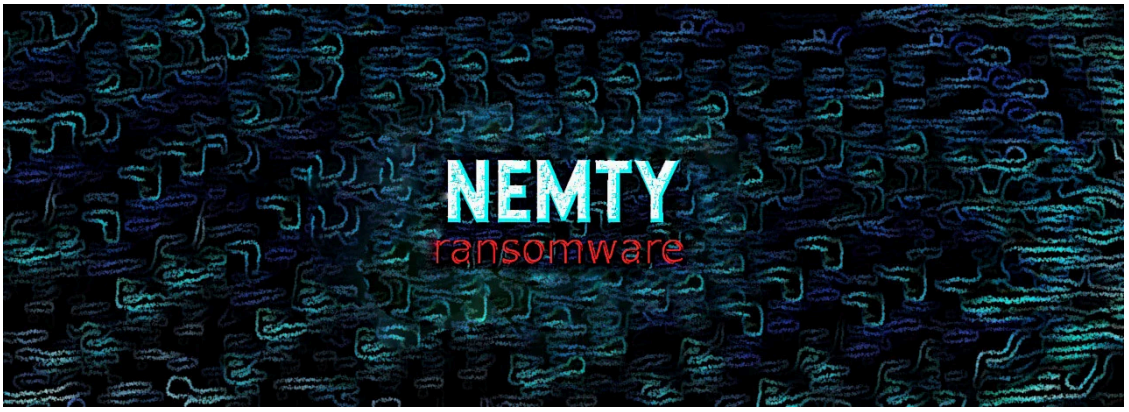
Nemty Ransomware Punishes Victims by Posting Their Stolen Data

By Lawrence Abrams

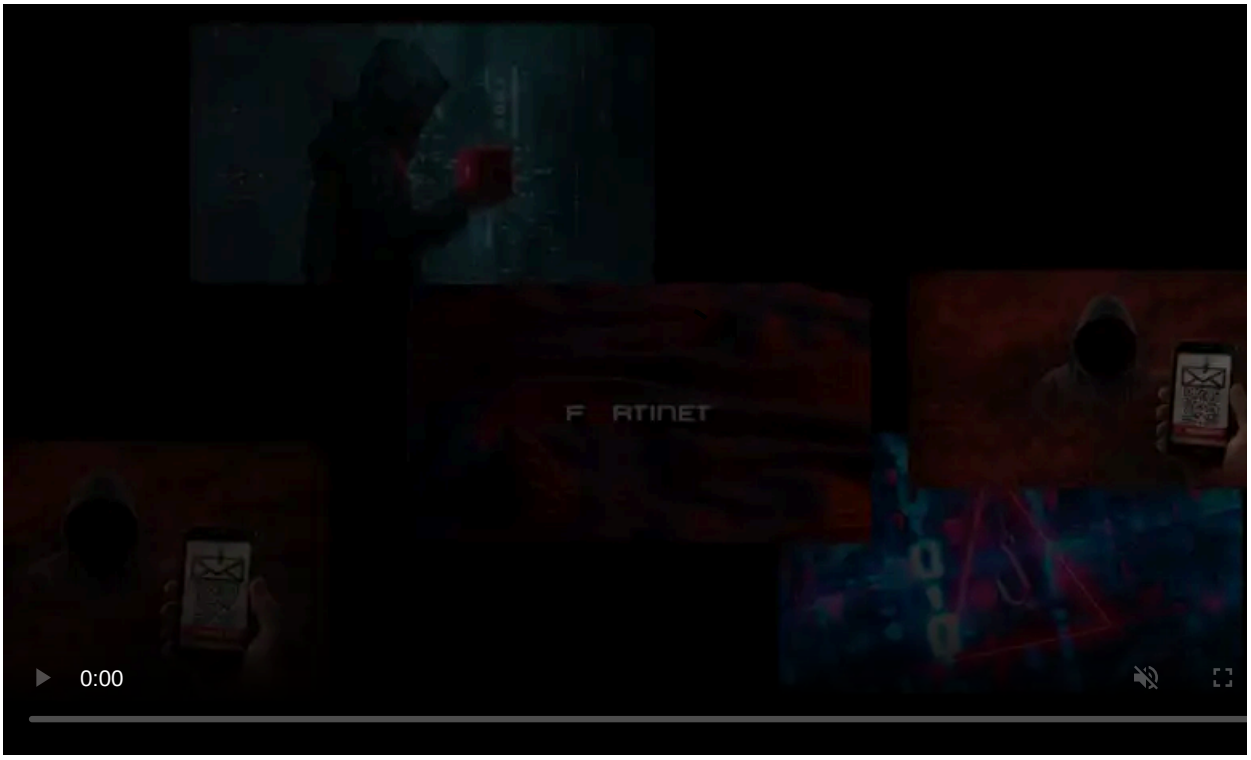
Published: 2020-03-03 · Archived: 2026-04-05 20:55:46 UTC

