Aktuální hrozby na internetu
AVG Web Threat Research Team
19. 4. 2013

1. Spam využívá krutého bostonského maratonu a láká uživatele na nakažené stránky

Pravděpodobně si myslíte, že pachatel, nebo pachatelé zodpovědní za bombové útoky na bostonském maratonu, jsou přinejmenším bezcitní a měli by být potrestáni.

Seznamte se s jejich přívrženci – podvodníkům se přes noc podařilo vytvořit spam s malwarem a masivně jej rozšířit.

Členové AVG Web Threats Research týmu objevili spamové emaily, ve kterých byly exploze na bostonském maratonu využity jako lákadlo pro potenciální oběti malwarů a exploitů.

Tyto spamové emaily mají velmi jednoduchý předmět, jako např.:

- „Exploze na bostonském maratonu“
- „Běžci dopadeni. Maratonská exploze“
- „AKTUÁLNĚ – Exploze na bostonském maratonu“
- „Následky exploze na bostonském maratonu“
- „2 exploze na bostonském maratonu“

a jsou tvořeny numerickým URL s koncovkou “/boston.html” or “/news.html:

Mohou se objevit také jiné verze URL odkazů, se kterými jsme se zatím nesetkali, nebo se může stát, že koncovka tohoto podvodného odkazu přemění formát URL, jakmile je spam spuštěn. Nemyslete si tedy, že email o bombových útocích na bostonském maratonu s jiným URL, který jste možná obdrželi, musí být bezpečný.

Kliknutí na odkaz v emailu přesměruje potenciální oběti na tuto stránku:

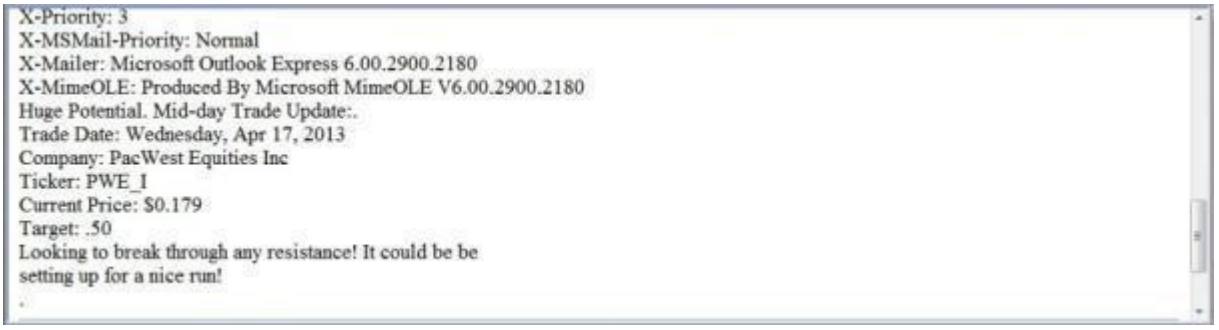
“Horké novinky: Videa exploze na bostonském maratonu 2013”

Stránka obsahuje toto:

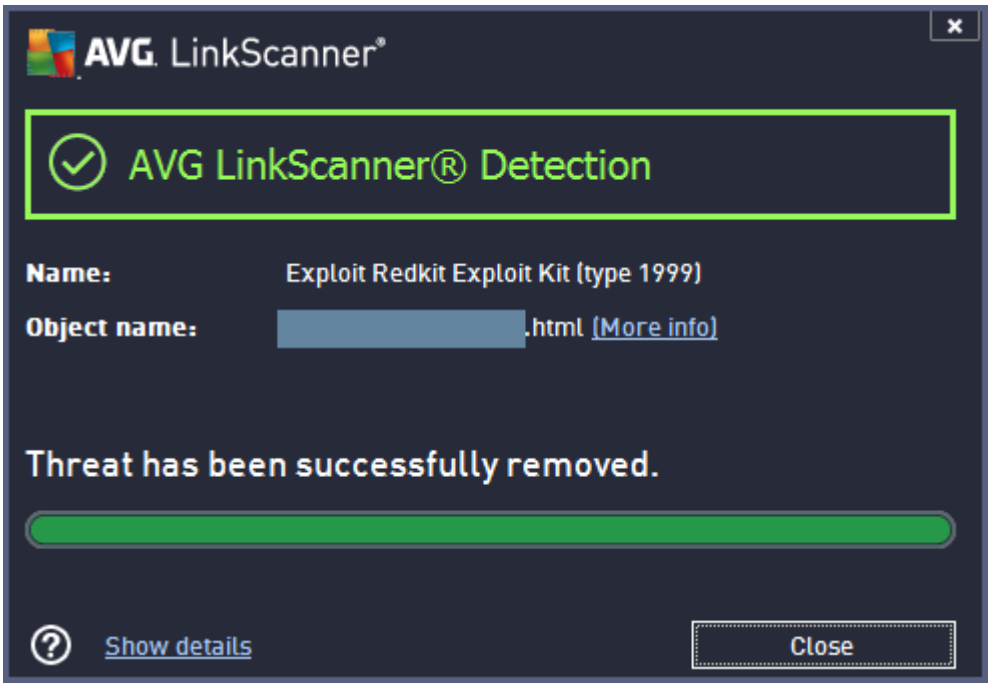
1. Automatické stažení škodlivého spouštěče, který je aktuálně nazván jako “boston.avi_____.exe”. Ale i tento název se může lišit.
2. Čtyři odkazy na videa explozí z bostonského maratonu na Youtube
3. Iframe, který uživatele přesměruje na stránku s Redkit Exploit Kitem

