All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

The year of the Trojans (and their unintended side effects)

2014 was not so different than previous years in many ways. But a distinguishing feature was how clear it became that we cannot trust what we are told in terms of information protection.

Context

As context, this year it became clear to all who were watching and interested that many of the "theoretical" results that were not widely acknowledged as realistic before, but were long on the list of bad things that could happen, were made the mainstream.

- Trojan horses placed in hardware at the point of creation, during transport, and during operations were all revealed as present in modern devices.
- Companies who provide software that uses passwords, for example, to retrieve emails, were revealed as taking control of those passwords, and in some cases collecting the emails in their own databases to "help" their customers access them.
- SSL and other encryption schemes were demonstrated as being interceptable and intercepted en-route by government and private companies as well.
- The supposedly secure high-speed links between sites based on trust in the large telecommunications providers were revealed as tapped for content and traffic patterns.
- The software stack, from microcode to operating systems to libraries to applications to recursive languages and programs, all demonstrably not only hackable, but hacked.
- Networks with all of their interdependencies were subjected to attacks at all points, from the drivers to the hardware, to the switches and routers, to the supporting infrastructure, the cable and wireless service providers, radios, wifi hot spots, cellular towers, and bluetooth connections, all hacked at the end points and in the middle.
- The physical separation of devices was shown weakened by introductions of Trojans.
- Demonstrations of optical, sonic, RF, power, and even visual videos of passive objects vibrating in the sound of the room were shown usable as listening devices.

Companies of all sizes, individuals, governments, organized crime groups, you name it others, and anonymous attackers were complicit in this collapse of trust in the systems and methods of the information age. No vertical was spared:

  - Power, water, fuel, governance, entertainment, finance, investment, retailers, wholesalers, service industries, product industries, manufacturers, growers, government agencies, individuals, movie stars, the emerging high tech giants, mom and pop stores, all successfully targeted and exploited.

Governments responded by increasing surveillance of their citizens and others. Big data analytics mined that data for advantage to those who controlled it. Intentional weaknesses were put into systems by police, governments, the companies that cooperate with themm and others, under color of authority or for financial gain.

Fear, uncertainty, and doubt (FUD) has been taken to extremes in 2014.

- Nobody knows where to turn for comfort, reliability, and certainty.
- The hyperbole surrounding APTly named Advanced Persistent Threats understate the revelations about the reality of the situation.
- Governments are not only unhelpful, they are a key enemy of effective protection.
- The companies you relied upon had their good names tarnished, one after another, by their own acts, errors, and omissions.

That was the year 2014 in information protection.

Easily lost and hard to regain

Trust is easily lost.

- When Google admitted that it didn't encrypt the links between its data centers, it revealed just how inept Google was at taking their responsibility seriously and how they wrongly trusted others to do their job.
  - But Google also admitted the lapse, and adapted publicly, quickly, and directly by encrypting those links, and that went a long way to restore the trust.
- Facebook has a long history of untrustworthy behavior, and nothing they do indicates in any way that they will change it.
  - From updating contracts to do what they want to, to performing experiments on their customers against the scientific norms of the day, they continue to amaze as they abuse. And yet they stay in business so far.
- Apple gained trust by refusing to yield to government pressure to decrypt iPhones.
  - But they remain in their walled garden and don't play well with others, making many resent the fact that they still have to choose Apple over the alternatives.
- Sony is losing their reputation as their internal memoranda are revealed along with their demonstrated inability to keep their own communications private or fight off the anonymous threats they now claim to be from a nation state.
  - The FBI indicated a nexus with North Korea. But “security community” members are fighting against it without a factual basis. The FBI says it cannot tell how they know, the “security community” cries foul, and the little trust built over years is lost.
- The US government has demonstrated its lack of trustworthiness to other nation states, not because of their spying activities, but by their inability to keep them secret. Every nation state spies, but few are as embarrassingly unable to keep their secrets in such high volume from the general public and those they are spying on.
  - Inept leadership when facing what they pretty apparently knew to be vulnerabilities, decided not to do their duty to protect. The result was the biggest leak ever only a few years after the 2nd biggest leak ever.

Across the board, there were clear winners and losers in terms of trust, but the biggest losers are the public at large and the millions of small and medium-sized companies.

How do they lose trust so fast, and why can't they get it back?

It's easy. The people in charge don't get what most folks in the field have known for years:

(1) Be competent.
(2) Work to do the right thing.
(3) Admit your mistakes.
(4) Correct your mistakes as well and quickly as you can.

The losers in this game:

(a) Don't worry about competence. Rather they favor thinking they are always right and always have the best advice, even though it's clearly not true.
(b) Don't worry about doing the right thing. Do the most expedient thing.
(c) Never admit mistakes.
(d) Don't fix problems. Instead, do something else that makes life painful for others, and then claim to have fixed the problem.

