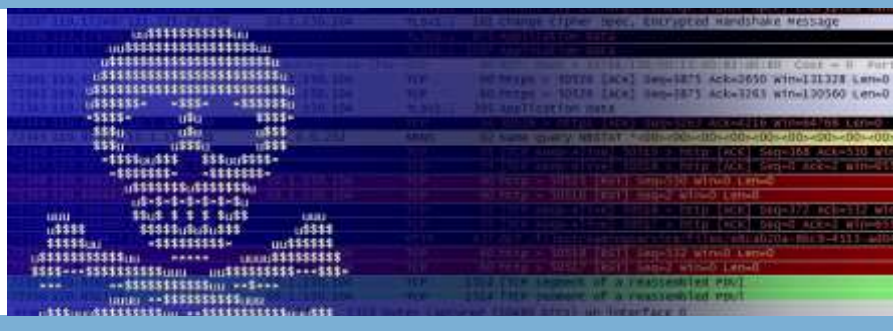
Western Australian
Auditor General's Report



Malware in the WA State Government

Report 28: December 2016

Office of the Auditor General
Western Australia

7th Floor Albert Facey House
469 Wellington Street, Perth

Mail to:
Perth BC, PO Box 8489
PERTH WA 6849

T: 08 6557 7500

F: 08 6557 7600

E: info@audit.wa.gov.au

W: www.audit.wa.gov.au

National Relay Service TTY: 13 36 77
(to assist people with hearing and voice impairment)

We can deliver this report in an alternative format.

ISSN: 2200-1913 (Print)
ISSN: 2200-1921 (Online)

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Malware in the WA State Government

Report 28
December 2016

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

MALWARE IN THE WA STATE GOVERNMENT

This report has been prepared for submission to Parliament under the provisions of section 25 of the *Auditor General Act 2006*.

The audit objective was to determine whether selected government agencies have effective controls to prevent, detect and respond to malware threats and malicious software infecting their computer systems.

I wish to acknowledge the assistance of the staff at the agencies involved in this audit.

COLIN MURPHY
AUDITOR GENERAL
7 December 2016

Contents

Auditor General's overview

My office has been reporting on the issue of cybersecurity for over a decade. Now, hardly a day goes by when the issue is not reported in the media. Australia's preeminent cybersecurity organisation, the Australian Signals Directorate, cannot be clearer about this threat – attacks are becoming more frequent, more sophisticated and more dangerous.

This report assessed how well 6 state agencies are handling the threat from one type of cybersecurity threat – malware. Malware is a blanket term used to describe all kinds of harmful or undesirable computer programs. Computer viruses, worms, and Trojans are all types of malware. Malware is used to steal files and sensitive information, disrupt operations, and destroy data.

The audit found that all the agencies were under constant threat. In the report we comment on the types of incidents we saw and the agency controls that were used to defend against the attacks. Unfortunately, the controls were not always effective in preventing or detecting infection.

The audit highlighted the need for improved central governance arrangements to identify, warn of and prevent attacks. In my view, this would help address existing vulnerabilities.

Executive summary

Introduction

Malware, short for malicious software, is a more visible part of a growing cyberthreat. Industry experts agree it is a case of not if, but when, an entity will be breached. Government agencies that store significant amounts of confidential and highly desirable personal information are prime targets for infiltration and attacks. The cost to the Australian economy of responding to cybercrime, including malware, is estimated to be as high as $1 billion per year.

The objective of this audit was to determine whether selected government agencies have effective controls to prevent, detect and respond to malware threats and malicious software infecting their computer systems.

Overview

Malware is a term used to describe all kinds of harmful or undesirable computer programs. Computer viruses, worms, and Trojans are all types of malware.

Malware can be designed to steal information from a user, such as usernames and passwords for online accounts, credit card numbers, and files or documents. It can also enable an attacker to have remote control of a computer and access to any connected networks.

In recent years, a popular malware variety known as ‘ransomware’ has emerged. This encrypts a user’s files and demands a ransom payment to unlock them. Some malware will also delete or corrupt files to disrupt a user. Ransomware attacks, when they succeed, are obvious to the user. Other types of malware will try to hide, operating without the user knowing for as long as possible.

There are 3 main ways that malware can infect a computer: downloading a malicious file, opening attachments to spam email, or using an infected USB stick or device. Malware creators will either trick a user into running their malware, or, exploit vulnerabilities in software to force the installation. Often, the user will be unaware that malware has installed itself.

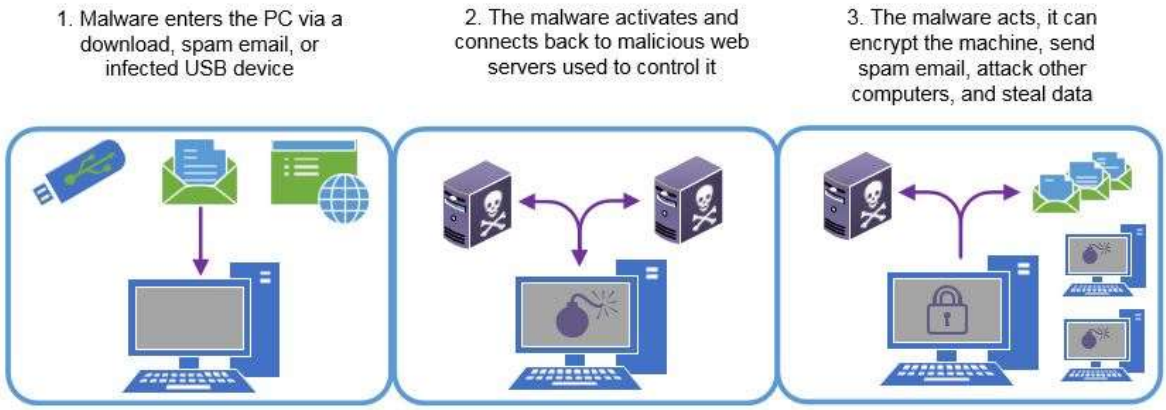


Figure 1: Simple overview of the malware infection process

There are many parties involved in the protection and security of Australian government networks. Federally, the Australian Cyber Security Centre (ACSC) and the Australian Signals Directorate (ASD) mandate security requirements. Federal agencies are also required to report all security incidents to the ACSC.

