The Good, the Bad and the Ugly in Cybersecurity – Week 41

sentinelone.com/blog/the-good-the-bad-and-the-ugly-in-cybersecurity-week-41-5/

October 13, 2023

The Good | New Resources to Help Fight Ransomware

Extortion and ransomware continue to be the top cyber security concern for many enterprises, not least as we see threat actors pushing into new areas such as targeting ESXi servers and exploiting known vulnerabilities to gain initial access. Good news then that CISA has launched two new resources this week for combating ransomware campaigns.

As part of its wider Ransomware Vulnerability Warning Pilot (RVWP) scheme, the agency has added a “Known to be used in ransomware campaigns” column to its existing Known Exploited Vulnerabilities (KEV) catalog. For example, the recent WS_FTP vulnerability (*aka* CVE-2023-40044) is now marked in the catalog as ‘Known’ under the new column after reports that threat actors are using multiple attack chains to compromise organizations.

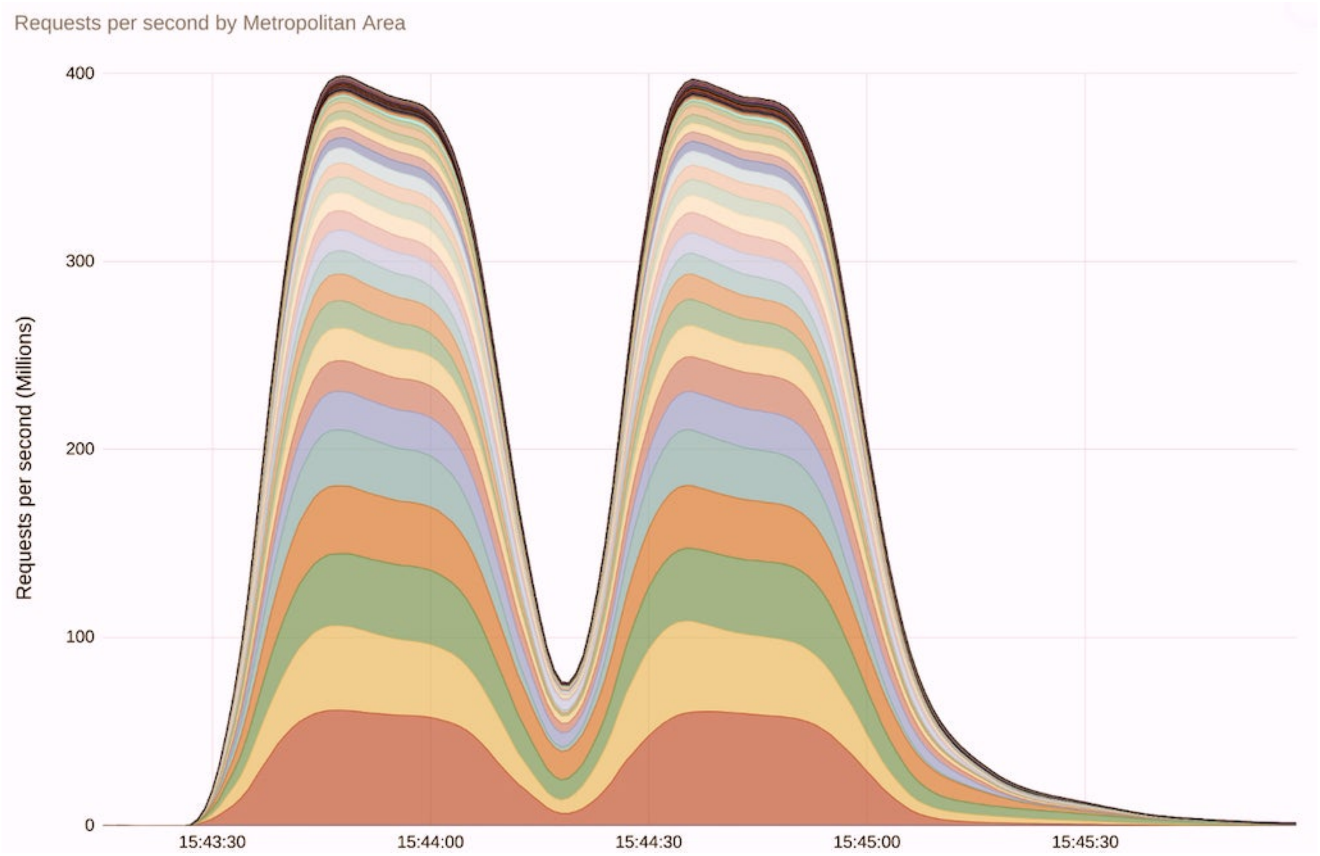
In addition, CISA is maintaining a list of “Misconfigurations and Weaknesses Known to Be Used in Ransomware” on its StopRansomware site. This list provides information on weaknesses and misconfigurations that are commonly exploited by threat actors in ransomware campaigns and, unlike the previously mentioned KEV catalog, contains information not based on CVEs. For each entry, a short description is provided along with the name of the vulnerable service and commonly used ports.

