**Day 4 Observations - 00:00-23:30 August 23rd 2024**

**Summary:**

This is a collection of data from the T-Pot honeytrap I configured to run on a Debian 11 EC2 instance. This fourth day’s data is from 00:00 August 23rd 2024 through 23:30 August 23rd 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 3(August 22nd) to Day 4(August 23rd) 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 6,160 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: 49,185 * Dionaea: 9,650 * Ciscoasa: 6,231 * Cowire: 1449 * Tanner: 208 * Mailoney: 145 * Citrix Honeypot: 53 * Redishoneypot: 51 * ConPot: 48 * Dicompot: 19 * Elasticpot: 18 * Ipphoney: 7 * Sentrypeer: 7 * ABDhoney: 6 * Heralding: 1 |  |
| 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. * 8728: a port used for APIs. Third most attacked port with a steady but low number of attacks throughout the day. * 37215: a port used by Huawei routers that are vulnerable to an attack where attackers send specially crafted packets that can lead to arbitrary code execution. A steady but low number of attacks throughout the day. * 23: a port used by the Telnet protocol. Also sees a steady but low number of attacks 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. * Romania also shows a consistent number of attacks throughout the day but at a much lower volume than the United States. * Kazakhstan has a single very large spike of attacks at 02:00 * Pakistan also has a single large spike of attacks at 06:30 * Lithuania 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: 65% * Romania: 6% * Kazakhstan and Pakistan: 5% * Lithuania, United Arab Emirates, and The Netherlands: 4% * The United Kingdom: 3% * Venezuela and Armenia: 1%   Today we see a few new countries launching attacks including Kazakhstan, United Arab Emirates, and Armenia. |  |
| This shows the distribution of ports attacked based on the country of origin.   * The United States: 99% of attacks still focused on port 18080. * Romania: 40% of attacks are on port 80(HTTP), 20% of attacks are at 14818(unassigned), 14761(unassigned), and 14641(unassigned). * Kazakhstan and Pakistan: 100% of attacks leveraged against port 445. * Lithuania: 100% of attacks leveraged against port 18080. |  |
| 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: 96% * Mass Scanner: 4% |  |
| This graph shows the distribution of common OS used by attackers. The three most common being Linux 2.2.x-3.x(72%), Windows 7 or 8(12%), Linux 2.2.x-3.x barebone(10%), and Windows NT kernel(5%). 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 the last three days. The last three days these attacks were focused around the middle of the night or very early morning but this day they spiked around 06:00, 08:00, and 16:00 which is at the beginning and end of the typical workday. |  |
| 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 variety of usernames attempted has gone up 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. 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-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-2006-3602: Directory traversal vulnerability in jscripts/tiny\_mce/tiny\_mce\_gzip.php in FarsiNews 3.0 BETA 1 allows remote attackers to include arbitrary files via a **..** sequence and trailing null (%00) byte in the language parameter in the advanced theme. * 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-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-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. * CVE-2021-42013: It was found that the fix for CVE-2021-41773 in Apache HTTP Server 2.4.50 was insufficient. An attacker could still 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 Apache 2.4.50 and not earlier versions. * CVE-2023-26801: A series of LB-Link branded routers (LB-LINK BL-AC1900\_2.0 v1.0.1, LB-LINK BL-WR9000 v2.4.9, LB-LINK BL-X26 v1.2.5, and LB-LINK BL-LTE300 v1.0.8) were discovered to contain a command injection vulnerability via the mac, time1, and time2 parameters at /goform/set\_LimitClient\_cfg. |  |

**Top 10 IP Addresses**

| **IP Address** | **Count** | **City/State** | **Country** | **ISP** |
| --- | --- | --- | --- | --- |
| 162.218.65.219 | 26,366 | Virginia | The United States | Lionlink Networks |
| 80.94.95.175 | 3,680 | England | The United Kingdom | UNMANAGED LTD |
| 45.132.85.251 | 3,106 | Karagandy | Kazakhstan | Optinet LLP |
| 202.141.252.141 | 3,052 | Karachi | Pakistan | Multinet Pakistan Pvt Ltd |
| 80.64.30.188 | 2,501 | Moscow | Russia | Horizon LLC |
| 186.88.193.227 | 899 | Anaco | Venezuela | CANTV Servicios Venezuela |
| 46.241.159.170 | 899 | Yerevan | Armenia | Ucom CJSC |
| 115.84.87.184 | 667 | Vientiane | Lao People’s Democratic Republic | Lao Telecommunication Co Ltd |
| 122.52.125.244 | 651 | Mandaluyong City | Philippines | Bluesun Philippines Inc |
| 170.64.186.36 | 649 | Sydney | Australia | DigitalOcean LLC |

**Conclusion**

This day saw another drop in total attacks with only 67,000 attacks which is more than 6,000 less attacks than the previous day. Even with the decrease in attacks see some differences in data 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 49,185 attacks, which equated to 73% of the total attacks and Dioneae recorded 9,650 attacks which equates to 14% of the total attacks for the day and Ciscoasa is still the third most attacked honeypot with 6,231 attacks or 9% of total attacks. Another similarity we see is that the United States still is the most prolific attacker with 65% of the total number of attacks for the day. CVE-2020-11899 still is the most commonly used exploit with a total number of 730 attacks recorded which is very consistent over the past four days.

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-2002-0013 with 10 attacks. This CVE targets vulnerabilities in SNMPv1. As far as the top 10 countries we see Romania being the second most prolific with 6% of attacks followed by Kazakhstan and Pakistan tied at 5%. This is also the first day we see Kazakhstan, Pakistan, and the United Arab Emirates. We still see ports 18080 and 445 still being the most common ports attacked and port 23 still in the top 5 but this day also sees port 8728 which is a port used by APIs and port 37215 which is used by Huawei routers which is vulnerable to arbitrary code execution. Unlike the previous three days where we see the number of usernames tried by attackers to gain access going down, we see an explosion of unique usernames today with over 40 names recorded.

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 Huawei routers reminds us to make sure we are vigilant about any exploits that target our infrastructure and to make sure all our components and systems are up to date and vulnerabilities are patched.