2026

CNI HACKING EFFORTS

Pax Consulting

17-08-2026

Index

1. PURPOSE

Files hacked[1] from the Italian company Hacking Team (HT) that suffered the attack in 2015 revealed many customers which were buying its products. A lot has been written about dubious customers, such as repressive regimes. Paxconsulting has decided to focus on a medium-size intelligence service such as the Spanish CNI.

The goal is to unveil the efforts that such a service, dealing with the national security of a regional power, the fourth economy of the EU, has been doing to collect the required data to fulfil its tasks.

Starting with the files provided by the hacked files, Paxconsulting has continued focusing on other software that have been used by the CNI. **Software provided by HT is important because it sets the basic line that the CNI has kept ever since, increasing eventually its gathering digital data capabilities.**

2. EXECUTIVE SUMMARY

The relationship between the CNI and HT is documented from at least June 2008 through October 2011, with administrative follow-up in February-March 2013. The record includes a formal Spanish procurement package, invoices, an internal order workbook, an accounts ledger, and bond correspondence.

The invoice ledger contains seven CNI entries categorized as offensive security, totalling €340,000. Four individually described invoices total €209,000; the remaining €131,000 is visible only at ledger level in the reviewed files.

The strongest access signal is the €72,000 2010 package: a one-year Zero-Day Exploit Portal (€48,000) plus five target modules for macOS and iOS (€24,000, including first-year maintenance). The €72,000 total matches invoice 129/2010 and its documents exactly.

The exploit portal was designed to build malicious PDF, DOC, and HTML-type files carrying the RCS agent; it provided social, public, private, and zero-day exploit categories and promised three working zero-days at any given time during the year.

Separate records show a €17,500 Remote Mobile Infection Module and €67,500 of technical maintenance and RCS mobile

[1] Downloadable at https://ddosecrets.org/article/hacking-team

licenses for Android, confirming sustained interest in remote access to mobile devices.

The signed capability annex shows the kinds of access available on the macOS and iPhone modules, but it is a feature matrix, not an operational log. It supports an inference about desired capability breadth; it does not establish that every function was selected or used.

3. FORMAL PROCUREMENT AND BUSINESS

Files show three procurement envelopes: general administrative documentation, the commercial offer, and specific technical documentation. It includes declarations on eligibility to contract, an electronic notification address, submission to Spanish courts, a signed commercial offer, a signed technical description, and a stamped four-page compatibility annex. That structure indicates Hacking Team formally responded to a CNI procurement process.

The commercial offer is dated 2 November 2010, identifies file 3010310046500, and commits Hacking Team to supply additional modules for RCS. Its two-line items total €72,000. Invoice 129/2010 dated 31 December 2010, bills CNI €72,000 for an RCS upgrade under the same file. The exact match in expedient and amount makes this the clearest purchase-to-invoice chain in the file set.

The historical ledger shows seven CNI entries from June 2008 to October 2011, **everyone categorized as *Sicurezza Offensiva* (offensive security). Their amounts come up to €340,000.** The ledger also records bank-transfer settlement amounts equal to the invoice values.

Date	Invoice	Amount	Description in record	Evidence
2008-06-30	**047/2008**	**€108,000**	**Offensive security; file 301038033800**	**Ledger only**
2010-02-25	**011/2010**	**€12,000**	**Offensive security**	Ledger only
2010-03-31	**021/2010**	**€11,000**	Offensive security	Ledger only
2010-12-31	**129/2010**	**€72,000**	**RCS upgrade; matches €48k exploit portal + €24k macOS/iOS modules**	**Direct match**

2010-12-31	**130/2010**	**€52,000**	**RCS upgrade; file 3010310060900**	**No feature detail**
2010-12-31	**140/2010**	**€17,500**	**Remote Mobile Infection Module**	**Direct invoice**
2011-10-12	**109/2011**	**€67,500**	**Technical maintenance and RCS mobile licenses for Android**	Direct invoice

An additional workbook planning row reads "CNI" and "€120,000, of which €40,000 maintenance," but it lacks an invoice number and date and appears alongside country/customer forecast entries. It is therefore not counted as a complete transaction.

