**Day 2 Observations - 00:00-23:30 August 21st 2024**

**Summary:**

This is a collection of data from the T-Pot honeytrap I configured to run on a Debian 11 EC2 instance. This second day’s data is from 00:00 August 21st 2024 through 23:30 August 21st 2024 and will be analyzed to provide insights into common attack behaviors, geographic location of attackers, and CVEs exploited. I will then compare the findings from Day 1(August 20th) to Day 2(August 21st) to see the difference in behaviors, geographic locations, and exploits leveraged by attackers.

**The Honeypots of T-Pot:**

* Honeytrap: a honeypot that emulates various types of network services and protocols, such as SSH, Telnet, FTP, HTTP, SMTP, and more. Can be configured to listen on multiple ports and simulate authentic behavior of various services to attract and trap attackers.
* Dionaea: a honeypot that emulates a vulnerable Windows environment designed to capture malware and attack payloads. Uses Python as its scripting language, supports IPv6 and TLS, uses libemu to detect shellcode, and collects hash values of collected files for later analysis.
* Cowire: a SSH and Telnet honeypot designed to emulate a system and provide a shell environment that captures the attacker’s actions on the system. This includes things like tools, techniques, credentials, and commands.
* Redishoneypot: a honeypot designed to emulate Redis servers and databases. Can collect the attacker’s IP address and commands used during connection attempts
* ADB Honeypot: a honeypot designed to emulate an ADB-enabled Android device and log unauthorized access attempts
* Snare/Tanner: a honeypot designed to emulate Windows systems and services that can capture attackers IP addresses, commands issued, tools, techniques, and procedures to identify patterns and send the collected data to security professionals.
* Ciscoasa: a honeypot designed to emulate Cisco Adaptive Security Appliances and software to track attacks targeting Cisco ASA devices.
* Citrix Honeypot: a honeypot designed to emulate a vulnerable Citrix environment.
* Mailoney: a honeypot designed to emulate a vulnerable mail server.
* Conpot: a honeypot designed to emulate SCADA protocols and industrial control systems.
* Elasticpot: this is a honeypot that simulates a vulnerable ElasticSearch server that is open to the internet.
* Dicompot: a honeypot that is designed to simulate a Digital Imaging and Communications in Medicine(DICOM) server.
* Sentrypeer: an open source VoIP fraud detection tool that tracks the IP addresses of attackers making calls to a SIP server.
* Heralding: a simple honeypot that is designed to log credentials of login attempts across multiple protocols.

