Cybersecurity and its Effects on Telcos

JAVED SAMUEL

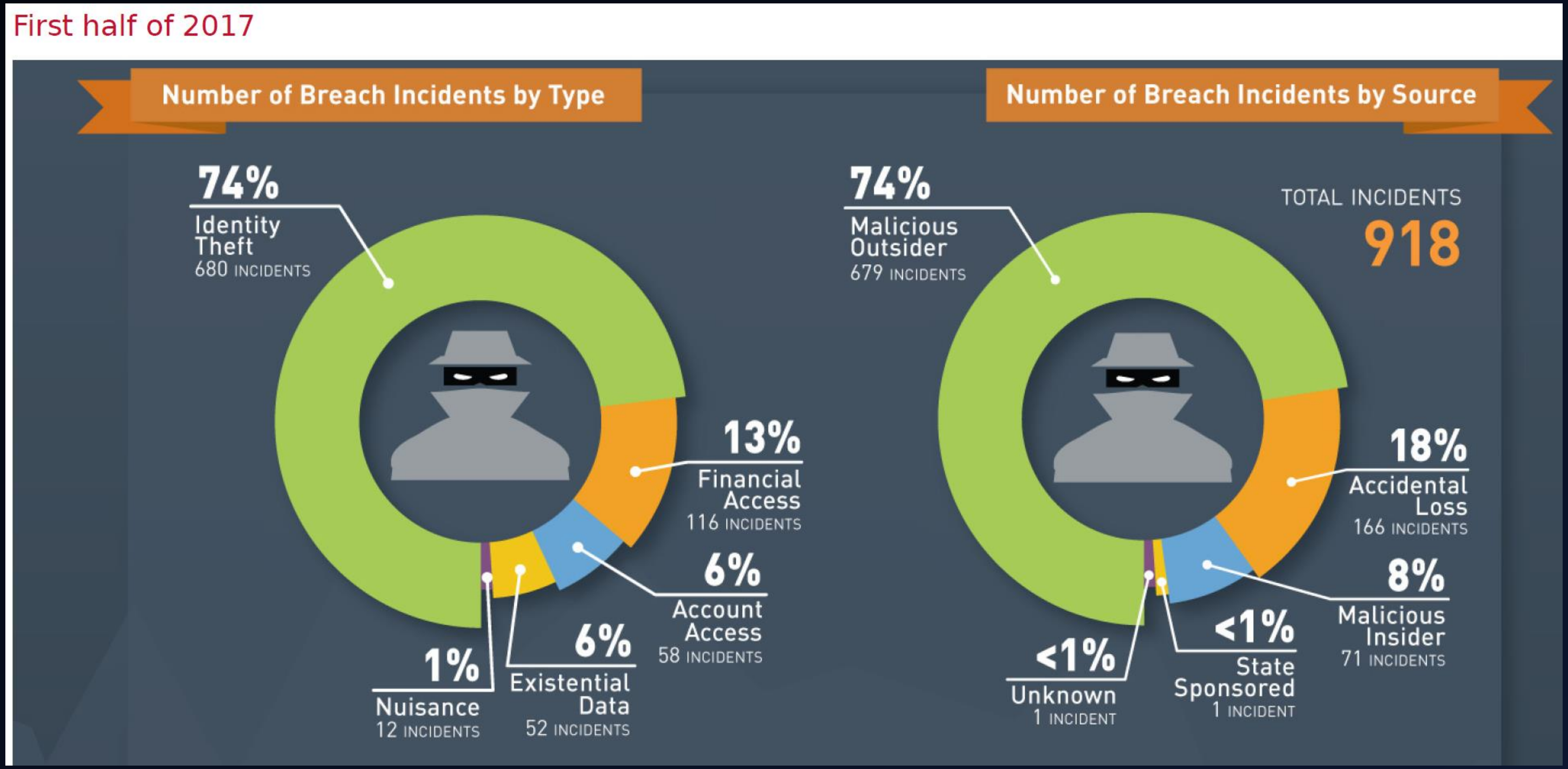
CYBER-SECURITY CONSULTANT

Cybersecurity Agenda

- Who are My Attackers?
- Telecos’ Cybersecurity Threats
- Telecos’ Customers Cybersecurity Threats
- Recommendations – What Can I Do?
- Conclusions
- Questions and Answers

Who Are My Attackers?

