COMPUTER NEWS from the

JUNE 2013 Volume 1 NO. 6

As found on the web and other sources

Why Does Malware Exist?

FROM"Askbobrankin.com".

Computer viruses are everywhere. Spam is abounding. Computer intrusions, identity theft, denial of service attacks and other cybercrimes are commonplace. Who does this stuff, and what's wrong with them? Let's take a look at what motivates the miscreants who menace millions on the Internet...

Hackers, Spammers and Cybercriminals

Have you ever wondered why there's so much spam, so many computer viruses, rampant identity theft, and other perils of using the Internet? Perhaps it boils down to the ancient philosophical question, "Why is there evil in the world?"

Greed is the most common motivation for cybercrimes, as it is in the real world. There are big bucks to be made in malware that steals credit card, bank account, and identity details, corporate secrets, and other valuable data. The gullible will readily give money in exchange for counterfeit goods or just the false promise of goods. Some people will pay good money to have business competitors beaten up online. Most of the online damage is done for money.

Hatred is another ugly motivator. Often, it is disguised as heroism, a noble fight against a perceived evil enemy, which may be an individual, organization, corporation or government. But it's hatred, none the less. Examples of this include those who maliciously deface the websites of organizations with whom they disagree. Or it could be a group like Anonymous or LulzSec that perpetrate denial of service attacks against their philosophical enemies.

Egotism is a third motivation. The desire to show the world how good your skills are, to do what others have failed to do, to make yourself look smart by making others look stupid, are all very satisfying to insecure egos. Some hacking groups have done this by breaking into websites, stealing embarrassing or confidential information, and publishing it online.

Grab That Cash With Both Hands and Make a Stash...

How do cybercrooks make money? The answer has changed over time. But mostly, it's All About the Money. (Hat tips to Pink Floyd and Travis Tritt.)

Sanford Wallace was the original self-styled "Spam King." In the 1990's, he had an ostensibly legitimate advertising business, sending out millions of unsolicited emails that advertise products or services for sale. He got paid a pittance for each email he sent, and a commission for each sale consummated in response to an email. According to "Spamford," he made millions of dollars providing a perfectly legal service to merchants and consumers.

But eventually, spam stopped paying so well. Spam filters improved, and consumers became more wary of unsolicited offers. Spammers increasingly switched from selling things in annoying but legitimate ways to deliberately trying to defraud people.

Most modern spam intends to sell your identity, not to sell you a product. That cheap product may not even exist; all that matters is that you complete the order form with your name, address, and credit card or bank account data. This data is sold to others who take the risk of making bogus charges and cash withdrawals.

Many millions of people fall for such ID theft, depressing the market value of an individual's information. Spammers, or phishers as most of them are these days, have to do very high volumes of mailings to make any serious money. So they turn to malware in order to get others to work for them for free.

Botnets, Scammers and Hackers

Botnets are networks of computers that have been enslaved by hidden malware. The botnet malware uses a slave computer to make more mailings and distribute copies of itself, all unbeknown to the computer's owner. A botnet is controlled and directed from a central server, which receives the stolen identity information. A few highly successful botnets have enslaved millions of computers worldwide. See my related article BOTNET ALERT: Are You Vulnerable? http://askbobrankin.com/botnet_alert_are_you_vulnerable.html to learn more about botnets, and some encouraging news about the takedowns of some of the biggest offenders.

Then there are the low-volume, high-value cybercrooks. They include so-called Nigerian "419 scammers" who find affluent and gullible victims to milk for thousands of dollars. I wrote about the 419 Scam http://askbobrankin.com/nigerian_scammers.html back in 2006, and it's still going strong today. They also include online bank robbers who hack into financial institutions and steal millions at once, often just skimming a few unnoticed cents off of each customer's account. One of the boldest cases involved the theft of over $45 million in 27 countries over the course of a few hours.

In that case, hackers broke into the networks of several banks and swiped PINs associated with the banks' own accounts, not those of customers. Debit cards were forged that could use the stolen PINs to withdraw cash from ATMs. Hundreds of co-conspirators drained ATMs dry at approximately the same time, delivering the ringleaders' share of the cash to their bosses and pocketing their wages. Only seven New Yorkers have been arrested in that case so far.

