The people I meet.

A little while back I awoke to a beautiful Thursday morning in Brisbane, the world's best city and as it was already 5.00am, I decided to cut my morning 25km run a bit short and only complete my alternate 10km course. Normally I'd wake about 3.30am, slip on the pink lycra athletics suit with my favourite Dunlop Volleys and pound the 25km at full steam, but this morning, as I'd been up studying quantum mechanics until 2.00am, I'd slept in.

It wasn't a real problem, as I normally do about 150km a week at full pelt, I am an extraordinarily fit specimen, the envy of many, it is just that I like to stick to a routine and fitting in 10km that morning instead of my normal 25km wouldn't hurt the physique too much. Being a trained Radtech, I have, of course, a well ordered and brilliant brain and I was able to adjust mentally to the change in routine very quickly.

So it was out of bed, on with the full lycra suit (to shield the Radtechitis) some Mum under the arms, a bit of Vaseline smeared on the inside of the thighs to stop rub chaffing, then it was onto the street. I always keep a jar of Vaseline handy beside the bed in case of emergencies. As usual, most of the elderly matrons along the street were out at their front gates as I went by, pretending to gather up their newspapers but I suspect it was to catch a glimpse of my magnificence as I steamed by.

Returning home after my minor workout, as was my custom, it was into the hot shower to cleanse the body followed by a 15 minute plunge into the icy cold water in the bath, to close the pores. As, later in the day, I would be attending the monthly RAAF Vietnam midday luncheon at Fridays on the river, where I would be mixing with lesser mortals, it was necessary to mask up. Being of Radtech descent and being possibly the best the RAAF has ever had, my magnificence continuously radiates Radtechitis, an allure that is unavoidable to the female species and in order to be able to move amongst the female population without being mobbed it was necessary to cover the body with a protective coating to contain it. I've found over the years, that Johnson's Baby Oil does the job perfectly so stripped to my birthday suit, I gave myself a generous lathering.

Once protected, so as not to attract attention to myself, I dressed, making sure I wore clothing to match those also present. I then hopped into the aging Beetle and drove to the station where I caught the train to Central, walked the short distance to Fridays, found a table away from the crowd and settled in to enjoy the afternoon. Although being a magnificent Radtech, I am really a very modest and shy person and I try and remain inconspicuous by sitting apart from others. This gives them the opportunity of talking amongst themselves and not all talking at once praising me for my past endeavours.

I was protected and was looking forward to a quiet Thursday afternoon watching my friends enjoy themselves.

Unfortunately, Fridays being on the river, attracts a certain bird, commonly called a “bin chicken” or to give it it’s proper name, a white Ibis. These native to Australia birds scavenge for food-stuffs and as I had accidentally dropped some food onto the floor while eating my calamari, a couple of them were at my feet cleaning up. One was a bit over exuberant and brushed against my leg and for an instant removed a tiny amount of the protective covering of Baby Oil. A minute amount of Radtechitis escaped and was whisked away by the anabatic wind.

Little did I know that at that very moment Jillian O’Toole was at her home in far away Arana Hills working at her lathe manufacturing an automatic gearbox for her 1952 DeSoto Diplomat. Jillian had imported the car from the USA some months ago however it arrived with a 3 speed manual transmission that needed a lot of TLC and instead of spending time repairing the old “box” she decided to build a new 7 speed torque converter automatic transmission and fit it to the car. She had spent her informative years serving in the Australian Army and like many others had learned how to manufacture engines, gear-boxes, axles and other items from scratch. The Army does this in case a tank or APC gets damaged by enemy fire and parts need machining while in the field. Jillian has been known to have manufactured a complete set of tracks for a Sherman tank in less than a day while on bivouac, very handy having this sort of knowledge.

Recently she had ordered a ton of stainless rod and was busily turning down gears when that minute amount of Radtechitis arrived – being carried by the easterly breeze. She registered it immediately and her whole metabolism froze. She dropped the idler gear she had recently made, spun around 3 times trying to register from where that alluring attraction was coming. Being inside her metal workshop she was not able to decide so she scampered onto the very hot roof and hopping from one foot to the other she decided it must be coming from near the Brisbane River. Knowing how attractive it was to other females, she knew she had to get there quickly and devour as much Radtechitis as possible as quickly as possible before her sisters beat her to the punch.

Down off the roof, it was into the leathers, on with the bone-dome and onto the little postie-bike she normally keeps hidden in the lounge room, out onto the road and with the little Honda engine red-lined she headed for the city.

She headed straight for Eagle St as she rightfully assumed anyone out dining would be at one of the river-front cafes. Picking Fridays on a punt, she jammed on the brakes, but with only the front one working, with young girls screaming in terror and school children terrorised, she screeched to a halt with the rear wheel a foot off the ground.

She allowed the poor over-worked little Postie bike to drop unceremoniously to the ground and scampered up the stairs to Fridays where she spotted me sitting quietly by myself enjoying the afternoon.

