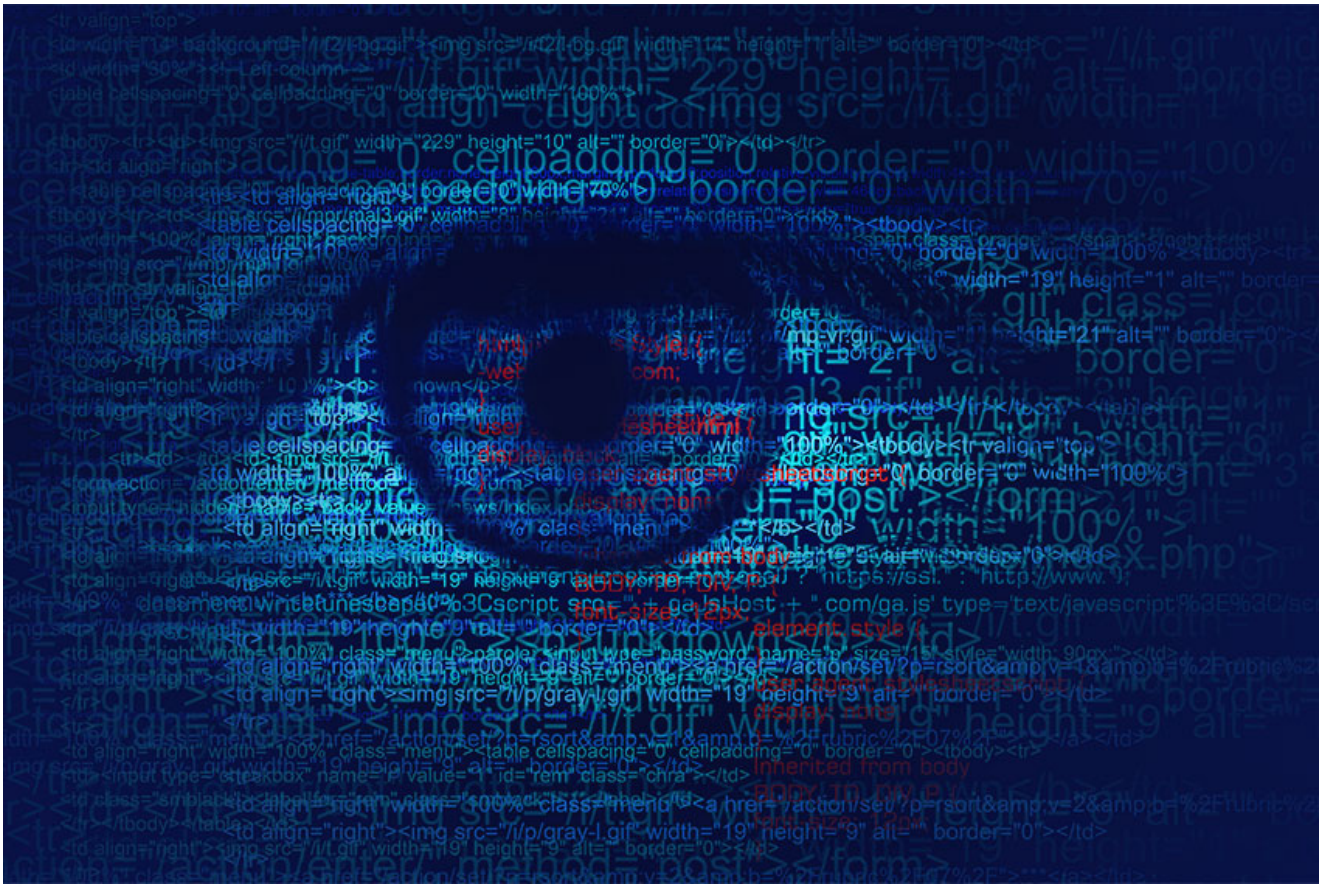
No rest for the wicked: HiatusRAT takes little time off in a return to action

blog.lumen.com/hiatusrat-takes-little-time-off-in-a-return-to-action/



BLACK LOTUS LABS Black Lotus Labs Posted On August 17, 2023

0
15.0K Views

Executive Summary

In March 2023, Lumen Black Lotus Labs reported on a complex campaign called "HiatusRAT" that infected over 100 edge networking devices globally. The campaign leveraged edge routers, or "living on the edge" access, to passively collect traffic and functioned as a covert network of command and control (C2) infrastructure.