- Nation States
- Organized Crime
- Criminals
- Hackivists
- Insiders



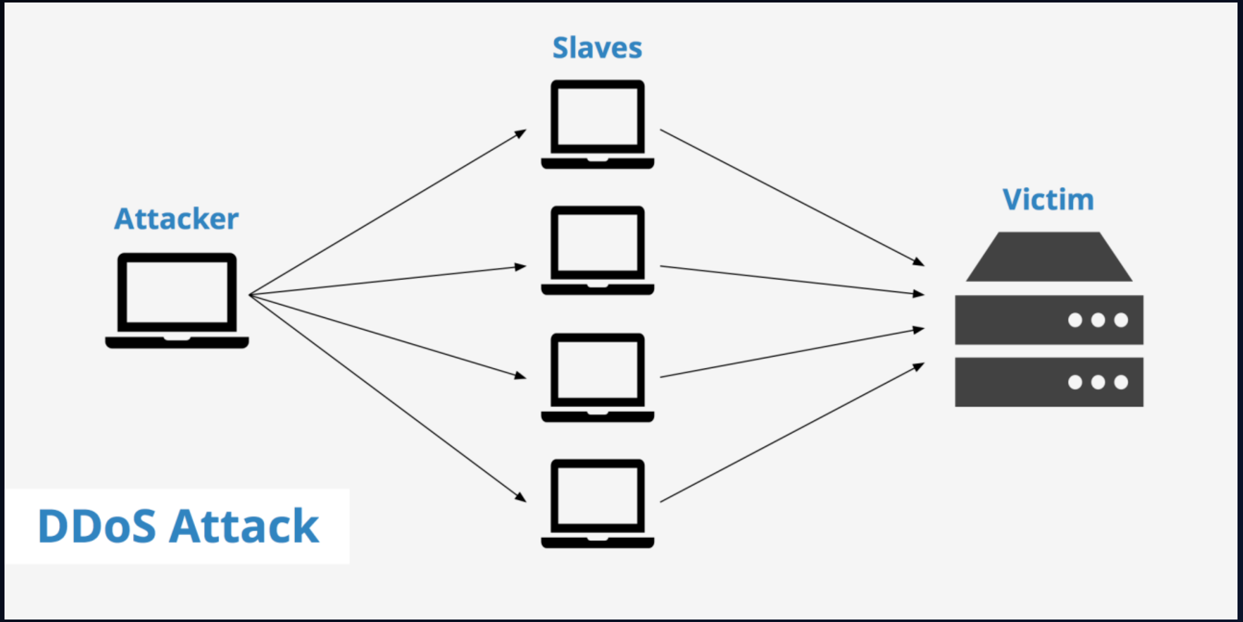
First half of 2017

Telecos’ Cybersecurity Threats

- Distributed Denial of Service (DDoS)
- Unaddressed Vulnerabilities in Software Applications and Network Devices
- Service Misconfigurations
- Malicious Insiders

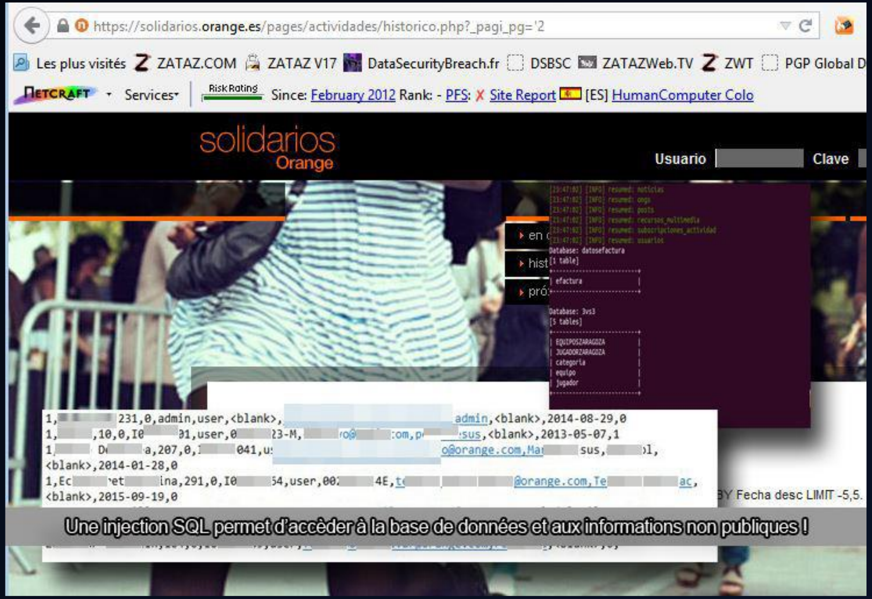
Distributed Denial of Service (DDoS)

- Reduce network capacity
- Degrade performance
- Increase traffic exchange costs
- Disrupt service availability
- Use of vulnerable IoT devices in botnets to launch DDoS attacks.
- Cover for a deeper, more damaging secondary attack



Unaddressed Vulnerabilities in Software Applications and Network Devices

- Application Vulnerabilities
  - Injection Attacks
  - Authentication Bypasses
  - Cross Site Scripting
- Network Device Vulnerabilities
  - SYNful knock
  - Enable third-party access to network traffic
  - Access to sensitive data