She raced over and draped her arms around my person endeavouring to soak up as much Radtechitis as possible. I allowed this to continue for 57 minutes before being forced to extricate myself from her clutches.

Such is the torment a Radtech much endure.

Jilly was one of the lead riders on the recent Scooterville event, apart from being an excellent rider she has also a wicked sense of humour, was a load of fun and we all look forward to seeing her on Scootaville 2023.

C

A blond was very upset and wanted to end it all. As she held a gun to her head her boy friend began to laugh. She said to him “keep laughing you rat, you’re next”.

Did You Know?

The popular candy bar Snickers was created by Frank and Ethel Mars, of the Mars candy family, and named after their favourite horse.

The pride of Penang set to sail again.

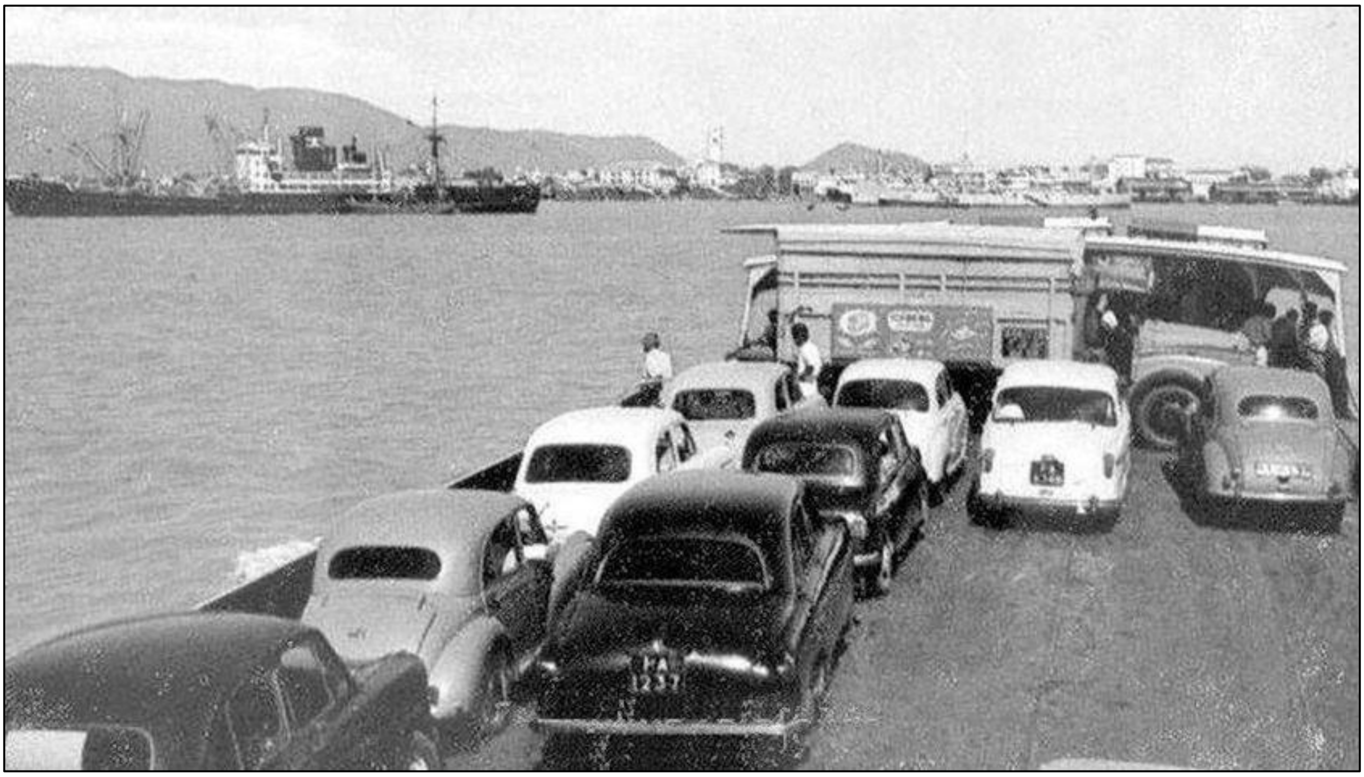
MARCO FERRARESE

The people of UNESCO-inscribed Penang island rejoiced in the last week of December 2022 after new Malaysian prime minister Anwar Ibrahim agreed to bring back the original fleet of Penang ferries in 2023. The historic double-decker ferry services connecting Penang island’s main city of George Town to Butterworth were a joy to travel on until December 31, 2020, when they ceased operations after more than 120 years. In the last few decades, the service had been largely overshadowed by the practicality of two direct bridge links to the Malaysian mainland, which opened respectively in 1985 and 2014. The people of Penang are now excited about the announced return because the old ferry service represents a tourist attraction and is part of the island’s unique character and multi-ethnic heritage.

