Hive Pro

Threat Level

Red

HiveForce Labs

# THREAT ADVISORY

## ATTACK REPORT

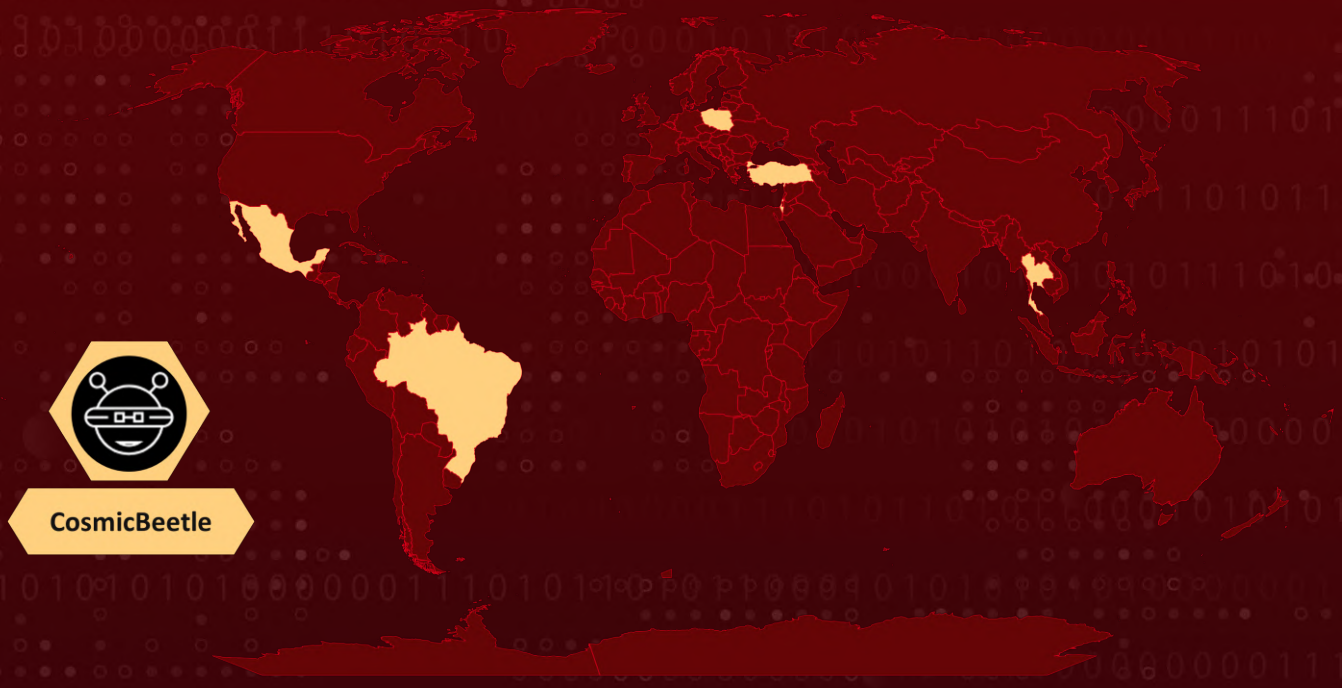
# Spacecolon Toolset Fuels Surge in Scarab Ransomware Attacks


| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| August 24, 2023 | A1 | TA2023344 |

# Summary

**First Seen:** May 2020
**Malware:** Scarab Ransomware, Spacecolon
**Threat Actor:** CosmicBeetle
**Attack Region:** Thailand, Israel, Poland, Brazil, Turkey, Mexico
**Targeted Industry:** Hospital, Hospitality, Insurance, Government, Entertainment, Education
**Attack:** CosmicBeetle, an active cyber threat group, has been utilizing a malicious toolset called Spacecolon in an ongoing campaign. This toolset is used to distribute variants of the Scarab ransomware by targeting vulnerable web servers and exploiting weaknesses in RDP credentials.

