**Day 3 Observations - 00:00-23:30 August 22nd 2024**

**Summary:**

This is a collection of data from the T-Pot honeytrap I configured to run on a Debian 11 EC2 instance. This third day’s data is from 00:00 August 22nd 2024 through 23:30 August 22nd 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 2(August 21st) to Day 3(August 22nd) 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 4,400 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. 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: 51,542 * Dionaea: 16,249 * Cowire: 2,908 * Ciscoasa: 1,536 * Mailoney: 347 * Tanner: 239 * Conpot: 218 * Redishoneypot: 71 * Citrix Honeypot: 57 * Elasticpot: 32 * Dicompot: 16 * ADBhoney: 11 * Ipphoney: 7 * Sentrypeer: 1 * Heralding: 0   This day sees a sharp uptick in attacks focused on Ciscoasa compared to the first two days. |  |
| 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. * 2323 and 23: both of these ports are used for the Telnet protocol and see a consistent number of attacks during business hours from around 06:00 to 14:00. * 25: this port is used for Simple Mail Transfer Protocol(SMTP) and sees a low but consistent 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. * India shows the second most number of attacks with two large spikes around 04:00and 05:00 with a few much smaller bursts of attacks throughout the day. * Vietnam shows the third most number of attacks with focused from 04:00 to 14:00 * Venezuela shows the fourth most number of attacks spiking around 06:00 * Ukraine is the final country on the graph with a very large spike of attacks at 10:00 |  |
| This graph shows the top 10 countries based on the percentage of attacks.   * The United States: 60% * India: 7% * Vietnam: 6% * Venezuela and Ukraine: 5% * Russia, United Kingdom, The Netherlands, and Lithuania: 4% * Romania: 2%   Compared to the first two days we see new countries Ukraine and Russia being responsible for 5% and 4% of the attacks respectively. |  |
| This shows the distribution of ports attacked based on the country of origin.   * The United States: 99% of attacks still focused on port 18080. * India, Venezuela, and Ukraine: 99% of attacks focused on port 445. * Vietnam: 58% of attacks focused on port 2323 and 42% of attacks focused on port 23. |  |
| This graph shows the reputation of the source IP of attackers. Most of the attacks are performed by known attackers or mass scanners.   * Known Attackers: 96% * Mass Scanner: 3% * Bot, Crawler: <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(16%), Linux 2.2.x-3.x barebone(9%), and Windows NT kernel(4%). This day shows an uptick of Windows NT kernel based systems being used for attacks. 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. * Attempted Administrative Privilege is the second most common form of attacks with spikes at 00:00, 00:30,01:00, 01:30 and 11:30. 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 variety of usernames attempted has gone down as the honeypot has been up. 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 shrunk as the honeypot has been up. 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-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. |  |

**Top 10 IP Addresses**

| **IP Address** | **Count** | **City/State** | **Country** | **ISP** |
| --- | --- | --- | --- | --- |
| 162.218.65.219 | 26,490 | Virginia | The United States | Lionlink Networks |
| 103.28.33.101 | 3,861 | Da Nang | Vietnam | Viet Digital Technology Liability Company |
| 190.89.30.131 | 3,153 | Maracay | Venezuela | Corporación Fibex Telecom C.A |
| 193.30.245.5 | 3,147 | Rakhiv | Ukraine | PP Kabel-Plus |
| 103.111.235.197 | 3,146 | Jalalpur | India | Twincity Communication Pvt Ltd |
| 109.187.92.103 | 2,800 | Rayevskiy | Russia | PJSC Bashinformsvyaz |
| 80.94.95.175 | 1,504 | England | The United Kingdom | Unmanaged Ltd |
| 103.140.180.55 | 1,362 | Dhaka | Bangladesh | Data Edge Ltd |
| 59.178.244.128 | 1,259 | Phillaur | India | Mahanagar Telephone Nigam Ltd |
| 103.169.39.142 | 953 | Tengah | Indonesia | PT Boombas Carlo Medianet |

**Conclusion**

This day saw over 73,000 attacks which is more than 4,400 attacks than the second day. With the increase of attacks we start to see some differences in data but we still see a lot of similarities.

The first similarity we see between this day and the previous day is that Honeytrap and Dioneae are still the most popular honeypots targeted by attackers. Honeytrap recorded 51,542 attacks, which equated to 70% of the total attacks for the day and Dioneae recorded 16,249 attacks which equates to 22% of the total attacks for the day. Another similarity we see is that the United States still is the most prolific attacker with 60% of the total number of attacks for the day. CVE-2020-11899 still is the most commonly used exploit with a total number of 731 attacks recorded, followed by CVE-2021-3449 with 30 attacks recorded, and CVE-2019-11500 with 24 attacks recorded.

Some differences between this day and the previous one is that the second most common attacker was India with 7% of attacks followed by Vietnam switching positions in the list of top 10 countries. There was also a sharp increase in the number of attackers getting caught by the Ciscoasa honeypot that simulates Cisco Adaptive Security Appliances going from 10 attacks the previous day to 1,536 today. We see ports 18080 and 445 still being the most common ports attacked but this day also sees ports 2323 and 23 both of which are used for the Telnet protocol, and 25(SMTP) ranking among the top 5 ports. We see a few new countries appear with both Ukraine, accounting for 5% of attacks, and Russia, accounting for 4% of attacks. There's been a trend over these first three days where the number of unique usernames tried by attackers have shrunk with today only seeing 5 names attempted compared to the day before having 7 and 11 the first day.

It’s important to know what attackers are interested in attempting to exploit so we know where to focus our energies in cyber defense. We should always focus on making sure we’re following network security best practices like strong usernames and passwords but the data today shows we should make sure we should close ports we’re not using, especially vulnerable ones like those used by Telnet.