Yanluowang ransomware operation matures with experienced affiliates

bleepingcomputer.com/news/security/yanluowang-ransomware-operation-matures-with-experienced-affiliates/

Ionut Ilascu

By
Ionut Ilascu

- November 30, 2021
- 06:56 AM
- 0

An affiliate of the recently discovered Yanluowang ransomware operation is focusing its attacks on U.S. organizations in the financial sector using BazarLoader malware in the reconnaissance stage.

Based on observed tactics, techniques, and procedures, the threat actor is experienced with ransomware-as-a-service (RaaS) operations and may be linked with the Fivehands group.

Fivehands ransomware connection

Researchers at Symantec, a division of Broadcom Software, note that the actor has been hitting higher-profile targets in the U.S. since at least August.

While its interest is in financial institutions, the Yanluowang ransomware affiliate has also targeted companies in the manufacturing, IT services, consultancy, and engineering sectors.

Looking at the tactics, techniques, and procedures (TTPs), the researchers noticed a possible connection to older attacks with the Thieflock, a ransomware operation developed by the Fivehands group.

Fivehands ransomware itself is relatively new on the scene, becoming known in April - first in a report from Mandiant, who is tracking its developer as UNC2447, and then in an alert from CISA.

At the time, Mandiant said that UNC2447 showed “advanced capabilities to evade detection and minimize post-intrusion forensics,” and that its affiliates had been deploying RagnarLocker ransomware.

Symantec notes that the link found between recent Yanluowang attacks and older ones with Thieflock is tentative, as it relies on several TTPs found in Fivehands ransomware attacks, such as:

- the use of custom password recovery tools and open-source ones (e.g. GrabFF)
- using open-source network scanning tools (e.g. SoftPerfect Network Scanner)
- using the S3 Browser and Cent browser to upload and download data

“This link begs the question of whether Yanluowang was developed by Canthroid [a.k.a. Fivehands]. However, analysis of Yanluowang and Thieflock does not provide any evidence of shared authorship. Instead, the most likely hypothesis is that these Yanluowang attacks may be carried out by a former Thieflock affiliate,” the researchers say.

Tools of the trade

After gaining access to the target network, the attacker uses PowerShell to download tools, such as the BazarLoader malware to help with moving laterally.

BazarLoader is delivered to corporate targets by the TrickBot botnet, which also spreads Conti ransomware. More recently, TrickBot operators started to help rebuilding the Emotet botnet.

The Yanluowang threat actor enables the remote desktop service (RDP) from the registry and installs the ConnectWise tool for remote access.

The researchers say that the affiliate discovers systems of interest with the AdFind tool - to query the Active Directory, and SoftPerfect Network Scanner - to find hostnames and network services.

Several tools are used to steal credentials from the browsers (Firefox, Chrome, Internet Explorer) of compromised machines: GrabFF, GrabChrome, BrowserPassView.

Symantec's researchers also noticed that the attacker used KeeThief to steal the master key for the KeePass password manager, a screen capture tool, and the data exfiltration utility Filegrab.

In a previous report about Yanluowang attacks, the company said that the hackers threatened with distributed denial-of-service (DDoS) and data wiping attacks if the victim did not comply with the demands.

Today's report on the Yanluowang affiliate includes indicators of compromise for the tools and malware used in the attack.

Related Articles:

Free decryptor released for Yanluowang ransomware victims

BlackCat/ALPHV ransomware asks $5 million to unlock Austrian state

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

New 'Cheers' Linux ransomware targets VMware ESXi servers

- Affiliates
- FiveHands
- Ransomware
- Yanluowang

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.

- Previous Article
- Next Article

You may also like: