Tunisian Republic

Ministry of Higher Education and Research

Private Higher School of Technologies & Engineering

PROJECT REPORT

Level : SSIR

AridViper

établie par BY GHASSEN LANDOULSI AND BELHASSEN HASHOUS

2024 - 2025

Contents

Chapter 1

General Introduction

Cyber threats pose a significant risk to national security, corporate integrity, and individual privacy. This report delves into the activities of a selected threat actor, providing an in-depth analysis of their campaigns, tactics, and motivations. The aim is to offer actionable insights that enhance cybersecurity defenses against such adversaries.

The selected threat actor, **AridViper**, is a Middle Eastern Advanced Persistent Threat (also known as (APT-C-23, Bearded Barbie, Desert Falcon) group primarily attributed to operations targeting the Middle East. It is known for its politically motivated cyberespionage activities, focusing on government organizations, military institutions, and political activists.

1.1 Objective

The objective of this report is to:

- Provide a comprehensive understanding of the selected threat actor.
- Analyze their campaigns and methodologies.
- Identify Indicators of Compromise (IoCs) and Tactics, Techniques, and Procedures (TTPs).
- Suggest mitigation strategies to counter their threats.

1.2 Scope

This analysis focuses on:

- The threat actor's origin, objectives, and targets.
- Detailed case studies of their campaigns.
- Tools and malware employed.
- Recommendations for cybersecurity enhancements.

Chapter 2

Introduction of the Threat Actor

Arid Viper, also known as Desert Falcon, is a politically motivated Advanced Persistent Threat (APT) group originating from the Middle East. This group has been active since at least 2013, targeting government organizations, military institutions, and media outlets. They are particularly noted for their focus on entities in Israel, Palestine, and other Middle Eastern regions.

2.1 Timeline of Their Activity

Arid Viper has conducted numerous operations over the years. Below is a summary of their activity timeline:

- **2013**: The group begins operations, focusing on espionage against Middle Eastern targets.
- **2015**: Launches "Operation Arid Viper," targeting Israeli and Kuwaiti organizations. This campaign used spear-phishing emails to deliver custom malware for exfiltrating sensitive data.
- **2017**: Expands to deploy mobile malware, including GnatSpy, targeting Android devices in Palestine and Egypt.
- **2022**: Leveraged custom mobile apps disguised as legitimate tools to infiltrate Arabic-speaking targets.

2.2 Threat Actor Profile

- **Name:** Arid Viper (aka Desert Falcon, APT-C-23).
- **Motivation:** Espionage-driven, politically motivated operations.
- **Primary Targets:**
  - Government and military organizations.
  - Media outlets.
  - High-profile individuals in academia and diplomacy.
- **Primary Tools:** Micropsia malware, GnatSpy mobile malware.
- **Geographical Focus:** Israel, Palestine, Egypt, and other Middle Eastern countries.

2.3 The Attack Method

Arid Viper employs multiple sophisticated methods to compromise their targets:

- **Spear-Phishing:** Their primary tactic involves highly tailored phishing emails containing malicious attachments or links.
- **Custom Malware:** Deployment of tools like Micropsia (desktop malware) and GnatSpy (mobile spyware).
- **Social Engineering:** Leveraging fake profiles on social media and dating apps to deliver malware.
- **Command and Control (C2):** They utilize servers to manage infected devices and exfiltrate sensitive data.

2.4 An Example of an Attack Scenario

A notable operation by Arid Viper is their **2015 spear-phishing campaign**, which was part of **Operation Arid Viper**. This operation targeted Israeli government institutions, military personnel, and journalists, with the primary goal of exfiltrating sensitive military and government data. The group utilized highly sophisticated social engineering tactics to manipulate victims into opening malicious attachments or clicking on links that led to the installation of custom malware.

The attack was meticulously planned, with emails crafted to appear legitimate, often masquerading as official government communications or urgent documents related to national security. The attackers used politically relevant themes, such as current military operations or sensitive political affairs, to increase the chances of the targets engaging with the malicious emails.

The **Arid Viper** group employed a variety of **social engineering** tactics, including exploiting ongoing geopolitical tensions between Israel and its neighboring countries. By using these timely and relevant lures, they increased the likelihood of their malware being executed by unsuspecting targets. The malware used in this operation included the **Micropsia RAT**, which allowed the attackers to maintain persistence on infected machines, conduct surveillance, and exfiltrate valuable data.