| Total amount of attacks leveraged against the different T-Pot honeypots. A total of 6,600 attacks less than the previous day over the same span of time. |  |
| --- | --- |
| This graph shows the distribution of attacks across all of the honeypots that make up T-Pot. Much like the first day Honeytrap and Dionaea are the most targeted honeypots.   * Honeytrap: 49,511 * Dionaea: 14,491 * Cowire: 3,233 * Tanner: 767 * Mailoney: 420 * Redishoneypot: 150 * Citrix Honeypot: 109 * ConPot: 60 * ADBhoney: 35 * ElasticPot: 18 * Dicompot: 13 * Ciscoasa: 10 * Ipphoney: 5 * Sentrypeer: 5 * Heralding: 2 |  |
| This diagram shows the most commonly attacked ports over time.   * 18080: unofficial but commonly used for Monero cryptocurrency P2P network communications. Sees a steady stream of attacks. * 445: a Microsoft networking port that runs SMB and is linked to NetBIOS in earlier versions of Windows. This is the second most commonly attacked port but is seen in large bursts every few hours. * 80: this port is used for HTTP. This port saw a few spikes throughout the day with the largest being around 20:00. * 22: this port is used for the SSH protocol to remote into a system. This port experienced a large spike around 09:00. * 25: this port is used for SMTP relaying. This port sees attacks throughout the day with small spikes and valleys but at low numbers. |  |
| This graph shows the number of attacks attributed to specific countries over a period of time.   * The United States shows a consistent high rate of attacks over the whole 24 hour period. * Vietnam shows the second highest rate of attacks with a large spike continuing on from the end of the first day, a second spike around 04:30, and again a large spike near the end of the day. * India has the third highest rate of attacks with a low level of attacks sustained throughout the day but with a large spike around 05:00. * Argentina has the fourth highest rate of attacks all concentrated at around 05:00 * China is the final country with a consistent but low number of attacks throughout the day with a large spike around 08:00 |  |
| This graph shows the top 10 countries based on percentage of attacks.   * United States: 62% * Vietnam: 8% * India, Argentina, and China: 5% * The Netherlands, Turkiye, and Lithuania: 4% * United Kingdom: 2% * France 1%   Compared to the first day we see new countries like Argentina, China, and Turkiye and we don’t see other countries from the first day such as Singapore and Indonesia. |  |
| This graph shows the distribution of ports attacked based on the country of origin.   * The United States: 99% of attacks focused still on port 18080 * Vietnam, India, and Argentina: 99% of attacks all focused on port 445 * China: has the widest distribution of ports attacked with 84% of attacks leveraged against port 22(SSH), 9% on port 23(Telnet), 3% on port 6379(Redis), 2% on port 1433(SQL), and 2% on port 2375(Docker) |  |
| This graph shows the reputation of the source IP of the attackers. Most are known attackers or mass scanners   * Known Attackers: 95% * Mass Scanner: 4% * Bot, Crawler: ~1% * Tor Exit Node: ~1% |  |
| This graph shows the distribution of common OS used by attackers. The three most common being Linux 2.2.x-3.x(70%), Windows 7 or 8(19%), and Linux 2.2.x-3.x barebone(9%). Attackers may choose these older OSs for many reasons from using them to evade detection aimed at more current OSs, environmental factors like limited resources and technical expertise, or known exploits that haven’t been patched. |  |
| This graph shows the categories of the Suricata alerts at different times of day.   * Generic Protocol Command Decode is most common and consistent alerts throughout the whole day * Attempted Administrative Privilege is the second most common form of attacks with spikes at 00:00, 02:30,12:30, 17:00 and 23:30. These attacks attempt to gain administrative privileges and are commonly conducted outside of common office hours to remain unnoticed. |  |
| This is a list of the most commonly attempted usernames to gain access to the instance, with the most common during this time period being “root.” The names are usually default names and ones that commonly appear in dictionary attacks. It is important to choose a strong and unique username and to not use the defaults. |  |
| This shows the most commonly attempted passwords to gain access to the instance. The most commonly attempted one was simply no password at all, followed by the common top 10 like password, 12345, root, etc. Much like usernames it's important to choose strong passwords that cannot be easily cracked. |  |
| Top 10 CVEs:   * CVE-2020-11899: this exploit uses the Windows Graphic Device Interface(GDI) and a specially crafted image to allow attackers to execute arbitrary code on the system when the image is opened by the victim. * CVE-2021-3449: this exploit allows attackers to crash OpenSSL TLS servers by sending a maliciously crafted renegotiation ClientHello message. OpenSSL 1.1.1-1.1.1j versions are affected by this exploit. * CVE-2019-11500: this exploit affects Dovecot, an open source IMAP and POP3 server for Unix-based systems, versions before 2.2.36.4 and 2.3.x before 2.3.7.2. This exploit can grant out-of-bound writes and remote code execution to attackers because protocol processing can fail for quoted strings because ‘\0’ characters are mishandled. * CVE-2023-46604: This vulnerability may allow a remote attacker with network access to either a Java-based OpenWire broker or client to run arbitrary shell commands by manipulating serialized class types in the OpenWire protocol to cause either the client or the broker to instantiate any class on the classpath. Upgrading both brokers and clients to versions 5.15.16, 5.16.7, 5.17.6, or 5.18.3 will fix this issue. * CVE-2002-0013: Vulnerabilities in the SNMPv1 request handling of a large number of SNMP implementations allow remote attackers to cause a denial of service or gain privileges via GetRequest, GetNextRequest, and SetRequest messages. * CVE-2002-1149: The installation procedure for Invision Board, a web forum software that uses PHP, suggests that users install the phpinfo.php program under the web root, which leaks sensitive information such as absolute pathnames, OS information, and PHP settings. * CVE-2018-11776: Apache Struts, an open source framework for creating Java applications, versions 2.3 to 2.3.34 and 2.5 to 2.5.16 are vulnerable to possible Remote Code Execution when alwaysSelectFullNamespace is set to true which can either be set by the user or a plugin like Convention Plugin. * CVE-2019-12263: Wind River VxWorks 6.9.4 and vx7 has a Buffer Overflow in the TCP component. There is an IPNET security vulnerability where the TCP Urgent Pointer state is confused due to race conditions. * CVE-2006-2369: RealVNC 4.1.1, and other products that use RealVNC such as AdderLink IP and Cisco CallManager, allows remote attackers to bypass authentication via a request in which the client specifies an insecure security type such as "Type 1 - None", which is accepted even if it is not offered by the server. * CVE-2021-41773: A flaw was found in a change made to path normalization in Apache HTTP Server 2.4.49. An attacker could use a path traversal attack to map URLs to files outside the directories configured by Alias-like directives. If files outside of these directories are not protected by the usual default configuration "require all denied", these requests can succeed. If CGI scripts are also enabled for these aliased paths, this could allow for remote code execution. This issue only affects Apache 2.4.49 and not earlier versions. The fix in Apache HTTP Server 2.4.50 was found to be incomplete, see CVE-2021-42013. |  |

