Advisory

Imperial Kitten

aeCERT
One of Telecommunications Regulatory Authority (TRA) Initiatives
P O Box 116688, Dubai, United Arab Emirates (UAE)
www.aecert.ae | www.tra.gov.ae

Version: 1.0
Ref: ADV-19-055
Document Date: 08/10/2019

Document Details

Disclaimer

Whilst every effort has been made to ensure the accuracy of the information contained within this report, aeCERT and the TRA bear no liability or responsibility for any recommendations issued or inadvertent damages that could be caused by the recipient of this information.

Accessing third-party links in this advisory will direct you to an external website. Please note that aeCERT bears no responsibility for third-party website traffic. aeCERT will have no liability to the entities for the content or use of the content available through the hyperlinks that are referenced.

Contents

Summary

As the leading trusted secure cyber coordination center in the region, aeCERT has researched and found out about a new malicious website managed by an Iranian-based adversary group called Imperial Kitten. The malicious website has been identified in September 2019 and claims to be a job application website with the domain "apply-jobs[.]com", targeting people who search for jobs. Moreover, the website is mainly used to download the Checkmate malware tool.

Details

In September 2019, the domain apply-jobs[.]com was observed to have been created by the Imperial Kitten adversary group. Imperial Kitten has engaged in intrusions against military veterans, maritime and IT services targeting Saudi Arabia and India. The group uses social media and job ads to deliver a malicious tool called Checkmate.

Analysis of the website has shown that the job-themed website mimics the legitimate job website "talent-recruitment[.]org" by including resume submission protocol, employees list, countries of operation and contact address as shown below. Recently, the website replaced the contact email address "jobs@talent-recruitment[.]org" with a new email address "info@apply-jobs[.]com". Furthermore, the website includes a list of employees with their information and personal photo copied from the legitimate website "talent-recruitment[.]org".

The malicious website includes a download page path "hxxps[:]//apply-jobs[.]com/download" that redirects to another page, which downloads a compressed executable file; this contains the Checkmate executable malware. Furthermore, the Checkmate payload uses the C2 configuration to acquire the final payload from cortanaservice[.]com.

The hacker group also uses social engineering as a method to deliver the Checkmate malware. Moreover, the hacker group researches and gathers information about the victims, then uses it to gain access to the victim's Microsoft account by accessing the secondary email inbox for the Microsoft account. Once it gains access, the group resets the password for the primary account to use the reset link in the secondary email for taking control of the primary Microsoft account.

Recommendations

In order to avoid and mitigate the impact of the threat, we highly recommend the following:

- Frequently check on login history for the email accounts.
- Implement two-factor verification on Microsoft account to improve the account security.
- Visit the legitimate/official company websites when applying for a job instead of third-party websites.
- Use antimalware tools and ensure the latest patches are installed on the system.
- Implement more cybersecurity awareness workshops.

Indicators of Compromise

The following is a list of the indicators of compromise:

Domain

apply-jobs[.]com

SHA256 hashes

Online-Interview.zip: 5068534c27af8d63908de3e0ae511217d6f1ecee0ac5b8fc203008abb39911c

Online-interview.exe:

be457f2419bb879b5bd62ce0b664112038760583cb319888968d0906e4d86889

C2 Configuration for the Checkmate Payload - version.dat:

804e8cac38c25f757f9325edb40edae93887f5c595db3aec8da6cddbc143597f

In addition, the following table indicates the three personas that have been listed on the website:

Name	Corporate Title	Company Email
Edward Miles	Manager	Edward-miles@apply-jobs[.]com
Scarlett Grant	Consultant	Scarlett-grant@apply-jobs[.]com
James Sharpe	Consultant	James-sharpe@apply-jobs[.]com

References

CyberScoop

ZDNet

aeCERT Contact Info

P.O. Box 116688

Dubai, United Arab Emirates

Tel (+971) 4 777 4003

Fax (+971) 4 777 4100

Email incident[at]aeCERT.ae

Instagram @TheUAETRA

Twitter @TheUAETRA

For secure communications with aeCERT with regards to sensitive or vulnerability information please send your correspondences to incident[at]aeCERT.ae