Additionally, the group is known to have used fake profiles and manipulated social media to further their phishing efforts. By building trust with potential victims through seemingly innocuous social interactions, they effectively bypassed some security measures.

2.4.1 An Example of a Spear-Phishing Attack

In **2015**, Arid Viper launched a spear-phishing attack that specifically targeted high-ranking officials and military personnel in Israel. The emails were crafted with extreme precision, using politically relevant content to lure the victims into opening malicious attachments. These emails often contained documents purporting to be reports or internal communications concerning regional security issues, such as military operations or intelligence assessments.

The attached document would prompt the victim to enable macros or execute the embedded code in order to view the full content. Once the macro was enabled, the **Micropsia RAT** was deployed onto the victim's machine. Micropsia is a Python-based **Remote Access Trojan (RAT)** that enables the attackers to maintain control of the compromised system. Once installed, the malware allowed the group to:

- **Steal sensitive data**: Documents, credentials, and email communications were extracted.
- **Conduct surveillance**: Keystroke logging and screenshots were used to monitor the victim's activities.
- **Maintain persistence**: The RAT was capable of re-establishing connections to the attacker's Command and Control (C2) servers, ensuring continued access.

The attack was particularly effective because it leveraged **current geopolitical tensions**, which were a part of the lure, convincing the victims that the email was relevant to their work. The attackers used common vulnerabilities in **Microsoft Office** (such as **CVE-2017-11882**) to exploit the targets' machines.

One of the most notable features of the campaign was the use of **fake social media profiles** to target specific military personnel. The attackers posed as individuals with shared interests or common backgrounds, establishing trust before sending the malicious emails. This added a layer of legitimacy to the operation, making it more difficult for the targets to recognize the attack for what it was.

The **Micropsia RAT**, which was used in this campaign, was specifically designed for espionage. Once executed, it would quietly perform reconnaissance, sending sensitive data back to the attackers. This malware was able to **bypass traditional security defenses** and provide the attackers with **long-term access** to the victim's machine. The exfiltrated data was typically used to gain insights into Israeli defense strategies, political decisions, and internal communications. This operation underscores the growing trend of cyber espionage being used to gain access to critical national security information.

In addition to this spear-phishing campaign, **Arid Viper** continued to evolve its

tactics and malware arsenal, making their future operations even more effective. The group's use of **social engineering** and **custom malware** like **Micropsia** allowed them to remain a persistent threat in the region, often targeting high-value government officials and military personnel.

Chapter 3

Threat Actor Campaign

Arid Viper, also known as Desert Falcon or APT-C-23, has conducted a series of targeted campaigns characterized by their advanced malware, social engineering tactics, and strategic targeting of Middle Eastern organizations. Below, two notable campaigns are detailed with enhanced insights.

3.1 First Operation: THE DESERT FALCONS TARGETED ATTACKS

This campaign, first identified in February 2015, primarily targeted Israeli organizations, including military institutions, government entities, and academia. The operation is notable for its use of custom malware and phishing tactics aimed at exfiltrating sensitive data.

3.1.1 Steps of the Operation

Deceive and Infect: Malware writers use multiple technical and social engineering methods to deliver their files and encourage the victims to run them; creating an effective infection vector, even when they are targeting what should be well-protected organisations such as governments, banks and leading media outlets. In this case the attackers depended mainly on social engineering to exploit:

- Victims' trust in social networking forums
- Victims' curiosity about news relating to political conflict in their country.

Email samples

Email information	Time of delivery
From: السكرتير التنفيذي (Executive Secretary) **Subject:** المستحقات المالية (The financial benefits) **Attachment:** //المستحقات.rar//التقرير الفاصل بخصوص المستحقات.scr (a detailed report on the benefits)	March 2014
From: الاعلامية رنا (The media reporter Rana) **Subject:** مرحبا أ.(مدير مكتب المحامي ديفيد) اود تذكيرك بالاجتماع ومراجعة الصور والتقرير (Hi, this is the manager of the Lawyer David, to remind you of the meeting to review the pictures and the report)	March 2014

Figure 3.1: Email samples.