“Back in the 1970s, the ferries were all painted in yellow, and nothing major has changed since. The only difference is that they reduced the passengers’ area to make way for more vehicles in recent years,” says Penang-born comic book artist Lefty Julian, who dedicated one-third of an exhibition, “Sama-Sama: George Town, a Multicultural Art Journey” to celebrate the ferries of yore.

D

The first Penang ferries appeared sometime between 1893 and 1894, thanks to a local Chinese entrepreneur, Quah Beng Kee. It was the only link between the island and the railway to Singapore. The original fleet consisted of three big steamers and seven smaller launches that shuttled between the Kedah Pier on the island and the Bagan Than Keel Pier in Butterworth. From 1925, cars started to be ferried across using floating decks towed by launches until a proper steam ferry vessel was introduced shortly afterwards. The Japanese occupation of Malaya during World War II disrupted services until 1945. A new prototype of bigger barges debuted in May 1957, right before the country gained independence, to accommodate the increasing need for transporting cars. With the opening of two new terminals on September 24, 1959, the Penang ferry enjoyed 25 years of unparalleled success. “There was always a long queue, and it would take about two hours to board if you came on a motorbike,” says 76-year-old Chan Mun Khee, a resident of Bukit Mertajam on Penang state’s mainland, of its 1972 maiden voyage on the Penang ferry. “It was so exciting: passengers stayed on the upper deck to enjoy the views of George Town’s skyline, while motorbikes were stored at the front of the lower deck, and cars loaded at the back.”



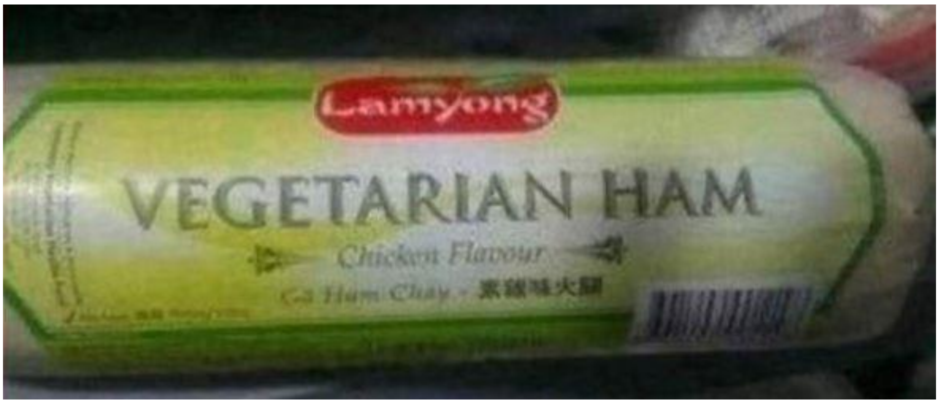
But the old world ferry couldn’t keep up with the island’s development. “At that time, the first Penang bridge to the mainland still had to be built, and the whole ferry journey by car, including embarking and disembarking, would take up to four or five hours,” says Chan. Traffic congestion became the very reason for the decline of the service. Penang’s first 13.5km-long bridge opened on September 14, 1985, under prime minister Mahathir Mohamad, marking the beginning of 35 years of slow agony for the iconic ferry service.

A couple of years back, Penang Port and the State Government announced that the six remaining historical barges from the mid-1970s and 1980s would have a full makeover. In line with the Penang Public Transport Users Association, an advocacy group for the betterment of public transport in Penang, local activists such as Khoo Salina Nasution of Penang Heritage Trust have wished that the ferries continued to cross the channel, albeit with reduced frequency. “Penang could use the old ferries like the Beaufort train in Sabah: the historic vehicles keep running, and people love the experience of riding them,” she says.

At the end of June 2021, the Penang Port Commission announced plans to upholster the old fleet and transform it into new floating tourist attractions. According to those plans, the Pulau Kapas and Pulau Payar barges will become floating seafood restaurants operated by Chuen Shin Aquaculture. The two ferries will cruise off the waters of Pulau Jerejak, an inhabited islet adjacent to the eastern coast of Penang. Two other ferries, the Pulau Undan and Pulau Talang Talang, will be equipped with restaurants, shops, conference and wedding halls and turned by Kantan Jaya Marine Services into tourist ferries for pleasure cruises around the island.

The sunken Pulau Pinang will become a Penang ferry museum moored off the Tanjung City Marina. “The main reason for changing the function of the Pulau Pinang to a museum is that its capability to keep serving passengers is now questionable,” said Tan, whose main concern is prioritising public safety. One last ferry in the fleet, Pulau Angsa, will be managed by the tourism branch of the State Government. “The preliminary concept is to refurbish this historical icon into an arts space to flourish Penang’s creative ecosystem and complement our venture in the creative terrain,” says Yeoh Soon Hin, Penang State executive councillor for tourism and creative economy.