Historically, the WA government has only had high-level cybersecurity requirements. A Public Sector Commissioner's Circular[1] requires agencies to address cybersecurity risks. The Office of the Government Chief Information Officer (GCIO), which was established in July 2015, recently published the *WA Digital Security Policy*. However, the all-important security standards that will support the policy are still in development.

We performed 2 types of tests to assess if IT security at 6 agencies was effective at countering malware threats:

- Compared agencies' security processes and tools against recommended good practice. The traditional defence for malware has been anti-virus software. However, attacks have evolved to require more layers of security controls.
- Analysed agency network traffic for any evidence of active malware infections and attempted malware attacks. At the first agency we captured traffic from outside its network, but this did not allow us to fully analyse the results. At the remaining 5 agencies we captured traffic from inside their networks.

Our assessment of network traffic had limitations. We could only capture data for short periods, 10 to 12 days including weekends, per agency due to the enormous volume of data. We were also unable to analyse encrypted network traffic, and our automated analysis tool could only check for known malware. It is therefore possible that there were more infections than we found in this audit. Further details of how we conducted this audit are included in Appendix 1.

Audit conclusion

Malware is a constant threat for agencies. All 6 agency networks experienced numerous attempted attacks and malware downloads.

We did not observe a substantial number of ongoing malware infections, which indicated that the 6 agencies generally deal with malware they or their systems identify. However, the infections that were active constituted a serious threat to the agency networks.

All agencies experienced attacks that were able to defeat at least 1 security control or technology. This highlights the need for agencies to employ layered controls with constant monitoring and improvement. The layering of controls is a 'defence in depth' approach to cybersecurity.

The control failures we identified were consistent with the findings in our annual Information Systems Audit Reports. The findings illustrated yet again the importance agencies should place on ensuring that often basic, easy to implement controls are in place and operating effectively. But, the evolving malware threat also requires agencies to be constantly improving their security processes, and upgrading to more advanced security tools to further strengthen their networks.

The audit highlighted a need for the WA public sector to have a coordinated approach to the management of cyberthreats. At the time of our audit, there were no statewide requirements for cybersecurity and anti-malware controls. Each agency has to carry the full cost of planning for and guarding against malware threats as there are no official forums for collaboration, sharing of advice, resources and experiences.

[1] Public Sector Commissioner's Circular 2010-05: Computer Information and Internet Security.

Key findings

- We observed malware related communication on all networks we tested. This included attempted attacks by malicious web pages, downloads of malware files and active malware communicating out to the internet. These attacks appeared to originate from 18 different countries, including Australia, though we do not know where the attackers themselves were based. The high volume of attacks shows a committed threat that is working to defeat security controls and a need for agencies to understand the threats and fix any gaps in their security controls.

- Two agencies had signs of persistent malware infections that had bypassed their security controls. One agency had a single infection that was active for most of the 12 day sample period. Another agency had in excess of 5 infections active for approximately 2 days, with at least 1 computer reinfected during the assessment period. These active infections placed the agency networks, systems and data at risk.

- IT control failures are still common. Our testing revealed all agencies had some control failures, or missing controls. Common issues were around missing security patches and outdated operating systems. We also noted problems with management of anti-virus software, assignment of access rights, and network design. These ineffective or missing controls place agencies at risk of malware infections and breaches. While some performed well, there is still a need for ongoing assessment of risks and improvement of controls.

- People are essential for strong defence. Agencies cannot rely solely on automated tools, as these tools can only deal with known threats. Skilled professionals are required to monitor the IT environment and identify issues proactively. All of the agencies we visited had IT staff working in information security roles. Some were fortunate to have more than 1, however most represent a single point of reliance, and failure. Agencies must assess their security skills requirements, ensuring their IT teams have the resources needed to secure the network.

- Most agencies did not provide adequate awareness training for their staff. Many of the malware attacks that we observed required some level of interaction from a staff member (user). Attackers will try to trick an innocent user into clicking links, downloading files or entering their login details. Diligent and security conscious staff are key to preventing and detecting these malware threats.

- The WA Government lacks a coordinated approach to cyberthreats, including malware. At the time of our audit, there was no whole-of-government security policy or framework providing guidance to agencies on how to implement a successful security program. Agencies are also not required to report malware incidents to a central agency. As a result, no single body was able to provide us with an overview of the size or nature of the malware threat faced by agencies.

    - Without central guidance and support, agencies work in isolation. There are few formal avenues for collaboration, support, and resource sharing. Increased cooperation and sharing can reduce costs to agencies through economies of scale.

    - A whole-of-government view of cyberthreats allows for properly informed and more efficient security programs. Other jurisdictions with better central coordination have a more mature approach to security. Infections and breaches are found and remediated more quickly[2].

