

# PRESS REVIEW ARCHIVE

Digital Media Monitoring & Documentation Service

**Source URL:** <https://www.nuovavenezia.it/cronaca/mestrino-mette-in-guardia-sulla-sicurezza-informatica-apbz9i4x>

**Archived Date:** August 15, 2025 at 15:04

**Published:** December 27, 2013

**Document Type:** Web Page Archive

**Wayback Machine:** [https://web.archive.org/web/\\*/https://www.nuovavenezia.it/cronaca/mestrino-mette-in-guardia-sulla-sicurezza-informatica-apbz9i4x](https://web.archive.org/web/*/https://www.nuovavenezia.it/cronaca/mestrino-mette-in-guardia-sulla-sicurezza-informatica-apbz9i4x)

## Page Screenshot



The screenshot shows a news article on the website 'la Nuova Venezia e Mestre'. The article is titled 'Mestrino mette in guardia sulla sicurezza informatica' and is dated '27 dicembre 2013'. The author is 'Di Francesco Macaluso'. The article text mentions 'Gianluca Pericoli, insieme a un coetaneo veronese, ha creato un osservatorio Un "super computer" su 400 in Italia può essere esposto ad attacchi di hacker'. Below the text is a photograph of two men. To the right of the article is a 'LEGGI ANCHE' section with three related articles: 'Venezia, mense Caritas aperte a Ferragosto: «Non lasciamo solo nessuno»', 'San Donà, dorme ubriaco in auto: 36enne espulso dalla polizia locale', and 'Appartamenti saccheggiati a Mestre, i residenti: «Turni per vigilare»'. The website header includes navigation links for 'CRONACA', 'REGIONE', 'NORDEST', 'ITALIA', 'MONDO', 'CULTURA E SPETTACOLI', 'SPORT', and 'VIDEO LOCALI'. The top right corner has links for 'LEGGI IL QUOTIDIANO', 'ABBONATI', and 'ACCEDI'.

[Home](#) > [Cronaca](#)

## Mestrino mette in guardia sulla sicurezza informatica

Gianluca Pericoli, insieme a un coetaneo veronese, ha creato un osservatorio Un "super computer" su 400 in Italia può essere esposto ad attacchi di hacker

Di Francesco Macaluso

27 dicembre 2013

3' di lettura



**I** super computer automatizzati che gestiscono molti aspetti della nostra quotidianità rendendo sicura la società come noi la conosciamo non sono così inviolabili. Anzi, uno su 400 in Italia e uno su 330 in Svizzera, anche operativi nella produzione pubblica di energia e altri strategici per la sicurezza, sono facilmente rintracciabili in Internet e quindi potenzialmente esposti ad attacchi di hacker e terroristi, che li potrebbero raggiungere interrogando semplici motori di ricerca come Google e Shodan.

Si può leggere questo fra gli sconcertanti risultati emersi da un'approfondita ricerca pubblicata on line sul portale [www.scadaexposure.com](http://www.scadaexposure.com) dal mestrino Gianluca Pericoli e dal veronese Francesco Ongaro, due 28enni laureati in informatica che hanno creato il primo osservatorio permanente sul fenomeno, sponsorizzato da ISGroup srl, società di soluzioni di sicurezza informatica che si è guadagnata con questo studio le prime pagine dei giornali elvetic venendo contattata persino dal servizio nazionale di sicurezza informatica del Liechtenstein.

«I sistemi informatizzati di supervisione e controllo, denominati in gergo con l'acronimo "Scada" che abbrevia l'inglese supervisory control and data acquisition», spiegano i due informatici, «sono la componente intelligente che governa gran parte delle infrastrutture automatizzate pubbliche o private di grandi dimensioni. Noi li abbiamo mappati tutti e

abbiamo indicato quelli rintracciabili perché indicizzati nella rete pubblica».