The ferry will be a focal point for creatives to connect, collaborate and create. “Fundamentally, Penang will maintain the iconic symbolism of the ferry to uphold public sentiment while transforming it into a remarkable space to accelerate tourism development, art appreciation and expression,” Yeoh says. Both ferry terminals should be completely refurbished by August 2023.



The longer I look at this the more I understand
why aliens don’t visit us anymore.

F

Tea or Coffee? See HERE.

The 10 worst computer viruses in history.

How-To Geek

Computer virus:

Those two words instantly make us sweat and for good reason. Since the 1980s, viruses have wreaked havoc on everything from our inboxes to industrial facilities. While cybersecurity has improved, the damage done by viruses throughout history is a reminder of what these bugs can do.

It’s 1986, and you see a message on your Windows PC saying your computer is infected with a virus. To remedy the situation, you’re instructed to call brothers Basit and Amjad Farooq Alvi. At that moment, as you pick up your phone and start to dial, you immediately regret pirating the brothers’ software.

The virus was known as Brain, the first PC virus. It was technically built for the protection of software, however, the good intentions didn’t last. Soon, viruses were malicious in nature, resulting in billions of dollars of damage, identity theft, wrecked hardware…the list goes on and on.

Millions of viruses have existed since Brain in 1986 however, some have been considerably worse than others.

Melissa – 1999

In 1999, computer viruses were still a relatively new concept however, the Melissa virus, known as the fastest-growing virus of that time, quickly highlighted them as a growing concern for all. It all started when a man named David Lee Smith used an AOL account to upload a file to the internet that, when downloaded, would hijack early versions of Microsoft Word. If a user also had Microsoft Outlook, the virus would send itself via email to the top 50 people in a user’s address book.

While that may not seem like that big of a deal, it was. According to the FBI in the USA, many corporate and government email servers became overloaded and had to be shut down. In addition, internet traffic slowed to a trickle.

G

This virus did have a happy ending though. A few months after David Lee Smith was sentenced for his crime, the FBI developed its Cyber Division, which still investigates cyber crime to this day.

ILOVEYOU – 2000.

Who doesn't want to find a love letter in their inbox? Unfortunately, many Romeos and Juliets in 2000 fell victim to a virus after clicking what looked like a love letter in Microsoft Outlook. The ILOVEYOU virus (known as Love Bug back then) was technically a worm and started as a seemingly innocent email. The subject line, "ILOVEYOU," drew email users to click. Inside, a text file titled "LOVE-LETTER-FOR-YOU.TXT.VBS" was waiting.

Once the text file was opened, the worm would go on to permanently damage files such as photos and critical documents on a user's computer. Even worse, it would attach itself to all the addresses in Microsoft Outlook, spreading like wildfire. As a worm, no further human intervention was required to keep ILOVEYOU moving. As a result, millions of computers became infected in only a matter of days.

Code Red – 2001.

One of the more ominous-sounding viruses on the list, Code Red took over corporate IT in 2001 and is regarded by many as the first severe attack on a corporate system. The Code Red worm specifically targeted systems running Microsoft Internet Information Services (IIS) for Windows Server. As described in a Microsoft Security Bulletin, the attacker could use an unchecked buffer, establish a server session, conduct a buffer overrun, and execute code on the web server.

The result? Important websites would display "*Welcome to http://www.worm.com! Hacked by Chinese!*" and nothing else. The worm was also the cause of various dangerous denial-of-service (DoS) attacks.

But that ominous-sounding name? It was inspired by the drink the security employees were sipping when they found the worm: Mountain Dew Code Red.

192.168.1.1: bytes=32 time=196ms
192.168.1.1: bytes=32 time=213ms
192.168.1.1: bytes=32 time=229ms

Nimda – 2001

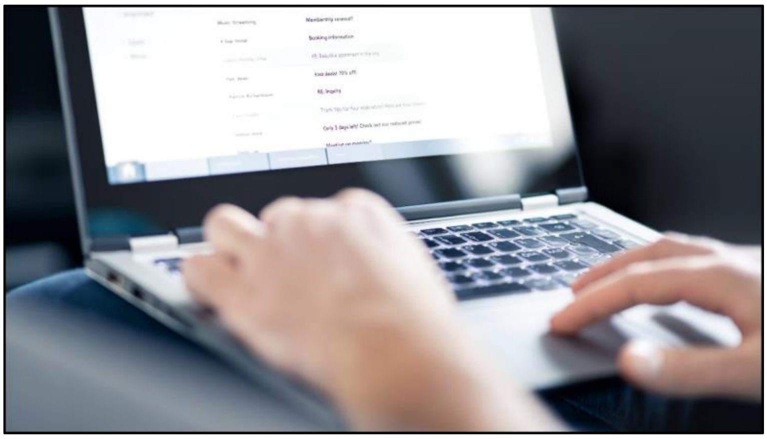
Nimda struck just a few months after Code Red and just a short time after the September 11th attacks that left us in shock. As a worm, Nimda was similar to ILOVEYOU and Code Red in that it replicated itself, however, Nimda was particularly damaging as it was able to spread in various ways, including via email and compromised websites. Nimda affected Windows operating systems and was able to modify system files and even create guest accounts.