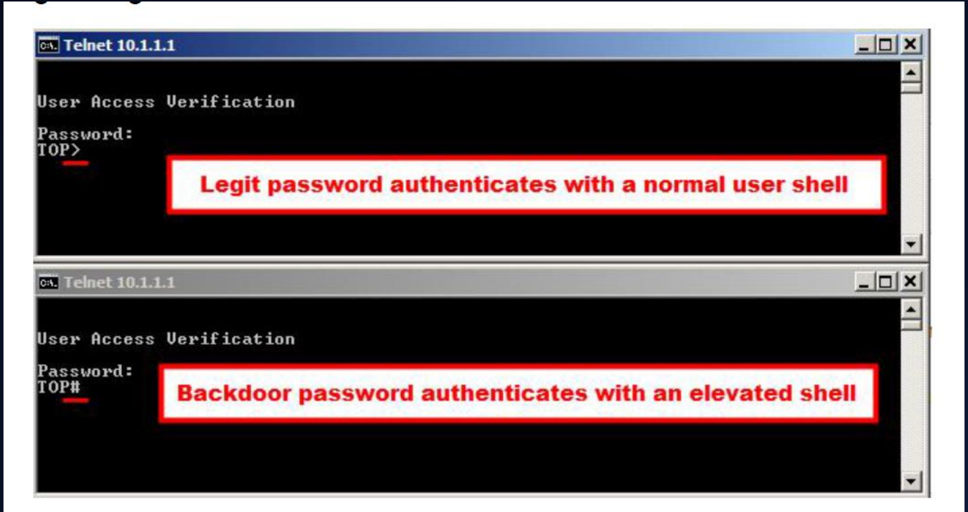


```
[21:47:02] [INFO] resumed: noticias
[21:47:02] [INFO] resumed: ongs
[21:47:02] [INFO] resumed: posts
[21:47:02] [INFO] resumed: recursos_multimedia
[21:47:02] [INFO] resumed: subscripciones_actividad
[21:47:02] [INFO] resumed: usuarios
Database: datosefactura
[1 table]
+---------------------------+
| efactura                  |
+---------------------------+

Database: 3vs3
[5 tables]
+---------------------------+
| EQUIPOSZARAGOZA           |
| JUGADORZARAGOZA           |
| categoria                 |
| equipo                    |
| jugador                   |
+---------------------------+
```

```
1,[redacted]231,0,admin,user,<blank>,[redacted]admin,<blank>,2014-08-29,0
1,[redacted],10,0,I0[redacted]91,user,0[redacted]23-M,[redacted]o@[redacted]:om,p[redacted]sus,<blank>,2013-05-07,1
1,[redacted] D[redacted]a,207,0,[redacted]041,u[redacted]o@orange.com,Ma[redacted]sus,[redacted]l,
<blank>,2014-01-28,0
1,Ec[redacted]et[redacted]ina,291,0,I0[redacted]54,user,00[redacted]4E,t[redacted]@orange.com,Te[redacted]ac,
<blank>,2015-09-19,0
```

BY Fecha desc LIMIT -5,5.

Une injection SQL permet d'accèder à la base de données et aux informations non publiques !



```
User Access Verification

Password:
TOP>
```

Legit password authenticates with a normal user shell

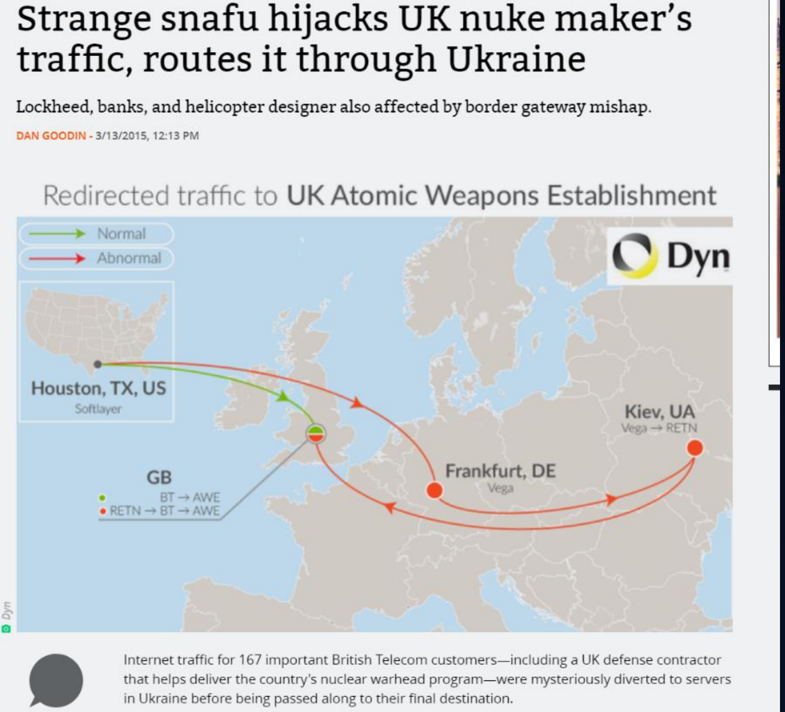
```
User Access Verification

Password:
TOP#
```

Backdoor password authenticates with an elevated shell

Figure 2. SYNful knock backdoor sign-in credentials request

Service Misconfigurations

- Publicly exposed GTP/GRX ports on devices
- BGP attacks where acceptance and propagation of routing information from other peers allows MITM attacks or denial of service.



