

Digital Souks:

A Glimpse into the Middle Eastern and
North African Underground

Mayra Rosario Fuentes

Trend Micro Forward-Looking Threat Research (FTR) Team

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Contents

4

When Culture and Ideology Meet Cybercrime

8

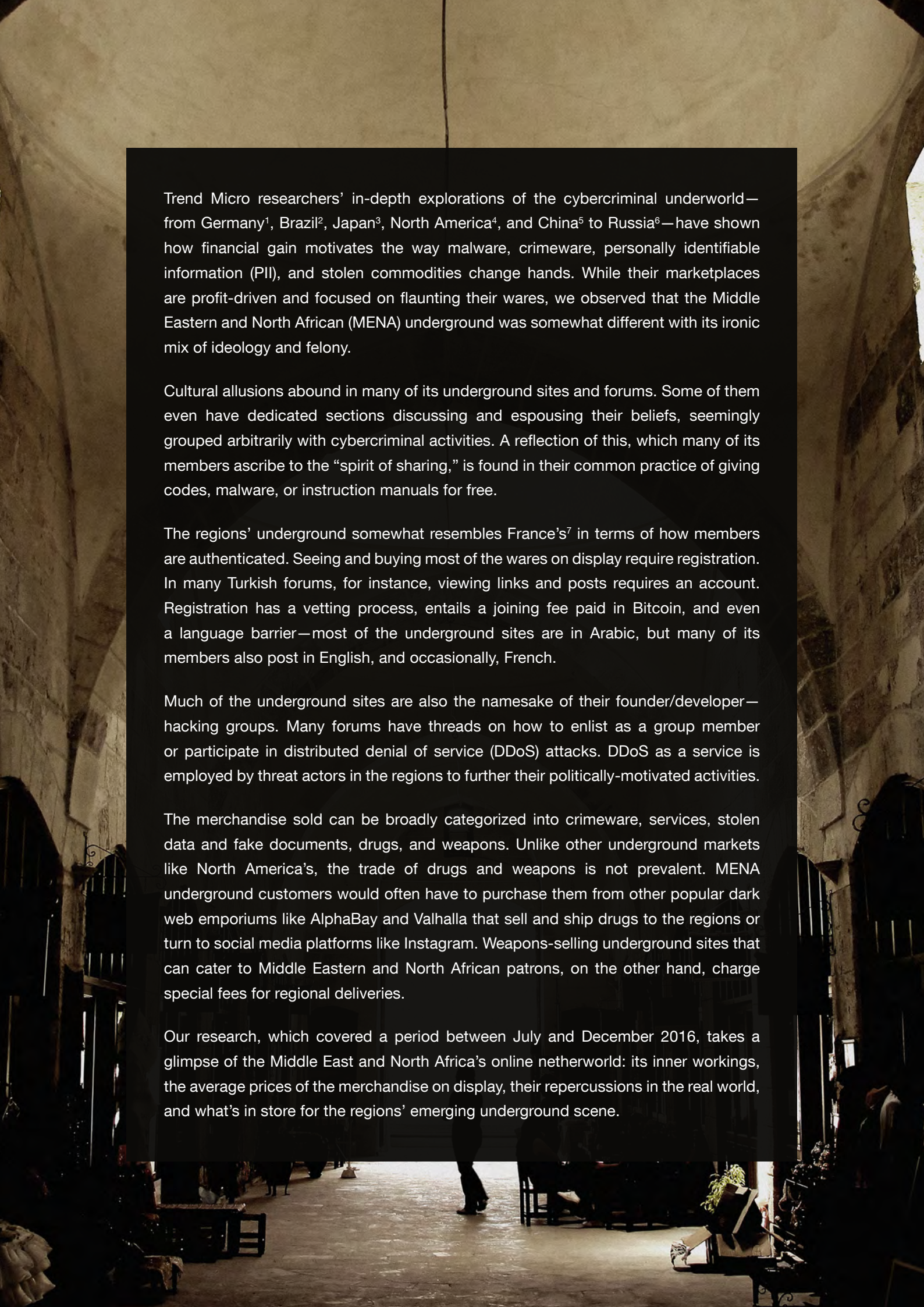
Middle Eastern and North African Underground: An Anatomy

9

Middle Eastern and North African Underground Offerings

37

A Sign of Things to Come



Trend Micro researchers' in-depth explorations of the cybercriminal underworld—from Germany¹, Brazil², Japan³, North America⁴, and China⁵ to Russia⁶—have shown how financial gain motivates the way malware, crimeware, personally identifiable information (PII), and stolen commodities change hands. While their marketplaces are profit-driven and focused on flaunting their wares, we observed that the Middle Eastern and North African (MENA) underground was somewhat different with its ironic mix of ideology and felony.

Cultural allusions abound in many of its underground sites and forums. Some of them even have dedicated sections discussing and espousing their beliefs, seemingly grouped arbitrarily with cybercriminal activities. A reflection of this, which many of its members ascribe to the “spirit of sharing,” is found in their common practice of giving codes, malware, or instruction manuals for free.

The regions' underground somewhat resembles France's⁷ in terms of how members are authenticated. Seeing and buying most of the wares on display require registration. In many Turkish forums, for instance, viewing links and posts requires an account. Registration has a vetting process, entails a joining fee paid in Bitcoin, and even a language barrier—most of the underground sites are in Arabic, but many of its members also post in English, and occasionally, French.

Much of the underground sites are also the namesake of their founder/developer—hacking groups. Many forums have threads on how to enlist as a group member or participate in distributed denial of service (DDoS) attacks. DDoS as a service is employed by threat actors in the regions to further their politically-motivated activities.

The merchandise sold can be broadly categorized into crimeware, services, stolen data and fake documents, drugs, and weapons. Unlike other underground markets like North America's, the trade of drugs and weapons is not prevalent. MENA underground customers would often have to purchase them from other popular dark web emporiums like AlphaBay and Valhalla that sell and ship drugs to the regions or turn to social media platforms like Instagram. Weapons-selling underground sites that can cater to Middle Eastern and North African patrons, on the other hand, charge special fees for regional deliveries.

Our research, which covered a period between July and December 2016, takes a glimpse of the Middle East and North Africa's online netherworld: its inner workings, the average prices of the merchandise on display, their repercussions in the real world, and what's in store for the regions' emerging underground scene.

When Culture and Ideology Meet Cybercrime

Distinct regional culture and ideology propel the Middle Eastern and North African underground scene. This is reflected by the kind of cordiality we observed across all levels of communication among customers and purveyors. In this underground scene, proverbial and cultural bywords precede and conclude all kinds of conversations and business transactions. Forum members who like a post would also reply in similar fashion. Forum and website posts feature a combination of religious references, sociopolitical discourse, and crimeware trading.

The marketplaces also have dedicated sections espousing their beliefs and ideologies. The Arab Security underground forum, for instance, features dedicated sections curiously grouped with topics such as encryption, messaging, programming, and reverse engineering. The different ways members prepare for religious holidays like Ramadan is a popular topic. We observed negative sentiment against terrorist group Islamic State of Iraq and the Levant (ISIS), as well as an Algeria-based underground site with a banner image in the corner of its homepage that says, “They are with Gaza”.



Figure 1: Forum post on the Dev-point forum;
the first line translates to “asking for blessings and mercy from Allah”

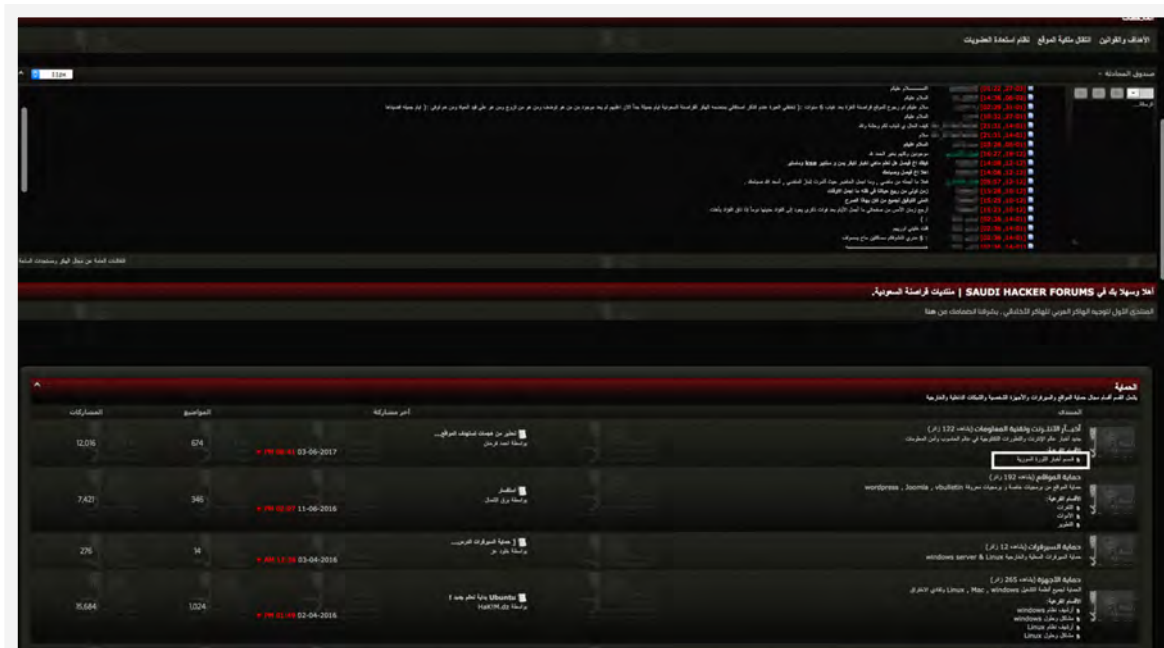


Figure 2: A section in the Pirates of Saudi Arabia forum showing news about Syria

