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 researchers’ in-depth explorations of the cybercriminal underworld—from Germany, Brazil, Japan, North America, and China to Russia—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’s 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, Shamoon—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](image1)

![Figure 5: Forum post on Ashiyane Security giving away SCADA ports](image2)
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

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.

Figure 6: Distribution of products and services available in the Middle Eastern and Northern African underground sites
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 group notable for having one member charged 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.
Figure 7: Bulletproof hosting advertisement from the Ashiyane Security forum
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 fingerprint is mandatory when purchasing SIM cards. In Turkey, Egypt, and Iran, 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](image)

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

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)
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
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 Dyn\(^\text{15}\) and Brian Krebs\(^\text{16}\).

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 ads on Russian underground forums, and has been doing so as early as 2014. CTB-Locker emerged in 2014, going through a number of changes 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)
Figure 18: Fizik’s advertisement for CTB-Locker

Figure 19: Forum post from Iranian Security Team offering crypters
Passport Scans and Identity Documents

In the Middle East and North Africa, the demand for personally identifiable documents is influenced by geopolitical tensions, 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 refugees.

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](image-url)
Figure 21: Advertisement on Facebook (top left) for passports (bottom) and birth certificates (top right)
Figure 22: Advertisement on AlphaBay selling identity scans from Iraq

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.

Figure 24: Advertisement on AlphaBay selling Middle East-based credit cards
Table 2: Price of credit cards based on country and card type

<table>
<thead>
<tr>
<th>Credit Card’s Country of Origin</th>
<th>Description</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canada</td>
<td>Visa/Mastercard</td>
<td>$11–15 per number</td>
</tr>
<tr>
<td></td>
<td>Amex/Discover</td>
<td>$22–28 per number</td>
</tr>
<tr>
<td></td>
<td>Full</td>
<td>$35–50 per fullz</td>
</tr>
<tr>
<td>United States</td>
<td>Visa/Mastercard</td>
<td>$5 per number</td>
</tr>
<tr>
<td></td>
<td>Amex/Discover</td>
<td>$8 per number</td>
</tr>
<tr>
<td></td>
<td>Full</td>
<td>$25 per fullz</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>Visa/Mastercard</td>
<td>$30 per number</td>
</tr>
<tr>
<td></td>
<td>Amex/Discover</td>
<td>$38 per number</td>
</tr>
<tr>
<td></td>
<td>Full</td>
<td>$53 per fullz</td>
</tr>
<tr>
<td>Israel</td>
<td>Full</td>
<td>$33 per fullz</td>
</tr>
<tr>
<td>Russia</td>
<td>Full</td>
<td>$25 per fullz</td>
</tr>
<tr>
<td>Turkey</td>
<td>Full</td>
<td>$18 per fullz</td>
</tr>
</tbody>
</table>

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.

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

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
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.

<table>
<thead>
<tr>
<th>Offering</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Worm</td>
<td>$1-12</td>
</tr>
<tr>
<td>Keylogger</td>
<td>Free-$19</td>
</tr>
<tr>
<td>Known Ransomware</td>
<td>$30-50</td>
</tr>
<tr>
<td>Malware Builder</td>
<td>Free-$500</td>
</tr>
<tr>
<td>Citadel (fully undetectable)</td>
<td>$150</td>
</tr>
<tr>
<td>Ninja RAT (fully undetectable)</td>
<td>$100</td>
</tr>
<tr>
<td>Havij 1.8 (cracked)</td>
<td>Free</td>
</tr>
</tbody>
</table>

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.](image)

![Figure 33: Advertisement from the Iranian Security Team forum selling VPN access with drain points in Saudi Arabia, Jordan, and Kuwait](image)
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.

<table>
<thead>
<tr>
<th>Offering</th>
<th>Price (New)</th>
<th>Price (Used)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assault Rifle</td>
<td>$2,300</td>
<td>$700</td>
</tr>
<tr>
<td>Pistol</td>
<td>$850</td>
<td>$560</td>
</tr>
<tr>
<td>Sub Machine Gun</td>
<td>$2,900</td>
<td>$700</td>
</tr>
<tr>
<td>RPG/Rocket Launcher</td>
<td>$1,440</td>
<td>$870</td>
</tr>
</tbody>
</table>

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


TrendMicro 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.