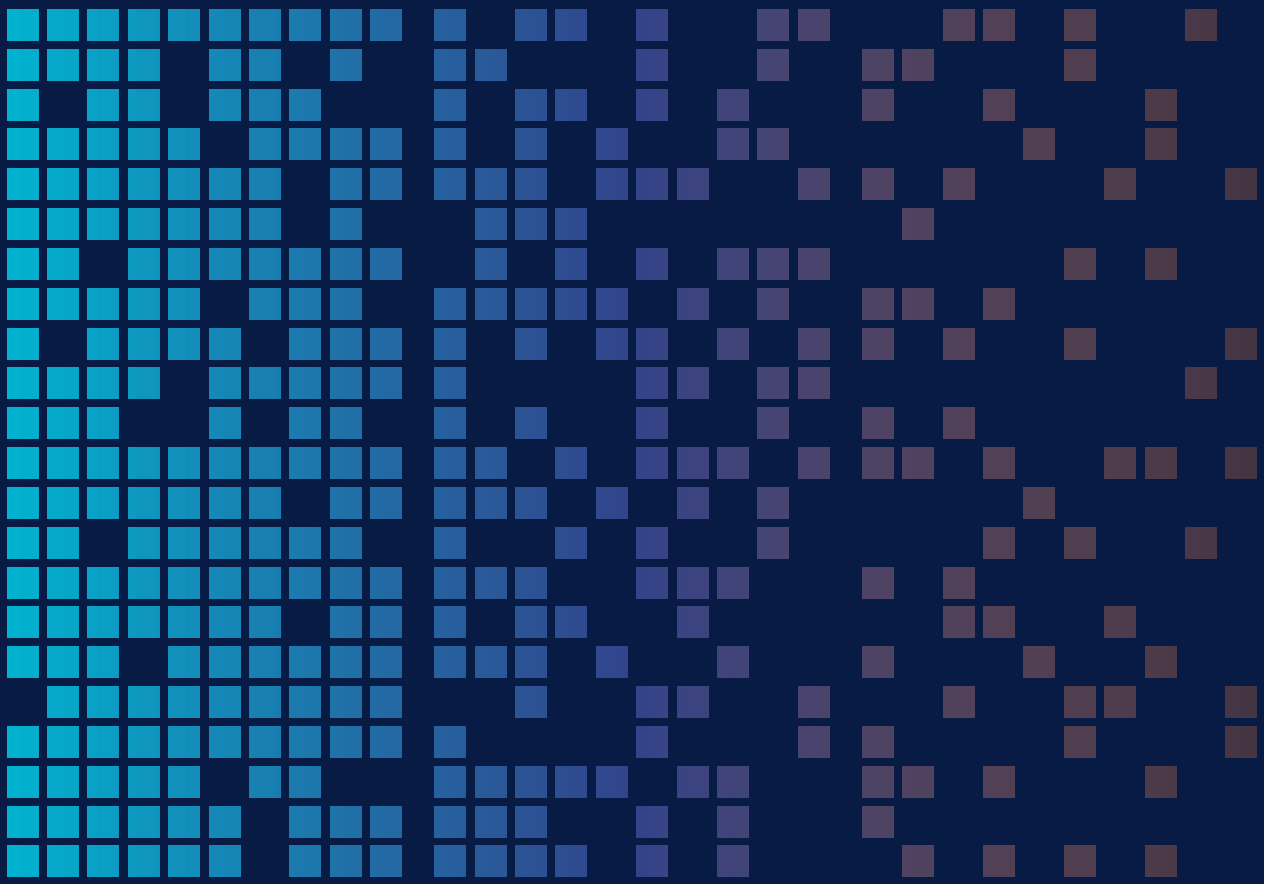
Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre



The silent heist: cybercriminals use information stealer malware to compromise corporate networks

Content Complexity
MODERATE ● ● ○

cyber.gov.au

Table of contents

Context

Information stealer malware steals user credentials and system information that cybercriminals exploit, predominantly for monetary gain. Information stealers have been observed in cybercrime attacks against multiple organisations and sectors worldwide, including Australia. This publication provides readers with cyber security guidance on information stealer malware, including threat activity and mitigation advice for organisations and their employees.

