DEALING WITH THE MALWARE THREAT

Daniel Driver *explores the growing threat of malware and what can be done to fight back*

In reality, the biggest security threat that most organisations are exposed to exists within their own network. Social Engineering is a growing method for hackers who want to break into networks, and endpoint security cannot identify if an authorised user's device is sending out sensitive data. Bring Your Own Device (BYOD) and tools that encourage online collaboration also blur the lines between trusted and untrusted data sources, making identification of threats far more difficult.

Malware damage can range from loss of data to serious financial consequences. Understanding the major types of malware can help you make informed decisions about acquiring tools to protect your system.

Ramsomware is one of the key cyber crime methods that IT network owners should be vigilant of. Becoming increasingly common, and covered in the media with regularity, ransomware encrypts data on a corporate network and demands a payment to receive the decryption code. We're seeing a significant increase in ransomware attacks targeting businesses, and the pay-outs are increasing to tens of thousands of pounds per attack.

Knowledge of what is on your network is vital in reducing exposure to attacks

When it comes to data exfiltration malware, however, this is becoming more difficult for attackers. As more businesses start to take cyber security very seriously, attackers are less able to steal data in massive volumes very quickly without setting off alarm bells. Hence low and slow data exfiltration is now also becoming a favoured attack method. This moves data out of a network so slowly that it is unlikely to be detected by traditional network security tools.

STAYING UP TO DATE

To prevent infection from any of these threats, having up-to-date antivirus software on all network assets and ensuring that a firewall is enabled on your network is vital, alongside confirmation that the latest software updates are installed and keeping your operating system current.

While it is important to do all of the above, it is still possible that a determined attacker will use more advanced evasion and infiltration techniques. Examples include using Social Engineering to get a valid password from an employee or an attacker using their custom malware utilising zero-day exploits. For those instances, it is important to know that malware is active on your system as soon as possible so that remedial action can be taken. It is, of course, proactive monitoring for behaviours indicative of an attack on your network that will provide this essential insight.

Protection against cyber attacks doesn't have to be expensive, certainly not for smaller businesses. This can be broken down into preventing, mitigating, detecting, and responding. Preventing means putting something in place to defeat the known threats in a way that doesn't affect the day-to-day running of a business, this includes firewalls and endpoint protection (anti-virus). Mitigating refers to being able to understand vulnerabilities on a system. For example, what machines have been forgotten about and left unpatched, why does the Smart TV in the boardroom have internet access, do we monitor for vulnerable network elements? Detection is the process by which you would be able to identify an attack in progress, so having some way of discovering threat-like network behaviours. Responding means being able to react to an attack should the worst happen. Having some way of being able to record how an attack occurred can greatly decrease clean-up costs, and being able to prove that proper processes were in place to stop attacks will help massively when it comes to facing up to any fines.

Up-to-date software patches and AV alone are no longer a sufficient measure of malware mitigation. The actions of the user are often the biggest risk and training plays a key role in mitigating this. Training staff not to fall for phishing schemes or social engineering of any kind, and enforcing good password behaviour is a must. User security awareness training should make users think twice before clicking the link, plugging the USB drive in or divulging any data to external parties that could be used to build an attack. This should also cover simple concepts to minimise the impact if a user account is breached, such as good password management to avoid the same one being used across multiple sites.

A periodic audit and review of the security of the IT environment ensures no legacy equipment is left unmanaged, user accounts do not have excessive network/system access, no rogue devices have been plugged in, and that there isn't a better way to configure a device for improved security.

Understanding what is on your network is vital in reducing exposure to potential attacks. In the event that an organisation is subjected to an attack it is key to understand what happened and why, in order to prevent it from inflicting further damage, prevent repeated attacks, and understand the impact such as what has been stolen.

The standard 'boiler plate' security solutions have inherent weaknesses and with networks becoming more complex and attack techniques increasingly advanced, organisations need a good understanding of their network and how their systems/data are accessed. Only with a good understanding of this can the attack surface be better understood and informed decisions be made about the security or weakness of a particular area. Organisations must also be able to identify when they do not have the necessary internal resources (skills and/or time) to ensure adequate cyber protection.

