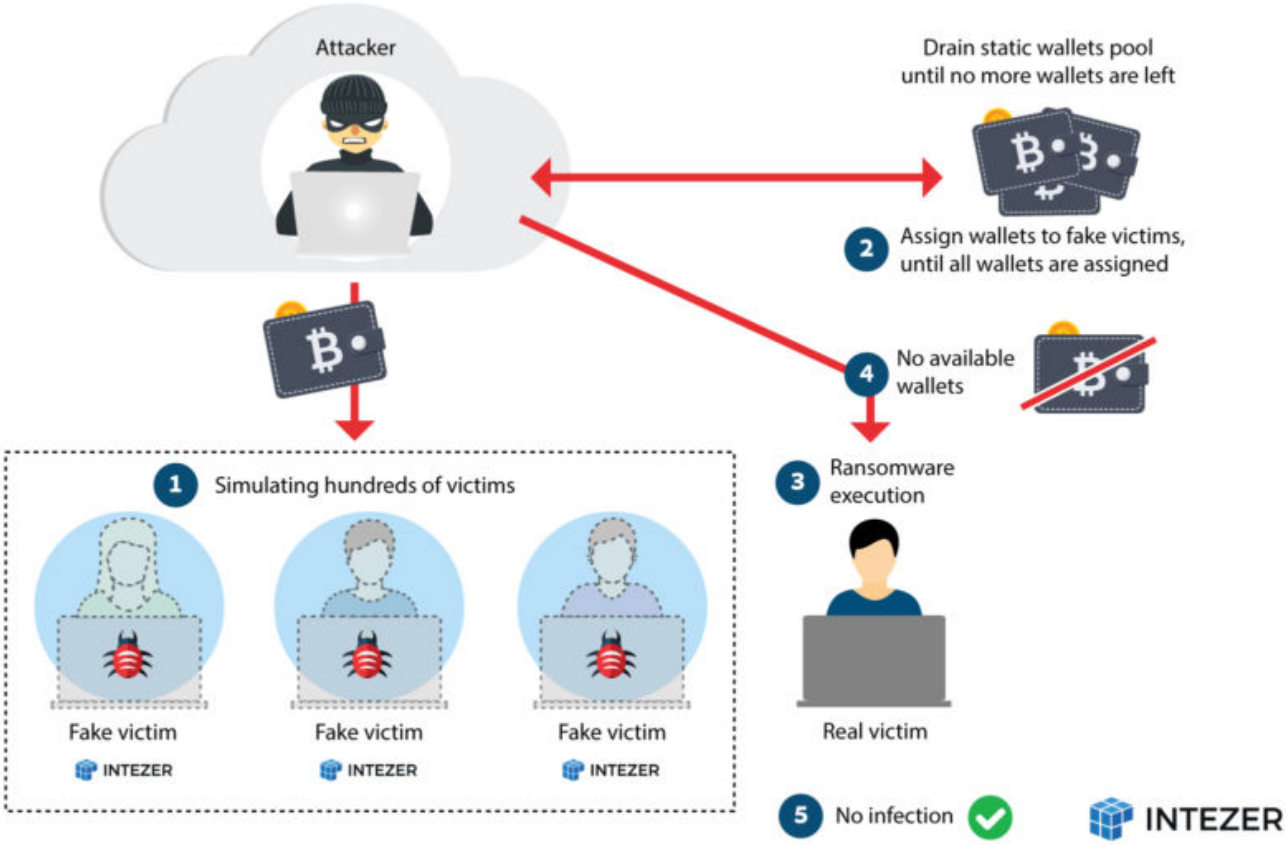
Whitehats use DoS attack to score key victory against ransomware crooks



Enlarge / A diagram showing how a DoS shut down an ongoing ransomware campaign.

reader comments

21 with 14 posters participating

Share this story

Whitehats used a novel denial-of-service hack to score a key victory against ransomware criminals. Unfortunately, the blackhats have struck back by updating their infrastructure, leaving the fight with no clear winner.

Researchers at security firm Intezer performed the DoS

technique against ransomware dubbed QNAPCrypt, a largely undetected strain that, as its name suggests, infects network storage devices made by Taiwan-based QNAP Systems and possibly other manufacturers. The hack spread by exploiting secure shell, (or SSH) connections that used weak passwords. The researchers' analysis found that each victim received a unique bitcoin wallet for sending ransoms, a measure that was most likely intended to prevent the attackers from being traced. The analysis also showed that QNAPCrypt only encrypted devices after they received the wallet address and a public RSA key from the command-and-control server.

Intezer researchers soon noticed two key weaknesses in that process:

1. The list of bitcoin wallets was created in advance, and it was static, meaning there was a finite number of wallets available, and
2. The attackers' infrastructure didn't perform any authentication on devices that connected and claimed to be infected

The weaknesses allowed the researchers to write a script that could emulate an unlimited number of simulated infections. After spoofing infections for nearly 1,100 devices from 15 separate campaigns, the whitehats exhausted the supply of unique bitcoin wallets the attackers had pre-generated. As a result, the campaigns were disrupted, since devices are only encrypted after they receive the wallet. The image above this post shows how the DoS worked.

"Attackers (and malware developers) are eventually like any other developers, and sometimes they have design flaws, exactly like in this case," Ari Eitan, Intezer's VP of research, wrote in an email. "We took advantage of it as defenders. As far as we know, no one did this type of DoS operation in the past."

The empire strikes back

The ransomware developers responded by updating their code to include the wallets and RSA key inside the executable file that gets delivered to targeted machines. This “connectionless” payload, as Intezer researchers called it, allowed the attackers to defeat the DoS, but it came at a cost—they had to walk away from their earlier campaigns.

While the QNAPCrypt operators have lived to fight another day, the whitehats scored another small victory. The updated implant shares almost identical code with Linux.Rex, a ransomware strain that was first spotted in 2016 infecting Drupal servers in ransomware and DDoS operations. That gives Intezer and other defenders new insights and intelligence in defeating a ransomware strain that, so far, has gone largely undetected. Intezer has more details here.

https://arstechnica.com/?p=1534219