allot
See. Control. Secure.

How Effective are CSP Security Services for the Mass Market?

Telco Security Trends, Q2 2018

Executive Summary

Welcome to Allot's third Telco Security Trends Report in a series of three that looks at different aspects of delivering value-added security services to the mass market. The first report: A Consumer View on Mobile Security focused on consumer awareness, willingness to pay and preference for security service providers. The second report: Build Revenues and Brand Loyalty, presented the business results of CSPs that deliver network-based security services, including the ramp-up rate of service introduction and adoption rates of up to 40%.

This report looks at the security aspect of delivering network-based security services. It has been prepared with the support of our security researchers in Spain and Israel, whose primary task is to support our CSP customers. By analyzing the mobile and IoT threats that consumers face, we can help CSPs to communicate best practices and increase the effectiveness of the security protections provided by our platforms.

Our findings reveal that the mass market is a significant target for cybercrime, and that it would benefit from professional security services since subscribers lack the expertise to effectively protect themselves. Safety in numbers - a behavior adopted by most consumers - is not applicable due to the dynamic and automated nature of the threat landscape. Our research is based on data from four CSPs in Europe and Israel, covering seven million protected customers over a period of four months from November 2017. It provides the following highlights:

Demonstrating the automated nature of the threat landscape, we found that on average, two protections were activated per mobile device per day. We also found that an IoT device will get infected within minutes of being connected to the Internet. Our direct findings resulted in 42.5 seconds while other research found that things start to misbehave within three minutes of being connected to the Internet.

This report is particularly timely because we saw an escalation of crypto-jacking (the hijacking of a device or smartphone for crypto-mining that generates coins to the attacker's wallet) corresponding to the rising valuations of crypto currency. Such an escalation demonstrates the dynamic nature of the threat landscape.

When considering only direct financial loss, the cost of cybercrime to the subscriber is $38.26 per month on average. This yields a 1:40 cost-effectiveness of the service to the subscriber when compared to the ~$1 per month that they would need to pay their service provider for robust security protection. When we take into account indirect costs such as the deterioration of battery life due to cryptojacking or the cost to remove malware, the cost-effectiveness of such a service increases by tenfold or more.

Cybercrime is big business and is most likely here to stay. With the threat landscape being automated and dynamic, security protections must be controlled by professionals (not the consumer) in order to adapt to new threats. Supporting this claim is the fact that we witnessed the use of evasion techniques by cybercriminals; the use of encryption, methods that evade DNS-based protections and processes that hinder reverse engineering and analysis of the malware itself.

CSPs are in the best position to deliver security to the mass market and significant revenue can be achieved, as demonstrated in previous reports – leading to a win-win for the CSP and the consumer. What is required is a robust architecture that delivers a unified, multi-layer security service network, CPE and endpoint that hides all the complexities from the end user.

Introduction

We are living in an increasingly connected world. The growth of IoT and mobility means that connectivity is pervasive. It extends way beyond communication because it now profoundly affects how we live, work, learn and entertain ourselves. From workflow apps to gaming; from vehicle navigation systems to remotely-controlled household lighting and heating; everything we do, everywhere we go can benefit from mobility and IoT connectivity.

The mass market presents a large and increasing attack surface. It's estimated that there are currently about six billion consumer IoT devices connected worldwide and 2.6 billion smartphone subscriptions globally. Projections suggest that both these numbers will treble by 2020. In correlation, cybercrime is expanding and transforming to take advantage and maximize returns in this space by employing automations and high levels of innovation. With stakes like these, the business of protecting the mass market is more significant than ever. Consumer software security is estimated to be $5B USD and we expect this to grow alongside the growth of IoT and Mobile devices and rising consumer awareness.

The Threat Landscape

The threat landscape has proven to be dynamic, owing to constant innovation and automation. Over the past two years we have seen the following characteristics and attributes that continue to make mobile security threats a significant concern:

If it works don't fix it | Many types of common malware can be detected with high levels of confidence and many exploit vulnerabilities that are well known and have available patches. Yet cybercriminals continue to use them because consumers don't patch their smartphones, they don't employ security technologies at all or at best do it ineffectively, thereby remaining exposed. They want someone else to secure them.

