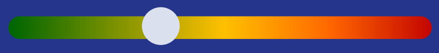
ZENDATA CYBER SECURITY

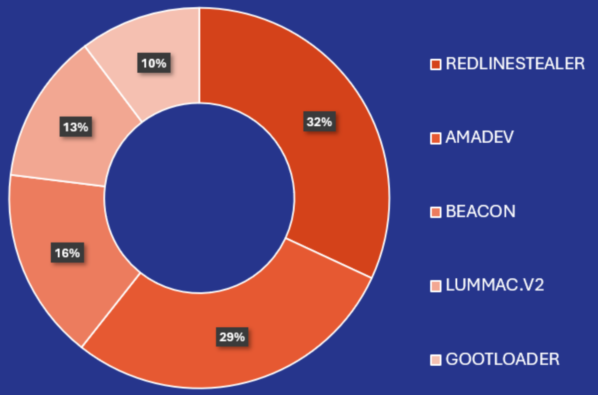
DEFCON LEVEL

October 2024



The threat alert level has remained unchanged from last month due to ongoing attack campaigns and persistent threat actors.

Most Active Malware



Recent Events

Recently, there has been an increase in cyberattacks targetting German-speaking schools in Europe. Last month, The Vocational Training Center, BBZ, fell target to a ransomware attack. The attackers blocked access to many systems and demanded ransom by using encryption malware on the servers. It is reported that access was gained through a security gap in the firewall. So far there is no confirmation whether any personal information was stolen or not.

To combat these rising threats, it is vital to perform vulnerability management, carry out frequent incident responses and follow real-time threat intelligence.

TOP THREAT: UNC5351

UNC5351 is a cluster activity related to phishing campaigns primarily focused on harvesting Telegram user data. Campaigns begin with posts in public Telegram channels promoting financial assistance programs that lead to phishing sites designed to harvest the full name, phone number, and telegram details of victims.

TOP VECTOR: REDLINESTEALER

REDLINESTEALER is a credential stealer malware that is capable of stealing credentials from web browsers, files, FTP applications and cryptocurrency wallets. The malware can download and launch additional payloads or launch a hidden command shell for the attacker. REDLINESTEALER has been advertised for sale on hacking forums.

Recent Critical Vulnerabilities

CVE-2020-1472

An improper privilege management vulnerability that when exploited allows a remote attacker to bypass certain security mechanisms. Attackers could exploit this vulnerability to gain access to administrator privileges without user credentials. The vulnerability needs to be exploited from a system with access to the Domain Controller.

CVE-2020-5902

A path traversal vulnerability that when exploited, allows a remote attacker to execute arbitrary code. Attacker would need to create a specially crafted HTTP request to the server hosting the TMUI utility for the BIG-IP system. Failed attempts cause denial-of-service condition when the applications crash.

Monthly Recommendations

Mitigation options to protect against access to administrator privileges due to improper privilege management includes following the principle of least privilege when assigning access rights to entities in a software system and following the principle of separation of privilege as it requires multiple conditions to be met before permitting access to a system resource. Patch and workaround should also be considered.

To offset the possibility of exploitation, following measures can be taken: restricting access to the Traffic Management User Interface (TMUI) by adding a LocatioMatch configuration element to httpd, disabling access to the Configuration utility for all configured self Ips, restricting access to the management interface using the secure configuration instructions provided by F5.