مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

# Cicada 3301 Ransomware Campaign

Tracking #:432316215

Date:03-09-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a new ransomware group, Cicada 3301, has emerged on the cyber landscape, first observed in June 2024 and already listed 23 victims on its extortion portal since mid-June.

## TECHNICAL DETAILS:

A new ransomware-as-a-service operation called Cicada 3301 has emerged, targeting both Windows and Linux/ESXi hosts. The group uses a Rust-based ransomware with similarities to the defunct ALPHV/BlackCat group. Cicada 3301 gains initial access by brute-forcing ScreenConnect credentials using a botnet called "Brutus". The ransomware encrypts files using ChaCha20 and RSA, and appends encrypted files with a unique extension. Similarities to ALPHV include the use of Rust, ChaCha20, and nearly identical code for shutting down VMs and removing snapshots. The timeline of events suggests a possible connection to the demise of BlackCat and the emergence of Brutus.The IP address used by the threat actor, 91.92.249[.]203, has been tied to the Brutus botnet.

**Technical Analysis:**

- The ransomware is an ELF binary written in Rust version 1.79.0
- It uses various parameters to control functionality like sleep timers, printing encryption progress, and shutting down VMs without snapshots
- The key parameter is used to decrypt the ransomware note. If invalid, the binary will terminate.
- ChaCha20 is used for symmetric encryption of files. RSA is used to encrypt the ChaCha20 key with a hardcoded public key.
- Encrypted files have the extension appended along with the RSA-encrypted ChaCha20 key.

**Similarities to ALPHV Ransomware:**

- Both are written in Rust
- Use ChaCha20 for encryption
- Have almost identical commands to shut down VMs and remove snapshots
- Use the same naming convention for ransom notes
- Code to decrypt the ransom note is nearly identical

**YARA Rule for Cicada3301 Threat Hunting:**

```
rule elf_cicada3301{

    meta:
        author = "Author Name"
        description = "Detect ESXi ransomware by the group Cicada3301"
        date = "2024-08-31"

    strings:
        $x1 = "no_vm_ss" nocase wide ascii
        $x2 = "linux_enc" nocase wide ascii
        $x3 = "nohup" nocase wide ascii
        $x4 = "snapshot.removeall" nocase wide ascii
```

```
        $x5 = {65 78 70 61 6E 64 20 33 32 2D 62 79 74 65 20 6B} //Use of ChaCha20 constant
expand 32-byte k

    condition:
        uint16(0) == 0x457F
        and filesize < 10000KB
        and (all of ($x*))
}
```

## RECOMMENDATIONS:

- Implement strong access controls and multi-factor authentication for remote access solutions like ScreenConnect.
- Monitor for brute-force attempts and suspicious login activity on remote access systems.
- Ensure robust backup and recovery procedures are in place, with offline/air-gapped backups.
- Implement Advanced Threat Detection Tools: Utilize intrusion detection systems and endpoint protection platforms that can detect and prevent ransomware infections.
- Regularly Update Software and Systems: Ensure all software and systems are up-to-date with the latest security patches to prevent vulnerabilities that ransomware can exploit.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

## REFERENCES:

- https://www.truesec.com/hub/blog/dissecting-the-cicada