KASPERSKY lab

KASPERSKY SECURITY INTELLIGENCE

Threat Intelligence Report for the Telecommunications Industry

Table of Contents

Introduction 3

Executive Summary 4

Typical Threats Targeting Telecoms 5

- Overview 5
- Threats Directed at Telecoms Companies 5
  - Targeted Attacks 6
  - Unaddressed Software Vulnerabilities 6
  - The Impact of Service Misconfiguration 7
  - Vulnerabilities in Network Devices 9
  - Malicious Insiders 11
- Threats Targeting CSP/ISP Subscribers 12
  - Overview 12
  - Social engineering, Phishing and Other Ways In 13
  - Vulnerable Kit 13
  - The Risk of Local Cells 15
  - USIM Card Vulnerabilities 16

Conclusion 17

Introduction

The telecommunications industry keeps the world connected. Telecoms providers build, operate and manage the complex network infrastructures used for voice and data transmission – and they communicate and store vast amounts of sensitive data. This makes them a top target for cyber-attack.

According to PwC's Global State of Information Security, 2016, IT security incidents in the telecoms sector increased 45% in 2015 compared to the year before. Telecoms providers need to arm themselves against this growing risk.

In this intelligence report, we cover the main IT security threats facing the telecommunications industry and illustrate these with recent examples.

Our insight draws on a range of sources. These include:

- The latest telecoms security research by Kaspersky Lab experts.
- Kaspersky Lab monitoring systems, such as the cloud antivirus platform, Kaspersky Security Network (KSN), our botnet tracking system and multiple other internal systems including those used to detect and track sophisticated targeted (advanced persistent threat, APT) attacks and the corresponding malware.
- Underground forums and communities.
- Centralized, specialized security monitoring systems (such as Shodan).
- Threat bulletins and attack reports.
- Newsfeed aggregation and analysis tools.

Threat intelligence is now a vital weapon in the fight against cyber-attack. We hope this report will help telecoms providers to better understand the cyber-risk landscape so that they can develop their security strategies accordingly.

We can provide more detailed sector and company-specific intelligence on these and other threats. For more information on our Threat Intelligence Reporting services please email intelligence@kaspersky.com.

Executive Summary

Telecommunications providers are under fire from two sides: they face direct attacks from cybercriminals intent on breaching their organization and network operations, and indirect attacks from those in pursuit of their subscribers. The top threats currently targeting each of these frontlines feature many classic attack vectors, but with a new twist in terms of complexity or scale that place new demands on telecoms companies.

These threats include:

- **Distributed Denial of Service (DDoS) attacks.** DDoS attacks continue to increase in power and scale and, according to the 2016 Data Breach Investigations Report, the telecommunications sector is hit harder than any other. Kaspersky Lab's research reveals that in Q2, 2016, the longest DDoS attack lasted for 291 hours (or 12.1 days) – significantly longer than the previous quarter's maximum (8.2 days), with vulnerable IoT devices increasingly used in botnets. Direct DDoS attacks can reduce network capacity, degrade performance, increase traffic exchange costs, disrupt service availability and even bring down Internet access if ISPs are hit. They can be a cover for a deeper, more damaging secondary attack, or a route into a key enterprise subscriber or large-scale ransomeware attack.
- **The exploitation of vulnerabilities in network and consumer devices**. Our intelligence shows that vulnerabilities in network devices, consumer or business femtocells, USBs and routers, as well as root exploits for Android phones, all provide new channels for attacks – involving malware and technologies that individuals, organisations and even basic antivirus solutions cannot always easily remove.
- **Compromising subscribers with social engineering, phishing or malware**. These classic techniques remain popular and can easily be mastered by entry-level cybercriminals, although 2016 sees changes in how more sophisticated attackers conduct their campaigns. Growing numbers of cyber-attackers now combine data sets from different sources, including open sources, to build up detailed pictures of potential targets for blackmail and social engineering purposes.
- **Insider threat is growing**. Detailed profiles of targets are also used to recruit insiders to help perpetrate cybercrime. Some insiders help voluntarily, others are coerced through blackmail. Insiders from cellular service providers are recruited mainly to provide access to data, while staff working for Internet service providers are chosen to support network mapping and man-in-the-middle attacks.