Cybercrime and (occasionally) Punishment

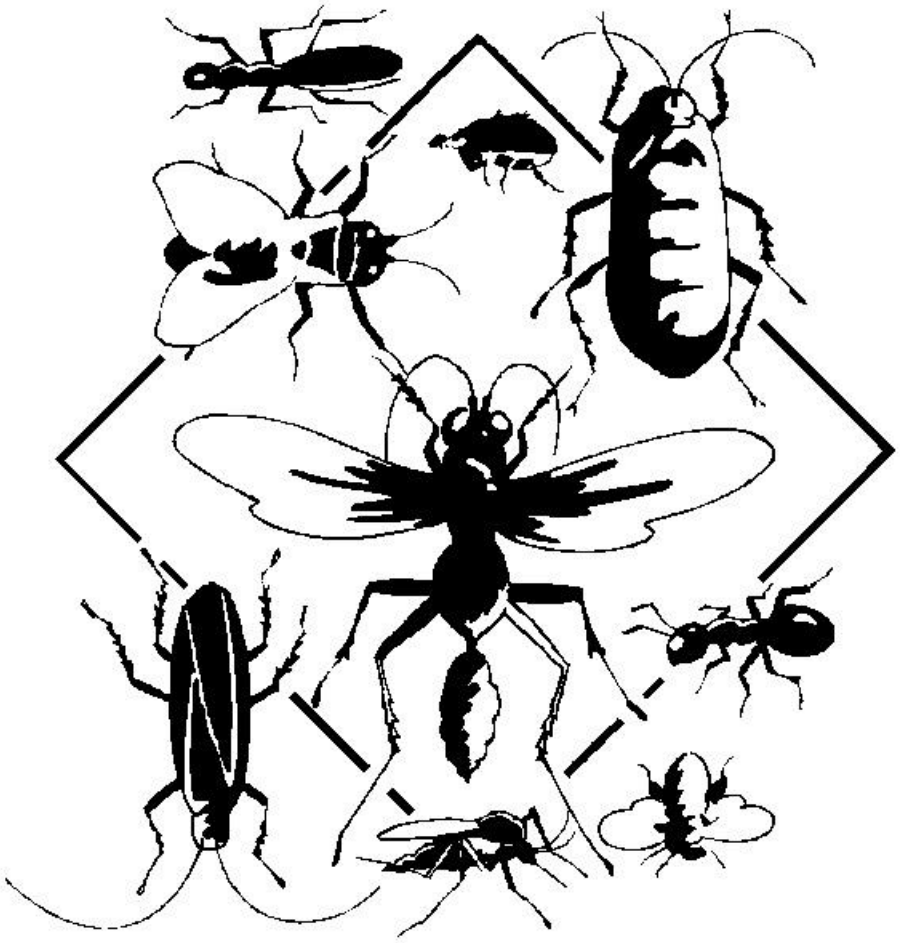
Relatively few online crooks are caught and punished. It's very difficult to investigate and prove such crimes because the criminal activity is hard to trace and often spans international borders. The few successful prosecutions we read about tend to be very large cases that are worth the trouble and expense to prosecutors. One recent arrest involved the alleged ringleader of the LulzSec hacking organization. http://mashable.com/2013/04/24/lulzsec-arrested-australia/

"Spamford" Wallace now faces the prospect of jail time and fines of several hundred million dollars. Oleg Nikolaenko is a 25 year-old Russian "spam king" who allegedly ran a botnet that churned out over 10 billion spam emails every day, an estimated one-third of all spam in the world. He is currently awaiting trial in a Wisconsin jail on charges of violating the U.S. CAN-SPAM Act. A few other spammers have been convicted, but thousands more remain in business.

There is no end in sight to the war on cybercrime, and sadly, most goes unpunished. The best that you can do is try to avoid becoming a victim. Keep your malware and anti-spam defenses

up. Be wary of phishing attempts. Monitor your credit and bank accounts for unauthorized transactions. Look for more computer security information on on this website, or check out my ebook "Everything You Need to Know About INTERNET SECURITY and PRIVACY".