[2] https://www2.fireeye.com/m-trends-2016-asia-pacific.html

Recommendations

1. We have provided detailed recommendations to each agency in the audit. At a high level, we have recommended that they:
    a. assess the risk posed by the malware threats we observed
    b. improve any controls that we identified as ineffective
    c. consider additional controls to better secure their networks, systems and data against malware.
2. We recommend that the WA public sector, by way of the Office of the Government Chief Information Officer:
    a. continue the rollout and implementation of the Digital Security Policy, including its supporting guidelines and controls
    b. consider methods to foster collaboration, information and resource sharing between agencies
    c. gather information to properly understand the threat posed by malware and other cyberthreats to the WA public sector.

Agency responses

Department of the Attorney General

The Department of the Attorney General values the opportunity to work with the OAG in assessing its current risks and protections. The Department found the report and recommendations in the "Malware in the WA State Government" very useful and having regard to this Report will undertake a review of its current ICT security architecture and Security Management practices.

The Department welcomes the recommendations of the audit and is working to address comments directed specifically to the agency. The Department is optimising the use of its existing ICT budget to carry out changes to systems and controls on the basis of risk. Given these constraints some risks identified in this report may not be fully addressed.

We support the recommendations of assistance from the Office of the Government Chief Information Officer in the rollout of information security capability within the public sector.

Department of Mines and Petroleum

The Department of Mines and Petroleum has valued the opportunity for an independent external review of its malware protection performance by the Office of the Auditor General. The favourable findings from the review validate the ongoing commitment of the Department towards effective and strong information security practices.

Department of Transport

The Department of Transport (DoT) accepts the findings with the report providing insight into current vulnerabilities. Although the data capture was limited to only two-thirds of traffic, the department takes comfort that our perimeter defences prevented any significant findings or significant breach of security. DoT has already started to address all recommendations. The recommendations provide further support to ensure DoT's ICT Governance and Security frameworks are fully implemented and adhered to.

Main Roads Western Australia

Main Roads will undertake a risk assessment of malware threats and make appropriate improvements to controls as required. Additionally, Main Roads look forward to working collaboratively with the Office of the Government Chief Information Officer and other agencies to improve overall information security for WA Government

Office of the Government Chief Information Officer

The recommendations are supported.

Cyber Security will continue to be a growing issue as these types of security threats are continuously evolving, sometimes on a daily basis. Some countries have dedicated teams breaking through virtual security barriers in order to gain commercial advantage or simply cause anarchy. As the WA Government, not unlike other governments around the world, moves into more on line access for its staff and the community, the threat of loss of data or viruses remains a high risk, high impact consideration for government.

It should be noted that, publishing a security policy only sets a standard. There must be ongoing audits to measure compliance. That cannot be undertaken by the Office of the Government Chief Information Officer as we do not have the resources.

There also is a significant skills gap in the public sector to ensure that appropriate security measures are in place, that CEO's and CIO's instil the right disciplines and ensure that their government agency proactively mitigates its security risk from outside threats. It is imperative that government works in a collaborative manner to achieve this outcome, the OGCIO is attempting to lead this outcome. It is suggested that Government CEO's must have cyber security as a standing agenda item on their corporate executive Risk Register and reviewed frequently throughout the year.

Audit focus and scope

The audit objective was to determine whether selected government agencies have effective controls to prevent, detect and respond to malware threats and malicious software infecting their computer systems.

We based our audit on the following lines of inquiry:

- Have agencies implemented controls to prevent, detect and respond to malware threats?
- Are agency controls effective at managing malware threats?

In undertaking this audit we:

- reviewed agency policies, procedures and guidelines
- compared agency security processes and tools against recommended good practice. This built on testing we normally do for general computer controls audits
- captured agency network traffic for a period of 10 to 12 days at each agency
- analysed agency network traffic for any evidence of active malware infections and attempted malware attacks
- spoke to a representative from the Office of the Government Chief Information Officer
- liaised with a representative from the Australian Cyber Security Centre (ACSC).

Further detail on the scope of the audit is included in Appendix 1.

We conducted this narrow scope performance audit under section 18 of the *Auditor General Act 2006* and in accordance with Australian Auditing and Assurance Standards. Narrow scope performance audits have a tight focus and generally target agency compliance with legislation, public sector policies and accepted good governance. The approximate cost of tabling this report is $320,000.

Agencies we audited

We audited 6 agencies, selected because of the services they provide to the public and the sensitivity of the data they store. Most of these agencies also provide IT services to other agencies, acting as a shared service provider. We assessed the network traffic of these 'sub-agencies' as it passed through the main network. We expected these agencies to have secure IT environments and a mature approach to risk management.

Main service provider agency	
Department of Agriculture and Food	Department of Mines and Petroleum
Department of the Attorney General	Department of the Premier and Cabinet
Main Roads Western Australia	Department of Transport

Table 1: Agencies included in the audit

We conducted the control testing at all agencies. We also conducted a high-level capture at 1 agency. However, there was insufficient detail to draw firm conclusions, so we changed our approach to do a more complete network capture and analysis at the other 5. Because of the risk of any weaknesses being exploited, we have not attributed any findings or recommendations to individual agencies.

Audit findings

Agencies are under constant threat

The agencies we assessed coped well with most of the multiple attacks and attempted intrusions we observed during our short sample window. However, there were gaps in security controls and processes that leave them vulnerable. Consequently, attacks had breached the first line of defence at all agencies.

The majority of these attacks were launched from malicious websites designed to attack innocent users that visit them. We also observed attacks from email that used malicious attachments, or contained dangerous links.