Tali sistemi gestiscono ad esempio intere università, banche, catene produttive di enormi fabbriche, la produzione di energia delle centrali elettriche, sistemi antifurto di musei o di negozi di lusso, cancelli e sbarre di interi stadi di calcio. «I dati di questo studio condotto nel mese di novembre», continuano, «sono stati raccolti dall'Italia, anche se il focus del lavoro riguarda in particolare la nostra nazione e la vicina Svizzera, mediante un semplice pc portatile collegato al world wide web tramite una semplice connessione adsl. Non abbiamo violato alcun sistema e non ci siamo mai connessi direttamente a questi dispositivi pur avendoli rintracciati, ma sappiamo che sono esposti su Internet e addirittura indicizzati in database pubblici come Shodan e Google. Lo scopo della nostra ricerca è mettere in guardia i produttori internazionali di questi sistemi e i loro clienti, non solo privati ma soprattutto i governi, sugli enormi rischi che corrono a connettere on line con la rete internet pubblica gli Scada senza le adeguate misure di sicurezza. Negli ultimi anni infatti la realizzazione di questi sistemi da parte delle case produttrici internazionali si è basata sempre di più sulle tecnologie che si interfacciano con l'accesso da Internet. Ciò per l'esigenza dei tecnici che vi lavorano e vi eseguono costantemente la manutenzione di intervenire da remoto, quindi anche da chilometri di distanza dall'impianto tramite una semplice connessione internet, per risolvere eventuali anomalie. Questo ha portato però ad un pericoloso minor isolamento degli impianti verso il mondo esterno, esponendoli di fatto ad una serie di nuove minacce che vanno dai malware, software creati con il solo scopo di causare danni a pc o sistemi più complessi, fino a veri e propri attacchi informatici su larga scala che possono paralizzare intere città, annullare intere giornate di produzione di beni o energia, creare disagi di massa, con danni incalcolabili. Col nostro sistema di identificazione è addirittura possibile localizzare in rete in poche ore 509.199 dispositivi Scada in tutto il mondo: infatti effettuando una scansione casuale ad una velocità di 10 Ip per secondo, è possibile rintracciare on line un sistema Scada al minuto esposto ad attacchi. Del totale, 2742 sono collocati in Svizzera e 17074 in Italia che in tutto rappresentano il 3.9% dell'esposizione globale ai rischi. La Svizzera è proporzionalmente più esposta dell'Italia (+14.8%)».

Maggiori informazioni contattando l'email [info@scadaexposure.com](mailto:info@scadaexposure.com).

©RIPRODUZIONE RISERVATA

**ARGOMENTI:** SICUREZZA INFORMATICA INTERNET

*Riproduzione riservata © La Nuova Venezia*

**LEGGI ANCHE**

**Venezia, mense Caritas aperte a Ferragosto: «Non lasciamo solo nessuno»**



**San Donà, dorme ubriaco in auto: 36enne espulso dalla polizia locale**



**Appartamenti saccheggiati a Mestre, i residenti: «Turni per vigilare»**



---

## VIDEO

**Colta da un malore a pochi passi dal rifugio, cade e sbatte la testa sui sassi: donna ferita a Sappada**



**Aggressione a Venezia: borseggiatori in azione con spray al peperoncino. Il video**



**Trieste, che cosa è successo in via Revoltella: la lite e poi l'incendio, la videoricostituzione**



**Lo striscione della Uefa a inizio partita: "Basta uccisioni di bambini e civili"**



**La lunga onda del Cup ultras: 200 tifosi del Psg in corteo verso lo stadio Friuli**



**la Nuova**  
di Venezia e Mestre

**CONDIZIONI DI VENDITA**

**GERENZA**

**PRIVACY**

**WHISTLEBLOWING**

**Nord Est Multimedia S.p.a.**

Nord Est Multimedia S.p.a. - Sestiere Santa Croce 563, Venezia. Cap. Soc. i.v. Euro 1.432.522,00 C.F. 05412000266 e REA VE-454332

*I diritti delle immagini e dei testi sono riservati. È espressamente vietata la loro riproduzione con qualsiasi mezzo e l'adattamento totale o parziale.*

Per qualsiasi necessità o domanda, il nostro servizio clienti è a tua completa disposizione.

Puoi contattarci al numero **02 89362545** o scrivendo una mail a **servizioclienti@grupponem.it**.

**ilNordEst.**

**IL PICCOLO**

**CorriereAlpi**

**il mattino**  
di Padova

**la tribuna**  
di Treviso

**Messaggero**  
Veneto