After publishing our initial research, Black Lotus Labs continued to track this actor resulting in new malware samples and infrastructure associated with the HiatusRAT cluster. In the latest campaign, we observed a shift in reconnaissance and targeting activity; in June we observed reconnaissance against a U.S. military procurement system, and targeting of

Taiwan-based organizations. This ran contrary to the prior campaigns that primarily targeted Latin America and European organizations. The shift in information gathering and targeting preference exhibited in the latest campaign, are synonymous with the strategic interest of the People's Republic of China according to the 2023 ODNI threat assessment.

Despite our prior reporting, this group continued with their operations nearly unabated; in a truly brazen move, they recompiled malware samples for different architectures that contained the previously identified C2 servers. The actor then hosted this newly compiled malware on different procured virtual private servers (VPSs). One of which was used almost exclusively to target entities across Taiwan, including commercial firms and at least one municipal government organization. We subsequently observed a different VPS node performing a data transfer with a U.S. military server used for contract proposals and submissions. Given that this website was associated with contract proposals, we suspect the threat actor could gather publicly available information about military requirements, or search for organizations involved in the Defense Industrial Base (DIB).

Technical Details

Starting in mid-June through August 2023, Black Lotus Labs observed multiple newly compiled versions of the HiatusRAT malware discovered in the wild. In this latest campaign, our investigation also uncovered prebuilt Hiatus binaries that target new architectures such as Arm, Intel 80386, and x86-64 and previously targeted architectures such as MIPS, MIPS64, and i386. We associated these samples to our prior report with high confidence, as the threat actor employed the same heartbeat and upload server for malware communications detailed in that report. The only notable difference was that the HiatusRAT payloads were hosted on a newly observed VPS, IP address 207.246.80[.]240 from June through July**.** Starting in August, we observed them transition the payload hosting server yet again to a VPS at IP address 107.189.11[.]105.

Having identified the IP address hosting malicious files associated with HiatusRAT, we searched our telemetry for connections made to this server in an effort to identify potential targets. We found that over 91% of the inbound connections stemmed from Taiwan, and there appeared to be a preference for Ruckus-manufactured edge devices. The Taiwanese targeting affected a wide range of organizations from semiconductor and chemical manufacturers and at least one municipal government organization.

Realizing that this infrastructure was still active, we searched through our global telemetry to search for upstream, or Tier 2, servers that appear to operate and manage tier 1 servers. We identified one node in the PRC at IP address 101.39.202[.]142 as well as three additional VPSs in the U.S.:

