Hive Pro

Threat Level

Amber

Hiveforce Labs

# THREAT ADVISORY

## ACTOR REPORT

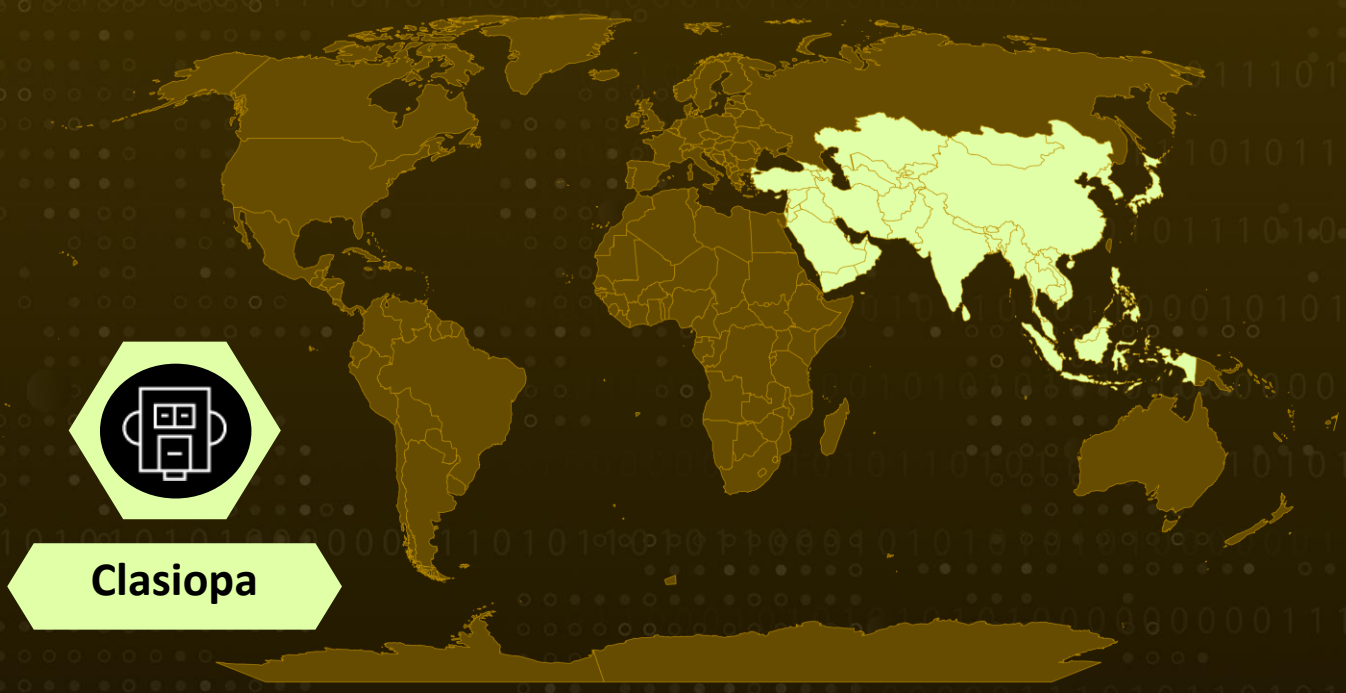
# New Attack Group Clasiopa Targets Materials Research Organization in Asia with Custom Malware

| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| February 23, 2023 | A1 | TA2023100 |

# Summary

**First Appearance:** 2023
**Actor Name:** Clasiopa
**Target Region:** Asia
**Target Sector:** Materials research

## Actor Map



# Actor Details

**#1**

A new attack group called Clasiopa has been observed targeting a materials research organization in Asia using a distinct toolset that includes a custom malware called Backdoor.Atharvan. It is unclear where Clasiopa is based or who they act on behalf of, although there are indications that imply the group may have links to India. The attackers gain access through brute force attacks on public-facing servers and use multiple backdoors to build lists of file names and exfiltrate them.

**#2**

The attackers used legitimate software packages, Agile DGS and Agile FD servers, developed by Jiangsu for document security and protection in transit. The attackers also used Lilith RAT, Thumbsender hacking tool, and a custom proxy tool. The Atharvan RAT contacts a hardcoded C&C server in South Korea and uses its own simplistic HTTP parser and encryption algorithm to fetch and execute commands.