Infiltrate and Spy: The Desert Falcons depend on two different backdoors to spy on victims. Both backdoors are homemade and are under continuous development. We were able to identify and collect more than 100 malware samples used by the Desert Falcons. Once they have infected the victim's computer, attackers have full access and control, and they usually proceed as follows:

1. New victims are categorized into groups before being infected (e.g. A001, A002, and so on)
2. One of the cybercriminals is appointed to each new victim after infection
3. A complete list of all files (especially XLS, DOC, JPG and WAV) is retrieved from the victim's machine
4. The cybercriminal browses and collects any interesting pictures and files
5. The cybercriminal also collects chats and screenshots
6. Depending on the importance of the victim, the surveillance is then either intensified or dropped

Track and Control: The Desert Falcons' operation can be divided into three different campaigns, each operated from a different CC/IP, targeting different types of victims and operated mostly by different team members.

The campaigns can be classified by the type and version of malware and the type of vic-

tims targeted:

- Campaign 1: Active in Palestine, Egypt, Jordan and the Gulf states (KSA, UAE and Qatar)
- Campaign 2: Active in Israel
- Campaign 3: Active in Egypt

C&C Domains	IPs	Victims	Malware used	Registration Date
ahmedfaiez.info	188.40.75.132 188.40.106.84	Media & Government	Falcons Trojan	2013-03-29
fpupdate.info	188.40.75.132	Mobile	Falcons Trojan	2013-04-14
flushupate.com	188.40.75.132		Falcons Trojan	2014-02-16
flushupdate.com	188.40.75.132	Media	Falcons Trojan	2014-02-16
ineltdriver.com	188.40.75.132	Military & Government	Falcons Trojan	2014-09-14
mixedwork.com	188.40.81.136	Israeli Victims	Falcons Trojan	2014-02-18
plmedgroup.com	188.40.81.136	Israeli Victims	Falcons Trojan	2014-02-18
pstcmedia.com	188.40.81.136	Unknown, currently sinkholed	Falcons Trojan	2013-07-04
advtravel.info	188.40.106.84	Activists	DHS Spyware	2013-11-17
linksis.info	188.40.106.84	Politicians and Activists	DHS 2015/IRat	2014-12-01

Figure 3.2: Campaign - targeting computer devices and mobiles

3.1.2 Technical Features

The custom malware used in this operation included: **Falcons' Downloader:** This module is used for the initial infection. Once executed, the Falcons' downloader will send a registration request to the Command and Control (CC) server with the victim's IP address and a harddisk ID. The downloader will request a registration confirmation from the CC. Encrypted versions of the latest Falcons' backdoor will then be downloaded and installed on the victim's machine. **Falcons' Backdoor** The Falcons' backdoor communicates with CC servers using HTTP requests with encrypted content, providing the attackers with full backdoor functionality including: • Screenshots

- Keylogs
- Upload/Download files
- Information on all the .doc and .xls files on the victim's hard disk or connected USB devices
- The ability to steal passwords stored on the system registry (Internet Explorer and live Messenger)

All the files and screenshots collected by the backdoor are sent to the CC in a password-protected archive.

Cryptor/decryptor tool: The cybercriminals also developed other tools, for example, a public/private key-based file cryptor/decryptor tool.