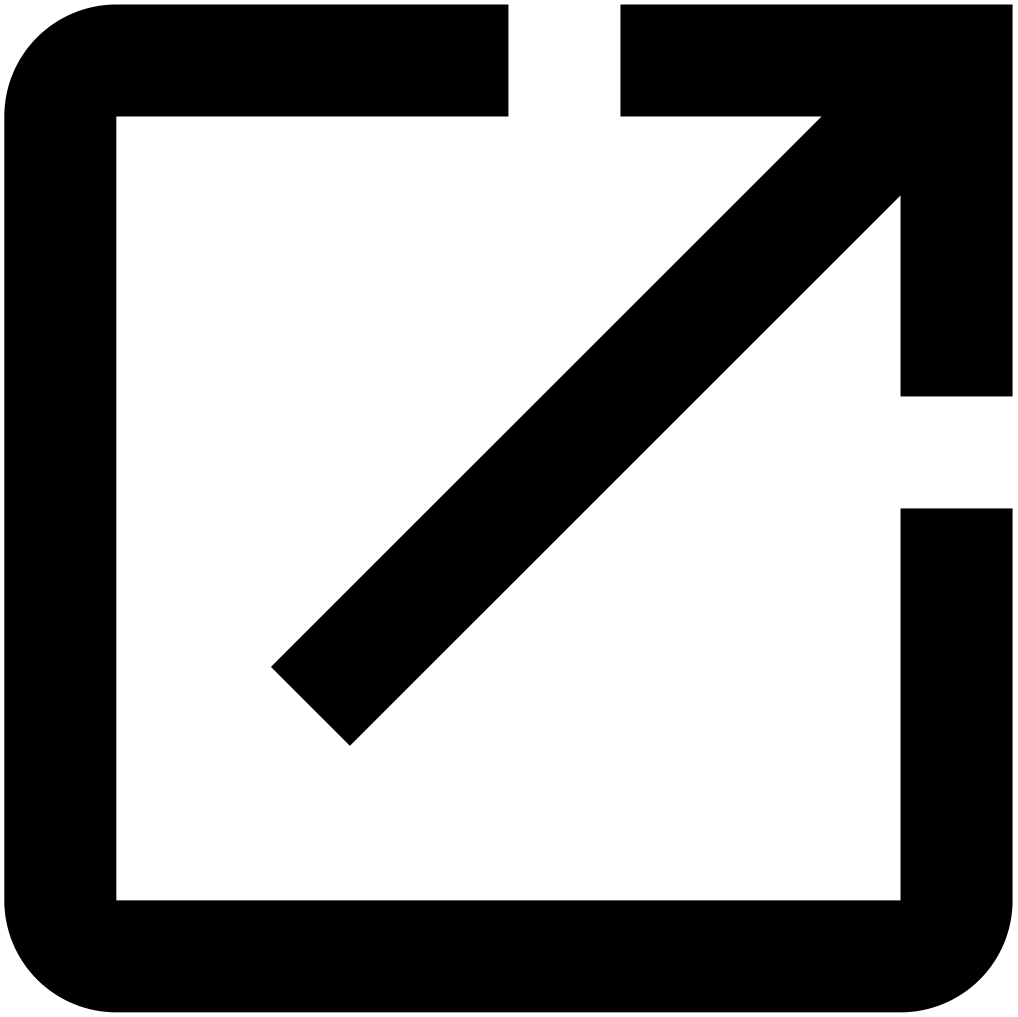


The Nemty Ransomware is the latest cybercrime operation to create a data leak site to punish victims who refuse to pay ransoms.

In 2019, ransomware operators began to use the concerning tactic of stealing victim's files before encrypting computers and then publicly posting these files if the victim does not pay.