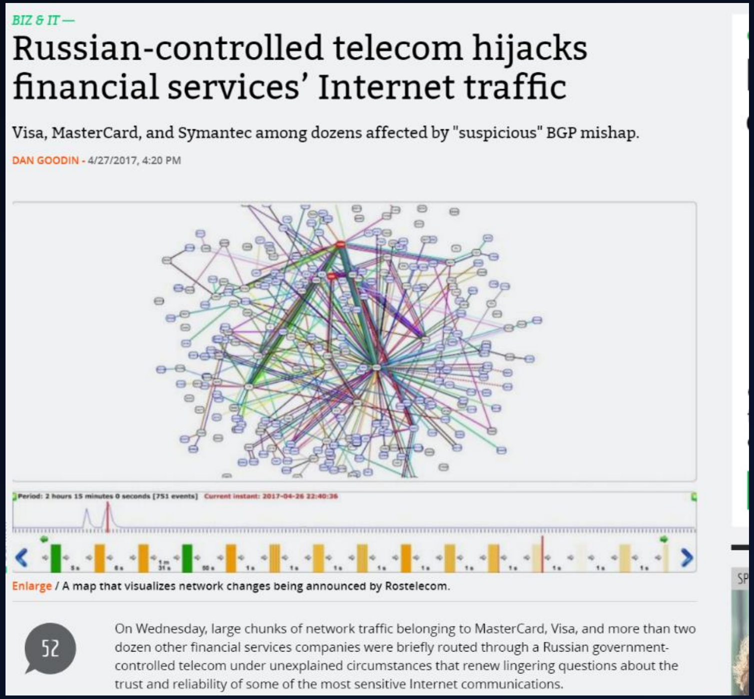
Strange snafu hijacks UK nuke maker's traffic, routes it through Ukraine

Lockheed, banks, and helicopter designer also affected by border gateway mishap.

DAN GOODIN - 3/13/2015, 12:13 PM

Redirected traffic to UK Atomic Weapons Establishment

Internet traffic for 167 important British Telecom customers—including a UK defense contractor that helps deliver the country's nuclear warhead program—were mysteriously diverted to servers in Ukraine before being passed along to their final destination.



BIZ & IT —

Russian-controlled telecom hijacks financial services' Internet traffic

Visa, MasterCard, and Symantec among dozens affected by "suspicious" BGP mishap.

DAN GOODIN - 4/27/2017, 4:20 PM

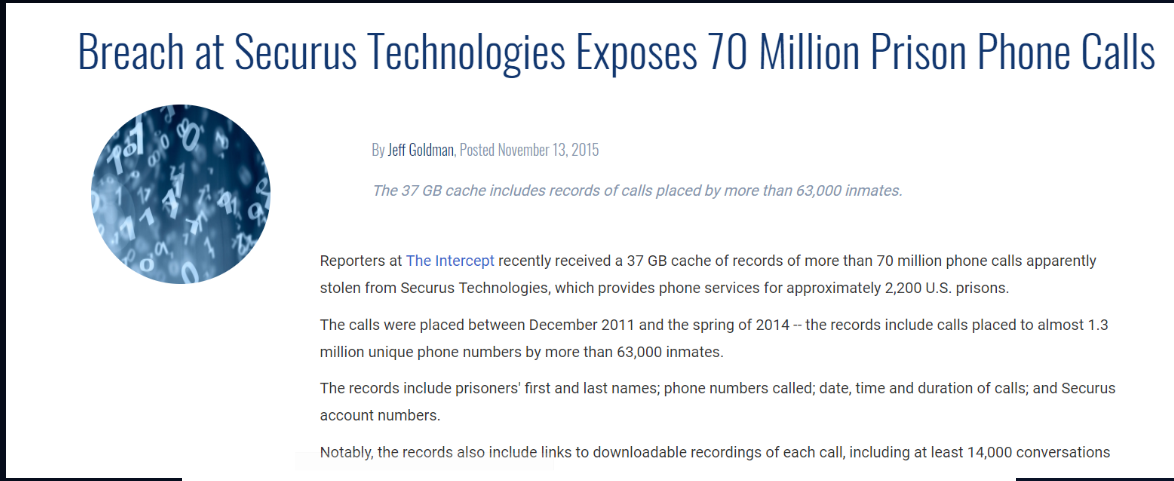
Period: 2 hours 15 minutes 0 seconds [751 events] Current instant: 2017-04-26 22:40:36

Enlarge / A map that visualizes network changes being announced by Rostelecom.

On Wednesday, large chunks of network traffic belonging to MasterCard, Visa, and more than two dozen other financial services companies were briefly routed through a Russian government-controlled telecom under unexplained circumstances that renew lingering questions about the trust and reliability of some of the most sensitive Internet communications.

Malicious Insiders

- Cheaper and easier to comprise a network with the help of a hired or blackmailed insider.
- Cybercriminals recruit insiders through two approaches
  - Entice or coerce individual employees with relevant skills
  - Trawl around underground message boards looking for an appropriate employee or former employee.



