Cyber Threat Intelligence: Four Continents

Analysis coverage: 27 October 2024 to 3 November 2024

In this experiment my objective is to generate Cyber Threat Intelligence (CTI) from eight continents and identify any differences between them. So far, four of my servers (AU, UK, US, and SG) have begun identifying the methods used by hackers. I made a mistake in the custom log format for the ZA server, which prevented me from using proper data for this analysis.

TL;DR

1. The AU server faced a disproportionately high number of hacking attempts, while SG encountered the fewest challenges. The UK and US servers were comparable.
2. Most attack types were common across continents, and I have highlighted a few topics in the "Interesting Common Attacks" section below.
3. The AU server exhibited some very unusual attack types, which I have documented in the "Australia Specific Attacks" section further below. I will monitor whether this trend continues in the future.
4. **For those who operate servers, I suggest vigilance against unauthorised cryptocurrency mining, harden your php installation, and update your Pulse Secure and Fortinet, VMWare Horizon, if you use those.**
5. **For home and home office users, if you are using GPON Home Routers, see my suggestion below. Australian friends who still use Windows 7 in 2024, please unfriend me.** 😉.

I have suggested solutions for each attack type.

Interesting Common Attacks

1. **.env files**: There were numerous scripted scans searching for all kinds of ".env" files related to GitHub, AWS, APIs, documents, and other typical cloud-based applications.

   (Solution: Scan for and remove such files if you do not need them or restrict access. Use chroot.)

2. **Cryptocurrency mining**: A widespread botnet made attempts to mine Ethereum and Monero, specifically targeting cloud servers that had recently been issued SSL certificates.

   (Solution: Implement rate limiting, IDS, patching, and monitor CPU utilisation.)

3. **GPON Home Routers**: There were attempts to exploit vulnerabilities in GPON home routers.

   (Solution: Update the firmware or replace the device.)

4. **MGLNDD**: A botnet searched for responses to a malformed query, aiming to confirm connections on ports 80 and 443. Most queries were directed at a "wildcard server." Some researchers point to a scanner named "Stretchoid," but I could not verify this.

   (Solution: Avoid using wildcard servers, although you may have obtained the SSL certificate using one. It is easy to drop default traffic to the wildcard server with the 444 status code on Nginx.)

5. **MOZI.m**: A botnet attempted to use "wget" to download and run the "MOZI.m" script.

   (Solution: Restrict access to wget and shell.)

6. **PHPINFO / INFO**: Multiple scripted scans targeted files typically named "info.php" or "phpinfo.php."

   (Solution: Remove such files. Harden your PHP installation. Hide the version number.)

7. **PRI**: A botnet searched for "PRI ," resembling a probing request over HTTP/2.0.

   (Solution: Only allow GET or POST methods and disallow others if you do not need them.)

8. **Pulse Secure / Fortinet / SSTP_DUPLEX_HOST**: There were sophisticated attempts to bypass SSTP and gain stored credentials or session tokens.

   (Solution: Update your Pulse Secure and Fortinet appliances immediately and follow vendor recommendations.)

9. **SH**: Across all continents, there were numerous attempts at directory traversal to access the "/bin/sh" file.

   (Solution: Use chroot and Fail2ban.)

10. **SMB**: Attempts were made to exploit weaknesses in the Server Message Block protocol.

    (Solution: Do not expose SMB to the internet.)

11. **STAGER64**: A botnet searched for "stager64," which may be a malware component.

    (Solution: Search for the IOC in your log files.)

12. **T4**: On servers in the UK and Australia, hackers attempted to access the "/t4" endpoint. I have no idea what kind of endpoint "t4" represents, and my search yielded nothing useful.

    (Solution: Use Fail2ban or an equivalent tool to block such irrelevant searches.)

13. **TLS/SSL Exploitation Attempts**: Several entries included malformed TLS/SSL handshake attempts (with \x16\x03\x01 and \x16\x03\x02 as typical TLS record headers).

    (Solution: Use correct TLS configuration, preferably only TLS 1.3.)

14. **VMware Horizon or other VDI**: On servers in the UK and Australia, hackers attempted to access "/remote/login" and used brute force.

    (Solution: Implement rate limiting, IP-based restrictions, and MFA.)

Australia-Specific Attacks

15. **CONNECT / tunnel**: Hackers used the CONNECT method, attempting to use my server as a tunnel to connect to other servers (Outlook, Google, GitHub, httpbin, ip-api).

    (Solution: Only allow GET and POST methods.)

16. **Gh0st**: Attempts were made to exploit a backdoor.

    (Solution: Implement firewall and NDS.)

17. **PHP / hello.world**: These automated attacks originated from various IP addresses and targeted configuration weaknesses in PHP's "allow_url_include" function, which allows the inclusion of remote files. They also attempted to exploit "auto_prepend_file," which executes before the main PHP script.

    (Solution: Update your PHP application, harden your PHP configurations, and use a list of disallowed functions.)

18. **Windows 7 Professional**: Come on, hackers! Is there such a thing in 2024?

Stay safe!

Santosh Pandit

London, 3 November 2024