Podle konfigurace vašeho webového prohlížeče může být stažený materiál automaticky uložen do vaší složky „stažené soubory“, nebo může spustit zobrazení dialogového okna s žádostí o potvrzení uložení souboru “Boston.avi exe”.

Spuštění tohoto programu ale rozhodně není dobrý nápad. Zatímco probíhá vstupní analýza tohoto podvodného souboru, začne trojský kůň ihned po jeho spuštění rozesílat spamy. I virový skener měl problém s rozpoznáním tohoto Trojana.



Na štěstí pro ty, kdo používají bezpečnostní produkty AVG, rozpozná LinkScanner stránky s Redkit Exploit Kitem v iframu a upozorní je, aby program nespouštěli.



Dejte na tyto rady a vyhněte se tak stažení a rozšíření malwaru.

Aktuálně:

Členové AVG Web Threats Research týmu objevili další pokus kyberzločinců o nalákání obětí na malware a exploity. Útoky, které jsme nashromáždili, ale nejsou zatím povedené: obrázky jsou nefunkční, text je neupravený a hypertextové odkazy také nefungují. Přesto ale představují nebezpečí, protože dávají uživatelům, kteří na link najedou ukazatelem myši, dostatek informací k tomu, aby zadali do svého prohlížeče URL a byli tak infikováni. Pokud navíc podvodníci zaznamenají svou chybu, snaží se ji opravit v naději, že napálí další oběti.

Nejnovější spamový email měl v předmětu toto:

“Předmět: [SPAM] Názor: Exploze na bostonském maratonu mají na svědomí radikální gayové? Opravdu? – CNN.com”

Powered by ?

?* Please note, the sender's email address has not been verified.

You have received the following link from BreakingNews@mail.com.com: ?

