SOPHOS NEWS

SOPHOS SecOps

The Top 10 Ways Ransomware Operators Ramp Up the Pressure to Pay

Ransomware operators don't just target systems and data, they target people in their ever-increasing efforts to get the victim to pay

Written by Peter Mackenzie

OCTOBER 28, 2021

Ransomware has been around for decades and continues to thrive, largely because ransomware operators are quick to evolve and adapt as the cybersecurity landscape advances.

For instance, as organizations have become better at backing up their data and being able to restore encrypted files from backups, attackers have begun to supplement their approach of demanding a ransom in return for decryption keys, with additional extortion measures designed to ramp up the pressure to pay.

Some of the tactics attackers use to coerce victims into paying are ruthless and could potentially be more damaging to an organization than a period of downtime. Attackers deliberately try to undermine their target's relationships, trust and reputation. Sometimes the approach they take is very public; at other times it's more direct and personal.

For example, Sophos' Rapid Response team has seen cases where attackers email or phone a victims' employees, calling them by their name and sharing personal details the attackers have stolen, such as details of any disciplinary action or financial or passport information, with the aim of scaring them into demanding their employer pays the ransom.

This kind of behavior shows how ransomware has evolved from a purely technical attack targeting systems and data into one that also targets people.

To help organizations improve their ransomware defenses, Sophos Rapid Response has compiled the top 10 pressure tactics that adversaries used in 2021:

1. Stealing data and threatening to publish or auction it online

The list of ransomware groups that now use, have, or host a public "leak" website for exfiltrated data is long. The approach is now so common that any victims of a sophisticated intrusion need to assume that an attack with ransomware means they've also experienced a data breach.

Attackers are publishing stolen data on leak sites for competitors, customers, partners, the media, and others to see. These websites often have social media bots that automatically publicize new posts, so there is little chance of keeping an attack secret. Sometimes, the attackers put the data up for auction on the dark web or among cybercriminal networks.

However, the biggest worry for victims could be the *type* of data that attackers steal. While this may include product blueprints or secret sauce recipes, attackers generally dig out information such as corporate and personal bank details, invoices, payroll information, details of disciplinary cases, passports, drivers' licenses, social security numbers, and more, belonging to employees and customers.

For instance, in a recent Conti ransomware attack on a transport logistics provider that Sophos Rapid Response investigated, the attackers had exfiltrated details of active accident investigations, featuring the names of the drivers involved, fatalities and other related information. The fact that such information was about to fall into the public domain added significant stress to an already difficult situation.

The loss or exposure of personal data also puts victims at risk of breaching data protection laws, such as the California Consumer Privacy Act (CCPA) or Europe’s GDPR.

