Securing Business Communications in the Cyberespionage Era

ABIresearch®
www.abiresearch.com

ABIresearch®

Innovative business leaders trust ABI Research to help make transformative technology decisions. For more than 25 years, ABI Research has been embedded in the planning and workflows of the world's leading technology and innovation organizations. We are their execution partner, providing business intelligence and accelerating their overall decision-making process to more quickly and confidently execute strategies.

silent circle

Silent Circle is a leader in enterprise privacy, delivered through a revolutionary mobile platform of devices, software and services, starting with ZRTP to build a fundamentally different mobile architecture. For more information, please visit silentcircle.com.

Securing Business Communications in the Cyberespionage Era

Enterprise cybersecurity is only as good as the weakest link, and the communications channel is often one of the weak links that is often overlooked. Cyberattacks directed against enterprises have grown both in numbers and sophistication over the past decade to the point where breaches and data theft have become commonplace. Cyberthreats, such as advanced persistent threats (APTs), are continually evolving and the communications channel is an increasingly common threat vector for launching many of these attacks.

Corporate espionage is rife with actors looking to leverage the weakest link in order to steal data from competitors. Criminal espionage has flooded the market, with the resale of corporate data on black markets finding unscrupulous buyers keen to purchase stolen information and intellectual property.

Cyberespionage in the Mobile Era

More dangerously, cyberespionage has come of age, and the mobile platform is no exception to eavesdropping efforts. In fact, its vulnerability has made it a prime target for threat actors. Cellular monitoring, intercept, and data exfiltration are common and widespread practices, performed similarly by cybercriminals as by nation states. The state of cyber insecurity has reached the point where cyberwarfare is a reality. Practices include reaching across borders to infiltrate, intercept, disrupt, and paralyze foreign digital assets. Governments are taking part in two distinct types of cyber activities: covert infiltration for political and economic espionage, and covert surveillance for active disruption.

The extent of cyberespionage undertaken by state actors and quasi-official organizations in countries such as China and Russia are far reaching, and actors are expanding their own competencies in many other countries, including: Iran, Israel, Saudi Arabia, Syria, South Africa, Japan, North and South Korea, Canada, the United Kingdom, the United States, Australia, New Zealand, Germany, France, and Italy, among many others.

China is often touted as one of the most dangerous state actors on the APT scene. The country has developed extensive capabilities and invested significant resources in cyberespionage. Its efforts aim to propel national industrial development and international political influence. China's economic Five-Year Plan identifies seven priority industries, and the majority of victim organizations hit consistently by Chinese APTs correspond to the sectors outlined in China's 5-year plan. Security outfit Mandiant was the first to observe that the industries targeted by the People's Liberation Army's (PLA) APT1 matched four of the seven new industries identified in China's 12th Five-Year Plan back in 2013.

A number of governments, security research firms, and private sector organizations have admitted to suffering repeated Chinese-based cyber intrusions and theft. The attacks have focused on infiltrating specific companies and extracting confidential business information and intellectual property as surreptitiously as possible. And the country has been highly successful at doing so.

Doing business with China or even traveling there on business can be hazardous for enterprises. At customs and in hotels, it is common for electronic devices, laptops, and smartphones to be tampered with, and the government closely monitors cellular communications, as well as Internet traffic. Many foreign governments and enterprises provide guidance for business travelers on safeguarding data before going to China. But even enterprises that are not working with Chinese players or focusing on the market are fair game for its aggressive APT campaigns.

While Chinese efforts may be more obvious than others, they are not the only country actively engaged in mass surveillance. The extent of cyberespionage undertaken by the U.S. National Security Agency (NSA) and a number of its allies was ignominiously revealed by former contractor Edward Snowden, who leaked vast amounts of classified information in 2013 detailing the agency's cyber activities. The leaks revealed that the agency, together with other government agencies, including the FBI and the CIA, is actively accessing, intercepting, and analyzing vast amounts of data from an incredible number of U.S. companies in the information and telecommunication sector. In addition, the documents published showed a network of partnerships with various other governments (including the United Kingdom, Australia, Canada, New Zealand, France, Germany, Italy, Switzerland, Denmark, Norway, the Netherlands, Spain, Israel, and Singapore, among others) to gather and share data collected by those organizations within their own countries. Both the United States and the United Kingdom have openly admitted to the development of offensive cyberweapons for espionage and sabotage, with the support of Five Eyes.

