

Forum:[Hack Forums](#)

Thread: [Operational Security for Liars, Cheats, and Other Proud Deviants](#)

Nakamoto - October 8, 2014, 1:40 am

I talk a lot about the technological aspects of remaining anonymous and keeping your data private, but oddly enough many of the problems we face when it comes to doing exactly that are non-technical in nature. Simply put, most of us say far too much.

Today I'm going to be covering Operational Security (OPSEC) and why it is absolutely crucial. The goal here is to show you guys why you need to actually take this seriously while also keeping this easy to read and understand so that it can be picked up by just about anyone.

I will be dividing this post up into three sections and each of these sections will have detailed explanations followed by scenarios designed to further your understanding of the subject matter. So, without further ado, let's begin.

Section One - Well, what is it?

Paranoia does not work retroactively.

Operational security can be defined as a process by which you identify critical data, analyze (and define) friendly actions, and eliminate or minimize to an acceptable state vulnerabilities in your system that would allow an adversary to access critical data. To break that down (Jargon incoming):

- a) Identify the actions and information that can be observed by an adversary
- b) Determine what information can be used by an adversary to piece together more information
- c) Determine and properly execute specific actions that must be taken in order to eliminate or minimize to an acceptable state the likelihood of an adversary obtaining critical information on your operation.

Translation time (because not everyone understands intelligence/military jargon):

- a) What information can be gathered on you already?
- b) Which pieces of that information can be used in conjunction with other pieces to determine patterns, preferred procedures, and other pieces of critical operational information?
- c) What can you do to make sure they cannot or it be incredibly hard to obtain critical operational information?

Here's a scenario now. I said I wanted to keep this as easy to understand as possible, so I'll keep it simple.

Bob is a freedom fighter. Bob comes home from his menial office job every day at around 5:30 PM and hops on IRC as soon as possible (typically within 30 minutes of being home). To protect himself, Bob uses Tor to connect to the IRC network, however Bob often complains about his job and the weather in his area being so shitty all of the time. Sometimes when the room goes dead, Bob begins asking questions about the other people in the channel like "What is your favorite food?" which he almost always follows up with his own answer. To make matters worse, Bob did not configure his IRC client properly, so when he is whois'd by Alice, she gets his realname (Bob-PC).

Despite Bob using Tor to connect to the IRC network, effectively hiding his home ip address and location, he makes the mistake of saying too much about his work life, personal life, and dietary habits. With this information alongside the information retrieved due to Bob's improper configuration of his IRC client, the search for Bob is now narrowed significantly.

Bob soon realizes this, but it's too late. Critical information that can be used to help identify Bob has been obtained by an adversary (Alice). Paranoia does not work retroactively. You must be actively paranoid in order for this to work. Fortunately, it isn't very hard to be paranoid.

Section Two - But how?

The game is the game. Always.

"See, the thing is you only got to fuck up once. Be a little slow, be a little late, just once. And how you ain't gonna never be slow? Never be late? You can't plan for no shit like this man, it's life." - Avon Barksdale

All it takes is one little push for the dominos to be set in motion. One tiny mistake and your whole operation can be cracked wide open for everyone to see. Maybe it's placing too much trust in the wrong person, or not enough trust in the right person. Perhaps you let something slip to the wrong person at the wrong time. So how do we deal with this?

As stated previously, paranoia does not work retroactively. You must plan ahead. So what can we do?

First, I would highly suggest immediately get Tor and use that as a base for everything that you do related to your illegal/underground/anonymous operations. Second, I also implore you to learn how to tighten up your security in terms of software choice, passwords, etc. Now onto the fun part.

Set up multiple cover identities. Name, place of residency (country, state, province, etc), date of birth, hobbies, email, facebook, twitter, etc. This takes a lot of practice and an incredible amount of patience to become efficient at. You do this so that if you fuck up, the heat gets thrown at someone who does not exist.

Have inconsistent hours of operation. Try your best to get on at different times every day and for different lengths of time.

Never cross contaminate. The cover identity used to create your hacker persona should never come in contact with you or other cover identities. Never do anything illegal from your own home or a location near your home. Not even your cousin's house.

You should never mix up illegal/underground operations with recreational activity. Always treat this like a business. Take your time and think things through.

Compartmentalize. Only tell people what they need to know, so if someone gets busted and is turned into a covert witness they can't give up enough information to shut down the operation and it will be very easy to tell when they turn state.

Most importantly: Shut the fuck up. If you don't say it, they can't use it against you.

Scenario time.

Bob and Alice decide that they both want to start an illegal operation. They appoint each other as leaders for certain groups for which they are responsible for recruiting new members who themselves will attempt to recruit new members. Bob uses Tor and attempts to make use of multiple cover identities while making sure not to cross contaminate. Alice uses Tor as well and makes use of multiple cover identities, does not cross contaminate, and compartmentalizes. One day, a member in a splinter group headed by Bob's 2nd man disappears suddenly only to reappear some

days later. Unfortunately, Bob has not properly compartmentalized and has made his existence known to the members in this splinter group. Eventually Bob is confirmed to be the head of this operation and an investigation is launched. Bob continues to make an appearance in the splinter group's channel and over time leaks enough information to condemn himself. Alice however has indeed properly compartmentalized and is left untouched because she never gave Bob any information that would allow him to rat her out.

Bob goes to prison, and Alice remains free. One little mistake is all it takes.

Section Three - And if it works?

You only do two days - The day you go in, and the day you get out.

You'll know if all of the hard work and time and effort you put into making sure you don't go to prison worked if you don't go to prison. If nothing happens, congratulations, you did it. That's it. You can stop now. No, really. You're done. Carefully remove the masks and cloaks, slip into the shadows, and move on with your life. It's over.

Bob did everything correctly. He planned ahead, took his time, thought things through before executing, and made a ton of cash doing it. He retires his operation, marries Alice, and lives out the rest of his life comfortably. Y'know, not in jail and with a ton of money.

Thank you for reading. No really, thank you. If you have any questions feel free to ask them below or in a private message or over Jabber.

I would also appreciate feedback. I'm sure there are things that I could have explained better, and there is likely something that I left out. If you have any feedback, please give it.

Again, thank you for reading. I hope you learned something new.

crazyycast13 - October 8, 2014, 3:36 am

Already knew everything you just said, but I doubt other people even consider this.

tl;dr the schizophrenics type paranoid will always one up you on anonymity, try to make one of those people your friend, you will learn a lot.

I'll add something to this though:

If you can pay someone to write posts for you talking about threads you don't care for, do it. One of your personas gains an aspect that you previously wouldn't have been able to make. It also throws people off your tracks a lot more than you would think.

Looking forward to more threads.

Nakamoto - October 8, 2014, 3:57 am

(Oct 8, 2014 03:36 AM)crazyycast13 Wrote: [\[CITE\]](#) Already knew everything you just said, but I doubt other people even consider this.

tl;dr the schizophrenics type paranoid will always one up you on anonymity, try to make one of those people your friend, you will learn a lot.

I'll add something to this though:

If you can pay someone to write posts for you talking about threads you don't care for, do it. One of your personas gains an aspect that you previously wouldn't have been able to make. It also throws people off your tracks a lot more than you would think.

Looking forward to more threads.

Thanks for the feedback. That is an interesting suggestion as well.

?Criminal - October 8, 2014, 9:15 am

Prob me nakamoto and like a few other people actually know the true potential of opsec, OSINT also goes hand in hand, if your opsec is shit chances are theres tons of OSINT about you laying around for malicious actors to use against you.

How bout using your brain - October 8, 2014, 10:18 am

Somebody really likes the gruggq ?

I like the happy end with Bob marrying Alice. Although considering that Bob was arrested earlier, this might be just a trick to get to Alice and put her in jail as well ? never marry people you met on irc guys.... basic rules :D

Nakamoto - October 8, 2014, 12:40 pm

(Oct 8, 2014 10:18 AM)The Onion Router Wrote: [\[CITE\]](#) Somebody really likes the gruggq ?

I like the happy end with Bob marrying Alice. Although considering that Bob was arrested earlier, this might be just a trick to get to Alice and put her in jail as well ? never marry people you met on irc guys.... basic rules :D

The Gruggq's work is a fantastic resource for learning about OPSEC and CI. I would be lying if I said that he didn't influence a large portion of this thread.

(Oct 8, 2014 09:15 AM)maybeBlue Wrote: [\[CITE\]](#) Prob me nakamoto and like a few other people actually know the true potential of opsec, OSINT also goes hand in hand, if your opsec is shit chances are theres tons of OSINT about you laying around for malicious actors to use against you.

Sadly enough too many people don't take any of this into account when doing something illegal. Hence, this thread.

DrPanda - October 8, 2014, 1:31 pm

I some how feel like I read this before.... like a couple of defcons ago I went to there was a guy handing out OpSec leaflets that kinda said close to the same thing....

But man, thanks for refreshing it in my head I lost it years ago, grate share that everyone who does anything should memorize and learn like a religion, for there own personal safety.

Nakamoto - October 8, 2014, 1:51 pm

(Oct 8, 2014 01:31 PM)DrPanda Wrote: [\[CITE\]](#) I some how feel like I read this before.... like a couple of defcons ago I went to there was a guy handing out OpSec leaflets that kinda said close to the same thing....

But man, thanks for refreshing it in my head I lost it years ago, grate share that everyone who does anything should memorize and learn like a religion, for there own personal safety.

No problem man. I'm glad I could assist you.

Cyrus - October 8, 2014, 8:00 pm

Best security: Don't talk much. Never brag about your activities, anywhere.

Nakamoto - October 8, 2014, 8:10 pm

(Oct 8, 2014 08:00 PM)Cyrus Wrote: [\[CITE\]](#) Best security: Don't talk much. Never brag about your activities, anywhere.

Exactly this. Most of the time people have a setup that is suited for defense against other hackers but they end up drawing attention from the feds. Their defense isn't meant to protect against an adversary of that strength and they get owned immediately.

kingcope - October 9, 2014, 7:57 am

You didn't write this, go away skid.

Nakamoto - October 9, 2014, 1:34 pm

(Oct 9, 2014 07:57 AM)kingcope Wrote: [\[CITE\]](#) You didn't write this, go away skid.

You're absolutely right. I hired a small group of children from the local sweatshop to write this for me.

0/10 - made me reply.

boststin - October 9, 2014, 1:47 pm

(Oct 9, 2014 01:34 PM)Nakamoto Wrote: [\[CITE\]](#) You're absolutely right. I hired a small group of children from the local sweatshop to write this for me.

I highly doubt that...

[I hate the character limit :|]

JaimeLannister - October 11, 2014, 11:38 am

Thank you for the post, I'm not sure if this has been posted before (I'm sure people have posted similar threads) but I'm sure there are plenty of people here (this is under the beginner's section) that have not read a lot of this info before. And when it comes to protecting your privacy doing it right IS essential (and I'm not even talking about just for people who commit crimes; there are plenty of people/organizations out there that love to track people for various reasons). If you mess up on certain things it just means you fail- but if you mess up when it comes to privacy it could be catastrophic.

Thank you Nakamoto

Nakamoto - October 11, 2014, 11:41 am

(Oct 11, 2014 11:38 AM)jm357 Wrote: [\[CITE\]](#) Thank you for the post, I'm not sure if this has been posted before (I'm sure people have posted similar threads) but I'm sure there are plenty of people here (this is under the beginner's section) that have not read a lot of this info before. And when it comes to protecting your privacy doing it right IS essential (and I'm not even talking about just for people who commit crimes; there are plenty of people/organizations out there that love to track people for various reasons). If you mess up on certain things it just means you fail- but if you mess up when it comes to privacy it could be catastrophic.

Thank you Nakamoto

Thank you for the kind words. I'm glad you see the importance in the information that I've laid out here.

JaimeLannister - October 11, 2014, 3:54 pm

No problem, important stuff. It makes one think about the comments they post; although I do feel like there is some level of community here you have to be careful who you trust- and realize that even if the people you are writing for ARE trustworthy people other than the intended readers could easily read it as well.