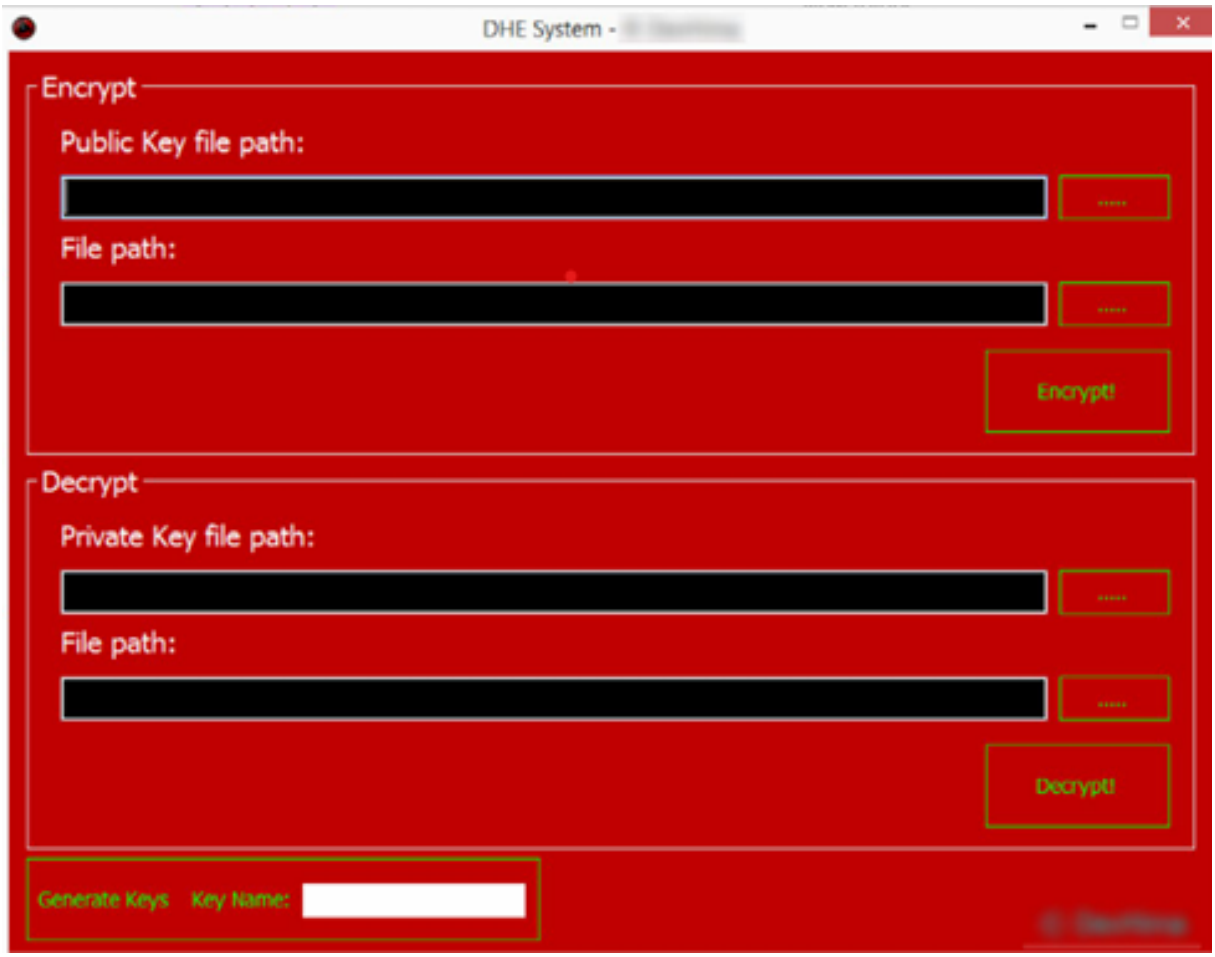

Figure 3.3: Cryptor/decryptor tool

3.1.3 Impact of the Operation

This campaign compromised multiple systems, exposing sensitive data related to national security and intellectual property. It highlighted the group's ability to exploit geopolitical tensions and organizational vulnerabilities effectively.

Conclusion: The Desert Falcons' attacks show clearly that zero day techniques are not a must for efficient targeted attacks. Using phishing emails, social engineering and homemade tools and backdoor, the Desert Falcons were able to infect hundreds of sensitive and important victims in the Middle East region through their computer systems or mobile devices.

3.2 Second Operation: Operation Bearded Barbie

The campaign operators use sophisticated social engineering techniques, ultimately aimed to deliver previously undocumented backdoors for Windows and Android devices. The goal behind the attack was to extract sensitive information from the victims devices for espionage purposes.

3.2.1 Steps of the Operation

Luring the Victims: To get to their targets, APT-C-23 has set up a network of fake Facebook profiles that are highly maintained and constantly interacting with many Israeli citizens. The social engineering tactic used in this campaign relies mostly on classic catfishing, using fake identities of attractive young women to engage with mostly male individuals to gain their trust.