- 45.63.70[.]57
- 155.138.213[.]169

- 66.135.22[.]245

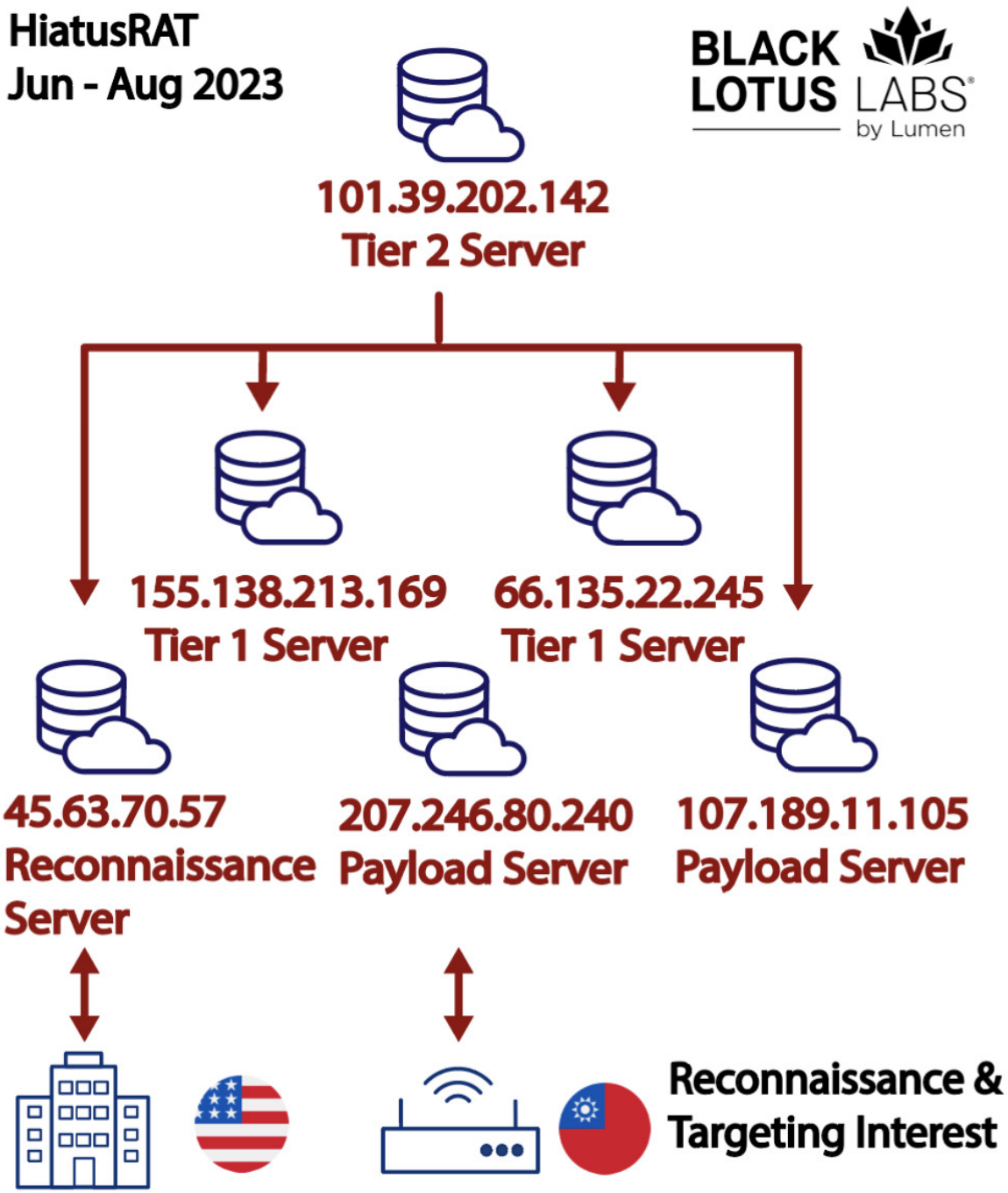


Figure 1: Depicting the logical connections in the new HiatusRAT network

Black Lotus Labs' global visibility suggests the threat actors used both 207.246.80[.]240 and 45.63.70[.]57 to connect to a U.S. military server associated with submitting and retrieving proposals for defense contracts. Over the course of roughly two hours on June 13, we observed over 11MBs of sampled bi-directional data transferred. In this period, the IP address 207.246.80[.]240 initiated a short five-minute connection to the server. Ten minutes

after this session ended, there was a second 90–minute connection from the IP address 45.63.70[.]57. We suspect this actor was searching for publicly available resources related to current and future military contracts. Given that this website was associated with contract proposals, we suspect the objective was to obtain publicly available information about military requirements and searching for organizations involved in the Defense Industrial Base (DIB), potentially for subsequent targeting.

Conclusion

While we acknowledge that all threat actors have different tolerances when it comes to public disclosures, this activity cluster ranks as one of the most audacious Black Lotus Labs has observed. Despite prior disclosures of tools and capabilities, the threat actor took the most minor of steps to swap out existing payload servers and carried on with their operations, without even attempting to re-configure their C2 infrastructure. This highlights the difficulty of dealing with edge and IoT-based malware, as there currently is no universal mechanism to clean up these devices.

One other notable shift that took place over the summer regards who the actor was targeting. In our prior report spanning late 2022 through March 2023, we noted that the majority of the data transfer to the C2s stemmed from Latin America and Europe. Based upon our telemetry, the actor behind this activity cluster pivoted focus to Taiwanese-based entities and was observed researching the United States Department of Defense. Potentially indicating a strategic shift which would align with a slew of recent reporting of Chinese-oriented operations against U.S. based entities, such as those from Storm-0558 and Volt Typhoon. At this time, Black Lotus Labs tracks HiatusRAT as a distinct activity cluster that does not appear to have overlap with any public reporting.

Establishing access to high value targets by compromising perimeter assets, such as edge network devices, is a tactic the industry has observed against several verticals from PRC-based actors. We suspect the HiatusRAT cluster serves as another example of tradecraft that could be applied against the U.S. Defense Industrial Base with a sense of impunity. We recommend defense contractors exercise caution and monitor their networking devices for the presence of HiatusRAT. The adversary has shown interest in targeting smaller DIB firms and those supporting Taiwan for intelligence gathering purposes.

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:

Businesses should consider:

1) Comprehensive Secure Access Service Edge (SASE) or similar solutions that use VPN-based access to protect data and bolster their security posture.

2) 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 using the feature which terminates if secure connections cannot be established), encrypted IMAP, and encrypted POP3 (defined in RFC 2595 which used ports 993 & 995).

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 models to ensure patching against known vulnerabilities.

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 Mastodon @BlackLotusLabs.

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.

Post Views: 15,037