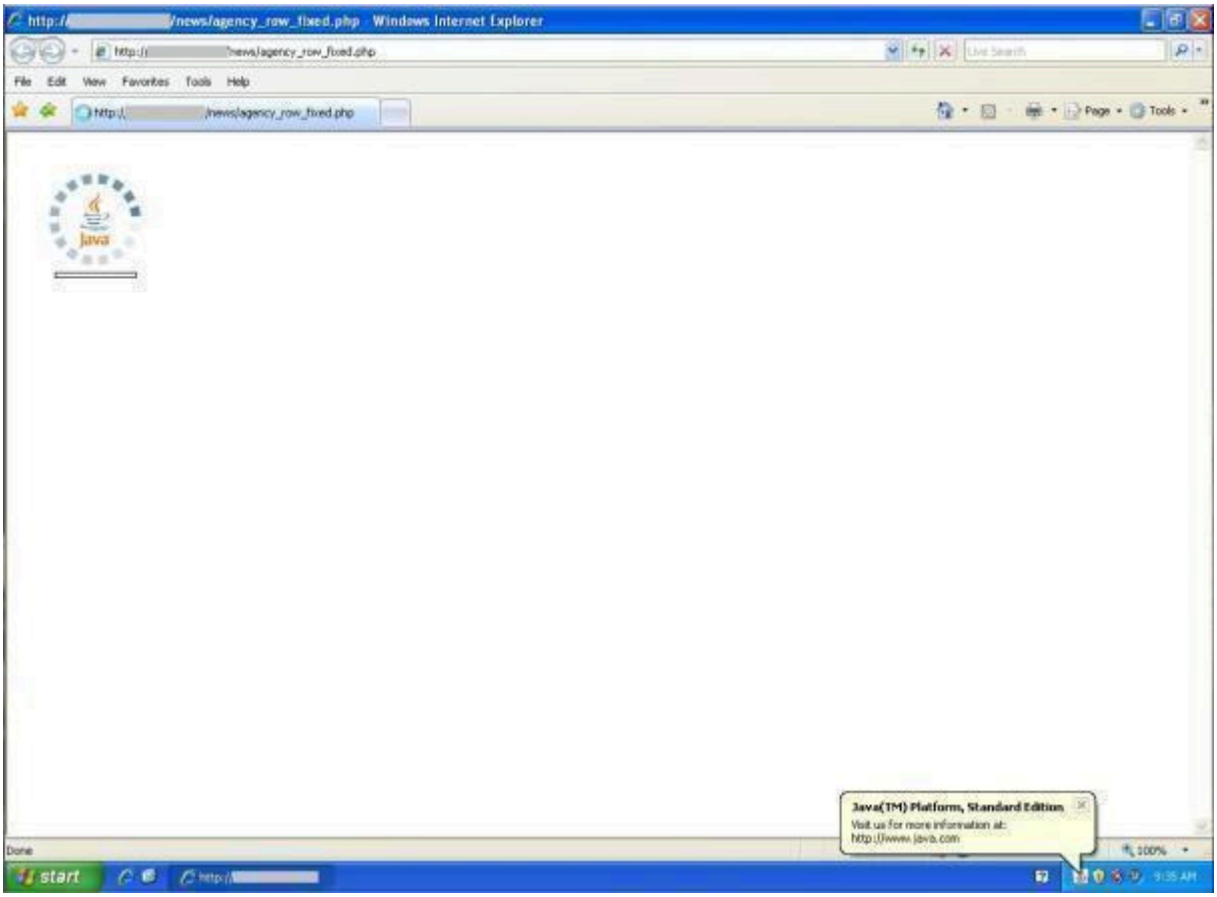
Click the following to access the sent link:

Boston Marathon Explosions made by radical Guys? Really? - CNN.com*

Get your EMAIL THIS Browser Button and use it to email content from any Web site. Click here for more information.

*This article can also be accessed if you copy and paste the entire address below into your web browser.