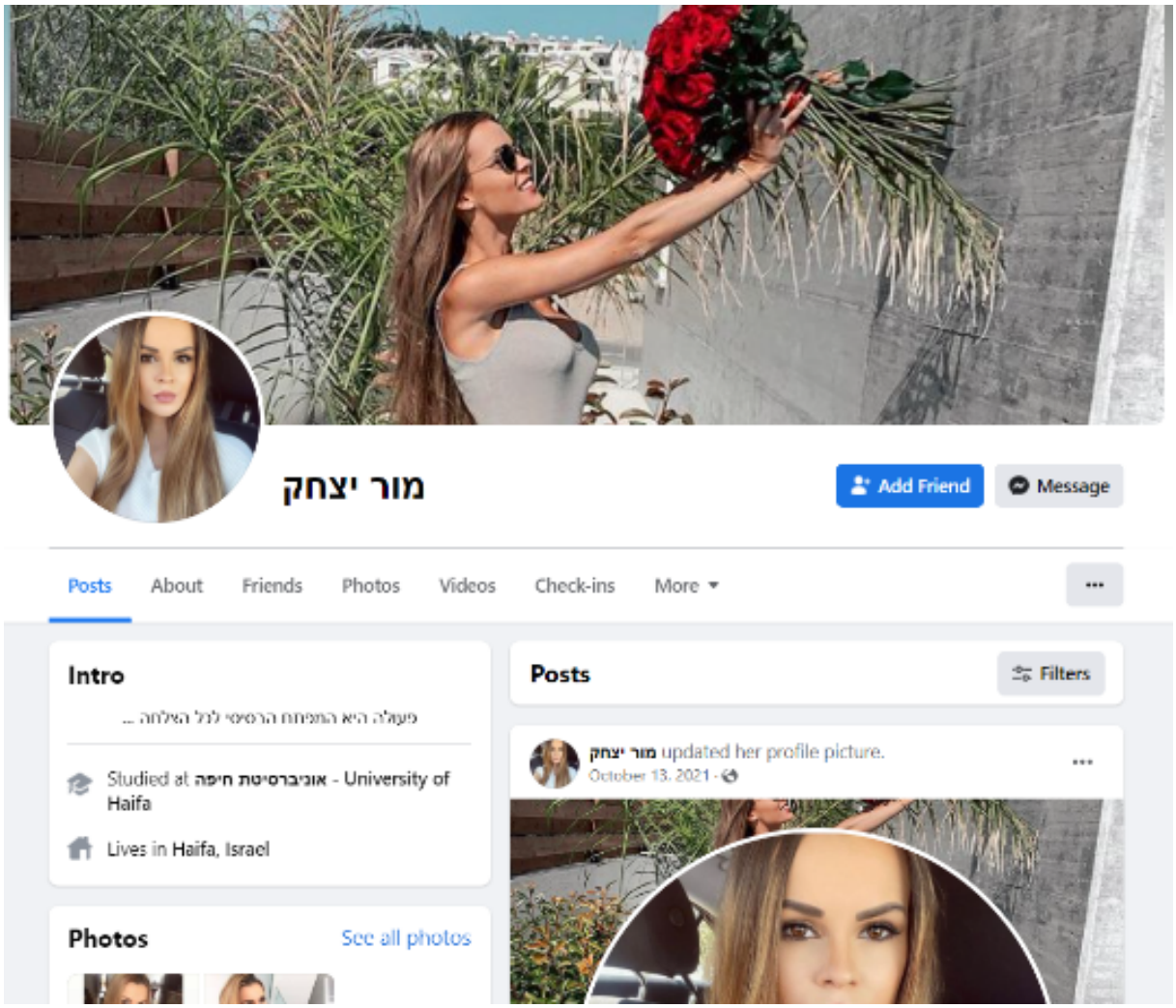

Figure 3.4: Fake Fcaebook account.

Over time, the operators of the fake profiles were able to become "friends" with a broad spectrum of Israeli citizens, among them some high-profile targets that work for sensitive organizations including defense, law enforcement, emergency services and other government-related organizations.

Barb(ie) Downloader: Barb(ie) is a downloader component used by APT-C-23 to install the BarbWire backdoor. As mentioned below, in the infection phase the downloader is delivered alongside a video in a .rar file. The video is meant to distract the victim from the infection process that is happening in the background.

Figure 3.5: initial infection chain of the campaign.

