

Forum:[Hack Forums](#)

Thread: [Black Mole - Private and Public Key Hunter](#)

boombunny - September 27, 2013, 1:17 am

Hey guys, a friend of mine wanted me to show him how easy it was to steal private/public key rings from computers, as I have no interest in industrial espionage and basically no use for this code I am giving it away.

With all the NSA spying lately people believe that the NSA can break ALL encryption..... They couldn't be more wrong, while some weaker encryption has been broken, methods using larger keys remain safe.... for now.

How does NSA break these encryption methods?... simple, they attack the weakest point.... Us.

Because we can't remember these complex keys we all store our Public and Private keys on our computers and other storage medium, this is the weak point.

Now the key rings are encrypted right? Well if you combine this with a keylogger then you will eventually get the passphrase used to open these key rings.

Here is a proof of concept, it is a VERY SIMPLE class that when started it will look for exported keys and public/private key rings and when it finds them it will send them to your mailbox.

It works by looking for files with known extensions, when found it will read the text looking for the PGP header or it will read the first two bytes to make sure the files are actually what we want, if the file is less than 9mb it will email it to us.

It will also send us the Username and Domain name for environments such as corporate domains and forests.

To use it just declare a new class and run it calling .Start()

Enjoy.

PS: I am usually drunk while coding so if you don't like how I code things then let me know in a civilized way.

Spoiler ([Click to View](#))

FaTaL_ErRoR - September 27, 2013, 10:37 am

Yes i know a more civilized way - c#

OperationFatSarah - September 27, 2013, 10:52 am

(Sep 27, 2013 10:37 AM)? ~ F?TâL?Er?o? ~ ? Wrote: [\[CITE\]](#) Yes i know a more civilized way - c#
LOL ?

@OP: Though this is proof of concept, I'd recommend using php to grab the data rather than using SMTP to send it.

Tastylicious - September 27, 2013, 12:56 pm

(Sep 27, 2013 10:37 AM)? ~ F?TâL?Er?o? ~ ? Wrote: [\[CITE\]](#) Yes i know a more civilized way - c#
Yeah sure... You know what shit's about ?

boombunny - September 28, 2013, 2:54 am

(Sep 27, 2013 10:52 AM)OperationFatSarah Wrote: [\[CITE\]](#) @OP: Though this is proof of concept, I'd recommend using php to grab the data rather than using SMTP to send it.

Not a bad idea, I just liked the disposable nature of email accounts but you are right, adding the php upload would be easy enough.