Other threats facing telecommunications companies include targeted attacks; poorly configured access controls, particularly where interfaces are publicly available to any Internet user; inadequate security for 2G/3G communications; and the risk of telecoms providers being drawn into unrelated attacks that exploit telecoms resources, and suffering collateral damage as a result.

Typical Threats Targeting Telecoms

Overview

We can divide the main threats facing the telecommunications industry into two, interrelated, categories:

- **Threats targeting telecommunication companies directly**. These include DDoS attacks, targeted attacks (APT campaigns), network device vulnerabilities and human-related threats like insider access, social engineering and the risk of allowing third parties to access information.
- **Threats targeting subscribers of telecoms services – particularly the customers of cellular service providers (CSPs) and Internet service providers (ISPs)**. These include malware for mobile devices, subscriber data harvesting, end-user device vulnerabilities, and more.

Threats Directed at Telecoms Companies

DDoS

DDoS (distributed denial of service) attacks remain a serious threat to telecoms providers around the world as attackers discover ever more ways of boosting the power and scale of attacks. Kaspersky Lab's DDoS intelligence report for Q2, 2016 notes that websites in 70 countries were targeted with attacks. By far the most affected country was China, with South Korea and the US also among the leaders. 70.2% of all detected attacks were launched from Linux botnets, with cybercriminals paying close attention to financial institutions working with cryptocurrency. Another trend observed in Q2 was the use of vulnerable IoT devices in botnets to launch DDoS attacks.

The telecommunications sector is particularly vulnerable to DDoS attacks. According to the 2016 Data Breach Investigations Report, the telecommunications sector was hit around twice as hard as the second placed sector (financial exchanges), with a median DDoS packet count of 4.61 million packets per second (compared to 2.4 Mpps for exchanges.)

The impact of a DDoS attack should not be underestimated. Direct attacks can reduce network capacity, degrade performance, increase traffic exchange costs, disrupt service availability and even bring down Internet access if ISPs are affected. With a growing number of connected devices and systems supporting mission-critical applications in areas such as healthcare and transport, unexpected downtime could be life threatening.

Further, DDoS attacks can be a cover for a deeper, more damaging secondary attack, or a route into a key enterprise subscriber or large-scale ransomware attack.

A good example of the first is the 2015 cyber-attack on the UK telecoms company, TalkTalk. The hack, allegedly perpetrated by a couple of teenagers, resulted in the loss of around 1.2 million customers' email addresses, names and phone numbers, as well as many thousands of customer dates of birth and financial information – all ideal for use in financially-motivated social engineering campaigns. The forensic investigation revealed that the hackers had used a smokescreen DDoS attack to conceal their main activities.

DDoS attacks are also evolving. 2015 saw attackers amplify the power of DDoS attacks by turning them into DrDoS (Distributed reflection Denial of Service) attacks through the use of standard network protocols like NTP, RIPv1, NetBIOS (Network Basic Input/Output System) and BGP (Border Gateway Patrol). Another approach that is becoming more commonplace is the compromise of end-user routers via network-scanning malware and firmware vulnerabilities. Today's faster mobile data transfer speeds and the growing adoption of 4G are also making smartphone-based botnets more useful for implementing DDoS attacks.

The worrying thing is that even inexperienced attackers can organize quite an effective DDoS campaign using such techniques.

Targeted Attacks

The core infrastructure of a telecommunications company is a highly desirable target for cybercriminals, but gaining access is extremely difficult. Breaking into the core requires a deep knowledge of GSM architecture, rarely seen except among the most skilled and resourced cybercriminals. Such individuals can generally be found working for advanced, international APT groups and nation-state attackers, entities that have a powerful interest in obtaining access to the inner networks of telecommunication companies. This is because compromised network devices are harder to detect by security systems and they offer more ways to control internal operations than can be achieved through simple server/workstation infiltration.

Once inside the core infrastructure, attackers can easily intercept calls and data, and control, track and impersonate subscribers.

