INNOVATIVE SOLUTIONS

Your Business. Secured!

# DNSpionage campaign targeting **Middle East**

Recently, Middle East has witnessed another **wave of cyberattacks** to its governmental entities and some private corporations. The current wave has been divided in 5 separate campaigns which were targeting the entities using phishing emails or social media. It has been observed that attackers did their homework very well before targeting the organizations and used the email and social media coupled with job opportunities to attract the users.

## ATTACK ANATOMY

Attackers have used the fake job sharing websites to post jobs online which contained malicious word office documents with embedded macros to infect the victims. The document when executed drops malicious files which are designed to avoid sandbox detection. These files are then used to start communicating with C&C servers to register the victim machines and download further instructions from C&C. This hackers enabled the malicious traffic to use HTTP and DNS mode for communicating with the C&C to avoid detection from proxies and other security devices.

## ATTACK ARTIFACTS

### Fake Websites

1. hr-wipro[.]com
2. hr-suncor[.]com
3. 0ffice36o[.]com
4. ns2.0ffice36o[.]com
5. ns1.0ffice36o[.]com
6. flarium[.]xyz
7. www.bizziniinfissi(.)com
8. hxxp://adobeupdate[.]co

### Malicious Documents

1. d2052cb9016dab6592c532d5ea47cb7e
2. c00c9f6ebf2979292d524acff19dd306
3. 807482efce3397ece64a1ded3d436139
4. 48320f502811645fa1f2f614bd8a385a
5. ba6bd22449d990be6fd9acf7e710c192
6. 6f9f5082bd4bdc1ee12cabc8facda6a0
7. d3c73d656e94dd48a1f70b5e8ee988f0
8. 744b6f1b3099d482e10c8561387f4a8b
9. 82285b6743cc5e3545d8e67740a4d04c5aed138d9f31d7c16bd11188a2042969
10. 5d65ebdde1aef8f23114f95454287e7410965288f144d880ece2a2b8c3128645
11. d8d919d884b86e4d5977598bc9d637ed53e21d5964629d0427077e08ddbcba68

### Malicious IPs

1. 185.20.184.138
2. 185.20.187.8
3. 185.161.211.72

**Our offices**

Riyadh | Jeddah | Al Khobar | Dubai | Abu Dhabi

info@is.com.sa | www.is.com.sa

INNOVATIVE SOLUTIONS

## ATTACK RESPONSE

**Innovative Solutions (IS)**, MSSP division acted swiftly and acquired the IOCs for these campaigns from the internal sources before the attack was widespread. IS team analyzed the malware behavior and shared their finding with the clients immediately for further actions. IS team proactively scanned all their client's environments for the IOCs and shared the recommendations with clients for continued protection. Few of the actions that were taken by IS team are mentioned as highlights below:

- **Scan environments** for the malicious IOCs.
- **Create Watch Lists** in Endpoint security solutions for auto bans and future alerts
- **Ban hashes** on the endpoint protection solutions for stopping execution of any malicious artifact.
- **Shared recommendations** with clients for further preventive measure to be taken from client end.
- **Update client's actively** about the incident by staying on the top of the response activity.
- **Continuous monitoring** of the client's environments for any malicious activity.

IS MSSP division has always strived for the excellence in the services being offered. We have track record of adopting the pro-active approach utilizing the skills for early detections and providing immediate support to our esteemed clients. IS currently provides four different services to their clients under the umbrella of **deep (i)™** suite to cover the security spectrum:

### deep (i)™ suite offers

- **Managed SOC Monitoring**
  Continuous Cyber Security Monitoring
- **Managed Incident Response**
  Proactive Response & Remediation
- **Managed Web Security**
  Analytics & Vulnerability Management
- **Managed Endpoint Protection**
  Complete Endpoint Detection & Response


Speed up **threat detection** and **incident response** with **deep (i)™**

**> Get free deep i demo**

Our offices
Riyadh | Jeddah | Al Khobar | Dubai | Abu Dhabi
info@is.com.sa | www.is.com.sa

INNOVATIVE SOLUTIONS