
SMART AND SAFE DIGITAL
CYBER SECURITY REPORT
JUNE 2019
DARKMATTER
darkmatter.ae

# Table of Contents

# EXECUTIVE SUMMARY

In our first semi-annual report for 2019, DarkMatter documents a growing incidence of cyberattacks across the UAE and the wider Middle East. As cybercriminals keep abreast of emerging developments in technology, they are striking in ever more sophisticated ways and aiming their weapons where they are likely to cause the most damage.

THIS REPORT HIGHLIGHTS THE THREATS AND TRENDS DARKMATTER HAS OBSERVED BETWEEN OCTOBER 2018 AND MARCH 2019 REGIONALLY AND IN THE WIDER THREAT LANDSCAPE. THE GOAL OF THIS DOCUMENT IS TO PROVIDE CLIENTS AND STAKEHOLDERS WITH A SNAPSHOT OF THE STATE OF CYBERSECURITY AND OF THE HEADLINE INCIDENTS AFFECTING THE UAE.

Breaches in the Middle East are both widespread and frequently undetected. They also increasingly appear to be state-sponsored.

This report also provides a particular focus on the UAE's critical infrastructure sectors identified as the following: **Oil and Gas, Financial, Transportation, and Electricity and Water.**

A hit on any of these critical infrastructure activities could disrupt the industry and harm the economy. Oil and Gas in particular, a pillar of the UAE's economy that is of strategic importance to the world, faces the greatest risks from globally reaching actors called Advanced Persistent Threats (APTs). General reporting remains high worldwide when it comes to long-established threat actors targeting oil and gas, such as those believed to be linked to Iran. The same actors also aim at other sectors such as transport.

Two chief motivations stand out in DarkMatter's review of threat actors operating in the region. **Espionage** is now the most prominent menace for regional organizations, accounting for the majority of the assessed campaigns. Such campaigns commonly seek illicit access to credentials and personally identifiable information to facilitate follow-on attacks. **Sabotage** is another significant motivation, as seen with the Shamoon wiper malware (also known as Disttrack) or in website defacements, and it will remain a constant threat.

Public-facing assets and infrastructures comprise the general attack surface in the UAE, partly a consequence of the country's high internet penetration rate. However, as outlined in our previous report, most of the UAE's publicly accessible hosts are located outside the nation's borders, limiting the ability to safeguard these assets.

Adequate safeguards are yet to be enforced consistently across the UAE, DarkMatter's examination reveals. Unprepared organizations remain largely exposed due to negligent and disordered systems. Weak passwords, outdated and unsupported software, insecure protocols, and open, unrestricted networks are among the most frequent vulnerabilities.

This DarkMatter report contains actionable insights for UAE enterprises, with recommended general policy outlines and a set of technical best practices.

# UNITED ARAB EMIRATES

# CRITICAL INFRASTRUCTURE: HITTING WHERE IT HURTS

In 2017, a Triton malware strike against Saudi oil giant Petro Rabigh came close to triggering high-pressure explosions of toxic hydrogen sulfide gases along the Red Sea coast.[1] Had the attack succeeded, it could have taken a considerable toll on business and human life. Other examples of destructive attacks, such as Shamoon in Saudi Arabia and Black Energy in Ukraine, left their targets with deleted files, delayed operations and proprietary losses.[2]

These are some ways critical infrastructure can be targeted to devastating effect. The term defines an asset or system that is essential to the functioning of a society and to its health and safety. As explained by the EU,[3] the damage or disruption of such resources, whether intentional or not, poses a significant danger to the security of a nation and its citizens.

In the age of hyper-connected digital economies, technology is no longer merely an extension of critical infrastructure services but plays an enabling role at the core of each service.[4] Security must consequently be ringfenced around these touchpoints. However, cyberattacks on critical infrastructure are now more sophisticated and occur more frequently, exposing worldwide governments and businesses to new risks.

In the UAE, the Telecommunications Regulatory Authority (TRA) has established the National Cyber Security Strategy (NCSS) with the aim of securing national information and communications across the country. The NCSS identifies four essential infrastructure sectors, namely oil and gas, electricity and water, finance and transportation.[5]

## Oil and Gas

Half of all cyberattacks in the Middle East target the oil and gas sector, according to a joint Siemens and Ponemon Institute report. Cybersecurity breaches remain widespread and frequently undetected, **and an estimated 75% of regional oil and gas companies have had their security in their operational technology (OT) environment compromised.**[6] Moreover, energy supply chains can extend the surface of attack, as we saw with the Shamoon 3 campaign, detailed herein, which crippled an Aramco supplier using destructive malware.

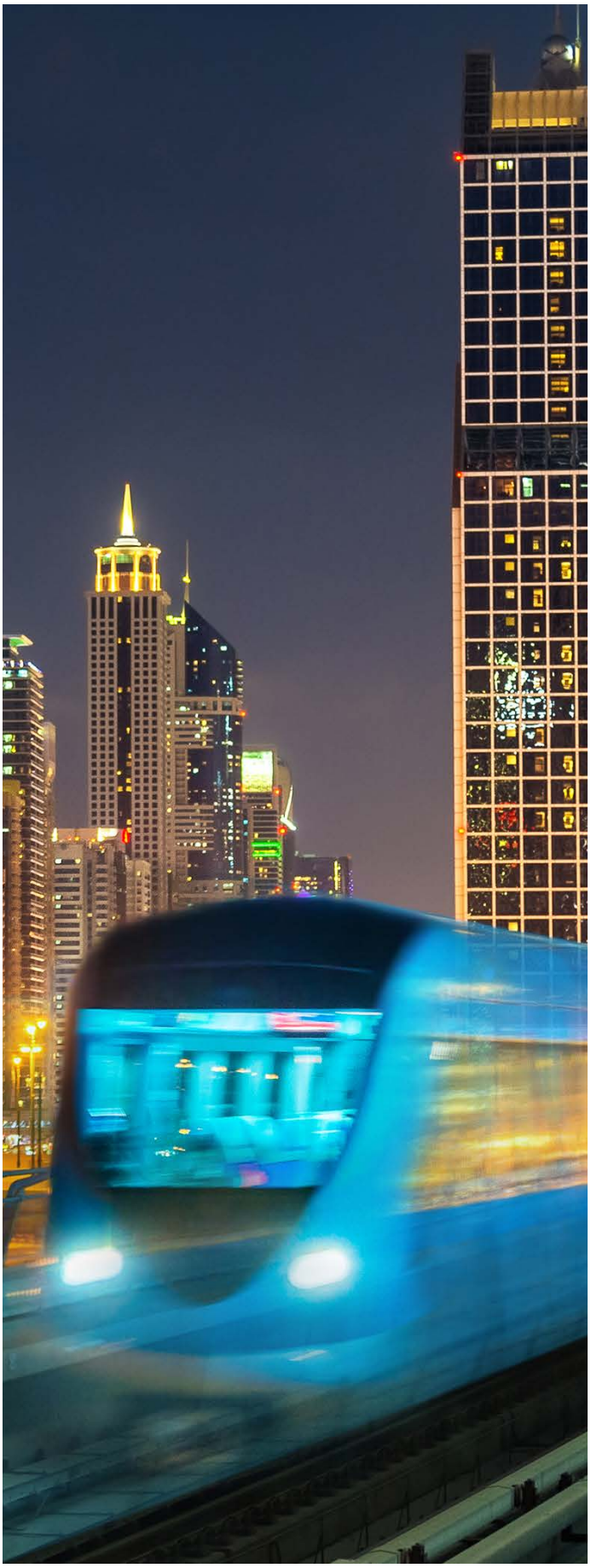
The energy industry is the mainstay of Gulf economies, and the GCC boasts $835bn in active oil and gas construction projects. In the UAE alone, sectoral contracts were worth an estimated $29.6bn between Q4 2018 and Q1 2019.[7] This commercial and strategic magnitude makes the industry an attractive target for geopolitical or economic rivals.


