rewterz

2023

THREAT INTEL INSIGHTS

APRIL 2023

1

EVASIVE PANDA APT DELIVERS MGBOT MALWARE TO TARGET INTERNATIONAL NGOS IN MAINLAND CHINA

Evasive Panda is a well-known Chinese APT group that has been active for several years and has previously targeted organizations and individuals in various countries. Their latest campaign, as reported by researchers, involved distributing malware through an automatic update for the Tencent QQ messaging app. The campaign's victims are members of an international NGO and located in specific provinces of China, suggesting that the attack was targeted and focused. This is a common tactic used by APT groups, where they conduct extensive reconnaissance on their targets before launching an attack

2

NEW ALL-IN-ONE STEALER 'EVILEXTRACTOR' CAMPAIGN TARGETS WINDOWS USER DATA

A new type of malware called EvilExtractor is being marketed for sale to other threat actors as an "all-in-one" stealer malware. The malware is designed to steal data and files from Windows systems, and has been observed in a surge of attacks in March 2023, primarily targeting victims in Europe and the U.S. This all-in-one stealer malware has surfaced on the dark web and is being sold by an actor named Kodex on cybercrime forums like Cracked since October 22, 2022. The malware is continually updated and contains various modules to steal system metadata, passwords, and cookies from various web browsers. Additionally, it can record keystrokes and even act as ransomware by encrypting files on the target system.

3

QBOT MALWARE CAMPAIGN LEVERAGING HIJACKED BUSINESS CORRESPONDENCE

A new QBot malware campaign has been discovered by Kaspersky researchers, which is leveraging hijacked business correspondence to trick victims into installing the malware. The campaign began on April 4, 2023, and has primarily targeted users in several countries, including Germany, Argentina, Italy, Algeria, Spain, the US, Russia, France, the UK, and Morocco. QBot, also known as Qakbot or Pinkslipbot, is a banking trojan that has been active since at least 2007. The malware is capable of stealing passwords and cookies from web browsers and acting as a backdoor to inject next-stage payloads such as Cobalt Strike or ransomware.

4

NEW 'MONEY MESSAGE' RANSOMWARE DEMANDS A MILLION DOLLAR RANSOM

A new ransomware variant called Money Message has surfaced, attacking victims worldwide. The group has been discovered to be demanding ransoms of up to a million dollars in Bitcoin in order to decrypt files. In one of their recent attacks, they targeted an Asian airline with annual revenue close to $1 billion. It was first reported by a victim on researcher forums and then shared by researchers on Twitter. Money Message claims to have successfully accessed the company's file system, providing a screenshot as proof of the breach.

5

NORTH KOREAN LAZARUS APT GROUP PUSH LINUX MALWARE IN RECENT ATTACKS VIA FAKE JOB OFFERS

The North Korea-linked APT group, Lazarus, has been identified as the culprit behind a new campaign called Operation DreamJob, also known as DeathNote or NukeSped. This campaign reportedly used Linux malware and social engineering techniques, specifically fake job offers, to compromise its targets. Operation Dream Job, also known as DeathNote or NukeSped involves multiple attack waves where the North Korea-linked APT group, Lazarus, uses fraudulent job offers to lure unsuspecting victims into downloading malware. Operation In(ter)ception and Operation North Star, two more Lazarus clusters, show overlaps with this campaign.

6

HR COMPANY SD WORX SHUTS DOWN UK PAYROLL AND HR SERVICES DUE TO CYBER ATTACK

SD Worx, a leading HR and payroll management firm, became the victim of a cyber attack that led to its IT systems being shut down in the UK and Ireland services. SD Worx is a Belgian-based European HR and payroll management provider that serves 5.2 million employees for over 82,000 companies. The company has a team of over 7,000 HR professionals that are dedicated to providing secure, reliable HR and payroll services to its clients. Being a full-service HR and payroll provider, the company handles a lot of confidential information on behalf of its clients' workers.

7

IRAN-LINKED HACKERS TARGETS U.S. ENERGY AND TRANSIT SYSTEMS

An Iranian government-backed actor, dubbed as Mint Sandstorm, has been linked to attacks on critical infrastructure in the U.S between late 2021 to mid-2022. Mint Sandstorm is a threat actor group known for targeting both private and public organizations, including political dissidents, journalists, activists, the Defense Industrial Base (DIB), and employees from multiple government agencies. The group has been known to engage in cyber espionage, stealing sensitive information and credentials, as well as conducting cyberattacks aimed at disrupting the operations of targeted organizations.