2. Emailing and calling employees, including senior executives, threatening to reveal their personal information

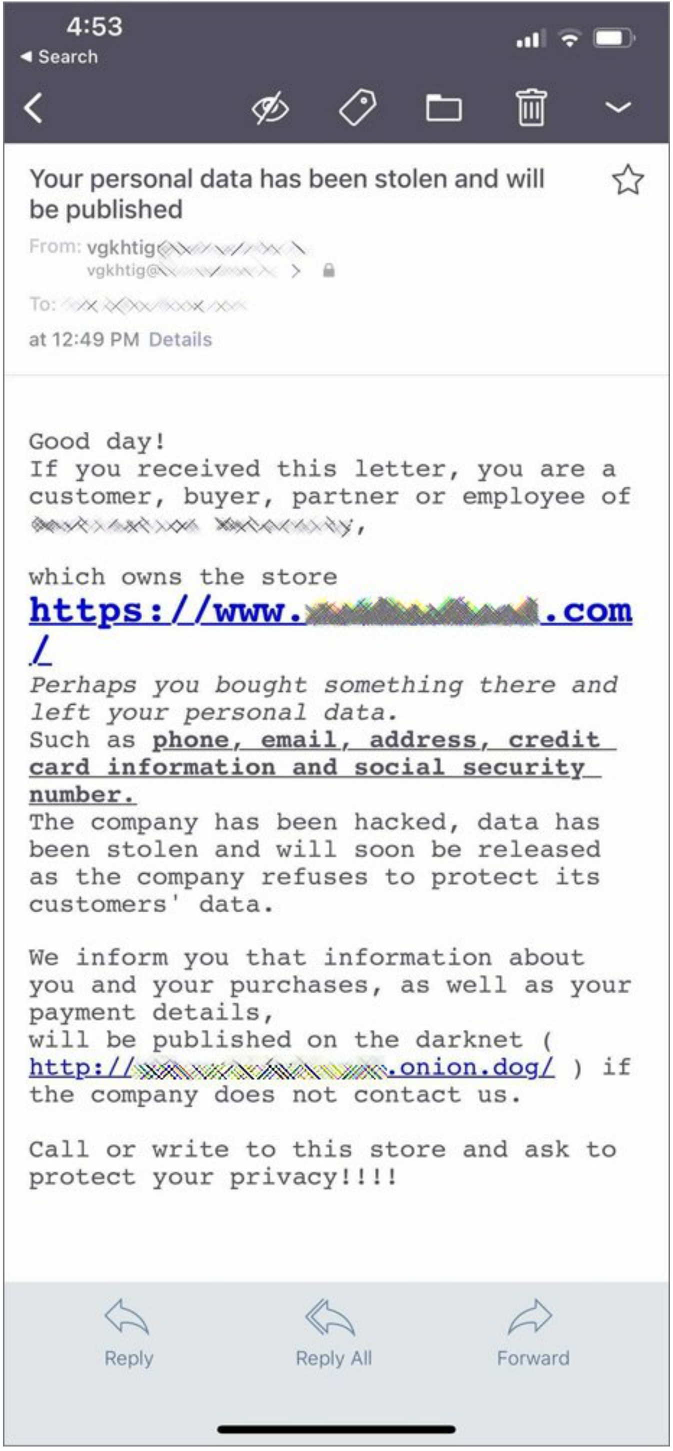
REvil, Conti, Maze, SunCrypt, and other ransomware families have used this intimidation tactic, which can be extremely distressing for recipients.

The operators behind REvil ransomware are reported to have said they call the media and victims’ business partners, providing details of the attack and asking them to urge the victim to pay. They also claimed to have set up a free service providing voice scrambled VOIP calls for their affiliate customers to use.

3. Notifying or threatening to notify business partners, customers, the media, and more of the data breach

This tactic involves emailing or messaging people or organizations whose contact details the attackers found in stolen files and telling them to demand that their target pays the ransom to protect their privacy.

REvil, Clop and other ransomware families use this approach, as seen below.



Your personal data has been stolen and will be published

From: vgkhtig[redacted]
vgkhtig@[redacted]

To: [redacted]

at 12:49 PM Details

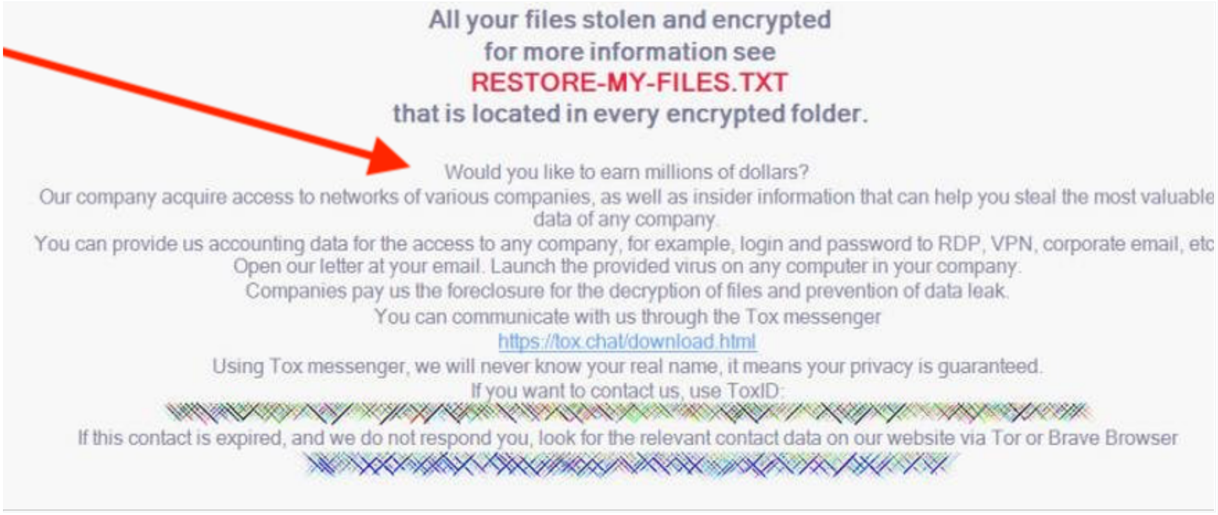
```
Good day!
If you received this letter, you are a
customer, buyer, partner or employee of
[redacted],

which owns the store
https://www.[redacted].com
/
Perhaps you bought something there and
left your personal data.
Such as phone, email, address, credit
card information and social security
number.
The company has been hacked, data has
been stolen and will soon be released
as the company refuses to protect its
customers' data.

We inform you that information about
you and your purchases, as well as your
payment details,
will be published on the darknet (
http://[redacted].onion.dog/ ) if
the company does not contact us.

Call or write to this store and ask to
protect your privacy!!!!
```