Breach at Securus Technologies Exposes 70 Million Prison Phone Calls

By Jeff Goldman, Posted November 13, 2015

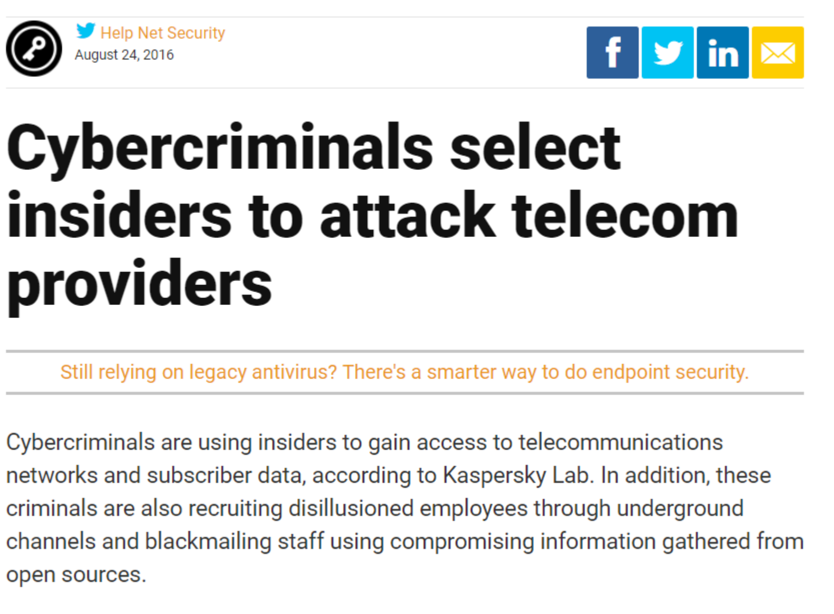
The 37 GB cache includes records of calls placed by more than 63,000 inmates.

Reporters at The Intercept recently received a 37 GB cache of records of more than 70 million phone calls apparently stolen from Securus Technologies, which provides phone services for approximately 2,200 U.S. prisons.

The calls were placed between December 2011 and the spring of 2014 -- the records include calls placed to almost 1.3 million unique phone numbers by more than 63,000 inmates.

The records include prisoners' first and last names; phone numbers called; date, time and duration of calls; and Securus account numbers.

Notably, the records also include links to downloadable recordings of each call, including at least 14,000 conversations



Help Net Security
August 24, 2016

Cybercriminals select insiders to attack telecom providers

Still relying on legacy antivirus? There's a smarter way to do endpoint security.

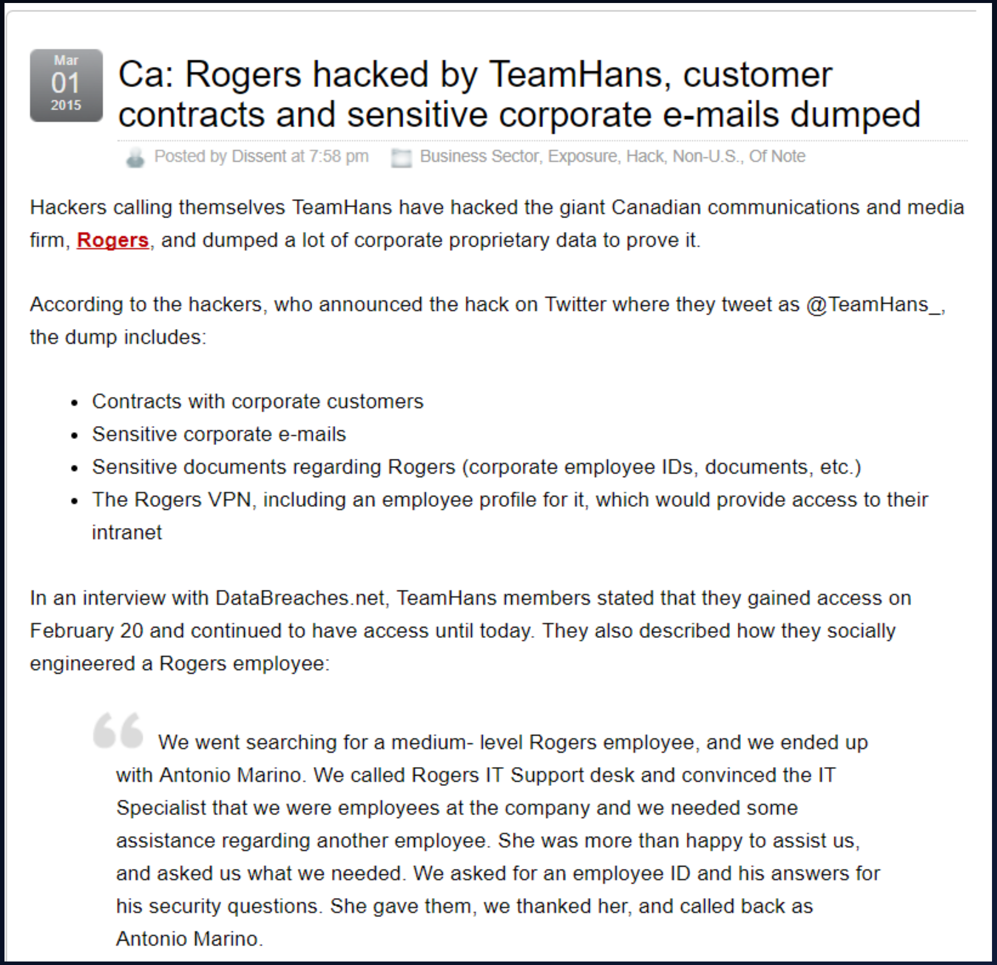
Cybercriminals are using insiders to gain access to telecommunications networks and subscriber data, according to Kaspersky Lab. In addition, these criminals are also recruiting disillusioned employees through underground channels and blackmailing staff using compromising information gathered from open sources.