BarbWire Backdoor: The backdoor component of APT-C-23's operation is a very capable piece of malware, and it is obvious that a lot of effort was put into hiding its capabilities using a custom base64 algorithm. Its main goal is to fully compromise the victim machine, gaining access to their most sensitive data. The backdoor's main capabilities include: Persistence

OS Reconnaissance

Data encryption

Key logging

Screen capturing

Audio recording

Download additional malware

Local/external drives and directory enumeration

Steal specific file types and ex filtrate data

3.2.2 Technical Features

The custom malware used in this operation included: **VolatileVenom Android Implant:** VolatileVenom is one of APT-C-23's arsenal of Android malware. The attackers lure the victims into installing the VolatileVenom under the pretext that the suggested app is more "secure" and "discrete." it seems that VolatileVenom has been operationalized and integrated into the group's arsenal since at least April of 2020, and disguises itself using icons and names of chat applications

VolatileVenom has a rich set of espionage capabilities, which enable attackers to extract a lot of data from their victims.

The main espionage capabilities are the following:

Steal SMS messages

Read contact list information

Use the device camera to take photos

Steal files with the following extensions: pdf, doc, docs, ppt, pptx, xls, xlsx, txt, text

Steal images with the following extensions: jpg, jpeg, png

Record audio

Use Phishing to steal credentials to popular apps such as Facebook and Twitter

Discard system notifications

Get installed applications

Restart Wi-Fi

Record calls / WhatsApp calls

Extract call logs

Download files to the infected device

Take screenshots

Read notifications of the following apps: WhatsApp, Facebook, Telegram, Instagram, Skype, IMO, Viber Discards any notifications raised by the system

Conclusion: This campaign shows a considerable step-up in APT-C-23 capabilities, with upgraded stealth, more sophisticated malware, and perfection of their social engineer-

ing techniques using a very active and well-groomed network of fake Facebook accounts that have been proven quite effective for the group.

Chapter 4

Threat Actor's Techniques

Arid Viper, also known as Desert Falcon or APT-C-23, has consistently demonstrated its technical sophistication and adaptability in conducting espionage campaigns. This chapter explores the techniques, tools, artifacts, recommendations, and Indicators of Compromise (IoCs) used in their operations.

4.1 Techniques Used

Arid Viper relies heavily on a combination of social engineering, custom malware, and strategic targeting to achieve its objectives. Key techniques include:

Spear-Phishing: The primary infection vector for most campaigns. Arid Viper crafts convincing phishing emails with malicious attachments, often exploiting political or military themes to engage targets.

Social Engineering: Fake social media profiles, particularly on Facebook, are used to lure victims into downloading malicious files or sharing sensitive information. This tactic is especially effective in campaigns like *Operation Bearded Barbie*.

Mobile Espionage: Custom Android implants, such as *VolatileVenom*, enable data exfiltration and surveillance on mobile devices.

Command and Control (C2): Encrypted communication with C2 servers ensures the attackers maintain persistent access and stealth during operations.

Modular Malware Design: The group uses modular malware like Falcons' Downloader and BarbWire Backdoor to add functionality and customize attacks based on the target.

4.2 Tools Used

Arid Viper's arsenal includes a mix of custom and publicly available tools designed for espionage:

Falcons' Downloader: Used for initial infections, registering victims with the C2 server, and deploying additional payloads.

BarbWire Backdoor: A Windows backdoor that provides capabilities like keylogging, screen capturing, and file exfiltration. It uses custom base64 encoding for obfuscation.

VolatileVenom: An Android implant with extensive espionage capabilities, including stealing files, recording calls, and intercepting app notifications.

Micropsia RAT: A Python-based malware designed for reconnaissance and data theft on Windows systems

Custom Cryptor/Decryptor Tools: These are used to protect stolen data and malware payloads during transmission.

4.3 Artifacts

Artifacts left by Arid Viper in their campaigns provide valuable insights into their operations:

Malicious Document Names: Examples include *"SecurityUpdates.docx"* and *"MeetingAgenda.pdf"* used in phishing campaigns.

File Extensions Targeted: Includes `.doc`, `.pdf`, `.ppt`, and multimedia file types like `.jpg` and `.wav`, emphasizing a focus on sensitive documents and images.

C2 Infrastructure: Known domains include `oowdesign[.]com` and `smilydesign[.]com` used for victim registration and data exfiltration.

Keylogging and Screenshots: Captures user activity for monitoring and espionage.

4.4 Recommendations

To mitigate the risks posed by Arid Viper and similar groups, organizations should:

Enhance Email Security: Use advanced phishing detection tools and sandboxing for email attachments.

