The market for exploiting software vulnerabilities can be traced back to the 90s where "phreaking" - modifying telecommunications technology - was popular.Jennifer/Flickr, CC BY-SA

The attack of ransomware “WannaCry” has put governments and businesses around the world on edge, but in fact the underground market for exploit or software vulnerabilities bugs like this has been an existence at least since the 1990s.

Informal sharing of these vulnerabilities goes back to the dawn of computing - notably phone “phreaking” - tinkering with telecommunication devices and the Massachusetts Model Railway Club credited with the early fostering of a hacker sub-culture from the 1960s onwards.

From here it slowly developed into a global market in the sale of exploits and exploit kits. This included hacking tools such as Blackhole, Zeus and Spyeye – sometimes known as “script kiddies” because the programming skills required are basic and the hacks more or less delivered via a menu-driven program.

The Russian carding market, which developed in the 1990s as online forums for the sale of stolen credit cards and identities, morphed into a sophisticated business enterprise. It mimicked online legal markets such as eBay. In short these criminals industrialised.

The Australian Communication Media Authority’s Spam Intelligence Database showed that spam-distributed malware, with the capability of locking data-files on an exposed computer system, begun to appear in 2012 with many cases reported in 2013 onwards.

The modern malware market

The industrialisation of the cybercrime market developed rapidly with the advent of virtual private networks (VPNs) and The Onion Router or “Tor” for short in the

mid-2000s. The
UNODC’s 2013 Comprehensive Report on Cybercrime
flagged the importance of these markets in the spread of monetised hacking tools.

The RAND corporation’s report on the Hacker’s Bizarre in 2014 notes:

These black markets are growing in size and complexity. The hacker market — once a varied landscape of discrete, ad hoc networks of individuals initially motivated by little more than ego and notoriety — has emerged as a playground of financially driven, highly organized, and sophisticated groups….Black and gray markets for hacking tools, hacking services, and the fruits of hacking are gaining widespread attention as more attacks and attack mechanisms are linked in one way or another to such markets.

The Australian Cyber Security Centre’s 2015 Threat report highlights the emergence of cybercrime as a service, introducing new business models to cybercriminals, and increasing their spread and sophistication. The FBI's Cybercrime Division prosecutor, Gavin Corn, observed that networking among criminal groups has been greatly enhanced by the emergence of new encrypted applications:

Cybercrime wasn't even a part of organized crime before, and now it's the epitome of it.

The evolution of the internet has also seen the rapid take up of encrypted and anonymous technology.

The value of this underground market today is guessed to be in the hundreds of millions. Some vulnerabilities have been reportedly sold for as much US$900,000 recently . Higher prices are paid for the more secure systems such Apple iOS – iphones and so on, but lower fees for older legacy operating systems like Windows XP.

The market operates in an orderly way with testing and evaluation prior to purchase. It's similar

to the carding business in that it seeks to create a stable reliable service encouraging repeated use.

Don’t just blame the black market

When it comes down to the effectiveness of the products - malware, ransomware - where the underground market drops off, businesses with lax security are most at risk.

Legitimate penetration testing by cyber-security companies as well as national security agencies wanting to improve cyber arsenals for offensive purposes also have had a role in boosting the value of exploits. The secret acquisition of exploits leaves many users unaware of the “bug” and thwart legitimate bug bounty projects.

In reality, any enterprise in e-commerce or dependent on the internet should also be a security company. Intrusions that target confidential data or service delivery are now common and can devastate trust in the business.

A stand out problem is the presence of legacy computing systems or applications with old operating systems that are no longer supported by the vendor. The Windows XP operating system is a good example and exploits frequently target these older systems.

It’s estimated that half of all web pages still run on the old unsecure http script, rather than the more secure https, now the industry standard. This legacy of older web page formats, leaves everyone exposed to the risk of being compromised by cybercriminals. These criminals hijack websites and create fake website addresses to redirect victims to such sites in order to unwittingly download a virus such as a Trojan or other malware.

The mass distribution of the “WannaCry” ransomware signals the shift of ransomware intrusion techniques from a specialist or individually tailored mode of cybercrime, to one capable of simultaneously targeting many vulnerable computer systems or networks. Coupled with the creation of large scale botnets (a network of computers that can be controlled remotely), often designed to deliver mass-spam emails or social media messages, the scale of these events grows.

At best attacks on this scale have been described as “weapons of mass annoyance” – disruptive but not fatal. The emergence of campaign style attacks is now common place.

They are capable of delivering well designed social engineered messages that trick users into visiting a compromised webpage and inadvertently downloading an executable file that locks up data. In other attacks, hidden programs that log keystrokes or manipulate the computer’s operating system can be implemented via unpatched bugs in many older systems.

The notion of the “digital divide”, where some have access to certain technology and others don’t, has the additional dimension of security as well. Consumers and enterprises constantly reviewing the trustworthiness of their online exchanges becomes more difficult than ever, as cybercriminals can easily duplicate perfect examples of well known trusted enterprises.

Roderic Broadhurst does not work for, consult, own shares in or receive funding from any company or organisation that would benefit from this article, and has disclosed no relevant affiliations beyond the academic appointment above.

Read more http://theconversation.com/what-the-underground-market-for-ransomware-looks-like-77703