4. Silencing victims

Conti and RagnarLocker have recently started threatening victims with messages saying the victim should not contact law enforcement or share details of ransom negotiations. This could be to prevent victims from getting third-party support that might help them to avoid paying the ransom. It also suggests that ransomware brands are becoming more concerned about drawing attention to their activities, particularly from law enforcement.

5. Recruiting insiders

Another recent and unusual tactic ransomware operators are using is trying to recruit insiders to enable a ransomware attack in return for a share of the takings. In one, widely reported example, the operators behind LockBit 2.0 included a recruitment ad for insiders to help them breach and encrypt the network of "any company" in return for a substantial payout. The below notice, posted on the victim's computers after encryption, suggests that adversaries are trying to recruit insiders in victim organizations to help them breach third-party partners or suppliers – an extra cause for concern for both the victim and its partners .



All your files stolen and encrypted
for more information see
RESTORE-MY-FILES.TXT
that is located in every encrypted folder.

Would you like to earn millions of dollars?
Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company.
You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc
Open our letter at your email. Launch the provided virus on any computer in your company.
Companies pay us the foreclosure for the decryption of files and prevention of data leak.
You can communicate with us through the Tox messenger
https://tox.chat/download.html
Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.
If you want to contact us, use ToxID:
[redacted]
If this contact is expired, and we do not respond you, look for the relevant contact data on our website via Tor or Brave Browser
[redacted]

6. Resetting passwords

After breaching the network, many ransomware attackers create a new domain admin account and then reset the passwords for the other admin accounts. This means that the IT administrators can't log in to the network to fix the system. Instead, they must set up a new domain before they can even begin trying to restore from backups.

