All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Provide for the Common Defense

We are now facing a new level of crap. All of those attack methods that were originally considered theoretical are now being widely and openly exploited. Why is this? I think it's largely because the US government is incompetent. That incompetence runs deep and wide and crosses political boundaries and the ages. But I will be a bit more specific:

- They wrote (and presumably still write) attack programs for their offense but deprecate the defense wherever they can so they can gain the attack advantage. It's call equities.
  - Then they leak all the attack code. They can claim they tried to protect it.
    - They apparently thought they could secure their newer attack codes like they did for the stuff that Manning leaked then the stuff that Snowden leaked.
      - At least that part worked. They secured it just as badly.
      - And they won't follow advice of real experts. So we are screwed again.
- They don't now tell us how to defend against the attacks they wrote or help us do so.
  - Perhaps they want to retain their equities? Or create attacks they can't defend?

When will the US government do the right thing?

Apparently never again. The incompetence is spreading, all the way to the top, and back down through the "deep state". Fear not, those in charge will fire the competent folks. Then the incompetence will go all the way down. Dying with a whisper rather than a BANG!

I think it's time for class action

The People v. the United States. We the people, finding an incompetence beyond the pale, and based on an ongoing intent by the government to put their attack capabilities over providing for the common defense, do hereby declare and demand that the full resources of the US government be brought to bear to defend against cyber attack on its people. That includes the NSA, the CIA, the DoD, the FBI, DoJ, and all the rest. Spend a few trillion on protecting us instead of ineptly attacking them, and maybe we won't keep losing at cyberwar!

- The supercomputers used to break enemy codes should break randsomware codes.
- The intelligence capabilities used to spy should be used to track the attackers and the weapons used to fight wars should be used to physically destroy cyber attackers.
- And the US government should have to pay for all the costs and consequences of their attack codes used against our citizens, corporations, and others who suffer from it.

It's not ALL their fault… But most of it is.

The US government and "defense" contractors should be held personally and corporately liable for the costs and consequences of their acts against the people of the United States and their failure to act to provide for the common DEFENSE. They should be liable for their failure to act reasonably and prudently, they either knew or should have known that their cyber attack codes would get out and be used against their own people. It's time to re-balance the equities in favor of the defense of the people of the United States!

A Rant

I usually try to be a bit careful in my comments, but I have now seen far too many folks expressing in deliberate and careful terms in an introduction to some desired potential future action relating to information protection that there is somewhat of a basis for concern relating to the potential negative effects of cyber-related incidents.

Screw that!

We are in a global war, and decision-makers are acting as if we are in a minor family tiff.

- How many more top executives and their boards will sit by and decide to consider carefully when to contemplate action in this security thing?
- How many CIOs will tell others in top management that they have it under control when we all know or should know by now that this stuff is not under our control?
- How many months will it take to decide to do a security assessment, even after you have suffered an almost existential outage?
- How many more months will it take till the assessment is done?
- How many years will it take to do the first few recommendations from this assessment?

Urgent and important

It’s London, World War 2, there are bombs falling around the city every day, but your store hasn’t been hit yet, even though your next door neighbor just lost a child. The sirens are sounding. What do you do?

- **Option 1:** Schedule a time next month to set up a committee meeting to consider whether to take up concerns about possible future bomb effects on your business and, based on that meeting, if appropriate, form a study committee to get you a report in the next 6 months on options to consider for the coming year.
- **Option 2:** Get to the underground until the all clear and figure out how to better protect your family and recover from damage as/if it happens as soon as the all clear sounds.

If you are corporate today, Option 1 is the apparent choice. If you are rational, it’s Option 2.

Just got hit – now what?

It’s July 1, 2017. You just got put out of business for a few days from an “accidental” side effect of a cyber attack aimed at someone else. You are barely operating. What do you do?

- **Option 1:** Schedule a time next month to set up a committee meeting to consider whether to take up concerns about possible future cyber effects on your business and, based on that meeting, if appropriate, form a study committee to get you a report in the next 6 months on options to consider for the coming year.
- **Option 2:** Get your corporate ass(essment) in gear and figure out how to better protect your business and recover from damage as/if it happens, and fix it right now.

Conclusions:

Option 2!