StingRay, for example, is a cellular surveillance toolkit manufactured by Harris Corporation used by U.S. and U.K. military and law enforcement. In effect, it is an IMSI-catcher; essentially, a telephone eavesdropping device used for intercepting mobile phone traffic and tracking movement of mobile phone users. The toolkit has both passive (digital analyzer) and active (cell site simulator) capabilities. When operating in active mode, the device mimics a wireless carrier cell tower in order to force all nearby mobile phones and other cellular data devices to connect to it. StingRay is also capable of recording numbers for a mobile phone's incoming and outgoing calls, as well as intercepting the content of voice and text communications.

More recently, media outfits Le Monde and The Intercept published further information leaked by Snowden about the interception of phone calls and data by U.S. and U.K. intelligence services made from civil aircraft operated by the likes of Air France, Air Mexico, Etihad, Aeroflot, Qatar Airways, Saudi Airlines, Oman Air, among others. The documents reveal the agencies developed the "Southwinds" program to gather cellular activity, voice communication, data, metadata, and content of calls on board such aircrafts using Inmarsat satellites in real time. The data interception could be done on numerous mobile devices, including BlackBerry, but applications including web mail, IM, social networks, travel and Maps, currency converters, media, VOIP, BitTorrent, and Skype were also targeted.

As information on surveillance and espionage campaigns keep leaking, their true extent is difficult to discern, but continues to provide insight into an extensive and almost unfathomable global surveillance network, targeting all kinds of communications services, regardless of location or technology.

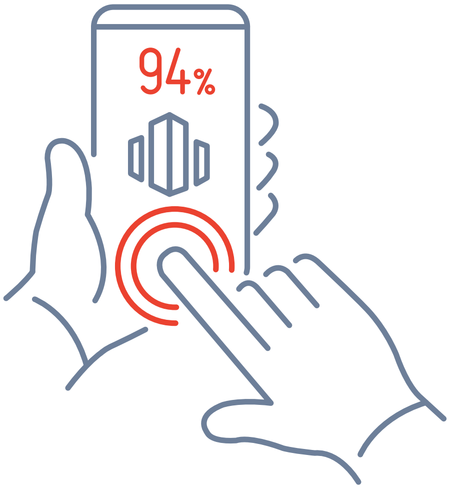
Advanced Threat Actors and Business Risks

Uncorrupted and integral communication is fundamental to all successful business endeavors. Communication technologies play a key role in how modern enterprises operate. The Internet has empowered enterprises, enabling new and diverse methods of communication between stakeholders: employees, executives, clients, and partners. In addition to voice and text, video conferencing, group messaging, and media sharing are all being transmitted using digital technologies. The advent of the cloud and mobile devices has opened up immense potential, allowing remote and interactive collaboration instantaneously between numerous parties. Digital platforms have been instrumental in keeping employees connected to the enterprise, and are the key enablers for the mobile workforce.

The growth of IP communications has been driven on a global scale by 3G/4G connectivity and the proliferation of smart devices. As of 2016, there are almost 1 billion users of VoIP worldwide, and 2.3 billion users of the top five mobile messaging apps (WhatsApp, Facebook Messenger, WeChat, Line, and Viber). This communication evolution has permeated the corporate space. Smartphones and digital communication apps are rife within enterprises, spurring BYOD adoption and the consumerization of IT. Business communications on smartphones represents 95% of work done over those devices, more than any other type of work performed. The general lack of security mechanisms around business communications, and notably IP-based platforms, makes them an ideal threat vector for data theft.

With threat vectors littering the wider ecosystem, IP communications have become a favorite target for organized cybercrime and APTs. The loss of control and the dispersion of corporate assets across heterogeneous environments run remotely by third-party platforms have caused a serious deterioration of enterprise security postures, which threat actors have been quick to exploit.

A large part of the problem encountered is that many enterprises are generally unaware of threats and do not fully understand the value of data that they share over their ICT infrastructure. Security beyond simple anti-virus solutions and a firewall is not seen as a necessary requirement. IT personnel are limited by budget requirements and management understands the security issue even less. Many organizations find it difficult to justify spending money on potential threats that cannot be qualified precisely. It is usually only after a breach has occurred that an enterprise will start reassessing their security strategy.



94% of companies investigated learn about the breach from an external source, normally law enforcement or other from third parties. The average number of days that elapse before a breach is discovered is 400 for large enterprises. 1,673 data breaches were reported in 2015, with over 707.5 million records compromised globally.

