AUTOMATED DEFENCE SYSTEMS

Nicola Whiting *argues that governments must look to automated defence systems to combat the rise in cyber-crime groups and nation-state hackers using automated tools to launch attacks*

The implications of recent developments are clear: easily accessible, automated software is enabling even amateurs to conduct sophisticated cyber attacks just as the pipeline of specialists needed to protect against them is perilously low.

Recent reports show that hackers have been using automated tools to dramatically simplify and multiply sophisticated cyber attacks on public sector organisations, critical national infrastructure and governments. This has not only dramatically increased the number of attacks, but also the number of potential attackers as automated hacking tools now allow individuals to carry out sophisticated attacks with very little prior knowledge or skills.

A SHORTFALL OF 1.8 MILLION CYBER SECURITY WORKERS BY 2022 IS CURRENTLY PROJECTED

The array of autonomous tools now in widespread circulation includes automated distributed denial of service (DDOS) 'stressor' tools that bombard networks with data until they crash, 'exploit kits' that attack unpatched 'zero-day' vulnerabilities and software that can autonomously 'hopscotch' across and attack different Internet of Things devices. With nation states and criminal gangs dedicating time and resources to developing and 'copying' advanced malware, some of which is inevitably leaked on to the black market, the number of advanced automated threats is increasing at an alarming rate.

At the same time, the supply of human talent needed to find and patch cyber security vulnerabilities is far less than the demand as businesses of all shapes and sizes become more cyber security aware. (ISC)2's 2017 Global Information Security Workforce Study, the largest ever survey of the global cyber security workforce, recently painted a picture of a growing cyber security skills shortage with a projected shortfall of 1.8 million cyber security workers by 2022.

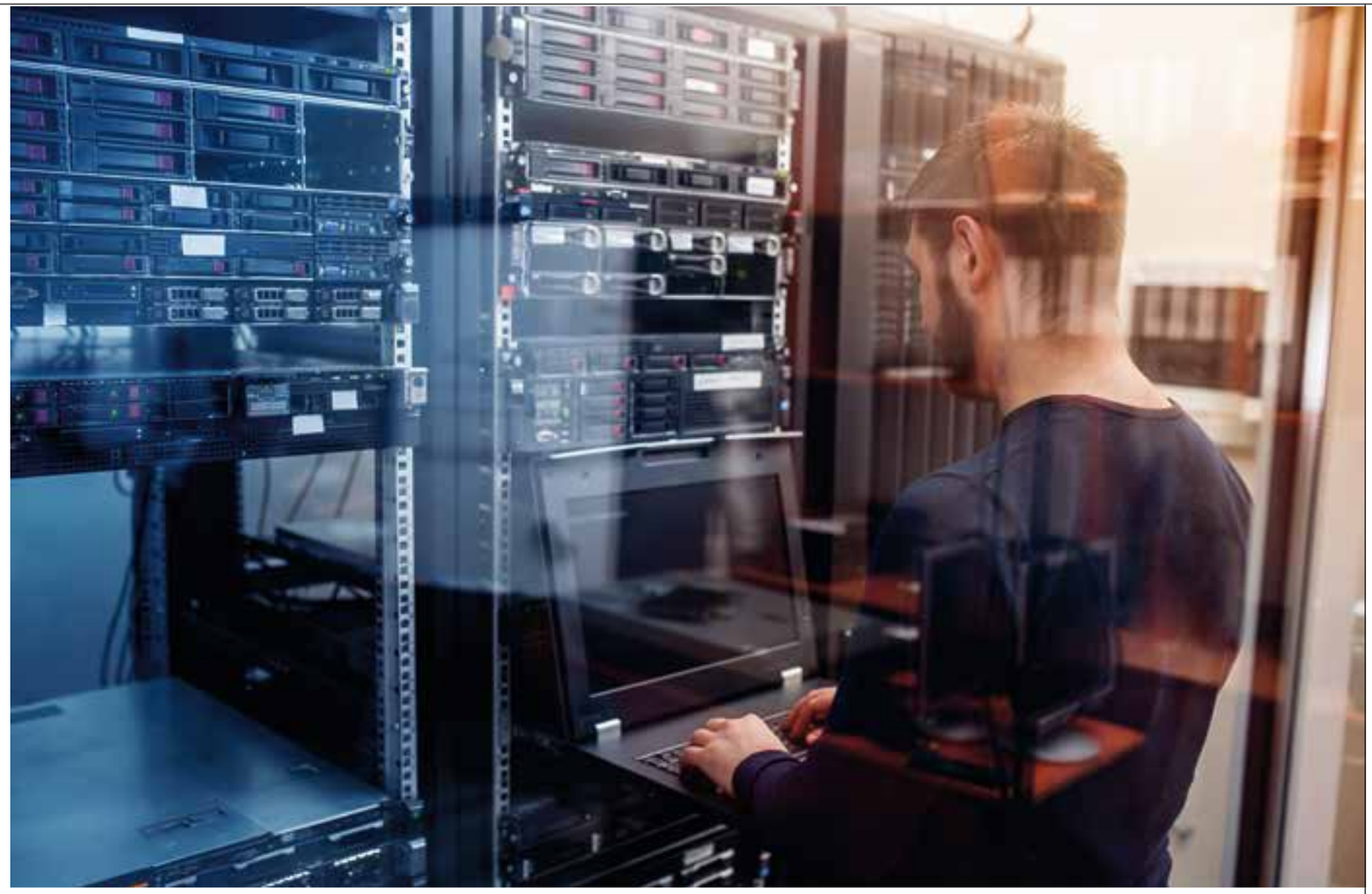
The fundamental problem is that machines are faster, cheaper and more efficient than people at finding and exploiting online vulnerabilities. As a result, sophisticated cyber attackers, including nation-state hackers, are increasingly turning to intelligent software to dramatically cut the cost and manpower needed to launch assaults on society. Nation-state hacking teams are employing automated custom-made and even open-source software as a means to carry out 'early-stage' surveillance and seek vulnerabilities in future targets efficiently and at low cost. Cyber crime syndicates and nation-state attackers are also turning to automated tools because they make it easier to cover their tracks and reduce traceability.

