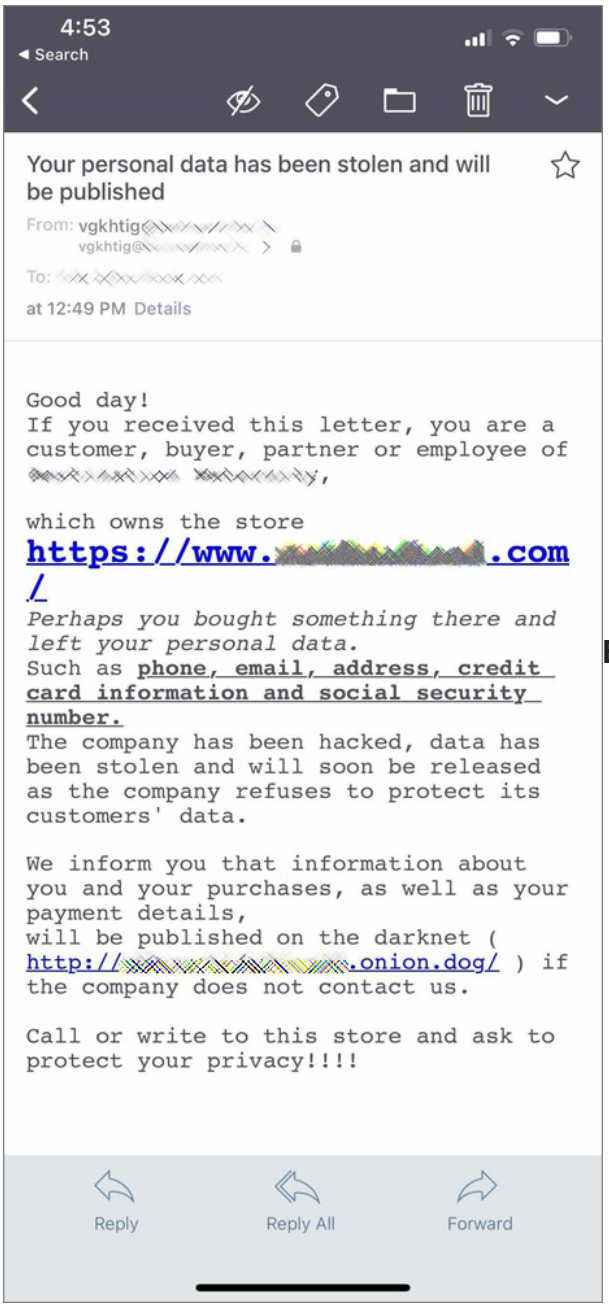
The tactic first started with Flagstar Bank customers and then with people exposed in the University of Colorado's Accellion hack.

In an email seen by BleepignComputer, Clop is now using the same tactic to the customers of an online maternity clothing store, which will not be naming.

In these emails, Clop is sending customers threatening emails with the subject "Your personal data has been stolen and will be published."

These emails say that the recipient is being contacted as they are a customer of the store, and their personal data, including phone numbers, email addresses, and credit card information, will soon be published if the store does not pay a ransom.

"Perhaps you bought something there and left your personal data. Such as phone, email, address, credit card information and social security number," the Clop gang states in the email.



Email to customer's of an online store

Clop then tells the customer to "Call or write to this store and ask to protect your privacy!!!!"

In other words, the Clop gang is hoping that if enough customers contact the store about their stolen data, the store will pay the ransom to prevent the data from being published.

While I do not think this tactic will work, it illustrates the continuing pressure ransomware gangs apply to victims by leaking their data and scaring their customers.

Clop is not alone in their attempts to apply maximum pressure on victims to get them to pay ransoms.

Earlier this month, we reported that the REvil ransomware operation was planning on DDoSing victims or making VOIP calls to victims' customers to apply further pressure.

Sadly, regardless of whether a ransom is paid, consumers whose data has been stolen are still at risk as there is no way of knowing if ransomware gangs delete the data as they promise.

Related Articles:

Industrial Spy data extortion market gets into the ransomware game

Shutterfly discloses data breach after Conti ransomware attack

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

General Motors credential stuffing attack exposes car owners info

New RansomHouse group sets up extortion market, adds first victims

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.