7. Phishing attacks targeting victim email accounts

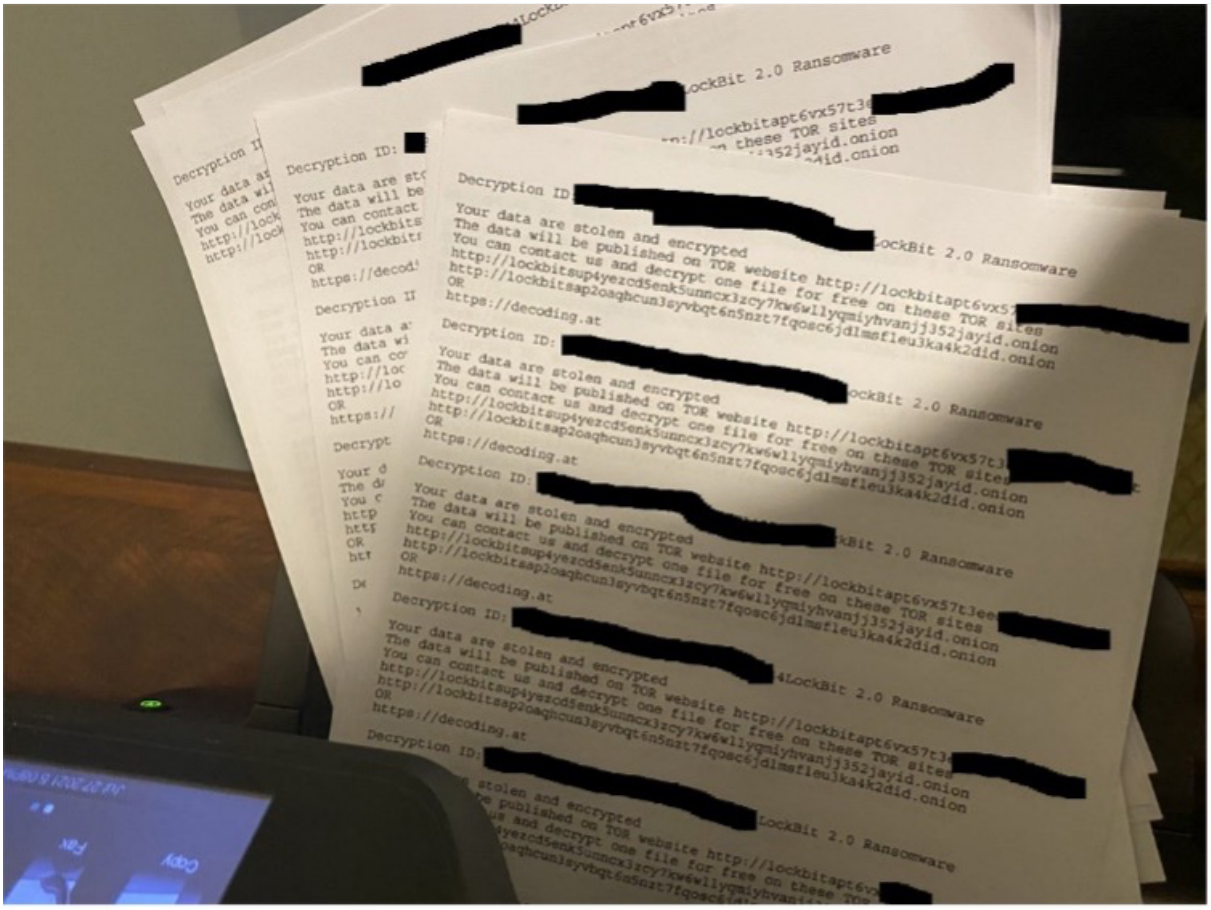
In one incident investigated by Sophos Rapid Response and involving Lorenz ransomware, the attackers targeted employees with phishing emails to trick them into installing an application that provided the attackers with full access to the employees' email, even after they reset their passwords. The attackers then used the compromised email accounts to email the IT, legal, and cyber insurance teams working with the targeted organization to threaten further attacks if they didn't pay.

8. Deleting online backups and shadow volume copies

During their reconnaissance of a victim's network, most ransomware operators will look for any backups connected to the network or the internet and delete them so that the victim cannot rely on them to restore encrypted files. This can include uninstalling backup software and resetting virtual snapshots. In one example seen by Sophos Rapid Response, involving DarkSide ransomware, the attackers deleted the victim's local backups and then used a compromised admin account to contact the vendor hosting the victim's off-site cloud backups, asking them to delete the off-site backups. The vendor complied because the request came from an authorized account. Luckily, the vendor was able to restore the backups once they had been informed of the breach.

9. Printing physical copies of the ransom note on all connected devices, including point of sale terminals

A flood of printed threats is not just a nuisance in terms of paper supply, but unsettling for people in the office. Ransomware operators including Egregor and LockBit have applied this tactic.