Hackers sometimes use open-source software to disguise malicious surveillance because open-source software is so widely used that it is difficult to discover who is behind the attack or what their intentions are. In addition, nation states sometimes covertly distribute sophisticated state-manufactured attack tools to non-state actors such as cyber crime gangs, enabling governments to outsource sophisticated attacks to surrogate groups. Admiral Michael Rogers, US Cyber Command Chief and Director of the National Security Agency warns of: "Nation states using surrogates as a way to overcome our capabilities in attribution". Criminals often subsequently clone sophisticated malware (malicious software) from hostile states and use it in extortion and criminal enterprise.

BLURRED LINES

In this way, the line between government and non-government attackers becomes increasingly blurred as automated hacking tools find their way into criminal hands, transferring state-level expertise to a myriad of surrogate and renegade attackers. The cloning of sophisticated automated cyber-attack tools also means advanced hacking methods are no longer the preserve of those with nation state-level resources, but can be deployed even by amateurs.

Autonomous hackers can wreak chaos at a greater speed and scale than humans. The famous Stuxnet worm, which severely damaged Iran's nuclear weapons programme, was the first-known autonomous threat to target and sabotage entire industrial control systems on a massive scale.



Picture credit: Titania

By automating defence systems, skilled IT experts can focus on more strategic cyber security applications

Studies have since shown how an automated worm can infect connected light bulbs and then 'jump across' and contaminate all neighbouring light bulbs, spreading like wildfire to knock out or control thousands of lights across cities. Recently, a more sophisticated malware attack even disabled Ukraine's national power grid.

Nation states often carry out Advanced Persistent Threat (APT) attacks by mapping out the network architecture, domains, servers and IP addresses of their potential victims and creating specialised software tools customised for each target. These automated tools can then autonomously lay low, gather sensitive information and delete or encrypt vital data.

Cleverly designed malware can even lie dormant inside infrastructure or organisations for months and conduct covert surveillance, like a robotic 'sleeper cell', extracting sensitive information to prepare the ground for a future attack. A recent investigation showed the UK's national rail network had been unwittingly infiltrated by four nation state cyber attacks, which appeared to be exploratory infiltrations.