Additionally, two HT faxes addressed to Centro Nacional de Inteligencia in February and March 2013 seek the return of original bonds and an expiry statement. They link three files to invoices 109/2011, 129/2010, and 130/2010. The second fax says CNI confirmed that it held the original bonds. This is evidence of ongoing contract administration, not a new 2013 purchase.

4. TYPE OF ACCESS IN CNI INTEREST

CNI's documented interest covered the full access chain: obtaining an initial foothold through exploits, extending the implant beyond Windows to macOS and iOS, and maintaining remote access to mobile targets, including Android. The attached feature grid shows a broad surveillance and control capability after infection.

- **Automatic payload delivery.** The portal created malformed versions of common files such as PDF, DOC, and HTML-type content with the RCS agent as the payload. Infection occurred when the target opened the file and triggered the relevant vulnerability.
- **A maintained exploit supply.** Operators accessed an exploit repository hosted on HT servers in Milan; the RCS console downloaded updated exploit lists and code. The contract covered social, public, private, and zero-day categories.
- **Reserved zero-day capacity.** HT promised three working zero days at any given time during the subscription year, replacing one when it became patched and was reclassified as private.

- **Platform reach.** The 2010 compatibility annex marks the Exploit Portal as available for Windows and macOS. It does not mark the portal as an iPhone infection vector.

The third line of the first paragraph is explicit: five target modules for two platforms, macOS and iOS, including first-year maintenance. The technical description says these modules were controlled through the same RCS console and compatible with the customer's existing RCS network infrastructure.

The wording “target modules different from Windows” strongly suggests **CNI already had or was extending a Windows-centred RCS capability.** That is a reasonable inference, but the precise original Windows/base-system purchase is not identified in the reviewed top-level files.

Invoice 140/2010 bills €17,500 for one Remote Mobile Infection Module, referencing an offer accepted on 30 December 2010. The line item is unambiguous about the desired access method but does not identify the mobile operating system or infection vector.

Invoice 109/2011 bills €67,500 for technical maintenance and RCS mobile licences for Android. An internal order workbook independently names CNI, identifies file 3010311028400, describes Remote Control System, and records the same €67,500 amount. Together they show a shift from the 2010 macOS/iOS expansion to maintained Android capability in 2011.

Invoice 130/2010 records a €52,000 RCS upgrade under file 3010310060900, and the 2013 bond correspondence confirms that contract's continued administrative existence. No reviewed top-level file itemizes the features in that upgrade, so assigning it to a specific access technique would be speculation.

5. MEANING OF THE 2010 CAPABILITY GRID

The compatibility grid was part of the signed/stamped technical annex for the same 2010 procurement. It therefore shows the capabilities CNI was invited to evaluate alongside the macOS/iOS modules. The checks below describe product availability in that annex; they are not evidence that CNI activated every feature.

5.1 macOS module:

- **Collection:** Skype/voice-call audio, camera images, chat sessions, clipboard content, keystrokes, organizer data, screen snapshots, and visited URLs.

- **Control:** synchronize collected data, start or stop the agent, execute arbitrary commands, and uninstall the backdoor.
- **Infection paths shown:** exploit portal; a legitimate executable combined with the backdoor; and bootable CD-ROM/offline media.

5.2 iOS module:

- **Collection:** keystrokes; email/SMS/MMS; microphone audio; organizer/address-book/task/calendar data; GPS or GSM-cell position; screenshots; and visited URLs.
- **Control:** synchronize data, start or stop the agent, send a covert SMS, and uninstall the backdoor.
- **Infection path shown in the 2010 grid:** manual jailbreak and file copying. The matrix does not mark the exploit portal or WAP Push for iPhone at that time.

5.3 Other systems:

- Documents list capabilities for Windows, Windows Mobile, Symbian, and BlackBerry. Those entries show the wider RCS product architecture, but the priced line item specifically names macOS and iOS. Likewise, the later RCS9 training manual and 2014 brochure describe a more mature Galileo platform, network-injection products, social-app monitoring, and intelligence correlation; neither later file names CNI. They are useful background, not proof of what CNI bought or used in 2010-2011.

6. ASSESSMENT OF THE RELATIONSHIP

The relationship appears to have evolved from an earlier offensive-security engagement into a formal RCS expansion and mobile-access program.

It started with a reliable remote delivery of the RCS implant through crafted documents/files and a maintained supply of exploits, including zero-days.