H

Due to Nimda, millions of machines were infected and many large corporations had to shut down their networks and operations. The actual cost of Nimda has yet to be fully estimated but it was a lot.

Sobig – 2003

While opening an email may not lead to infection, email attachments are a whole other can of worms. Opening weird attachments from email addresses you don't recognize is a big no-no and while many email users today know this, things were different in 2003.



The Sobig worm infected millions of Microsoft computers via email. The threat would arrive in your inbox with a subject line like "Details" or "Thank you!" and inside, there would be an attachment just begging for a click. When clicked, Sobig would infect the computer, search for other email addresses in various computer files and then quickly replicate by sending itself to those addresses. What's worse, Sobig had multiple variants, including A, B, C, D, E, and F. The "F" variant was by far the worst of the group. In August of 2003, it was reported that one out of every 17 emails was a copy of the Sobig.F virus.

Due to its spreading capabilities, Sobig overwhelmed networks worldwide and resulted in billions of dollars in damages.

Mydoom – 2004.

"I'm just doing my job, nothing personal, sorry."

This was the email message sent by the email worm, Mydoom, first discovered in 2004 and a job it did, indeed. Mydoom quickly became the fastest-growing email worm in history. In fact, it still holds the title. Similar to Sobig and other worms on this list, Mydoom was primarily spread through email attachments. If the attachment was opened, the worm would send itself to other email addresses found in the user's address book or other local files.

The fast growth of Mydoom slowed internet traffic worldwide. At the time, it was reported that some websites were experiencing response times 8 to 10% lower than the average. Mydoom was also behind multiple DoS and DDoS attacks, including attacks against the US and South Korea.

Zeus – 2007.

Zeus, also known as Zbot, is trojan malware infecting Microsoft Windows. The malware most commonly targets financial or banking information. The first sighting of Zeus was in 2007, when the malware was found stealing information from the US Department of Transportation.

Zeus works by developing a botnet, which is a network of remote-controlled computers or bots that have been infected by malware. As a result, an attacker can control multiple computers at once. Zeus often infects a computer after a user clicks a malicious link in an email or downloads an infected file. Why is Zeus so dangerous? For example, the malware can use keylogging to capture sensitive information such as online banking passwords. In fact, in 2010, the FBI busted a crime ring that used the Zeus trojan to steal around $70 million from its victims.

Stuxnet – 2010.

Stuxnet made headlines in 2010 as the first worm developed to target industrial control systems. The worm inflicted physical damage on Iran’s nuclear facilities, particularly centrifuges. How? By exploiting vulnerabilities found within Windows to gain access to the software used to control the industrial equipment.

Stuxnet was also unique in that the worm was first introduced to computers using infected USB drives. Even now, Stuxnet is hailed as the world’s first cyberweapon.

PoisonIvy – 2011.

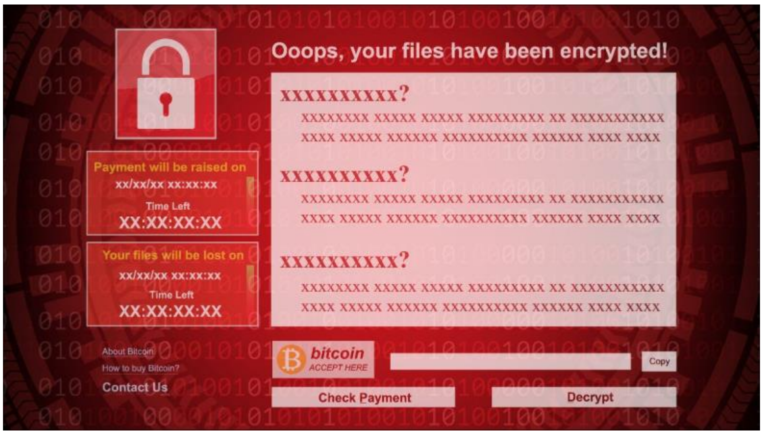
PoisonIvy does more than make its victims itch. Known as a backdoor trojan or remote access trojan (RAT), PoisonIvy is used to gain access to a victim’s computer. While PoisonIvy isn’t a virus but a type of malware, it deserves a place on the list nonetheless.

PoisonIvy was first identified in 2005. However, one of the most notable attacks using the trojan occurred in 2011. Known as the Nitro hacking attacks, PoisonIvy was used to steal critical information from chemical manufacturers, government agencies, and other organizations. PoisonIvy is dangerous because threat actors can access a computer for keylogging, screen capturing, and more. The trojan is also used to steal passwords and other critical personal information.

WannaCry – 2017.