Groups within Russia and China have been credited with deploying very advanced automated malware tools alongside off-the-shelf tools as part of their arsenal of offensive cyber weaponry. Chinese hackers generally focus on developing tools to snoop on sensitive executive discussions and steal business IP in order to gain an advantage for strategic sectors of its economy. Groups within Russia are suspected of using automated tools to attack energy infrastructure. And some nation states have developed invisible 'fileless malware' which, unlike signature-based malware, attacks and resides in the target's memory, just as 'stealth bombers' leave no radar signature. A Kaspersky lab report found that up to 140 banks were recently infected with this memory-based stealth technology.

All the evidence indicates that these sophisticated tools are now falling into criminal hands, with devastating consequences.

RANSOMWARE ATTACKS

A global ransomware cyber attack recently crippled the NHS, affecting over 16 health organisations and infecting over 300,000 computers from the Russian Interior Ministry to a major German rail operator. A second wave of attacks struck Asia, with 29,000 institutions affected in China alone. It was later revealed

that the incredibly sophisticated and large-scale attack was carried out by amateurs that may have stolen an automated 'cyber weapon' from America's military intelligence unit the NSA.

The global chaos that ensued showed how sophisticated automated hacking tools can give even amateur hackers the ability to launch devastating attacks with nation state-level sophistication, the equivalent of giving weaponised drones to criminals.

And the increase in nation-state malware being developed and occasionally leaked 'into the wild' means that advanced cyber-warfare innovations are trickling down from nation states into the criminal underworld at increasing speed.

We are facing a cyber-security threat landscape populated with human and autonomous threat actors growing at a faster pace than the human resources needed to defend against them. And with more critical national infrastructure, law enforcement and defence assets going online, the attack surface is growing wider every year.

THE NUMBER OF ADVANCED AUTOMATED THREATS IS INCREASING AT AN ALARMING RATE

8.4 billion connected objects will be in use by the end of 2017, with everything from rail transport networks to cargo ships connected to the internet.

At the same time, a critical cyber security skills shortage means a limited supply of human auditors have to race against an ever-growing array of automated tools and hackers to scour their organisation's networks for chinks in the armour.

The shortfall of human talent is getting progressively worse; in Britain alone, 66 percent of companies have too few cyber security workers and 46 percent report that the talent shortfall is causing cyber security breaches.

With a perfect storm of a critical cyber security skills gap and growing use of automation in cyber attacks, organisations need to fight fire with fire by embracing automation in cyber security.

Traditional automated vulnerability scanning tools – which simply mimic an attack by indiscriminately bombarding a device from the outside in the hope of finding a breach – cannot keep up with sophisticated modern attackers that dedicate time and effort to finding every potential weakness in the network.

Leading defence and law enforcement organisations such as NATO, the FBI and the US Department of Defence are instead turning to pioneering 'intelligent' software to analyse complex cyber infrastructure-seeking vulnerabilities, which could otherwise be exploited by hackers. New software in development from cyber security and defence experts can autonomously scour the specific design of any network to find structural vulnerabilities and produce detailed reports on how to fix them.

This advanced software can automatically analyse the entire configuration or blueprint of an entire network for underlying systemic weaknesses in everything from the switch to the firewall. It is the equivalent of an engineer conducting a detailed analysis of an entire tank blueprint to identify hidden design flaws in its armour, instead of bombarding it with weaponry in the hope of finding any weak points. Intelligent automated auditing tools are now capable of replicating the work of hundreds of top cyber security consultants and at far greater speed.

This dramatically reduces demands on human resources and enables organisations to use programmes to conduct rapid, detailed and accurate security audits far faster and more accurately than human auditors enable. Crucially, with cyber security skills in short supply, this allows defence, law enforcement and security organisations to focus human resources on high-level strategic work, including cyber offensive programmes, while using automation for baseline security.

With advances in automation enabling the replication of skilled cyber criminals by machines, we must use the same smart methodology to reinforce the work of security experts and strengthen defences, allowing skilled workers to focus on more strategic cyber security roles ●

Nicola Whiting is Chief Operations Officer at Titania, which developed the first advanced and detailed configuration-auditing tool in the world. Titania recently received the Queen's Award for Enterprise and supports many of the world's most recognisable organisations including: the Department of Defence, MoD, FBI, PayPal, Cisco, BT, Deloitte and KPMG.

Picture credit: Getty

With more and more things becoming internet connected, robust cyber security is essential