# Finance

The storage and movement of money has become more vulnerable as the financial sector adopts electronic channels and relies increasingly on technology. **Forbes estimates that cybercriminals target financial firms 300 times more frequently than other industries.**[8] Looked at another way, 19% of total incidents globally last year were aimed at banking and insurance, IBM reports, citing the quick monetization of customer data as incentives.[9]

The GCC is among the world's fastest growing markets with a mature and profitable banking sector. As the UAE has established itself as the region's financial hub, the nation's banks have also grown.

**The extent of the sector sees the UAE ranked sixth on Kaspersky's list of most targeted countries by banking malware** attacks in Q3 2018.[10] As financial activity increases, a further increase in malware attacks is to be expected.



# Transportation

Transportation comprises complex networks, high volumes of real-time data and large numbers of embedded devices. Technology underpins the value chain from satellite communications to the delivery of a parcel, and minimal damage to one segment can adversely affect multiple businesses and civilians.

**IBM identified transportation services, including air, bus, rail and water, as the second most targeted sector globally in 2018, with 13% of all recorded cyberattacks.**[11] The industry's continuous reliance on information technology presents a wide attack surface for malicious entities, proving an attractive target for cybercriminals such as DarkHydrus, OilRig, and APT39.

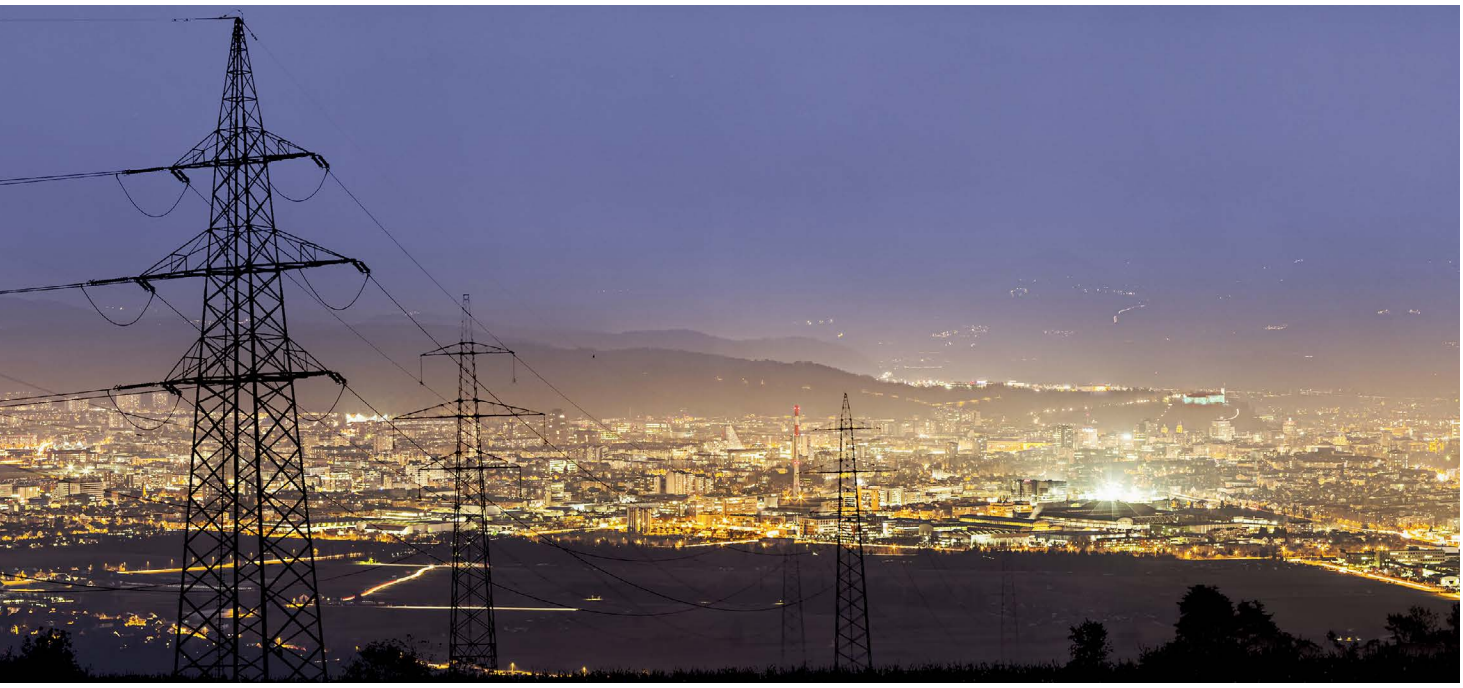
In the UAE, transport remains a significant business activity. Both Abu Dhabi and Dubai consider the sector as a development pillar of their vision strategies for the decade to 2030,[12] and greater prominence raises the likelihood of adverse actions in the future.

# Water and Electricity

Utilities such as water and electricity present a prime target for cybercriminals, with their role as the backbone of every nation's infrastructure. Both are essential to economic and national security and to the daily functioning of a wide range of other industries.

**When compared with other industries, an attack on the utilities sector has significantly greater potential for damage, with widespread outage and cascading effects rippling across the economy, since every enterprise relies on energy for its daily functions.**

Government departments in the UAE's utilities sector have made significant efforts to bolster defenses around water and energy facilities.[13]