Other APTs with telecommunications on their radar

The Regin APT campaign, discovered in 2014, remains one of the most sophisticated ever seen and has the ability to infiltrate GSM networks, while the Turla group, has developed the ability to hijack satellite-based Internet links as part of it's Command & Control process, successfully obscuring its actual location.

Others, such as Dark Hotel and a new cyber-espionage threat actor likely to be of Chinese origin, exploit telecoms networks in their targeted campaigns. In these cases, the telecoms providers often suffer collateral damage even though they are not directly related to the attack. Further details on these can be found on Kaspersky Lab's expert Securelist blog or through a subscription to the Kaspersky APT Threat Intelligence Reporting service.

Unaddressed Software Vulnerabilities

Despite all the high profile hacks and embarrassing data leaks of the last 12 months, attackers are still breaching telecoms defenses and making off with vast quantities of valuable, personal data. In many cases, attackers are exploiting new or under-protected vulnerabilities.

For example, in 2015, two members of the hacker group, Linker Squad allegedly gained access to Orange Spain through a company website vulnerable to a simple SQL injection with the intention of stealing customer and employee data.

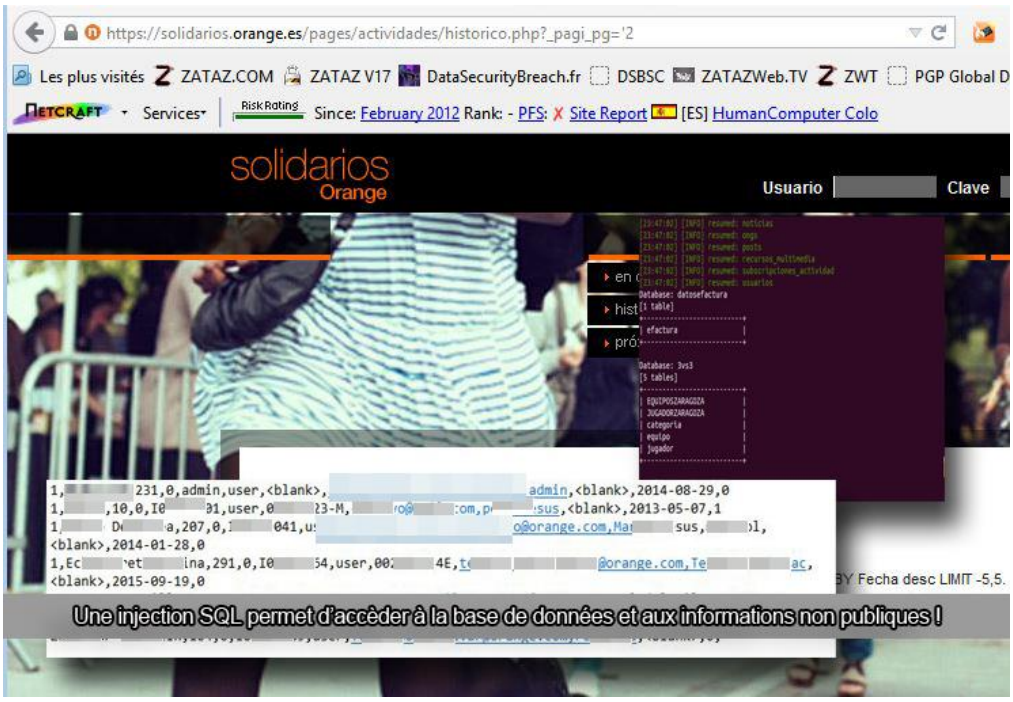

Figure 1. SQL injection vulnerability on Orange Spain web site

The Impact of Service Misconfiguration

In many cases, the hardware used by the telecommunications industry carries configuration interfaces that can be accessed openly via HTTP, SSH, FTP or telnet. This means that if the firewall is not configured correctly, the hardware in question becomes an easy target for unauthorized access.

The risk presented by publicly exposed GTP/GRX (GPRS Tunneling Protocol/GPRS Roaming Exchange) ports on devices provides a good example of this.

