Content Insider #407 - Lovin Code

Hacking – The Job that Just Keeps on Giving

Source - Hackers," United Artists

"*This is our world now. The world of the electron and the switch; the beauty of the baud. We exist without nationality, skin color, or religious bias. You wage wars, murder, cheat, lie to us and try to make us believe it's for our own good, yet we're the criminals. Yes, I am a criminal. My crime is that of curiosity."* – **Agent Bob, "Hackers," United Artists, 1995**

The hacking "industry" has come a long way since 1972 when Woz and Jobs would make blue boxes similar to Draper's "Cap'n Crunch" boxes and would sell them to folks who wanted to make free phone calls anywhere in the world.

If they hadn't decided to make Macs, the business would have died because you can't find a phone booth anymore, can you? Or, they could have done jail time like Draper.

Gee, tough choice.

A lot has changed in the past 40+ years, but a lot is the same. People want to poke around and others want to stop them.

Because the Internet and personal devices have become our lifelines to the world, cybersecurity has become a major issue for governments, companies and individuals.

It's no wonder the Black Hat Security Conference (DefCon) keeps drawing more and more computer hackers, information technologists and corporate/government specialists hell-bent on learning the latest tactics to infiltrate and protect networks, systems, devices.

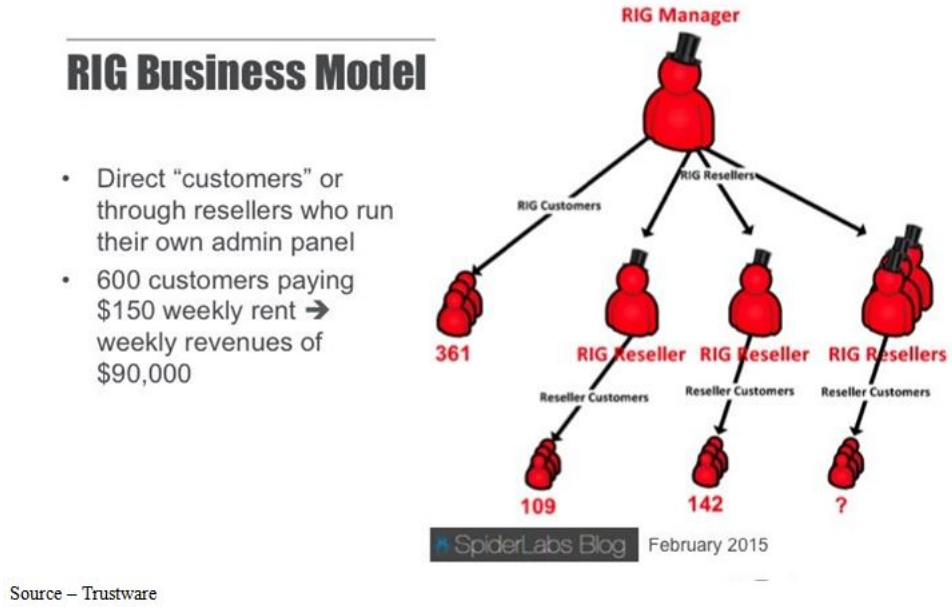
There is certainly enough bad code out there to keep both sides working for years to come since most of the software and apps are built from modules of old code, perpetuating old holes and creating new ones.

Of course, sloppy users help too; and no amount of bitching 'n screaming is going to change bad habits.

Big Business
So hacking is a big business– hell, its huge – bad and good.

On the bad side you have people who may not even be decent code writers but are real good at making a dishonest buck. You know, people ranging from individuals to gangs and mafias with finely-tuned systems that function just like any other profit-oriented business.

Their scale of operations would blow your mind.



Source – Trustware

> ***Dark Side –*** *There are good and bad hackers who make their living off the internet. The good find and repair penetration areas. The bad exploit penetration areas and people's gullibility, stupidity, greed. For the bad, it's just good business.*

A recent ***Business Insider*** article cited facts painstakingly compiled by security firm Trustwave. They found a cybercriminal with average intelligence and tools/services that can be bought online (if you have the right connections) could easily clear $80-$90K a month.

