rewterz

2022

THREAT INTEL INSIGHTS

JULY 2022

1

MANTIS BOTNET POWERED THE LARGEST DDOS ATTACK

A DDoS mitigation provider announced it has mitigated the greatest HTTPS DDoS attack launched by a botnet known as Mantis in June 2022. Approximately, 5000 hijacked virtual machines and potent servers were used by the Mantis botnet to produce 26 million requests per second.

2

AMADEY MALWARE SPREADS VIA SOFTWARE CRACKS

Recently, the SmokeLoader is used by the Amadey Bot malware's creators to spread a newer version via keygen and crack sites. Amadey Bot is a data-stealing malware that enables operators to install additional payloads and is available for sale on underground forums.

3

BLACK BASTA RANSOMWARE

The Black Basta Ransomware's operators add QakBot trojan and PrintNightmare exploit to their attack arsenal. Before this activity, the group also added a new capability that encrypts VMware ESXi virtual machines (VMs) on Linux servers.

rewterz

4

RASPBERRY ROBIN WORM INFECTED WINDOWS NETWORKS

Raspberry Robin infected hundreds of Windows networks. It is a new Windows virus found by researchers having worm-like capabilities that spreads via removable USB devices. Raspberry Robin makes use of Windows Installer to connect to QNAP-related domains and download a malicious DLL.

5

BLACKCAT RANSOMWARE INCREASES STAKES UP TO $2,5M IN DEMANDS

The BlackCat, aka ALPHV ransomware group, has increased stakes up to $2,5M in demands. According to the most recent forecast, worldwide ransomware extortion activities would reach $265 billion by 2031, and business losses will top $10,5 trillion globally.

6

BITTER APT GROUP CONTINUES TO TARGET BANGLADESH

The recent campaign specifically targets Bangladeshi (military) groups. Threat actors use Remote Access Trojans to perform espionage using malicious document files and intermediary malware stages. Bitter attack arsenal include several sorts of Malware, such as keyloggers, stealers, or remote access Trojans (Almond RAT was also utilized)

7

HIVE RANSOMWARE UPGRADES TO RUST

Hive Ransomware upgrades to rust for a more improved encryption method. Hive is one of the quickest evolving ransomware families which likely operates as an affiliate-based ransomware, and employs a wide variety of tactics, techniques, and procedures (TTPs), creating significant challenges for defense and mitigation.