In many cases, breach and data theft will have been ongoing for some time and the damage done to the enterprise will already be significant. An alarming 94% of companies investigated learn about the breach from an external source, normally law enforcement or other third parties. And even more worrying, the average number of days that elapse before a breach is discovered is 400 for large enterprises. According to the Breach Level Index, 1,673 data breaches were reported in 2015, with over 707.5 million records compromised globally. The simple fact is that many of these breaches can be countered if adequate security measures are put in place comprehensively.

Enterprises in all sectors are at risk and the intensity or duration of attacks will depend on a number of factors and vary according to the threat actor's motivation. High-profile enterprises, such as multi-national organizations, and those in critical sectors, such as finance, energy, and pharmaceutical, for example, will be targets across all threat actor groups. Valuable data often targeted in these sectors include patents and other intellectual property (IP) rights, information related to mergers, acquisitions, and joint ventures, executive strategy documents, financial account information, management and IT staff credentials, private and confidential information, employee contact information, partnership information, P&L of privately-held companies, and investment and funding activities, among other data.

The focus of advanced threat actors is a serious challenge for enterprises. What many organizations fail to grasp is the importance of securing business communications, regardless of the platform or device used. This is a crucial exercise that must be performed at all levels of the enterprise: from the lowest intern to the CEO, from the building automation system contractor to the accounting firm employed. Any omission of an asset becomes a weak link in the chain and presents itself as a potential threat vector.

Malware delivery is complex and includes multiple facets, such as being augmented by social engineering techniques, notably through communication channels, and insider weaknesses in order to boost an attack's effectiveness. Certain actors in specific sectors will be difficult to detect, let alone counter.

Contrary to the complex vector of delivery discussed in the previous paragraph, the actual malware used to obtain enterprise data is not always very sophisticated; in fact, it rarely is. Threat actors will attempt to breach an enterprise's security using the simplest tools. For example, the SS7 signaling protocol is a technology that has been successfully subverted for some time, at least since 2008, and was most recently used against WhatsApp, Telegram, and Facebook Messenger mobile communications applications. The hack enabled threat actors to intercept and record calls and messages, forward calls, and track the location of the mobile device. All of this was done using the same system that mobile network operators use for service availability and to deliver communications.

One particular trend that is fundamental to understanding today's threat environment is the growth of IM. It is starting to displace emails as the primary form of communication between employees, notably within the younger workforce. This increasingly common scenario is fraught with danger, as data are rarely secured on such applications and devices. Threat actors have developed malware targeting these types of consumer applications, such as mSpy and WhatsSpy Public for spying on calls, browsing, text messages, WhatsApp conversations, and more, and many fake desktop varieties impersonating the applications in order to intercept data. For those that are not secured with encryption, the vulnerabilities are much greater. Zero-day exploits have been targeting WeChat, DI vulnerabilities in Facebook Messenger, a Facetime vulnerability that allowed audio to be kept open after termination of communication, and many more.

IT functions within many organizations are unaware of the apps being used and, therefore, cannot secure them effectively. Service providers of these tools do not offer that layer of security for voice and text, and even when they do, the management and control is often out of the enterprise's hands. When IT is informed about such tools being used by employees, they are often unable to securely connect such tools to enterprise business systems and this means functions such as reporting, auditing, or compliance cannot be fulfilled. Even more worrying is that, when an employee leaves the enterprise, data exchanged on those tools will also leave with them.

The fact that IT administrators are generally the last to know or are unable to exert control and management over business communications is a real problem. This lack of basic protection allows corporate information to flow freely outside the enterprise on unsecured channels. All employees are guilty of embracing BYOD without informing IT administrators. The unfortunate reality of Business 2.0 is that productivity, availability, and efficiency routinely come before security.

Enterprise Cybersecurity is a Multi-Layered Approach

Securing the hardware itself, then securing the applications, and then the communication vector, as well. This is important for enterprises.

Most important of all for enterprises to understand is that security cannot be selectively applied. All the holes need to be plugged, at all levels. Employees and executives alike are concerned by this breakdown in security; third-party contractors across the supply chain represent a potential threat vector. A resolved perpetrator will often find the easiest point of entry, and once inside, escalate internally to reach the most valuable assets. Unfortunately, business communication security is often overlooked in favor of securing email servers, databases, networks, and systems. And yet, communication technologies are at the center of highly valuable data exchanges between employees at all levels who define strategies, create plans of action, and make key decisions regarding business operations.

