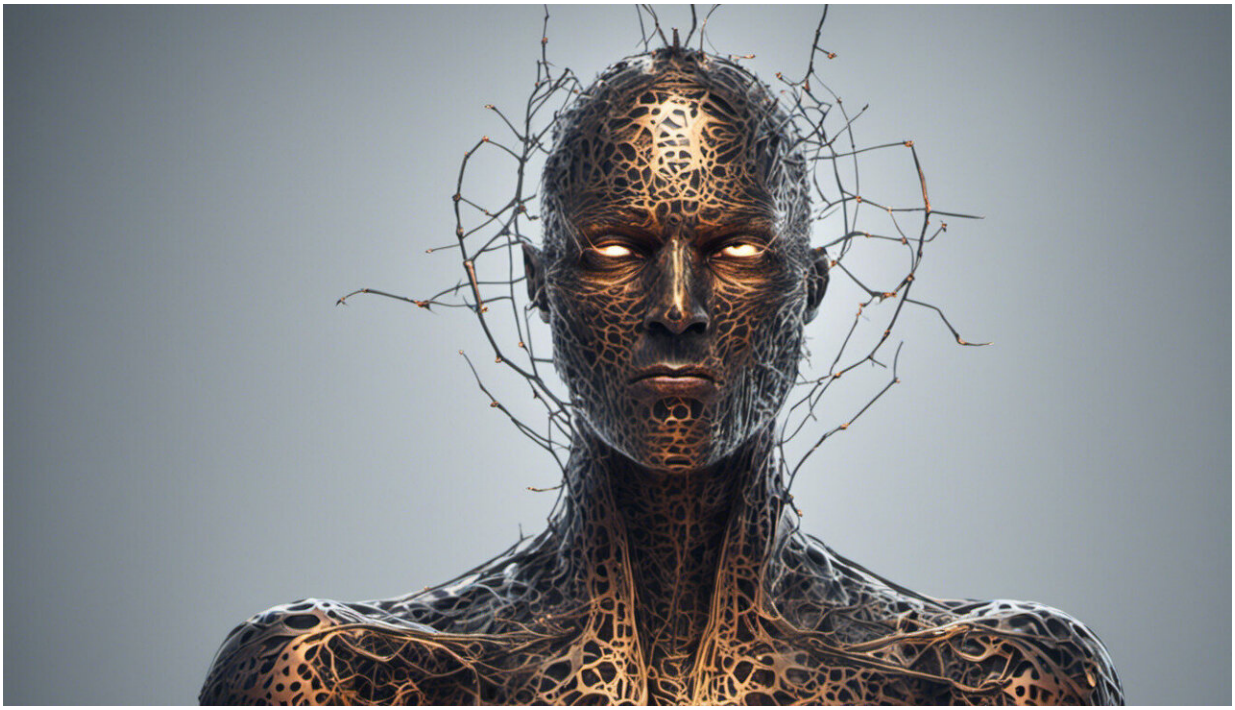
Human and technical ingenuity will be required to defeat shape-shifting malware

April 16 2015, by John Walker



Credit: AI-generated image (disclaimer)

The FBI and Europol recently brought down a criminal botnet – a network of remotely-controlled PCs – powered by Beebone, an advanced, polymorphic malware capable of shape-shifting up to 19 times a day to prevent detection by antivirus scanners.

By cutting off the command and control (C&C) servers used to issue commands to Beebone, the malware could be more easily located and removed. This particular botnet incorporated around 12,000 infected PCs, but researchers estimate Beebone has infected another 5m computers worldwide.

Widespread use of polymorphic software is a major change in the computer security arms race. In fact it's Beebone's polymorphism that has allowed it to remain a continual threat since it appeared way back in 2009.

The first virus

The story of the computer virus or what we now call malware began in 1983, when Fred Cohen wrote a parasitic program that seized control of computers. This was the first computer virus and the first use of the term. Cohen's test was soon followed by the work of a 15-year-old teenager who wrote Elk Cloner, the first widespread virus which targeted the Apple II computer via the floppy disk.

