Clasiopa: New Group Targets Materials Research

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

Threat Hunter TeamSymantec

Group uses distinct toolset but there are few clues to its origins.

A hitherto unknown attack group has been observed targeting a materials research organization in Asia. The group, which Symantec calls Clasiopa, is characterized by a distinct toolset, which includes one piece of custom malware (Backdoor.Atharvan). At present, there is no firm evidence on where Clasiopa is based or whom it acts on behalf.

Clasiopa Tactics, Techniques, and Procedures

The infection vector used by Clasiopa is unknown, although there is some evidence to suggest that the attackers gain access through brute force attacks on public facing servers.

Aside from the distinct toolset used, there were a number of attack hallmarks observed:

- The attackers checked the IP addresses of the computers they were on using: https://ifconfig.me/ip
- An attempt was made to disable Symantec Endpoint Protection (SEP) by stopping the SepMasterService. The result of this query was checked and then a second attempt was made to disable SEP using "smc -stop". Note that any commands attempting to stop SEP will only work if the attacker has administrative credentials and the SEP administrator has disabled anti-tamper protection.
- The attackers used multiple backdoors to build lists of file names and exfiltrate them. These lists were exfiltrated either in a Thumb.db file or a Zip archive.
- Sysmon logs were cleared using wsmprovhost.
- All eventlogs were cleared using PowerShell.
- A scheduled task named "network service" was created to list file names.

There is some evidence to suggest that the attackers used two legitimate software packages. One compromised computer was running Agile DGS and Agile FD servers, software developed by Jiangsu. These packages are used for document security and protection in transit. Malicious files were dropped into a folder named “dgs” and one of the backdoors used was renamed from atharvan.exe to agile_update.exe. It is unclear if these software packages are being injected into or installed by the attackers.

HCL Domino (formerly IBM Domino) was also run on a compromised machine in close proximity to the execution of backdoors, although it is unclear if this was a coincidence or not. However, both the Domino and Agile software appear to be using old certificates and the Agile servers use old vulnerable libraries.

Tools Used

- Atharvan: Custom developed remote access Trojan (RAT).
- Lilith: The attackers used modified versions of the publicly available Lilith RAT. The versions used were capable of carrying out the following tasks:
    - Killing the process
    - Restarting the process
    - Modifying the sleep interval
    - Uninstalling the RAT
    - Executing a remote command or PowerShell script
    - Exiting the process
- Thumbsender: Hacking tool which, when it receives a command from a command-and-control (C&C) server will list file names on the computer and save them in a file called Thumb.db before sending them to a specified IP address.
- Custom proxy tool.

Atharvan

Atharvan is so-named because when the malware is run, it creates a mutex named: "SAPTARISHI-ATHARVAN-101" to ensure that only one copy is running.

It will then contact a hardcoded C&C server. The hardcoded C&C addresses seen in one of the samples analyzed to date was for Amazon AWS South Korea (Seoul) region, which is not a common location for C&C infrastructure.

The C&C communications are formatted as HTTP POST requests where the Host header is hardcoded as "update.microsoft.com", e.g.:

POST /update.php HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.105 Safari/537.36 Edg/84.0.522.52

Host: update.microsoft.com

Content-type: application/x-www-form-urlencoded

Content-length: 46

id=Atharvan&code=101&cid=H^[REDACTED]&time=5

The request body includes the following parameters:

- "id": hardcoded string "Atharvan"
- "code": represents request purpose, which can be one of:
  - 101: fetches commands
  - 102: sends command outputs or error messages
  - 103: fetches file body to write when processing command 0x12
- "cid": hardcoded string "H^" followed by the network interface hardware address of the affected computer as 12 hexadecimal digits
- "time": interval between communication attempts
- "msg" (optional): depending on the request purpose as specified using "code" parameter:
  - when the "code" parameter is 102, it includes output of commands or error messages in encrypted form
  - when the "code" parameter is 103, it identifies the file to fetch in non-encrypted form

When encrypting the "msg" value, the malware uses the following encryption algorithm:

```
def encrypt(plaintext):
    return bytes([((2 - byte) & 0xff) for byte in plaintext])
```

The malware uses its own simplistic HTTP parser to extract the body from the server response. The extracted body is decrypted using the following algorithm:

```
def decrypt(ciphertext):
    return bytes([((2 - byte) & 0xff) for byte in ciphertext])
```

When fetching commands, the malware expects the decrypted body to contain a sequence of strings separated by the "\x1A" character.

The first byte of each string specifies the command to execute and the remaining bytes are interpreted as command parameters.

Table 1. Atharvan commands

Command	Description
0x11	Configures interval between communication attempts
0x12	Downloads arbitrary file from specified control server
0x15	Runs arbitrary executable and sends its output to the remote attacker
0x16	Configures communication to use schedule type 0x16
0x17	Configures communication to use schedule type 0x17
0x18	Configures communication to use schedule type 0x18

When configuring a communication schedule, the command parameters specify the times and days for the communication attempts. Several different times can be specified, with the hour and minute of the day encoded.

The days are interpreted as:

- No restrictions (communication schedule type 0x16)
- Bitmask specifying days of month (communication schedule type 0x17)
- Bitmask specifying days of week (communication schedule type 0x18)

This scheduled communication configuration is another unusual feature of the malware and is not commonly seen in malware of this kind.

Attribution

There is currently no firm evidence on where Clasiopa is based or what its motivation is. A Hindi mutex is used in the Atharvan backdoor: "SAPTARISHI-ATHARVAN-101". Atharvan is a legendary Vedic sage of Hinduism. The backdoor also sends a post request to a C&C

server with the arguments:

d=%s&code=%d&cid=%s&time=%dtharvan

In addition to this, one of the passwords used by the attackers for a ZIP archive was “iloveindea1998^_^”.

While these details could suggest that the group is based in India, it is also quite likely that the information was planted as false flags, with the password in particular seeming to be an overly obvious clue.

Protection/Mitigation

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

Indicators of Compromise

If an IOC is malicious and the file available to us, Symantec Endpoint products will detect and block that file.

5b74b2176b8914b0c4e6215baab9e96d1e9a773803105cf50dac0427fac79c1b – Backdoor.Atharvan

8aa6612c95c7cef49709596da43a0f8354f14d8c08128c4cb9b1f37e548f083b – Backdoor.Atharvan

95f76a95adcfdd91cb626278006c164dcc46009f61f706426b135cdcfa9598e3 – Lilith

940ab006769745b19de5e927d344c4a4f29cae08e716ee0b77115f5f2a2e3328 – Lilith

38f0f2d658e09c57fc78698482f2f638843eb53412d860fb3a99bb6f51025b07 – Lilith

c94c42177d4f9385b02684777a059660ea36ce6b070c2dba367bf8da484ee275 – Thumbsender

f93ddb2377e02b0673aac6d540a558f9e47e611ab6e345a39fd9b1ba9f37cd22 – Custom Proxy Tool

3aae54592fe902be0ca1ab29afe5980be3f96888230d5842e93b3ca230f8d18d – Backdoor

0550e1731a6aa2546683617bd33311326e7b511a52968d24648ea231da55b7e5 – Backdoor

8023b2c1ad92e6c5fec308cfafae3710a5c47b1e3a732257b69c0acf37cb435b – Hacktool

1569074db4680a9da6687fb79d33160a72d1e20f605e661cc679eaa7ab96a2cd – Hacktool

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 comment on this post?