Telecos’ Customers Cybersecurity Threats

- Social engineering, Phishing Etc
- Vulnerable Kit
- Local Cells and SIM Attacks

Social Engineering, Phishing of Telecos’ Customers

- Target unaware or poorly aware subscribers and telecoms employees.
- Lack of user awareness and egress protections.
- Poor password handling and storage discipline.
- Use of Ransomware
- Lack of two-factor authentication
- Lack of user permission segregation.



Mar 01 2015

Ca: Rogers hacked by TeamHans, customer contracts and sensitive corporate e-mails dumped

Posted by Dissent at 7:58 pm Business Sector, Exposure, Hack, Non-U.S., Of Note

Hackers calling themselves TeamHans have hacked the giant Canadian communications and media firm, **Rogers**, and dumped a lot of corporate proprietary data to prove it.

According to the hackers, who announced the hack on Twitter where they tweet as @TeamHans_, the dump includes:

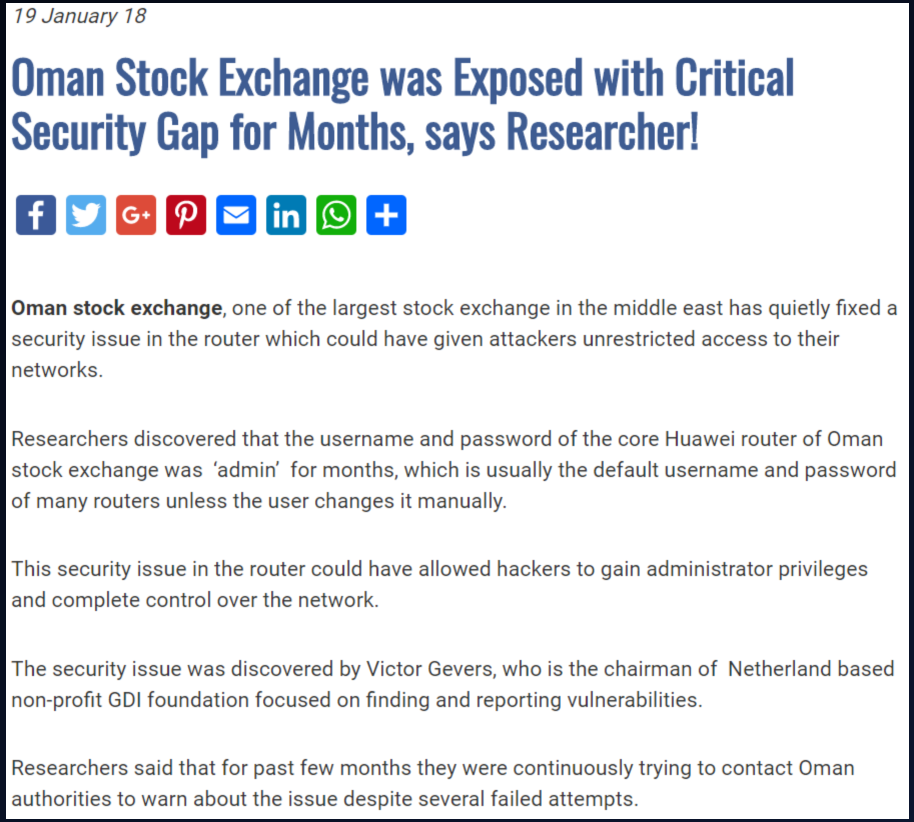
- Contracts with corporate customers
- Sensitive corporate e-mails
- Sensitive documents regarding Rogers (corporate employee IDs, documents, etc.)
- The Rogers VPN, including an employee profile for it, which would provide access to their intranet

In an interview with DataBreaches.net, TeamHans members stated that they gained access on February 20 and continued to have access until today. They also described how they socially engineered a Rogers employee:

> “ We went searching for a medium- level Rogers employee, and we ended up with Antonio Marino. We called Rogers IT Support desk and convinced the IT Specialist that we were employees at the company and we needed some assistance regarding another employee. She was more than happy to assist us, and asked us what we needed. We asked for an employee ID and his answers for his security questions. She gave them, we thanked her, and called back as Antonio Marino.

Vulnerable Kits Provided to Telecos' Customers

- Insufficient authentication
- Remote Code Execution from web scripts.
- Arbitrary device firmware modification due to insufficient consistency checks



19 January 18

Oman Stock Exchange was Exposed with Critical Security Gap for Months, says Researcher!

Oman stock exchange, one of the largest stock exchange in the middle east has quietly fixed a security issue in the router which could have given attackers unrestricted access to their networks.

