rewterz

2023

THREAT INTEL INSIGHTS

MARCH 2023

1

PLAY RANSOMWARE GANG LEAKS DATA STOLEN FROM CITY OF OAKLAND

The Play ransomware group disclosed the data obtained in a recent attack against the City of Oakland. The security breach started on February 8, 2023. The City of Oakland took the affected systems offline to secure the impacted infrastructure. The initial data leak consists of a 10GB multi-part RAR archive allegedly containing confidential documents, employee information, passports, and IDs. Oakland later declared a local state of emergency to allow the City to expedite orders, materials, and equipment procurement, and activate emergency workers as needed.

2

NEW GOLANG-BASED BOTNET GOBRUTEFORCER BREACHES WEB SERVERS

The Golang-based botnet named GoBruteforcer was discovered targeting web servers running FTP, MySQL, phpMyAdmin, and Postgres services. This botnet is designed to carry out brute-force attacks, which involve trying out multiple username and password combinations until it finds the correct one to gain unauthorized access to a target system. Golang, also known as Go, is a programming language that has gained popularity in recent years due to its simplicity and efficiency. Unfortunately, cybercriminals have also been adopting Golang to create new and sophisticated malware.

3

U.K NCA SETS UP FAKE DDOS-FOR-HIRE SITES TO TRAP CYBERCRIMINALS

The UK National Crime Agency (NCA) has taken an innovative approach to combat cybercrime by setting up several fake DDoS-for-hire or ‘booter’ services. These services allow users to rent or purchase the use of a network of compromised devices to launch DDoS attacks on targeted websites or networks. By infiltrating the online criminal marketplace in this way, the NCA is attempting to gather intelligence on the individuals and groups involved in this type of criminal activity.

4

CYBERSECURITY AGENCY WARNS OF FATAL POTENTIAL OF ROYAL RANSOMWARE

The U.S. Cybersecurity Agency issued an alert on Royal ransomware and expressed concern about its new methods and effects. Royal ransomware is a custom-designed program that has been targeting US and international organizations since September 2022. The group behind this malware is believed to be made up of seasoned threat actors who used to be part of Conti Team One. The group uses various methods of initial access, including call back phishing, remote desktop protocol (RDP), exploitation of public-facing applications, and initial access brokers (IABs). The ransom demands vary from $1 million to $11 million, with the threat actors targeting various critical sectors such as healthcare, education, communications, and manufacturing.

5

NORTH KOREAN GROUP APT43 FUNDS ITS ESPIONAGE ACTIVITIES THROUGH CYBERCRIME

Researchers discovered another North Korean threat actor gang, APT43, that uses cybercrime operations to fund espionage activities against South Korean and US government organizations. The campaign includes strategic intelligence collection linked with Pyongyang's geopolitical goals, credential harvesting, and social engineering to enable espionage efforts, and financially driven cybercrime to fund operations.

6

CYBER ATTACK ON PAKISTAN SUPREME COURT'S WEBSITE

The Pakistani Supreme Court’s official website suffered a cyber attack recently. The unknown attackers seized control of the official website of the Supreme Court (SC) in the morning and uploaded a message saying, “Our spring sale has started.” In a short period, government IT professionals were able to restore the website.

7

THREAT ACTORS TARGET CHINESE NUCLEAR ENERGY INDUSTRY

The Chinese nuclear energy industry has lately been under attack from a cyberespionage hacking group known as Bitter APT, which used phishing emails to infect computers with malware downloaders. In the past, the group has targeted organizations in Pakistan, China, Bangladesh, and Saudi Arabia. The group focuses on the energy and government sectors. In a recent effort campaign, Bitter sends emails to numerous Chinese nuclear energy enterprises and academics involved in that subject while posing as the embassy of Kyrgyzstan in Beijing.