At the agency where our traffic capture device was outside the network, we observed several thousand attempted attacks over the 10 days of our audit but could not determine whether any of them succeeded. At the other 5 agencies, we observed an average of 10 attacks in the 10 to 12 days of our audit window that entered an agency's network. Agency security systems would have blocked many more. The lowest number was 2 and the highest 17.

Our initial assessment of the captured data generated almost 10 million alerts. The sheer volume of alerts forced us to automate the analysis of the remaining data using pattern-based tools and published lists of websites known to be malicious. This increased the risk that attackers using newer techniques or unknown addresses would go undetected. Malware creators go to great lengths to evade detection by rules-based tools like ours.

After automated analysis, we investigated an average of 2,700 alerts at each agency. At 2 agencies, there were over 160 individual computers that generated alerts, which we needed to follow up.

This high tempo of attacks requires constant vigilance from agency IT staff and users. Most attacks were able to bypass at least 1 layer of agency security but were blocked by others. However, some attacks evaded detection altogether. Some of these attacks led to successful malware infections. Threats are constantly changing and attackers try to stay one step ahead of defensive measures. Agencies need strong layers of controls to reduce single points of failure and increase the effort required by an attacker.

We observed similar types of attacks at all agencies. Because of the gaps between our traffic captures, we did not see malware from the same sources at different agencies. However, 2 agencies experienced attacks from addresses later flagged by the ASD as 'Indicators of Interest'. These are addresses that ASD have seen targeting Australian organisations. This highlights the effectiveness of sharing data and creating a wider understanding of the threat environment.

Common malware successfully attacked some agency computers

The attacks and malware we observed were common and well understood. These attacks used techniques that security tools and agencies should be aware of, yet they were still able to enter the network and attempt to infect computers. This is indicative of weak or missing security controls.

We observed common malware that was able to activate and go undetected at 2 agencies. A large business unit in 1 of our assessed agencies had infections on at least 5 computers. Because of its network design, we were not able to find out the exact number. However, it did appear that at least 1 of these computers was infected multiple times, and 3 appeared to be infected by the same malware.

We identified these infections through the network communications, as the malware tried to connect back to its command and control system. Fortunately, the agency blocked most of these connections. This blocking occurred because the malware used a non-standard

connection mechanism[3], not because it was identified as malicious. IT staff were not aware of the infections until alerted by users of problems with their computers.

Another agency had a single computer infected with a common Trojan. This piece of malware tried to connect to its command and control system multiple times a day for most of our capture period. The agency's web content filter detected the destination as malicious and blocked the connections. However, the infected computer had not been located and cleaned.

In some IT environments, it is reasonable to expect a certain amount of malware to evade defences and activate. A lot of common malware does not pose a serious risk to government or corporate networks if quickly detected and removed.

However, the success of common attacks is a possible indicator of a more serious issue. Skilled attackers that target an agency will deliberately use uncommon techniques and more advanced malware to avoid detection. These attacks may also go undetected.

Agencies cannot rely on a single layer of security to prevent malware infections

The attacks we saw all bypassed at least 1 layer of agency security controls. It is common for malware and other attacks to bypass some level of security. For this reason, it is essential for agencies to employ layers of security. This layering concept is known as 'defence in depth'.

The traditional tool for stopping malware is anti-virus software (AV). While still a useful tool, agencies cannot rely on AV as their sole defence.

All of the infected computers we identified had AV installed. These systems were unable to automatically detect and remove the active malware infections we found. In some instances, this was because the software was not configured properly. However, malware that can evade immediate detection by AV is common. Attackers go to great lengths to design their malware to defeat AV tools. There will always be a gap between the identification and analysis of new threats and the distribution of AV updates.

All of the agencies included in this audit were progressing with defence in depth strategies; some more mature than others. We noticed a higher number of successful attacks at agencies that performed poorly in our controls testing.

The successful prevention of malware requires a large amount of proactive security, including secure design of systems and continuous improvement.

Most of the attacks we saw attempted to exploit security flaws in software, known as vulnerabilities. Agencies need to patch their software regularly to reduce the effectiveness of exploit kits (Figure 2). However, patches are not always available.

A software vendor might be unable to, or refuse to develop, a patch to address a threat. Patching software can be time consuming and costly for vendors. They may not create a patch because of these high costs. Sometimes, vulnerabilities are too complex for effective patching. Patches can also take a long time to develop, test, and deploy. This gap leaves users exposed and vulnerable to attack. Agencies must design networks and systems to limit the potential impact of security vulnerabilities.

[3] The malware tried to communicate using non-standard web ports. Workstations were permitted to browse on ports 80 and 443 only. Outbound connections on other ports were blocked by the agency's perimeter firewall.

Exploit kits are used to build malicious web pages that attack a victim's web browser and related software. When you browse to an attack page, the exploit kit checks the browser version and searches for security vulnerabilities it knows it can exploit. If it finds a match, it will try to forcibly install malware. Attackers will often hack into a legitimate website and force it to redirect innocent users to their attack page. Entrepreneurial hackers create these exploit kits and on-sell them as a commercial product. This 'off the shelf' approach makes launching a malware campaign much simpler.

We saw confirmed attacks from common exploit kits named Angler, Neutrino, and Rig. The ACSC highlighted exploit kits as a serious risk to Australian networks in its 2016 Threat Report.[4]

Figure 2: Exploit kits are a reason agencies need to patch regularly

While exploit kits are a reason agencies need to patch regularly, patching may not always be effective against them. Sometimes, attackers will also find vulnerabilities in software and keep them secret, adding them to their exploit kits knowing that no patch is available. These are termed 'zero-day' vulnerabilities. This type of vulnerability illustrates the importance of additional layers of security.