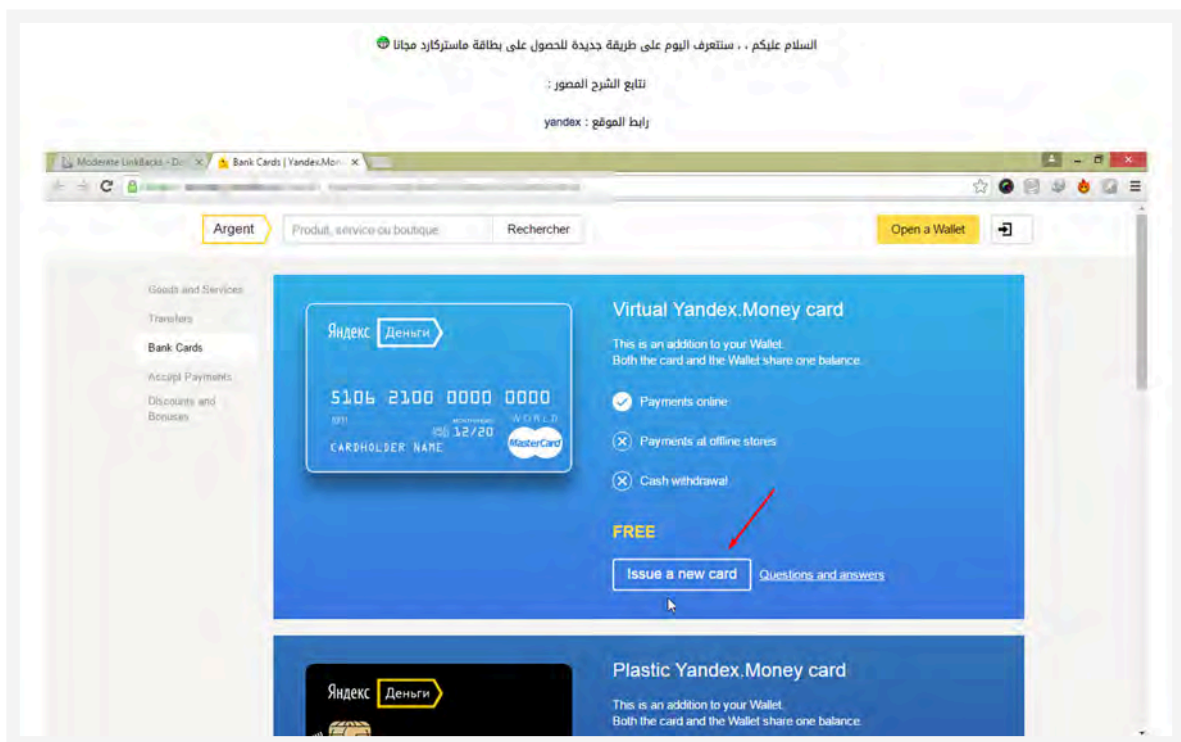


Figure 3: A Dev-point forum post explaining how to obtain a free Yandex Money Card, preceded by a message (top) that translates to “may peace be upon you”

Hacktivism is also a driving force in these marketplaces. DDoS attacks and website defacements are staples in their arsenal and done as a concerted effort by members who take ideological umbrage and distrust toward Western countries, their own government, and state-sponsored hacking groups.

Even their own are not exempt. For example, Shamoon⁸—a malware notorious for being used in targeted attacks in the Middle East and North Africa—is mocked and looked down on within underground forums in Saudi Arabia. The sentiment is understandable, as Shamoon mostly affected organizations in the country. In some of the forum posts we saw, Shamoon’s operators were branded as “traitors” and their malware deemed “insignificant”—gaining infamy only because it was from the “ministries,” which we interpret as a reference to state-sponsored groups.

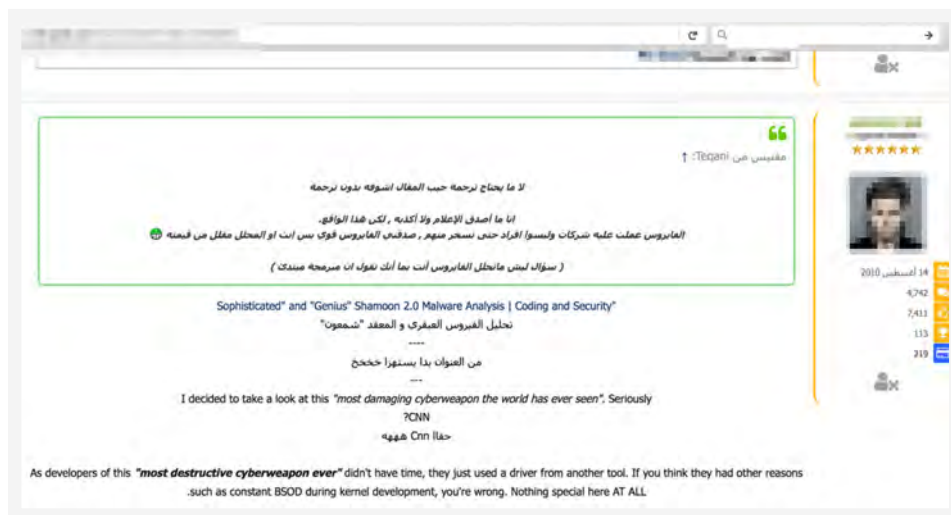


Figure 4: Dev-point forum thread discussing Shamoon



Figure 5: Forum post on Ashiyane Security giving away SCADA ports

Indeed, the Middle Eastern and North African underground is where culture, ideology, and cybercrime meet. Their confluence is the seeming impetus for the sale, trade, and distribution of contraband and malware. It also propels many illicit activities that transpire within its forums and websites. Among them is the common practice, sprung from a sense of brotherhood, to share or give hacking tools such as crypters, keyloggers, malware builders, and SQL injection tools for free. Information on Supervisory Control and Data Acquisition (SCADA) port numbers, for instance, were handed out “for the sake of good fortune.”

Middle Eastern and North African Underground: An Anatomy

We delineated the MENA underground as marketplaces, websites, and forums hosted within the regions. Arabic is the prevalent language, although some sites are in Turkish, Farsi, English, and occasionally, French. While these digital souks sell commodities to and from the Middle East and North Africa, they are also peddled worldwide. This includes markets, wares, and clientele in:

- Algeria
- Bahrain
- Egypt
- Iran
- Iraq
- Jordan
- Kuwait
- Lebanon
- Libya
- Morocco
- Oman
- Qatar
- Saudi Arabia
- Syria
- Tunisia
- Turkey
- United Arab Emirates
- Yemen

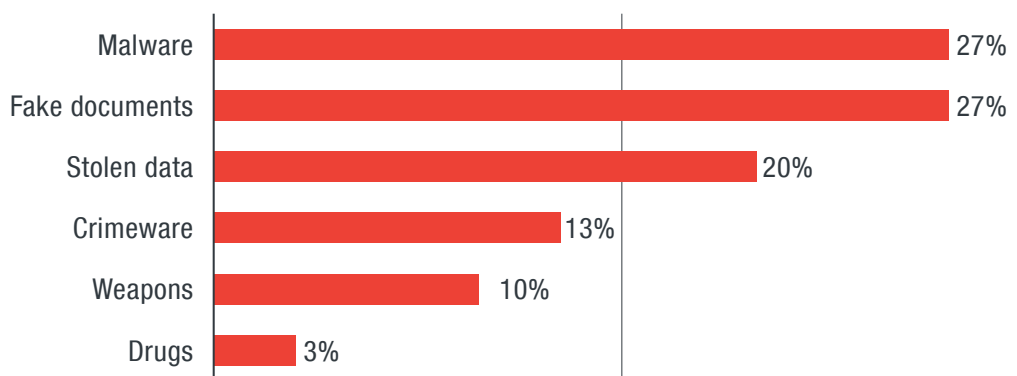


Figure 6: Distribution of products and services available in the Middle Eastern and Northern African underground sites

This research covers a period between July and December 2016, back when AlphaBay was still active and one of the largest marketplaces in the dark web. We updated the price of some of the wares sold during that time in May 2017.

Middle Eastern and North African Underground Offerings

Many Middle Eastern and North African underground sites are named after hacking groups, some of which are widely believed to be state-sponsored, suggesting that they manage these forums and sites. The most widely available sites sell malware and fake documents. Crimeware is uncommon, or sometimes outdated, given the relative ease of access to fake documents and stolen data. Drugs and weapons are sold in the dark web, but they are neither heavily sold nor readily available. Buyers often find drugs on English-based marketplaces like AlphaBay, Dream Market, and Valhalla. There are only a few sites trading weapons, as it's already a lucrative regional business that does not need to be hidden in the underground.

Hosting Services

In this underground market, hosting providers make a significant profit by selling hosting spaces. Regionalized hosting allows for local language and time settings in addition to faster connection speeds. A single IP connection and 50GB of hard disk space, for instance, cost US\$50 per month. Smaller plans exist for as low as \$3. To some extent, prices are at par with other underground marketplaces such as China's.

Among these hosting providers is Iran-based Ashiyane Security, whose website is ranked 412th in the country, according to website traffic and analytics company Alexa (© 2017, Alexa Internet [www.alexa.com]). The site is maintained by the Ashiyane Digital Security Team—a hacking group⁹ notable for having one member charged¹⁰ with conducting DDoS attacks against the U.S.'s financial sector. Its forum also offers hosting, while members advertise programming assistance services.

Another is Dev-point, a Saudi Arabian underground forum currently ranked 300th in the country (5,530 globally, according to Alexa). Disguised as a security forum, it offers free malware such as remote access Trojans (RAT). It also sells Remote Desktop Protocol (RDP) servers, available with host systems in Windows Server 2008 R2, Windows Server 2012 R2, and Windows Server 2016. Prices start at \$8 for two months. Upgrading the CPU speed, hard drive space, and RAM has additional fees.

آشپانه هاست

ADVANCED & SECURE WEB HOSTING

پشتیبانی
درباره ما
تمایزهای
میزبانی سرور
میزبانی وب
صفحه اصلی

برخی از مشتریان ما: **انجمن گرویدگان جوان**

اجاره سرورهای

• مجازی • اختصاصی • لینوکس • ویندوز

اجاره سرور مجازی در خارج و داخل ایران

آشپانه

گروه اختصاصی آتشیانه



●
●
●
●

سرویس های میزبانی آشپانه هاست

هاست لینوکس

سرویس های هاست لینوکس برای سایت هایی با برنامه نویسی PHP یا PERL یا CGI مناسب می باشد. از مزایای آن سادگی و قدرت آن نسبت به هاست ویندوز می باشد. سرویس های این نوع سرویس، همگی در بستر شبکه ای دنیا سستر آشپانه و از کنترل پنل cpanel استفاده می کنند و سرویس آن ها لایت اسپید می باشد. همچنین قابلیت انتخاب وزن های مختلف PHP را به شما میدهد.

50 مگابایت / 25,000 تومان



هاست ویندوز

سرویس های ویندوز آشپانه هاست از نظر نرم افزار، سخت افزار و امنیت از آخرین تکنولوژی روز بهره مند است و همین امر باعث می شود سایت شما در تمام مدت شبانه روز با سرعت بالا در دسترس همگان باشد!

50 مگابایت / 30,000 تومان

سرورهای اختصاصی امن

شرکت امنیتی آشپانه پس از 11 سال تجربه موفق در زمینه ارزیابی امنیتی سرورها و نرم افزارهای تحت وب و ارائه سرویس های میزبانی وب و پشتیبانی از سرورهای لینوکس و ویندوز، هم اکنون آمادگی ارائه سرور اختصاصی در بهترین دیتاسنترهای آمریکا، کانادا و چین را دارد. همچنین آشپانه هاست می تواند مسئولیت نگهداری، مانیتورینگ و پشتیبانی فنی و امنیتی سرورهای شما را در هر کجای دنیا به عهده گیرد.

سرورهای مجازی امن

ما معتقدیم سرورهای مجازی و یا Virtual Private Servers که به VPS معروف شده اند، نسل بعدی سرویس های هاست هستند و به همراه خود انعطاف، صرفه اقتصادی و کارایی به مراتب بیشتر از سرویس های هاستینگ Shared به ارمغان می آورند. تیم فنی آشپانه هاست 24 ساعت شبانه روز سرورهای مشتریان را مانیتور می کند تا در صورت بروز مشکل بر روی سرورها یا کوتاه ترین زمان ممکن مشکل حل شود.