Decryption ID: [redacted]ockBit 2.0 Ransomware
Your data are stolen and encrypted
The data will be published on TOR website http://lockbitapt6vx57[redacted]
You can contact us and decrypt one file for free on these TOR sites
http://lockbitsup4yezcd5enk5unncx3zcy7kw6wllyqmiyhvanjj352jayid.onion
http://lockbitsap2oaqhcun3syvbqt6n5nzt7fqosc6jdlmsfleu3ka4k2did.onion
OR
https://decoding.at

Decryption ID: [redacted]ockBit 2.0 Ransomware
Your data are stolen and encrypted
The data will be published on TOR website http://lockbitapt6vx57t3[redacted]
You can contact us and decrypt one file for free on these TOR sites
http://lockbitsup4yezcd5enk5unncx3zcy7kw6wllyqmiyhvanjj352jayid.onion
http://lockbitsap2oaqhcun3syvbqt6n5nzt7fqosc6jdlmsfleu3ka4k2did.onion
OR
https://decoding.at

Decryption ID: [redacted]kBit 2.0 Ransomware
Your data are stolen and encrypted
The data will be published on TOR website http://lockbitapt6vx57t3ee[redacted]
You can contact us and decrypt one file for free on these TOR sites
http://lockbitsup4yezcd5enk5unncx3zcy7kw6wllyqmiyhvanjj352jayid.onion
http://lockbitsap2oaqhcun3syvbqt6n5nzt7fqosc6jdlmsfleu3ka4k2did.onion
OR
https://decoding.at

Decryption ID: [redacted]4LockBit 2.0 Ransomware
Your data are stolen and encrypted
The data will be published on TOR website http://lockbitapt6vx57t3[redacted]
You can contact us and decrypt one file for free on these TOR sites
http://lockbitsup4yezcd5enk5unncx3zcy7kw6wllyqmiyhvanjj352jayid.onion
http://lockbitsap2oaqhcun3syvbqt6n5nzt7fqosc6jdlmsfleu3ka4k2did.onion
OR
https://decoding.at

Decryption ID: [redacted]LockBit 2.0 Ransomware
stolen and encrypted
be published on TOR website http://lockbitapt6v[redacted]
us and decrypt one file for free on these TOR
4yezcd5enk5unncx3zcy7kw6wllyqmiyhvanj
oaqhcun3syvbqt6n5nzt7fqosc6

10. Launching distributed denial-of-service attacks against the target's website

Avaddon, DarkSide, RagnarLocker, and SunCrypt have used distributed denial of service (DDoS) attacks when ransom negotiations have stalled, to force targets back to the table. Adversaries also use DDoS attacks as distractions to tie up IT security resources while the main ransomware attack activity is taking place elsewhere on the network, or as standalone extortion attacks.

What defenders can do

The fact that ransomware operators no longer confine their attacks to encrypting files that targets can often restore from backups, shows how important it is for defenders to take a defense-in-depth approach to security. This approach should combine advanced security with employee education and awareness.

The following steps may help organizations deal with threatening attacker behaviors:

- Implement an employee awareness program that includes examples of the kind of emails and calls attackers use and the demands they might make
- Establish a 24/7 contact point for employees, so they can report any approaches claiming to be from attackers and receive any support they need
- Introduce measures to identify potential malicious insider activity, such as employees trying to access unauthorized accounts or content

It is also worth revisiting the following steps to enhance IT security against a wide range of cyberthreats, including ransomware:

- Monitor network security 24/7 and be aware of the five early indicators an attacker is present to stop ransomware attacks before they launch
- Shut down internet-facing remote desktop protocol (RDP) to deny cybercriminals access to networks. If users need access to RDP, put it behind a VPN or zero-trust network access connection and enforce the use of Multi-Factor Authentication (MFA)
- Educate employees on what to look out for in terms of phishing and malicious spam and introduce robust security policies
- Keep regular backups of the most important and current data on an offline storage device. The standard recommendation for backups is to follow the 3-2-1 method: 3 copies of the data, using 2 different systems, 1 of which is offline, and test the ability to perform a restore
- Prevent attackers from getting access to and disabling security: choose a solution with a cloud-hosted management console with multi-factor authentication enabled and Role Based Administration to limit access rights
- Remember, there is no single silver bullet for protection, and a layered, defense-in-depth security model is essential – extend it to all endpoints and servers and ensure they can share security-related data

- Have an effective incident response plan in place and update it as needed. Turn to external experts to monitor threats or to respond to emergency incidents for additional help, if needed