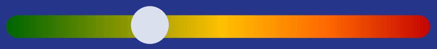
ZENDATA CYBER SECURITY

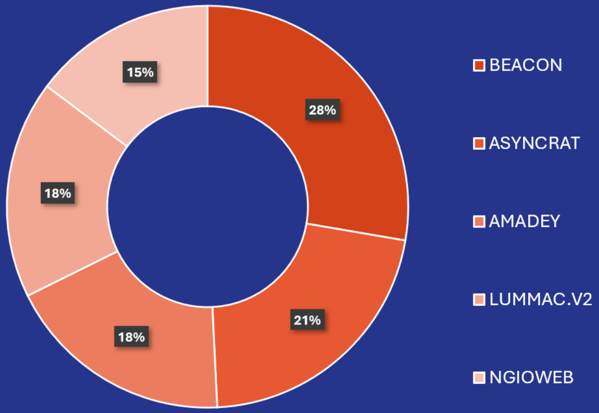
DEFCON LEVEL

November 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

The National Cyber Security Centre (NCSC) issued an alert about a new phishing campaign that was targeting Swiss residents through fake postal letters that contained malicious QR codes. The letters were cleverly crafted to look like they had been sent by the nation's Federal Office of Meteorology and Climatology. When scanned via Android smartphones, the QR code would automatically download an information stealer that would extract data from pre-loaded applications, including banking apps. This technique is unprecedented and highly sophisticated. As this is an evolving threat, there are no anti-phishing technologies designed for malware spread by QR codes, in turn, making it very unassuming for victims.

TOP THREAT: UNC 4536

UNC 4536 is associated with attacks carried out in various countries in Europe, including Switzerland. It is a cluster of activity associated with a malware distribution service offered by the actor "eugenfest." This service distribute its clients' malware by manipulating search engine results to direct traffic to malicious websites that serve malware masquerading as common or popular software.

TOP VECTOR: LUMMAC.V2

LUMMAC.V2 is one of the malwares associated with UNC 4536. LUMMAC.V2 is an information stealer malware that is capable of stealing data from browsers and cryptocurrency wallets, putting financial information and browsing history at risk. It employs binary morphing to alter the internal code, making it significantly harder for traditional security software to detect and eliminate.

Recent Critical Vulnerabilities

CVE-2023-46805

CVE– 2023-46805 is a path traversal vulnerability exists that, when exploited, it allows a remote attacker to bypass certain security mechanisms. This vulnerability has been confirmed to be widely exploited in the wild, and exploitation of this vulnerability is trivial and exploit code may not be needed. It is a critical-risk vulnerability.

CVE-2014-6271

CVE-2014-6271 is an input validation vulnerability exists that, when exploited, allows a remote attacker to execute arbitrary code. This vulnerability has been confirmed to be exploited in the wild, and non weaponized, proof-of-concept and weaponized code is publicly available. It is a critical risk vulnerability.

Monthly Recommendations

With evolving and emerging threats on the rise, threat actors are able to successfully execute sophisticated attacks. As they move to discrete ways of exploiting victims it is good practice to make sure training awareness programs are frequent and in line with latest trends. Training awareness should be considerate of modern types of attack techniques that are being used such as QR code phishing.

To reduce the risk of attacks from improper input validation, organizations should verify and sanitize all incoming data to ensure it adheres to expected formats, values, and rules before processing or communication. This can be achieved through allowlists, rejecting inputs that deviate from specifications, and implementing input encoding or escaping to handle special characters safely.