پشتیبانی آنلاین



پشتیبانی آنلاین

چک کردن نام دامنه

[جستجو دامین](#)

رود کاربران

آدرس ایمیل:

کلمه عبور:

✚ ایجاد حساب کاربری
✚ ورود به پل کاربری

بازگشت به صفحه

انتخاب آشنایه هاست

- ✚ تریک جدول ماه ریم و ارائه تخفیف به مشت
- ✚ مشکلات شبکه
- ✚ ارائه انحصاری سیستم عامل محبوب هکر ها
- ✚ امکان انتخاب نسخه های مختلف در CPane
- ✚ تغییر و افزایش تعرفه خدمات ثبت دامنه

آرشیو خبرها

آخرین ارسال های انجمن آشپانه

- ✚ سوال در مورد زور مربوط به هاست...
- ✚ آموزش کانفیگ سرو...
- ✚ سوال در مورد وصل شدن به putty...
- ✚ مشکل اینترنت کالی...
- ✚ مشکل در نصب لینوکس...

آرشیو ارسالها

پرداخت آنلاین



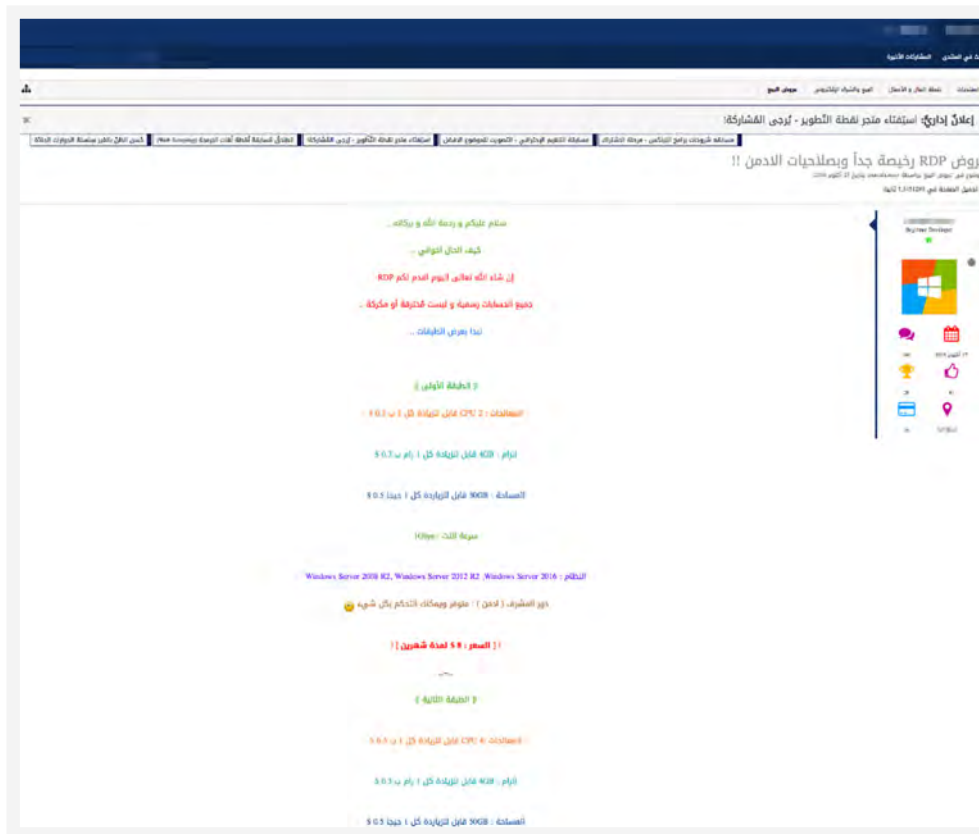


Figure 8: Advertisement on Dev-point forum selling cheap RDP servers

Cashout Services

Similar to the Russian underground, cashout services also abound here. These services are platforms for converting physical items, usually stolen, into cash. These services are paid in bank cards, Bitcoins (BTC), or direct cash transactions.

Turkish underground website Darbe Turk has a dedicated section for cashout services. Only members can see full forum posts. Registration can take weeks, and some of its restricted areas require a joining fee paid in Bitcoin. Physical goods like Sony PlayStation 4 are often sold at a considerable discount, but vendors impose a service charge typically ranging between 2–10%, which is paid during processing of the transaction.

These cashout services are also notable for being able to bypass security mechanisms and legal requirements in the region, such as those in place for purchasing mobile phones and disposable SIM cards. Buying these require a passport, residence permit, or personally identifiable document in many Middle Eastern and North African countries. In Saudi Arabia, for instance, a biometric fingerprint¹¹ is mandatory when purchasing SIM cards. In Turkey¹², Egypt¹³, and Iran¹⁴, the handset or mobile device must be registered as well. Some of the phones are sold by Russian traders who also peddle them beyond MENA's underground.

Some sites also post instructions on using cashout services and recommend drop shipment vendors. Among them is Reship, whose payment plans start at \$5 per shipment, with no annual fees.



Figure 9: Cashout services offered on Darbe Turk forum

Country/ Region	Seller Item	Purchase Method	Price
Egypt	Sony Xperia Z2 D6503	BTC	\$210–250
Jordan	Apple iPad mini Retina	Amazon Gift Card	\$125
Iraq	Samsung 8-piece Surround Sound System	Escrow, BTC	\$450 (including shipping)
MENA	10 Pieces Samsung Galaxy S8 64GB	BTC, credit card	\$6,000
MENA	5 Pieces Apple iPhone 7 Plus 32GB	BTC, credit card	\$2,600

Table 1: Average prices of various cashout services

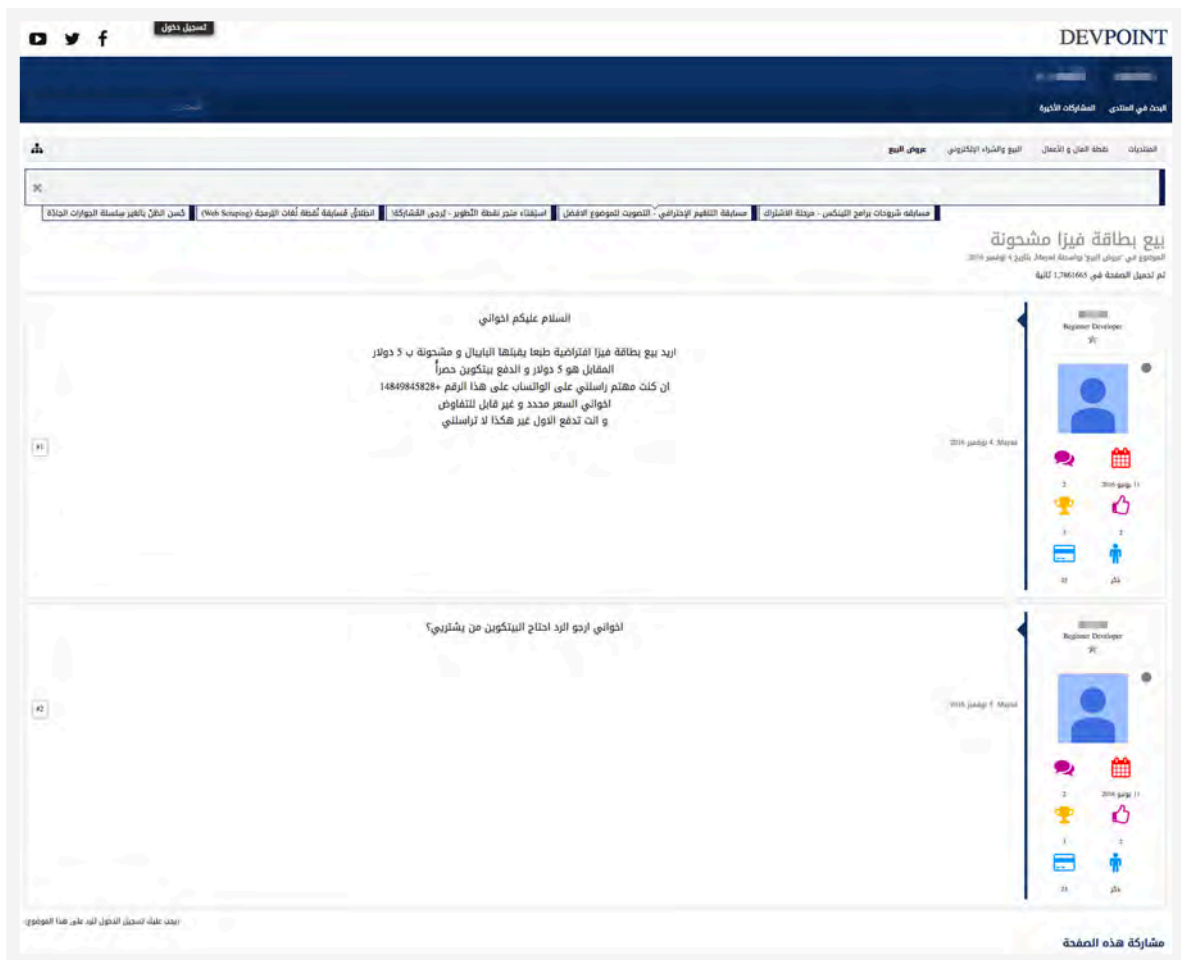


Figure 10: Dev-point forum ad that translates to, “Peace be upon you my brothers,
I want to sell a Visa Gift Card for bitcoins”

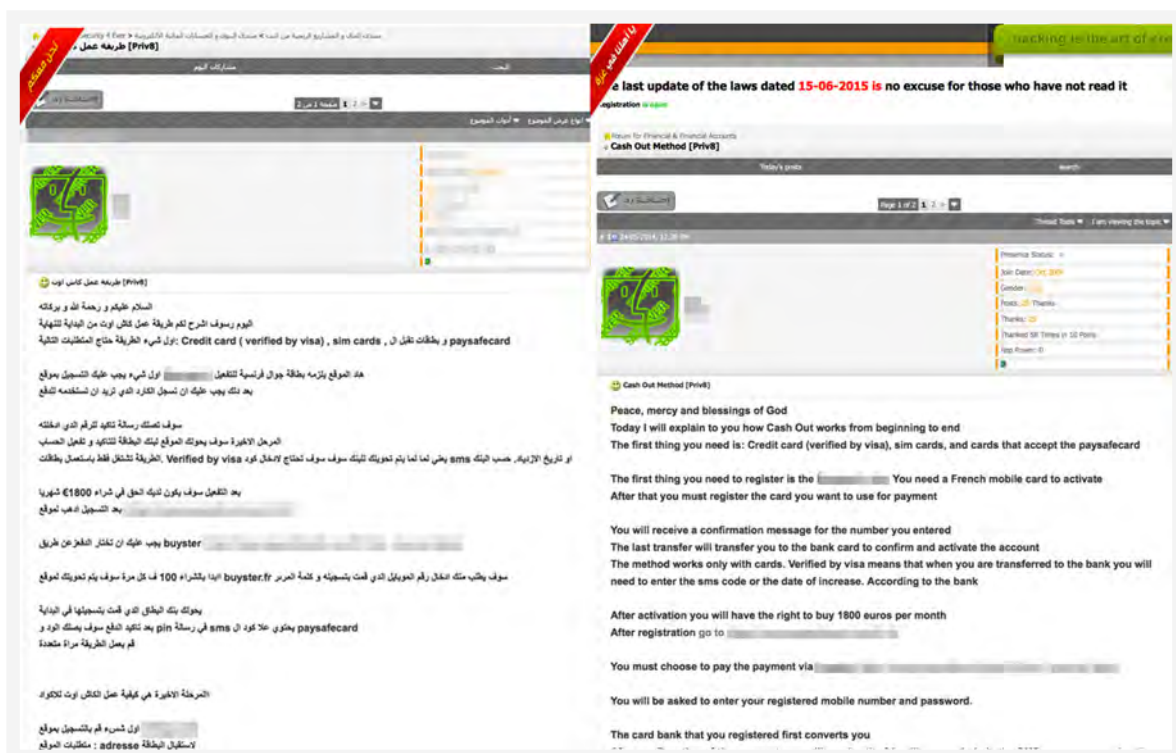


Figure 11: Permanent sticky note on the Algerian underground forum Sec4ever on how to use cashout services (original on the left, partially translated on the right)