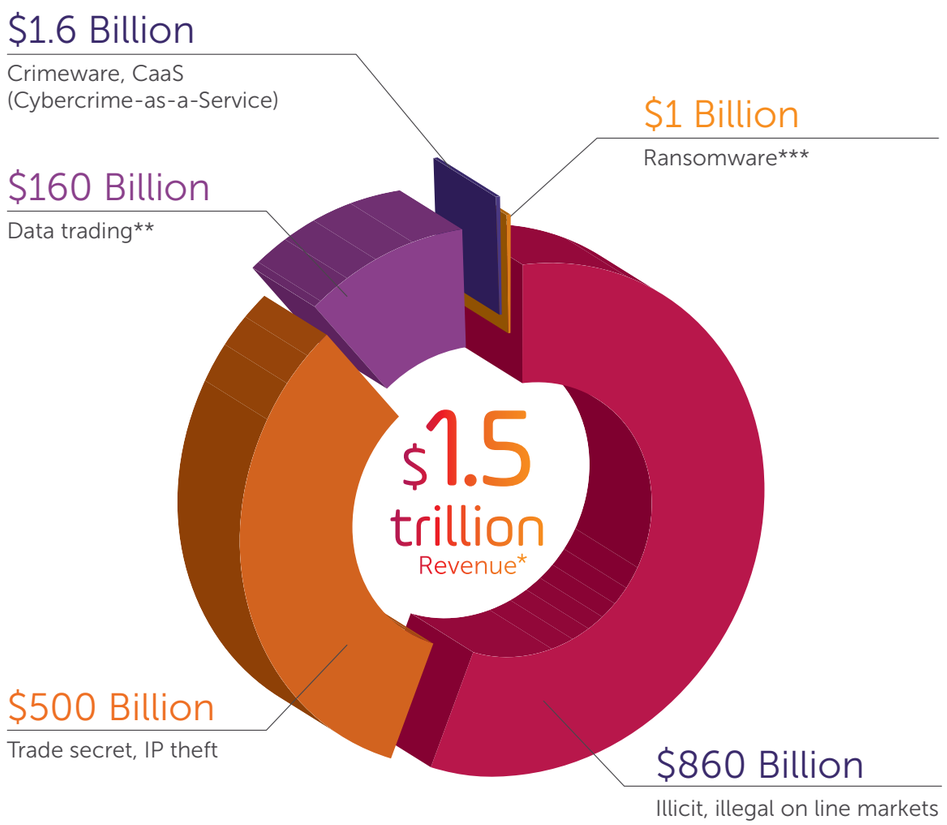
Evasion techniques | Google has tightened Android OS to make it harder to get superuser rights. Cybercriminals counter this action by achieving the same result with admin rights. DNS protections are countered with the use of hardcoded IP addresses or DNS servers to circumvent DNS based protections. In-line systems are countered with encryption. This is a financially motivated arms-race.

Entrepreneurship | The motivation for targeting the mass market is purely financial, and the level of creativity employed is akin to the startup community. When cryptocurrencies reached elevated valuations, the criminal community found new sources of revenue. When IoT started to achieve critical mass, cyber criminals found a new domain for exploitation. The cybercrime industry is in touch with, and takes advantage of, new and changing consumer trends.

The Threat Landscape

Financial monetization

Cybercrime is here to stay. A lot has been written about the cost of cybercrime to the economy with estimations ranging in the area of $600 billion USD a year worldwide. But this is not what directly motivates cybercriminals. Cybercrime is here to stay to because it has become a significant "industry" that is expected to be larger and more profitable than the global trade of all major illegal drugs combined, by 2021. It is estimated that cybercrime already generates about $1.5 trillion in revenue. This is a conservative estimate, based on data drawn from only five of the highest profile, most lucrative varieties of revenue-generating cybercrimes (see Appendix A for examples of monetization techniques and associated malware):



* Totals are approximate

** Revenues derived from trading in stolen data, such as: credit and debit card informationbanking log-in details, loyalty schemes and so on