Catching and prosecuting them is tough, but not impossible.

Then there's the grey operations run by government agencies around the globe that poke into country/company systems while trying to patch/protect their own systems.

The majority who congregated in Las Vegas wanted to find out where the vulnerabilities were in our now digital world and how to fix 'em.

Yeah, there were a lot of suits/dresses there who wanted to hire these folks for their organization to stop cyber intruders and anticipate/prevent future attacks.

When you consider the fact that 90 percent of the world's data has been produced in the last two years; by 2020, 30-50 billion devices will be connected to the Net and we'll be trying to store 40K Exabytes, the Internet is kinda' important.

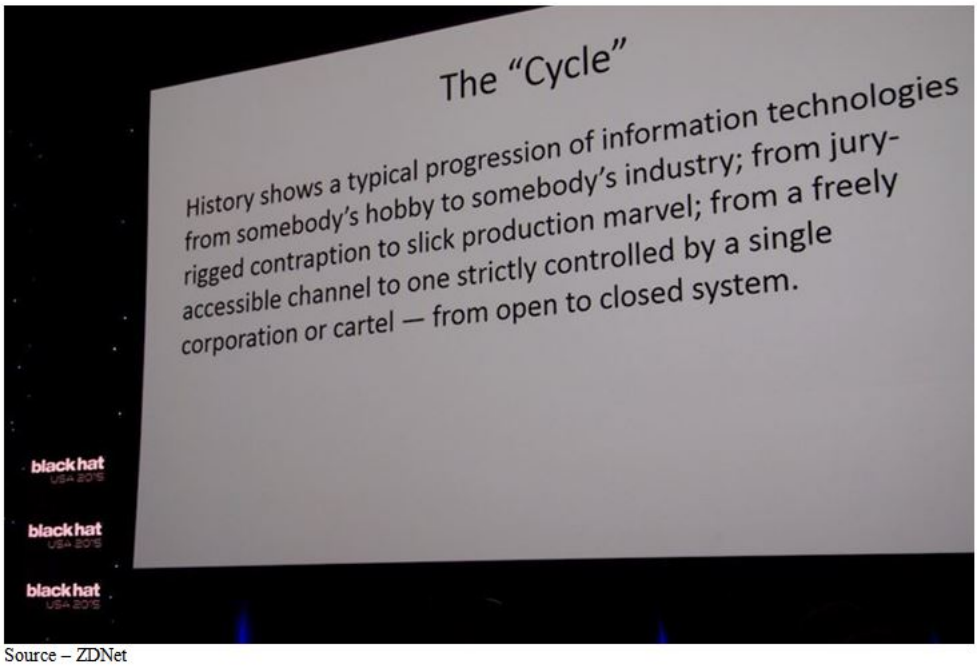
No one can pinpoint when the Internet lost its virginity.

It could have been when Admiral Grace Hopper, who developed the first compiler back in 1944 and found a bug (actually, a dead moth) in Harvard's Mark II computer in 1947.

Or it could have been in 1991 when hyperlink creator Tim-Berners Lee and the team at CERN (Conseil Européen pour la Recherche Nucléaire) developed the Web and people quickly figured out they could make money across the Internet and on the Web.

We're Dead

To get the good Black Hatters fired up, Jennifer Granick, Director of Civil Liberties at the Stanford Center for Internet and Society, started things off by telling them they could lose the Internet or the semi-free, semi-open Internet we know today.



Source – ZDNet

> ***Evolution –*** *Starting this year's Black Hat Conference with a dire warning, the director of Civil Liberties at the Stanford Center for Internet and Society said that business as usual will only lead to a controlled, monitored Internet unless the community protects the Internet.*

Ms. Granick voiced what the crowd already knew -- every country's lame government wants to control the Internet so they can guarantee their citizens security and anonymity while making it easier for them to watch what folks are doing, censor it and centralize control.

Exactly what Vint Cerf and the other guys didn't have in mind!