Security needs to be implemented comprehensively and enterprise-wide for business communications, and any half measure will be as useless as no measure.

One of the primary measures to deploy is end-to-end encryption, whether over cellular or IP. Using a VPN to encrypt communications is a necessary first step. But enterprises should also make sure that the devices and the backend infrastructures are also secure, ensuring that the service provider does not offer any backdoors that can be used by governments. In many countries, such a feature can be a legal requirement, specifically made by national security agencies.

In addition, security of communications can be hardened through a secure hardware foundation within the device itself, which can provide secure boot and root of trust functionalities and, therefore, a secure foundation for applications.

The difficulty with deploying this level of comprehensive end-to-end security throughout a company is providing a frictionless experience. The communication tools must remain easy to use, the security must be easy to manage, and the overall deployment must be cost effective. Encryption is not an easy technology to implement or simplify. And with modern digital communication technologies, it must be scalable to the entire employee population, be platform-agnostic, and be usable worldwide.

silent circle

Solution Spotlight

Silent Circle's mobile secure communications platform addresses exactly those difficulties. It is a simple, secure solution that can be deployed for the whole enterprise. The platform consists of three pieces, which together, form a comprehensive secure business communications solution.

Silent Phone is the first piece of the platform. It is a secure VoIP voice and messaging application for smartphones. The encryption used for securing communications end-to-end is ZRTP, a true peer-to-peer key negotiation and management for secure VOIP communications. Silent Phone includes features such as video chat and conference calling capability, as well as encrypted texts with burn (self-destruct) functionality, and encrypted file sharing (files to 100MB, including Word, PDF, PowerPoint, etc.) on any Silent OS, iOS or Android device. Silent Phone offers HD quality calls offered over mobile data network or Wi-Fi. The application also offers short authentication strings safeguard against Man-in-The-Middle attacks.

Silent World is a feature of Silent Phone and offers an extended encrypted calling service. Users can make or receive calls from standard mobiles or land lines, as well as from the Blackphone. Silent World calls are routed through Silent Circle's secure servers before reaching the public switched telephone network. The leg of the call between the device and Silent Circle servers is encrypted. Users can securely connect to other devices in 83 different countries, with no roaming charges.

Blackphone is the second piece; a smartphone with secure boot and integrity verification, encrypted by default with 128-bit AES to protect stored data. An enhanced Android OS (Silent OS) offers numerous privacy and security settings housed in one central app: the Security Center. Security features include remote wipe, blocking unknown sources, fine tuning individual permissions, managing app sharing and privacy, individual privacy control, and the creation of individual virtualized spaces. Blackphone integrates with popular MDM systems and the Android for Work Program. Silent Circle maintains its own distribution system to directly issue Silent OS updates. OTA updates to address major vulnerabilities are submitted for certification within 72 hours of vulnerability notification.

Silent Manager is the third and final piece of the platform; a software console that ties it all in, offering a simple and secure web-based service to manage the users, groups, plans and devices in place across the enterprise. The console is set up to be simple, with zero-touch deployment. Silent Manager includes Active Directory Single Sign-On and LDAP integration, and secure administrator access to manage plans, users, and groups. Furthermore, it is API-enabled and can be catered to large scale Circle in Circle deployments.

These three pieces—Silent Phone, Blackphone, and Silent Manager—together form the Silent Circle's mobile secure communications platform. Targeting the device, the software, and the service, Silent Circle offers a global comprehensive solution for secure business communications. Deployed throughout the enterprise, it can lock down those weak links and threat vectors regardless of location, while providing a frictionless communication channel for employees and executives alike.

Published January 3, 2017

©2017 ABI Research
249 South Street
Oyster Bay, New York 11771 USA
Tel: +1 516-624-2500
www.abiresearch.com

© 2017 ABI Research • abiresearch.com • No part of this document may be reproduced, recorded, photocopied, entered into a spreadsheet or information storage and/or retrieval system of any kind by any means, electronic, mechanical, or otherwise without the expressed written permission of the publisher.

Exceptions: Government data and other data obtained from public sources found in this report are not protected by copyright or intellectual property claims. The owners of this data may or may not be so noted where this data appears.

Electronic intellectual property licenses are available for site use. Please call ABI Research to find out about a site license.