*** Revenues derived from extortions based on encrypting data and demanding payments

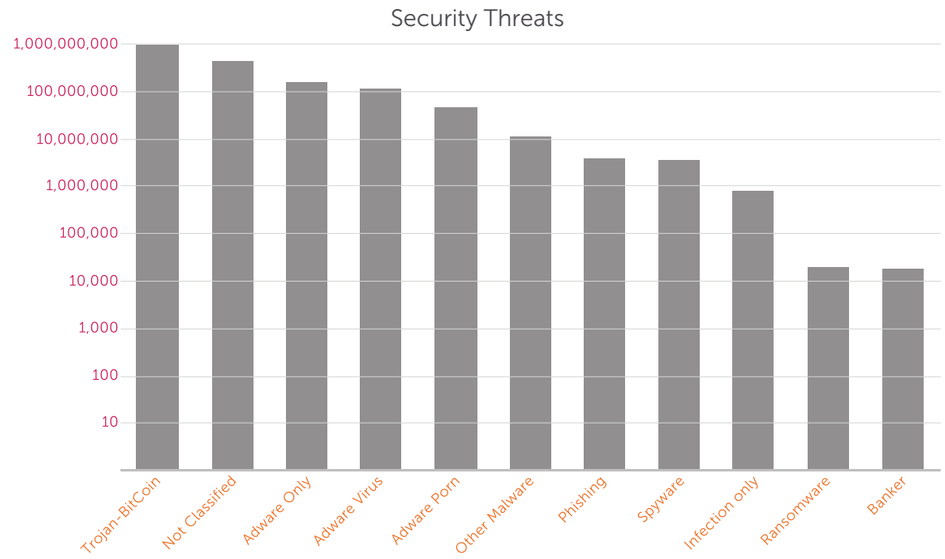
What We Found

Our research focuses on two primary attack vectors: mobile security and consumer IoT security. The information gathered in these two areas is based on actual consumer-related threats to mobile and IoT endpoints, either identified or protected in the wild.

Mobile-related threats

The following data was collected from four mobile operators in Europe and Israel, protecting slightly over seven million subscribers over a period of four months, from the beginning of November 2017 to the end of February 2018. During that period 1.73 Billion protections were activated, on average two (2.03) protections were activated per user per day. The large sample of seven million subscribers represents ~0.5% of the combined population in the countries studied, and provides about a 1% statistical error for the total population.

The type of protections activated were on upstream requests where the URL and SNI for encrypted requests are inspected for malicious websites and infected pages that are blocked and in-line downstream inspection of data payloads for malware (clear text only). The downstream inspection represents about 15% of the activated protections. The graph below shows the different categories of malware / adware blocked on a logarithmic scale for clarity.



Threat analysis

Direct attacks on the end user in the form of ransomware and banking trojans have received a lot of attention in the media due to their aggressive nature but they are the least common type of threat, with 40,000 protections activated (about 1.4 attacks per 1000 subscribers per month). However, these attacks represent a scarier, frontal attack on the subscriber and his pocket. This may also be the reason that they are rarer since there are stealthier and more indirect means of monetization.

What We Found

Cryptojacking

Our findings show that during the period coinciding with the buzz about crypto currencies and their elevated valuations, cryptomining malware was the leading security threat, with almost one billion activated protections. The malware used is based on Coinhive libraries. Coinhive is a mining site that enables websites to monetize their content by mining coins instead of relying on advertising revenue. As long as permission is provided by the visitor, this is not illegal. The problem begins when the Coinhive library is used to hijack the processing power of the user's phone, computer or device to mine coins without the subscriber's consent or knowledge and sometimes without the knowledge of the website owner. Infection with the cryptojacking malware takes place when visiting websites that load the malicious cryptomining software onto the browser or when downloading innocent looking applications that include the malicious code as depicted above. In order to understand the effect of cryptojacking on a phone, we infected a Sony Xperia M2. The effect on the phone was a spike in CPU usage to 99%, dramatic overheating of the battery and the phone became unresponsive. These results are not always the case. The malware can be configured in such a manner to limit the CPU/GPU usage, thus reducing its impact and avoiding detection by not rendering the phone totally useless.

Cryptojacking in an innocent app and the resulting performance hit on a Sony Xperia M2

Monetization

Adware is a broad category of malware. Adware stands for advertising malware that presents unwanted advertisements using intrusive and at times dangerous methods. Not all adware is malicious. At best it is a nuisance. But at its worst, it can undermine your security settings to track your activities and display ads where it normally wouldn't have access. These security breaches can then be exploited by more dangerous players. Adware continues to dominate the threat landscape as it seems to be a fairly safe means of monetization for the criminal. Most people are unaware of the privacy issues that adware creates because personal information can be stolen and traded. The real damage is to the advertising industry. Its reputation suffers. It pays for fraudulent clicks and furthermore, websites lose advertising revenue.

