



## CAT - Cracca Al Tesoro torna ad Orvieto

*Il 3 luglio a Orvieto si parlerà di sicurezza delle reti domestiche ed aziendali, protezione dei dati personali e violazione della privacy: i temi sui quali la manifestazione è impegnata in un'opera di sensibilizzazione dell'opinione pubblica*

Orvieto, 30 giugno 2010 – Torna ad Orvieto dopo il successo dell'edizione dello scorso anno e dopo l'esperienza a Milano in occasione del Security Summit, CAT, l'ormai noto hacking game cittadino che per la prima volta in Italia porta la tecnologia e l'informazione all'interno dei centri cittadini.

Il 3 luglio orvieto diventerà nuovamente la capitale dell'hacking e della sicurezza informatica ospitando hacker, esperti informatici, docenti universitari, esponenti delle istituzioni e curiosi per sfidarsi in uno dei contest più impegnativi e per discutere delle nuove frontiere della protezione dei propri dati personali e della propria privacy in rete.

La manifestazione quest'anno è organizzata in collaborazione con Orvieto LUG che ha garantito il supporto logistico e l'organizzazione sul territorio e con il già consolidato team di superesperti in sicurezza tecnologica (Cristiano Cafferata, Raoul Chiesa, Paolo Giardini, Alessio Pennasilico), consulenti di tutte le principali organizzazioni di lotta alla criminalità informatica nazionali ed internazionali che per la Summer Edition di CAT hanno preparato un percorso "ad ostacoli" che metterà in difficoltà anche i più preparati.

La giornata del 3 luglio vedrà al mattino una conferenza per discutere con **Andrea Violetti**, Presidente Nazionale di AIP-ITCS (la maggiore organizzazione nazionale di categoria per la professione informatica), **Angelo Iacubino**, Ingegnere Informatico dell'Università degli Studi dell'Insubria e **Corrado Giustozzi**, Docente di "Informatica forense" presso l'Università degli Studi dell'Aquila di violazione della privacy, tutela dei propri dati su Facebook, tecniche per reperire informazioni personali sulla rete e sicurezza delle applicazioni per iPhone e proseguirà nel primissimo pomeriggio con gli interventi di **Luisa Franchina** della Presidenza del Consiglio e di **Gianna Detoni**, Presidente di HI CARE Onlus che illustreranno ai presenti lo stato dell'arte delle infrastrutture critiche nel nostro paese e della gestione in caso di crisi degli asset aziendali.

A seguire il briefing per le squadre e l'avvio della competizione.

Le squadre, armate di un dispositivo portatile (notebook, netbook, palmare, smartfone, playstation, etc.), una connessione Internet wireless e molta, molta intelligenza, tenacia, pazienza e competenza tecnologica dovranno "craccare", cioè violare, le barriere di sicurezza che il tema tecnico ha creato attorno ad una serie di "access point" strategicamente disposti all'interno della città di Orvieto.

I bersagli che le squadre dovranno violare sono basati su apparati di utilizzo comune, configurati di proposito in modo non sicuro, ricalcando le problematiche più comunemente presenti nelle infrastrutture aziendali e nelle implementazioni domestiche.

Lo scopo del gioco è, infatti, mettere in luce come una non corretta configurazione della propria rete possa inevitabilmente condurre a facili intrusioni da parte di qualsiasi appassionato di sicurezza informatica.

Solo superando tutte le prove sarà possibile accedere alle informazioni che porteranno alla tappa successiva. Un percorso "ad ostacoli" di sempre maggior complessità ed articolazione, con qualche nota scherzosa che permetterà alle squadre di accumulare punti extra, che permetterà agli "ethical hackers" di giungere, alla fine del percorso, ad individuare la sfida finale, il Tesoro, che dà titolo alla gara.

Lo scorso anno la manifestazione ha prodotto un incremento del XX% (Emanuele ha il dato) degli apparati domestici configurati in modo corretto ad Orvieto, garantendo così una maggiore sicurezza non solo per i proprietari di quegli apparati, ma di tutto l'ecosistema Internet.

