vehere

HUNT
BEFORE BREACH

MOON TREADER'S QUARTERLY THREAT REPORT

(APRIL-JUNE '23)

Introduction:

When it comes to cyber threats, Vehere's research wing, Moon Treader, is at the forefront, diligently shielding the organization's valued customers from potential harm. The team continuously analyzes the latest threats and develops robust detection mechanisms, ensuring customers and their sensitive data remain protected at all times. In this comprehensive report, get a glimpse into the recent endeavors of the Moon Treader team over the last quarter, which include the identification of new vulnerabilities, the creation and updating of new detections, and significant enhancements for the threat feed.

Executive Summary:

During the last quarter, the team has been busy fighting all kinds of threats and developing new detection methods to keep our customers safeguarded. Some of the important highlights are as follows:

- Discovering the first zero-day vulnerability and making responsible disclosure to the vendor. The disclosure process and policy regarding the same were also defined.
- Significant improvements in threat intelligence with domain verification.
- Impressive progress made in validating and publishing Blacklisted/Bot/Tor IPs with a high degree of confidence, reducing false positives to almost '0'.
- Addition of new coverage for threats.
- Improved coverage for existing detections.

Unveiling our progress:

1. Moon Treader's First Zero Day Discovery:

The team found a zero-day vulnerability in ImageMagick, which it responsibly reported to the vendor in April. It was assigned the CVE ID of CVE-2023-2157. This vulnerability was a heap buffer overflow while processing a crafted TIFF file.

Read the exclusive blog post to know more: https://vehere.com/threat-severity-high/breaking-down-the-imagemagick-cve-2023-2157-vulnerability-moon-treaders-findings/

This milestone was announced globally via press release and garnered media coverage in some prominent platforms like: http://finance.yahoo.com/news/vehere-takes-lead-tracking-first-130200475.html

https://www.businesswire.com/news/home/20230530005376/en/Vehere-Takes-the-Lead-With-Tracking-Its-First-ever-Zero-day-Vulnerability-and-Subsequent-Responsible-Disclosure

2. Continuously Improving the Threat Intelligence:

Vehere's Threat Feed is a collection of IOCs that can help identify a variety of threats based on IP, domains, and SSL fingerprints. This is released daily and is an integral part of threat prevention. We have been working on improving the IOC database so that we provide accurate detection without many false positives. In the last quarter, we modified the Threat Intelligence database to verify all the domain names and remove the expired ones. This has reduced the threat intelligence database significantly by removing around 70,000 expired domains. We have also made significant improvements in validating and publishing Blacklisted/Bot/Tor IPs with a high degree of confidence, reducing false positives to '0'.

3. New coverage released during Q2 2023

The team has been analyzing latest threats on a regular basis and have added few new detections as mentioned below:

- Malware Coverage Improvements

  - **Gozi Malware:** Gozi is a banking malware which has a lot of obfuscation techniques. It has been used in healthcare and banking industries. The detection is based on two protocols: HTTP and SMB; Two rules have been created

    - TI02153 Gozi Malware HTTP Traffic detected
    - TI02152 Gozi Malware SMB Traffic detected

  - **Mirai Malware:** This malware is used by cybercriminals to target computer systems in distributed denial of service (DDoS) attacks. For this one new rule has been created.

    - TI02151 Mirai Malware Activity detected

4. Vulnerability Coverage Improvements:

New rules have been created to cover following vulnerabilities:

- TI04150 Vmware Workspace One Access Identity Manager vulnerability (CVE-2022-22954)
- TI14148 Apache Log4j logging Remote Code Execution Vulnerability (CVE-2021-44228)
- TI04147 Apache Common Text Library Vulnerability (CVE-2022-42889)
- TI04149 Zyxel Firewall Unauthenticated Command Injection (CVE-2022-30525)
- TI05152 Windows ProxyShell Vulnerability

5. Updated Coverage:

We have improved a few rules by updating the detection checks. The following rules have been updated:

- TI01056 Suspicious DNS Query with Base64 Encoded String
- TI10126 Exe Upload to System32 Dir using SMBv1 Lateral Movement
- TI01059 Cobalt Strike DNS Beaconing
- TI01056 Suspicious DNS Query with Base64 Encoded String
- TI10146 High SMB Peer
- TI08101 ICMP Unreachable Host

Striding forward:

Continuing their efforts, the team will persist in discovering new vulnerabilities, analyzing emerging threats, and enhancing the detection capabilities of the Threat Feed. Moreover, updates to existing detections will be undertaken to enhance their effectiveness whenever necessary.

Conclusion:

Vehere NDR's Rule Engine is constantly updated to detect various threats. In addition to a comprehensive set of Rules, the NDR's ML engines are trained to detect behavioral anomalies in customer networks which safeguard them from potential threats. Moon Treader will continue to monitor the latest developments in the cyberthreat landscape and keep upgrading the detection capabilities for improving 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

© Vehere. All rights reserved.
Vehere and Vehere Logo and product names referenced herein are trademarks of Vehere. Unauthorized use, duplication, or modification of this document in whole or in part without the written consent of Vehere is strictly prohibited.