Key points

- Information stealer malware, also known as info stealers, are a type of malware designed to collect information from a victim's device. This can include user names and passwords, credit card details, cryptocurrency wallets, local files, and browser data including cookies, user history and autofill form details.
- Cybercriminals may seek to purchase and use stolen user credentials associated with corporate accounts to gain initial access to devices of the victim's employer, their clients and other enterprise systems. Subsequent impact to these organisations can include ransomware, extortion, business email compromise and theft of intellectual property.
- The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) has identified corporate network breaches that originated in employees accessing work resources from compromised personal devices. In multiple instances, cybercriminals gained initial access to corporate networks by using stolen valid user credentials. Our investigations showed that extensive compromises usually occurred after cybercriminals had successfully accessed privileged user accounts.
- Organisations that facilitate employees, contractors, managed service providers or other entities to access their network remotely, including with Bring Your Own Device (BYOD) hardware, need to be aware of the risks of info stealers and protect themselves from this threat. Cybercriminals deploy info stealers to victim devices using a wide range of techniques, including phishing emails, pirated software downloads, search engine optimisation (SEO) techniques, malicious advertisements or malicious links posted on social media platforms. In general, devices that are used for both work and personal purposes are at a higher risk of infection via these techniques due to user behaviour and reduced security controls.
- Info stealers offer an attractive model for cybercriminals to monetise cybercrime activity, particularly for entry-level cybercriminals and those with limited technical proficiency. Some cybercriminals will market info stealer products under a Malware-as-a-Service (MaaS) style program, charging a monthly subscription fee for their use.

Background

The use of info stealers by cybercriminals presents a threat to the security and wellbeing of Australian organisations. Info stealer infections commonly present as precursor activity to major cyber security incidents, as cybercriminals use them to gather user credentials. These user credentials, especially those providing access to internet-facing remote services or privileged accounts, are then exploited to enable initial access into corporate systems and data.

Note: Initial access brokers play a specialised role within the cybercrime ecosystem by purchasing and validating stolen user credentials. They then auction off high-quality user credentials, for sought-after corporate environments, to cybercriminals who will use the user credentials to exploit the organisation's corporate network.

Stolen valid user credentials are highly valuable to cybercriminals, because they expedite the initial access to corporate networks and enterprise systems. With stolen valid user credentials, cybercriminals can bypass several typical tactics and techniques, including:

- identifying and researching a target
- enumerating the target's network for vulnerabilities
- developing vectors for initial access, such as:
    - phishing material
    - exploitation of software vulnerabilities
    - targeting remote services, including Remote Desktop Protocol (RDP) or virtual private network (VPN) services
    - brute force attacks against user credentials (password guessing).

These steps require an investment of time and a level of technical aptitude that present a barrier to some cybercriminals. In particular, cybercriminals who are unable to penetrate corporate network defences can directly benefit from info stealer infections, as these infections can provide quick and easy user credential access for desirable corporate networks.

In remote work settings, some employees use personal devices for both work and personal internet browsing. In doing so, employees may opt to store their user credentials in their web browsers' password stores and extensions, or they may make use of web browser autofill features. Info stealers target these password stores, along with authentication cookies and other personal data within the web browser.

Unlike corporate devices, personal devices do not always have enforced enterprise security policies, which poses a higher risk to organisations. For example, employees may engage in activities, such as downloading pirated software and high-risk online browsing, increasing their exposure to cyber threats and malware infections.

Info stealers, distributors, initial access brokers and ransomware affiliates now form a core portion of a cybercrime ecosystem driven by financial profit. The ecosystem grows more efficient when cybercriminals specialise and develop capabilities that target particular stages of an attack, and then sell that capability as a service to other criminal affiliates.

Threat activity

ASD's ACSC is tracking and monitoring a rise of info stealer activity globally, which presents a growing threat to Australian networks. Industry reporting indicates that info stealers were the most popular malware variant across cybercrime activity throughout 2023. The increasing volume of stolen data for sale on dark web marketplaces, and an increase in initial access broker activity leveraging this data, is reflective of this rising trend, which has accelerated into 2024.