It's been a long road since then, with malicious software escalating in capability and complexity resulting in all manner of damage and embarrassing incidents. The infamous Robert Morris Jnr worm in 1988 saw its creator accidentally cripple the early academic internet, for which he received a US$10,000 fine. Fifteen years later in 2003 the Slammer worm crippled the modern internet, practically knocking South Korea off the net. Governments have also got in on the act with Stuxnet and all manner of software used by the NSA and GCHQ as revealed by Edward Snowden's leaked files.

Clusters Found by the McAfee Labs Sample Harvester	
Visual Basic Code Hash	Number of Samples
e9e18926d027d7edf7d659993c4a40ab	934
2381fb3e2e40af0cc22b11ac7d3e3074	540
d473569124daab37f395cb786141d32a	500
7738a5bbc26a081360be58fa63d08d0a	379
d25a5071b7217d5b99aa10dcbade749d	362
7856a1378367926d204f936f1cfa3111	353
13eae0e4d399be260cfc5b631a25855d	335
987e0ad6a6422bec1e847d629b474af8	335
0988b64de750539f45184b98315a7ace	332
63463a5529a2d0d564633e389c932a37	320

File signature comparison reveals many different variants of the virus, all widespread. Credit: McAfee

An arms race escalation

However, one of the most significant changes in the malware landscape was the arrival of one the first polymorphic viruses – the 1260 virus – around 1990. The 1260 virus could change its signature, which hides the

appearance of the file to scanners such as antivirus program. It did this by encrypting and decrypting parts of itself while inserting randomly-generated garbage code, which had the effect of padding the size of the file, altering its signature to avoid detection.

The shape-shifting AAEH or Beebone malware arrives as an obfuscated (disguised) piece of Visual Basic code. By faking its identity as an unthreatening file type it tempts the user to run it, using Windows security flaws to gain privileged access (administrator rights) over the machine.

In order to make detection more difficult, its two internal components can each download variants of the other from C&C servers. This makes it harder to detect as each component must be a known version for antivirus scanners to detect the malware correctly. Once the Beebone agent has taken control, those operating it over the internet can send further instructions to the Beebone agent, for example whether to download other malware such as hacking tools, Trojans, keyloggers, or even ransomware such as Cryptolocker.

Computer exploits such as hacking into systems or writing viruses were in the early days chiefly for gaining notoriety more than anything else. But in the last decade the growth of the net and its reach into most parts of society has brought with it criminals looking to profit. Cybercriminal attacks are now estimated to net US$445 billion each year in illicit revenue. Obviously, where there's money to be made there will be people who will invest – in this case organised crime prepared to pay for the best tools for the job.

Police and investigators have had some success in countering the threat, shutting down several botnets over the last few years. But ultimately with each botnet shut down another springs up to take its place – constructed from software and other people's compromised computers, a botnet used

for criminal means is inherently expendable.

Defences must evolve too

The solution of deploying antivirus scanners to detect and remove malware is looking more and more out of date, as malware grows more capable of defending itself. Beebone, for example, can prevent efforts to remove it by blocking the internet addresses of known security and anti-virus software firms, and preventing anti-virus software from running.

The speed with which so-called zero-day-exploits – security holes known only to those who discovered them, and not the creator of the software – can spread before patches to provide adequate protection can be written has increased with the internet. This means it's possible to compromise many, many machines before knowledge of the exploit is even public.

There is more to defence now than antivirus scanners alone, and perimeter defences and other forms of intrusion detection systems are able to detect suspicious network traffic rather than just suspicious files. Nevertheless with imaginative and ingenious criminal and programming minds at work, it's really only skilled and experienced human talent that provide the awareness required – technology alone cannot offer a total solution.

We've come a long way since floppy disk viruses were created for fun not profit, but the angles of attack have changed and our defences must change with them.

Source: The Conversation