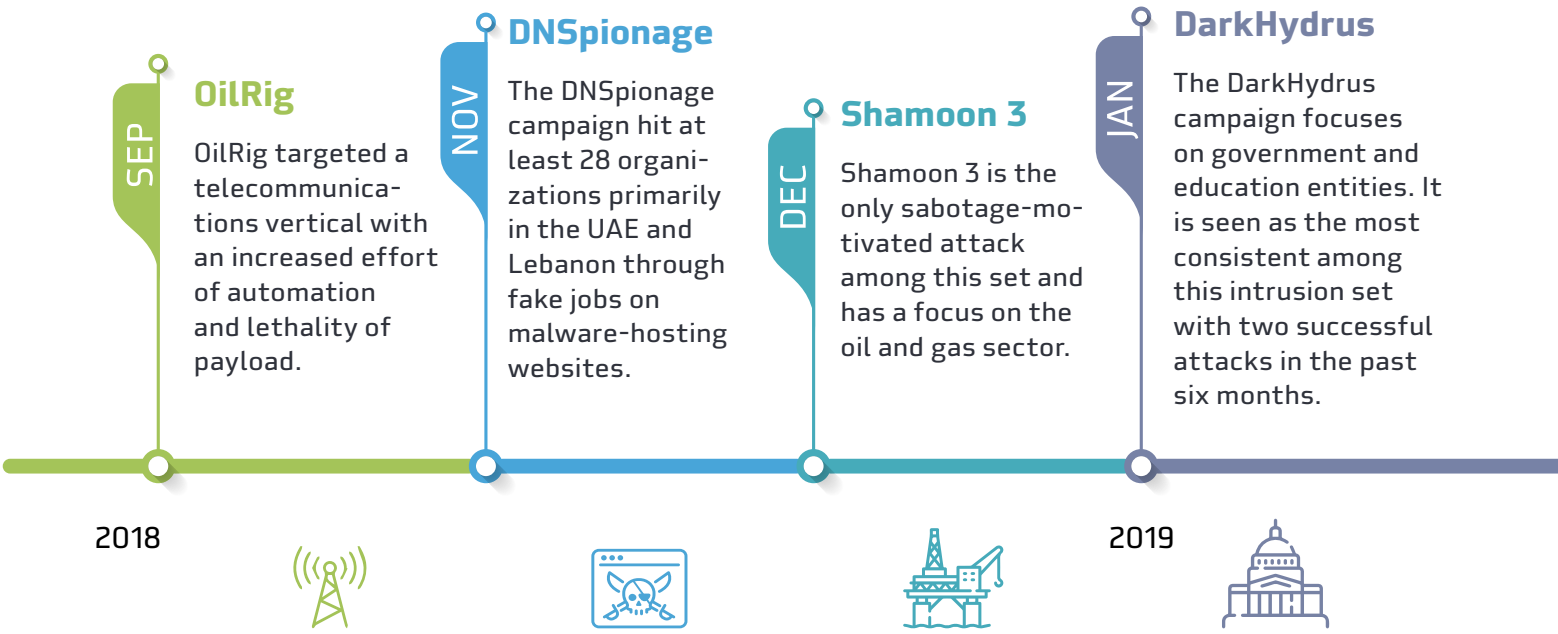


# INTRUSION SETS

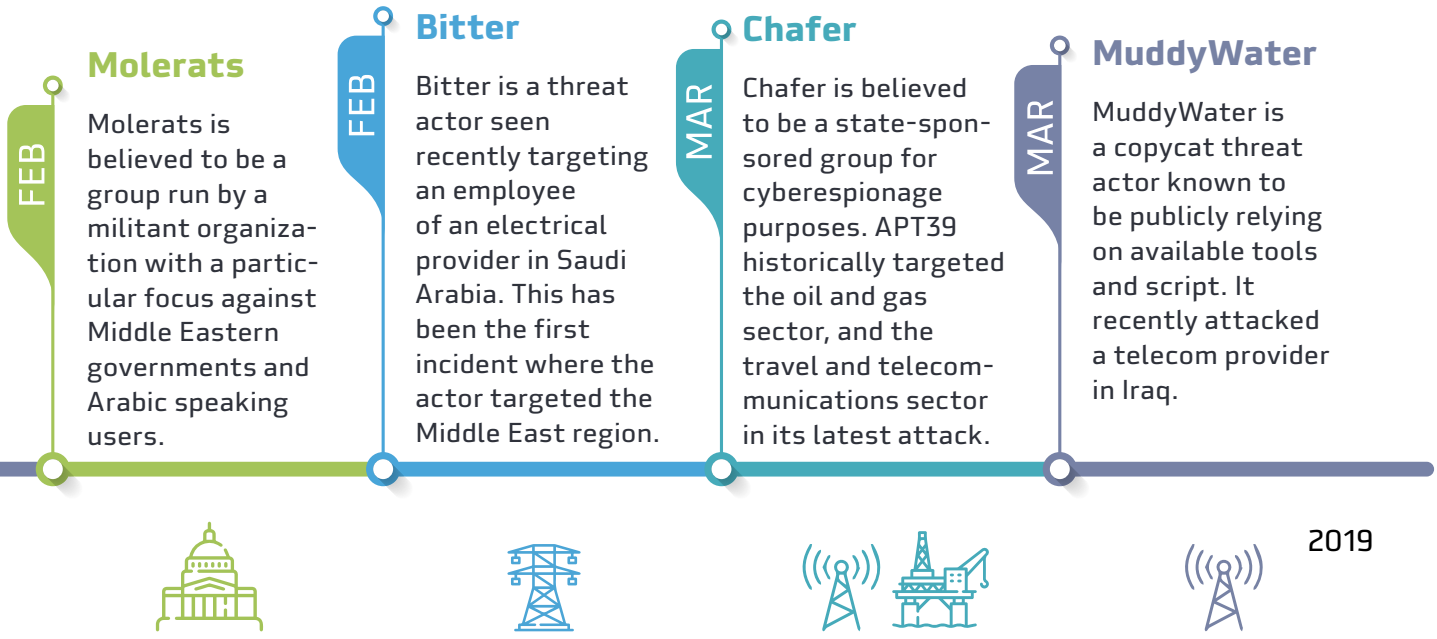
An intrusion set is a group of antagonistic actions and resources with common properties that is thought to be orchestrated by a single organization. Below, DarkMatter describes the threat actors and campaigns targeting critical infrastructure observed since the last DarkMatter Cyber Security Report in November 2018.

The most common motivation is **cyberespionage**, where the objective is to obtain confidential or sensitive information towards a broader goal. Credential and personally identifiable information theft are included in this understanding of a threat actor's intent. Such information is often used in follow-on operations such as crafting spear phishing attacks or compromising target systems in order to acquire further data.

Cyberespionage differs from **sabotage**, another common kind of cyberattack, in that threat actors seek to undermine an organization by corrupting its assets or conducting denial of service attacks. DarkMatter details one campaign, Shamoon 3, where sabotage appeared to be the primary motivation. The figure below provides a timeline of activities.




Note: Indicated dates are when cyber activities were reported.




DarkMatter's analysis of the actors and campaigns covered in this report establishes that **spear phishing is the principal means of gaining access to targets.** This could be because cybercriminals have become better at creating authentic-looking emails, or because more personal information is now available on social media, helping aggressors create personalized and believable messages. Moreover, **75% of documented intrusion sets appear to be motivated primarily by cyberespionage actions**, such as stealing remote access credentials and personal information. Finally, all the identified intrusion sets in the following section have hit critical infrastructure in the UAE and regionally.

Eight actors and campaigns are covered in this report.

# A. MuddyWater

A copycat actor relying on known and publicly available code that has been operational since 2017, MuddyWater recently attacked Korek Telecom, an Iraq-based telecom provider that services at least 18 provinces. According to 360Lab researchers,[14] the attack on the Iraqi organization used Powerstats, a PowerShell backdoor, and was delivered via a spear phishing email that induced users to open Microsoft Word documents.

MuddyWater mainly targets victims in the Middle East using Living off the Land (LotL) techniques.[15] Its previous targets include several government agencies, communications firms, and oil and gas companies in the Middle East between 2017 and 2018.[16]

**THREAT ACTOR**

MuddyWater, Static Kitten

**THREAT VECTOR**

Spear phishing

**TARGET COUNTRIES**

UAE, Saudi Arabia, Oman, Lebanon, Pakistan, India, Iraq, Georgia, Turkey, Tajikistan, Israel, USA

**TARGET INDUSTRIES**

Oil and Gas, Government, Telecommunications

**MOTIVATION**

Cyberespionage

**MALICIOUS TOOLS**

Powerstats

# B. Chafer

Chafer is a cyberespionage threat actor believed to be sponsored by the Iranian government. Previously mentioned in DarkMatter's November 2018 Cyber Security Report, the group has historically targeted critical infrastructure sectors. It began cyberespionage activities as early as 2014 but was only exposed by Symantec in December 2015.[17] Recent victims have been travel and telecommunications companies in Turkey, as well as diplomatic missions within Iran, where it has sought to harvest personal data about individuals of interest. The latest attack used a Python-based payload, which Palo Alto Unit 42 calls MechaFlounder.[18] Created by Chafer itself, the MechaFlounder Trojan supports file upload, download and command execution functionality to help the threat actor meet its objectives. Chafer also uses the Living off the Land (LotL) tactic to evade endpoint protection platforms with highly sophisticated attacks. The recent development shows a greater interest in stealing personal data, in contrast with other Iranian groups that traditionally target government and commercial information.

**THREAT ACTOR**

Chafer, APT39

**THREAT VECTOR**

Spear phishing

**TARGET COUNTRIES**

UAE, Saudi Arabia, Turkey, India, Iran, Scotland, Italy, UK

**TARGET INDUSTRIES**

Oil and Gas, Transportation, Government, Telecommunications

**MOTIVATION**

Cyberespionage

**MALICIOUS TOOLS**

Remexi, POWBAT, Mimikatz, SEAWEED, xCmdSvc, CACHEMONEY, webshells

# C. Bitter

Bitter is a threat actor seen recently targeting an employee of an electricity provider in Saudi Arabia. Its activities were first observed in 2015, and it has previously attacked Pakistan and China by delivering a variant of the ArtraDownloader malware via spear phishing mails. Bitter's victims are critical infrastructure utilities, such as the Saudi electricity provider and a Pakistani hydraulics company.