Researchers discovered that the username and password of the core Huawei router of Oman stock exchange was 'admin' for months, which is usually the default username and password of many routers unless the user changes it manually.

This security issue in the router could have allowed hackers to gain administrator privileges and complete control over the network.

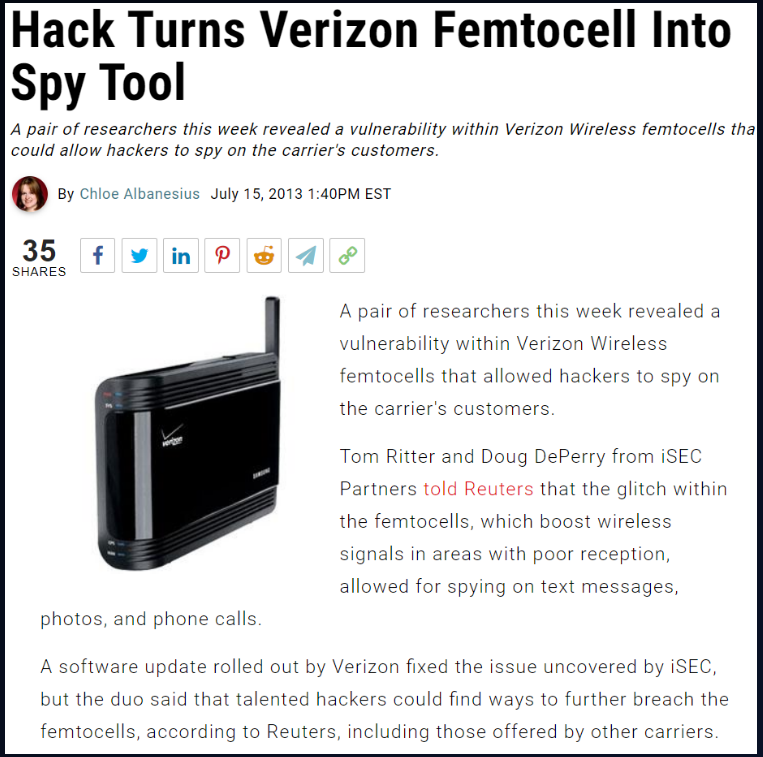
The security issue was discovered by Victor Gevers, who is the chairman of Netherland based non-profit GDI foundation focused on finding and reporting vulnerabilities.

Researchers said that for past few months they were continuously trying to contact Oman authorities to warn about the issue despite several failed attempts.

Local Cells and SIM Attacks

- Attacker can gain complete control over devices that signal coverage inside buildings.
  - Can lead to call interception, service abuse or internal network access.

- Clone SIM cards
  - Use differential power analysis for the encryption key and extracting secrets.
  - This was thought to be impossible



Hack Turns Verizon Femtocell Into Spy Tool

A pair of researchers this week revealed a vulnerability within Verizon Wireless femtocells tha could allow hackers to spy on the carrier's customers.

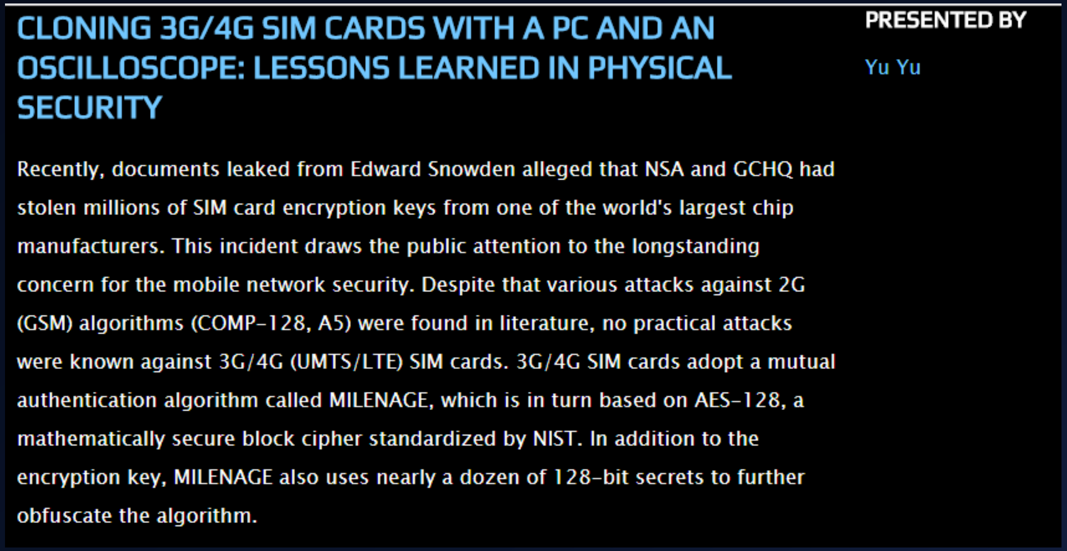
By Chloe Albanesius July 15, 2013 1:40PM EST

35 SHARES

A pair of researchers this week revealed a vulnerability within Verizon Wireless femtocells that allowed hackers to spy on the carrier's customers.

