Quorum Cyber

Threat Intelligence HiatusRAT Malware

TLP Status: White

Prepared by: Mike Pini

+44 333 444 0041
quorumcyber.com
Verdant, 2 Redheughs Rigg, Edinburgh, United Kingdom, EH12 9DQ

Microsoft Solutions Partner

Table of Contents

Document Control

Revision History

Version		Date	Summary of Changes
0.1		01/02/2023	Initial Report
1.0		13/04/2023	Final PDF Formatting

Related Documents

The following documents are either referenced within, or are related to, the content of this document:

Document Name	Date	Version
-	-	-

HiatusRAT

Overview

Cyber threat actors have debuted a new router malware variant, HiatusRAT, which was initially detected to have targeted end-of-life DrayTek Vigor 2960 and 3600 series routers as part of Operation Hiatus[1]. Black Lotus Labs assessed that the goal of the attacks was data theft and intelligence-gathering, stating that HiatusRAT malware operators launched the campaign in July 2022.

The campaign consisted of three main components: a bash script for post-exploitation activities, the HiatusRAT, and "tcpdump" to enable packet capture. Black Lotus Labs observed four variants of packet capture binaries compiled for ARM, i368, and MIPS64 big endian and MIPS32 little endian byte order system architectures. Threat actors used HiatusRAT to execute commands remotely on affected routers, turning the router into a SOCKS5 proxy and subsequently establishing a connection to its command-and-control (C2) server.

When executed on the target router, HiatusRAT monitors network traffic to port 8816 to search for running services. In the event that a process was already running on that port, HiatusRAT terminates the process and collects the victim network and host data, including the MAC address, kernel version, system architecture and firmware version.

Impact

Recent research has indicated that the initial compromise by HiatusRat occurs via the delivery of a bash script to the target router, which is responsible for installing a packet-capturing tool that monitors network traffic to TCP ports associated with mail servers and FTP connections. The monitored ports are port 21 (FTP), port 25 (SMTP), port 110 (POP3), and port 143 (IMAP). Due to the unencrypted communication that occurs via these ports, successful exploitation would allow threat actors to steal sensitive email content and FTP credentials. Such data could be used in future attack campaigns.

Vulnerability Detection

A comprehensive endpoint detection and response (EDR) solution, such as Microsoft Defender, can provide effective protection against malware threats such as HiatusRAT. EDRs can alert system users of potential breaches and terminate the malware process during early stages of the attack chain, therefore limiting the scope of damage.

Affected Products

- DrayTek Vigor router models 2960 and 3900

[1] https://blog.lumen.com/new-hiatusrat-router-malware-covertly-spies-on-victims/

Containment, Mitigations & Remediations

As previously stated, one main method of reducing the threat of HiatusRAT is to detect it in the early stages, whilst implementing an effective and monitored EDR solution. An effective EDR will increase detection of malicious attempts of HiatusRAT compromise and halt the malware's progress if detected.

It is strongly recommended that the following mitigation steps are adhered to in an attempt to strengthen defence efforts against exploitation by HiatusRAT:

- Users with self-managed routers should follow best practices and regularly monitor, reboot and install security updates and patches
- End-of-life systems should be replaced with vendor-supported models to ensure that patches have been applied against known vulnerabilities.
- Businesses should consider implementing solutions that utilise VPN-based access to protect data and bolster their security posture
- Users should enable the latest cryptographic protocols to protect data in transit, such as only using email services which rely upon SSL and TLS. Examples of secure email services include secure simple mail transfer protocol and encrypted versions of IMAP or POP3.

Indicators of Compromise

HiatusRAT Associated File Hashes (SHA-256):

- 07cc70b287cbed13ef965c5a9815e1e2dcb7bfa4664beafdc7b57b5af3a8dd12
- 15960d2d7584ff90922e1c69f33c00508de4caa8b05a1341142b31f1661dd56f
- 193481c4e2cbd14a29090f500f88455e1394140b9c5857937f86d2b854b54f60
- 27b957fe2c5e9f3c98cfae5e90a2cd90a9adb8c9ac9de21118a751d9679bc4af
- 36f6045fac9289df716ea9f3f657fd9c560660bfc70bebd0e07c1d42025f9a3a
- 382d64d5943001a1df569f8ddae9490509ed96ba8128de6e74acff6d879d7035
- 4877bdc4fa80ad8e38600d1e0f3e9fdfbce2a6658ba050347281842345c5dd5e
- 6e21e42cfb93fc2ab77678b040dc673b88af31d78fafe91700c7241337fc5db2
- 6eb7357c0492960150286418e2a2f18513f50e925630bf2e6235422143f2e6c6

HiatusRAT Associated File Hashes (SHA-1):