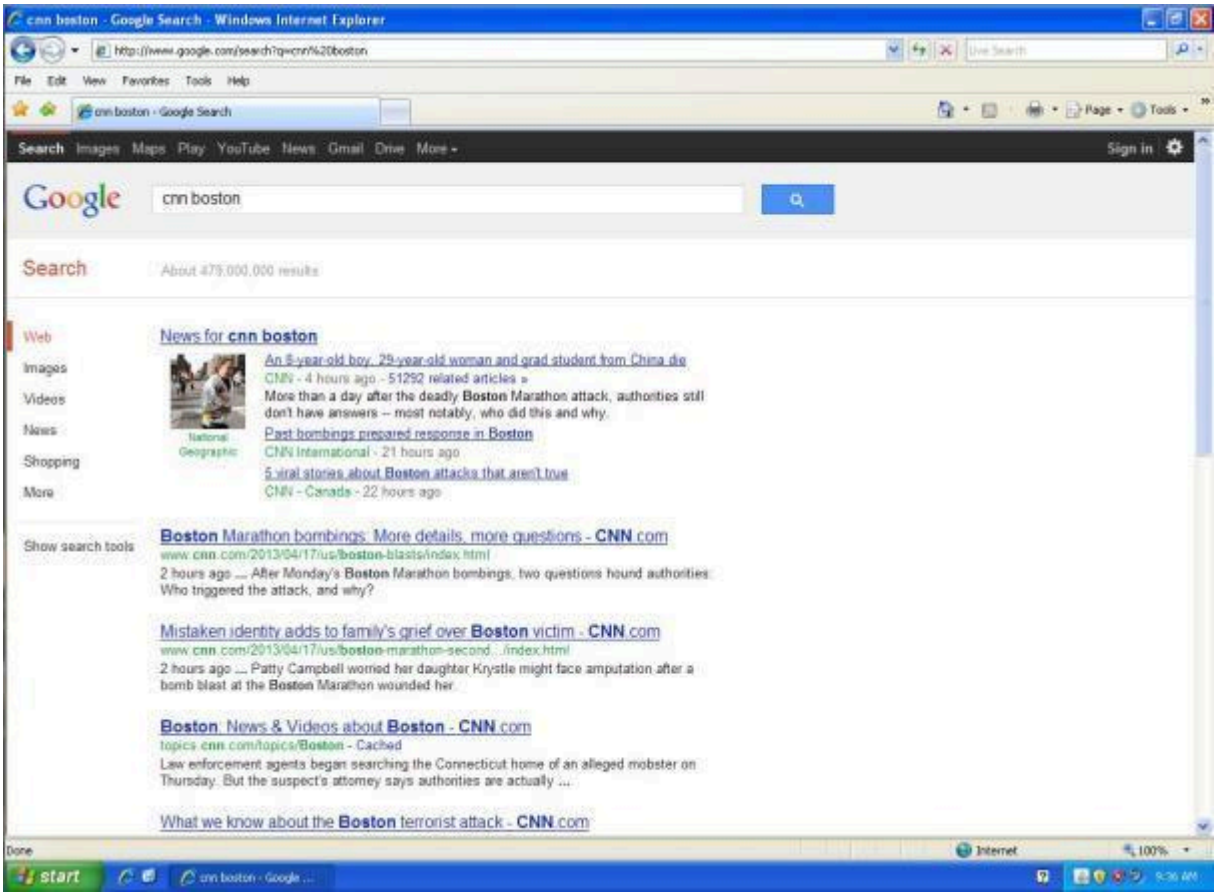
Pokud jsou hypertextové odkazy funkční, nebo pokud se podvodníkům podaří chyby ve spamech opravit, je uživatel přesměrován na stránky, které AVG LinkScanner detekuje jako Blackhole exploit kit. Exploit kit stáhne trojského koně, který může být použit ke vzdálenému přístupu, zamítnutí služeb, nebo k rozšíření útoků způsobujících zamítnutí služeb. Může také rozeslat spam, nebo získat informace z uživatelova počítače.



..

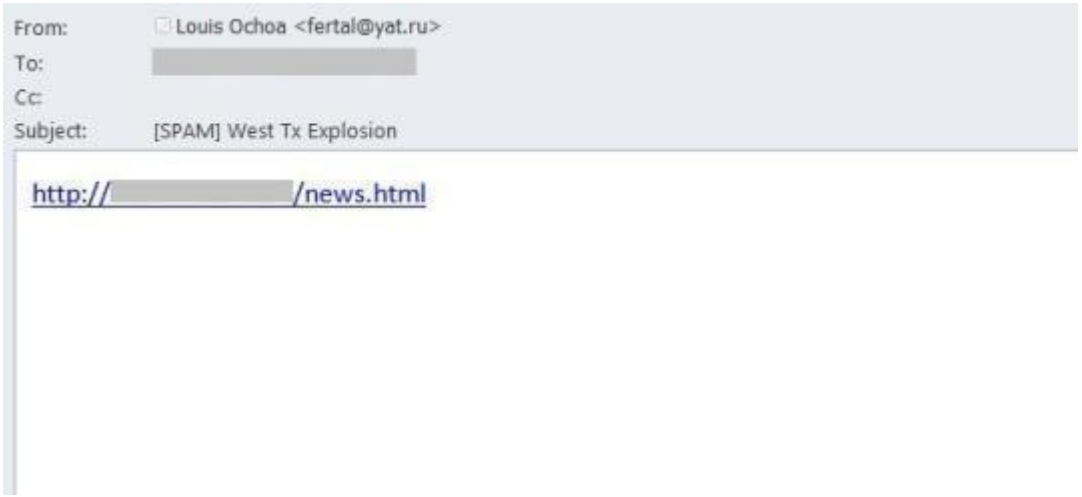
Když se škodlivým stránkám podaří získat to, co chtěly, je uživatel přesměrován na (neinfikovaný)

Google s výsledky vyhledávání pro „CNN Boston“.



2. **Pozor na spammery využívající také exploze v Texasu!**

Kyberzločinci se také aktuálně snaží profitovat z exploze v továrně na hnojiva poblíž města Waco v Texasu.