Information stealer ecosystem

Stage 1: Acquire the malware

Info stealers are usually offered, on cybercriminal marketplaces, as MaaS or Stealer-as-a-Service, or sold as source code. MaaS refers to a business model whereby a malware developer sells a subscription to their malicious software to individuals via a web-based platform, similar to legitimate Software-as-a-Service offerings. The MaaS model has lowered the barrier to entry for cybercriminals, as it allows individuals without extensive technical skills to distribute malware and collect stolen information for use in cyber attacks.

Info stealers offered as MaaS are generally advertised for a relatively inexpensive monthly fee, and provide cybercriminals with access to an info stealer dashboard. The dashboard facilitates the creation of info stealer malware, organises stolen data and tracks the number of compromised systems. MaaS operators offer feature updates, tools and technical support to evade detection by antivirus software and to attract and retain subscribers. Many info stealers have the ability to delete themselves from the victim's device after performing data exfiltration.

Stage 2: Distribution

Cybercriminals who distribute info stealers and collect information from compromised devices are known as 'Traffers' (traffic distributors). Traffers direct victims to malicious links, facilitating the spread of info stealers as part of broad campaigns. Most campaigns are indiscriminate, relying on opportunistic infections. However, some campaigns are tailored to specific industries and involve targeted spear-phishing against specific victims. Traffers conduct these more targeted campaigns in response to customer demand; for example, where buyers are seeking access to specific high value organisations or sectors.

Traffers will deploy info stealers to victim devices using a wide range of techniques, including:

- **botnets:** networks of compromised computer systems controlled by cybercriminals to carry out malicious actions, such as delivering phishing messages or malware

- **phishing:** attempts to gain sensitive information by deception, including via emails or direct messages on social media, forums and messaging apps, which are common distribution methods that have lowered the barrier to entry for cybercriminals:
    - These messages commonly contain a malicious link, rather than attaching malicious files to the email itself.
- **malicious search results:** delivered via search engine optimisation (SEO) techniques that direct targets to websites serving malware disguised as legitimate software or other content
- **malvertising:** the use of harmful code, injected into legitimate online advertisements, to distribute malware
- **cracked or pirated software:** downloads, including video games, shared via YouTube videos, with malicious links in the video description or comments, or from untrustworthy download sites
- **social media advertisements and posts:** directing targets to disguised malware files
- **malicious software updates:** commonly disguised as web browser updates

Stage 3: Data harvesting

Once an info stealer executes on the victim's device, it begins collecting sensitive data from the compromised machine. Apart from stealing user credentials, in cases where info stealers are part of a botnet, cybercriminals can remotely control the compromised device by sending configuration commands to activate additional capabilities or deliver other malware. In general, info stealers are capable of stealing:

- user names and passwords, particularly those stored in web browsers' multi-factor authentication (MFA) user sessions / tokens
- authentication cookies
- web browser autofill form information
- email credentials, contents and contacts
- web browsing history
- user documents
- credit card details
- chat logs from desktop messaging apps
- system information
- cryptocurrency wallets
- VPN or File Transfer Protocol (FTP) credentials.