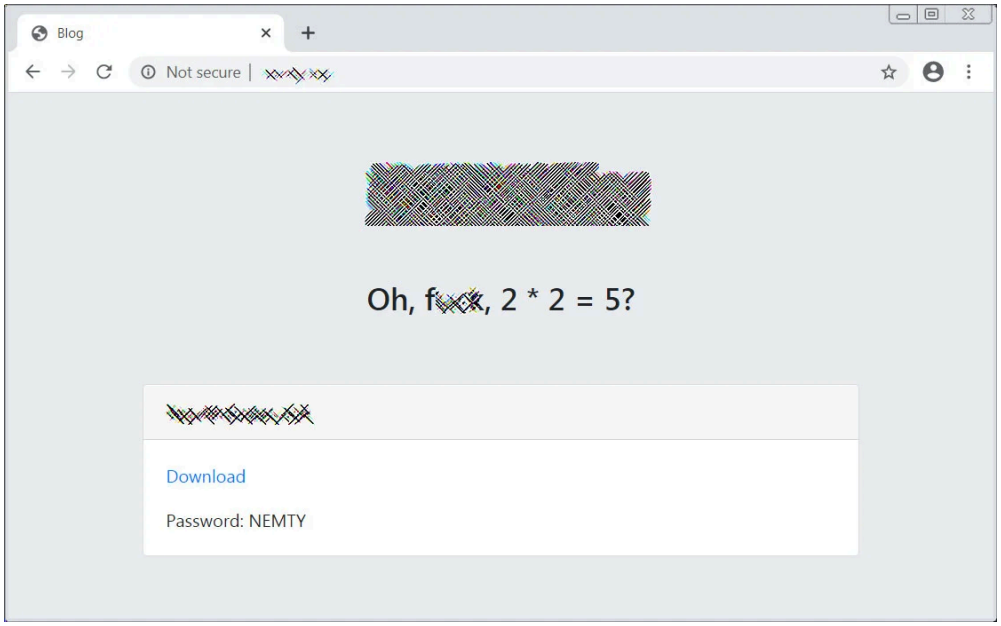
The stealing and publishing of stolen data, which in many cases includes company financials, personal information of employees, and client data, automatically escalated these ransomware attacks into data breaches.


F RTINET
0:00



Once Maze Ransomware followed through with their threat and posted stolen files, other ransomware families such as DoppelPaymer and Sodinokibi started to launch leak sites to extort victims in a similar manner.

In a new site shared with BleepingComputer by Damien, the Nemty Ransomware operators have started to punish their non-paying victims by releasing files that were stolen before devices were encrypted.



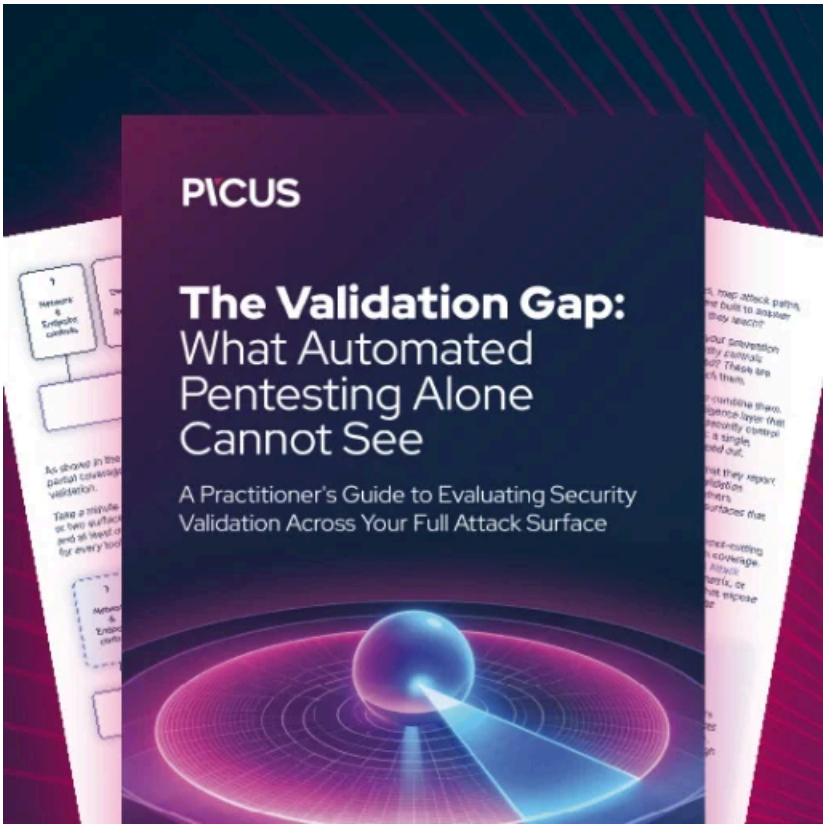
Nemty Leak Site

This blog currently lists a single victim, an American footwear company, and contains a link to 3.5 Gigabytes of files that were allegedly stolen from the company.

As more ransomware operators begin to utilize this extortion tactic, victims will need to consider all ransomware attacks a data breach. This means file noticed with the government, alerting affected people, and sending out breach notifications.

The attackers are hoping that these extra costs and the potential reputation hit may push some victims into paying a ransom.

BleepingComputer has contacted the listed company to confirm if this is indeed their data but had not heard back at this time.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/nemty-ransomware-punishes-victims-by-posting-their-stolen-data/