Some of the exploit kits we observed included zero-day vulnerabilities that were exploited in the past year. We also found outdated software with known vulnerabilities at all agencies. Outdated software with known vulnerabilities is a particular risk because attackers will be able to easily find and exploit the vulnerabilities. Agencies need to have additional controls in place to address this risk.

Agencies cannot expect, or be expected to, prevent all malware infections. They therefore need to ensure they have good controls in place to detect infections and respond quickly. IT staff will need to be able to identify an infection, understand its impact on systems and data, and act to remediate it as soon as possible.

Some agencies may consider bolstering their layers of security with more rigorous controls and advanced technology. However, the costs can be significant. More importantly, these controls would require ongoing effort and expertise to operate properly. Agencies need to conduct honest risk assessments, and assessments of their own capabilities, to decide the controls they can successfully implement.

Control failures are still common, leaving agencies vulnerable

As we regularly report in our annual Information Systems Audit Report, agencies often do not ensure that their basic, easy to implement controls are fully effective.

Each of the audited agencies had 1 or more weaknesses in controls such as not: applying software patches, restricting administrator rights, and limiting or monitoring USB devices attached to computers. These controls directly affect an agency's effectiveness in dealing with malware risks. Responding to malware threats also requires agencies to investigate the use of more sophisticated controls such as segregating their networks or only allowing trusted applications to run on systems.

Agencies can do more to manage security vulnerabilities in their software

Our data analysis indicated that all agencies had vulnerable versions of commonly used software communicating with the internet. These numbers ranged from very low (4) to in excess of 400 installations. In some cases, we saw vulnerable software communicating with

[4] https://www.acsc.gov.au/publications/ACSC_Threat_Report_2016.pdf

attack sites hosting exploit kits. Patching of software vulnerabilities is relatively straightforward and essential to stopping malware.

Agencies need to improve their ability to find vulnerabilities in their software. While many patching systems can be automated, agencies must know what software is installed, and which computers are using it. Three of the agencies we audited were not aware of all the software installed on their computers. Because of this, agencies did not install patches, leaving vulnerabilities exposed.

Two agencies relied solely on automated patching systems and notifications from software vendors. They were not proactively looking for vulnerabilities. The remaining 4 agencies used scanning software to search their networks for vulnerable software. However, we noted that 2 agencies had not configured their scanning tools optimally, which risked returning incomplete results. These scans would provide the agency with false assurance. Two of the agencies were also not following up scan results, or running the scans at regular intervals.

All of the agencies we audited also had some computers that were running operating systems and software that was unsupported by the vendor. This left any security vulnerabilities exposed.

Common examples include Microsoft Windows XP and Microsoft Windows Server 2003. We found these platforms at all agencies. Some agencies were still working to replace these systems. Others were managing the remainder through tighter security and increased monitoring.

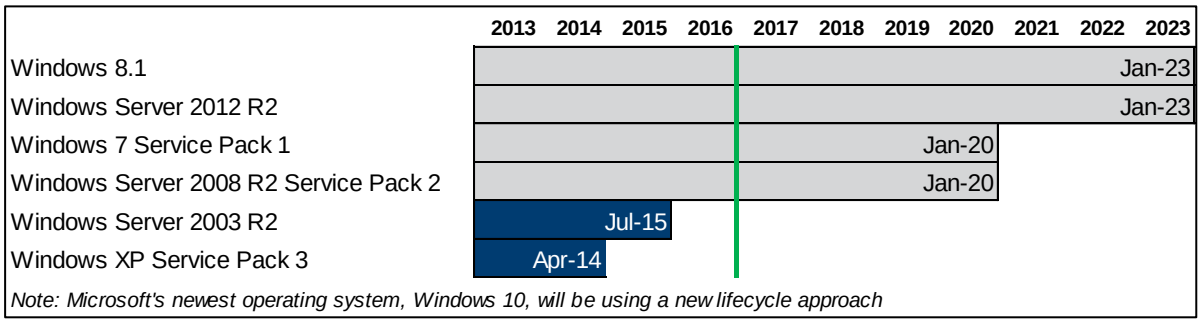


Figure 3: Microsoft Windows support end dates[5]

When no patch is available or a patch cannot be installed, agencies must consider any additional risks. This can involve isolating the system and limiting its use, increasing monitoring, and installing additional security tools.

These types of alternative mitigations are essential for software that is no longer supported by its vendor.

Anti-virus software management

Two agencies had deployed their AV incorrectly, limiting its effectiveness. Correctly deployed and configured AV is still an essential defensive layer. It provides protection against common malware and attacks.

As mentioned earlier, 2 agencies had signs of persistent malware infections. A large business unit in 1 agency had in excess of 5 infections active for approximately 2 days, with at least 1 computer reinfected during our assessment period. This business unit provided many of its own IT services, so its security processes differed from the rest of the agency. The other agency had a single infection that was active for most of our 12 day sample period.

[5] https://support.microsoft.com/en-au/lifecycle/search?sort=PN&alpha=windows%20server&Filter=FilterNO as of the 21/11/16.

The business unit affected by multiple active malware infections was not using centralised management for its AV to control the AV 'agents' installed on each computer. As a result, the scan settings on the client computers were inconsistent. None of the computers were set to run regular, scheduled scans. A small number of computers also had the on-demand scanning feature disabled. These computers had, effectively, no AV protection.

In a centralised management system, the manager will distribute updates and new malware detection patterns to all its clients. The clients will report their status to the manager, and most importantly, log any malware detections or events. The IT team is able to review the logs centrally to get a high-level view of the status of computers on its centrally managed system. The IT team can also use the manager to set uniform configuration across all computers.