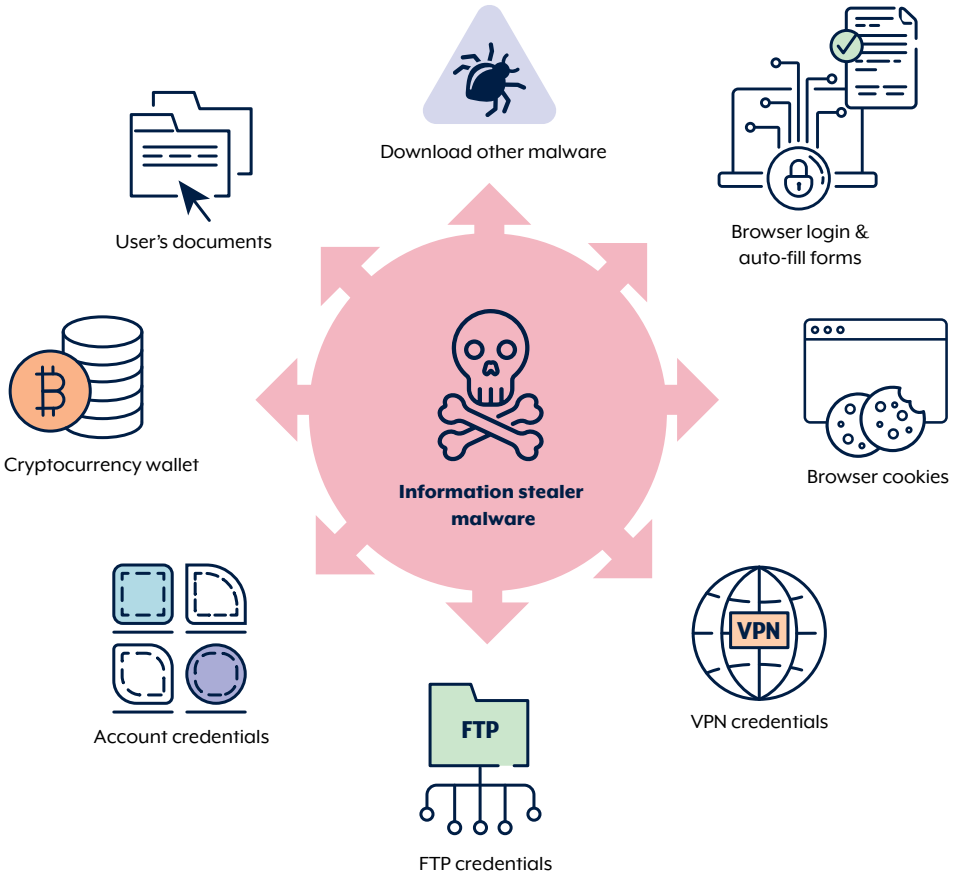


Figure 1. Info stealers capability

Some web browser authentication cookies keep a user logged into an account or service for multiple days at a time, so that users are not required to re-authenticate. If stolen, these authentication cookies could effectively bypass MFA requirements and provide cybercriminals access into victim accounts, corporate networks and enterprise systems.

Stage 4: Data aggregation and monetisation

Info stealers are configured to exfiltrate victim information, known as 'logs', to malicious command-and-control servers. In general, info stealers leverage popular messaging apps, such as Telegram and Discord, to share a feed of logs with cybercriminals.

Specialised marketplaces exist on Telegram and across the dark web for the sale and trade of logs. Cybercriminals monetise the logs in various ways, including:

- selling logs on criminal marketplaces, including to initial access brokers
- exploiting the victim directly, via identity theft and extortion
- leveraging the information for initial access into corporate networks for ransomware activity.