## Attack Regions




## CVEs

| CVE | NAME | AFFECTED PRODUCT | ZERO -DAY | CISA KEV | PATCH |
|---|---|---|---|---|---|
| CVE-2020-1472 | Microsoft Netlogon Privilege Escalation Vulnerability (ZeroLogon) | Microsoft Netlogon | ✗ | ✓ | ✓ |

# Attack Details

**#1** The malicious toolset known as Spacecolon is currently being utilized by the group CosmicBeetle in an ongoing campaign to distribute various versions of the Scarab ransomware. This campaign targets vulnerable web servers and employs tactics such as exploiting weaknesses in RDP credentials through brute force methods. Notably, the Spacecolon code includes a significant number of Turkish language strings, implying a potential association with Turkish-speaking developers. The origins of Spacecolon can be traced back to at least May 2020.

**#2** Spacecolon consists of three core Delphi components: ScHackTool, ScInstaller, and ScService. The primary orchestrator component is ScHackTool, which enables CosmicBeetle to deploy the other components. On the other hand, ScInstaller has a singular function - installing ScService. ScService operates as a backdoor, offering CosmicBeetle the means to execute customized commands, download and run payloads, and gather system information from compromised machines.

**#3** In terms of initial access, CosmicBeetle exploits the CVE-2020-1472 vulnerability (also known as ZeroLogon) or employs a custom .NET tool to gain entry. This is accomplished through brute-forcing RDP credentials as well. Beyond these initial access methods, victims of Spacecolon are susceptible to the techniques employed by CosmicBeetle. The geographic distribution of victims reveals a concentration in several countries, including Thailand, Israel, Poland, Brazil, Turkey, and Mexico.

**#4** The attacks aim to utilize ScService's access to introduce a variant of the Scarab ransomware. Scarab, coded in Delphi, shares similarities with Buran and VegaLocker ransomware. It uses an embedded configuration similar to **Zeppelin** ransomware, determining encrypted file details, filenames, targeted extensions, and ransom messages. CosmicBeetle's financial motives are strengthened by ransomware deploying clipper malware. This monitors the clipboard, altering crypto wallet addresses to divert funds.

# Recommendations

**ZeroLogon Vulnerability Mitigation:** Prioritize **patching** systems to address the CVE-2020-1472 vulnerability (ZeroLogon) and prevent unauthorized access. Employ network segmentation to contain potential breaches and restrict lateral movement.

**Robust Backup Strategy:** Establish regular backups for all assets to guarantee their comprehensive security. Employ the 3-2-1-1 backup framework and utilize specialized tools to enhance backup durability and accessibility.

# Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| **TA0043** Reconnaissance | **TA0042** Resource Development | **TA0001** Initial Access | **TA0002** Execution |
| **TA0003** Persistence | **TA0005** Defense Evasion | **TA0006** Credential Access | **TA0007** Discovery |
| **TA0009** Collection | **TA0010** Exfiltration | **TA0011** Command and Control | **TA0040** Impact |
| **T1595.002** Vulnerability Scanning | **T1583.001** Domains | **T1587.001** Malware | **T1587.003** Digital Certificates |
| **T1190** Exploit Public-Facing Application | **T1059.003** Windows Command Shell | **T1059.001** PowerShell | **T1059.005** Visual Basic |
| **T1053.005** Scheduled Task | **T1133** External Remote Services | **T1547.001** Registry Run Keys / Startup Folder | **T1136.001** Local Account |
| **T1543.003** Windows Service | **T1078.003** Local Accounts | **T1140** Deobfuscate/Decode Files or Information | **T1070.001** Clear Windows Event Logs |
| **T1003.001** LSASS Memory | **T1082** System Information Discovery | **T1115** Clipboard Data | **T1071.001** Web Protocols |
| **T1041** Exfiltration Over C2 Channel | **T1095** Non-Application Layer Protocol | **T1529** System Shutdown/Reboot | **T1486** Data Encrypted for Impact |

# Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| **Path** | %USERPROFILE%\Music\, %ALLUSERSPROFILE%\ |
| **Mutex** | 46E4D4E6-8B81-84CA-93DA-BB29377B2AC0, 7F57FB1B-3D23-F225-D2E8-FD6FCF7731DC |

| TYPE | VALUE |
| --- | --- |
| SHA1 | 40B8AF12EA6F89DB6ED635037F468AADEE7F4CA6, 1CB9320C010065E18881F0AAA0B72FC7C5F85956, EF911DB066866FE2734038A35A3B298359EDABCE, 0A2FA26D6EAB6E9B74AD54D37C82DEE83E80BDD7, B916535362E2B691C6AEF76021944B4A23DDE190, 95931DE0AA6D96568ACEBC11E551E8E1305BF003, 6700AFB03934B01B0B2A9885799322307E3299D5, 4B07391434332E4F8FAADF61F288E48389BCEA08, B9CF8B18A84655D0E8EF1BB14C60763CEFFF9686, E2EAA1EE0B51CAF803CEEDD7D3452577B6FE7A8D, 8F1374D4D6CC2899DA1251DE0325A7095E719EDC, 2E4A85269BA1FDBA74A49B0DF3397D6E4397DB78, 7AA1A41F561993C4CCA9361F9BAEF2B00E31C05D, 7BC7EEAAF635A45BC2056C468C4C42CC4C7B8F05 |
| IPv4 | 3.76.107[.]228, 87.251.64[.]19, 87.251.64[.]57, 87.251.67[.]163, 162.255.119[.]146, 185.170.144[.]190, 185.202.0[.]149, 193.37.69[.]152, 193.37.69[.]153, 193.149.185[.]23, 206.188.196[.]104, 213.232.255[.]131 |
| Domains | u.piii[.]net, up.awiki[.]org, ss.688[.]org, akamaicdnup[.]com, b.688[.]org, sys.688[.]org, update.inet2[.]org, up.vctel[.]com, u.cbu[.]net, update.cbu[.]net, cdnupdate[.]net |

## Patch Link

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1472

## References

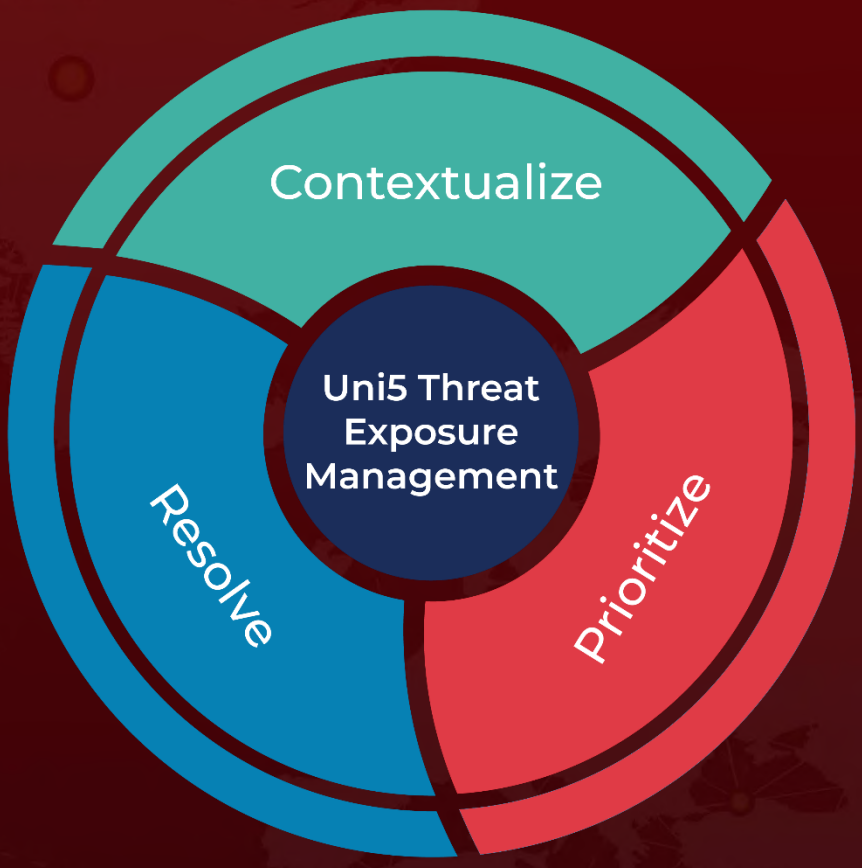
https://www.welivesecurity.com/en/eset-research/scarabs-colon-izing-vulnerable-servers/

https://www.hivepro.com/zeppelin-ransomware-target-organization-in-europe-and-usa/

# What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.




REPORT GENERATED ON

**August 24, 2023 • 7:00 AM**



More at www.hivepro.com