

THREAT INTEL INSIGHTS

AUGUST 2023



1

RUSSIAN MISSILE MANUFACTURER TARGETED IN CYBER INTRUSION LINKED TO NORTH KOREAN THREAT ACTOR 'SCARCRUFT'

Cybersecurity researchers have linked a significant cyber compromise of NPO Mashinostroyeniya, a major Russian missile engineering company, to two distinct North Korea-affiliated Advanced Persistent Threat (APT) groups. The firm had been previously sanctioned by the U.S. Treasury Department in 2014 for its support of the Russian government's actions in destabilizing eastern Ukraine and its occupation of Crimea. In this recent incident, two instances of compromise were detected related to North Korea. These cyber threat actors breached the company's sensitive internal IT infrastructure, including an email server, and were found using a Windows backdoor named OpenCarrot.

2

NEW LINUX LOCKER BY MONTI RANSOMWARE TARGETS VMWARE ESXI SERVERS


The Monti ransomware group, which had taken a two-month hiatus, reemerged with a new Linux version of their encryptor. This variant was used in targeted attacks against government and legal sector organizations. The Monti group has been active since June 2022, following the shutdown of the Conti ransomware gang. Researchers noticed similarities in tactics, techniques, and procedures (TTPs) between Monti and Conti, with Monti using Conti's leaked source code as the foundation for their encryptor. Unlike the previous version, which heavily relied on the Conti source code, this variant employed a different encryption approach and exhibited distinct behaviors.



3

A MALICIOUS CAMPAIGN COMPROMISED AROUND 2,000 CITRIX NETSCALER SERVERS

A substantial cybersecurity incident has come to light involving the exploitation of nearly 2,000 Citrix NetScaler servers through the critical-severity remote code execution vulnerability known as CVE-2023-3519. The fact that more than 1,200 servers were already backdoored before administrators had the opportunity to install the patch to address the vulnerability. Even more concerning is the ongoing exploitation of these compromised systems because they have not been checked for signs of successful exploitation. The vulnerability, which received a patch on July 18, had been exploited by hackers as a zero-day, allowing them to execute code without authentication.



4

CARDERBEE APT GROUP UTILIZES LEGITIMATE SOFTWARE IN SUPPLY CHAIN ATTACK TARGETING ORGANIZATIONS IN HONG KONG

A new Advanced Persistent Threat (APT) hacking group, named 'Carderbee,' has recently been identified engaging in cyberattacks against organizations primarily in Hong Kong and other parts of Asia. This group employs a unique approach by utilizing legitimate software, specifically Cobra DocGuard developed by the Chinese company EsafeNet, to compromise target computers with the PlugX malware. The presence of PlugX malware, a known tool often used by Chinese state-backed threat groups, suggests a likely connection between Carderbee and the Chinese cyber threat landscape. The first traces of Carderbee's activities were noticed by researchers in April 2023, but another report from September 2022 indicates that their operations might date back to September 2021. This suggests that the group might have been active for a longer period than initially observed.

5

REPTILE ROOTKIT: TARGETED ATTACKS ON LINUX SYSTEMS IN SOUTH KOREA

Researchers have detected a notable cyber threat involving the use of the open-source rootkit known as Reptile, which is being deployed in targeted attacks against systems within South Korea. Unlike typical rootkits, Reptile, designed for Linux systems, offers the unique feature of a reverse shell, enhancing its capabilities. The malware incorporates port knocking, wherein a specific port on an infected system is opened, waiting for a specially crafted Magic Packet from attackers to establish a Command and Control (C2) connection. This campaign utilizing Reptile has been active since 2022, with multiple instances of attacks observed.

6


TARGETING NATO-ALIGNED NATIONS: RUSSIAN THREAT ACTORS FOCUS ON MINISTRIES OF FOREIGN AFFAIRS

Russian threat actors are reportedly involved in an ongoing campaign that targets the foreign affairs ministries of NATO-aligned nations. This campaign employs phishing attacks that utilize PDF documents with diplomatic-themed lures, some of which are crafted to appear as if they originate from Germany. The purpose is to deliver a variant of the Duke malware, which has been attributed to the APT29 group, also known as BlueBravo, Cloaked Ursa, Cozy Bear, Iron Hemlock, Midnight Blizzard, and The Dukes. “The threat actor used Zulip – an open-source chat application – for command-and-control, to evade and hide its activities behind legitimate web traffic.”

7

KMSDBOT MALWARE EVOLVES TO TARGET IOT DEVICES WITH ENHANCED ABILITIES

An updated version of a malware botnet named KmsdBot is now focusing on attacking Internet of Things (IoT) devices, demonstrating an expansion in its capabilities and potential targets. This new version of KmsdBot includes additional features, such as support for Telnet scanning and compatibility with more CPU architectures. The revised KmsdBot has been active since July 16, 2023. This update comes a few months after it was discovered that the botnet was being offered as a service for distributed denial-of-service (DDoS) attacks, highlighting its continued relevance and effectiveness in real-world cyberattacks.



8

LAZARUS GROUP DEPLOYS STEALTHY QUITERAT MALWARE VIA ZOHO MANAGEENGINE FLAW

The North Korea-linked threat actor known as Lazarus Group has recently been observed exploiting a critical security vulnerability in Zoho ManageEngine ServiceDesk Plus, a flaw that has since been patched. This exploitation is part of their strategy to distribute a remote access trojan (RAT) called QuiteRAT. The targets of these attacks have included internet backbone infrastructure and healthcare entities across Europe and the United States. The malware QuiteRAT is positioned as a successor to MagicRAT, which itself follows in the footsteps of TigerRAT. Additionally, during investigations into the adversary's attack infrastructure reuse, a new threat named CollectionRAT was uncovered.