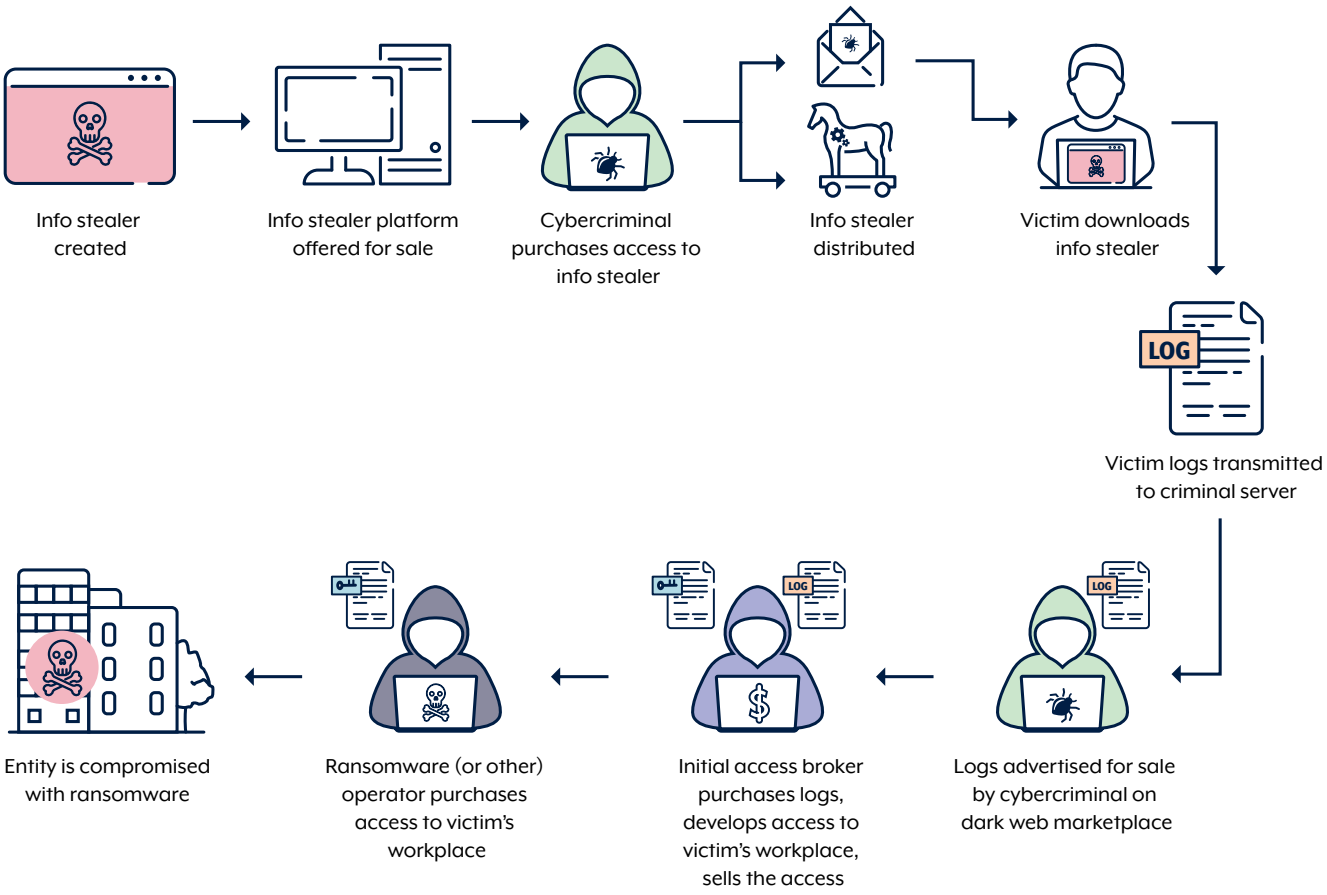


Figure 2. Info stealer ecosystem and possible impact on an organisation

Implications

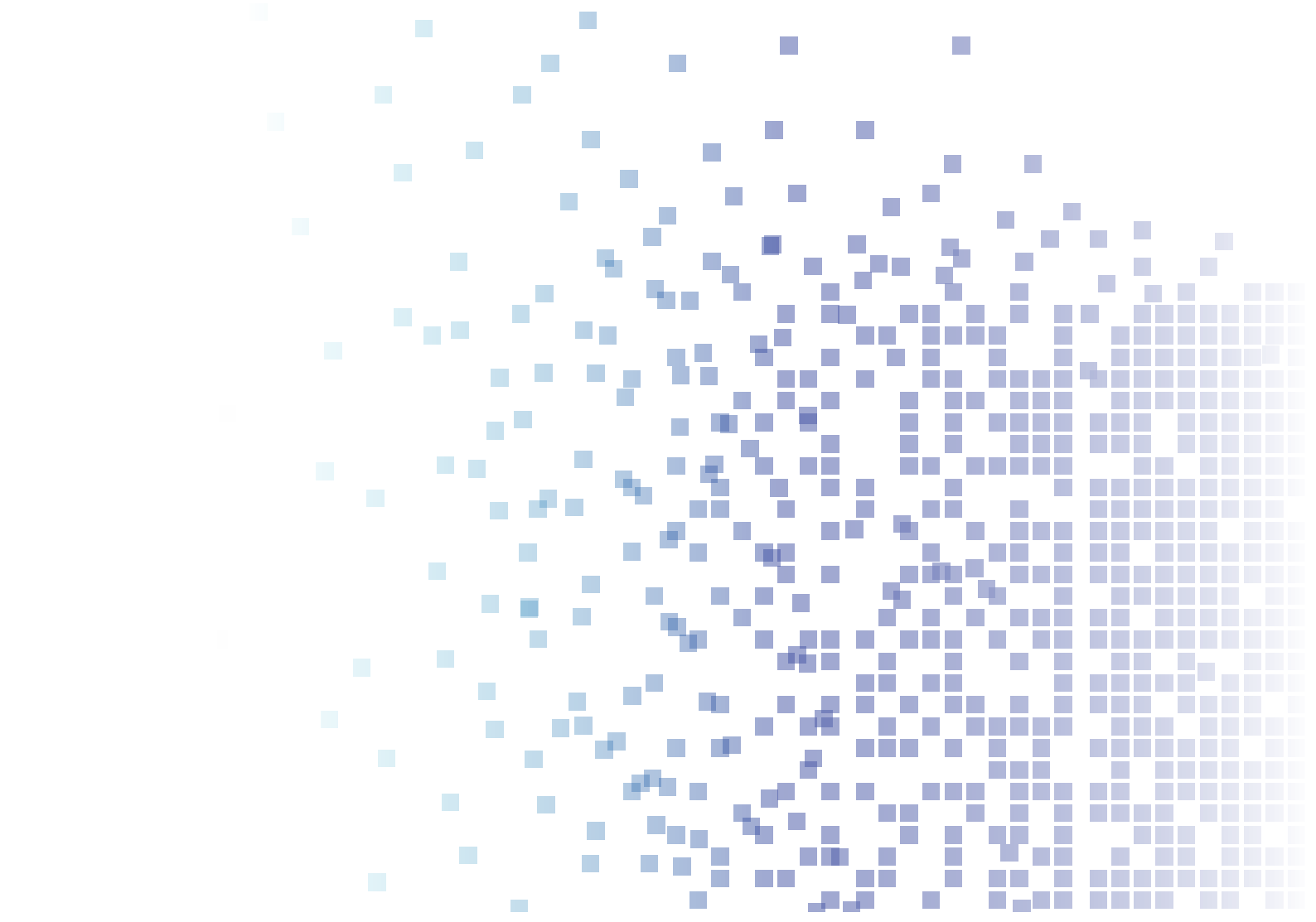
Info stealers can have severe implications for both individuals and organisations. Where info stealers collect user credentials, cybercriminals may use these user credentials to access corporate networks or enterprise systems with valid user accounts, often delaying detection by system owners.