As CSPs encrypt the GPRS traffic between the devices and the Serving GPRS Support Node (SGSN), it is difficult to intercept and decrypt the transferred data. However, an attacker can bypass this restriction by searching on Shodan.io for devices with open GTP ports, connecting to them and then encapsulating GTP control packets into the created tunnel.

Table 1. Top 10 countries with GTP/GRX ports exposed to Internet access

#	Country	Number of GTP/GRX
1	China	52.698
2	Turkey	8.591
3	United States of America	6.403

#	Country	Number of GTP/GRX
4	Canada	5.807
5	Belgium	5.129
6	Colombia	2.939
7	Poland	2.842
8	Morocco	1.585
9	Jamaica	862
10	United Arab Emirates	808

The Border Gateway Protocol (BGP) is the routing protocol used to make decisions on routing between autonomous systems. Acceptance and propagation of routing information coming from other peers can allow an attacker to implement man-in-the-middle (MITM) attacks or cause denial of service. Any route that is advertised by a neighboring BGP speaker is merged in the routing database and propagated to all the other BGP peers.

Table 2. Top five countries with BGP protocol exposed to Internet access

#	Country	Number of devices (end of 2015)
1	Republic of Korea	16.209
2	India	8.693
3	United States of America	8.111
4	Italy	2.909
5	Russian Federation	2.050

An example of such an attack took place in March 2015, when Internet traffic for 167 important British Telecom customers, including a UK defense contractor that helps to deliver the country's nuclear warhead program, was illegally diverted to servers in Ukraine before being passed along to its final destinations.

To avoid probable attacks against BGP from unauthorized remote malefactors, we recommend that companies provide network filtering, allowing only a limited number of authorized peers to connect to BGP services. To protect against malicious re-routing and hijacking initiated through authorized autonomous systems we recommend that they monitor anomalies in BGP communications (this can be done through specialized software solutions or by subscribing to alerts from vendors providing this kind of monitoring.)

Vulnerabilities in Network Devices

Routers and other network devices are also primary targets for attacks against telecommunications companies.

In September 2015, FireEye researchers revealed the router malware "SYNful knock", a combination of leaked privilege (root) credentials and a way of replacing device firmware that targets Cisco 1841, 2811 and 3825 routers (see Cisco advisory here).

Put simply, SYNful knock is a modified device firmware image with backdoor access that can replace the original operating system if the attacker has managed to obtain privileged access to the device or can physically connect to it.

SYNful is not a pure software vulnerability, but a combination of leaked privileged credentials combined with a certain way of replacing device firmware. Still, it is a dangerous way of compromising an organization's IT infrastructure.