حالة الشواحد

تاريخ التسجيل: May 2016

الجنس: ذكر

المشاركات: 23

شكرات: 2

تم شكره 16 مرة في 3 مشاركات

عدد تقييم المستوى: 0

و أهمنه في الشوب Drop Ali

سلام عليكم و رحمة الله و بركاته

هو ارسال سلعة لاحد شركات الشحن : **Drop & Shipping** او لا تعريف ثم تحويلها لعنوانك الرئيسي

drop & shipping من اهم الخطوات لنجاعة عملية الشوب هي ان تعمل حسب تجريبي فهذه المواقع تساعد بنسبة 90% في اتمام عملية الشراء من افضل المواقع التي تعامل معها

\$ سعر الخدمة 5

\$ على كل سلعة تصل تقوم بدفع 5

يقوم الموقع بحفظ سلعتك لمدة شهرين مجانا و بعد انتهاء المدة يقوم بسحب \$1 يوميا حتى 90 يوم

يعطيك الموقع 2 عناوين سواحد في كندا و الآخر في أمريكا

يمكنك ارسال كل السلع في طرد بريد واحد

يمكن التقاط صورة لسلعتك عند وصولها

Figure 12: Suggestions on using Reship from the Algerian underground forum Sec4ever (July 2016)

Hacking as a Service

MENA's underground is unique because of the way ideology impels the trade of hacking services. In other marketplaces like North America's or Russia's, for instance, their purveyors mostly focus on selling their wares and forum participants don't band together to plan cyberattacks.

Compromising systems, illicitly disclosing information, and distributing crimeware are largely spurred by hacktivism. In many cases, threat actors and hacktivist groups use MENA underground forums to coordinate and purportedly execute website defacements or DDoS attacks. High-profile attacks against organizations such as the National Aeronautics and Space Administration (NASA), apparently carried out by the Lord Hacking Team, are examples.

Hacktivist groups like Anonymous, Anonysec, Cyber Soldiers, Security Team, Lord Hacking Team, Danger Security Team, Test Team, Termint Security Team, Best Iranian, and StreeT BaX are known to use these underground forums to coordinate defacement attacks on websites in the Middle East and North Africa.

Some of them also enlist members. The Turkish underground forum Siber Harekat has a recruitment section. The screening process includes asking candidates their date of birth, age, programming skills, and favorite OS.

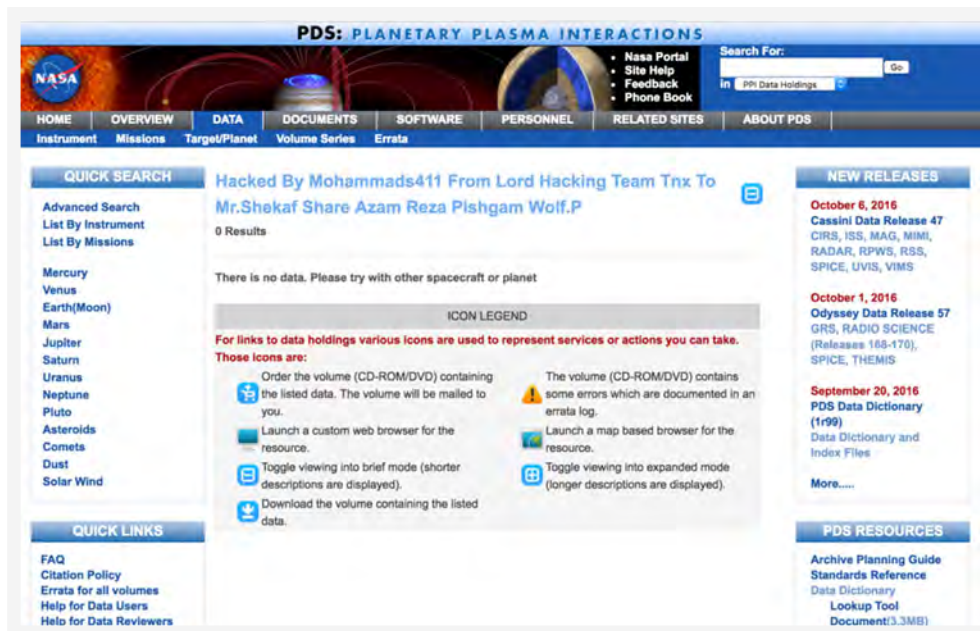


Figure 13: Defaced website of NASA attributed to Lord Hacking Team

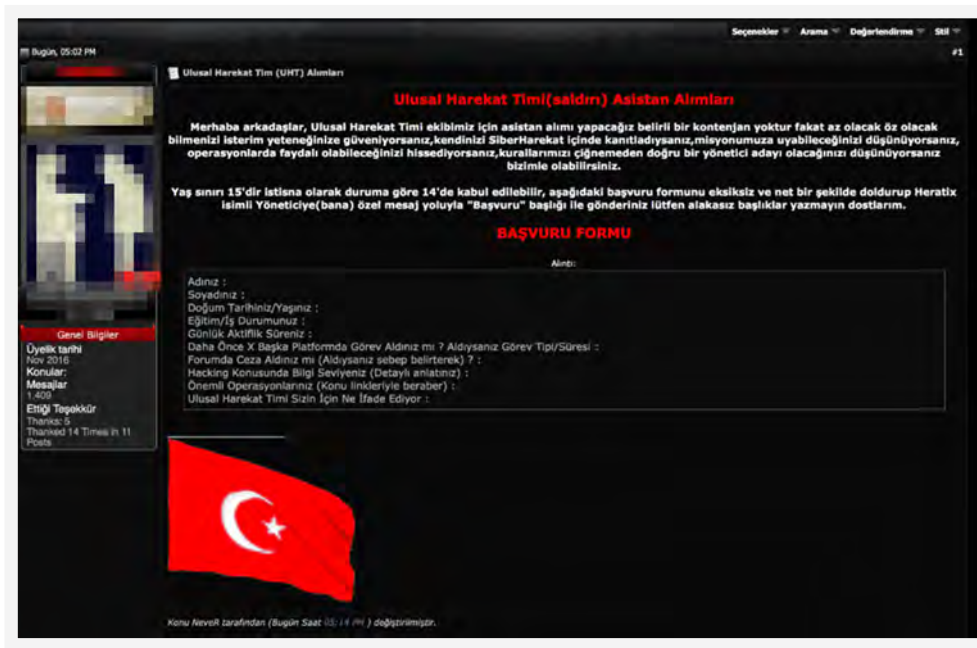


Figure 14: Forum post on Siber Harekat advertising positions for their hacking team

DDoS as a Service

DDoS as a service is a type of cyberattack commoditized for customers aiming to render their target's systems or network's resource unavailable. This service is gaining traction among cybercriminals due to its severe impact and relative ease of deployment—as exemplified by record DDoS attacks on DNS provider Dyn¹⁵ and Brian Krebs¹⁶.

In the MENA underground, DDoS services can be bought by hacktivists and threat actors to further their ideology, with private businesses and public organizations the usual targets. However, the service is not as prevalent despite it being widely discussed. Its rarity commands a steep price: the average cost is \$45 per hour, with three-hour packages at \$275, and involves tools like Low Orbit Ion Cannon (LOIC) or Lizard Stresser.



Figure 15: Ashiyane Security forum topics on DDoS

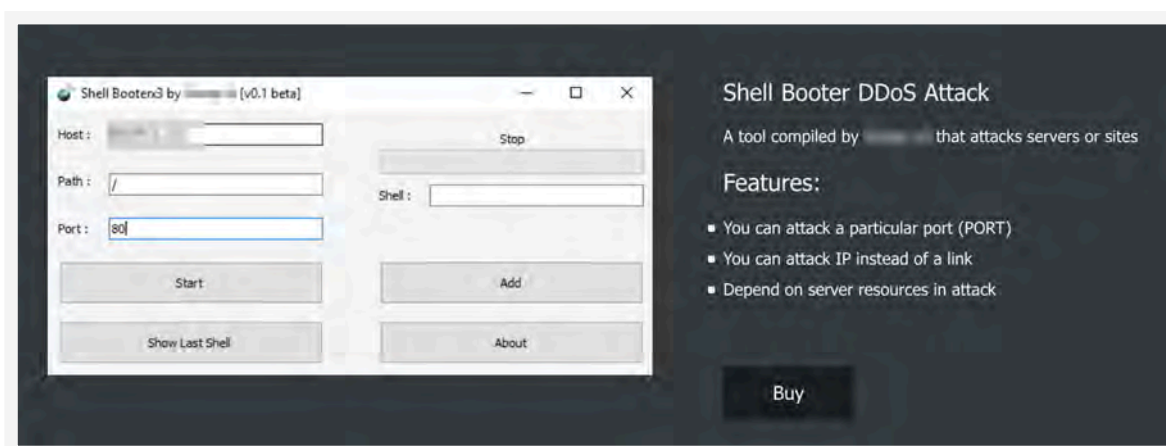


Figure 16: Pirates of Saudi Arabia's BlackFox's Store selling Shell Booter for DDoS attacks

Malware as a Service

Malware as a Service (MaaS) is the most widespread in the MENA underground. It typically includes a purveyor—a malware developer selling a single binary or a combination of binary and builder marketed as fully undetectable.

In some instances, the MaaS author would sell a piece of malware and access to a command and control (C&C) web interface, providing budding cybercriminals the resources for mounting their own campaigns regardless of their technical knowledge. Average prices are \$20 for a binary, and \$30–110 for a binary with C&C infrastructure. A binary-builder package costs around \$150–400.