Of course, that also didn't sit well with the hackers but a lot of the security pros didn't see much wrong with it.

In an ideal world, the Internet would be open, free, decentralized.

The problem is there's always the "Yes but…"

Individuals shouldn't be harassed, bullied. There are loosely defined social norms and courtesies that should be observed for groups and individuals. We owe it to our children to let them

explore, make mistakes, learn … after all, they are our future. People have to be protected from their own stupidity and greed.

As it is, the Internet isn't free, isn't safe, isn't secure; and that's what most of the Black Hatters and security pros were focused on at the event.

They were there to learn newer, better techniques to deliver that balance.

Opportunities Everywhere
Along the way, a guy/gal has to have a little fun like hacking each other's phone/tablet/computer/watch, tapping into ATM machines, fiddling with slots and finding their way into anything with a computer chip in it and a line of code.

Source – ZDNet

> ***How to Protect –*** *To protect anything you have to find out where its weaknesses are. That's the focus of the Black Hat Conference where people learn how anything/ everything is hacked and how it can be protected.*

With 100 sessions to attend, black hatters found that damn near everything could be hacked:

- Most Android-flavored smartphone users should be a little concerned and iPhoners shouldn't be too smug.
- Chrysler recalled tons of cars, Musk got a patch out for the Tesla, the rest of the increasingly computerized car makers sweat bullets.
- Government hacks – it's tough to keep a scorecard here with every government agency around the globe hacking every other county's agencies, with other folks hacking the agencies and probably country agencies nosing around each other's locations.
- Display hacks – Folks were up in arms over Adobe's flash player hack, saying it was time to pronounce it deceased; but then HTML5 has its share of problems so the name calling will continue and we're wondering how we'll enjoy all those cat videos.
- Folks hacking smartguns, skateboards, drones and GPS (seriously folks, I have a tough enough time finding my way from point A to point B).
- House hacking – thermostats, lights, locks, refrigerators, media centers, stoves, toilets … anything/everything can be hacked.

- Infrastructure –a country's very foundation (electrical, water, transportation, emergency services) can be hacked.
- 50B connected things – By 2020, Cisco projects we'll have intelligent sensors, connections with just about anything you can imagine giving creative selling opportunities for almost everyone and more targets that need to be tested, protected

.

Help Wanted

With software holes and opportunities for holes everywhere you turn, the black hat and DefCon were also giant job fairs.

Source – US Army

> ***Recruitment –*** *With all the right stuff the Black Hat Conference is an excellent place to find a job or move up in the cyberprotection world. The more experience you have, the more certified training the more offers that come your way. Hacking isn't just a job; it's a career for bad or good.*

Exhibitors and headhunters were everywhere, searching for seasoned hackers to recruit.

They only validated what Burning Glass Technologies recently reported – there aren't enough cybersoldiers to fill the open positions in the U.S. or around the globe.

The company noted that cybersecurity jobs have grown three times faster than other IT jobs and the skill sets that are needed continue to rise.

Sure, government and spook agencies preprinted offer form letters but the financial, healthcare, auto and consumer goods organizations also had their eyes out for possible recruits.

The demand/shortage also means cybersecurity jobs also offer salary premiums ($80K U.S. plus, compared to other IT jobs).

The problem is almost all of the jobs call for a Bachelor degree, cyber certification and three years of experience.

Then too, more of the job openings call for accounting, financial, other specialty skills as well as a security clearance.
Not sure if that last requirement is too high or too low because Snowden had one while working for the NSA (National Security Agency) and it didn't slow him down too much.

But organizations have to start somewhere.

None of the headhunters looking for folks work for organizations – here or abroad – that are inherently evil (O.K., a few maybe) but it is impossible for them to deliver everything Ms. Granick wants – a free, open Internet; free speech; online safety/security and the right to privacy.

Remember, it's a network of networks built with new code using old code to do things people didn't even think about a few years ago.

That's pretty hard to destroy and rebuild from the ground up.

Source - Hackers," United Artists

Ms. Granick probably agrees with Kate Libby, "*Never send a boy to do a woman's job.*"

# # #