Threat Hunter Team
Symantec

POSTED: 30 NOV, 2021 | 3 MIN READ |
THREAT INTELLIGENCE

SUBSCRIBE FOLLOW

SHARE

Yanluowang: Further Insights on New Ransomware Threat

At least one attacker now using Yanluowang may have previously been linked to Thieflock ransomware operation.

Yanluowang, the ransomware recently discovered by Symantec, a division of Broadcom Software, is now being used by a threat actor that has been mounting targeted

uses a n

Thiefloc

affiliate v

The atta

have als

enginee

Lateral movement

In most cases, PowerShell is used to download tools to compromised systems including BazarLoader to assist in reconnaissance. The attackers then enable RDP via registry to enable remote access. After gaining initial access, the attackers usually deploy ConnectWise (formerly known as ScreenConnect), a legitimate remote access tool.

In order to perform lateral movement and identify systems of interest, such as the victim's Active Directory server, the attackers deploy Adfind, a free tool that can be used to query Active Directory, and SoftPerfect Network Scanner (netscan.exe), a publicly available tool used for discovery of hostnames and network services.

The next phase of the attack is credential theft and the attackers use a wide range of credential-stealing tools, including:

- GrabFF: A tool that can dump passwords from Firefox
- GrabChrome: A tool that can dump passwords from Chrome
- BrowserPassView: A tool that can dump passwords from Internet Explorer and a number of other browsers

Along with these tools, the attackers also use a number of open-source tools such as KeeThief, a PowerShell script to copy the master key from KeePass. In some cases, customized versions of open-source credential-dumping tools were also observed (secretsdump.exe). Credentials were also dumped from the registry.

In addition, the attackers have also used a number of other data capture tools, including a screen capture tool and a file exfiltration tool (filegrab.exe). Cobalt Strike Beacon was also deployed against at least one targeted organization.

Other tools used include ProxifierPE, which can be used to proxy connections back to attacker-controlled infrastructure, and the free, Chromium-based Cent web browser.

The Thieflock connection

There is a tentative link between these Yanluowang attacks and older attacks involving Thieflock, ransomware-as-a-service developed by the Canthroid (aka Fivehands) group. Sev

Thieflock attacks, inclu

- Use of custom pas

  password dumpin

- Use of open-sourc
- Use of free browse

This link begs the question of whether Yanluowang was developed by Canthroid. 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.

Protection

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

Indicators of Compromise

a710f573f73c163d54c95b4175706329db3ed89cd9337c583d0bb24b6a384789 – NetScan

2c2513e17a23676495f793584d7165900130ed4e8cccf72d9d20078e27770e04 – Adfind

43f8a66d3f3f1ba574bc932a7bc8e5886fbeeab0b279d1dea654d7119e80a494 – BazarLoader

9aa1f37517458d635eae4f9b43cb4770880ea0ee171e7e4ad155bbdee0cbe732 – Veeamp

85fb8a930fa7f4c32c8af86aa204eb4ea4ae404e670a8be17e7ae0adf37a9e2e – GrabFF

e4942fde1cd7f2fcfb522090fd16298bce247295fe99182aecf7b10be3f5dc53 – ConnectwiseInstaller

fe38912d64f6d196ac70673cd2edbdbc1a63e494a2d7903546a6d3afa39dc5c4 – WmiExecAgent

c77ff8e3804414618abeae394d3003c4bb65a43d69c57c295f443aeb14eaa447 – NetScan

2fc5bf9edcfa19d48e235315e8f571638c99a1220be867e24f3965328fe94a03 – Secretsdump

4ff503258e23d609e0

GrabFile

1c543ea5c50ef8b0b4

GrabChrome

0b9219328ebf065db

OpenChromeDumps

b556d90b30f217d5ef20ebe3f15cce6382c4199e900b5ad2262a751909da1b34 – BrowserPassView

5e03cea2e3b875fdbf1c142b269470a9e728bcfba1f13f4644dcc06d10de8fb4 – ConHost

49d828087ca77abc8d3ac2e4719719ca48578b265bbb632a1a7a36560ec47f2d – Yanluowang

myeeducationplus.com

185.53.46.115

Symantec by Broadcom Symantec Enterprise Blogs

YOU MIGHT ALSO ENJOY

2 MIN READ

New Yanluowang Ransomware Used in Targeted Attacks

New arrival to the targeted ransomware scene appears to be still in development.

About the Author

Threat Hunter Team

Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.

Want to

We encourage you to s

POSTED: 22 OCT, 2024 | 5 MIN READ

Exposing the Danger Within: Hardcoded Cloud Credentials in Popular Mobile Apps

POSTED: 17 OCT, 2024 | 3 MIN READ

Ransomware: Threat Level Remains High in Third Quarter

POSTED: 2 OCT, 2024 | 5 MIN READ

Stonefly: Extortion Attacks Continue Against U.S. Targets

POSTED: 12 SEP, 2024 | 3 MIN READ

Ransomware: Attacks Once More Nearing Peak Levels

SUBSCRIBE FOLLOW

Privacy Policy Cookie Policy Data Processing and Data Transfers Supplier Responsibility Terms of Use Sitemap