J

The WannaCry ransomware attack took place in May 2017. The goal was simple: to hold a user's files hostage and get paid in Bitcoin. The WannaCry attack used a leaked hack known as EternalBlue to gain access to computers running Microsoft Windows. Once in, WannaCry would encrypt the computer's data then, users would see a message demanding a Bitcoin payment for the release of their files.



Ooops, your files have been encrypted!

Payment will be raised on xx/xx/xx xx:xx:xx Time Left XX:XX:XX:XX

Your files will be lost on xx/xx/xx xx:xx:xx Time Left XX:XX:XX:XX

Unfortunately, WannaCry did have its victims. In 2017, the damage was estimated to be in the billions. Even today, WannaCry still exists, highlighting the importance of protecting ourselves from ransomware.

The computer virus is alive and well

As technology evolves, so does the work of cybercriminals. While you may see the years listed above and get the impression that viruses are a thing of the past, that couldn't be further from the truth.

Serious threats such as ransomware are alive and well. The best thing you can do? Protect yourself. Even the most basic security practices can help prevent viruses from infecting your devices.

So let me get this straight, I go to Coles and buy:

- A kilo of sliced ham wrapped in plastic
- A loaf of sliced bread wrapped in plastic
- A litre of milk in a plastic bottle
- A ready made meal in a plastic container.
- A litre of yoghurt in a plastic container
- A bottle of tomato sauce in a plastic container.

But they won't give me a plastic bag to carry it home because the plastic bag is bad for the environment?

How to protect yourself from Ransomware.

Ransomware is a type of malware that tries to extort money from you. There are many variants, starting with CryptoLocker, CryptoWall, TeslaWall, and many others. They hold your files hostage and hold them for ransom for hundreds/thousands of dollars.

K

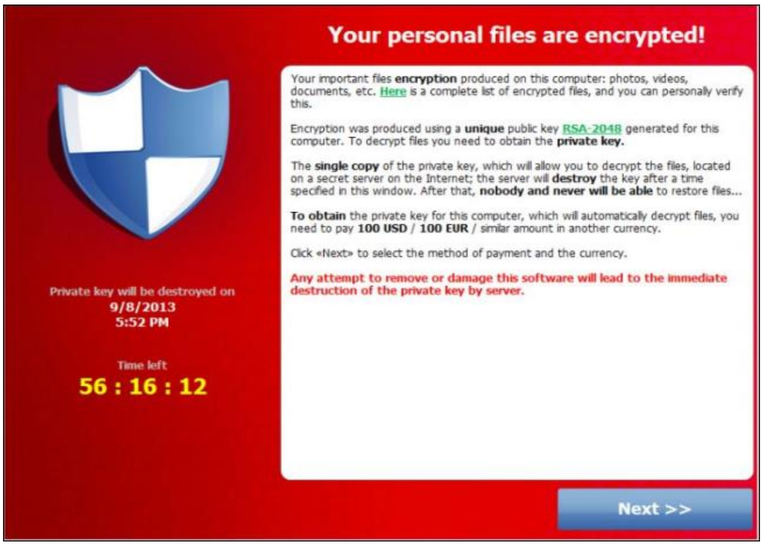
Most malware is no longer created by bored teenagers looking to cause some chaos, much of the current malware is now produced by organized crime for profit and is becoming increasingly sophisticated.

How ransomware works.

Not all ransomware is identical. The key thing that makes a piece of malware “ransomware” is that it attempts to extort a direct payment from you. Some ransomware may be disguised, it may function as “scareware,” displaying a pop-up that says something like “Your computer is infected, purchase this product to fix the infection” or “Your computer has been used to download illegal files, pay a fine to continue using your computer.”

In other situations, ransomware may be more up-front. It may hook deep into your system, displaying a message saying that it will only go away when you pay money to the ransomware’s creators. This type of malware could be bypassed via malware removal tools or just by reinstalling Windows.

Unfortunately, Ransomware is becoming more and more sophisticated. One of the most well-known examples, CryptoLocker, starts encrypting your personal files as soon as it gains access to your system, preventing access to the files without the encryption key. CryptoLocker then displays a message informing you that your files have been locked with encryption and that you have just a few days to pay up. If you pay them $300, they’ll hand you the encryption key and you can recover your files. CryptoLocker helpfully walks you through choosing a payment method and, after paying, the criminals seem to actually give you a key that you can use to restore your files.



Your personal files are encrypted!

Private key will be destroyed on
9/8/2013
5:52 PM

Time left
56 : 16 : 12

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **100 USD** / **100 EUR** / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

You can never be sure that the criminals will keep their end of the deal, of course. It’s not a good idea to pay up when you’re extorted by criminals. On the other hand, businesses that lose their only copy of business-critical data may be tempted to take the risk — and it’s hard to blame them.