What We Found

Cost of not having protection

According to Kaspersky (at the time of writing this report) the cost of the following security incidents to the consumer are: $76 to fix malware, money lost or stolen $281 (including the effects of phishing or banking trojan), and ransom paid $125. When considering only direct financial loss as a result of money lost or stolen and ransomware we get an average of $38.26 saved per end user per month. This yields a ~1:40 cost effectiveness of the service to the consumer when compared to the cost of the service typically at ~$1 per customer per month. When we take into account indirect costs such as the deterioration of battery life due to cryptojacking or the cost to remove malware, the cost-effectiveness of having protection increases tenfold or more.

Consumer IoT threats

IoT has opened a new attack vector for cybercrime exploitation. With the growth of consumer IoT and the extreme lack of security in many of these devices, cybercriminals are recruiting them into herds of botnets for the purpose of spam, cryptojacking or DDoS attacks (DDoS attacks are monetized by being offered as a service). In order to understand the extent of this threat and for the purpose of improving the security capabilities of our HomeSecure solution, we set up honeypots that simulated consumer IoT devices and exposed them to the Internet. The results were alarming. Immediate successful attacks on the devices, peaked at a rate of 1000 per hour, as can be seen in the results below. Based on the aggressive speed and attacks on our honeypots we calculated that on average, a connected device will get infected within 42.5 seconds.

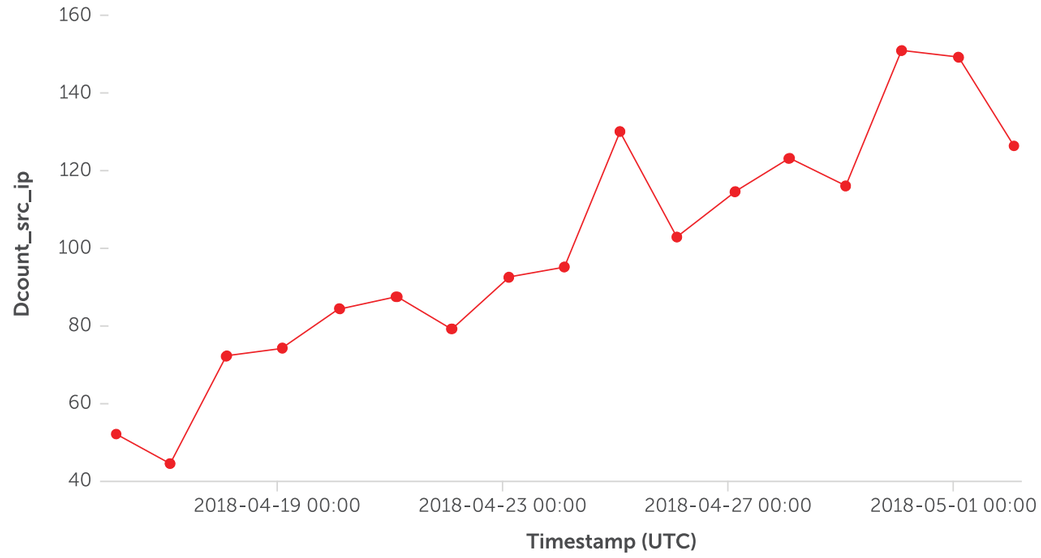
What We Found

Below are the results of two such honeypots with an average of 2033 successful connections per day per machine, median 1363 and peak at 26,762 successful connections per day!

Successful hourly attacks on two IoT honeypots over a period of six weeks: April 24 - May 2 2018

What We Found

In addition, and as expected we saw an increase of unique IP addresses attacking the honeypots over time from 44 a day to a peak of 155 a day in under a month of exposure.



IoT attack flow

The flow of the attacks we experienced and some of the accompanying activity we saw are generalized below with some insights into the innovation involved.

I. The attacker scans for vulnerable devices over the internet. The sources of the scan were either from previously hacked devices or attack servers.
   - It is notable that home devices or home CPE were the sources of the peak scans that we can safely assume directly affected the devices' user experience and congested the Internet connection of those homes by populating the NAT table of a home router.

II. Hacking the device through password brute force or using a known exploit in the operating system of the device.
   - Available malware such as Reaper and Satori exploit device vulnerabilities.
   - Infamous Mirai exploited default or weak passwords

III. After successfully hacking into the device the attacker usually drops its payload (the actual malware)
   - Downloading the payload through common methods - wget, curl, tftp, ftpget including more than one for backup. In most cases downloading it from hardcoded IPs without using domains to circumvent DNS based security.
   - "Writing" the malware on the device using an echo command. This avoids the need for a second connection.