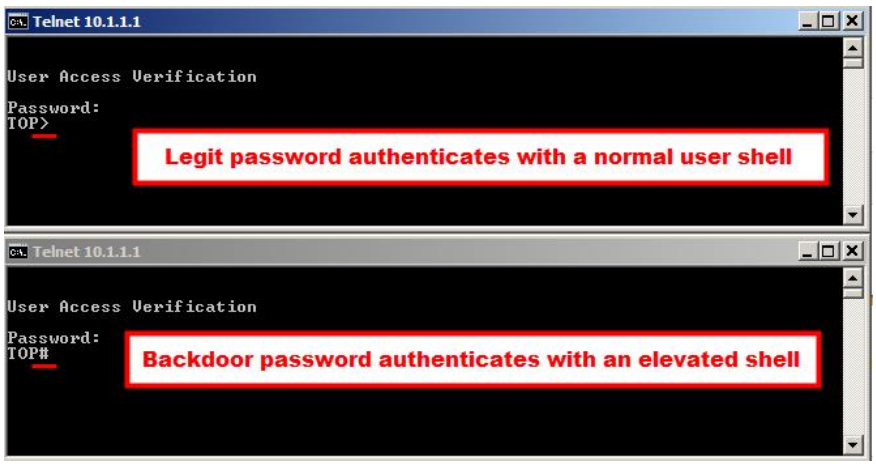

Figure 2. SYNful knock backdoor sign-in credentials request

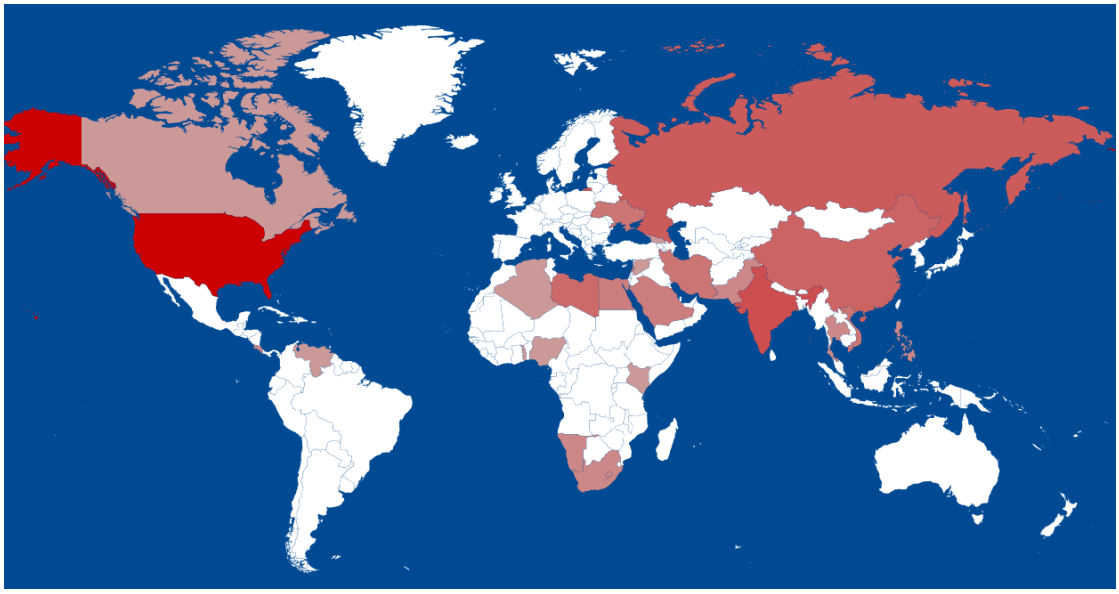

Figure 3. Worldwide distribution of devices with the SYNful knock backdoor

The latest information on the number of potentially compromised devices is available through the link https://synfulscan.shadowserver.org/stats/.

A second Cisco vulnerability, CVE-2015-6389 enables attackers to access some sensitive data, such as the password file, system logs, and Cisco PCA database information, and to modify data, run internal executables and potentially make the system unstable or inaccessible. Cisco Prime Collaboration Assurance Software releases prior to 11.0 are vulnerable. Follow this Cisco bulletin for remediation actions.

For further information on Cisco fixes for its devices see https://threatpost.com/cisco-warning-of-vulnerabilities-in-routers-data-center-platforms/115609.

Juniper, another network device manufacturer, has been found to carry vulnerabilities in its operating system for its NetScreen VPN appliances, enabling third-party access to network traffic. The issue was reported by the vendor in the security advisory JSA10713 on December 18th, 2015, along with the release of the patch.

It appears that the additional code with hardcoded password was planted in the source code in late 2013. The backdoor allows any user to log in with administrator privileges using hard-coded password "<<< %s(un='%s') = %u".This vulnerability has been identified as CVE-2015-7755 and is considered highly critical.

Top countries where ScreenOS devices are used are the Netherlands, the United States, China, Italy and Mexico.