Interestingly, we saw purveyors from other regions, especially Russia. A vendor going by the handle Fizik was seen selling the CTB-Locker (Critroni or Curve-Tor-Bitcoin) ransomware on Siber Harekat's forum. Fizik has been posting similar ads¹⁷ on Russian underground forums, and has been doing so as early as 2014¹⁸. CTB-Locker emerged in 2014¹⁹, going through a number of changes²⁰ while affecting enterprises and users mainly in Europe, Middle East, and Africa, as well as in countries like the U.S., France, Japan, China, and India.

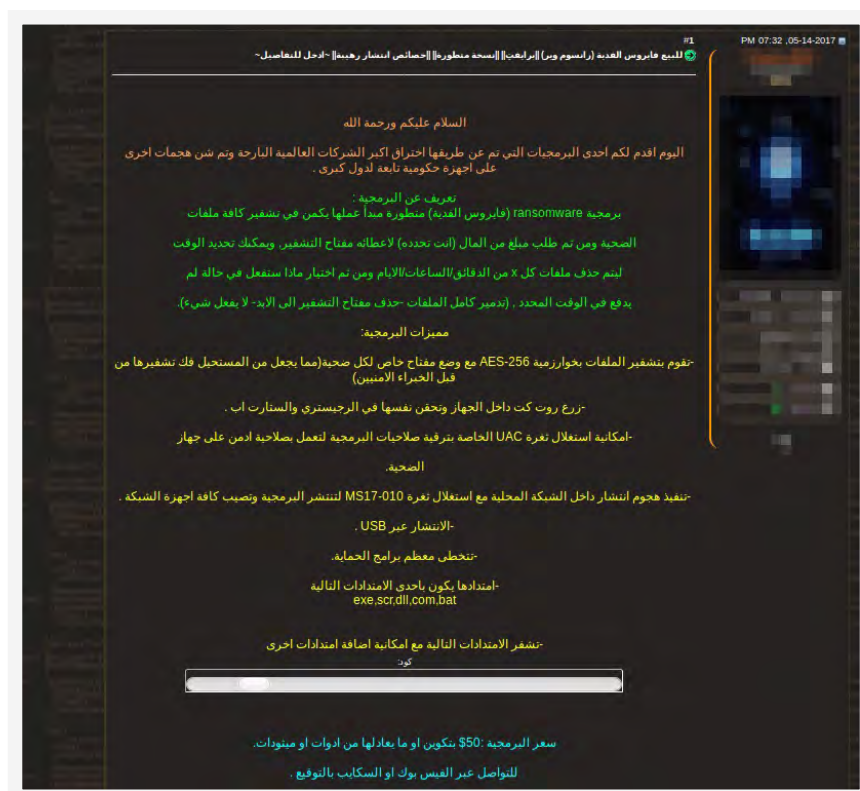


Figure 17: Forum post on hack-int selling WannaCry ransomware (May 14, 2017)



Passport Scans and Identity Documents

In the Middle East and North Africa, the demand for personally identifiable documents is influenced by geopolitical tensions²¹, their buyers wanting to flee active war zones, for instance, leveraging them to migrate to other countries as refugees. On the other hand, cybercriminals can also purchase fake documents to perpetrate insurance fraud or prove residence status. A daunting real-world implication: terrorists can buy these fake documents to slip into other countries as refugees²².

Stolen Middle Eastern and North African identities are duplicated and sold on Arabic forums such as hack-int, which is popular in Egypt. Passport scans go for \$18 and up. Identification papers are also up for sale, with packages comprising copies of driver's licenses, local utility bills, and other documents to help establish citizenship in another country. These fake documents are peddled in social media sites like Facebook, with posts in Arabic. They are also sold in English-based dark web marketplaces catering to Middle Eastern and North African buyers and sellers, such as AlphaBay, Dream Market, and Valhalla.



Figure 20: An advertisement on hack-int offering fake documents such as passports, National IDs, driving licenses, and Visa cards



Figure 21: Advertisement on Facebook (top left) for passports (bottom) and birth certificates (top right)



6 Identity Scans from Iraq

Iraq - 6 scans, all are passport scans These 6 scans are part of my Mega Scans Pack, to just buy these 6 scans order here. To buy the Full Mega Scans Pack Which Includes these scans and many other scans go to -

Sold by [redacted] - 0 sold since May 31, 2016 **Vendor**

Level 5 **Trust Level 4**

	Feature	Feature
Product class	Digital	Origin country Worldw
Quantity left	Unlimit	Ships to Worldw
Ends in	Never	Payment Escrow


Default - 1 days - USD +0.00 / item

Purchase price: USD 2.00

Qty: **Buy Now**

0.0034 BTC

Figure 22: Advertisement on AlphaBay selling identity scans from Iraq




109 Identity Scans from Egypt

Egypt 109 scans about 40 passport scans and the rest other docs These 109 scans are part of my Mega Scans Pack to just buy these 109 scans order here To buy the Full Mega Scans Pack Which Includes these scans and many other scans go to http://[redacted] onion listing php id [redacted]

Vendor [redacted] **Price** ₪0.01349109 **Location** Worldwide

(0)



1 Passport Scan Egypt

Accurate Digital Passport Colored Scan other products digital items identity data

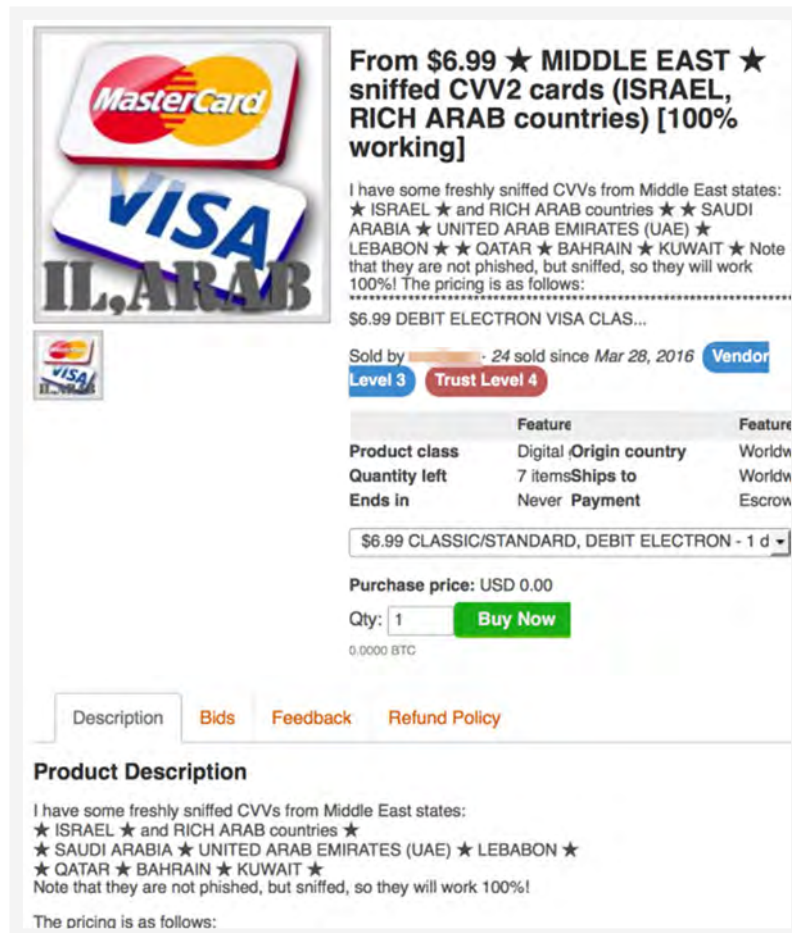
Vendor [redacted] **Price** ₪0.01260292 **Location** Finland

(97)

Figure 23: Advertisement on AlphaBay selling identity scans from Egypt

Credit Card Dumps

Credit card dumps are commonly sold and traded either as CVV2 numbers or fullz. The latter includes the credit card number, as well as the cardholder's name, birth date, address, PINs, and other information, which can be used to counterfeit credit cards or make illicit online purchases. Prices are higher than average compared to other marketplaces, probably due to their lower availability.



The screenshot shows an advertisement on the AlphaBay marketplace. On the left, there is a graphic with the MasterCard and Visa logos, and the text 'IL, ARAB' below them. The main text of the ad reads: 'From \$6.99 ★ MIDDLE EAST ★ sniffed CVV2 cards (ISRAEL, RICH ARAB countries) [100% working]'. Below this, a detailed description states: 'I have some freshly sniffed CVVs from Middle East states: ★ ISRAEL ★ and RICH ARAB countries ★ SAUDI ARABIA ★ UNITED ARAB EMIRATES (UAE) ★ LEBABON ★ ★ QATAR ★ BAHRAIN ★ KUWAIT ★ Note that they are not phished, but sniffed, so they will work 100%! The pricing is as follows:'. A table follows with columns for 'Feature' and 'Feature', listing 'Product class' as 'Digital', 'Origin country' as 'Worldw', 'Quantity left' as '7 items', 'Ships to' as 'Worldw', and 'Ends in' as 'Never Payment'. Below the table, a dropdown menu shows '\$6.99 CLASSIC/STANDARD, DEBIT ELECTRON - 1 d'. The purchase price is listed as 'USD 0.00'. A 'Buy Now' button is present, along with a 'Qty' field set to '1'. A 'Vendor' section shows 'Level 3' and 'Trust Level 4'. At the bottom, there is a 'Product Description' section with the same text as the main description.

From \$6.99 ★ MIDDLE EAST ★ sniffed CVV2 cards (ISRAEL, RICH ARAB countries) [100% working]

I have some freshly sniffed CVVs from Middle East states:
★ ISRAEL ★ and RICH ARAB countries ★ SAUDI ARABIA ★ UNITED ARAB EMIRATES (UAE) ★ LEBABON ★ ★ QATAR ★ BAHRAIN ★ KUWAIT ★ Note that they are not phished, but sniffed, so they will work 100%! The pricing is as follows:

\$6.99 DEBIT ELECTRON VISA CLAS...

Sold by [Vendor] - 24 sold since Mar 28, 2016

Level 3 Trust Level 4

	Feature	Feature
Product class	Digital	Origin country
Quantity left	7 items	Ships to
Ends in	Never	Payment

Escrow

\$6.99 CLASSIC/STANDARD, DEBIT ELECTRON - 1 d

Purchase price: USD 0.00

Qty: 1 Buy Now

0.0000 BTC

Description Bids Feedback Refund Policy

Product Description

I have some freshly sniffed CVVs from Middle East states:
★ ISRAEL ★ and RICH ARAB countries ★
★ SAUDI ARABIA ★ UNITED ARAB EMIRATES (UAE) ★ LEBABON ★
★ QATAR ★ BAHRAIN ★ KUWAIT ★
Note that they are not phished, but sniffed, so they will work 100%!

The pricing is as follows:

Figure 24: Advertisement on AlphaBay selling Middle East-based credit cards

Credit Card's Country of Origin	Description	Price
Canada	Visa/Mastercard	\$11–15 per number
	Amex/Discover	\$22–28 per number
	Full	\$35–50 per fullz
United States	Visa/Mastercard	\$5 per number
	Amex/Discover	\$8 per number
	Full	\$25 per fullz
United Kingdom	Visa/Mastercard	\$30 per number
	Amex/Discover	\$38 per number
	Full	\$53 per fullz
Israel	Full	\$33 per fullz
Russia	Full	\$25 per fullz
Turkey	Full	\$18 per fullz

Table 2: Price of credit cards based on country and card type

سلام عليكم اخواني
 كالعادة معكم اخوكم نورجان<ديزد
 من< الجزائر
 اليوم بمناسبة العودة لشهر حيث اخذكم
 حسابات بنكية منها بحريش
 ومنها لا
 لكي تستطيع الشراء بها غير ابي جهزك الي
 ابي امريكي

Full Name : [redacted]
 Credit Card Number : [redacted]
 CVC : [redacted]
 Expiration Date : 09/2016

Full Name : [redacted]
 Credit Card Number : [redacted]
 CVC : [redacted]
 Expiration Date : 04/2016

Name: [redacted]
 Email: [redacted]
 Phone: [redacted]
 Username: [redacted]
 CreditCard: [redacted]
 Expiration: 10/14
 Code: [redacted]
 Address: [redacted]
 State: IL
 Country: USA
 Zip: [redacted]

Credit Card Number: [redacted]
 Exp.Date: 09 / 2017
 Card type: VISA
 :PIN
 CVV: [redacted]

Street: [redacted]
 City: [redacted]
 State: IL

المنتدى العراقي
 10-TEAM.ORG

المنتدى العراقي
 10-TEAM.ORG

Figure 25: Credit card dump for sale on Iraq-team forum

Stolen Credentials and Online Accounts

The stolen credentials and online accounts sold are the types that can be used to access e-commerce accounts and hijack government-owned systems and servers with weak authentication.

Account	Price
Deezer.com account (for monthly service, guaranteed for six months)	\$7
PayPal account	\$3-10
Israeli PayPal account	\$50
Souq.com account	\$1-3
Saudiairlines.com account	\$4-7
Wadi.com account	\$5-8
Windows Server 2008 RDP access	\$20-30 (depending on location)

Table 3: Common prices of stolen accounts



Figure 26: A post on the Sec4ever forum asking if anyone can sell Israeli PayPal accounts; the user is willing to pay 2.5 bitcoins or more if the account has a password, high available balance, and doesn't have a Gmail account

Crimeware

Crypters

Crypters, typically used to encrypt malware, are also available. The key difference here is how they're readily traded and handed out for free. A few are sold and touted as more advanced, with prices typically costing between \$12 and \$130. The steep prices, compared to other marketplaces, are likely because of the lack of crypter options, and because the demand is higher than the supply.

The crypters are typically programmed in English, but some have regional variances, such as one we found in Turkish. Peddlers also offer a single-file price at \$10–15 per file.

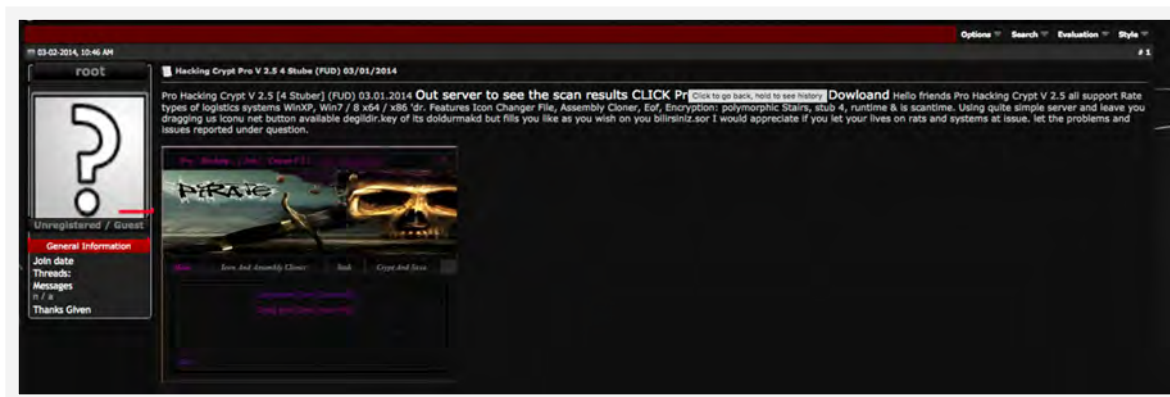


Figure 27: Forum post from Turk Hack Team advertising crypters

بسم الله الرحمن الرحيم

السلام عليكم و رحمة الله و بركاته

اليوم جايب لكم برنامجي المتواضع لتشفير جميع السيرفرات غير الدوت نت
لنن يريد تشفير سيرفرات الدوت نت بهذا البرنامج فعليه تحويل سيرفر الى لغة Native ببرنامج Net Reactor.

صورة البرنامج :



طريقة الاستعمال : قم بادراج السيرفر المراد تشفيره لخاصة Drag And Drop ثم قم بتوليد مفتاح التشفير

لتحميل البرنامج :

.....

ملاحظة مهم جدا : برنامج تشفير يعمل فقط على سيرفرات ليس من لغة برمجة دوت نت

منه :

CyberGate
Spynet

.....

في امان الله

الرجاء نقل الموضوع لقسم الحماية

Figure 28: Crypter offered for free on the Dev-point forum

Malware and Hacking Tools

The variety of malware for sale ranges from a run-of-the-mill worm given away for free to an advanced builder capable of generating an advanced malware binary that costs \$50. Many of these wares come with service level agreements (SLA) between the malware author and its buyer. A builder will have a predetermined time to be fully undetectable, for instance. SLAs vary based on the malware, with some lasting up to three months.

Kurdish underground hacking forum Hack for Kurds (h4Kurd), currently ranked 503rd in Iraq and 27,468th globally according to Alexa, features paid VIP sections, hacking discussions, and news on operating systems, mobile technologies, and programming. h4Kurd, which is also the name of the hacking team, also lists its members in the forum.

Offering	Price
Worm	\$1-12
Keylogger	Free-\$19
Known Ransomware	\$30-50
Malware Builder	Free-\$500
Citadel (fully undetectable)	\$150
Ninja RAT (fully undetectable)	\$100
Havij 1.8 (cracked)	Free

Table 4: Average prices of malware



Figure 29: Forum post from IQ-Team offering a free spam-emailing tool

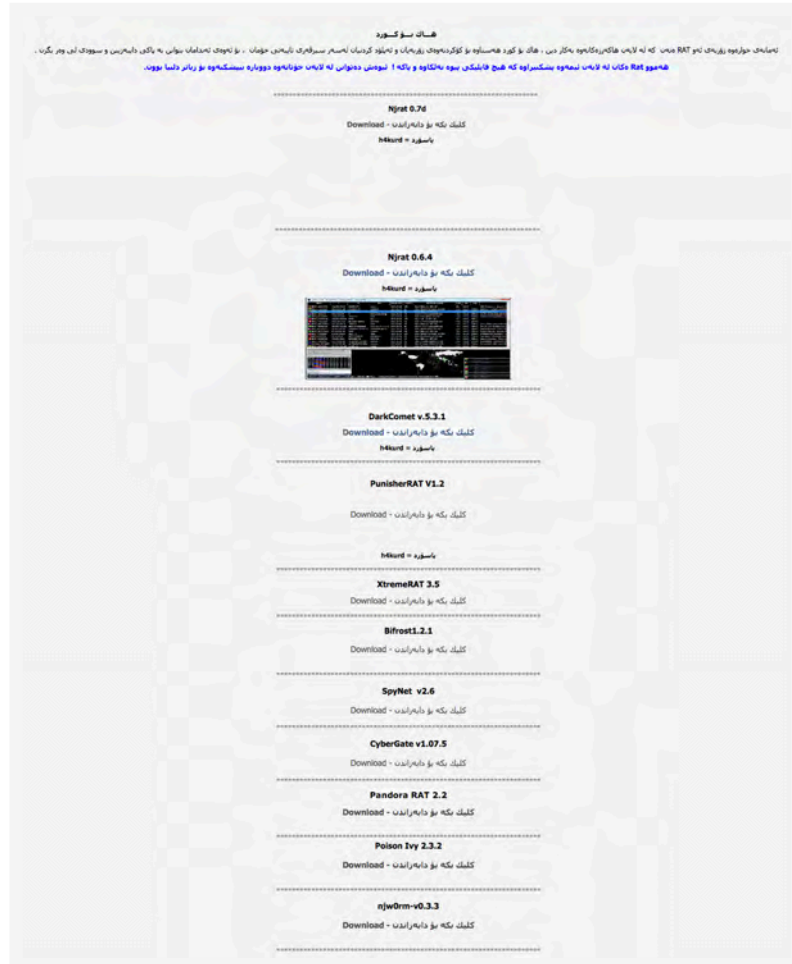


Figure 30: Post in Kurdish forum Hack for Kurds offering free RATs

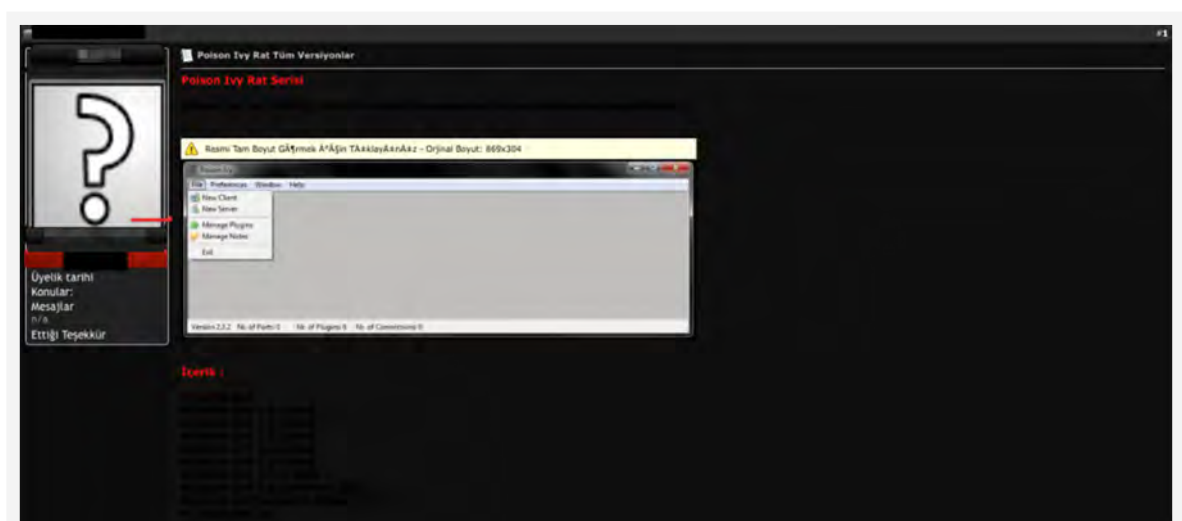


Figure 31: A forum post in Siber Harekat offering Poison Ivy RAT Serial SLA

Virtual Private Network (VPN)

VPNs are a mainstay for many cybercriminals because of the anonymity they provide. VPNs offered here are purportedly secure, don't store logs, and have multiple hop points. Cybercriminals typically use these servers as either part of a botnet, or a jump-off platform for further attacks to increase the number of hops away from the seller once the VPN is used. Prices for these are fairly consistent, ranging from \$20 to \$40 per month. Some forums do not provide their own VPN service but offer it as affiliates for other vendors instead.



Figure 32: Kurdish underground forum Hack for Kurds selling VPN services as an affiliate for another vendor, NVPN; prices start at \$6 per month.

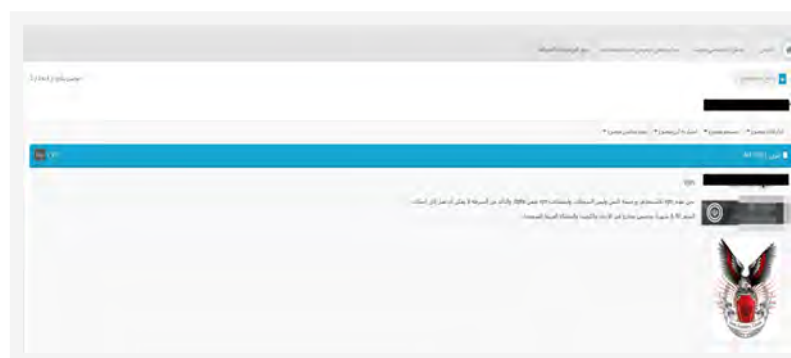


Figure 33: Advertisement from the Iranian Security Team forum selling VPN access with drain points in Saudi Arabia, Jordan, and Kuwait

Drugs and Weapons

The sale of drugs is not as popular and instead found on English-based marketplaces such as AlphaBay, Dream Market, and Valhalla, which also cater to sellers and customers within the Middle East and North Africa. Many advertise Afghani hashish, usually mailed from an address in the U.S. or U.K. Advertisements for drugs—marijuana, cocaine, and prescription drugs—shipped directly from the regions are uncommon.

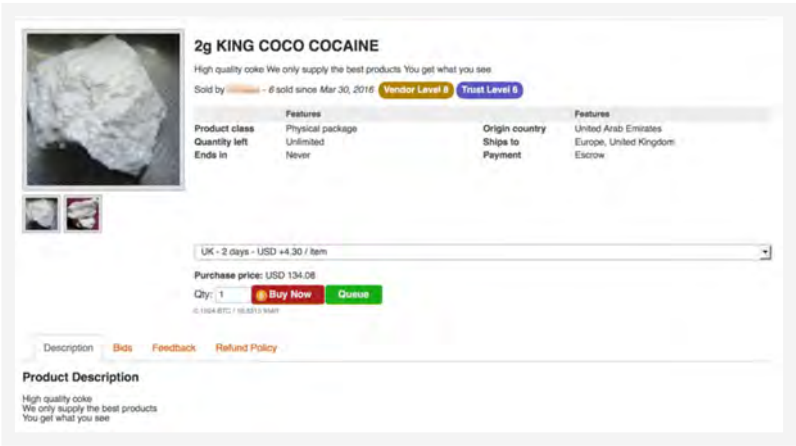


Figure 34: Advertisement on AlphaBay selling cocaine from United Arab Emirates

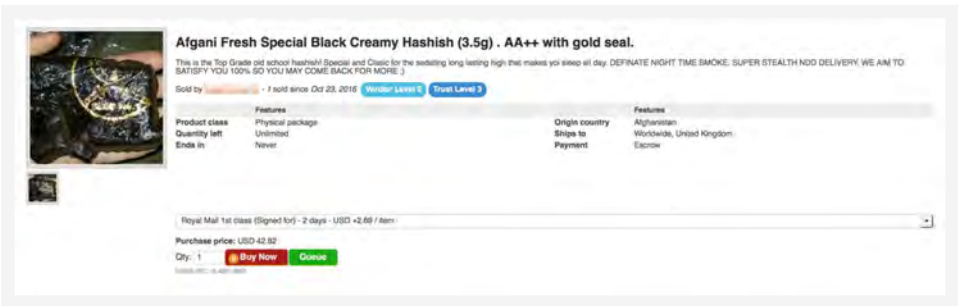


Figure 35: Advertisement on AlphaBay selling Afghani hashish from Afghanistan

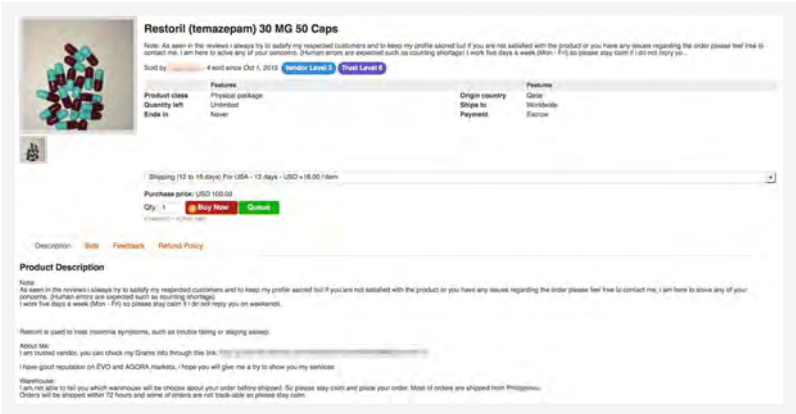


Figure 36: Advertisement on AlphaBay selling pills from Qatar

The trade of weapons is also not as pervasive as one would assume. Most of it transpires instead on English-based dark web sites that cater to worldwide customers. Unlike drugs that can be hidden and shipped in small doses, guns are difficult to deliver, particularly by mail. Buyers can also opt for their own local clandestine black markets instead of using a dark web site that may be unreliable or fraudulent.

Nonetheless, we found several sites that shipped these weapons to and from the Middle East and North Africa, but with additional fees. In fact, one of the sellers touted having warehouses in both regions. Their exact locations are not disclosed, supposedly to make deliveries easier in faraway areas.

Bitcoin is their preferred method of payment. Weapons are offered new or used and can be sold in bundles. Hand deliveries are also offered; buyers are promised that weapons will be received when shipped. Purveyors even abuse social media sites like Facebook and Instagram by posting advertisements for their weapons. Curiously, they also sell a miscellany of other commodities like livestock (i.e., sheep) and mobile phones. Case in point: Mredy, an Iraq-based forum that peddles goods ranging from cars, land, weapons, and livestock, among others.

Offering	Price (New)	Price (Used)
Assault Rifle	\$2,300	\$700
Pistol	\$850	\$560
Sub Machine Gun	\$2,900	\$700
RPG/Rocket Launcher	\$1,440	\$870

Table 5: Prices of commonly advertised weapons

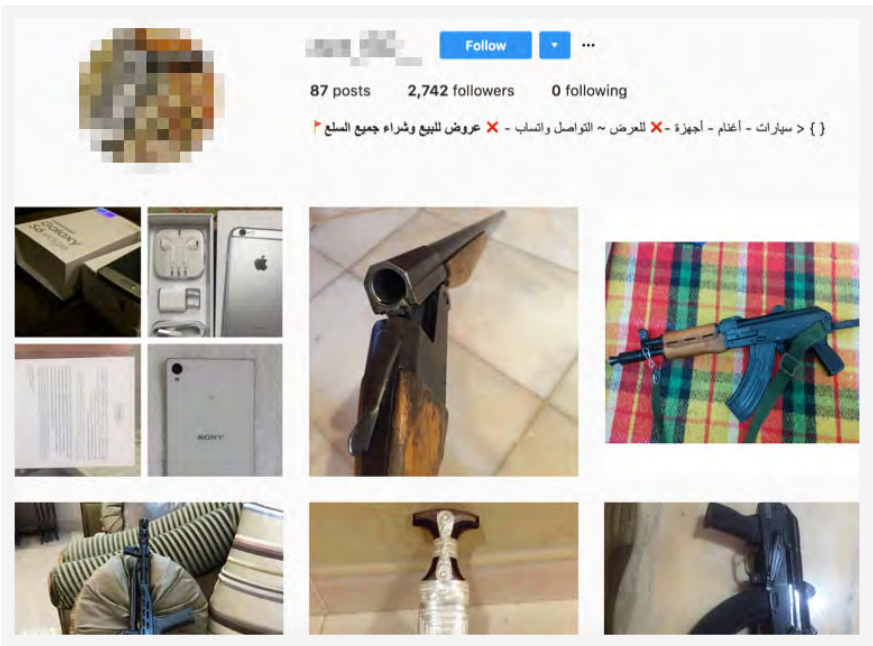


Figure 37: Weapons and other products being sold on Instagram

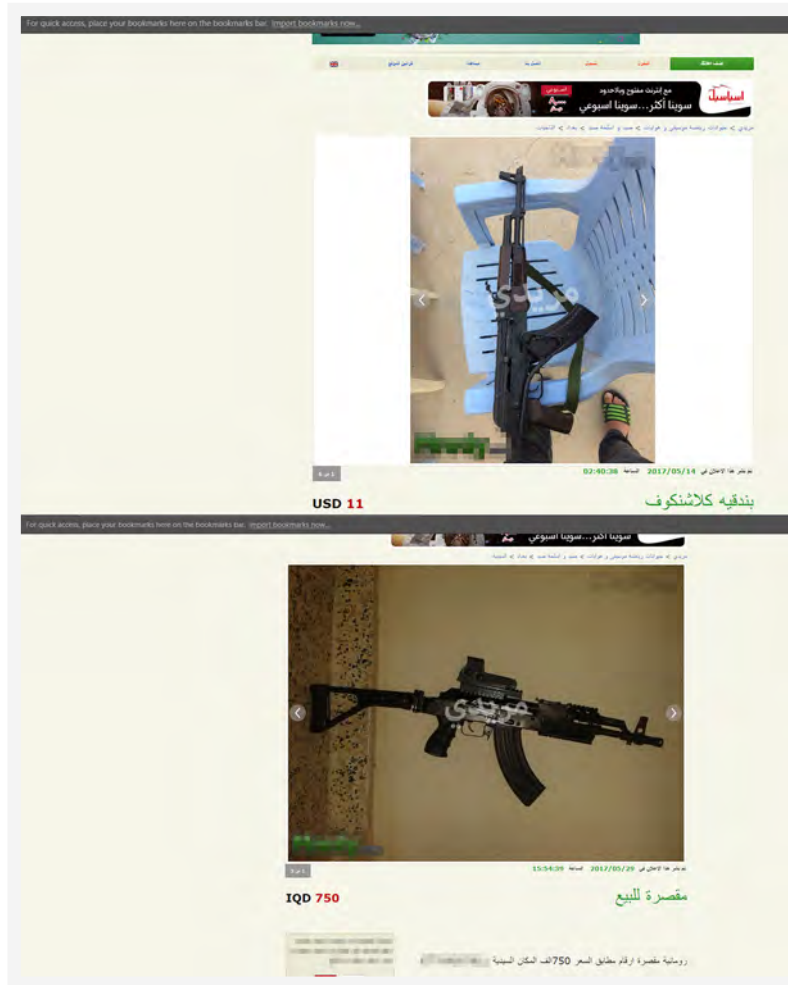


Figure 38: Mredy advertisements, translated (from top to bottom):
 “Ak-47 for 11 USD”, “Rifle for sale 750K Iraqi Dinar” (\$643)