Read more:
http://askbobrankin.com/why_does_malware_exist.html#ixzz2Tq9J2sxF



New “BadNews” Bug Found on Google Play Store

By Brandon Dimmel on 20130423 in “infopsckets.com”/

If you're an Android user, take note: security experts have discovered more than thirty applications on Google Play that contain a malicious bug known as BadNews.

BadNews is just that: when installed on smartphones -- like Samsung's Galaxy phone or the LG Optimus -- the bug racks up charges by repeatedly sending expensive text messages.

BadNews is also very hard to detect: according to security experts, it can remain dormant on a device for weeks without affecting performance.

Two to Nine Million Downloads So Far

It's not clear how many apps containing the BadNews bug have been downloaded. Insiders estimate that the number could be anywhere between two million and nine million copies of various Google Play applications.

BadNews can be found in a wide range of Google Play apps. Security firm Lookout says that it discovered the bug in cooking apps, home improvement apps, and games. Unsurprisingly, apps featuring adult content were also infected by BadNews.

TechCrunch reports that the most popular BadNews-infected app is "Savage Knife," a game that mimics the intense "5 Finger Filet" game seen in movies like Aliens.

It's estimated that Savage Knife has been installed on between one and five million systems so far. (Source: techcrunch.com)

All in all, about 32 different Google Play applications have been identified as infected with BadNews.

Watch Out for Aggressive Advertising

How do you figure out if your Android device has been infected? Detecting the bug can be difficult. According to Lookout, BadNews acts like an "innocent, if somewhat aggressive, advertising network." (Source: bbc.co.uk)

This means that if you start receiving information about other applications, be wary. There's a good chance BadNews is on your system and is using this method to install more malicious apps on your device.

Once installed, BadNews connects to a command and control server. From there, it can acquire a more devious version of the bug known as AlphaSMS.

Systems infected with AlphaSMS reportedly steal from victims by sending text messages using premium rate numbers.

The good news: so far, most of the BadNews activity has been limited to Eastern Europe

---

Many Home Routers Vulnerable to Attack:

By Brandon Dimmel on 20130422 in "INFOPACKETS>COM".

Do you use a Linksys, Netgear, Verizon, D-Link, or Belkin router for your home network? Then your network could be vulnerable to attack.Baltimore, Maryland-based security consultancy firm Independent Security Evaluators (ISE) says that in a test of popular home routers most were vulnerable to attack by hackers.

ISE put routers from Linksys, Netgear, Verizon, D-Link, and Belkin to the test after having installed each firm's latest firmware updates. ISE also left each router's default configurations in place when carrying out their tests.

Hackers Intercept Sensitive Information

ISE found that many of the routers were vulnerable to a "man-in-the-middle" attack. (Source: pcworld.com) As the name suggests, this type of attack involves a hacker intercepting messages without detection, meaning the communicating parties continue to exchange information without any awareness that their security has been compromised. In a successful man-in-the-middle attack, the hacker can perform a number of malicious acts, such as manipulating domain name server (DNS) settings and carrying out distributed denial-of-service (DDoS) attacks..

In many cases the routers studied by ISE required the hacker possess advanced hacking skills in order to bypass a network's security. However, the firm found that at least two routers from Belkin, the N300 and the N900, could be attacked by a hacker not in possession of authentication credentials.. In most cases, to bypass security, the hacker would have to convince a victim to click on links designed to infect the network with a malicious program.

Experts Advise Users to Change Default Passwords

Every single one of the tested routers was vulnerable to attack if the hacker accessed the network using login credentials.

Sound obvious? Not necessarily.

Many routers simply use WPA and WEP passwords visibly attached to the device. If a hacker could see passwords or acquire a list of passwords, they could use that information to access a network.That's why it's worth changing your router's default password after you buy it. (Source: digitaltrends.com) Another problem, according to ISE: in order to make a router truly secure against attack, a user must have an advanced knowledge of network equipment."Successful

mitigation often requires a level of sophistication and skill beyond that of the average user," ISE noted in its report. (Source: pcworld.com)

ISE says it has contacted Linksys, Netgear, Verizon, D-Link, and Belkin, and says that several of these firms are actively working to eliminate the vulnerabilities.