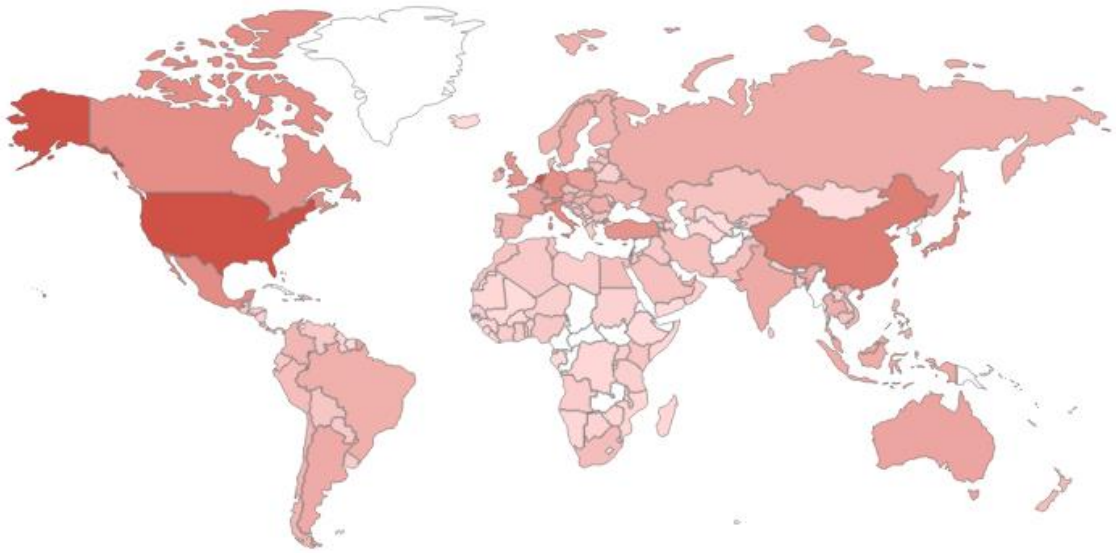

Figure 4. Juniper ScreenOS-powered devices worldwide

Another Juniper backdoor, CVE-2015-7756, affects ScreenOS 6.2.0r15 through 6.2.0r18 and 6.3.0r12 through 6.3.0r20 and allows a third party to monitor traffic inside VPN connections due to security flaws in the Dual_EC PRNG algorithm for random number generation.

To protect the organization from misconfiguration and network device vulnerability, Kaspersky Lab recommends that companies pay close attention to vulnerabilities in the network services of telecommunication equipment, establish effective vulnerability and configuration management processes, and regularly perform security assessments, including penetration testing for different types of attackers (a remote intruder, a subscriber, a contractor, etc.).

Malicious Insiders

Even if you consider your critical systems and devices protected and safe, it is difficult to fully control some attack vectors. People rank at the very top of this list. Their motivations are often hard to predict and anticipate, ranging from a desire for financial gain to disaffection, coercion and simple carelessness.

While insider-assisted attacks are uncommon, the impact of such attacks can be devastating as they provide a direct route to the most valuable information.

Examples of insider attacks in recent years include:

- A rogue telecoms employee leaking 70 million prison inmate calls, many breaching client-attorney privilege.
- An SMS center support engineer who had intercepted messages containing OTP (One-Time Passwords) for the two-step authentication required to login to customer accounts at a popular fintech company. The engineer was found to be freely offering his services on a popular DarkNet forum.

For attackers, infiltrating the networks of ISPs and CSPs requires a certain level of experience – and it is often cheaper and easier to stroll across the perimeter with the help of a hired or blackmailed insider. Cybercriminals generally recruit insiders through two approaches: enticing or coercing individual employees with relevant skills, or trawling around underground message boards looking for an appropriate employee or former employee.

Employees of cellular service providers are in demand for fast track access to subscriber and company data or SIM card duplication/illegal reissuing, while staff working for Internet service providers are needed for network mapping and man-in-the-middle attacks.

A particularly promising and successful attack vector for recruiting an insider for malicious intrusion is blackmail.

Data breaches, such as the 2015 Ashley Madison leak reveal information that attackers can compare with other publically available information to track down where people work and compromise them accordingly. Very often, these leaked databases contain corporate email addresses, including those of telecommunication companies.

Further information on the emerging attack vectors based on the harvesting of Open Source Intelligence (OSINT) can be obtained using Kaspersky Lab's customer-specific Intelligence Reporting services.