Il team tecnico controllerà il corretto svolgimento della gara e sarà in contatto costante con tutte le squadre dalla "situation-room", un centro di controllo superprotetto, dalla quale si potrà assistere in diretta allo svolgimento del contest con il commento degli esperti.

Con il patrocinio:





Così gli sfidanti dovranno dare prova di intelligenza intuitiva per individuare gli “access point”, capacità tecniche per violarne le protezioni, senso di squadra per organizzare un lavoro di équipe. E naturalmente senso goliardico per cogliere lo spirito di divertimento dell’iniziativa, serissima dal punto di vista dei contenuti, delle “regole di ingaggio” e delle difficoltà tecniche, ma allegra e giovanile nel suo modo di manifestarsi e di svolgersi.

Rispetto della privacy, delle tecnologie della città di Orvieto, nessuna invasione delle strutture esistenti, né pericoli tecnologici di alcun genere per i cittadini e le strutture che ospitano gli access point sono le regole di base che, come sempre, saranno condivise dai partecipanti.

La manifestazione ha ottenuto il patrocinio di Regione Umbria, Provincia di Terni, Comune di Orvieto, Co.Re.Com Umbria, Consorzio SIR Umbria, Agenzia Regionale di promozione turistica dell’Umbria, AIP-ITCS Associazione Informatici Professionisti - Italian Computer Society, Clusit, OPSI - Osservatorio per la Privacy e Sicurezza Informatica, Centro Studi Orvieto, Orvieto Linux User Group, Backtrack Italia, Accademia del Levante e ICT Academy.

“Siamo molto orgogliosi di aver ottenuto un così grande sostegno da parte delle istituzioni e di associazioni nazionali che operano in ambito informatico e della sicurezza come i numerosi patrocini dimostrano “ha dichiarato l’organizzazione di CAT. “Internet oggi è una grande risorsa per fare business, per informarsi, per ma troppo spesso le persone sottovalutano i rischi connessi ad un suo utilizzo improprio: furto d’identità, violazione della privacy, phishing, uso improprio dei propri dati, etc. Ecco perché è nato CAT: un modo divertente e innovativo per informare su tali rischi l’opinione pubblica e dare indicazioni su come poter utilizzare appieno il web in tutta sicurezza”.

La sfida è come sempre all’ultimo byte per dimostrare la propria competenza tecnica, il proprio ingegno e la capacità di poter competere con i migliori esperti sul mercato...e magari anche batterli aggiudicandosi i premi, tecnologici, messi a disposizione dagli sponsor.

Sostengono la manifestazione: @Mediaservice.net, Alba S.T., Norton from Symantec, Sonicwall, Studio Giardini @Solution.it, Apogeeonline, PDCA, Seeweb, Ithum

Organizzazione CAT: **Cristiano Cafferata**-BDM & System Engineer SonicWALL Italia; **Raoul Chiesa**-Senior Advisor, Strategic Alliances & Cybercrime Issues @UNICRI, Permanent Stakeholders Group Member @ENISA, Board of Directors @CLUSIT, Founder, Strategic Alliances on e-Crime @Mediaservice.net Srl; **Stefania Coltro**-Practice leader D’Antona&Partners, Strategic Communication Consultant, **Diego Frascati** – Presidente Orvieto Linux User Group; **Emanuele Gentili**-Backtrack Italia e Tiger Security; **Paolo Giardini**-Direttore OPSI, Comitato Esecutivo Centro di Competenza per l’Open Source della Regione Umbria, Staff Nazionale Backtrack Italia, Vice Presidente GNU/LUG Perugia; **Alessio Pennasilico**-Security Evangelist, CEO & Partner Alba S.T. s.r.l. - AIS Group, Board of Directors and Technical Committee CLUSIT, Board of Directors AIPSI, Board of Directors ILS, Executive Committee OPSI;

Per ulteriori informazioni: <http://www.wardriving.it> – Stefania Coltro [s.coltro@gmail.com](mailto:s.coltro@gmail.com) ; 349-6108183



Con il patrocinio:

