vehere

HUNT
BEFORE BREACH

MOON TREADER'S QUARTERLY THREAT REPORT (JULY-SEPT '23)

Introduction:

Last quarter, the team was focused on identifying various cyber threats, strengthening detection capabilities, and protecting the organization's valued customers from potential harm.

The team continued to discover new vulnerabilities, analyzing the latest threats, and implementing sophisticated detection mechanisms, ensuring customers and their sensitive data remain protected.

In this latest threat report published by Vehere's security research wing, Moon Treader, there are details pertaining to the recent undertakings of the team throughout the last quarter. These include the identification of new vulnerability, the creation and updating of new detections, and enhancements for the threat feed.

Executive Summary:

Some of the important highlights of the last quarter are as follows:

- Discovery of a second vulnerability in the Imagemagick software and responsible disclosure to the vendor.
- A comprehensive blog was published on the above-mentioned discovery.
- Three blogs have been published on Lateral Movement techniques and detection.
- Creation of a few new rules to provide coverage for various threats.
- Modification of a few rules to improve existing detections.
- Threat Feed Improvements.

Moon Treader's Progress:

1. Discovery of a second vulnerability:

The team discovered another vulnerability in ImageMagick, which it responsibly reported to the vendor in June. It was assigned the CVE ID of **CVE-2023-3428**. This vulnerability was an off-by-one read while processing a crafted TIFF file.

Click on the link to read the detailed blog post about this vulnerability:
https://vehere.com/threat-severity-high/identification-and-root-cause-analysis-of-cve-2023-3428/

2. Blogs on Lateral Movement techniques and detections:

Three comprehensive blogs on lateral movement techniques and detection have been published by the security research wing.

- **Common Lateral Movement Techniques:** This blog covers various common lateral movement techniques; Click to read more: https://vehere.com/threat-severity-high/lateral-movement-detection-i/

- **Lateral movement using Windows Service Control Manager Remote Protocol:** This blog gives an insight into the lateral movement techniques that use Windows Service Control Manager; Click to read more: https://vehere.com/threat-severity-high/lateral-movement-detection-ii/

- **Lateral movement using Windows Remote Registry:** This blog provides an in-depth view of the lateral movement techniques that use Windows Remote Registry; Click to read more: https://vehere.com/threat-severity-high/lateral-movement-detection-part-iii/

3. New Threats Coverage:

The team has been analyzing the latest threats on a regular basis and has added a few new detections that are mentioned below:

- **Detection of TI01158 RDP Recon Activity:** This rule detects RDP reconnaissance. The attacker scans the systems with open RDP ports and attempts to gain unauthorized access by identifying weak credentials or exploiting known vulnerabilities. Once successful, the attacker may steal sensitive data, install malware, or use the compromised system as a foothold for further attacks.

- **Detection of TI01156 SMB Recon Activity:** This rule detects SMB reconnaissance. It targets the Server Message Block (SMB) protocol used in Windows-based networks for file and printer sharing. The attacker scans for systems with open SMB ports, attempting to enumerate shares, user accounts, and system information. This reconnaissance allows the attacker to map the network's structure and identify potential vulnerabilities for further exploitation or unauthorized access.

- **Detection of TI01155 RPC Recon Activity:** This rule detects RPC Recon. The client is trying to scan for an open RPC port on the destination systems. The attacker identifies systems with open RPC ports and seeks to exploit weaknesses in the protocol or related services. By gaining insights into the network's configuration and service offerings, the attacker can plan targeted attacks to compromise or disrupt critical systems.

4. Updated Coverage:

The following rules have been updated to provide better detection for customers:

- **TI03020 Suspicious User Agent in Network Traffic:** This rule detects suspicious user agent strings by various hacking tools such as vulnerability scanners, brute force password crackers and exploitation tools.

- **TI03021 Download from unknown TLDs:** This rule detects the download of files from known suspicious TLDs.

- **Detection of TI01157 Port Sweep Activity:** This rule detects Port Sweep. The client IP tries to connect to multiple destination IPs on the same port, which could indicate malicious intent, indicating port sweep activity.

- **TI03036 Empty User Agent:** This rule detects HTTP traffic without a user-agent. All browsers and in-app browsers have a user-agent field. Absence of this field can be treated as an anomaly.

- **TI01108 Small Fragments in a flow:** This rule detects when an attacker is trying to gather information about the machine by sending an IP packet with a short fragmentation value, and that would cause the protocol header to truncate.

*[Note: *New or modified rules will be released after proper testing and QA validation.]*

5. Threat Feed Improvements:

We have been continuously making improvements to our existing threat feed, which has led to a significant reduction in false positives. We have added new threat feed sources and created a process to regularly monitor threat feed contents and proactively fix any issues that are found.

Striding forward:

The team will continue to discover new vulnerabilities, analyze emerging threats, and create new detections or update existing detections to protect customers more effectively.

Conclusion:

The threat landscape keeps evolving, and Vehere's security research wing, Moon Treader, is actively investigating and developing content on a regular basis. The team will continue to monitor the latest developments in the cyberthreat landscape and keep upgrading the detection capabilities to improve the security posture of Vehere's customers.

Authored by:

- Winny Thomas, Principal Security Architect
- Hardik Shah, Principal Security Researcher
- Parin Dedhia, Security Researcher

Learn more at www.vehere.com

Vehere InVehere Vehere