Content Insider #411 - Soft Facts

Keep The Good Hackers to Protect Us from Bad Hackers

Source - *"Dragnet," Mark* VII Ltd.

> **"***Ladies and gentlemen, the story you are about to see is true. The names have been changed to protect the innocent."* **- The Announcer, "Dragnet," Mark VII Ltd., 1951-1959**

When hackers took control of a Jeep and put it in a ditch, the media made it sound like a dangerous thing, Congress screamed and Chrysler recalled thousands of vehicles to fix the problem.

When word of the Stagefright exploit was announced that enabled hackers to send an MMS message containing a video that includes malware code to millions of Android-based smartphones, Google assured us, saying that it would be taken care of with the new software device manufacturers release with their next-generation devices.

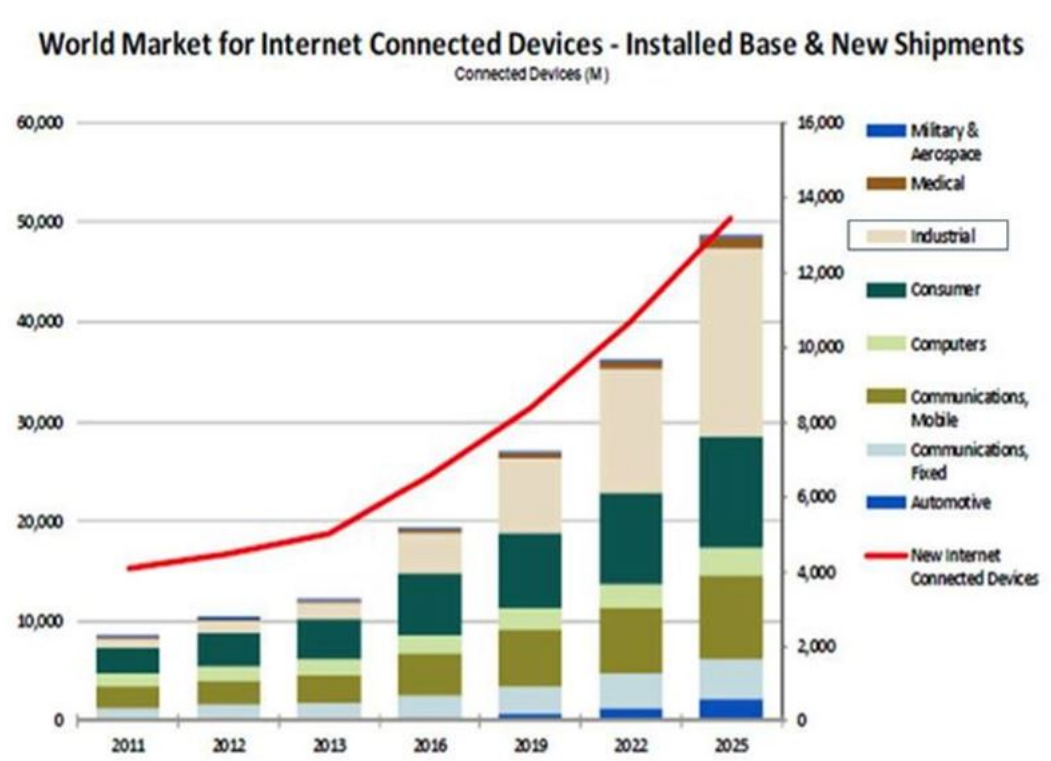
When Malwarebytes Labs announced that Hacking Team, the Italian security company specializing in offensive technology, offered a penetration tool for Adobe's Flash Player that could turn it into a weapon; villagers marched on the castle vowing to burn it at the stake and replace it with HTML 5.

Of course, HTML 5 folks kept quiet because their offering has its own share of issues.

Software problems are so bad that at the Black Hat Conference, someone noted that the speed with which attackers are weaponizing, zero-day vulnerabilities has essentially been cut in half.

So?

Back in prehistoric times, it used to be that only computers were connected to the Internet.



Source - IHS

Overwhelming Mass – *We talk a lot about the benefits and dangers we will have in the not too distant future when everything, anything is connected. But security and privacy are never the number one design specifications for hardware or software.*

Today, almost everyone on the planet has at least one connected device (smartphone) and kids who were born connected have four or five – smartphone, tablet, computer, game console, iPod, second phone, smart Watch/band, you name it.

The industry and media are touting (pushing) IoT (Internet of Things) and IoE (Internet of Everything) and lusting for the time when we'll have 50B things attached to the iNet running software and apps.

Every one of those big and little programs are designed/written to do something a little bit different from the other guy's, so they can differentiate themselves from the competition.

Security at the development stage isn't a high priority, but speed to market is.

That's why companies offer beta software so tens of thousands of eager people can be the first in their group to get their hands on it to play with, test and use.

That's akin to an auto manufacturer selling cars based on a rough design and early customer complaints.

Each new one shipped is improved based on customer beta testing and feedback.

It's such a part of the software "finish it and ship it" mindset that we don't even call them problems anymore.

They're not really bugs.

They're *"undocumented features."*

In defense of programmers everywhere, let me note that when you put even the most rigorously tested/proven software on your device and it interacts/works with other software, weird things can and do happen.