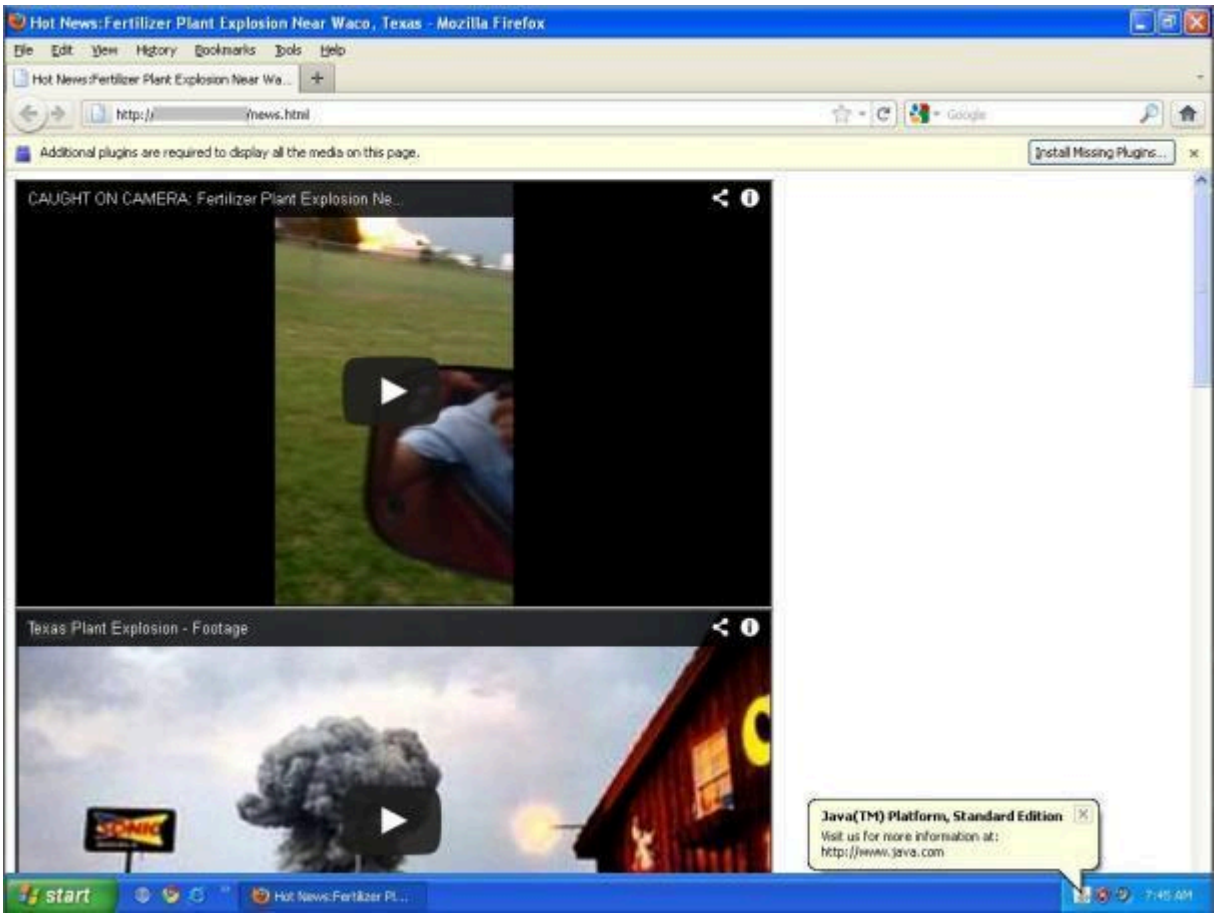
Předměty nových spamových emailů vypadají takto:

- Exploze v texaském Westu
- Exploze ve Waco HD
- ZACHYCENO NA KAMEŘE: Exploze v továrně na hnojiva poblíž města Waco v Texasu

Formát URL nejnovějšího spamu je podobný tomu, který byl použit u spamu s bostonským maratonem:

hxxp://XXX.XXX.XXX.XXX/news.html
hxxp://XXX.XXX.XXX.XXX/texas.html

Domény obsažené v URL jsou tvořeny numerickou IP adresou a stránka má název: „Horké novinky: Exploze v továrně na hnojiva poblíž města Waco v Texasu“.



I tyto nakažené stránky dokáže AVG LinkScanner spolehlivě odhalit.

- AVG Web Threats Research Team & Virová laboratoř AVG