## Actor Group

| NAME | ORIGIN | TARGET REGIONS | TARGET INDUSTRIES |
|---|---|---|---|
| Clasiopa | Unknown<br>**MOTIVE**<br>Espionage | Asia | Materials research |

# Recommendations

**Security Leaders**

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

**Security Engineers**

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

## Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| TA0002 Execution | TA0005 Defense Evasion | TA0003 Persistence | TA0011 Command and Control |
| TA0010 Exfiltration | TA0001 Initial Access | TA0006 Credential Access | TA0004 Privilege Escalation |
| T1098 Account Manipulation | T1090 Proxy | T1059 Command and Scripting Interpreter | T1059.001 PowerShell |
| T1071 Application Layer Protocol | T1204.002 Malicious File | T1071.001 Web Protocols | T1110 Brute Force |
| T1204 User Execution | T1190 Exploit Public-Facing Application | T1586 Compromise Accounts | T1219 Remote Access Software |
| T1055 Process Injection | T1036 Masquerading | T1569 System Services | T1562 Impair Defenses |

# Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| SHA256 | f93ddb2377e02b0673aac6d540a558f9e47e611ab6e345a39fd9b1ba9f37cd22<br>c94c42177d4f9385b02684777a059660ea36ce6b070c2dba367bf8da484ee275<br>95f76a95adcfdd91cb626278006c164dcc46009f61f706426b135cdcfa9598e3<br>940ab006769745b19de5e927d344c4a4f29cae08e716ee0b77115f5f2a2e3328<br>8aa6612c95c7cef49709596da43a0f8354f14d8c08128c4cb9b1f37e548f083b<br>8023b2c1ad92e6c5fec308cfafae3710a5c47b1e3a732257b69c0acf37cb435b<br>5b74b2176b8914b0c4e6215baab9e96d1e9a773803105cf50dac0427fac79c1b<br>3aae54592fe902be0ca1ab29afe5980be3f96888230d5842e93b3ca230f8d18d<br>38f0f2d658e09c57fc78698482f2f638843eb53412d860fb3a99bb6f51025b07<br>1569074db4680a9da6687fb79d33160a72d1e20f605e661cc679eaa7ab96a2cd<br>0550e1731a6aa2546683617bd33311326e7b511a52968d24648ea231da55b7e5 |
| SHA1 | 8bab70bdfb7f8df0356727d9cb3c6024acb383a2<br>67f9a8047d21b8e8261dce1d699e3377b7abeb5d<br>0a00a6711b190bc7e3a0f2fdfa2351271ba53252 |
| MD5 | 81738405a7783c09906da5c7212e606b<br>7c30ed6a612a1fd252565300c03c7523<br>59ec24539c786e6ac9467dad3183c280 |

# References

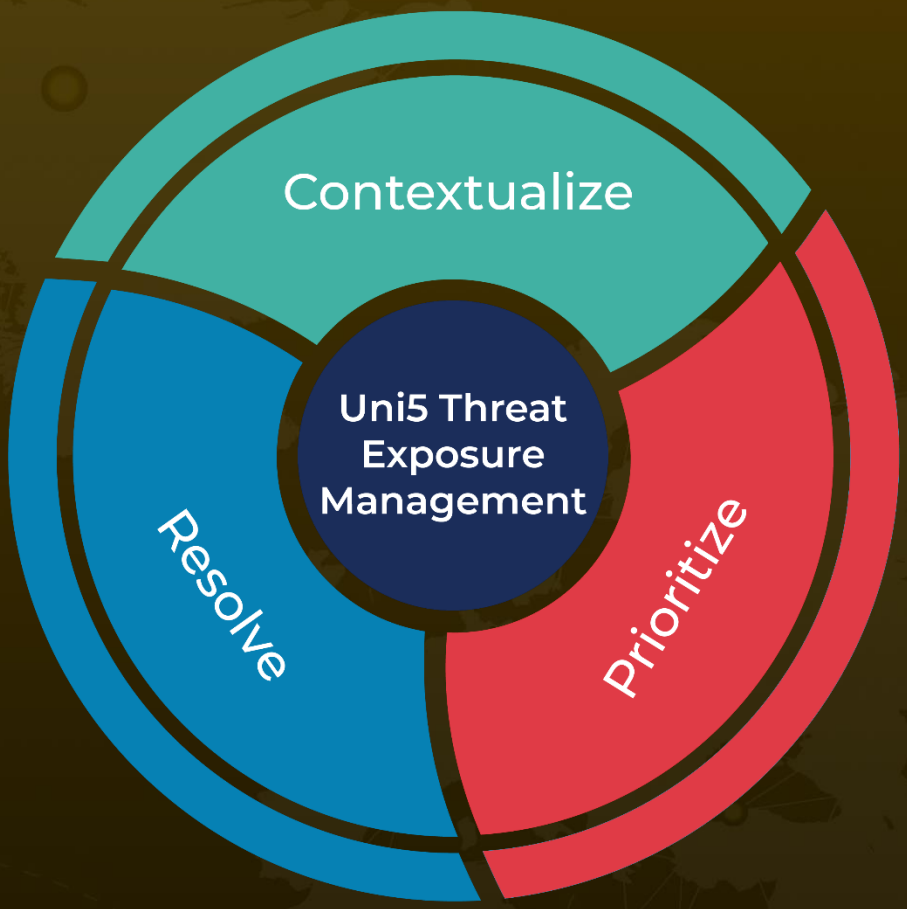

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/clasiopa-materials-research

https://www.bleepingcomputer.com/news/security/clasiopa-hackers-use-new-atharvan-malware-in-targeted-attacks/

# 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

**February 23, 2023 • 11:30 PM**



More at www.hivepro.com