All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

The Snowden virus – disrupting the secret world by exploiting their policies

First off, there is, as far as I am aware, no Snowden virus. But what if someone created one. The idea would be to have all of the classified documents from Snowden automatically released from a master virus in different evolutions, each with different spreading methods, so that one after another, they would appear around the Internet. Part of the mechanism would be designed to spam all of the email recipients of each instance of the virus with variations on the classified document contained in the spreading virus. It would also leave pointers to it and copies of it on Web sites of all sorts, embed it in videos, read it into audio, post it in social media groups related to security, and spread it around as much as possible.

So what? How would this cause any problem at all?

Technically, this would be no big deal. Just another of that however many similar viruses out there. Easily mitigated, no technical harm. But that's not the intent of such a virus in any case. The intent is to exploit policy to disrupt a group of people. Here's how it works:

- By policy, nobody with a US security clearance is allowed to have classified information unless they have a need to know, and very few cleared people need these documents.
- If someone with a clearance has such a document, they are required to report it immediately, not read it, and then follow a mitigation process that typically puts the computer more or less out of commission for at least a few hours.
- It doesn't matter if this is available to the rest of the world, cleared people still cannot have it. In other words, the most trusted people are not allowed to have what untrusted people, including the people most not supposed to have it, already have.

The consequences

By now, hopefully my readers will know what is coming next. It is the largest scale denial of services attack ever produced against the cleared community. As copies of the virus, emails from infected systems, audio files, videos, Web site visits, social media sites, etc. reach the unclassified systems of cleared users, millions of reports will start to show up before the responsible parties, and the million or two cleared people and their unclassified systems will have to be cleaned up... again and again. The email servers need to be cleaned, the browsers need to be cleaned, the backups need to be cleaned, and so forth. And worst of all, they are removing content that everyone else in the World is allowed to possess, including the very people the classified documents are supposed to be kept from. Only the people that are supposedly trusted cannot have these documents.

Summary

Would this really bring down the cleared community? Hopefully not. But you never know just how officious security folks can be or how intransigent top management can be when faced with their own concepts being publicly ridiculed. Policies that are ridiculous and officious have implications beyond inconveniencing those forced to exist under them. They can be used to disrupt the organizations using them. It's time to rethink this one – and several others...