Source
:htttp://www.infopackets.com/news/security/2013/20130422_many_home_routers_vulnerable_to_attack_report.htm

---

Microsoft: Boxed Software Gone 'Within a Decade'

By Brandon Dimmel on 20130510 in "infopackets.com."

Microsoft says it expects to phase out boxed software within the next decade or so. The firm feels confident that, over the course of the next ten years, people will become more comfortable with downloading their favorite software. "We think subscription software-as-a-service is the future," Microsoft noted in a recent blog on its official Office website. "Within a decade, we

think everyone will choose to subscribe because the benefits are undeniable." (Source: pcworld.com)

Subscription-based Office 365: A Sign of What's to Come

Microsoft has already initiated the process of moving away from boxed software by offering consumers Office 365, a cloud-only version of its popular Office business suite.Rather than pay a one-time fee, Office 365 users have the option of paying subscription fees for their software. The advantage of such a system: it's constantly updated, meaning the software is built to withstand technical problems and hacker attacks.And Microsoft certainly isn't the only firm headed in this direction. Adobe recently announced plans to phase out its Creative Suite software package and focus more on developing the Creative Cloud subscription-based service. (Source: hexus.net)

In the world of video games, in which Microsoft is playing an increasingly bigger role, physical media is also slowly being phased out by digital distribution platforms like Xbox Live.

Cost, Security Concerns Remain

Of course, not everyone will appreciate this trend. Many consumers like having physical media handy in case of a web connection issue. There are also concerns that extending cloud integration makes Windows 8 more vulnerable to attack by hackers. Finally, signing up for an Office 365 subscription can result in higher fees -- even though one would expect to pay less. "Cost of ownership is far lower for me buying Office, rather than subscribing," one commenter noted on Microsoft's Office website. "So long as that remains so, I will continue to buy."

Unfortunately, that option may no longer exist in a few years' time.

Wise Youtube Downloader 1.11.49

Looking for a easy and effective way to navigate YouTube's massive video library? Then check out Wide YouTube Downloader. It lets you search the YouTube video catalog and download high-quality, high-definition videos to your system.

http://www.wisevideosuite.com

Google Now Offering 15GB Free Cloud Storage

By Brandon Dimmel on 20130514 in "infopackets.com"

Looking for more storage space in the cloud? Then look to Google Drive, which now offers 15 gigabytes (GB) for free. Until now, Google has been offering users of its Google Drive cloud storage service 5GB for free. However, the company now says it will combine its Google Drive service with Gmail and Google+ Photos and give users access to 15GB free storage.

Google Drive director of product management Clay Bavor says that consumers will no longer have to stress about freeing up space for more files.

"Use Your Storage The Way You Want"

"With this new combined storage space, you won't have to worry about how much you're storing and where," Bavor said. (Source: pcmag.com)

"For example, maybe you're a heavy Gmail user but light on photos, or perhaps you were bumping up against your Drive storage limit but were only using 2 GB in Gmail. Now it doesn't matter, because you can use your storage the way you want," he added. Google launched Google Drive last year. Since then, it has competed with other cloud storage services, including DropBox, Apple's iCloud, and Microsoft's SkyDrive (which is now highly integrated with the firm's Windows 8 operating system).

Beyond those more prominent services, there are also smaller and more specialized cloud storage options, including SugarSync, Box, and YouSendIt.

Google Ups the Ante

Google Drive's new 15GB limit puts it in a position to leech customers from those other services. After all, DropBox only offers 2GB free storage space, while Microsoft SkyDrive users gain access to 7GB free space. To access more storage space, users must pay for a subscription. For example, DropBox users face a $99 per year fee if they want 50GB of storage space.

Gartner analyst Michael Gartenberg believes Google Drive's new storage limit will put a lot of pressure on smaller cloud storage services. "[Average consumers] don't have much of a relationship with these smaller [cloud] companies," Gartenberg said. (Source: computerworld.com)

"The challenge for these smaller companies is reaching out to consumers or shifting to somewhat of a different market; the problem is that Google also wants the business market, the small business market and ultimately the enterprise IT market."

QUOTE of the month

The most basic question is not what is best, but who shall decide what is best." Thomas Sowell, posted 11/17/11

. Till next month

Your editor: Bob Murray