Tom Ritter and Doug DePerry from iSEC Partners told Reuters that the glitch within the femtocells, which boost wireless signals in areas with poor reception, allowed for spying on text messages, photos, and phone calls.

A software update rolled out by Verizon fixed the issue uncovered by iSEC, but the duo said that talented hackers could find ways to further breach the femtocells, according to Reuters, including those offered by other carriers.



CLONING 3G/4G SIM CARDS WITH A PC AND AN OSCILLOSCOPE: LESSONS LEARNED IN PHYSICAL SECURITY

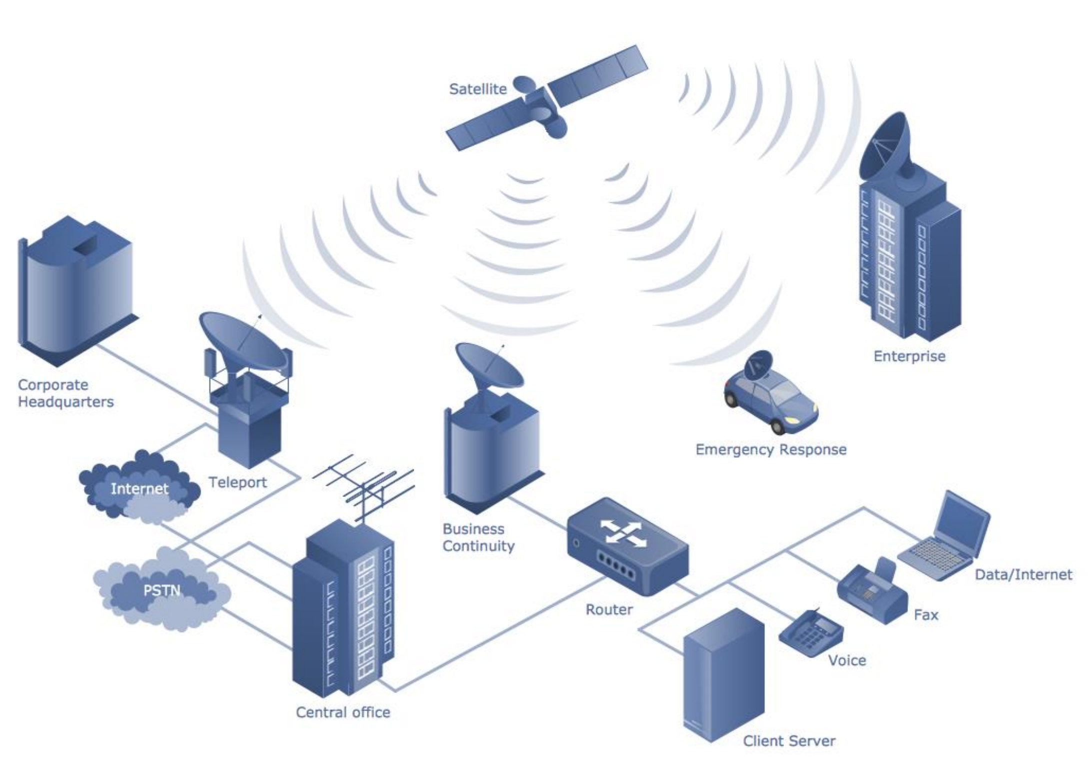
PRESENTED BY

Yu Yu

Recently, documents leaked from Edward Snowden alleged that NSA and GCHQ had stolen millions of SIM card encryption keys from one of the world's largest chip manufacturers. This incident draws the public attention to the longstanding concern for the mobile network security. Despite that various attacks against 2G (GSM) algorithms (COMP-128, A5) were found in literature, no practical attacks were known against 3G/4G (UMTS/LTE) SIM cards. 3G/4G SIM cards adopt a mutual authentication algorithm called MILENAGE, which is in turn based on AES-128, a mathematically secure block cipher standardized by NIST. In addition to the encryption key, MILENAGE also uses nearly a dozen of 128-bit secrets to further obfuscate the algorithm.

Recommendations – Secure Your Network

- Use Multi-Factor Authentication
- Use Strong Passwords
- Segment Your Network
- Audit Administrator Access
- Secure All Keys and Secrets
- Harden All Devices



Recommendations – Secure Your Applications

- Use recommended authentication mechanisms
- Do not trust user input and implement robust server side checks
- Ensure that applications continue to verify their assurance of a user's identity following authentication
- Using safe coding practices such as
  - Parameterized queries for database access
  - Use managed code for safe string handling
  - Pass an index to a list of files as a parameter, instead of an actual filename

Recommendations – Detect and Respond to Threats

- Implement threat detection and prevention tools
- Create and maintain an approved incident response plan
- Deploy reactive mechanisms to mitigate attacker’s progress
- Implement sufficient logging and auditing

Conclusions

- Security must be a core component of your entire enterprise
- Use both technical and non-technical solutions
- No quick-fix solutions will be completely effective
- Understand the changing threat landscape and react quickly

Questions and Answers

CONTACT INFO: JAVED.SAMUEL@GMAIL.COM