CISA says it hopes the new resources will help guide organizations to quickly identify and mitigate vulnerable software and services that are being actively exploited. Organizations are urged to review the resources regularly as part of their proactive security measures.

The Bad | HTTP/2 Rapid Reset Attack Could Overwhelm Unpatched Servers

While denial of service attacks may be further down the list of immediate threats for some organizations, there’s no doubt that DDoS campaigns can cause serious disruption and revenue loss for targeted organizations. Amazon, Cloudflare and Google have all reported this week that a massive campaign of DDoS attacks has been exploiting a vulnerability in the HTTP/2 protocol stack.

Google says the attacks, which began in August and are ongoing today, included one attempt to overwhelm internet services that was 7.5 times larger than the last previously recorded largest attack, reaching a peak of 398 million requests per second and continuing for two minutes. The service provider says that over two minutes, the attack generated more requests than the total number of article views on Wikipedia for an entire month.



Source: Google

Analysis of the attacks showed that threat actors are using a Rapid Reset technique that leverages the stream multiplexing capabilities of the HTTP/2 protocol. These capabilities enable clients to have multiple in-flight requests open on a single TCP connection. While the number of requests is theoretically limited to 100, by immediately canceling each request and then generating further requests, a malicious client can in effect have an indefinite number of requests in flight. Analysts say that even a modest-sized botnet can leverage this technique to overwhelm targets' defenses.

Enterprises or individuals serving HTTP workloads to the public internet may be at risk from the attack, and organizations are urged to verify that any vulnerable servers supporting HTTP/2 are patched against CVE-2023-444887. Multiple vendors have released patches for their products this week.

The Ugly | China Suspected in Attacks Exploiting Critical Confluence Bug

A zero-day bug in Atlassian's Confluence software reported last week to be under active exploitation is this week said to be being used by a nation-state actor linked to China, although details remain sparse.

CVE-2023-22515 is rated 10.0, the maximum possible score, on the CVSS severity rating system. The flaw is a critical privilege escalation vulnerability in Atlassian Confluence Data Center and Server, affecting versions 8.0.0 through 8.5.1, and is exploitable anonymously if the vulnerable server is exposed to the public internet. The bug allows attackers to create a Confluence administrator account within the application.

Warnings last week of active in-the-wild exploitation were followed up this week in a series of tweets from @MSFTSecIntel, claiming that a threat actor tracked variously under the names DarkShadow and Oro0lxy was behind the activity. Several IP addresses were observed sending exploit traffic:

- 192.69.90[.]31
- 104.128.89[.]92
- 23.105.208[.]154
- 199.193.127[.]231

The threat actor has a history of exploiting unpatched web applications. In 2020, the DoJ indicted two Chinese nationals, Li Xiaoyu (李啸宇) and Dong Jiazhi (董家志) for a long-running campaign spanning 11 countries in which they stole enterprise data from multiple companies, including Covid vaccine manufacturer, Moderna. Oro0lxy is known to be an online alias of Li. It is alleged that both individuals work on behalf of China’s Ministry of State Security. Both are currently wanted by the FBI.

Organizations using the affected versions of Confluence Data Center and Server are urged to update their instances as a matter of urgency and to take appropriate threat hunting measures to determine and mitigate any existing compromise.