UNDERSTANDING THE TYPES OF MALWARE CAN HELP YOU ACQUIRE TOOLS TO PROTECT YOUR SYSTEM

THE GDPR EFFECT

Accountability at board level will also improve the resources allocated to this risk, and we are seeing more impetus placed on cyber protection as the GDPR regulations place more accountability on senior staff members. Businesses may also want to invest in periodic red team testing of the network using multiple outside vendors to ensure that the defences remain strong and any vulnerability is closed. An organisation should also have a well understood procedure in place for how to manage an incident of varying levels, from a single malware infection to an advanced attack where systems may go offline and business continuity procedures may need to be implemented.

In the end, it comes down to a question of how important your data is and how much investment an adversary wants to invest so they can gain access to it. You could implement all best practices by the latest software updates, keeping AV up to date, and using the most robust firewalls, but a threat actor is likely to be able to defeat all these protections with enough time and tenacity. However, having a good understanding of the network structure and ongoing network activity should, in the event of an attack, allow quick response and damage limitation, as well as identifying human error an order of magnitude faster than normal.

Measures such as ensuring the network topology and devices present are clearly understood and

▶

ensuring good ongoing visibility of the network can radically reduce the impact of any attack, many businesses are now moving to this more proactive method of protection.

As a result, the traditionally applied security systems such as firewalls, Intrusion Detection Systems (IDS) and anti-virus should form only part of modern cyber defences. To enable a proactive approach to maintaining good network security, a more sophisticated layer is required.

FILTERING OUT THREATS

Such an effective network monitoring system will quickly identify activity caused by malicious behaviour and will have to sit at the core of the network yet remain passive so as not to interfere with other systems, identifying and classifying behaviour to filter out threats from the benign.

Most widely used cyber security systems are unable to identify and automatically alert on low and slow behaviours over long timescales. Perimeter and endpoint solutions typically only have the 'now' available to them, and false alarm rates would be too high to generate alerts over some of the behaviours involved in more advanced attacks. While SIEM tools can be used to gather data, over time it becomes nearly impossible to find the needle in such a large haystack. Also, due to the large amounts of data running through the network, the detection of the threat in advance of the attack tends to be less useful.

Artificial Intelligence, or AI, is a buzzword that we've heard within the IT domain for many years. It actually covers a broad range of technologies, a number of which are applicable in the fight against cyber security attacks, and when combined these can provide a powerful aid to monitoring cyber risk. Some typical examples of Machine Learning used in this area include Artificial Neural Networks (ANN) and Expert Systems.

The number of AI disciplines will continue to grow and the challenge will be to identify which are best suited to a given application. Blended solutions may be used to achieve better results and ensure that businesses are protected from future sophisticated attacks, whether they originate from inside or outside the organisation. Such behavioural-based solutions will help to address the need to make decisions based on an ever increasing vast amount of data, highlighting those important events in among the noise on the network. It also provides the ability to correlate disparate, seemingly benign, indicators that when combined present something of interest.

Where previously cyber security teams relied on large numbers of human analysts to work through disparate data, AI is able to draw conclusions by reasoning over events collected over potentially long periods of time. This allows humans to concentrate the effort in the most efficient way possible, vastly reducing the time required to conclude complex investigations and the size of the teams required to complete these tasks. It is, therefore, likely that a more collaborative approach will be taken in the future between the AI and human components, with the AI component effectively becoming "one of the team".

As malware becomes increasingly intelligent and devious, so the technology used to combat it must match it by identifying and linking malicious activity from months ago, followed by other behaviours a few weeks later, and then something else happening in the last few minutes. Such a system will deliver incredibly high detection rates with equally low false alarms. A step change is now needed in the approach and technologies used to combat the ever-evolving cyber security threat ●

Daniel Driver is Head of Perception Cyber Security at Chemring Technology Solutions. He has worked for the Chemring Group for seven years, taking on analysis, business strategy, and business leadership roles in areas covering bomb disposal, explosives detection, security sensors, and cyber security.

Training staff how not to fall for phishing scams is essential