2024-06-20

# HUNTER EMERGING THREATS

## SPECTRE RAT

The Spectre remote access trojan (RAT) is modular malware that was first seen in September of 2020, being available as a malware-as-a-service (MaaS) program. **Spectre RAT** is developed in C++ and gives the operator the means to employ techniques such as remotely executing commands and payloads, manipulation of processes, downloading and uploading of files, and stealing information. The RAT is made up of three parts, or modules; the core bot module, the stealer module, and the hidden applications module. Since the RAT is available as a malware-as-a-service to prospective operators, [Intel 471](https://intel471.com/)'s threat intelligence shows the malware has impacted entities within industries such as cryptocurrency, cloud services, gaming, marketing and sales consulting, and telecommunications. With recent campaign activity targeting United States industries being discovered and the evolution of **Spectre RAT** since its inception, it is important that analysts assess, understand and prepare for this remote access trojan going forward.

# THREAT SUMMARY

The Spectre remote access trojan (RAT) is modular malware that was first seen in September of 2020, being available as a malware-as-a-service (MaaS) program. **Spectre RAT** is developed in C++ and gives the operator the means to employ techniques such as remotely executing commands and payloads, manipulation of processes, downloading and uploading of files, and stealing information. The RAT is made up of three parts, or modules; the core bot module, the stealer module, and the hidden applications module. Since the RAT is available as a malware-as-a-service to prospective operators, [Intel 471](https://intel471.com/)'s threat intelligence shows the malware has impacted entities within industries such as cryptocurrency, cloud services, gaming, marketing and sales consulting, and telecommunications. With recent campaign activity targeting United States industries being discovered and the evolution of **Spectre RAT** since its inception, it is important that analysts assess, understand and prepare for this remote access trojan going forward.

**Intel 471 References**:

[TITAN Finished Intel Report: New phishing attacks linked to The Com deploy Spectre RAT malware]
(https://titan.intel471.com/report/fintel/418738e3c9607078ca741c06a6c0bcc1)

# SYNOPSIS

**Spectre RAT** is a remote access trojan (RAT) that gives operators the ability to gain administrative privileged access and control of a target computer. It has been observed to be delivered in the past via phishing emails with malicious attachments and malvertising campaigns; however, recent operators have been using social-engineering techniques to victimize users to download a malicious .SCR file and initiate the infection chain. These interactions have taken place within live chat sessions where operators communicated a maliciously crafted IMG link (redirecting to download the .SCR file). **Spectre RAT**  is considered modular malware, due to the makeup of the malware consisting of the bot, the stealer module and the hidden application module.

The core module, or the bot, gives operators the means to command or process execution, download and upload files, achieve persistence and self-update. The stealer module can exfiltrate any data collected from the compromised system to the C2 server;this module includes the functionality of a keylogger, credential harvester, screenshot collector and clipboard hijacker. Finally there is the hidden application module, which gives operators the capability to have a hidden remote interactive browser or shell session with the victimâ€™s machine; , observed to be conducted via a created hidden desktop. With multiple versions being created, currently at 9.0, the functionalities seen in this version may evolve in the near future and it is crucial to be aware of how they may do so.

# HUNT PACKAGES

**WMIC WINDOWS INTERNAL DISCOVERY AND ENUMERATION**
https://hunter.cyborgsecurity.io/research/hunt-package/bc0fd59c-4217-46a7-a167-764727118567

**AUTORUN OR ASEP REGISTRY KEY MODIFICATION**
https://hunter.cyborgsecurity.io/research/hunt-package/8289e2ad-bc74-4ae3-bfaa-cdeb4335135c

**POSSIBLE DELAYED EXECUTION IN COMMANDLINE ARGUMENT USING PING.EXE AND LOOPBACK ADDRESS**
https://hunter.cyborgsecurity.io/research/hunt-package/a2e40a77-69b7-4cdc-bf89-e04288bbe2c5

**LNK FILE CREATED IN STARTUP FOLDER – POTENTIAL INDIRECT MALWARE EXECUTION**
https://hunter.cyborgsecurity.io/research/hunt-package/abe99d8c-522c-4fe0-8377-07a51313c063

**SUSPICIOUS EXECUTABLE OR SCRIPTS LAUNCHED IN COMMON CONFIGURATION OR SYSTEM RELATED FOLDERS**
https://hunter.cyborgsecurity.io/research/hunt-package/F2DD3A46-1C5D-42D3-B3FA-5BEC58D75E0B

**FILE CREATED IN STARTUP FOLDER**
https://hunter.cyborgsecurity.io/research/hunt-package/8fedb48c-396b-4cd5-9483-69d7fc3eecee

**SCHEDULED TASK EXECUTING FROM ABNORMAL LOCATION**
https://hunter.cyborgsecurity.io/research/hunt-package/09a380b3-45e5-408c-b14c-3787fa48d783

**RELATED LINKS**
Sign up for free HUNTER access
Spectre RAT Emerging Threat Collection

# MITRE CONTEXT

- Tactic Names:
  - Execution
  - Initial Access
  - Defense Evasion
  - Persistence
  - Discovery
- Technique Names:
  - Windows Management Instrumentation
  - Time Based Evasion
  - Scheduled Task
  - Registry Run Keys / Startup Folder
  - Spearphishing Attachment
  - System Network Configuration Discovery
- Threat Names:
  - Spectre RAT

# REFERENCES

1. https://titan.intel471.com/report/fintel/418738e3c9607078ca741c06a6c0bcc1
2. https://x.com/DailyDarkWeb/status/1740825011932573712