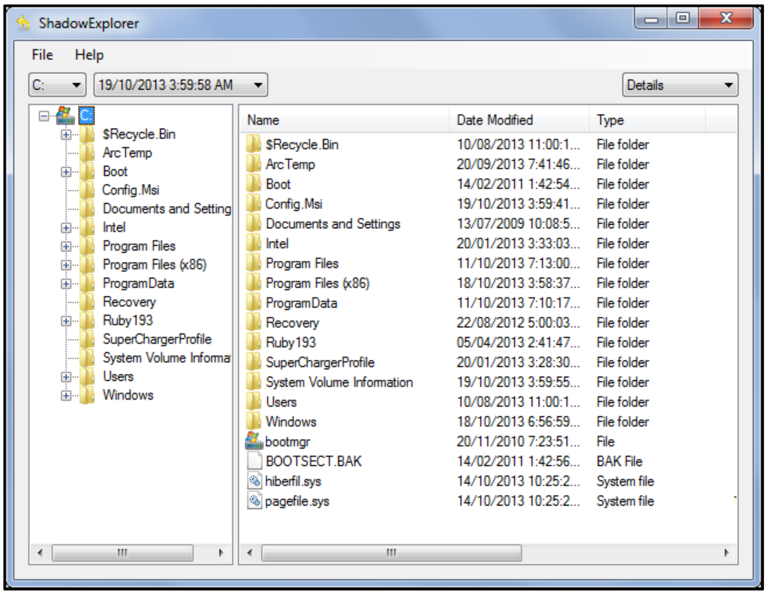
Protecting your files from ransomware.

This type of malware is another good example of why backups are essential. You should regularly back up files to an external hard drive or a remote file storage server. If all your copies of your files are on your computer, malware that infects your computer could encrypt them all and restrict access — or even delete them entirely.

When backing up files, be sure to back up your personal files to a location where they can't be written to or erased. For example, place them on a removable hard drive or upload them to a remote backup service like CrashPlan that would allow you to revert to previous versions of files. Don't just store your backups on an internal hard drive or network share to which you have write-access. The ransomware could encrypt the files on your connected backup drive or on your network share if you have full write-access.

Frequent backups are also important. You wouldn't want to lose a week's worth of work because you only back up your files every week. This is part of the reason why automated back-up solutions are so convenient.

If your files do become locked by ransomware and you don't have the appropriate backups, you can try recovering them with ShadowExplorer. This tool accesses "Shadow Copies," which Windows uses for System Restore — they will often contain some personal files.



C: 19/10/2013 3:59:58 AM Details

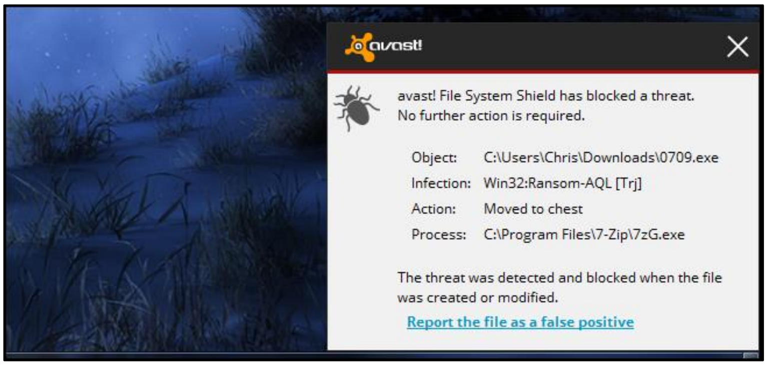
Name	Date Modified	Type
$Recycle.Bin	10/08/2013 11:00:1...	File folder
ArcTemp	20/09/2013 7:41:46...	File folder
Boot	14/02/2011 1:42:54...	File folder
Config.Msi	19/10/2013 3:59:41...	File folder
Documents and Settings	13/07/2009 10:08:5...	File folder
Intel	20/01/2013 3:33:03...	File folder
Program Files	11/10/2013 7:13:00...	File folder
Program Files (x86)	18/10/2013 3:58:37...	File folder
ProgramData	11/10/2013 7:10:17...	File folder
Recovery	22/08/2012 5:00:03...	File folder
Ruby193	05/04/2013 2:41:47...	File folder
SuperChargerProfile	20/01/2013 3:28:30...	File folder
System Volume Information	19/10/2013 3:59:55...	File folder
Users	10/08/2013 11:00:1...	File folder
Windows	18/10/2013 6:56:59...	File folder
bootmgr	20/11/2010 7:23:51...	File
BOOTSECT.BAK	14/02/2011 1:42:56...	BAK File
hiberfil.sys	14/10/2013 10:25:2...	System file
pagefile.sys	14/10/2013 10:25:2...	System file

How to Avoid Ransomware.

Aside from using a proper backup strategy, you can avoid ransomware in the same way you avoid other forms of malware. CryptoLocker has been verified to arrive through email attachments, via the Java plug-in and installed on computers that are part of the Zeus botnet. Use a good antivirus product that will attempt to stop ransomware in its tracks. Antivirus programs are never perfect and you could be infected even if you run one, but it's an important layer of defence.