The agency that had a single, persistent infection had not enabled scheduled scanning. When the malware infected file was downloaded to the computer, the on-demand scanner did not identify it as malicious. The file was left to activate itself and complete its tasks. This can happen if the malware installs itself before AV definitions have been updated. Scheduled scanning rechecks software and reduces the risk that malware remains undetected – refer Figure 4 for AV scan modes.

On access scanning: also known as 'real time', the AV will analyse files as the user accesses them. This is designed to ensure that any file a user wants to open has been checked using the most recent definition. This type of scanning can also scan the contents of USB drives that are plugged in.

Scheduled scanning: a complete scan of the computer. The AV will check all files (within configurable limits) on the computer. This is more thorough than on-access scanning, giving the AV the chance to recheck files with its updated definitions. However, it can affect system performance. Scheduled scans must be configured and timed to cause minimal system disruption.

Figure 4: Anti-virus scan modes

Agencies could further harden their computers

Agencies can do more to secure and 'harden' their computers to limit malware effectiveness.

Most agencies are limiting their users' rights to install software, or change settings, on their computers. We noted issues at 3 agencies where processes to monitor users with higher privilege levels were not in place or were insufficient.

The agency that had the most malware infections was not limiting access rights within 1 of its large business units. In this business unit, all users had full rights to install software and run any applications. This practice would in part at least, explain the high number of active infections we observed.

Four agencies had few controls in place to limit or monitor USB devices. These storage devices are convenient and often considered essential. However, they can introduce new malware, or be a cause of an existing infection spreading further. Like internet browsing and email, USB storage is another entry point to agency networks. Agencies must assess the risk posed by uncontrolled USB devices.

None of the agencies were using 'application whitelisting' to help prevent infections.

This technology prevents any software or tool that is not pre-approved from running. The ASD regards this as the best control to limit targeted cyber intrusions. Application whitelisting is an example of a high maturity control. However, it is costly to implement properly and requires ongoing maintenance.

Segmenting and securing the network are sophisticated controls that agencies could implement

Half the agencies we audited had not segregated their networks into functional areas or security zones. Instead, they used a traditional network design where everything inside the network is trusted. The flaw with this mode is the perimeter firewall is the only level of network defence. If an attacker gains remote access to a computer or server via malware, they can then roam the internal network freely.

In the agencies with a traditional design, all networked devices can communicate with each other. Only communication to and from the internet is limited. Some additional security is applied to websites and other systems that are accessed by the public. However, once inside the perimeter, the network is 'trusted'.

Only 3 agencies had implemented some basic network segmentation, where sensitive information is segregated from other parts of the network. Modern cyberthreats, including malware, have reduced the effectiveness of traditional network design and agencies need to do more to counter these modern threats. As part of a layered, defence in depth approach, all agencies need to consider reducing their trusted zones and in so doing, give a focus to protecting data and information.

Three agencies had no controls in place to prevent unauthorised devices connecting to their wired networks. Staff, contractors and potential attackers are free to plug in their own computers if they can access the network. Agency staff might also connect devices that use different technology, such as smartphones, tablets, or other connected devices without the knowledge of the agency's IT staff. These devices can introduce malware to the internal network. The software of different devices might also contain vulnerabilities, increasing the risk to the data they process and the network as a whole.

People are essential for strong defence

Dedicated information security personnel are critical to providing secure IT environments, especially in large networks. All the agencies we assessed had IT staff undertaking information security roles. Some had a single, dedicated role, or, the duty was shared between 2 or 3 individuals.

These skilled professionals are crucial to providing ongoing security management and monitoring. As we have noted above, automated tools are essential, but agencies cannot rely on them solely for robust defence.

Relying on a single security staff member is a concern. Agencies risk a single point of failure if these staff are absent, or leave the organisation. Agencies also depend on an individual's ongoing vigilance, skills and awareness of current threats and ability.

In some agencies, the workload is simply too great for a single role. Information security expertise is also required at different levels in the organisation. Skilled technical staff are needed for day-to-day operations. However, security input is required for high level strategic and risk discussions.

The agencies that performed the best in this audit have acknowledged the importance of security at the senior executive level. They consider the security implications of business decisions and ensure their security functions have the resources required to mitigate any risks.

Information security awareness

Most agencies had not implemented complete information security awareness programs. Two agencies were in the process of implementing new, comprehensive programs. The remainder had a variety of ad-hoc initiatives in place. While some of this training was

mandatory for new starters, it was either insufficient or attendance was not properly recorded. Most did not require refresher training.

Security awareness among agency staff is also key to managing malware and cyberthreats. Most of the malware attacks we saw relied on user action to be activated. This could be from a spam email asking the user to run an attachment, or a malicious website requesting a file download. Spam email that tries to exploit the reader is known as phishing. The ASD have highlighted phishing as the most serious risk to Australian networks.

We also noted instances of web browsing that placed agencies at risk. This included browsing adult material and file sharing websites. One of the most effective ways to combat malware attacks and encourage secure online behaviour is through increased awareness. Agencies need to have a security conscious and vigilant workforce.

Western Australia lacks a coordinated approach to cybersecurity

Historically there has been no lead agency for cybersecurity in WA. Previously, the Department of Finance and the Department of the Premier and Cabinet have in part taken on this role. As of July 2015, the Office of the Government Chief Information Officer (GCIO) has taken responsibility. However, there is still no whole-of-government view of the threats faced by the WA government.