Conduct Security Awareness Training: Educate employees on identifying phishing attempts and safe online practices.

Use Endpoint Protection: Deploy solutions capable of detecting custom malware like Falcons' Backdoor and VolatileVenom.

Implement Network Segmentation: Limit lateral movement within organizational networks to contain breaches.

Monitor Mobile Devices: Regularly audit and secure mobile endpoints to prevent the installation of malicious apps.

4.5 Indicators of Compromise (IoCs)

Known IoCs associated with Arid Viper include:

Domains: `oowdesign[.]com`, `smilydesign[.]com`.

File Hashes: Examples include `3a401a679d147b070eb8ccae5df3dc43` (malware sample hash).

File Names: *"Update$_5$chedule.docx*",

General Conclusion

The activities of Arid Viper, also known as Desert Falcon or APT-C-23, illustrate the growing sophistication and adaptability of modern cyber threats. This report has explored the group's operations, techniques, and the tools they employ, shedding light on their strategic targeting of Middle Eastern organizations. Arid Viper's campaigns reveal not only technical capabilities but also a deep understanding of psychological manipulation and social engineering, which they use to infiltrate well-protected systems.

Key Findings

*1. **Persistent Threat**: Arid Viper's continuous development and deployment of custom malware such as Falcons' Downloader, Micropsia RAT, and VolatileVenom highlight their persistence in achieving long-term access to compromised systems. Their operations often blend technological sophistication with human-focused social engineering tactics, making them highly effective against government, military, and media organizations.*

*2. **Social Engineering Expertise**: The group's ability to craft convincing spearphishing emails and leverage fake social media profiles underscores their mastery of exploiting human vulnerabilities. Campaigns like Operation Bearded Barbie demonstrate their capacity to manipulate trust to achieve infiltration.*

*3. **Advanced Malware Arsenal**: Arid Viper's use of malware with modular capabilities—ranging from keylogging and data exfiltration to surveillance via mobile devices—underscores the complexity and customization of their toolkit. This arsenal enables them to adapt to a wide variety of targets and objectives.*

*4. **Geopolitical Motivations**: The focus of Arid Viper's campaigns on politically*

sensitive regions and topics reflects their intent to gather intelligence and disrupt adversaries in the Middle East. Their attacks often exploit geopolitical conflicts and leverage them in their phishing lures to enhance their effectiveness.

Implications for Cybersecurity

The threat posed by Arid Viper extends beyond their immediate victims. Their campaigns serve as a reminder of the vulnerabilities inherent in human and technical systems alike. Organizations must recognize that traditional security measures, such as antivirus solutions and firewalls, may be insufficient against well-resourced and strategically adept adversaries like Arid Viper.

*To counter such threats, organizations must adopt a multi-layered approach to cybersecurity: - **Proactive Threat Hunting**: Continuous monitoring and analysis of network traffic to detect and mitigate potential intrusions. - **Advanced Email Filtering**: The use of machine learning-based tools to identify and block phishing attempts. - **Education and Awareness**: Regular training for employees to recognize social engineering tactics and suspicious communications. - **Mobile Security**: Enhanced security measures for mobile devices, which are increasingly becoming targets for espionage.*

Final Thoughts

As demonstrated by Arid Viper, the landscape of cyber threats continues to evolve, with attackers developing more sophisticated methods to bypass security measures. Their campaigns highlight the critical need for constant vigilance, innovation in defensive technologies, and collaboration among organizations to stay ahead of these adversaries.

This report underscores the ongoing challenge of combating cyber espionage and provides actionable insights to strengthen defenses against similar threats. Through a combination of technical advancements, strategic policies, and international cooperation, the impact of groups like Arid Viper can be mitigated, ensuring the resilience of critical systems and information in an increasingly interconnected world.

List of Figures

Liste des acronymes

APT - *Advanced Persistent Threat*

C2 - *Command and Control*

IoC - *Indicator of Compromise*

RAT - *Remote Access Trojan*

TTPs - *Tactics, Techniques, and Procedures*

SMS - *Short Message Service*

PDF - *Portable Document Format*

HTTP - *HyperText Transfer Protocol*

DOC - *Document (Microsoft Word file extension)*

XLS - *Excel Spreadsheet (Microsoft Excel file extension)*

PNG - *Portable Network Graphics*

JPG/JPEG - *Joint Photographic Experts Group*