**Day 5 Observations - 00:00-23:30 August 24th 2024**

**Summary:**

This is a collection of data from the T-Pot honeytrap I configured to run on a Debian 11 EC2 instance. This fifth day’s data is from 00:00 August 24th 2024 through 23:30 August 24th 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 4(August 23rd) to Day 5(August 24th) 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 193 less 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: 49,498 * Dionaea: 10,161 * Ciscoasa: 5,729 * Cowire: 974 * Tanner: 515 * Mailoney: 134 * Redishoneypot: 90 * Citrix Honeypot: 82 * Heralding: 77 * ADBhoney: 63 * ConPot: 39 * ElasticPot: 32 * Dicompot: 13 * Ipphoney: 3 * Sentrypeer: 1   This biggest change between the 23rd and 24th is a sharp increase in attackers targeting the Heralding honeypot going from 1 attack registered the previous day to 77 registered this day. |  |
| 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 steady but low number of attacks with occasional spikes. * 23: a port used for the Telnet protocol. This port experienced a steady but low number of attacks with a spike at the end of the day. * 7999: a port used for Azure infrastructure communications. This port experienced a steady stream of attacks with little fluctuations 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. * The United Arab Emirates also shows a consistent number of attacks throughout the day but at a much lower volume than the United States. * India shows a series of small spikes of attacks throughout the day and has a very large spike of attacks at 18:00and again at 23:00 * Indonesia also has a single large spike of attacks at 06:00 * The Netherlands has a series of small spikes of attacks every few hours throughout the day |  |
| This graph shows the top 10 countries based on the percentage of attacks.   * The United States: 63% * United Arab Emirates and India: 7% * Indonesia: 5% * The Netherlands and Lithuania: 4% * Palestine and the United Kingdom: 3% * Romania and China: 2%   This day sees more of the usual attackers with the only previously unseen country being Palestine. |  |
| 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). * United Arab Emirates: 60% of attacks targeted port 23(Telnet), 20% targeted port 5443(CDF management portal), and 20% targeted port 2443(PowerClient Central Storage Facility) * India and Indonesia: 99% of attacks targeted port 445(SMB) * The Netherlands: 97% targeted port 18080(Monero P2P), 1% targeted port 80(HTTP), 1% targeted port 443(HTTPS), and 1% targeted port 81(unofficial TorPack onion routing) |  |
| 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(69%), Windows 7 or 8(13%), Linux 2.2.x-3.x barebone(10%), and Windows NT kernel(7%). 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 today show a different pattern this day compared to previous days with only two large spikes at 02:00 and 10:30. This is surprising that one of the spikes was attempted in the middle of the average work day 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” compared to the first few days where “root” was the most attempted. 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, admin, etc. This day attackers tried a lot more strings of numbers compared to the previous days. 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-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-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-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-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-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-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-2018-10562: An issue was discovered on Dasan GPON home routers. Command Injection can occur via the dest\_host parameter in a diag\_action=ping request to a GponForm/diag\_Form URI. Because the router saves ping results in /tmp and transmits them to the user when the user revisits /diag.html, this allows attackers to execute commands and retrieve their output. |  |

**Top 10 IP Addresses**

| **IP Address** | **Count** | **City/State** | **Country** | **ISP** |
| --- | --- | --- | --- | --- |
| 162.218.65.219 | 26,497 | Virginia | The United States | Lionlink Networks |
| 80.64.30.188 | 4,477 | Moscow | Russia | Horizon LLC |
| 119.226.185.2 | 3,166 | Chennai | India | Sify Limited |
| 36.79.220.62 | 3,117 | Duren | Indonesia | PT Telkom Indonesia |
| 188.161.188.234 | 2,034 | Gaza | Palestine | Palestine Telecommunications Company |
| 80.94.95.175 | 1,215 | England | The United Kingdom | UNMANAGED LTD |
| 182.72.33.205 | 1,007 | Bhopal | India | Sai Prasad Media Pvt Ltd |
| 113.160.196.108 | 492 | Nam Dinh | Vietnam | VNPT Corp |
| 51.89.229.92 | 308 | London | The United Kingdom | OVH SAS |
| 221.207.6.174 | 304 | Xining | China | China Unicom Qinghai Province Network |

**Conclusion**

This day saw a slight downtick in total attacks with 67,000 attacks the previous day to 66,800 today which is only 190 less attacks than the previous day. This is the smallest discrepancy between two days that we’ve seen so far in this lab.

Again we see Honeytrap and Dioneae are still the most popular honeypots targeted by attackers. Honeytrap recorded 49,498 attacks, which equated to 74% of the total attacks and Dioneae recorded 10,161 attacks which equates to 15% of the total attacks for the day and Ciscoasa is the third most attacked honeypot with 5,729 attacks which is 8% of the total attacks. The United States is still the most prolific attacker with 63% of the total number of attacks for the day. CVE-2020-11899 still is the most commonly used exploit with a total number of 729 attacks.

Some differences between this day is which CVEs attackers attempted to exploit. The second most popular CVE was and the previous one is that the second most common attacker was CVE-2006-2369 with 77 attacks, this CVE targets vulnerabilities in VoIP phones. The third most common CVE was CVE-2002-1149 with 14 attacks and targets PHP. It seems CVE attempts were more popular today overall showing more attacks attempted. As far as the top 10 countries we see India and the UAE being tied for the second most prolific attackers with 7% of attacks, we also see a new country in Palestine enter the top 10. We still see ports 18080 and 445 still being the most common ports attacked and port 23(Telnet) still in the top 5 but this day also sees ports 80(HTTP) and 7999(Azure Infrastructure Communication) make their way back to the top 5. We see another sharp decline in attempted usernames going from over 40 the previous day down to only 10 with the usual “root” and “sa” being the most popular. We also see the Heralding honeypot see a sharp increase in activity going from being consistently the least attacked honeypot to experiencing 77 attacks today.

It’s important to know what attackers are interested in attempting to exploit so we know where to focus our energies in cyber defense. The attacks targeting vulnerable VoIP infrastructure and PHP backend web servers reminds us to make sure we are vigilant about any exploits that target our infrastructure and making sure we are following best practices in securing every front of our organization.