**Day 6 Observations - 00:00-23:30 August 25th 2024**

**Summary:**

This is a collection of data from the T-Pot honeytrap I configured to run on a Debian 11 EC2 instance. This sixth day’s data is from 00:00 August 25th 2024 through 23:30 August 25th 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 5(August 24th) to Day 6(August 25th) 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 7,900 more attacks than the previous day over the same span of time. |  |
| --- | --- |
| This graph shows the distribution of attacks across the various honeypots. Honeytrap by far being the most attacked followed by Dionaea and Ciscoasa, from there it is a sharp fall off in the amount of attacks for the remaining honeypots. The attacks are broken down as follows:   * Honeytrap: 48,966 * Dionaea: 15,489 * Ciscoasa: 7,432 * Tanner: 1021 * Cowire: 959 * Redishoneypot: 110 * Mailoney: 106 * ConPot: 87 * Citrix Honeypot: 70 * ElasticPot: 24 * Dicompot: 16 * ADBhoney: 10 * Ipphoney: 8 * Sentrypeer: 3 * Heralding: 1   The biggest difference between today and the previous days is the Tanner honeypot getting more attacks than Cowire. Also Heralding has fallen back from 77 attacks the previous day to 1 attack. |  |
| 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: a port used for HTTP. Third most attacked port with a large spike in the beginning of the day and a few smaller spikes throughout the day. * 23: a port used for the Telnet protocol. This port experienced a steady but low number of attacks with an increase in attacks around 06:00 * 37215: a port used by Huawei routers that when exploited by attackers allows them to perform remote code execution. This port was attacked steadily throughout the day.. |  |
| This graph shows the number of attacks attributed to specific countries over a period of time.   * The United States again shows a consistent number of attacks throughout the day. * India attacked in a few large spikes from around 02:00 to 06:30 and again at 20:00 with a few much smaller spikes between that time. * The United Arab Emirates launched a steady stream of attacks throughout the whole day. * Japan launched attacks early in the morning with a small spike of about 500 attacks around 01:00 and a much larger spike of around 3,000 attacks at 05:30. * Lithuania launched a series of attacks every few hours throughout the day. |  |
| This graph shows the top 10 countries based on the percentage of attacks.   * The United States: 55% * Inda: 17% * The United Arab Emirates: 7% * Japan: 6% * Lithuania and the United Kingdom: 4% * The Netherlands and Bulgaria: 3% * China and France: 1%   This is the first time Japan and Bulgaria have appeared in the top 10 countries. This is also the first time the United States has dropped below being responsible for 60% of the attacks logged. |  |
| This shows the distribution of ports attacked based on the country of origin.   * The United States: 99% of attacks still focused on port 18080(Monero P2P). * India: 100% of attacks aimed at port 445(SMB). * United Arab Emirates: 67% of attacks targeted port 23(Telnet), 20% targeted port 5443(CDF management portal), 13% targeted port 445(SMB). * Japan: 79% of attacks targeted port 445(SMB) and 21% of attacks targeted port 80(HTTP). * Lithuania: 100% of attacks targeted port 18080(Monero P2P). |  |
| This graph shows the reputation of the source IP of attackers. Most of the attacks are performed by known attackers or mass scanners.   * Known Attacker: 97% * Mass Scanner: 3% |  |
| This graph shows the distribution of common OS used by attackers. The three most common being Linux 2.2.x-3.x(67%), Windows 7 or 8(17%), Linux 2.2.x-3.x barebone(8%), and Windows NT kernel(6%). 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 still the most prevalent throughout the whole day. * The Attempted Administrative Privilege attacks this day was a single spike in the middle of the average work day at around 11:30 which is strange since attackers typically try these types of attacks outside of business hours to help avoid detection. |  |
| 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 “sa” like the previous day. The variety of usernames attempted has gone down again compared to the previous day. The names are still common and 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. Unlike the previous day there were more words tried rather than just strings of numbers. Similar to the username list the list of attempted passwords has increased compared to the previous day. 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-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-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-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-2002-1149: 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-2000-0868: The default configuration of Apache 1.3.12 in SuSE Linux 6.4 allows remote attackers to read source code for CGI scripts by replacing the /cgi-bin/ in the requested URL with /cgi-bin-sdb/. * 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-2021-41733: 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 | 26,308 | Virginia | The United States | Lionlink Networks |
| 80.64.30.188 | 5,226 | Moscow | Russia | Horizon LLC |
| 103.134.44.223 | 3,153 | Uttarakhand | India | Countrylink Communication Pvt Ltd |
| 14.194.174.234 | 3,150 | Mumbai | India | Tata Teleservices Ltd |
| 219.59.171.150 | 3,148 | Tokyo | Japan | SoftBank Corp |
| 182.75.135.46 | 3,146 | Delhi | India | Bharti Airtel Ltd |
| 103.104.180.50 | 2,203 | Kanpur | India | Arrowswift Communication Pvt Ltd |
| 79.110.62.8 | 2,160 | Amsterdam | The Netherlands | Emanuel Hosting Ltd |
| 43.163.220.204 | 824 | Tokyo | Japan | Aceville Pte. Ltd |
| 18.130.199.174 | 649 | London | The United Kingdom | Amazon Data Services UK |

**Conclusion**

This is the final day of the lab and today saw an uptick in total attacks with 74834 attacks which is almost 8,000 more attacks recorded than the previous day. This is the largest difference in total number of attacks seen all week.

As with every day before we see Honeytrap and Dioneae are still the most popular honeypots targeted by attackers. Honeytrap recorded 48,996 attacks, which equated to 65% of the total attacks and Dioneae recorded 15,489 attacks which equates to 20% of the total attacks for the day and Ciscoasa is still the third most attacked honeypot with 7,432 attacks which is ~10% of the total attacks. The United States is still the most prolific attacker with 55% 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.

Even though Honeytrap is still the most commonly targeted honeypot this is the first time all lab it has dropped below having 70% of all attacks target it. Today is the second time all lab that the United States is responsible for less than 60% of attacks. The only other time was the first day. CVE-2021-3449 is the second most used CVE for the first time since the second day with 27 attacks, this CVE targets OpenSSL TLS. As far as the top 10 countries we see India is responsible for 17% of attacks which is the highest percentage a country other than the United States has been responsible for all lab. Today we also see Japan enter the top 10 attackers. We still see ports 18080(Monero P2P) and 445(SMB) still being the most common ports attacked and ports 23(Telnet) and 80(HTTP) still being in the top 5 and a return of port 37215(Huawei routers).