At the time of our audit, there was no whole-of-government cybersecurity policy or framework in place to guide agencies. Agencies make their own decisions on risk and develop their own control strategies.

Agencies are also not required to report malware incidents to a central agency. As a result, no single body was able to provide us with an overview of the size or nature of the malware threat faced by agencies.

WA government agencies are becoming increasingly connected so they can share data and provide better services to the community. System integration is one of the strategic goals of the state's first ICT strategy, Digital WA[6]. The strategy also highlights the importance of common standards and strategies to ensure systems are secure.

As connectivity increases, agencies will rely more on the security of their peers' systems and networks rather than just their own. A breach at 1 agency has the potential to affect many more. For this reason, the state should view the malware and cybersecurity threat from a whole-of-sector perspective rather than on an agency-by-agency basis.

Federal government involvement

The Federal government is working to achieve this view by way of ACSC.

The ACSC offers advice to agencies and responds to incidents. The ASD publishes controls requirements and advice for the Federal government, informed by the incidents they respond to and the threats faced by the government, and the country. These agencies also have jurisdiction over the states and, in accordance with the Federal government's Cyber Security Strategy, plan to increase their presence in WA. The WA government will need to be ready to work alongside its federal colleagues.

The only formal avenue for information sharing between security teams is the Interagency Information Security Manager's Group. Primarily an email list, this group has a small core of active users. Contributions are sporadic and rely on members having free time. Sharing of experience and ideas is essential to develop successful security programs.

[6] http://gcio.wa.gov.au/initiatives/digital-wa-state-ict-strategy/

Cybersecurity collaboration has formed a large part of the national cybersecurity strategies for Australia, the US and the UK. All 3 countries now have dedicated cybersecurity centres or agencies, tasked with gaining visibility into cyberthreats. This allows for coordinated responses and development of effective prevention efforts.

Many agencies, including those in our sample, are doing good work in regard to security. Their experiences, techniques and tools are worth sharing with other agencies. They can offer valuable lessons learnt and help prevent repeated mistakes.

Appendix 1: How we conducted this audit

Assessing agencies' ability to prevent, detect, and respond to malware

We reviewed the security controls, both technical and non-technical, within agencies. This testing built on the work we already conduct during our annual general computer controls audits.

We reviewed some additional controls specific to preventing and detecting malware. The controls we assessed are seen as good practice by the industry. Our sources included the:

- Australian Signals Directorate (ASD) Strategies To Mitigate Targeted Cyber Intrusions
- Australian Government Information Security Manual (ISM), published by the ASD
- National Institute of Standards and Technology (NIST) Guide to Malware Incident Prevention and Handling (SP 800-83)
- ISO/IEC 27001:2013 Information Security Management Systems – Requirements
- ISO/IEC 27002:2013 Code of Practice for Information Security Controls.

Capturing network traffic

The easiest way to look for malware activity inside agencies was to look at their network traffic.

Most malware will enter networks via the internet or email. Once activated, malware will 'phone home' to servers on the internet. This allows it to join what is known as a botnet: a network of infected machines controlled by the same attacker. The owner of the botnet uses these servers to send commands to the malware, update it with new features, or allow the malware to upload data that it collects. These malicious servers are known as command and control systems.

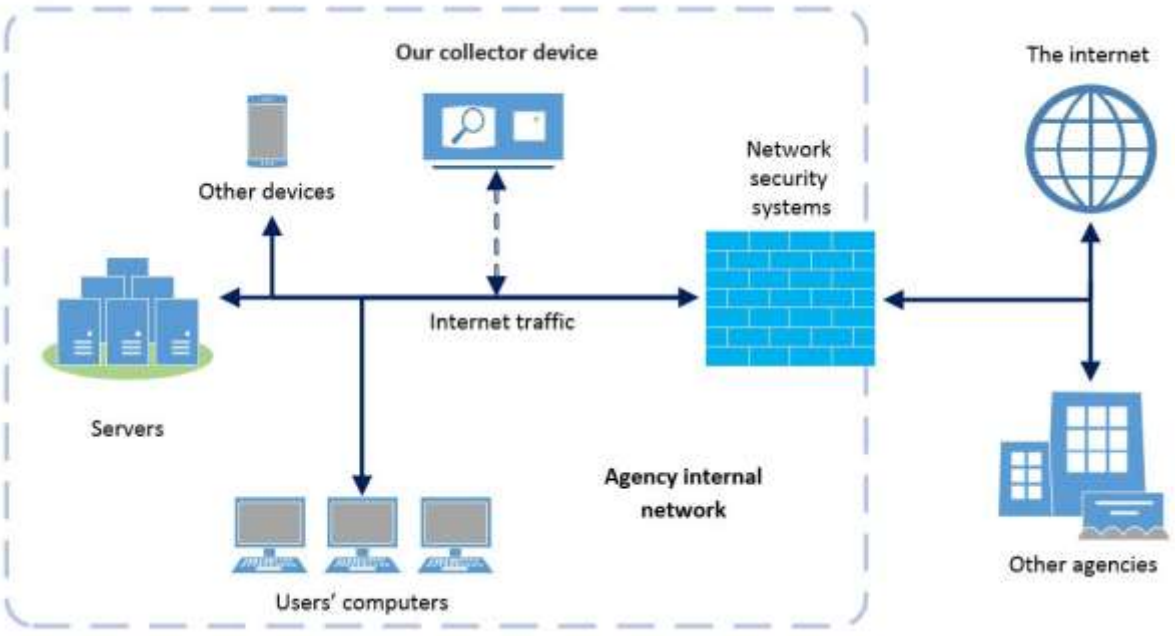


Figure 5: The typical deployment of our traffic collector device

To investigate agency traffic, we installed a collection device on their network that received a feed of all internet traffic. This device included 3 different technologies to analyse traffic and generate alerts on suspicious behaviour. See ‘Tools and Technology used’ further down.

