rewterz

2022

THREAT INTEL INSIGHTS

NOVEMBER 2022

1

WORLD CUP PHISHING EMAIL CAMPAIGNS SPIKE IN ARAB COUNTRIES

Email-based phishing campaign targeting individuals in the Middle East spiked by 100 percent in October in the lead-up to the World Cup in Qatar. These phishing attempts increased between September and October, when the number of malicious emails doubled. The campaigns use customized web sites that appear to be legitimate making it difficult for the victim to recognize any suspicious activity.

2

HIVE RANSOMWARE RECEIVED APPROXIMATELY US$100 MILLION IN RANSOM PAYMENTS

Hive ransomware operators have successfully extorted $100 million in ransom payments from over 1,300 companies across the world, as of November 2022. Threat actors targeted a wide range of organizations and critical infrastructure sectors including Government Facilities, Communications, Critical Manufacturing, and Information Technology (HPH), particularly Healthcare and Public Health.

3

IRAN-LINKED THREAT ACTORS COMPROMISE US GOVERNMENT NETWORK

Iran-linked threat actors used a Log4JShell vulnerability to compromise a Federal Civilian Executive Branch (FCEB) organization and installed XMRig crypto-mining malware. The attackers gained access to the federal network after hacking into an unpatched VMware Horizon server and exploiting a remote code execution vulnerability in Log4J Shell (CVE-2021-44228).

4

BLACK BASTA RANSOMWARE GANG TARGETED US COMPANIES

Black Basta Ransomware group targets US companies with aggressive qakbot campaign. The ransomware gang Black Basta has been observed aggressively using the QakBot malware to attack primarily US-based companies. In the end of the november, the ransomware gang used QakBot malware to create an initial point of entry and move laterally within an organization's network.

5

RUSSIAN-LINKED RANSOMBOGGS RANSOMWARE

Recent ransomware attacks by the Russian-based ransomware family tracked as RansomBoggs Ransomware has targeted a number of Ukrainian organizations. The attacks against various Ukrainian companies were first discovered on November 21, 2022. The malware written in .NET is new, its deployment is similar to previous attacks attributed to the Sandworm gang.

6

APT29 EXPLOITED A WINDOWS FEATURE TO COMPROMISE ON A EUROPEAN DIPLOMATIC ENTITY NETWORK

The APT29 nation-state actor with ties to Russia was discovered using Credential Roaming, a ‘lesser-known’ Windows feature, after conducting a successful phishing attack on European diplomatic entity. The usage of Credential Roaming in an organization allows attackers to exploit saved credentials for privilege escalation. In the attack, the experts observed numerous LDAP queries with atypical properties performed against the Active Directory system.

7

GULOADER MALSPAM CAMPAIGN TARGETED KOREA

Researchers identified the GuLoader malware being delivered to Korean corporate users. GuLoader is a downloader that has been widely circulated in the past for the purpose of downloading infected programs. This malware is displayed as a Word icon, and a 600MB Null value is appended to the end of the file. Before injecting malicious data, the loaded GuLoader runs a regular process in the “C:\program files\internet explorer\ieinstal.exe” directory. The injected regular process attempts to download additional malware by connecting to the URL.