Avoid running suspicious files. Ransomware can arrive in .exe files attached to emails, from illicit websites containing pirated software, or anywhere else that malware comes from. Be alert and exercise caution over the files you download and run.

Keep your software updated. Using an old version of your web browser, operating system, or a browser plugin can allow malware in through open security holes. If you have Java installed, you should probably uninstall it.



avast! File System Shield has blocked a threat.
No further action is required.

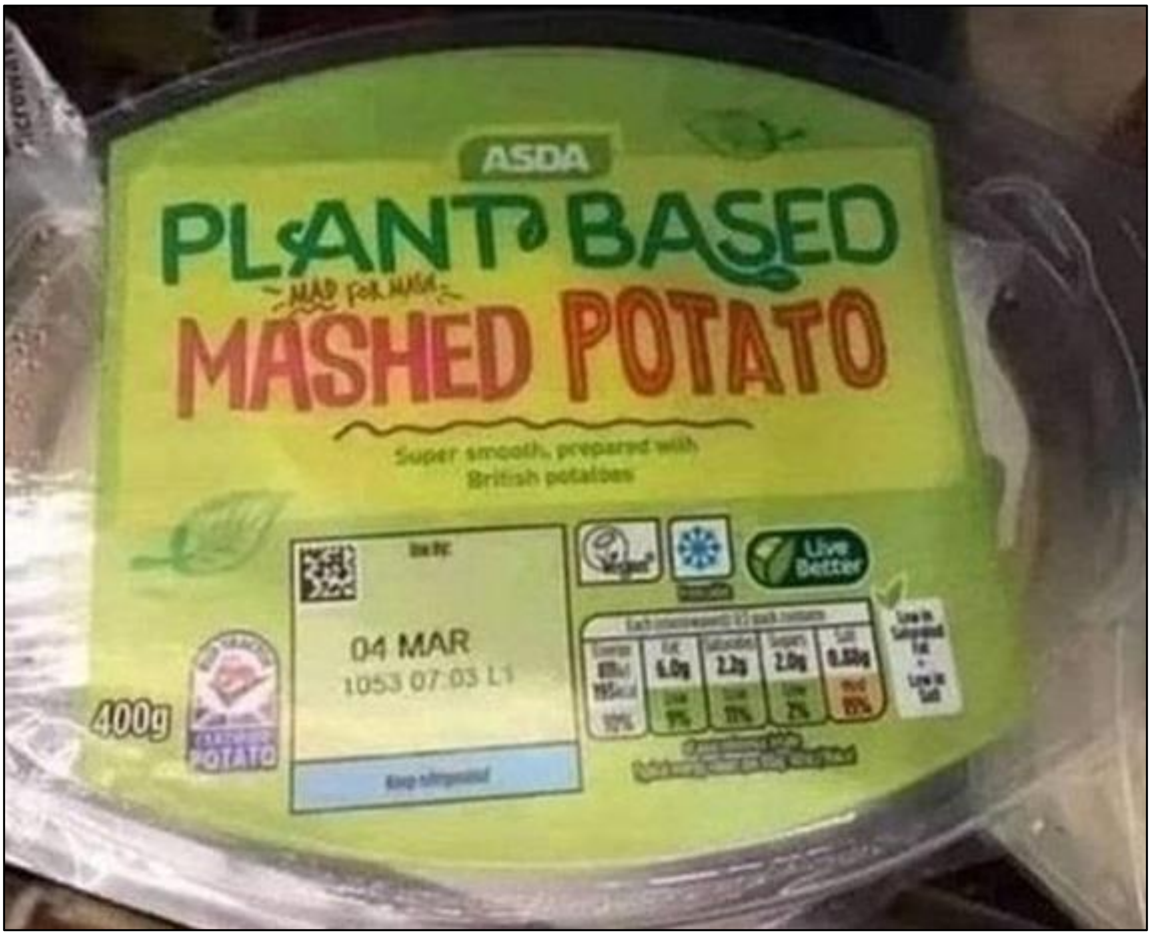
Object: C:\Users\Chris\Downloads\0709.exe
Infection: Win32:Ransom-AQL [Trj]
Action: Moved to chest
Process: C:\Program Files\7-Zip\7zG.exe

The threat was detected and blocked when the file was created or modified.

Report the file as a false positive

Ransomware, CryptoLocker variants in particular, is brutally efficient and smart. It just wants to get down to business and take your money. Holding your files hostage is an effective way to prevent removal by antivirus programs after it's taken root, but CryptoLocker is much less scary if you have good backups.

This sort of malware demonstrates the importance of backups as well as proper security practices. Unfortunately, CryptoLocker is probably a sign of things to come, it's the kind of malware we'll likely be seeing more of in the future.



Every year billions of innocent potatoes are ripped from their families and brutally abused. But no more! Scientists at ASDA revealed today that they have found a way to create mashed potato made entirely from plants.