A shift in geographic direction, coupled with Bitter's focus industries, amplifies the possibility that the UAE will be among its next targets.

**THREAT ACTOR**

Bitter

**THREAT VECTOR**

Spear phishing

**TARGET COUNTRIES**

Saudi Arabia, Pakistan, China

**TARGET INDUSTRIES**

Government, Electricity and Water (Electricity and Hydraulics)

**MOTIVATION**

Cyberespionage

**MALICIOUS TOOLS**

ArtraDownloader

# D. Molerats

Molerats' most recent activity was a phishing attack aimed at Arabic-speaking users, a tactic it has used since it was identified in 2012. The group first grabbed media attention that year after it attacked the Israeli government, temporarily cutting off internet access for its entire police force. After broadening its reach to Palestinian organizations and British and US targets, Molerats took aim at governments, oil and gas companies, media organizations, activists, diplomats and politicians in countries such as Egypt, the UAE, Yemen, Jordan, Libya, Iran, and Israel.[19]

Given its focus on the Middle East and its history of attacking the UAE, it is probable that this politically motivated group will resume targeting entities within the country and the region.

**THREAT ACTOR**

Molerats, Gaza Cybergang, Gaza Hackers Team, Moonlight, Extreme Jackal

**THREAT VECTOR**

Spear phishing

**TARGET COUNTRIES**

UAE, Saudi Arabia, Egypt, Jordan, Libya, Iran, Iraq, Israel, USA, UK

**TARGET INDUSTRIES**

Oil and Gas, Government (Diplomats), Media

**MOTIVATION**

Cyberespionage

**MALICIOUS TOOLS**

Xtreme RAT, njRAT

# E. DarkHydrus

DarkHydrus' latest attack came to light on 9 January 2019 when 360TIC researchers [20] secured several malicious Microsoft Excel documents containing politically charged content in Arabic. The campaign was aimed at the government, the transport industry and educational institutions in the Middle East, using lure documents containing malicious code to extract information from its targets. The group continues to deliver politically motivated content while developing new techniques to enrich its expanding playbook. The delivery documents revealed how the group is abusing open-source penetration-testing techniques while its payloads use the RogueRobin Trojan, developing different variants that employ the Google Drive cloud service as a C2 channel.

**THREAT ACTOR**

DarkHydrus, LazyMeerkat, RogueRobin

**THREAT VECTOR**

Spear phishing

**TARGET COUNTRIES**

UAE, Saudi Arabia, Turkey

**TARGET INDUSTRIES**

Transportation (Aviation), Government, Education

**MOTIVATION**

Cyberespionage

**MALICIOUS TOOLS**

RogueRobin, Phishery

# F. Shamoon 3

A modification of the data-wiping malware Shamoon, also known as Disttrack or Shamoon 3, hit Italian oil services firm Saipem in December 2018.[21] Saipem's facilities in three locations were affected: in the Middle East, Aberdeen in the UK, and in Italy. Saudi Arabia's Aramco is Saipem's largest customer. Symantec reported that two other organizations in Saudi Arabia and the UAE, both in oil and gas, were attacked in the same week.[22] The affected companies in the UAE were not identified.

Shamoon, a cybersabotage threat campaign that has suspected links with Iran because of its choice of targets, has targeted regional and international victims since 2012. Shamoon malware can overwrite the Master Boot Record (MBR) and damage system files and partitions with randomly generated data. Consistent with its predecessors, Shamoon 3's destructive payload was a wiper. The newest iteration is considered deadlier than before, since it renders files unrecoverable by first wiping them with Filerase malware. These actions indicate Shamoon's motivations go beyond financial gains towards supporting nation-state interests.

**THREAT ACTOR**

Shamoon 3

**THREAT VECTOR**

Spear phishing

**TARGET COUNTRIES**

UAE, Saudi Arabia, India, Scotland, Italy

**TARGET INDUSTRIES**

Oil and Gas, Transportation, Government

**MOTIVATION**

Sabotage

**MALICIOUS TOOLS**

Disttrack, Filerase

# G. OilRig

OilRig targeted a telecommunications player in early November 2018.[23] DarkMatter believes these attacks are highly likely to continue as OilRig builds capabilities and confidence in its methods, including increased levels of automation and deadlier payloads. OilRig attacks mainly use spear phishing emails as an initial infection vector. The group then deploys custom-developed backdoors such as Helminth[24] to control the compromised system, exfiltrate files and download other samples onto target machines. The initial part of Oilrig's attack process does not differ from other threat actors, such as DarkHydrus, in terms of establishing the foundation of attacks. Once in place, OilRig uses its new administrative rights to expand its privileges on the compromised system.

Other OilRig Tactics, Techniques and Procedures (TTPs) include account manipulation, brute force, and access to credentials in order to scrub sensitive accounts and information.

**THREAT ACTOR**

OilRig, APT34, Helix Kitten, Helminth, Clayslide, IRN2

**THREAT VECTOR**

Spear phishing

**TARGET COUNTRIES**

UAE, Saudi Arabia, Qatar, Kuwait, Turkey, Lebanon, Israel, USA

**TARGET INDUSTRIES**

Transportation (Aviation), Financial, Government, Energy, Chemical, Telecommunications

**MOTIVATION**

Cyberespionage

**MALICIOUS TOOLS**

Bondupdater

# H. DNSpionage

The DNSpionage campaign hit at least 28 organizations in various MENA countries, primarily the UAE and Lebanon, by luring victims to respond to a fake job campaign.[25] Fake job vacancies purportedly from the likes of Wipro and Suncor were posted on malware-hosting websites to attract intended victims. A DNS-hijacking technique then redirected all the target organization's traffic to attacker-controlled infrastructure.

DNSpionage's previous attacks on the UAE elevate the likelihood of a recurrence as attackers continue to support intelligence collection operations against their targets and organizations related to those targets.

**THREAT ACTOR**

DNSpionage, Cold River

**THREAT VECTOR**

Spear phishing

**TARGET COUNTRIES**

UAE, Saudi Arabia, Qatar, Kuwait, Lebanon, Turkey, Israel, Iran, USA

**TARGET INDUSTRIES**

Transportation (Aviation), Financial (Banks), Government, Energy, Telecommunications

**MOTIVATION**

Cyberespionage

**MALICIOUS TOOLS**

DNSpionage

# UAE INTERNET FOOTPRINT

DarkMatter outlines the general attack surface of the UAE in order to assess the likelihood of global threat actors targeting the region. The adoption rate of internet-connected devices as well as the depth of public-facing infrastructure outlines the scope of the attack surface, revealing possible targets as well as potential vulnerabilities that are ripe for exploitation.

The UAE's digital ecosystem offers an expanded attack surface for cybercrime. The UAE has the second-highest smartphone adoption rate globally at 85% after Singapore,[26] and the nation is one of the world's most interconnected countries.[27] The importance of the UAE provides an attractive mark for cyberattacks. With a GDP of $382 billion, the Middle East's third-largest economy is one of the region's most-targeted countries. Symantec's [28] 2019 Internet Security Threat Report ranks the UAE 10th in the rate of malicious emails (third in the Middle East) and ninth in the number of targeted attacks by known threat actors.

DarkMatter examined public-facing infrastructure as a whole, since it is accessed by all organizations and individuals. Our analysis also encompasses public-facing assets belonging to organizations within the main critical infrastructure sectors. Significant concerns became apparent. A large number of public-facing assets exhibit several critical or high vulnerabilities, and the majority of hosts under the AE top-level domain lie beyond the nation's political borders. **Digital assets belonging to UAE-based organizations in general are particularly exposed, with about 75% of hosts belonging to all observed UAE organizations located outside the UAE.**

On the other hand, public-facing assets from organizations within the critical infrastructure sectors are more localized. Only 8.6% of these assets were hosted outside, and they displayed far fewer vulnerabilities proportionally.