We tried to position the device ‘inside’ an agency’s network security systems. This way, any inbound attacks would need to have passed through the systems before hitting our device.

Our device would also capture the outbound connection from malware on agency computers and servers. Agency network security systems might block the outbound connections after they passed through our device. However, this traffic indicates that malware was able to install itself and activate.

We left the device to collect network traffic for a period of at least 10 days, including 2 weekends and a working week. After this period, we uploaded the data to a data analysis system. This allowed us to categorise, visualise, and sort alert data.

Analysing the results

A significant number of alerts of suspicious behaviour were generated. The data analytics system was able to provide some initial sorting and prioritising. We manually assessed the rest.

We looked for any evidence of suspicious or potentially malicious behaviour by analysing traffic patterns and connection protocols. This work was limited due to the sheer volume of data collected, most of which was legitimate traffic.

We provided the details of any alerts or issues we found to agency technical staff. They had the opportunity to investigate and act on the alerts. They were also able to tell us if any alerts were incorrect, known as a ‘false positives’ alerts.

Our approach had limitations

This assessment of agencies is limited, and it is entirely possible that some infections will have gone undetected.

Our network captures were limited to a 10 to 12 day period, and even this resulted in enormous volumes of data to process. In total, we collected almost 50 terabytes of data that was automatically processed. This processing generated almost 10 million alerts.

To analyse such a large amount of data efficiently, we were forced to rely on pattern-based tools and published list of websites known to be malicious. This increased the risk that attackers using newer techniques or unknown addresses would go undetected. Malware creators go to great lengths to evade detection by rules-based tools.

Malware can be located by analysing traffic patterns for unusual connections or uploads and downloads at suspicious times of the day. However, this is very time consuming and requires in-depth knowledge of the network. This was not feasible for our audit.

Finally, our device could not read or decrypt encrypted data. Web traffic secured using the HTTPS protocol is encrypted. At some agencies, this traffic makes up almost 50% of web browsing. Websites that handle sensitive information, like banks, use this encryption to protect their customers. Increasingly, attackers are also using encryption to hide malicious communications from security systems. During this audit, we observed encrypted connections to malicious websites.

Tools and technology used

The traffic collector device contained 3 different technologies:

A network traffic recorder: This system kept a copy of agency traffic, logging the details of all connections into a database. This database could be queried to search for and investigate suspicious traffic patterns.

An Intrusion Detection System (IDS): This tool uses pre-set rules to look for malicious behaviour in network traffic. The IDS that we deployed is ‘open source’; freely available to download and install. The detection rules for this system were compiled from a variety of sources, both commercial and freely available.

A ‘Sandbox Appliance’: This technology looks for files in network traffic that it does not recognise. If it finds an unknown file, it will take a copy of the file and run it inside an isolated virtual computer. The behaviour of the file is monitored to see if it behaves like malware. The sandbox appliance that we used was a commercial product.

Auditor General's Reports

Report number	Reports	Date tabled
27	Opinions on Ministerial Notifications	7 December 2016
26	Opinion on Ministerial Notification	23 November 2016
25	Opinion on Ministerial Notification	9 November 2016
24	Audit Results Report – Annual 2015-16 Financial Audits	9 November 2016
23	Western Australian Waste Strategy: Rethinking Waste	19 October 2016
22	Opinion on Ministerial Notification	13 October 2016
21	Opinion on Ministerial Notification	6 October 2016
20	Ord-East Kimberley Development	7 September 2016
19	Information and Communication Technology (ICT) in Education	17 August 2016
18	Opinions on Ministerial Notifications	11 August 2016
17	Financial and Performance Information in Annual Reports	21 July 2016
16	Grant Administration	7 July 2016
15	Management of Feedback from Public Trustee Represented Persons	30 June 2016
14	Management of Marine Parks and Reserves	30 June 2016
13	Maintaining the State Road Network – Follow-on Audit	29 June 2016
12	Regulation of Builders and Building Surveyors	22 June 2016
11	Information Systems Audit Report	22 June 2016
10	Opinions on Ministerial Notification	8 June 2016
9	Payment of Construction Subcontractors – Perth Children's Hospital	8 June 2016
8	Delivering Services Online	25 May 2016
7	Fitting and Maintaining Safety Devices in Public Housing – Follow-up	11 May 2016
6	Audit of Payroll and other Expenditure using Data Analytic Procedures	10 May 2016
5	Audit Results Report – Annual 2015 Financial Audits – Universities and state training providers – Other audits completed since 1 November 2015; and Opinion on Ministerial Notification	10 May 2016
4	Land Asset Sales Program	6 April 2016
3	Management of Government Concessions	16 March 2016
2	Consumable Stock Management in Hospitals	24 February 2016
1	Supplementary report Health Department's Procurement and Management of its Centralised Computing Services Contract	8 June 2016 17 February 2016

Office of the Auditor General
Western Australia

7th Floor Albert Facey House
469 Wellington Street, Perth

Mail to:
Perth BC, PO Box 8489
PERTH WA 6849

T: 08 6557 7500

F: 08 6557 7600

E: info@audit.wa.gov.au

W: www.audit.wa.gov.au

Follow us on Twitter @OAG_WA

Download QR Code Scanner app and scan code to access more information about our Office