Al-Dhahir, N. (2017). *Ethical Hackers: The Moroccan Entrepreneurs Battling Cybercrime - Forbes Middle East. Forbes Middle East.* Retrieved 26 September 2017, from https://www.forbesmiddleeast.com/en/ethical-hackers-the-moroccan-entrepreneurs-battling-cybercrime/

Forbes Middle East / Technology

20-Sep-2017 | Nadia Al-Dhahir, Forbes Middle East Staff

Ethical Hackers: The Moroccan Entrepreneurs Battling Cybercrime

Today, 24-year-old Mohamed Amine Belarbi (R) and Mohamed Zakariae El Khdime (L), have secured a post-seed-round funding of $225,000 from an angel investor from Saudi Arabia, which now values VUL9 at $3.25M. Photo: Courtesy of VUL9

Moroccan entrepreneurs, Mohamed Amine Belarbi and Mohamed Zakariae El Khdime, are going into battle with the world's cyber-criminals—protecting some of the biggest names in the Middle East by hacking their systems.

On May 12, the users of over 230,000 computers in 150 countries across the world awoke to find themselves and their businesses being held to ransom. By the end of the day, an estimated $4 billion was relinquished in economic losses.

Originating in Asia, the "WannaCry" virus targeted Microsoft Windows, encrypting data and demanding a payment of $300 from each user in the Bitcoin cryptocurrency to hand back

control. Ukraine, Russia, India and Taiwan were some of the worst affected countries, with the U.K.'s National Health Service and Spanish telecom provider Telefonica reporting severe damages.

Luckily WannaCry's Friday launch date softened the blow in the Middle East.

It gave Mohamed Amine Belarbi and Mohamed Zakariae El Khdime—founders of boutique cybersecurity firm, VUL9—a chance to secure the frontline throughout the weekend, preparing their clients for a virus-free week ahead.

They had already known which clients could be affected through a protective security system, an inventory of all the software their clients use, so the team was able to install a protective shield before anyone was targeted.

"As tech guys, we are always expecting the worst-case scenario, so our minds are wired to be prepared efficiently," explained El Khdime.

Belarbi and El Khdime first met in April 2015, at the International Hackathon for Social Good in the Arab World, New York University, Abu Dhabi. While Belarbi was studying at the institute, El Khdime travelled from Morocco to compete in the hackathon—which he eventually won.

Introduced by a mutual friend, they hit it off instantly thanks to a shared love of all things tech and a passion for ethical hacking. They began to form an idea: they were going to change things for the better, starting immediately.

They designed the VUL9 website that night, and the next day reached out to both potential clients, and potential co-workers: a community of White Hackers (ethical hackers that help companies avoid viruses) of which El Khdime was a member.

Today their staff are made up of this same community. Hackers and IT experts from the hall of fame of major tech companies, including Facebook, Google, Microsoft, LinkedIn, Twitter, Nokia, Paypal, Samsung and Sony.

The company's name was derived from these achievements, with "VUL" short for vulnerability and "9" representing the top nine tech companies in the world.

In June 2016, with $20,000 of their own money behind them, the founders secured a seed investment of $90,000 from Emirati businessman Mohammed Kamali.

The following month they registered the company in the U.A.E., establishing the emirates as their base of operations.

Their vision grabbed the attention of Kamali so much that he immediately became a partner after his seed investment.

"VUL9 brought a new concept to the table, one that avoided using traditional means of investigation," he explains.

By December 2016 they had secured a contract with the leading software provider in Morocco, Manageo, thanks to an introduction by early mentor and Moroccan tech legend, Taher Alami.

In less than a year the impassioned team had also obtained contracts with U.A.E. giants such as Careem, souq.com, Aramex and Wamda Capital, as well as the place where it all began: New York University, Abu Dhabi.

While first touting the company, the entrepreneurs went to the heart of the region's startup system to secure support.

Attending a Wamda Mix and Mentor event in December 2016, they approached guru Fadi Ghandour, founder of Aramex and CEO and Chairman of Wamda Capital, and asked him to be their mentor. Ghandour was convinced.

Photo credit: Shutterstock

"I liked their approach, their professionalism and their mature interaction. Not to mention their capabilities and services they offer," Ghandour reveals. Both Belarbi and El Khdime agree the best advice they received from Ghandour was to never waste time, and to focus on selling their services and products.

Albeit the new kids on the block, the VUL9 founders didn't face much difficulty in convincing industry leaders to trust them. Despite facing fierce competition from other U.A.E. cybersecurity companies such as DarkMatter, Belarbi and El Khdime had a winning tactic at hand: approach with evidence.

"We'd study the online and system vulnerabilities of the companies and present the facts," says Belarbi. Essentially this meant hacking a secure organization before it is hacked by someone else.

Today 24-year-old Belarbi and El Khdime have secured a post-seed-round funding of $225,000 from an angel investor from Saudi Arabia, which now values VUL9 at $3.25 million.

By the close of 2017, Series A funding from a host of other angel investors is estimated to push the value of the company to between $10 million and $15 million. VUL9's revenues for its first full fiscal year will reach $500,000.

In April 2017, they registered the company in Morocco. And with solid funding behind them, Saudi Arabia is the next goal.

Belarbi envisions VUL9's efforts rewarded with even bigger clients in the near future, although at the moment he is keeping them under wraps. For now, it is enough for these ambitious entrepreneurs to be realizing a young dream: changing the way the region understands cybersecurity, with their shields raised.