## Known Vulnerabilities

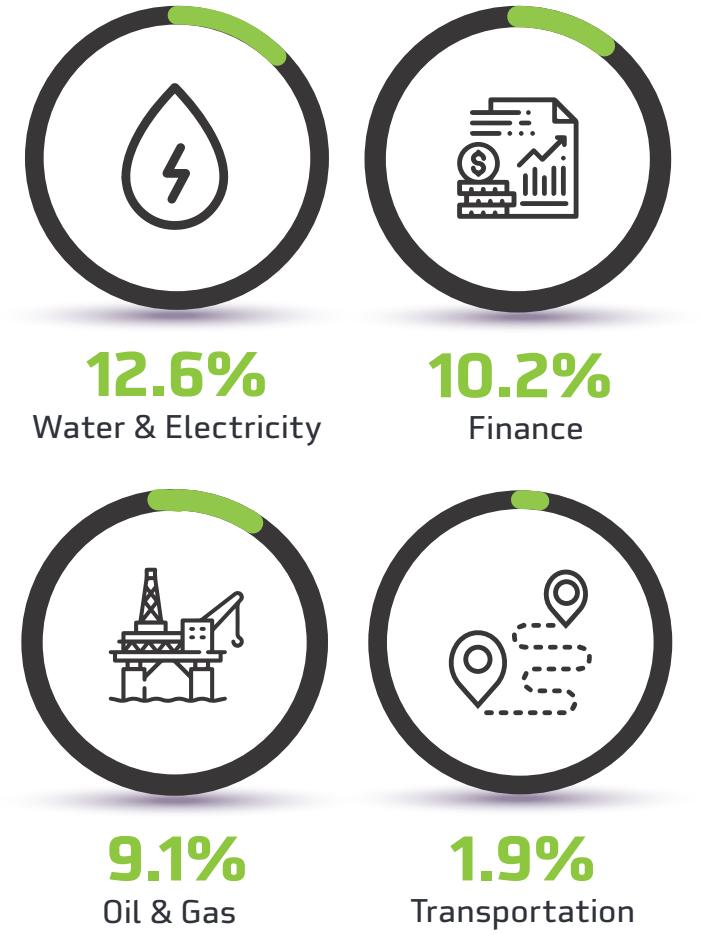
There were 64,530 vulnerabilities rated 'high' or 'critical' (a score of 7 or above on the Common Vulnerability Scoring System) from the 647,891 observed public-facing hosts located in the UAE. A total of 1,949 of these were rated as 'critical', with nearly 49% of vulnerabilities arising from management issues of permissions and access control. Public-facing assets in the critical infrastructure sector had a better security posture, with less than 1% reporting vulnerabilities rated as 'high' or 'critical'.

## Foreign Hosting

DarkMatter observed that 102,750 of the 137,000+ websites under the .AE top-level domain are hosted outside territorial borders. The use of international webhosting services indicates that the majority of UAE organizations do not have complete sovereignty of their systems and information, which places sensitive data and operations at risk.

Public hosts belonging to critical infrastructure-based organizations were more localized with just 8.6% situated outside the UAE. Public-facing systems in the electricity and water industry had the most international hosts at 12.6%, followed by finance at 10.2%, oil and gas at 9.1%, and transportation at 1.9%.