Former *New York Times* tech writer Dave Pogue once observed given the permeations of hardware, software, firmware that are possible, it's a miracle computers even worked at all.

With 1.5M apps available to you on iTunes and people downloading a couple of hundred just to try, it's a wonder they can even text.

In their infinite wisdom, boomer-plus folks globally elected (and anointed) government officials who have historically taken a dim view of the people (hackers) who discover these shortcomings/issues.

Last year, the U.S. Department of Justice (DoJ) prosecuted 194 CFAA (Computer Fraud and Abuse Act) cases--a fraction of the more than 56,000 total cases filed.

Of course, the DoJ says they are committed to ensuring the law isn't abused and that people doing research-oriented work won't be drug into court.

In some countries, hackers are tolerated and even valued when they're finding digital openings in other countries.

Finding the ways in the stuff at home?

They simply disappear.

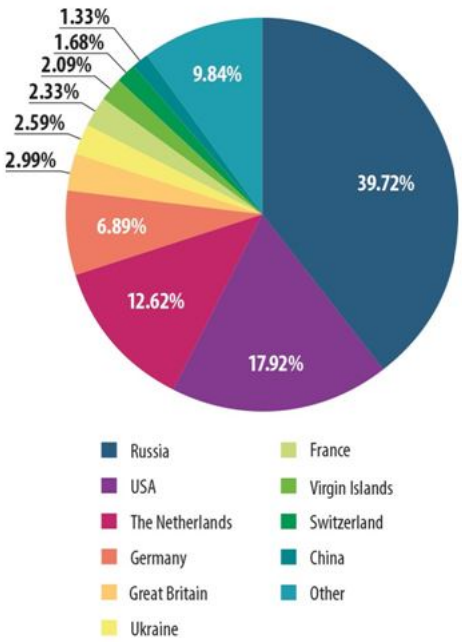
Still, there are countless reports of hackers who uncover bugs and holes, report them to the solution owners and nothing happens for months on end.

If the hacker – out of frustration – makes the vulnerability public, the company quickly responds by saying "we take our customers' security very seriously," and a rush patch is released.

Then they paint the reporting hacker as a really nasty guy/gal.

Gimme a freakin' break boss!

Of course hackers outside the U.S. – such as those in China and Korea – aren't too concerned about the CFAA and they're the ones U.S. government officials say are most intent on breaching their systems.



Source - Kaskpersky

> ***It's their Fault -- Every*** *country points at the other countries for all of their problems. However, 90 percent of notifications on blocked web attacks were triggered by attacks coming from web resources located in 10 countries. The other 186 countries just are not doing their part.*

They forget to note that the US is number two when it comes to attacks, according to Kaspersky, one of the globe's leading security providers.

The firm recently reported that about 51 percent of Web-born attacks were launched from Russia, followed by the US, the Netherlands, Germany, France, Virgin Islands (seriously, the Virgin Islands?), Ukraine Singapore, the UK and China. Yes, the UK beat out China when it comes to launching cyberattacks.

Giving white hat hackers the latitude to find and help resolve software issues will go a long way in making devices, systems and solutions operate more smoothly and safely.

Many government agencies around the globe are opposed to robust encryption, saying it cripples their fight against terrorism and crime.

Former U.S. high-ranging intelligence, homeland security and defense officials disagree.

A while back three of them wrote an op-ed piece in "*The Washington Post"* saying, *"We believe that the greater public good is a secure communications infrastructure protected by ubiquitous encryption at the device, server and enterprise level, without building in means for government monitoring."*

Let's see, it's impossible to develop/deliver 100 percent foolproof, bug-proof software today and tinkerers/hackers are in demand to find the problems.

But governments don't like these people who mess with the stuff.

However, government agencies want us to design in a backdoor and give them a duplicate key so they can come in and poke around just in case?

Sounds good to me … ***NOT!***

Long, long ago, computers – called mainframes – existed in big air-conditioned rooms and problems stayed inside the company.

Then we connected everyone's' computer to the internet and folks used antivirus and security software to protect them … and backed everything up (O.K., most trusted dumb luck but still…).

Today, computers (and software) are in everything – door locks, light bulbs, cars, refrigerators, thermostats and are constantly in your hands.

We have enough zero-day vulnerabilities that beta testers and hackers need to find without insisting we add one more for government folks that everyone knows about.

Software developers try to deliver rock-solid, bullet-proof software.

That's why they put their products in the hands of review companies that find problems. Those get solved and the software is … better.

But that doesn't mean it can't be hacked.

Source – theithelper

> ***Guaranteed –*** *Every company and developer works hard to give customers bug-free software. That's why they have teams of testers and reviewers. Everything is great until it's put in the hands of users, then…*

When the product is finally released; hundreds, thousands of code reviewers, tinkerers, and hackers beat it up and find bugs no one else found.

Instead of government agencies (and companies) threatening to take these people to court, they should offer bug bounties based on the severity of the problem and the sensitivity of the information organizations are trying to store, protect.

That's what all night, all weekend hackathons are all about.

Prime millennials, teens, tweens with Red Bull, Twinkies (they are back ya' know!) want to see what they find.

Software is never finished and always new, always better when the white black hatters are challenging it.

Source - *"Dragnet," Mark* VII Ltd.

But then, as Sgt. Joe Friday said, "*All we know are the facts, ma'am.*"

# # #