What We Found

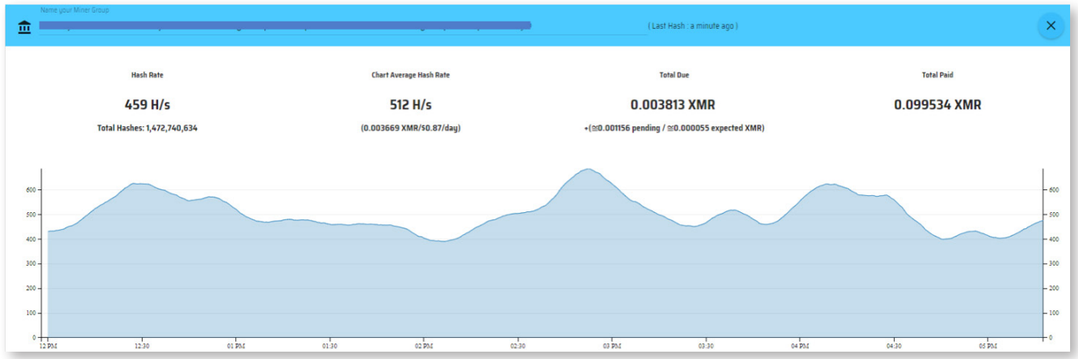
IV. Running the payload, which effectively recruits the device into the attacker botnet. These include:
- DDoS Botnet for hire
- Identifying additional vulnerable devices for further growth of the botnet
- Using the device as a HTTP proxy to anonymize traffic and hide other illegal activities
- Crypto-jacking

V. Innovative implementations that cybercriminals employ to increase their success rate.
- We found malware that uses hard coded DNS servers (Google 8.8.8.8 for example) and malware that changes the DNS server for the device itself to bypass DNS security protections.
- Also, some of the malware incorporated techniques to increase survivability: searching and killing other malware processes, closing telnet and other listening communication ports, and using anti debugging methods to obstruct research of their malware by security researchers.
- Upon successful connection, some attackers checked the system architecture, disk size etc. to make sure they were on a real device and not a honeypot before moving forward.

What We Found

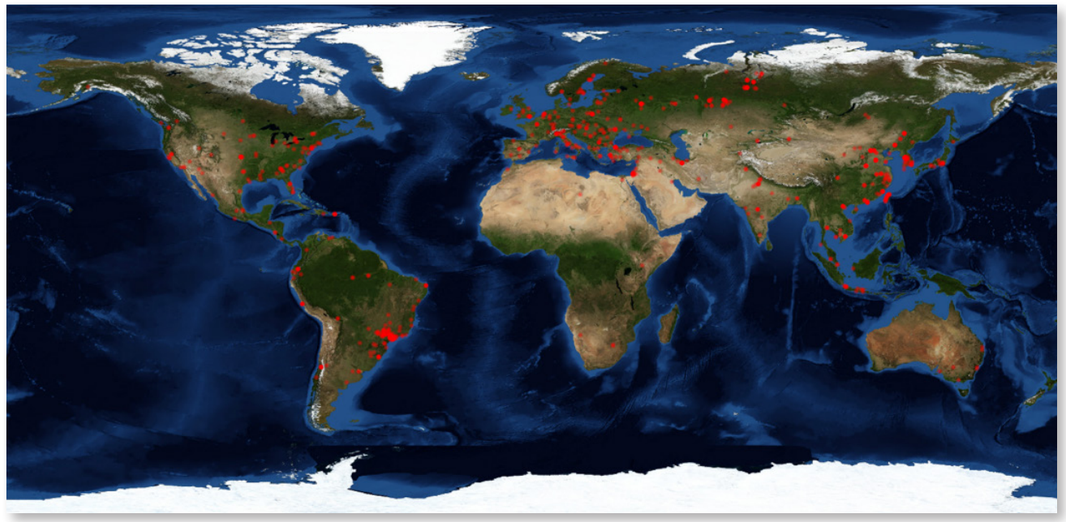
Cryptojacking devices

Our researcher also found several cryptojacking attempts that led to the attacker's currency source (one of a group). Although the amount generated by a single device was small when multiplied by many devices, it can reach substantial revenue.



Source of IoT scans and attacks

From a geographical perspective the borderless Internet enabled attacks to come from all over the map with no specific correlation. The diagram below shows the wide distribution of attacks and their sources.



