مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Threat Actor Leverages Thread Hijacking in Phishing Attacks to Steal NTLM Hashes

Tracking #:432315680

Date:06-03-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a Threat Actor using phishing emails with ZIP attachments to steal NTLM password hashes from targeted organizations. These stolen hashes can be used by attackers to gain unauthorized access to networks and sensitive data.

## TECHNICAL DETAILS:

A recent phishing campaign by the threat actor TA577 targets IT networks to steal NTLM password hashes. These stolen hashes can be used by attackers to gain unauthorized access to systems and networks, potentially leading to data breaches and other malicious activities.

TA577 is one of the major affiliates linked to QBot and is considered an initial access broker (IAB). The group's campaigns are associated with ransomware infections, such as Black Basta, and have recently been observed utilizing Pikabot as an initial payload.

At least two recent campaigns have been observed, The phishing waves disseminated thousands of messages and targeted hundreds of organizations worldwide. The messages themselves appeared as replies to previous emails, known as thread hijacking, and contained zipped HTML attachments.

The most common delivery mechanism is ZIP attachments, which come with an HTML file designed to contact an actor-controlled Server Message Block (SMB) server.

TA577's objective is to capture NTLMv2 Challenge/Response pairs from the SMB server to steal NTLM hashes. Based on the characteristics of the attack chain and tools used, these hashes could be exploited for password cracking or facilitate "Pass-the-Hash" attacks using other vulnerabilities within the targeted organization to move laterally within an impacted environment.

- **Attack Technique:** Thread hijacking emails with ZIP archive attachments containing malicious files
- **Target:** NTLM password hashes
- **Impact:** Unauthorized access to systems and networks, potential data breaches
- **Threat Actor:** TA577 (also known as Water Curupira)

## INDICATORS OF COMPROMISE(IOCs):

Attached in Excel File

## RECOMMENDATIONS:

- Block the attached IOCs on network and use the latest Threat Intelligence data to stay aware of actual TTPs and IOCs used by threat actors.
- Be cautious of unsolicited emails, even if they appear to be replies to existing threads. Verify the sender's identity and avoid opening attachments from untrusted sources.
- Regularly update all software, including operating systems and applications, to patch vulnerabilities.
- Implement strong authentication methods, such as multi-factor authentication (MFA), for all

critical systems and applications.

- Monitor network traffic for unusual or suspicious activities using intrusion detection systems (IDS) and intrusion prevention systems (IPS).
- **Secure Backups:** Maintain offline, immutable backups of critical data. Regularly test restoration procedures.
- **User Awareness Training:** Educate employees on phishing, social engineering, and secure password practices.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

## REFERENCES:

https://www.proofpoint.com/us/blog/threat-insight/ta577s-unusual-attack-chain-leads-ntlm-data-theft