## Percentage of Critical Infrastructure Hosts outside UAE

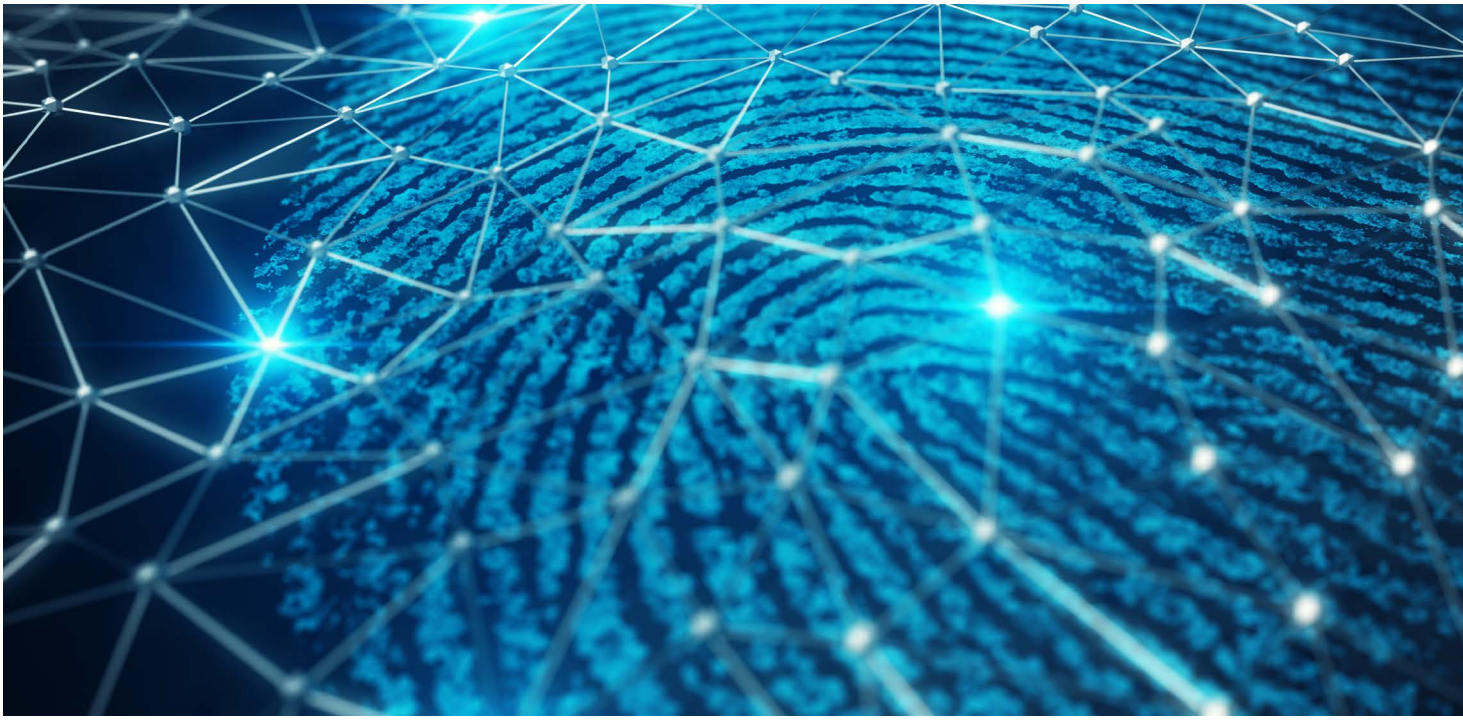


**12.6%**
Water & Electricity

**10.2%**
Finance

**9.1%**
Oil & Gas

**1.9%**
Transportation



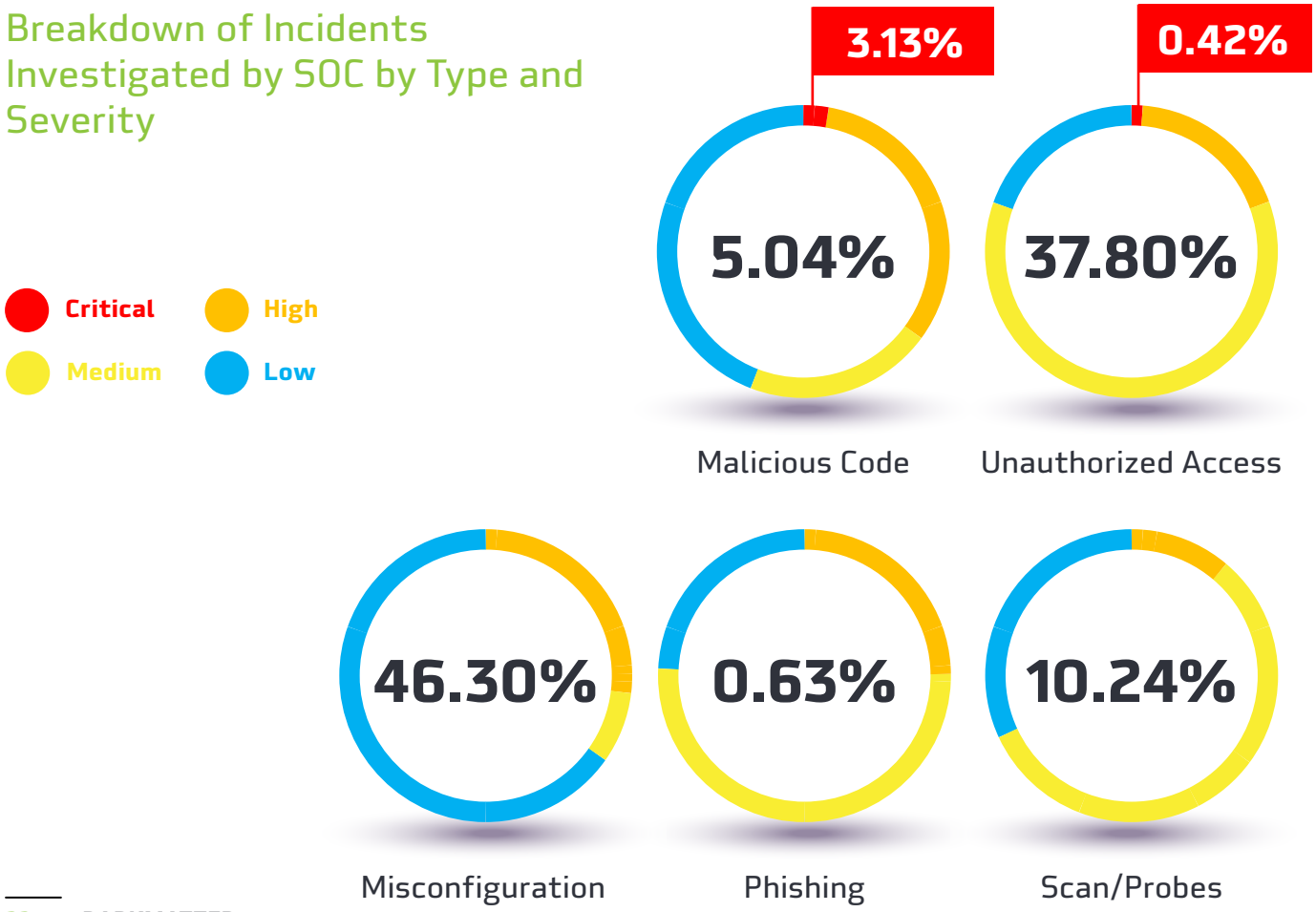
# INCIDENT TYPES

## Unauthorized Access and Misconfigurations at Fault

From November 2018 to March 2019, Security Operations Centers (SOCs) run by DarkMatter, investigated numerous incidents across multiple industries, including in critical infrastructure. Approximately 1% of incidents rose to the level of 'critical' and 23% were rated as 'high' according to aeCert's scale – meaning great harm could be done to an organization. These incidents were classified under the categories of 'Malicious Code' and 'Unauthorized Access'.

The vast majority of DarkMatter's investigations focused around unauthorized access (37.8%) and misconfiguration (46.3%). Those patterns of activity highlight devices with improper or insecure configurations.

### Breakdown of Incidents Investigated by SOC by Type and Severity



# Darkmatter Observed Attack

DarkMatter's Security Operations Centers were alerted to an attack against an individual at an organization in a critical infrastructure sector. DarkMatter's initial observations showed a carefully crafted email containing a OneDrive hyperlink. Delivery was instantly blocked and the email did not reach the intended party.

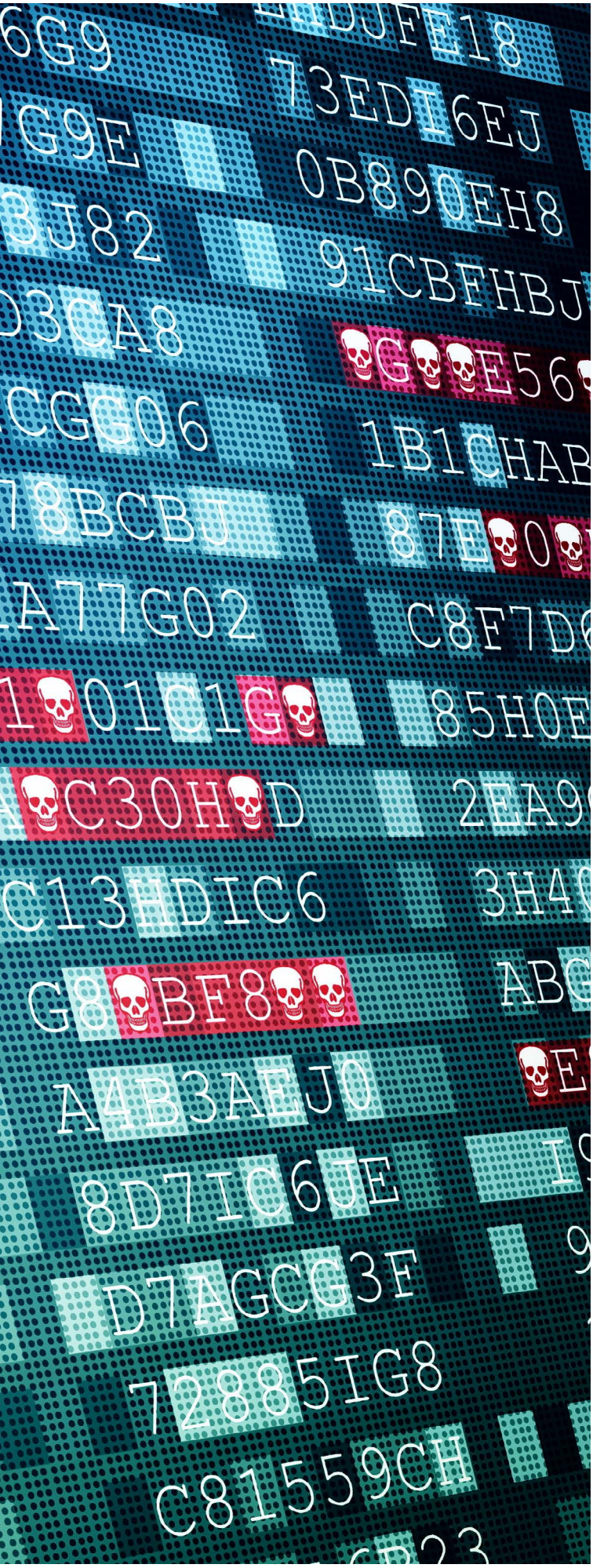
After further analysis, DarkMatter discerned that the email was crafted to appear to come from a legitimate and likely sender using "typosquatting", when a domain is structured to look like a known legitimate site. A OneDrive hyperlink within the email pointed to a compressed executable identified as NanoCore RAT, a popular remote access Trojan available on the open market since 2015. The malware's C2 was tied to an external Dynamic DNS domain.

A couple of indicators highlighted that **the strike was aimed specifically at individuals within the critical infrastructure sector**. The typosquatting domain was named to resemble a business that would be in correspondence with the individual's organization. Additional analysis suggests the domain was created specifically for this attack.

The attackers were halted from successfully implementing the first stage of their attack as DarkMatter was able to analyze and leverage the resulting indicators for further monitoring. Nevertheless, the nature of the incident reflects a common pattern we have observed with threat actors aiming at critical infrastructure in the UAE: **Attacks are highly customized when targeting individuals within the critical infrastructure sectors**.

| | |
|---|---|
| **SUMMARY** | Detection and mitigation of an Advanced Persistent Threat (APT) from a malicious email crafted to target an individual within an organization belonging to a critical infrastructure sector |
| **THREAT ACTOR** | Shares some infrastructure and tools with known state-sponsored actors |
| **THREAT VECTOR** | Payload delivery is through social engineering, targeting email as channel utilizing spear phishing. Typosquatting is leveraged to further appear legitimate |
| **FUNCTIONALITY** | . OneDrive hyperlink pointing to a compressed executable<br>. Executable installs NanoCore RAT<br>. Command and Control activity points to Dynamic DNS domain<br>. Domain was crafted spacifically for attack |
| **INDICATOR OF COMPROMISE** | Network level IOC - Domain C&C |
| **RESPONSE** | DarkMatter analysis provided additional indicators to further detect any additional targeting |
| **RECOVERY** | Advise client on the nature of the targeted attack. User awareness training on spotting similar spear phishing attempts |


4E
ABB
112
C3G
6EE0
9GGC
E62G5
JF2HG
C8FBJG
7EG202
35E
E
BG
812
D7AGCGBF
72885IG8
C81
CH
F96A6B23
9FC65B1B
JACA375I
EJ
AIA
4I833
IG857188
JF44CG65
4B330DID
J375H24E
34E5BABB



# Multiple Vulnerabilities Discovered in ABB Products

Security researchers from xen1thLabs, a DarkMatter company that conducts vulnerability research, discovered a number of vulnerabilities in February this year. These were identified in the Human Machine Interface (HMI) solution "Panel Builder 600" from ABB and its related components. ABB works closely with utilities, industry, transportation and critical infrastructure customers around the world. Supervisory Control and Data Acquisition (SCADA) systems are crucial for critical (industrial) organizations since they help to maintain efficiency and process data by communicating real-time system issues.

The discovered vulnerabilities could create security risks within the Industrial Control Systems (ICS) environment. A malicious attacker could abuse these vulnerabilities to compromise the software in order to execute attacker-controlled code on affected devices and computers. Even after a device has been restarted, the attacker still has control and will always have a way to regain access to the compromised environment. Examples of such attacks could be to inject a backdoor into all new and existing HMI projects, deliver a worm that will infect other SCADA systems on the same network, or cause significant damage to critical infrastructure.

Several of these issues exist within the authentication functionality, which allows exploitation without authentication. Furthermore, the transport protocols by browsers, used are standard protocols supported by browsers, making them ideal for spear phishing and watering hole attacks.

xen1thLabs performed coordinated disclosure with the vendor resulting in ABB patching nine security flaws in multiple affected SCADA and ICS products.

# SECURITY WEAKNESSES

DarkMatter's Cyber Network Defense team identified several vulnerabilities and configuration flaws during its technical assessments. Although the organizations involved in these assessments are not tied to the critical infrastructure sector, they offer an update to our November 2018 Cyber Security Report and highlight the security posture at UAE-based enterprises in general.

## Outdated Software

**91%** of our assessments found organizations with outdated software. Target organizations and their assets remain exposed as cybercriminals continue to find and exploit loopholes. Among operating systems and network services, we discovered numerous examples of critical assets missing essential security patches, including high-level risk vulnerabilities in outdated software and services such as Windows OS, Linux, and popular web servers such as IIS and Apache.

## Credential Problems

**91%** of DarkMatter's reviews discovered systems that are vulnerable to remote access due to easily exploitable weak or default passwords. 52% of issues were due to the sustained use of default administrative credentials. Credentials include passwords, usernames, e-mail addresses, and system certificates. Passwords in particular could be easily guessed or acquired through a simple dictionary attack, and in situations involving those with admin rights, attackers gained access to system functionalities. The risks are notably higher at public-facing assets as cybercriminals often employed automated processes and targeted accounts indiscriminately with default or predictable credentials.

## Insecure Protocols

**87%** of our assessments revealed organizations continue to use insecure protocols such as telnet, FTP, HTTP, and SMTP. In such cases, data was transferred over internal and external networks with clear-text packets.

## Unsupported Software

**83%** of our appraisals showed the continued use of unsupported software such as operating systems, web servers, and other network services. In contrast with outdated software, which requires critical security patches, unsupported software is no longer serviced by vendors. Therefore, protections for critical vulnerabilities that could be exploited by malicious actors are unlikely to be unavailable.

## Poor Configuration

**74%** of enterprises used critical network services with security issues arising from poor configuration, such as the failure to follow best practices with system permissions, allowing remote or anonymous logins, and disabling important security safeguards. DarkMatter observed configuration issues across a range of systems, including Microsoft Windows servers, Microsoft Active Directory, Linux servers and other network devices.

## Inadequate Network Segregation

**61%** of organizations failed to implement proper network segregation. In a few cases, DarkMatter discovered wireless guest networks with connectivity to business-critical internal networks. Appropriate segregation prevents users and devices from accessing services beyond their needs. This is important because even if a user's credentials are compromised, attack fallout is limited to specific network areas.

## Outdated Software: Most Frequent Vulnerabilities and Exposures (CVE) Types

DarkMatter leverages the Common Vulnerability and Exposure (CVE) standardization to describe publicly known vulnerabilities. Every known vulnerability has a CVE identification number and is categorized under a general type. All organizations assessed had systems with vulnerabilities identified by a CVE. Of the 20 most common CVEs discovered by DarkMatter's Cyber Network Defense team, Information Disclosure / Leak was the most common type. Such vulnerabilities allow an attacker to obtain sensitive information that could be used in launching further attacks. **Nearly half (45%) of the 20 most common CVEs affecting the organizations would have an impact severity of 'high' or 'critical'.**


Information Leak / Disclosure


Data Handling


Input Validation


Buffer Errors


Double Free


Improper Access Control


Other

# RECOMMENDATIONS

BASED ON OUR KEY FINDINGS OVER THE REVIEW PERIOD, DARKMATTER RECOMMENDS THE FOLLOWING BEST PRACTICES:

## Organizational

### Awareness Training

Ensure security awareness programs are implemented across the organization. The human factor remains the most targeted vulnerability by threat actors.

### Multi-factor Authentication

Stolen credentials are a key target for threat actors, so it is essential to implement multi-factor authentication. This simple security mechanism can help mitigate credential theft.

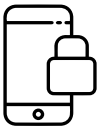
### Configuration Management

Misconfigurations are most likely to occur during security change processes. A configuration management procedure helps prevent such incidents. Standard configurations must accord with industry best practices and be continuously monitored for changes to quickly identify a misconfiguration weakness that could be exploited by threat actors.

### Password Hygiene

Change default passwords as soon as a new system or software is added to the network. Where possible, account lockout mechanisms should be enabled to mitigate authentication attacks. At a minimum, ensure that all passwords deployed are different, secure and follow a complex password policy defined by the organization. Such a policy must cover the following points:

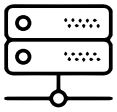
- Do not use passwords found in dictionaries.
- Passwords should be memorable.
- Use passphrases instead of passwords.



### Mobile Device Management

Implement a mobile device management solution for corporate devices, with effective security policies and the ability to quarantine devices.

## Technical



### Network

Implement a sender policy framework to help avoid the use of spoofed internal domains. Threat actors adopt such methods in spear phishing attacks to deceive the target into believing a malicious email originates from an internal source.