Eventually, the CNI sought for access beyond Windows, explicitly covering macOS and iOS and later Android. The CNI focused on communications, keystrokes, audio, location, screenshots, browsing, organizer data, and remote-control functions were supported by the target platform.

There was an operational continuity, including maintenance, updated exploit code, licences, and later contract/bond administration rather than a one-time product delivery.

What the files do not establish is equally important: they contain no CNI target list, named operation, infection log, collected evidence, operator activity, or proof that a particular exploit or sensor was deployed. The evidence supports procurement intent and capability access, not claims about actual surveillance operations.

Claim	Assessment	Basis
CNI was a repeat Hacking Team customer	High	Invoices, internal ledger, formal tender package, and later bond correspondence
CNI sought exploit-based remote entry	High	Signed €48k exploit-portal offer and technical description
CNI sought macOS and iOS endpoint coverage	High	Signed €24k line for five target modules across those two platforms
CNI sought mobile compromise and Android capability	High	Remote mobile infection invoice plus Android RCS maintenance/licensing invoice
Every feature in the compatibility grid was separately selected or used	Not established	The grid documents available functions, not CNI operational choices
The identities of CNI targets or actual deployments	Not established	No target names, case files, deployment logs, or collected evidence in reviewed top-level files

CNI was interested in remote, covert, cross-platform device access: first by expanding RCS through exploit-driven delivery and non-Windows modules, then by adding remote mobile infection and Android support. The surrounding documentation shows that the desired result was not merely network visibility; it was persistent endpoint-level collection and control. The reviewed files prove commercial and technical interest, but not how, where, or against whom CNI used the capability.

7. CARETO AND PEGASUS

HT tools were reinforced and replaced by Careto (malware) and later by NSO software Pegasus.

Careto (also known as "The Mask") is an advanced, highly sophisticated cyber-espionage malware active since at least 2007. It targets government institutions, embassies, and diplomatic offices globally to steal sensitive data like encryption and SSH keys, VPN configurations, and communication records.

Although the Spanish CNI has never publicly acknowledged responsibility for Careto, several indicators have been cited as suggestive of a possible connection. The **sophistication of the malware is consistent with capabilities normally associated with state-level actors.** In addition, **expressions embedded in the code appear to reflect usage specific to Spain[2] rather than Latin America,** while the **profile of some targets**—particularly Moroccan entities—corresponds to areas of strategic interest for Spain.

Initially exposed by Kaspersky Lab researchers in 2014, after which the operators quickly wiped their infrastructure. Cybersecurity analysts discovered that Careto resurfaced (2024) with new modular frameworks targeting entities in Latin America and Africa. **It happens that in 2023 the CNI was exposed using Pegasus (Catalangate) which might explain why the agency decided to resurface Careto (revamped) with new capabilities.**

Careto core capabilities:

- **Stealth infiltration:** Uses spear-phishing emails and exploits to gain initial access.
- **Data harvesting:** Intercepts network traffic, records keystrokes, and steals configuration files.
- **Deep persistence:** Employs advanced rootkits and bootkits to hide within infected operating systems

In 2015 the CNI started using Pegasus[3]. Its relationship with NSO had been developing since Careto was exposed.

About Pegasus there is a great piece of work at Forbidden Stories, which is focused on the use that Morocco has carried

---

[2] Careto is a slang word in Spain for ‘face’. But there are other examples embedded in the code.

[3] https://web.archive.org/web/20250115010831/https://elpais.com/espana/2022-04-20/el-cni-pidio-comprar-el-sistema-pegasus-para-espiar-en-el-extranjero.html

out of this NSO group software[4]. But this is a different story.

The use of Pegasus by the CNI is confirmed by the trips of NSO group employees to Spain in 2021, after the hacking of telephones of members of the Spanish cabinet —President Sánchez included— were hacked allegedly by Morocco in 2021[5].

In any case, **Careto and Pegasus represent an evolution of capabilities.** HT required an action by the user to be accessible but the new tools infected devices **with no need of user interaction.** In addition, **the new tools provided a deeper control over the device and apps installed in it.**

However, it should be noted that, in all cases, routine device updates frequently disrupted the normal operation of the malware.

