Ufficio Stampa della Provincia autonoma di Trento
Piazza Dante 15, 38122 Trento
Tel. 0461 494614 - Fax 0461 494615
uff.stampa@provincia.tn.it

COMUNICATO n. 2654 del 13/12/2016

Scoperta di una "falla" nei servizi online di Microsoft. Al ricercatore FBK un premio per il suo contributo alla sicurezza dei servizi online

In collaborazione con Nicolas Dolgin (stagista di SAP, Francia), Avinash ha recentemente scoperto una seria vulnerabilità nei servizi online di Microsoft che consente ai malintenzionati di venire in possesso di dati sensibili di altri utenti a loro sua insaputa.

Le conseguenze della "falla" scoperta dai ricercatori possono essere serie. Tra queste, l'utente malintenzionato può monitorare l'attività e le pagine che visita la vittima, acquisendo così dati sensibili. Questo non solo porta alla violazione della privacy, ma può consentire l'utilizzo dei dati raccolti per scopi fraudolenti (furto di identità, perdita di coordinate bancarie e di altre informazioni riservate). E ancora, il malintenzionato può ingannare la vittima utilizzando indebitamente la sua carta di credito, pagando per esempio servizi di cui non usufruisce, come la ricarica del credito Skype dell'utente malintenzionato.

La scoperta rientra nei criteri per il programma "Online Services Bounty" di Microsoft grazie a cui Avinash e Nicolas riceveranno un premio di 1.500 dollari. Il "Microsoft Security Response Center " fornisce infatti un riconoscimento in denaro e una menzione sul loro sito web ai ricercatori che contribuiscono a rendere più sicuri i servizi online.

Lo studio è stato condotto nell'ambito del progetto europeo "Security and Trust of Next Generation Enterprise Information Systems" (SECENTIS), a cui partecipano la Fondazione Bruno Kessler e SAP Labs in Francia. Si tratta di un dottorato industriale europeo, totalmente finanziato dalla comunità europea, che ha lo scopo di formare una nuova generazione di esperti di sicurezza, capaci di affrontare le sfide sia scientifiche che tecniche poste dalle tecnologie emergenti ed il loro conseguente impatto nelle aziende.

Avinash , insieme ad altri quattro studenti di dottorato, è stato selezionato nel 2013 nell'ambito del progetto SECENTIS . Il loro compito è di sviluppare tecniche di analisi di sicurezza e testing di protocolli *browser-based* che possano supportare gli sviluppatori, contribuendo ad individuare vulnerabilità nei sistemi.

Supervisionano il lavoro di Avinash i ricercatori Roberto Carbone, Luca Compagna, del SAP Labs Francia e il coordinatore del progetto SECENTIS , Alessandro Armando (responsabile in Fondazione Bruno Kessler dell'unità "Security and Trust").

Il filone di ricerca sviluppato da Avinash nell'ambito del progetto SECENTIS sta contribuendo a migliorare la sicurezza delle applicazioni web di grande popolarità. Durante la sua attività, Avinash ha scoperto serie vulnerabilità, simili a quella scoperta in Microsoft, in servizi forniti da Google, eBay e SAP [2]. Avinash ha inoltre condotto una analisi della sicurezza di siti web che usano soluzioni di *single sign-on* (SSO) forniti da importanti aziende quali PayPal, LinkedIn, Facebook e Instagram e reso evidenti dei "bachi" nell'accesso SSO di PayPal e nei siti web più popolari (quali LinkedIn, Pinterest [3]).

Il contributo di Avinash è stato pubblicamente riconosciuto da Yahoo (nella propria Security Wall of Fame) [1], oltre che da Pinterest [3] e SAP [2].

Avinash terminerà il suo PHD il prossimo anno e, grazie alle ricerche sviluppate in FBK, sta attualmente collaborando con il Cyber Security Innovation Lab (Poste italiane) in FBK e applicando per posizioni all'estero.

> Informazioni utili:

- **SECENTIS Project** : http://www.secentis.eu/

- **Microsoft Online Services Bug Bounty Terms**: https://technet.microsoft.com/en-us/security/dn800983

> Informazioni su Avinash Sudhodanan/SECENTIS:

[1] Yahoo: https://web.archive.org/web/20160122082559/http://bugbounty.yahoo.com/se...

[2] SAP: https://open.sap.com/pages/about

[3] Pinterest: https://web.archive.org/web/20160423020222/https://about.pinterest.com/e...

()