Disable unnecessary network protocols. When required by the business, they should be replaced with secure protocols such as Secure Shell (SSH), HTTPS and SNMPv3.

Employ network segmentation so that actual zoning isolation is effective. Segregate the network according to the principle of least privilege. Configure the network so users, servers, and other devices may only access the minimum services required to perform their tasks.

### Device

An automated enterprise software patch management solution is integral to a comprehensive security program. It is important that all applications including the underlying operating system and its components are up to date. New vulnerabilities and exploits are released frequently and when they are not patched, an organization is exposed to unnecessary risk.

Upgrade all outdated software to the latest version.

Deploy endpoint protection platform solutions that can monitor and flag suspicious real-time events, such as the use of PowerShell. Additional endpoint protection solutions that leverage whitelisting, where only explicitly allowed executables can be run by the user, would provide further protection. Any endpoint security solution should also include traditional malware detection methods.

# SUMMARY

DarkMatter's semi-annual report 2019 reviews the threat landscape against which the typical connected organization in the Middle East operates.

Cyberespionage has emerged as the principal security threat for the critical infrastructure sector, while sabotage remains a clear and ever-present danger. Attackers commonly use spear phishing to obtain credentials and now employ creative, customized and multi-layered approaches to deceive their targets into sharing access data. Additionally, public-facing web assets are being placed at considerable risk due to their exposure as a result of international hosting.

UAE ORGANIZATIONS ARE EXPOSED WITH WEAK CREDENTIALS, UNSUPPORTED SOFTWARE AND UNSEGREGATED NETWORKS, AMONG OTHER HAZARDS. DARKMATTER'S REVIEW OF SECURITY WEAKNESSES, TRENDS IN CAMPAIGNS AND THE SECURITY POSTURE OF ITS CLIENT BASE, REVEALS THAT VIRTUALLY ALL INDUSTRY SECTORS REMAIN VULNERABLE TO THESE OMNIPRESENT THREATS.

DarkMatter's analysis over the review period indicates that the UAE's critical infrastructure will remain frequently targeted by threat actors operating on a global scale.

DarkMatter's Threat Intelligence capability provides timely and actionable intelligence so that clients are better armed against today's attacks and can anticipate emerging threats and effectively manage their security posture.

DarkMatter's integrated and efficient solutions support enterprises through reliable and cost-effective threat information that protects the brand, data and information, and information systems. By collaborating with the highly specialized analysts in our Threat Intelligence Center (TIC), Security Operations Center (SOC), Cyber Network Defense Team (CND), Test and Validation Labs (xen1thLabs), and Cyber Intelligence Systems (CIS), DarkMatter clients benefit from insightful information about the UAE threat landscape. DarkMatter uses competencies across information security, cyber and threat intelligence and incident response to collect, analyze, disseminate and formulate multimodal strategies that can be leveraged to protect the enterprise from criminal activities and events.

# ABOUT DARKMATTER GROUP

The DarkMatter Group exists to enable businesses and governments to become smart, safe, and cyber resilient.

As an end-to-end provider of smart and safe digital transformation, we are uniquely positioned to provide organizations with the strategy, technology, and operating model to achieve business continuity amidst adverse and constantly evolving cyber threats. Our strength lies in the diversity of our practices:

**DARKMATTER**
CYBER DEFENSE

Provides an 'always on' cyber security transformation for businesses and governments so that they can safely perform their mission in the face of accelerating cyber risks.

**DIGITALX1**

Supports business and governments in digitally and smartly transforming their ways-of-working to achieve unprecedented levels of operational efficiency and effectiveness.

**DARKMATTER**
SECURE SOLUTIONS

Offers ultra-secure unified communications solutions that allow businesses and governments to protect their business operations and data, giving them control and peace of mind.

**DIGITALX1**

Enables businesses and governments in advancing the digital and cyber security dexterity of their human capital.

**DARKMATTER**
GOVERNMENT SOLUTIONS

Tailors technologies to help governments strengthen their defense and security to mitigate risks.

xen1thLabs

Conducts vulnerability research, including the testing and validation activities it covers across software, hardware and telecommunication. xen1thLabs houses a team of world-class experts dedicated to providing high impact capabilities in cyber security, uncovering new vulnerabilities that combat tomorrow's threats today.

DIGITALTRUST

Provides PKI and identity services, utilized to secure web sites, web services and TLS communications.

ajyal
Talent Management

Provides educational consultancy services and talent acceleration to strengthen the UAE's future generations of human capital.

DarkMatter Group provides bespoke solutions for a selection of vital sectors including defense and intelligence, civil government, financial services, transportation, energy, and telecommunications.

**CONTACT:**

Level 15, Aldar HQ, PO Box 27655
Abu Dhabi, United Arab Emirates
+971 2 417 1417
contactus@darkmatter.ae
darkmatter.ae

EXPO 2020 إكسبو
دبي، الإمـــارات العربيـة المتحـدة
DUBAI, UNITED ARAB EMIRATES

OFFICIAL PROVIDER | مزود رسمي

# REFERENCES


1. https://www.eenews.net/stories/1060123327
2. http://www.cybelius.fr/en/2017/12/19/industrie-energetique-top-6-des-plus-grandes-cyberattaques/
3. https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en
4. https://blogs.cisco.com/security/securing-critical-infrastructure-in-the-digital-age
5. https://www.government.ae/en/about-the-uae/strategies-initiatives-and-awards/federal-governments-strategies-and-plans/national-cyber-security-strategy-of-the-uae
6. https://cyber-peace.org/wp-content/uploads/2018/03/cyber_security_report.pdf
7. http://get.protenders.com/protenders-reports-2018-gcc-construction-overview
8. https://www.forbes.com/sites/bhaktimirchandani/2018/08/28/laughing-all-the-way-to-the-bank-cybercriminals-targeting-us-financial-institutions/#ce179876e906
9. https://community.ibm.com/community/user/security/events/event-description?CalendarEventKey=e1e34b7f-2183-4dd2-9321-86c13988cdda&CommunityKey=96f617c5-4f90-4eb0-baec-2d0c4c22ab50&Home=/community/user/events/upcomingevents
10. https://securelist.com/it-threat-evolution-q3-2018-statistics/88689/
11. https://www.ibm.com/security/data-breach/threat-intelligence
12. https://government.ae/en/more/uae-future/2021-2030
13. https://government.ae/en/information-and-services/environment-and-energy/water-and-energy
14. https://ti.360.net/blog/articles/suspected-muddywater-apt-organization-latest-attack-activity-analysis-against-iraqi-mobile-operator-korek-telecom/
15. https://reaqta.com/2017/11/muddywater-apt-targeting-middle-east/
16. https://unit42.paloaltonetworks.com/unit42-muddying-the-water-targeted-attacks-in-the-middle-east/
17. https://www.symantec.com/connect/blogs/iran-based-attackers-use-back-door-threats-spy-middle-eastern-targets
18. https://unit42.paloaltonetworks.com/new-python-based-payload-mechaflounder-used-by-chafer/
19. https://www.securityweek.com/hamas-linked-gaza-cybergang-has-new-tools-targets

20. https://ti.360.net/blog/articles/latest-target-attack-of-darkhydruns-group-against-middle-east-en/

21. https://unit42.paloaltonetworks.com/shamoon-3-targets-oil-gas-organization/

22. https://www.symantec.com/blogs/threat-intelligence/shamoon-destructive-threat-re-emerges-new-sting-its-tail

23. https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-november-helix-kitten/

24. https://unit42.paloaltonetworks.com/the-oil-rig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/

25. https://www.crowdstrike.com/blog/widespread-dns-hijacking-activity-targets-multiple-sectors/

26. https://www.arabianbusiness.com/technology/408796-uae-has-highest-smartphone-adoption-rate-in-mena-region

27. https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR-2018-Vol-1-E.pdf

28. https://www.symantec.com/security-center/threat-report