The Evolution of Cyber Threat and Defence

Since the existence of computer networks, hackers have exploited network-provided services for notoriety or personal gain. The exploitation of these systems has only grown, and in an increasingly connected world never more have networks, services, or devices been exposed to this risk.

In a threat landscape where security products continually have to be refined or updated to detect the latest exploitation, the challenge is to find a solution which offers a future proof defence to provide enduring network protection.
One of the earliest hackers to gain notoriety was Californian based Thomas Draper. Working under the alias of Captain Crunch, he exploited a vulnerability in telephone systems in the US in the early 1970s. He generated a specific audible tone down the line to make free calls – a technique which became known as phone phreaking.

In the late 1970s, Kevin Mitnick, aged just sixteen, gained unauthorized access to Digital Equipment Corp (DEC) and the computer network used for developing their RSTS/E operating system software. Mitnick broke into DEC’s network and copied its software, a crime he was convicted of in 1988. Such was the concern at this attack that US law enforcement officials kept Mitnick in solitary confinement for a time, convinced that Mitnick could “Start a nuclear war by whistling into a pay phone”.

Enter the 1990s, and systems administrator Gary McKinnon, carried out the “biggest military computer hack of all time”. Known as Solo, McKinnon is accused of hacking into 97 US military and NASA computers from a residential property in London. The US authorities accused him of deleting critical files and operating systems which shutdown the US Army’s district of Washington network of 2,000 computers. The total bill claimed by the US authorities to correct the damage caused exceeded $700,000.

Whether an individual’s skill in compromising systems lay in social engineering or in the use of a combination of brute force techniques and sophisticated hacking tools, the availability of exploits has become prolific. The complexity of these exploits has become ever more advanced and yet at the same time easier to execute.

**Counter Attack**

In response to the continual evolution of network-based threats, the security technology developed to defend systems against malicious activity has also evolved. In the late 1980s it was thought by many technology experts that “a good firewall was good enough”. This was the case until it was demonstrated that attacks such as web-based exploits and brute force password attacks would pass straight through these security devices unhindered.

The development of Intrusion Detection Systems (IDS) soon followed and in the mid 1990s these packet sniffing devices were widely adopted. IDS systems work by comparing traffic against a signature or rule set in an attempt to identify malicious behaviour. Of course, hacking techniques soon evolved to mask malicious activity from IDS systems, quickly rendering them of little practical use.

The next evolutionary phase of network defence in early 2000 saw the development of Intrusion Prevention Systems (IPS). These still relied mainly on an ever increasing list of signatures or rules to identify malicious activity in network traffic. However, in this incarnation the devices were inline and

---

**1988**

**Morris Worm** was considered to be the first worm and one which also resulted in the first conviction under the US Computer Fraud and Abuse Act.

**1999**

**Melissa** spread by emailing itself to 50 address in a victim’s Outlook address book and as a result spread faster than any previous virus. Designed to infect macros in word processing documents (Microsoft Word 97 / 2000) it was relatively benign and could have done significantly more damage. Its creator, David Lee Smith, was sentenced to 20 months in prison and fined $5,000.
had the ability to drop or block traffic in response to identifying threats or other malicious activity. Some of these systems also had the ability to counter evasion techniques including fragmentation, segmentation and encoding.

**New Generation of Cyber Defence**

During the mid to late 2000s, the availability of more complex attack tools became widespread and attack platforms capable of executing hundreds of attacks against vulnerable systems were readily available. These attack platforms were able to deliver a new type of attack, known as ‘Buffer Overflows’, against a vulnerable machine and inject payloads that would execute during a successful attack. When used in combination with multiple security evasion techniques, many Intrusion Prevention Systems (IPS) were found to be less effective than vendors claimed.

Today, there is a variety of readily downloadable scripts and compiled code capable of executing highly complex attack scenarios. This, combined with security evasion techniques requires a new generation of cyber security defence.

Of course, identifying and blocking the ‘known’ attack will always have its place, but systems will need to evolve to meet the complexity of today’s malicious activity. This requires identifying mutated or evolved ‘known’ exploits, as well as identifying new threats yet to be classified and blocked by traditional security defence solutions.

A new generation of cyber defence solutions is therefore emerging to meet today’s threats. These sophisticated systems are capable of gathering transmission characteristics from network devices and generating their own behavioural intelligence. This enables complex queries to be run to identify device or user behaviour that is indicative of a threat or other malicious activity.

These systems operate by looking for transmission characteristics in network traffic that are so unusual when compared with the majority of usual or benign traffic. The traffic is then further scrutinised for behavioural characteristics which may be indicative of a threat. For example, if a machine is identified as accepting a new connection and then immediately establishes a high volume of multiple simultaneous connections to external addresses, which have not been communicated with historically, this behaviour would be identified by a next-generation system as malware execution and propagation.

This new capability to apply powerful and complex queries against current and historical device and user behaviour is highly effective at identifying behaviour indicative of malicious activity. It has also been proven to identify botnet activity, beaconing and the stealthy exfiltration of data over long periods of time.

---

**ILOVEYOU** was considered to be one of the most damaging worms. Starting in the Philippines it rapidly spread by using all contacts in a the victim’s Outlook address book and infected more than fifty million computers in just 10 days. It is estimated to have cost at least $5 billion in damages worldwide.

**Code Red** targeted Microsoft Windows operating systems by exploiting zero-day flaws. Once compromised this worm attacked industrial Programmable Logic Controllers and is report to have ruined almost a fifth of Iran’s nuclear centrifuges.

**Stuxnet** targeted Microsoft Windows operating systems by exploiting zero-day flaws. Once compromised this worm attacked industrial Programmable Logic Controllers and is report to have ruined almost a fifth of Iran’s nuclear centrifuges.

**The Evolution of Cyber Threat and Defence**

2000

Code Red

infected more than 350,000 computers running the Microsoft IIS web server and at its peak compromised 2,000 computers per minute.
Extending Intelligence

It is clear to see that the highest levels of network-based cyber defence can only be achieved by an intelligent, blended technology that has the capability to identify both the ‘known’ and the ‘unknown’ (mutated or evolved) malicious activity, that traditional systems inhibited by a signature and rule set architectures cannot.

Perception™ by Chemring Technology Solutions, is the world’s first bio-inspired behavioural cyber defence system that utilises this blended approach to achieve the highest rates of ‘known’ and ‘unknown’ threat and malicious behaviour recognition.

Perception™ is not inhibited by traditional signature or rule set architecture, but instead uses a bio-inspired cognitive process, similar to that exhibited in humans, to process high volumes of network communication to expose only activity that is highly indicative of a threat or other malicious behaviour.

About Chemring Technology Solutions

Chemring Technology Solutions, based in Hampshire and Dorset, is the principal electronics research and development centre of Chemring Group. Comprising of Roke Manor Research Ltd and Chemring EOD Ltd, Chemring Technology Solutions is one of the UK’s leading suppliers of innovative solutions, product development and contract R&D. With more than 400 patents, it has a heritage of pioneering developments in electronic sensors, networks and communications technology.

Heartbleed is a ‘buffer over-read’ vulnerability in a component used to provide communication security over the Internet. At the time of discovery an estimated 17% of secure web servers were vulnerable to the attack.

Shellshock is a security bug in the widely used Unix shell called Bash. Used in many web servers this vulnerability, which has existed since around 1992, allows an attacker to gain access to a computer system.