Threats Targeting CSP/ISP Subscribers

Overview

Attacks targeting the customers of cloud and Internet service providers remain a key area of interest for cybercriminals. We've revealed a number of malware activities and attack techniques based on internal information and incidents that were caught in our scope. As a result of analyzing this data the following main threats were identified:

- **Obtaining subscribers' credentials.** This is growing in appeal as consumers and businesses undertake ever more activity online and particularly on mobile. Further, security levels are often intentionally lowered on mobile devices in favor of usability, making mobile attacks even more attractive to criminals.
- **Compromising subscribers' devices**. The number of mobile malware infections is on the rise, as is the sophistication and functionality of the malware. Experienced and skilled programmers are now focusing much of their attention on mobile – looking to exploit payment services as well as low-valued assets like compromised Instagram or Uber accounts, collecting every piece of data from the infected devices.
- **Compromising small-scale telecoms cells used by consumers and businesses.** Vulnerabilities in CSP-provided femtocells allow criminals to compromise the cells and even gain access to the entire cloud provider's network.
- **Successful Proof-Of-Concept attacks on USIM cards.** Recent research shows that the cryptography of 3G/4G USIM cards is no longer unbreakable. Successful attacks allow SIM card cloning, call spoofing and the interception of SMS.

Social engineering, Phishing and Other Ways In

Social engineering and phishing remain popular activities and they continues to evolve and improve, targeting unaware or poorly aware subscribers and telecoms employees.

The attackers exploit trust and naivity. In 2015, the TeamHans hacker group penetrated one of Canada's biggest communications groups, Rogers, simply by repeatedly contacting IT support and impersonating mid-ranking employees, in order to build up enough personal information to gain access to the employee's desktop. The attack provided hackers with access to contracts with corporate customers, sensitive corporate e-mails, corporate employee IDs, documents, and more.

Both social engineering and phishing approaches are worryingly successful. The Data Breach Investigations Report 2016 found that 30% of phishing emails were opened, and that 12% clicked on the malicious attachment – with the entire process taking, on average, just 1 minute and 40 seconds.

Social engineers and phishers also use multiple ways for increasing the likeness of authenticity in their attacks, enriching their data with leaked profiles, or successfully impersonating employees or contractors. Recently criminals have successfully stolen tens of thousands of Euros from dozens of people across Germany after finding a way around systems that text a code to confirm transactions to online banking users. After infecting their victims with banking malware and obtaining their phone numbers, they called the CSP's support and, impersonating a retail shop, asked for a new SIM card to be activated, thus gaining access to OTP (One Time Passwords) or "mTan's" used for two-factor authentication in online banking.

Kaspersky Lab recommends that telecommunications providers implement notification services for financial organizations that alert them when a subscriber's SIM card has been changed or when personal data is modified.

Some CSPs have also implemented a threat exchange service to inform financial industry members when a subscriber's phone is likely to have been infected with malware.

Vulnerable Kit

USBs, modems and portable Wi-Fi routers remain high-risk assets for subscribers, and we continue to discover multiple vulnerabilities in their firmware and user interfaces. These include:

- Vulnerabilities in web interfaces designed to help consumers configure their devices. These can be modified to trick a user into visiting a specially crafted page.
- Vulnerabilities that result from insufficient authentication. These can allow for the modification of device settings (like DNS server addresses), and the interception, sending and receiving of SMS messages, or USSD requests, by exploiting different XSS and CSRF vulnerabilities.
- RCE (Remote Code Execution) vulnerabilities based on different variants of embedded Linux that can enable firmware modification and even a complete remote compromise.

Figure 5. Built-in "service" backdoor allowing no-authentication access to device settings

Examples of these kind of vulnerabilities were demonstrated in research by Timur Yunusov from the SCADAStrangeLove team. The author assessed a number of 3G/4G routers from ZTE, Huawei, Gemtek and Quanta. He has reported a number of serious vulnerabilities:

- Remote Code Execution from web scripts.
- Arbitrary device firmware modification due to insufficient consistency checks.
- Cross Site Request Forget and Cross Site Scripting attacks.

All these vectors can be used by an external attacker for the following scenarios:

- Infecting a subscriber's computer via PowerShell code or badUSB attack.
- Traffic modification and interception.
- Subscriber account access and device settings modification.
- Revealing subscriber location.
- Using device firmware modification for APT attack persistence.