Conclusion

Cybercrime is thriving and will continue to draw on technical innovation to take advantage of the growing mobile and IoT attack surface given the financial motivation they provide. The levels of sophistication and automation and the dynamic nature of cybercrime requires a minimal level of security expertise that is not available directly to the consumer and hence must be provided as service.

From this and our two previous reports (A, B), the case for CSP-delivered security services to the mass market can be summarized as follows:

I. There is a high level of security awareness and a willingness to pay CSPs for security value-added services.

II. CSP network-based security, with built-in customer engagement capabilities achieves rapid customer acquisition and high adoption rates of 40%.

III. Network-based security services deliver a cost-effective service by a factor of 1:40 to the consumer and significant incremental business to the CSP of ~$1 per subscriber per month.

CSPs are best positioned to deliver security to the mass market and significant revenue can be achieved – leading to a win-win for the CSP and the consumer. What is required is a robust architecture that delivers a unified, multilayer security service implemented at the network layer, CPE, home LAN and endpoint that hides all complexities from the end user.

Click Here to Learn More About Preventing Cybercrime »

Appendix A

Examples of monetization techniques and associated malware mentioned in this report.

Super user / Root control

Rooting Malware has always been the biggest threat to Android users as it is designed to gain super user or admin rights that allow its users to do almost anything. Once a device is under control, any of the following monetization methods can be incorporated:

Clickers

This type of malware "clicks" on page elements on behalf of the user. The malware visits regular advertising pages, where it steals money from advertisers, rather than from the user. In other cases, it visits pages with WAP subscriptions, with the money being taken from the user's mobile account. A page with WAP billing usually redirects to a mobile operator page where the user confirms they agree to pay for the services. However, this doesn't stop the malware. It is able to click these pages as well. It can even intercept and delete SMSs sent by mobile operators containing information about the service costs.

Banking trojans

Mobile banking Trojans overlay a legitimate app's interface with its own phishing window, where a user is asked to enter their bank card details - an action that appears quite normal to the user. The targeted apps are designed to make payments and are therefore likely to request this sort of data. Modifications of banking trojans attack not only financial apps but also apps for booking taxis, hotels, tickets, etc.

Ransomware

Mobile ransomware is both simple and effective. It overlays all other windows with its own window, blocks the operation of the device or changes / resets the device's PIN code, then demands a ransom in order to go away. Some have acquired modifications capable of encrypting user files, though in general encryption functionality isn't that popular among mobile Trojans.

Cryptojacking

Cryptojacking is the act of using a target's computer resources to mine cryptocurrency or cryptomining without the knowledge or consent of the victim. Cryptomining is achieved by performing the computations necessary to create new cryptocurrency tokens. These newly mined tokens are deposited to wallets owned by the attacker, while the cost of mining, reduced battery life and typically an unresponsive phone - are borne by the victim.

Adware

Adware is the most common form of malware, since monetization is relatively "legal" depending on the country of operation. Once a user is infected, they can be tracked across the entirety of the Internet, and the content of any page on which they land can be modified. This is the essence of ad injection including Pop-ups, Display (Banner) Overlay/Replacement, Affiliate link replacement etc. They can also serve malicious activity such as Click fraud.

IoT attacks

With the growth of consumer IoT and the extreme lack of security in many of these devices, cybercriminals are easily recruiting them into herds of botnets for the purpose of spam or DDoS (DDoS attacks are monetized by being offered as a service) and cryptojacking.

Phishing

Websites mask themselves as a legitimate website of a bank or on-line store and capture financial or login credentials for use or to be traded as an asset. Phishing can be launched through well-crafted emails that direct you to their website, sometimes ironically asking you to authenticate yourself due to malicious behavior they have seen.

Telco Security Trends

Q2 2018

About Allot Communications

Allot Communications Ltd. (NASDAQ, TASE: ALLT) is a provider of leading innovative network intelligence and security solutions for service providers worldwide, enhancing value to their customers. Our solutions are deployed globally for network and application analytics, traffic control and shaping, network-based security services, and more. Allot's multi-service platforms are deployed by over 500 mobile, fixed and cloud service providers and over 1000 enterprises. Our industry leading network-based security as a service solution has achieved over 50% penetration with some service providers and is already used by over 18 million subscribers in Europe. Allot. See. Control. Secure. For more information, visit www.allot.com.

D261054