According to the available evidence, the malware reportedly used by the CNI appears to have been exposed at intervals of approximately **seven to eight years, suggesting a recurring pattern in the lifecycle of covert malware operations.** Irrelevant if malware is self-produced or hired.

[4] https://forbiddenstories.org/projects_posts/pegasus-project-inside-moroccos-spying-machine/

[5] https://theobjective.com/espana/2026-02-13/empresa-israeli-pegasus-urgencia-pinchazo-pegasus/

8. ANNEX. BILLS

]HackingTeam[

HT S.r.l.
Sede legale e operativa: Via della Moscova,13 – 20121 Milano – Tel: +39.02.29.06.06.03
e-mail: info@hackingteam.it – web: http://www.hackingteam.it – Fax: +39.02.63118946
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

Spett.le

Centro National de Inteligencia
Arda Padre Huidobro, s/n
28023 Madrid - Spagna

Tax ID: S2830132C

Milano, 12th October 2011

Invoice n. 109/2011

Assistencia Tecnica de Mantenimento Y Lycencias de RCS MOVIL PARA Android

Euro 67.500,00

VAT does not apply due to Italian decree *ex art. 7, co. 4, lett. E), DPR 633/1972*

Total **Euro 67.500,00**

Payment Terms: 30 days from invoice date
By wire bank transfer to:
HT S.r.l. - MPS - Monte dei Paschi di Siena
IBAN: IT 69 L 01030 33760 000000002541
BIC Swift Code- PASCITMMXXX

]HackingTeam[

HT S.r.l.
Sede legale e operativa: Via della Moscova,13 – 20121 Milano – Tel: +39.02.29.06.06.03
e-mail: info@hackingteam.it – web: http://www.hackingteam.it – Fax: +39.02.63118946
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

Spett.le

Centro National de Inteligencia
Arda Padre Huidobro, s/n
28023 Madrid - Spagna

Milano, 31st December 2010

Invoice n. 129/2010

RCS Upgrade (Expediente n° 3010310046500)	**Euro**	**72.000,00**

Total	**Euro**	**72.000,00**

VAT does not apply due to Italian Decree ex art. 7, co. 4, lett. E) - DPR 633/1972

Payment Terms: Payment at invoice date

By wire bank transfer to:
HT S.r.l. - MPS - Monte dei Paschi di Siena
IBAN: IT 69 L 01030 33760 000000002541
BIC Swift Code- PASCITMMXXX

]HackingTeam[

HT S.r.l.
Sede legale e operativa: Via della Moscova,13 – 20121 Milano – Tel: +39.02.29.06.06.03
e-mail: info@hackingteam.it – web: http://www.hackingteam.it – Fax: +39.02.63118946
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

Spett.le

Centro National de Inteligencia
Arda Padre Huidobro, s/n
28023 Madrid - Spagna

Milano, 31st December 2010

Invoice n. 130/2010

RCS Upgrade (Expediente n° 3010310060900)	**Euro**	**52.000,00**

Total	**Euro**	**52.000,00**

VAT does not apply due to Italian Decree ex art. 7, co. 4, lett. E) - DPR 633/1972

Payment Terms: Payment at invoice date

By wire bank transfer to:
HT S.r.l. - MPS - Monte dei Paschi di Siena
IBAN: IT 69 L 01030 33760 000000002541
BIC Swift Code- PASCITMMXXX

]HackingTeam[

HT S.r.l.
Sede legale e operativa: Via della Moscova,13 – 20121 Milano – Tel: +39.02.29.06.06.03
e-mail: info@hackingteam.it – web: http://www.hackingteam.it – Fax: +39.02.63118946
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

Centro National de Inteligencia
Arda Padre Huidobro, s/n
28023 Madrid - Spagna

Milano, 31st December 2010

Invoice n. 140/2010

Ref. offer acceptance of December 30th, 2010

Nr. 1 Remote Mobile Infection Module	**Euro**	**17.500,00**

Total	**Euro**	**17.500,00**

VAT does not apply due to Italian Decree ex art. 7, co. 4, lett. E - DPR 633/1972

Payment Terms: 30 days from invoice date

By wire bank transfer to:
HT S.r.l. - MPS - Monte dei Paschi di Siena
IBAN: IT 69 L 01030 33760 000000002541
BIC Swift Code- PASCITMMXXX