Most of these issues exist due to web interface vulnerabilities (like insufficient input validation or CSRF) or modifications made by the vendor during the process of branding its devices for a specific telecommunications company.

The Risk of Local Cells

Femtocells, which are essentially a personal NodeB with an IP network connection, are growing in popularity as an easy way to improve signal coverage inside buildings. Small business customers often receive them from their CSPs. However, unlike core systems, they are not always submitted to suitably thorough security audits.

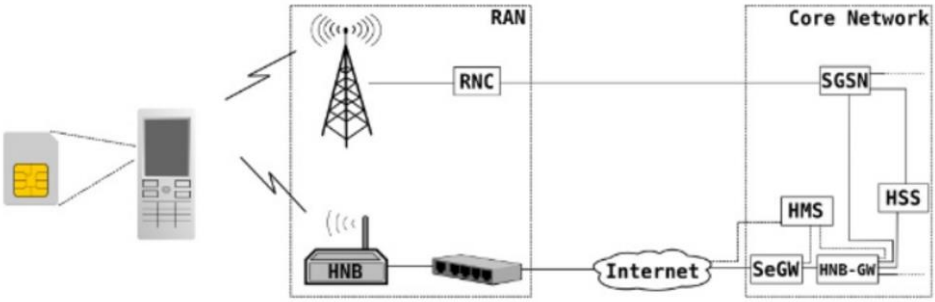

Figure 6. Femtocell connection map

Over the last year, our researchers have found a number of serious vulnerabilities in such devices that could allow an attacker to gain complete control over them. Compromising a femtocell can lead to call interception, service abuse and even illegal access to the CSP's internal network.

At the moment, a successful attack on a femtocell requires a certain level of engineering experience, so risks remain low – but this is likely to change in the future.

USIM Card Vulnerabilities

Research presented at BlackHat USA in 2015 revealed successful attacks on USIM card security. USIMs had previously been considered unbreakable thanks to the AES-based MILENAGE algorithm used for authentication. The reseachers conducted differential power analysis for the encryption key and secrets extraction that allowed them to clone the new generation of 3G/4G SIM cards from different manufacturers.

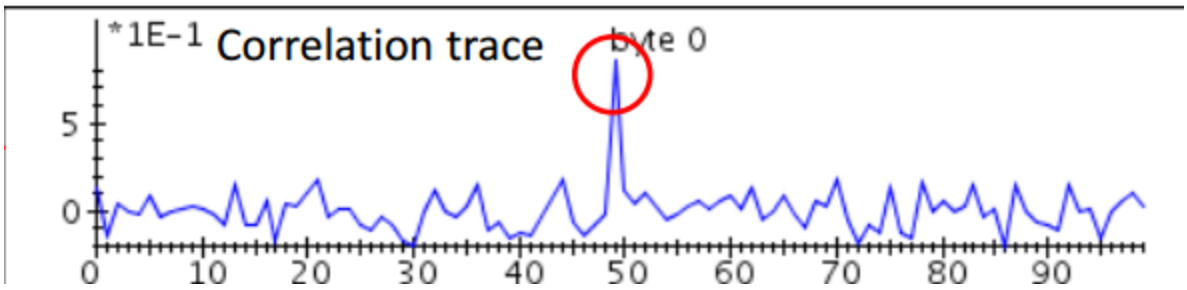

Figure 7. Right byte guess peak on differential power analysis graph

Conclusion

Telecommunications is a critical infrastructure and needs to be protected accordingly. The threat landscape shows that vulnerabilities exist on many levels: hardware, software and human, and that attacks can come from many directions. Telecoms providers need to start regarding security as a process – one that encompasses threat prediction, prevention, detection, response and investigation.

A comprehensive, multi-layered security solution is a key component of this, but it is not enough on its own. It needs to be complemented by collaboration, employee education and shared intelligence. Many telecommunications companies already have agreements in place to share network capability and capacity in the case of disruption, and now is the time to start reaping the benefit of shared intelligence.

Our Threat Intelligence Reporting services can provide customer-specific insight into the threats facing your organization. If you've ever wondered what your business looks like to an attacker, now's the time to find out. Contact us at intelligence@kaspersky.com