G Data press release 2013

Explozia de la Boston, exploatata de spameri

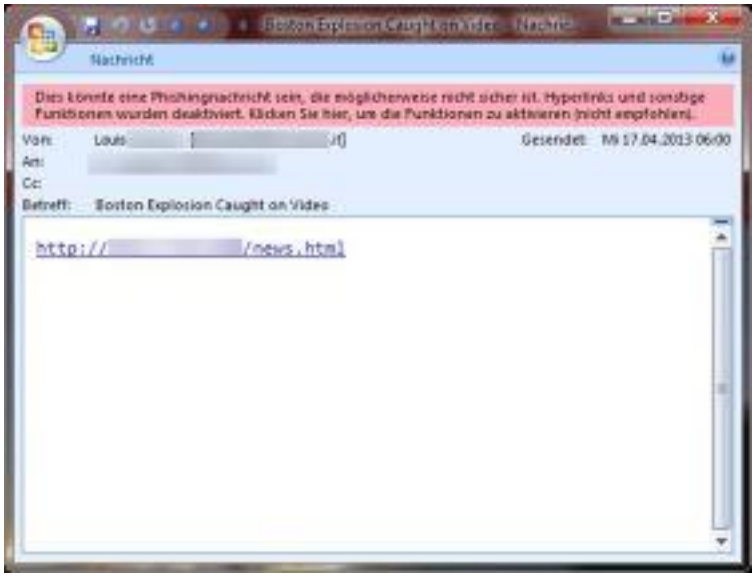
G Data a observat un urias val de spam ce ademeneste destinatarii pe site-uri infectate

Bucuresti (Romania) 19.04.2013 - In timp ce exploziile devastatoare de la maratonul din Boston au creat groaza si durere, infractorii cibernetici au profitat de pe urma atacurilor pentru a lansa un val imens de spam. G Data Security Labs observa o crestere masiva a email-urilor ce includ link-uri cu videoclipuri cu inregistrari ale expoziilor. Acestea blocheaza computerele infectate si ii santajeaza pe utilizatori cu plata unei "rascumparari". Computerele infectate sunt exploatate si pentru a distribui spam. In cea de-a doua varianta, parolele sunt sustrase si intreg traficul din retea este interceptat pentru a-i spiona pe utilizatori. G Data ii sfatuieste pe cei care receptioneaza acest gen de mesaje sa le stearga inainte de a le citi si sa nu accesezel-ink-urile, sub nicio forma.

Multe persoane folosesc Internetul ca prima optiune pentru a se informa, iar videoclipurile sunt, de regula, foarte populare printre utilizatori. In cazul in care destinatarul unui email, acceseaza link-ul continut de email, va fi directionat pe un site amorsat ce contine o fereastra cu cinci videoclipuri YouTube diferite. Doar ca, in afara celor cinci filmulete, atacatorii au integrat un Java applet in website ce a fost incarcat pentru a eploata o vulnerabilitate Java. In cazul in care varianta de Java instalata pe computer este mai veche decat versiunea 7 actualizarea 11, malware-ul de pe mail este instalat pe computer cu ajutorul unui exploit, iar PC-ul infectat este exploatat pentru a trimite email-uri in masa.

In cea de-a doua varaianta, atacatorii sustrag parolele salvate in browsere precum Firefox, parole folosite pentru conturi de magazine online, casute de email sau retele sociale si citesc tot traficul necriptat din retea. Aceasta ii ajuta pe acestia sa-i spioneze indeaproape pe utilizatori.

Imagine a spamului cu presupusul videoclip cu exploziile de la Boston:



G Data ii sfatuieste pe cei care receptioneaza spam-urile:

- Sa le stearga fara sa le deschida: Email-urile suspecte a fi spam-uri ar trebui sa fie sterse fara a fi citite. Atasamentele sau link-urile nu vor fi deschise sau accesate din motive de securitate.
- Sa isi instaleze solutii software de securitate antivirus: Utilizatorii ar trebui sa foloseasca o solutie de securitate eficienta care sa includa protectie antivirus, filtru antispam, filtru HTTP si protectie in timp real.
- Sa instaleze in mod regulat update-uri: Utilizatorii vor instala intotdeauna patch-urile si update-urile sistemelor de operare instalate pentru a pastra permanent computerele complet actualizate.

-###-