Trend Micro Releases 'Digital Souks,' a Comprehensive Whitepaper on the Regional Underground at GITEX 2017

Prices for malware and hacking tools at USD 19 in the region, as compared to USD 4 in North America

Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, today at GITEX 2017, released its comprehensive whitepaper, "Digital Souks: A Glimpse into the Middle Eastern and North African Underground," detailing criminal activities within the underground of this region. Prices for malware and hacking tools are generally a bit more expensive than in other regions. For example, a keylogger in the North American underground runs for USD 1-USD 4, but here it can be up to USD 19. However, the willingness for members to share content for a mutual cause helps balance out the price differences.

The Middle Eastern and North African underground is where culture, ideology, and cybercrime meet. Trend Micro has seen that regional marketplaces closely reflect the societies in which they operate. In this region, this facilitates itself in the "spirit of sharing" mindset, held by those that operate here, with a feeling of brotherhood and religious alliance that transcends the illicit transactions that occur.

"Still a propagating market, the region is not at par in terms of scale and scope when compared to other regions, but the products and services available remain common and sophisticated," said Ihab Moawad, Vice President, Trend Micro, Mediterranean, Middle East & Africa. "We now have a heightened awareness of the region, which then allows us to gather and analyze threat intelligence so that we can better help the region strengthen its cyber defenses. Trend Micro will continue to monitor regional marketplaces so we can proactively empower our ecosystem, and offer greater clarity to law enforcement agencies, here in the region, and globally."

"Also, the prevalence of giving services and malware away for free is interesting. Other underground marketplaces provide support to members, but the extent and willingness in this region is unique," added Moawad.

The ideology of hacking, as a service is unique to MENA's underground due to the ideology that drives its trade. In other marketplaces, like in North America or Russia, their purveyors mostly focus on selling their wares and forum participants don't band together to plan cyberattacks.

Hacktivism, DDoS attacks and website defacements are a staple in this region. These tactics are often carried out by members who present ideological distrust toward Western countries, as well as local governments. Major primary product categories are, malware: 27 percent, fake documents 27 percent, stolen data 20 percent, crimeware 13 percent, weapons 10 percent, and narcotics 3 percent.

Crimeware sold includes a variety of cryptors, malware and hacking tools. Worm USD1-USD 12, keylogger free-USD19, known ransomware USD 30-USD 50, malware builder Free-USD 500, citadel (FUD) USD150, ninja RAT (FUD) USD100, and Havij 1.8 (Cracked) for free.

Hosting providers in the region make significant profit by selling regionalized hosting spaces, which allows for local language and time settings in addition to faster connection speeds. A single IP connection and 50 GB of hard disk space, for instance, are sold for USD 50. Smaller plans exist, and start as low as USD 3. To some extent, the price is at par with other underground marketplaces, such as that of China.

Similar to the Russian underground, cashout services also abound here. These are platforms from which

physical items, usually stolen, are converted into cash. These services are paid in bankcards, Bitcoins (BTC) or via direct cash transactions.

A unique aspect of cash out services here is how they are used to bypass security mechanisms and legal requirements in the region, such as those in place for the purchase of cell phones, and disposable SIM cards. In the MENA underground, DDoS services can be purchased by hacktivists and threat actors to further their ideology.

Private and public organizations are often targeted, however the service is not as prevalent as is widely believed, and its rarity commands a steep price. The average is USD 45 per hour, with three-hour packages at USD 275, and involves tools such as Low Orbit Ion Cannon (LOIC) or Lizard Stresser.

Malware as a Service (MaaS) typically includes a purveyor, a malware developer selling a single binary or a combination of a binary and builder marketed as fully undetectable (FUD). Average prices are USD 20 for a binary, and USD 30–USD 110 for a binary with C&C infrastructure. A binary-builder package costs around USD 150–USD 400.

Stolen identities are sold in forums across the region. The Arabic forum hack-int in Egypt sells stolen identities for USD 18. 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 resident status. A daunting real-world implication is a dangerous person buying these fake documents, and slipping through to other countries as refugees.

Furthermore, Virtual Private Networks (VPNs) are a mainstay for cybercriminal activity and can be purchased due to the anonymity they provide. VPNs offered here are purportedly secure, don’t store logs, and have multiple hop points. Cybercriminals will typically use these servers as either part of a botnet, or a jump-off platform for further attacks.

For this research, Trend Micro 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 criminals sell commodities to and from the Middle East and North Africa, they are also operating globally.

###

About Trend Micro

Trend Micro Incorporated, a global leader in cybersecurity solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks and endpoints. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and control, enabling better, faster protection. With more than 5,000 employees in over 50 countries and the world’s most advanced global threat intelligence, Trend Micro enables organizations to secure their journey to the cloud. For more information, visit www.trendmicro.com.

---

https://newsroom.trendmicro.ca/2017-10-10-Trend-Micro-Releases-Digital-Souks-a-Comprehensive-Whitepaper-on-the-Regional-Underground-at-GITEX-2017