For **organisations** affected by info stealers, consequences may include:

- ransomware
- data breach
- business email compromise
- theft of intellectual property
- theft of sensitive information.

For an **individual** affected by info stealers, consequences may include:

- unauthorised access to personal email or social media accounts
- increased risk of identity theft
- increased risk of phishing attacks
- financial loss or unauthorised access to financial accounts
- loss of privacy.



Case study

This case study has been anonymised to enable public dissemination. It draws on multiple cyber security incidents that have impacted Australian entities that have reported to ASD's ACSC. The impacted entity is hereafter referred to as 'the organisation'. The names of the individuals in this case study are fictitious and details have been removed to protect the identity of victims.

The organisation is an Australian business that allows staff to access corporate systems from personal devices. Alice is an employee of the organisation who works remotely.

When working from home, Alice remotely accesses the corporate network of her organisation using her personal laptop. Alice **downloaded**, onto her **personal laptop**, a version of Notepad++ (which is a type of note-taking software) from a website she believed to be legitimate. An **info stealer** was disguised as the installer for the Notepad++ software.

When Alice attempted to install the software, the info stealer activated and began **harvesting user credentials** from her laptop. This included her work username and password, which she had saved in her web browser's saved logins feature. The info stealer then sent those user credentials to a remote command-and-control server controlled by a cybercriminal group.

The stolen logs were packaged with others and then **sold to cybercriminals** via a dark web marketplace.

A cybercriminal named Bob purchased Alice's user credentials, identifying user credentials for services on her organisation's network. Alice's organisation had **not configured MFA** for these services, which meant that Bob could use the stolen user credentials alone to successfully **authenticate and access** the corporate network.

Bob accessed the corporate network of Alice's organisation undetected using the stolen **valid user credentials**. Bob was able to pivot laterally through the corporate network, identifying sensitive data belonging to the organisation and exfiltrating it in order to extort the company.

Having stolen the sensitive data, Bob **encrypted** the organisation's **databases and file systems** to make them inaccessible.

Mitigations

Organisations may not be able to enforce controls on devices that connect to their corporate network, particularly on personal devices used by employees working remotely. ASD's ACSC recommends organisations focus on implementing controls to protect themselves from the risk of info stealers targeting user credentials. These mitigations include:

Provide cyber security awareness training for staff

- Prevent successful targeted social engineering and malicious file downloads by providing effective training to staff.
- Raise awareness of info stealers, their delivery methods and the phishing threats to your organisation.