And yet...

Despite all of the disgust I obviously hold for the miscreants of the World on all sides, I am still an optimist. I think:

- This comeuppance will help the situation rather than hurt it, in the long run.
- The increased understanding and awareness of the realities of what used to be considered theoretical attack methods will start to shine the bright light of day on the musty areas of information protection long held in dark corners of miscreants' minds.
- More and more executives, workers, programmers, users, customers, and just plain folks will start to believe they should make rational decisions about protection and stop believing the appeasers and folks that claim to be using “best practices”. The practices they use are not “best” and often they don't actually work.
- Executives need to be fired for failing to meet their responsibilities, and some of them are starting to be.
- The deceptions used by security “experts” to get the funding for what they want should be met by knowledgeable executives who won't put up with it anymore.

Ignorance is not bliss. It is dangerous.

- I think that as the reality starts to set in, executives will:
  - Choose to learn what they don't know.
  - Get sound advice from real independent experts.
  - Move away from the tripe of the big body shop consultancies.
  - Begin to really think about the issues of information protection they face on behalf of their enterprises.

There's a silver lining to the collapse in trust. It is the acknowledgement of the reality experts have long known. And perhaps the decision to address it for real will follow.

But let's not be too harsh on the year 2014 yet.

A year of progress as well

2014 was also a year of great progress in information protection.

- All of the public losses produced a lot of recognition.
  - When half the big box stores get hit, folks stand up and take notice.
  - The public relations surrounding the Sony attack, attribution to North Korea, debate in the media with computer security providers arguing publicly about the issues of attribution, denial of service attacks, media claims, release of the movie after the comments of the President, all formed up around the holidays.
  - When you look at the reality of what's going on, the vast majority of the losses to date are not very consequential to society as a whole.
  - The recognition of the reality of these cyber-security challenge along with the increasing visibility are producing more public and political will than we ever had in the 1980s-2000s.

The damages were low compared to the social rewards.

- Gartner declared 2015 the year of deception for defense. This area has the potential to change the leverage to favor defenders over attackers, and people will start to adopt it.
- Standards of practice were adopted as part of cyber-insurance processes as there was widespread recognition that cyber insurance lacked rationality. Rationality will win.
- Information sharing moved from concept to reality with increasing adoption of STIX and TAXI, progress by the ISACs in building the infrastructure and support for sharing, and increasing recognition that sharing is mostly about receiving, not giving.
  - If 1% give and 99% receive, we go from no statistical understanding to margins of error of a few percent.
  - Insurance will become rationalized by fusing protective strategy facts and outcomes across risk pools.
  - When cause (attacks) are mixed with mechanisms (protection) and mapped to effects (losses), we have a basis for science, which will move more quickly now.

And that is real progress.

Then there is the movement from physical wars to cyber-wars, a very good thing.

- Instead of blowing things up and killing people, we are seeing public relations attacks, embarrassing leaks, and minor service denials.
  - This is much better than people being shot and blown up.
  - Cyber attack becoming dominant in warfare is far better than the alternative.
- And there is a pleasant side effect that the critical path to success becomes development of scientific progress based on knowledge and information rather than brute force and explosives delivery.
- Like any conflict, investment in underlying technologies is critical to success.

In cyber-war...

Where will the resources go?

Wars of intelligence and intellect have the potential to advance the world in magnificent ways.

- Increased spending on innovation and ideas that translate into advances in key areas:
  - simulation and modeling
  - big data analytics
  - information protection

These are good things.

- We should expect progress and improvements in all areas of the human endeavor. The results of warfare will be reflected in advances in:
  - medicine, biology, and public health
  - agriculture and environmentally and physically sound buildings
  - transportation and communications
  - better and more capable mobile devices
  - increased public knowledge of events effecting us all
  - stopping politicians from being duplicitous
  - better and safer sharing
  - better differentiation of truth from lies

and the list goes on and on.

And the other Trojans

I got my Ph.D. from USC in 1986, and have been a fan of their sports teams ever since. I would be remiss if I didn't complement their new coach and all their fine players on the year of the USC Trojans as well. Their football team has come back from the brink of oblivion (due to previous violations of NCAA rules), and in 2014 they made a bowl game and won it. Fight on!

But returning to the subject at hand...

Summary

Big leaks have a chilling effect on people doing the wrong things, and that is good for us all.

The embarrassment of Sony's executives, the CIA, the NSA's, Google, big box stores, public figures, politicians, reporters, pundits, and so-called experts is a very good thing for society and human progress.

The pope's lesson to the church hierarchy is one we should all reflect upon. Competence and sincerity are what we need to demand of ourselves and others.

2014 was a building year, and 2015 will be even better.

Happy new year!