Their next step is to tackle the Saudi dilemma, becoming the go-to cybersecurity providers in the desert kingdom and the rest of the region.

Barely a year old, VUL9 has entered the market at a time when the growing threat of cyberattacks are causing disruption across the world on a regular basis.

One of the most vulnerable regions, the Middle East is now paying attention—its cybersecurity market is expected to be worth up to $10 billion by 2019. Despite escaping the worst of the WannaCry virus, the region has not gone unharmed.

"Cyberattacks are nothing new in the Middle East and we've been hit hard many times over," says El Khdime.

He's not exaggerating. Figures from PwC's Global Economic Crime Survey show that in 2016 cybercrime was the second most reported economic crime that Middle East organizations fell victim to, with 30% of businesses being targeted.

Surprisingly however, over 20% of organizations admit to not knowing if they have been victims of cybercrime in the last two years. Enter VUL9.

Belarbi explains that cybersecurity is about trust and confidence, given the sensitive nature of the information disclosed and access to client platforms, systems and networks.

VUL9's team is famed for the close bond they conjure, working out of client offices instead of being isolated in their own.

They do this to stay as close to their clients as possible, being accessible whenever needed and making sure their security consultants are not just there to secure systems, but also to ensure knowledge transfer to technical teams.

The team's approach has quickly had a significant impact, both on its clients and the startup economy. "There's a perception in the Middle East that innovation primarily happens in the U.S.

or Europe, but VUL9 are quickly proving that wrong," says Careem's co-founder, Magnus Olsson.

Demand for their services is growing. Symantec recently revealed that Saudi Arabia was the most targeted country in the Middle East and Africa for ransomware in 2016, with the U.A.E. coming in second.

Hackers use malicious emails as their weapon of choice, and they are upping their demands, with the global average ransom rising to over $1,000 last year—more than three times the $294 average demanded in 2015.

Around 30% of ransomware victims in the U.A.E are willing to fork out the payment. With one in every 136 emails sent in the U.A.E. containing a malicious link or attachment—the highest recorded rate in five years—that's a potentially massive payout for cyber criminals.

"It's a never-ending story because no one company is immune. Everyday can bring a whole new virus we've never encountered before," says Belarbi.

The biggest attack on Saudi Arabia hit the Kingdom last year. The crippling "Shamoon 2" virus sent shockwaves across the country in 2016 when it targeted government agencies and the private sector, disrupting computers by overwriting the master book record so that it would be impossible for computers to start up.

The first Shamoon virus hit four years earlier in 2012, when Saudi Aramco experienced a cyberattack so destructive that it wiped data from tens of thousands of computers.

Reports suggest that a third Shamoon attack was launched on Saudi in January 2017.

One of the major obstacles to winning this war is that hackers adopt new strategies constantly, and staying on top of the latest developments is key to helping educate Middle East organizations.

"We distinct ourselves with the human factor, which many other cybersecurity companies forget to incorporate," explains El Khdime. It's no longer enough to merely hand out protective software or to fly in when the damage is done—education is vitally important.

Most companies are still not prepared for an attack on any scale, with only 33% of organizations in the Middle East having a cyber-incident response plan in place.

Social engineering is the quickest way for hackers to get in and catching their errors in judgement is what the VUL9 team teaches best.

They make a point of spreading awareness and provide regular workshops for all levels of staff, updating them on how hackers favor the use of email phishing to spread viruses.

Social engineering is adopted by criminal hackers to manipulate and exploit human vulnerabilities by finding out confidential information and using that to attack. It costs organizations over $5 billion a year globally.

Crime will always happen where there's an opportunity to commit it. To remain resilient, Belarbi and El Khdime believe it's essential to guarantee that an organization has a culture based on shared values, supported by strong policies and ethics that are integrated into everyday decision-making.

Belarbi admits that social engineering will continue to plague businesses and consumers because it uses simple deception to persuade victims to open emails, download attachments or click on links.

He predicts the next step for hackers will be a move to newer messaging platforms beyond traditional email, such as popular applications like WhatsApp or Facebook Messenger.

As messaging applications open themselves up to FinTech and marketing content, they become increasingly vulnerable.

For example, Facebook Messenger has amplified its use of automated bots, which allow brands to insert their products into user conversations. A similar messaging application in China, WeChat, offers numerous features, of which a payment system is one.

Where financial transactions pop up, cyberattacks will leach on.

The world is also on the brink of life-changing technological advancements, such as driverless cars and the Internet of Things. Belarbi points out that there will be more chances of cybercrime when cars start to operate using the internet. And he warns that we could start to see much more than financial crime, with cars potentially becoming vulnerable to being used for abductions or purposeful crashes.

Under a continuous barrage of cyberattacks, with pressure increasing with the arrival of FinTech in the Middle East and a growing reliance on cloud services presenting a security blind spot, Belarbi and El Khdime have their work cut out.

But they are well-armed to fight this war. With a team of experts and a powerful awareness drive in their arsenal, they are committed to playing a role in downsizing the spread of sophisticated malicious activity across the Middle East.

They estimate that entering the Saudi market will help VUL9 reach $1.5 million in revenue by the end of the 2018 fiscal year—three times its current rate.

Based on current performance, they project that revenue will double year-on-year.

Their goal is to hit a $200 million valuation in five years with over $20 million in yearly revenue. “Cybersecurity needs are increasing all the time, which means we will be in more demand,” explains Belarbi.

“We are ready,” says El Khdime. “To protect anyone, at any length and any size.”