New Yanluowang Ransomware Used in Targeted Attacks

By About the Author

Archived: 2026-04-05 14:48:27 UTC

The Symantec Threat Hunter Team, a part of Broadcom Software, has uncovered what appears to be a new ransomware threat called Yanluowang that is being used in targeted attacks.

In a recent attempted ransomware attack against a large organization, Symantec obtained a number of malicious files that, upon further investigation, revealed the threat to be a new, if somewhat underdeveloped, ransomware family.

The Threat Hunter Team first spotted suspicious use of AdFind, a legitimate command-line Active Directory query tool, on the victim organization's network. This tool is often abused by ransomware attackers as a reconnaissance tool, as well as to equip the attackers with the resources that they need for lateral movement via Active Directory. Just days after the suspicious AdFind activity was observed on the victim organization, the attackers attempted to deploy the Yanluowang ransomware.

Before the ransomware is deployed on a compromised computer, a precursor tool carries out the following actions:

- Creates a .txt file with the number of remote machines to check in the command line
- Uses Windows Management Instrumentation (WMI) to get a list of processes running on the remote machines listed in the .txt file
- Logs all the processes and remote machine names to processes.txt

The Yanluowang ransomware is then deployed and carries out the following actions:

- Stops all hypervisor virtual machines running on the compromised computer
- Ends processes listed in processes.txt, which includes SQL and back-up solution Veeam
- Encrypts files on the compromised computer and appends each file with the .yanluowang extension
- Drops a ransom note named README.txt on the compromised computer

The ransom note dropped by Yanluowang warns victims not to contact law enforcement or ransomware negotiation firms. If the attackers' rules are broken the ransomware operators say they will conduct distributed denial of service (DDoS) attacks against the victim, as well as make "calls to employees and business partners." The criminals also threaten to repeat the attack "in a few weeks" and delete the victim's data.

Protection

File based:

- Ransom.Yanluowang

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise

- d11793433065633b84567de403c1989640a07c9a399dd2753aaf118891ce791c
- 49d828087ca77abc8d3ac2e4719719ca48578b265bbb632a1a7a36560ec47f2d
- 2c2513e17a23676495f793584d7165900130ed4e8cccf72d9d20078e27770e04

Source: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/yanluowang-targeted-ransomware