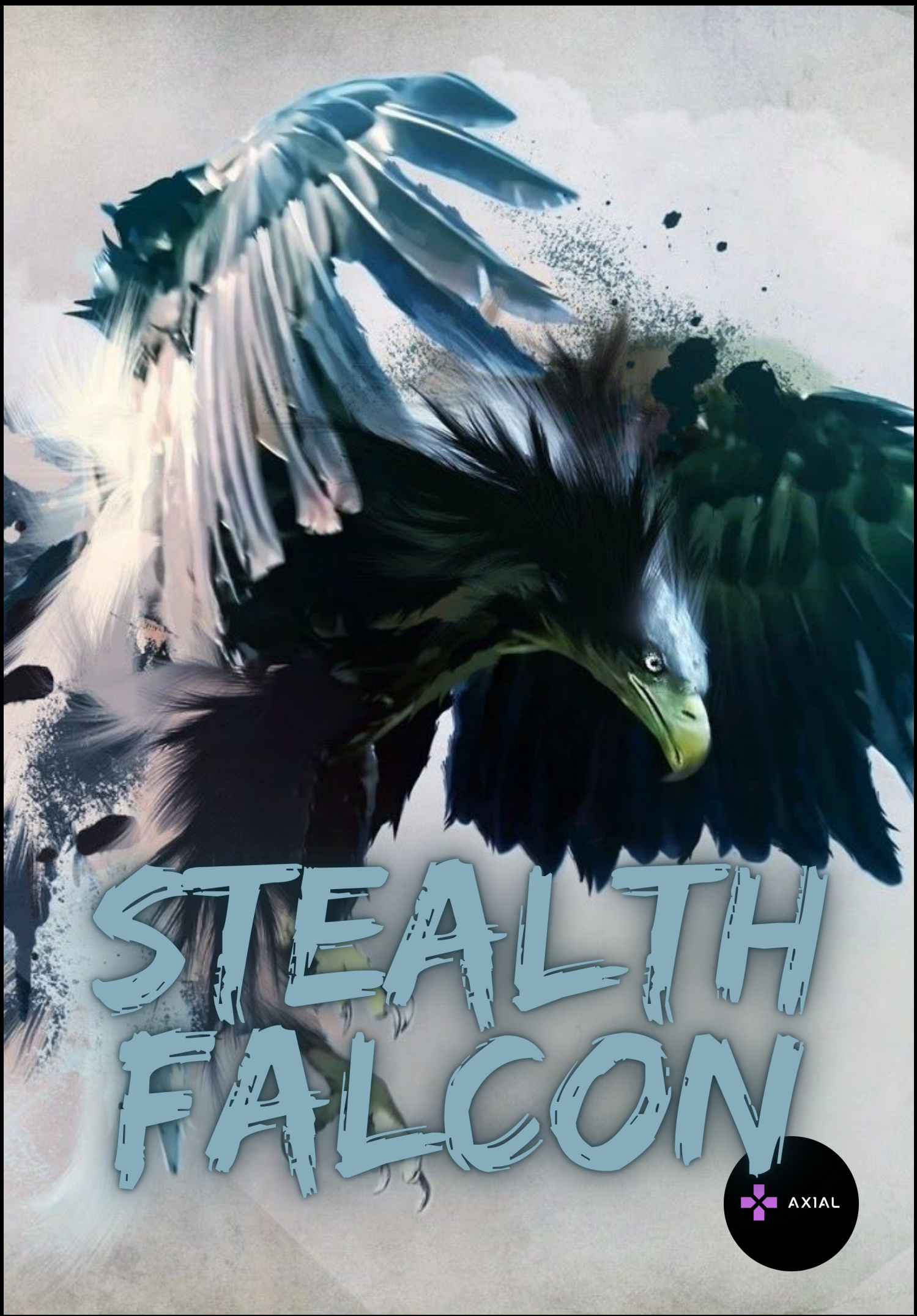
STEALTH
FALCON
AXIAL

A SURVEY ON STEALTHFALCON: ABOUT, WEAPON OF CHOICE, TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. ABOUT

Stealth Falcon (FruityArmor/Project Raven) is a campaign with circumstantial evidence linked to the Government of UAE. This threat group has been active since 2012 and has been constantly targeting Emirati Journalists, activists and dissidents.

II. TARGET SECTORS

Stealth Falcon has targeted Civil society groups and Emirati journalists, activists and dissidents in countries like Netherlands, Saudi Arabia, Thailand, UAE, UK.

III. METHODS USED

Stealth Falcon uses spear-phishing emails to target. Initial attack email will contain a link, which if clicked, will redirect to another site and will invoke JS on the target's computer. They also tend to use StealthFalcon and 0-day exploits.

IV. IOC

MD5

- 26e92360804b2660daad286034102b60
- 7031bdcc7031bdcc7031bdcc7031bdcc
- 80e8ef78b9e28015cde4205aaa65da97
- 8e722d60e8d42f60423732609c993460
- dc5b49bc50a32f2eadc531f869271a46

DOMAINS

1. footballtimes.info
2. vegetableportfolio.com
3. electricalweb.org
4. windowsearchcache.com
5. upnpdiscover.org
6. adhostingcache.com

V. OPERATIONS

- **2014**
  - An Ex-NSA operative revealed how they helped spy on targets for Arab Monarchy. They had joined Project Raven, a clandestine team that included more than a dozen former U.S. intelligence operatives recruited to help the United Arab Emirates engage in surveillance of other governments, militants and human rights activists critical of the monarchy.
- **2016**
  - StealthFalcon APT utilized Windows 0day CVE-2016-3393, which was reported to Microsoft by Kaspersky Lab in September
- **2018**
  - Stealth Falcon utilized CVE-2018-8453 in targeted attacks
  - They also used a 0day in Windows Kernel Transaction Manager (CVE-2018-8611)
- **2019**
  - ESET researchers discovered backdoor which was linked to malware used by Stealth Falcon APT group.

VI. ATTRIBUTIONS

According to CitizenLabs, In December 2012, an activist contacted them and asserted that an a7rarelemarat.com link was sent to him in a private message from the @WeldBudhabi account the same day that an individual accused of operating the account was arrested, and while the account was “reportedly hacked by authorities”. The Twitter account associated with a7rarelemarat.com, @a7rarelemarat, appears to have been under the control of Stealth Falcon at some point during October 2012 (and possibly before and after), as the account sent several aax.me links in October 2012.

VIII. REFERENCES

- https://www.reuters.com/investigates/special-report/usa-spying-raven/
- https://securelist.com/windows-zero-day-exploit-used-in-targeted-attacks-by-fruityarmor-apt/76396/
- https://securelist.com/cve-2018-8453-used-in-targeted-attacks/88151/
- https://securelist.com/zero-day-in-windows-kernel-transaction-manager-cve-2018-8611/89253/
- https://www.welivesecurity.com/2019/09/09/backdoor-stealth-falcon-group/