NETSCOUT

Triple Extortion

3

A little bit of ransomware, a little bit of DDoS extortion, and a whole lot of trouble.

From adding new weapons to their ransomware-as-a-service (RaaS) portfolio to offering payment portals and support centers for victims, ransomware gangs are laser-focused on parting unsecured organizations from their money.

HERE'S HOW IT WORKS:

1 Data Encryption

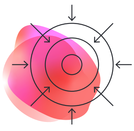
This is the bedrock ransomware ploy: Cybercriminals breach a network and encrypt valuable data, blocking it (and sometimes the entire system) from the victim organization. The attackers then demand payment in return for a decryption key.

2 Data Theft

With the double-extortion play, cybercriminals quietly remove data before locking the victim out and then threaten to publicly expose and/or sell the stolen data unless paid. This makes it harder for victims to ignore ransomware threats, because even those who can restore data via backups remain at risk of data exposure.

Ransomware gangs known to use double extortion:

- Maze
- Sodinokibi
- DoppelPaymer
- Nemty
- Nefilim
- CLOP
- Sekhmet



3 DDoS Attacks

To pull off triple extortion attacks, RaaS operators add DDoS attacks (commonly used as a stand-alone extortion method) to their list of services, to be launched after steps one and two. This further ratchets up the pressure on the victim in a couple of ways: First, it emphasizes the seriousness of the adversary. And second, maintaining availability adds yet another stressor to a security team already dealing with the first two events.

Ransomware families known to use triple extortion:

- SunCrypt
- Ragnor Locker
- Avaddon
- Darkside

Ransomware is big business.

$100,000,000

One ransomware group's collection in ransom payments in 1H 2021

According to Coveware

BIG PROFITS =

More money to pay for more-expensive attack tools such as single zero-day vulnerabilities

RANSOMWARE IS A GLOBAL CRISIS.

- Attacks affect not only companies but also governments, schools, and public infrastructure.
- Global coalition Ransomware Task Force (RTF) has called ransomware "a serious national security threat and public health and safety concern."
- Heads of state are getting involved, with U.S. President Biden pressuring Russia's President Putin to shut down ransomware groups.

FIGHTING BACK IS A GLOBAL EFFORT.

- The White House in July announced a flurry of new federal programs to fight ransomware.
- In April, the RTF released key recommendations designed to combat ransomware.
- Interpol has called for a global coalition of police and partners to work together.

Despite these recent global efforts, we still face a massive uphill climb to make even a small dent in ransomware activity.

NETSCOUT

SECIG_014_EN-2101 09/2021