**Top 10 IP Addresses**

| **IP Address** | **Count** | **City/State** | **Country** | **ISP** |
| --- | --- | --- | --- | --- |
| 162.218.65.219 | 26,555 | Virginia | The United States | Lionlink Networks |
| 14.174.135.196 | 4,521 | Hue | Vietnam | VNPT Corp |
| 132.255.224.74 | 3,151 | Villa Mercedes | Argentina | Sidecom SRL |
| 125.18.228.250 | 3,150 | Bhopal | India | Bharti Infotel Ltd |
| 101.126.66.68 | 2,686 | Beijing | China | Beijing Volcano Engine Technology Ltd |
| 176.88.173.58 | 2,469 | Istanbul | Turkiye | Superonline Iletisim Hizmetleri A.S |
| 14.167.110.134 | 805 | Thanh Hoa | Vietnam | VNPT Corp |
| 94.156.177.10 | 368 | Eygelshoven | The Netherlands | HOSTYPE LLC |
| 13.215.228.180 | 335 | Central Singapore | Singapore | Amazon Data Services Singapore |
| 87.251.67.202 | 266 | Amsterdam | The Netherlands | Xhost Internet Solutions |

**Conclusion**

This day saw only 68,000 attacks which is over 6,000 less attacks than the first day, but we still see a lot of similarities.

The first similarity we see between this day and the first day is that Honeytrap and Dioneae are still the most popular honeypots targeted by attackers. Honeytrap recorded 49,511 attacks, 72% of the total attacks for the day and Dioneae recorded 14,491 attacks which equates to 21% of the total attacks for the day. Another similarity we see is that the United States still is the most prolific attacker with 62% of the total number of attacks for the day. CVE-2020-11899 still is the most commonly used exploit with a total number of 727 attacks recorded, followed by CVE-2021-3449 with 25 attacks recorded, and CVE-2019-11500 with 24 attacks recorded.

Some differences between the first two days is that the second most common attacker was Vietnam with 8% of attacks followed by India, Argentina, and China all accounting for 5% of the attacks each. Ports 18080 and 445 are still the two most common ports attacked but this day also sees port 80(HTTP), 22(SSH), and 25(SMTP) ranking among the top 5 ports.