Figure 39: A package consisting of a handgun and cuffs being sold on Mredy; the advertisement translates to “only 2 bullets used previous for testing price range 27 USD”

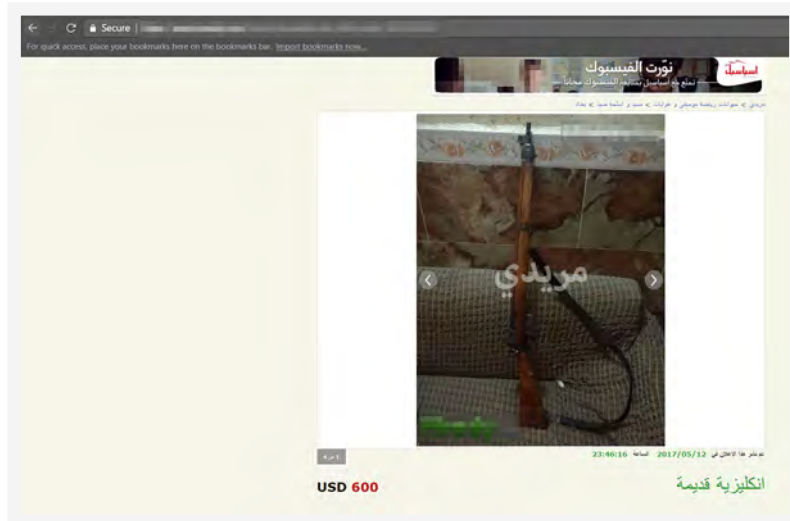


Figure 40: Mredy selling a rifle for \$600; the advertisement translates to:
 “Oh man it can shoot you instead of shooting others :D”

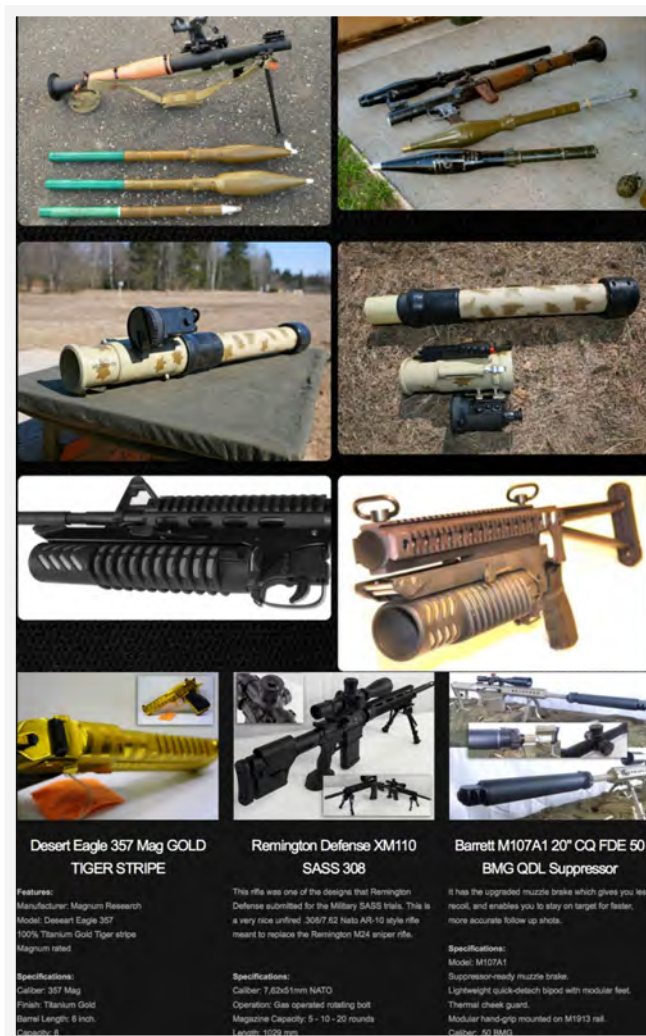


Figure 41: Types of weapons sold in the MENA underground

A Sign of Things to Come

Though not quite at par in terms of scale and scope compared to its counterparts, the products and services that have become common across the world's marketplaces—malware, crime tools, and weapons—are also available in the Middle Eastern and North African underground. The cultural and ideological overtones make the market unique and, based on what we've witnessed, are what influence the products and services offered.

The kinds of activities that now occur within its forums and websites are signs of things to come for this emerging underground scene and its players. It may still be young, but it is increasingly thriving as a place where threat actors coordinate and launch cyberattacks. As the regions' underground further develops and diversifies beyond DDoS and website defacement, so will the type of cyberattacks—and the resources and expertise needed for them.

As it's still a burgeoning market, we also expect more forum users coding and selling their own malware instead of giving them away for free. We also foresee continued and closer coordination with the Russian underground, whose purveyors are known to hire coders from the Middle East and North Africa. One of the underground sites we ventured into, for instance, now have pop-up features advertising Russian stores and offers from a China-based e-commerce platform.

Our forays into these digital souks have allowed us to gather and analyze threat intelligence that can help law enforcement organizations with their work while empowering legislators and enterprises strengthen their policies and posture against cybercrime. We will continue to monitor these marketplaces as they evolve while proactively coordinating with partners and authorities.

References

1. Forward-Looking Threat Research Team. (8 December 2015). *Trend Micro*. "U-Markt: Peering into the German Cybercriminal Underground." Last accessed on 13 February 2017, <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-u-markt.pdf>.
2. Forward-Looking Threat Research Team. (12 January 2016). *Trend Micro*. "Ascending the Ranks: The Brazilian Cybercriminal Underground in 2015." Last accessed on 13 February 2017, <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-ascending-the-ranks.pdf>.
3. Akira Urano. (13 October 2015). *Trend Micro*. "The Japanese Underground." Last accessed on 13 February 2017, <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-japanese-underground.pdf>.
4. Kyle Wilhoit and Stephen Hilt. (7 December 2015). *Trend Micro*. "North American Underground: The Glass Tank." Last accessed on 13 February 2017, <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-north-american-underground.pdf>.
5. Lion Gu. (23 November 2015). *Trend Micro*. "Prototype Nation: The Chinese Cybercriminal Underground in 2015." Last accessed on 13 February 2017, <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-prototype-nation.pdf>.
6. Max Goranchov. (28 July 2015). *Trend Micro*. "Russian Underground 2.0." Last accessed on 13 February 2017, <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/wp-russian-underground-2.0.pdf>.
7. Cedric Pernet. (14 September 2016). *Trend Micro*. "The French Underground: Under a Shroud of Extreme Caution." Last accessed on 13 February 2017, <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-french-underground.pdf>.
8. Cris Pantanilla. (17 August 2012). *TrendLabs Security Intelligence Blog*. "Disttrack Malware Overwrites Files, Infects MBR." Last accessed on 21 March 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/disttrack-malware-overwrites-files-infects-mbr/>.
9. Jeffery Carr. (12 January 2011). Forbes Media LLC. "Iran's Paramilitary Militia Is Recruiting Hackers." Last accessed on 30 November 2016, www.forbes.com/sites/jeffreycarr/2011/01/12/irans-paramilitary-militia-is-recruiting-hackers/.
10. The United States Department of Justice, Office of Public Affairs. (24 March 2016). *United States Department of Justice*. "Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector." [Press Release]. Last accessed on 2017 February 13, <https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged>.
11. Arab News. (26 January 2016). *Saudi Research and Publishing Company*. "Fingerprint to be recorded for issuance of mobile SIM." Last accessed on 20 February 2017, <http://www.arabnews.com/saudi-arabia/news/870691>.
12. Central Equipment Identity Register. (n.d.). *Information and Communication Technologies Authority of Turkey*. "Law on Amending the Radio Communication Law." Last accessed on 20 February 2017, <http://www.mcks.gov.tr/en/KonuDetay.php?BKey=42>.
13. National Telecommunications Regulatory Authority. (2 May 2010). *Arab Republic of Egypt, Ministry of Communications and Information Technology*. "The New Regulation of the Registration of Consumers' Personal Data in Selling and Activating Mobile Lines." [Press Release]. Last accessed on 20 February 2017, http://www.mcit.gov.eg/Media_Center/Latest_News/News/536.
14. Financial Tribune. (8 February 2017). *Financial Tribune Daily*. "Iran Unveils New Phases of Telecom Networks." Last accessed on 20 February 2017, <https://financialtribune.com/articles/economy-sci-tech/59092/iran-unveils-new-phases-of-telecom-networks>.
15. Kyle York. (22 October 2016). *Dyn*. "Dyn Statement on 10/21/2016 DDoS Attack." Last accessed on 25 March 2017, <http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/>.

16. Brian Krebs. (21 September 2016). *Krebs on Security*. "KrebsOnSecurity Hit With Record DDoS." Last accessed on 25 March 2017, <https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/>.
17. Tapkin. (28 October 2015). *OpenSC Security Research and Development Forum*. "Thread: Hello from my russia." [Post #1]. Message posted to <https://www.opensc.io/showthread.php?t=20250>.
18. Kafeine. (18 July 2014). *Malware don't need Coffee*. "Crypto Ransomware CTB-Locker (Critroni.A) on the rise." Last accessed on 30 November 2016, <http://malware.dontneedcoffee.com/2014/07/ctb-locker.html>.
19. Eduardo Altares II. (30 July 2014). *Trend Micro Security Intelligence Blog*. "New Crypto-Ransomware Emerge in the Wild." Retrieved from <http://blog.trendmicro.com/trendlabs-security-intelligence/new-crypto-ransomware-emerge-in-the-wild/>.
20. Trend Micro. (21 January 2015). *Trend Micro Security Intelligence Blog*. "CTB-Locker Ransomware Includes Freemium Feature, Extends Deadline." Last accessed on 8 February 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/ctb-locker-ransomware-includes-freemium-feature-extends-deadline/>.
21. Barbara Tasch. (16 September 2015). *Business Insider*. "Migrants are buying fake Syrian passports because they think it will help their chances of getting refugee status." Last accessed on 25 March 2017, <http://www.businessinsider.com/fake-syrian-passport-market-is-booming-2015-9>.
22. Julian Robinson. (26 January 2016). *The Daily Mail*. "ISIS have created an entire fake passport 'industry' using documents stolen in Iraq, Libya and Syria, warn French officials." Last accessed on 25 March 2017, www.dailymail.co.uk/news/article-3416967/ISIS-created-entire-fake-passport-industry-using-documents-stolen-Iraq-Libya-Syria-warn-French-officials.html.

Created by:

TrendLabs

The Global Technical Support and R&D Center of TREND MICRO

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver top-ranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit www.trendmicro.com.



Securing Your Journey
to the Cloud

www.trendmicro.com