- 167ea14b961877bec689cf8714b450e55a8033bd
- 22ff6af7256397267d1919cbb78bfdcccb6e5e39
- 2a770ad9d8e34b71323f026dcbe6b70b67e415db
- 525c04e97a0e2b38243f11debec9e100cc51fb15
- 5ec68cd73e3ca516b2518bc3307f5381bcc52b20

- a80c9729984976eeb6b20a48a5dae8b10e4dc724
- c55a8c027482ce281903f4b6b0b370a6efc7252c
- cb01eb90c2c968a1d1e17136ba8609ff1eafb9eb
- da1cd4b75787d8c3079ca4b7709bf788e7e2021e

HiatusRAT Associated IP Addresses:

- 104.250.48.192
- 46.8.113.227
- 149.248.0.203
- 66.42.108.185

Threat Landscape

DrayTek devices have a significant portion of the VPN router share. Threat actors generally utilise a combination of probability and asset value to determine which attack surfaces to focus on. As a result, the DrayTek routers become a prime target. Due to the fact that DrayTek devices are business-class VPN routers, they have become an integral aspect of business affairs. As such, threat actors will continue to exploit vulnerabilities contained within these devices in an attempt to facilitate their attack efforts and exfiltrate sensitive data from associated networks.

The relevant reports have documented that at least 100 businesses, primarily residing in Europe, North America, and South America, have been infected by HiatusRAT.

Black Lotus Labs telemetry data revealed that as of February 2023, approximately 4,100 DrayTek Vigor 2960 and 3600 series routers were exposed on the internet with Hiatus affecting around 100 of them. The majority of these routers were in Latin America, Europe, and North America. Although the number of bots connecting to HiatusRAT were minimal, evidence suggested that threat actors used minimal traces to obfuscate their origin and thwart analysis.

Threat Group

No attribution to specific threat actors or groups has been identified at the time of writing.

Mitre Methodologies

Reconnaissance
T1590 - Gather Victim Network Information[2]
T1591 - Gather Victim Host Information[3]

Execution

[2] https://attack.mitre.org/techniques/T1590/
[3] https://attack.mitre.org/techniques/T1592/

T1059.003 - Command and Scripting Interpreter: Windows Command Shell[4]

Defence Evasion
T1562 - Impair Defenses[5]

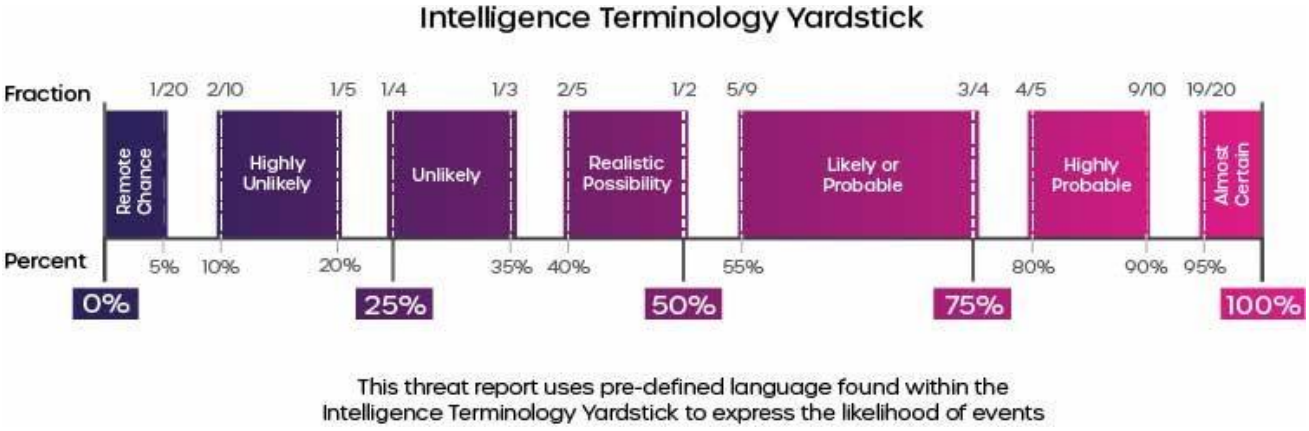
Collection
T1119 - Automated Collection[6]

Command and Control
T1090.002 - Proxy: External Proxy[7]

Further Information

- Lumen Report

Intelligence Cut-off Date (ICoD): 07/03/2023 10:00 GMT



[4] https://attack.mitre.org/techniques/T1059/003/
[5] https://attack.mitre.org/techniques/T1562/
[6] https://attack.mitre.org/techniques/T1119/
[7] https://attack.mitre.org/techniques/T1090/002/