Secure corporate accounts

- Implement MFA:
  - Implement MFA across external and internal services, systems and sensitive data repositories, particularly for webmail, VPNs, and privileged user accounts that access critical systems. Best practice is to implement phishing-resistant MFA on all accounts.
- Disable user accounts when they are no longer required.
- Restrict administrator privileges:
  - Perform network administration and other privileged tasks using a dedicated locked-down workstation only (i.e. a secure admin workstation).
  - Follow least-privilege best practice by requiring administrators to use privileged user accounts for managing systems and standard user accounts for non-administrative tasks.
  - Prevent privileged user accounts (excluding those explicitly authorised to access online services) from accessing the internet, email and web services.
  - Consider implementing just-in-time administration for systems and applications.
- Enforce the management and auditing of privileged user accounts.
- Update passwords periodically, particularly external-facing remote-access accounts.
- Enforce lifespan time outs and sunset policies on session tokens and cookies.

Harden enterprise mobility

- Perform an enterprise mobility risk assessment and implement enterprise mobility hardening guidelines.
- Implement a Bring Your Own Device (BYOD) policy if you allow employees to use personal devices for work, as corporately managed devices are more secure than unmanaged personal devices.

Review and assess supply chain risks from vendors accessing your networks, including Software-as-a-Service (Saas) vendors and Managed Service Providers. How to Manage Your Security When Engaging a Managed Service Provider.

Protect your corporate network

- Keep applications and operating systems up to date.
- Apply local security policies to enforce application control with a strict allow list.
- Implement network segmentation to separate network segments based on role and functionality.
- Audit and monitor user activities, especially for remote employees.
  - Monitoring privileged accounts can reveal unauthorised access to sensitive data or unusual data transfer activities, such as large volumes of data uploaded to an external network.
- Implement data-loss prevention policies and tools to prevent unauthorised data transfers.

Become an ASD Cyber Security Network Partner and join ASD's Cyber Threat Intelligence Sharing (CTIS) service

- CTIS is a two-way sharing platform that enables government and industry partners to receive and share information about malicious cyber activity.
- ASD's ACSC is tracking info stealer activity and shares details of active command and control infrastructure through the CTIS platform.
- Sign up to become a partner and protect your organisation and customer data from cybercriminal threats.

Prepare for a compromise

- Develop a cyber security incident response plan to use in the event of an info stealer compromise. Ensure that employees are aware of what to do and who to contact if they suspect they have downloaded a suspicious file.

Implement ASD's ACSC's Essential Eight

- In addition to the mitigations mentioned above, ASD's ACSC strongly recommends implementing the remainder of ASD's ACSC's Essential Eight.

Advice for your employees when working remotely

- Protect your information on your personal devices
  - Develop good cyber hygiene and do not click on suspicious links or pop-ups, or download files or software from unknown or untrusted sources.
  - Use distinct passwords for work and personal accounts. Use MFA for personal accounts where possible.
  - Do not store your work credentials in a personal password manager unless explicitly approved by your employer. This includes your web browser's password manager. **If in doubt, request that your employer provide a corporately supported password manager.**
  - Do not log in to your work accounts from shared or communal workstations.
  - Be aware of what is being stored in your web browser's autofill feature. Info stealers target the data that browsers save to autofill forms. When filling in web forms, consider manually entering sensitive data, such as credit card numbers, rather than saving it to your web browser's autofill feature.
  - Log out from all online services and clear web browser cookies after finishing a browsing session in order to reduce the information available to info stealers.
  - Ensure that your operating system's built in antivirus solution is enabled. If you use a third-party antivirus solution, ensure that it is kept up to date and is from a reputable vendor.

Assistance

Australian organisations that have been impacted or require assistance regarding an info stealer compromise can contact ASD's ACSC via **1300 CYBER1 (1300 292 371)** or by submitting a report at cyber.gov.au/report.

ASD's ACSC encourages entities to report suspicious network activity and indicators of compromise associated with info stealers, even if an incident is considered contained. We use the information you provide to improve our understanding of cyber threat actors' tactics, techniques and procedures, which helps us to warn other Australian organisations that have been targeted in the same way.

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre