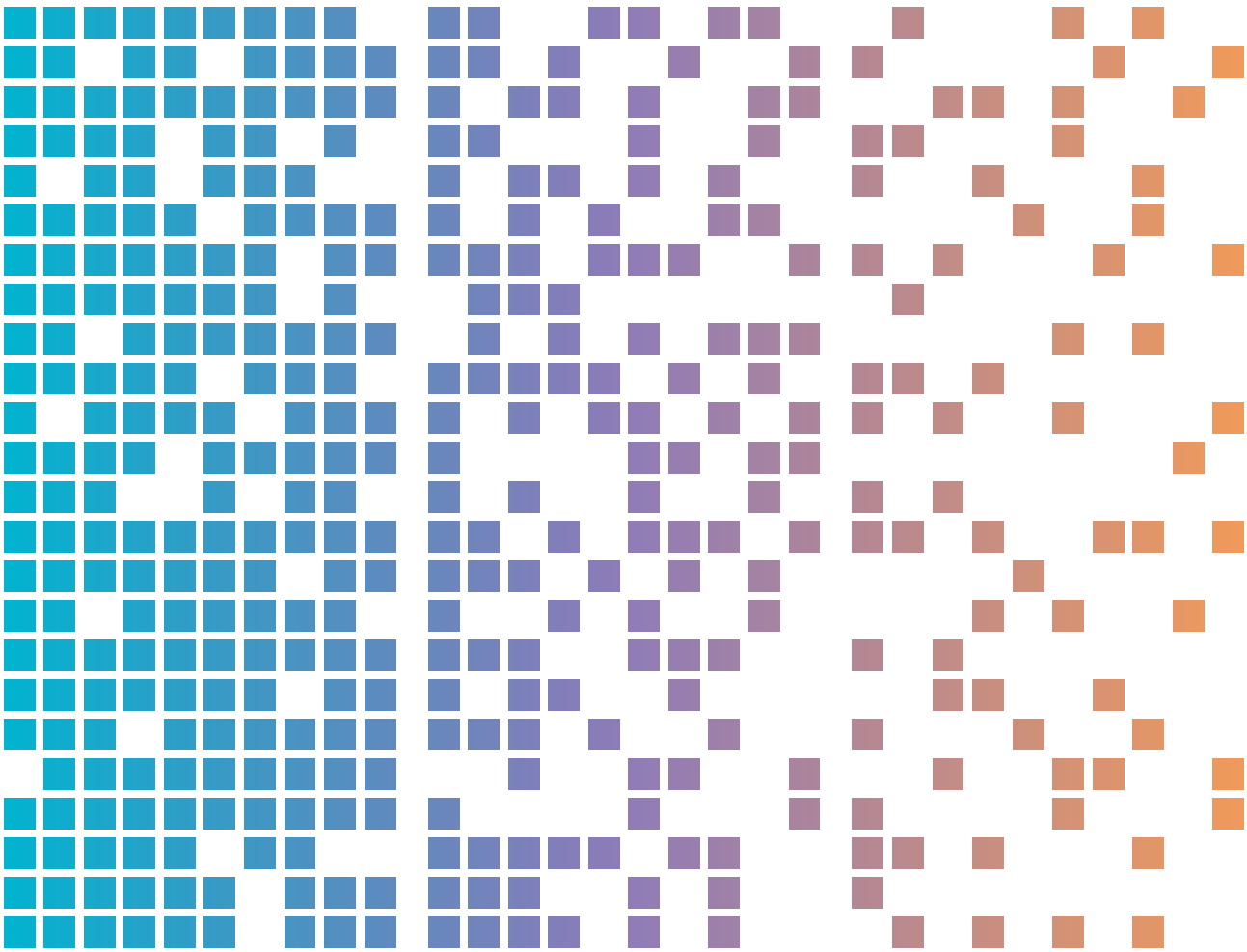
Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

# Ang silent heist: gumagamit ang mga cybercriminal ng malware na nagnanakaw ng impormasyon (information stealer malware) para ikompromiso ang mga corporate network



Ang pagiging kumplikado ng nilalaman
KATAMTAMAN

# Talaan ng nilalaman

# Konteksto

Ang information stealer malware ay nagnanakaw ng mga kredensyal ng user at impormasyon ng system na sinasamantala ng mga cybercriminal, pangunahin para makakuha ng pera. Ang mga info stealer ay naobserbahan sa mga cybercrime attack laban sa maramihang organisasyon at sektor sa buong mundo, kabilang ang Australya. Ang publikasyong ito ay nagbibigay sa mga mambabasa ng gabay sa cyber security ukol sa information stealer malware, kabilang ang threat activity at payo sa mitigasyon para sa mga organisasyon at kanilang mga empleyado.

# Mga pangunahing punto

- Ang information stealer malware, na kilala rin bilang mga info stealer, ay isang uri ng malware na idinisenyo upang mangolekta ng impormasyon mula sa device ng biktima. Maaaring kabilang dito ang mga user name at password, mga detalye ng credit card, mga cryptocurrency wallet, mga local file, at browser data kabilang ang cookies, user history at mga detalye ng autofill form.
- Maaaring nais ng mga cybercriminal na bumili at gumamit ng mga ninakaw na kredensyal ng user na nauugnay sa mga corporate account upang makakuha ng paunang access sa mga device ng employer ng biktima, kanilang mga kliyente at iba pang mga enterprise system. Maaaring kabilang sa magiging kasunod na epekto sa mga organisasyong ito ang ransomware, pangingikil, kompromiso sa email ng negosyo at pagnanakaw ng intelektwal na ari-arian.
- Tinukoy ng Australian Signals Directorate ng Australian Cyber Security Center (ASD's ACSC) ang mga paglabag sa corporate network na nagmula sa pag-access ng mga empleyado sa work resources mula sa mga nakompromisong personal device. Sa maraming pagkakataon, ang mga cybercriminal ay nakakakuha ng paunang access sa mga corporate network sa pamamagitan ng paggamit ng mga ninakaw na balidong kredensyal ng user. Ang aming mga pagsisiyasat ay nagpakita na ang malawak na kompromiso ay karaniwang nangyayari pagkatapos matagumpay na ma-access ng mga cybercriminal ang mga privileged user account.
- Ang mga organisasyong nagbibigay-daan upang ma-access ng mga empleyado, kontratista, pinamamahalaang service provider o iba pang entity ang kanilang network nang malayuan, kabilang dito ang Bring Your Own Device (BYOD) hardware, ay kailangang magkaroon ng kamalayan sa mga panganib na dulot ng mga info stealer (info stealers) at protektahan ang kanilang sarili laban sa bantang ito. Naglalagay ang mga cybercriminal ng mga info stealer sa mga device ng biktima gamit ang maramihang teknik, kabilang ang mga phishing email, pirated software download, mga teknik sa search engine optimization (SEO), malicious advertisement o malicious link na naka-post sa mga social media platform. Sa pangkalahatan, ang mga device na ginagamit para sa trabaho at para sa personal na paggamit ay mas nanganganib sa impeksyon sa pamamagitan ng mga teknik na ito dahil sa pag-uugali ng user (user behaviour) at nabawasang mga kontrol sa seguridad.
- Nag-aalok ang mga info stealer ng isang kaakit-akit na modelo para sa mga cybercriminal upang pagkakitaan ang aktibidad ng cybercrime, partikular para sa mga entry-level na cybercriminal at ang may limitadong teknikal na kasanayan. Ibebenta ng ilang cybercriminal ang mga produkto ng info stealer sa ilalim ng Malware-as-a-Service (MaaS) style program, na naniningil ng buwanang bayad sa subscription para sa paggamit nito.

# Background

Ang paggamit ng mga cybercriminal ng mga info stealer ay banta sa seguridad at kagalingan ng mga organisasyon sa Australya. Ang mga impeksyong info stealer ay karaniwang isang pasimulang aktibidad (precursor activity) sa mga malalaking insidente sa cyber security, dahil ginagamit ng mga cybercriminal ang mga ito upang mangalap ng mga kredensyal ng user. Ang mga kredensyal ng user na ito, lalo na ang mga nagbibigay ng access sa mga malayuang serbisyong nakaharap sa internet (internet-facing remote services) o mga privileged account, ay sinasamanta upang paganahin ang paunang pag-access sa mga corporate system at data.

**Tandaan**: Ang mga paunang access broker ay gumaganap ng espesyal na papel sa loob ng cybercrime ecosystem sa pamamagitan ng pagbili at pagba-validate ng mga ninakaw na kredensyal ng user. Pagkatapos, ang mga de-kalidad na kredensyal ng user, para sa mga hinahangad na corporate environment ay isusubasta (auction) nila sa mga cybercriminal na gagamitin ang mga kredensyal ng user upang samantalahin ang corporate network ng organisasyon.

Ang mga ninakaw na balidong kredensyal ng user ay lubos na mahalaga sa mga cybercriminal, dahil pinapabilis nita ang paunang pag-access sa mga corporate network at enterprise system. Sa paggamit ng mga ninakaw na balidong kredensyal ng user, maaaring lampasan ng mga cybercriminal ang ilang karaniwang taktika at teknik, kabilang ang:

- pagtukoy at pagsasaliksik ng isang target
- pag-enumerate sa network ng target para sa mga kahinaan
- pagbuo ng mga vector para sa paunang pag-access, tulad ng:
  - materyal sa phishing
  - pagsasamantala sa mga kahinaan ng software
  - pag-target sa malayuang serbisyo, kabilang ang RemoteDesktop Protocol (RDP) o virtual privatenetwork (VPN) na mga serbisyo
  - brute force na pag-atake laban sa mga kredensyal ng user (paghula ng password).

Ang mga hakbang na ito ay nangangailangan ng panahon at antas ng teknikal na kakayahan na nagiging hadlang sa ilang mga cybercriminal. Sa partikular, ang mga cybercriminal na hindi makapasok sa mga depensa ng corporate network ay maaaring direktang makinabang mula sa mga impeksyon ng info stealer, dahil ang mga impeksyong ito ay maaaring magbigay ng mabilis at madaling pag-access sa kredensyal ng user para sa mga hinahangad na corporate network.

Sa mga setting na malayuang pagtatrabaho, ang ilang empleyado ay gumagamit ng mga personal na device para sa trabaho at personal na pagba-browse sa internet. Sa paggawa nito, maaaring piliin ng mga empleyado na iimbak ang kanilang mga kredensyal ng user sa mga password store at extension ng kanilang mga web browser, o maaari nilang gamitin ang mga autofill feature ng web browser. Tina-target ng mga info stealer ang mga password store na ito, kasama ang authentication cookies at iba pang personal na data sa loob ng web browser.

Hindi tulad ng mga corporate device, ang mga personal device ay hindi palaging may ipinapatupad na mga patakaran sa seguridad ng enterprise, na nagdudulot ng mas mataas na panganib sa mga organisasyon. Halimbawa, ang mga empleyado ay maaaring magsagawa ng mga aktibidad, tulad ng pag-download ng pirated software at high-risk online browsing na nagdaragdag ng kanilang pagkakalantad sa mga cyber threat at mga malware infection.

Ang mga info stealer, mga distributor, mga broker ng paunang pag-access at mga kasapakat ng ransomware ay bumubuo na ngayon ng isang pangunahing bahagi ng isang cybercrime ecosystem na udyok ng kita sa pananalipi. Ang ecosystem ay nagiging mas mahusay kapag ang mga cybercriminal ay nagdadalubhasa at bumubuo ng mga kakayahan na nagta-target ng mga partikular na yugto ng isang pag-atake, at pagkatapos ay ibinebenta ang kakayahang iyon bilang isang serbisyo sa iba pang mga kasapakat sa krimen.

# Aktibidad ng pagbabanta (Threat activity)

Sinusubaybayan at mino-monitor ng ACSC ng ASD ang pagtaas ng info stealer activity sa buong mundo, na nagpapahayag ng lumalaking banta sa mga network ng Australya. Ipinapakita ng pag-uulat sa industriya na ang mga info stealer ang pinakapopular na variant ng malware sa cybercrime activity noong 2023. Ang pagtaas ng dami ng ninakaw na data na ibinebenta sa mga dark web marketplace, at ang pagtaas ng aktibidad ng paunang access ng broker na gumagamit ng data na ito, ay sumasalamin sa tumataas na trend na ito, na bumilis noong 2024.

# Ecosystem ng nagnanakaw ng impormasyon (Information stealer ecosystem)

## Yugto 1: Kunin ang malware

Karaniwang inaalok ang mga info stealer, sa mga cybercriminal marketplace, bilang MaaS o Stealer-as-a-Service, o ibinebenta bilang source code. Ang MaaS ay tumutukoy sa isang modelo ng negosyo kung saan ang isang malware developer ay nagbebenta sa mga indibidwal ng subscription sa kanilang malicious software sa pamamagitan ng isang web-based platform, katulad ng mga lehitimong handog na Software-as-a-Service. Sa modelo ng MaaS mas bumaba ang harang sa pagpasok ng mga cybercriminal, dahil pinapayagan nito ang mga indibidwal na walang malawak na teknikal na kasanayan na ipamahagi ang malware at mangolekta ng ninakaw na impormasyon para magamit sa mga cyber attack.

Ang mga info stealer na inaalok bilang MaaS ay karaniwang ina-advertise na may kamurahang buwanang bayad, at nagbibigay sa mga cybercriminal ng access sa info stealer dashboard. Pinapadali ng dashboard ang paglikha ng info stealer malware, inaayos ang ninakaw na data at sinusubaybayan ang bilang ng mga nakompromisong system. Nag-aalok ang mga operator ng MaaS ng mga feature update, mga tool at teknikal na suporta upang maiwasang matuklasan ng antivirus software at para maakit at mapanatili ang mga subscriber. Maraming mga info stealer ang may kakayahang tanggalin ang kanilang sarili mula sa device ng biktima pagkatapos magsagawa ng data exfiltration.

## Yugto 2: Pamamahagi

Ang mga cybercriminal na namamahagi ng mga info stealer at nangongolekta ng impormasyon mula sa mga nakompromisong device ay kilala bilang 'Traffers' (mga distributor ng trapiko). Idinidirekta ng mga traffer ang mga biktima sa mga malicious link, na pinapadali ang pagkalat ng mga info stealer bilang bahagi ng malawak na mga kampanya. Karamihan sa mga kampanya ay walang pinipili at umaasa sa mga pagkakataong makapagkalat ng impeksyon. Gayunpaman, ang ilang mga kampanya ay iniangkop sa mga partikular na industriya at nagsasangkot ng naka-target na spear-phishing laban sa mga partikular na biktima. Isinasagawa ng mga traffer ang mga mas naka-target na kampanyang ito bilang tugon sa demand ng customer; halimbawa, kung saan ang mga mamimili ay naghahanap ng access sa mga partikular na organisasyon o sektor na may mataas na halaga (high-value).

Magde-deploy ang mga traffer ng mga info stealer sa mga device ng biktima gamit ang malawak na hanay ng mga teknik, kabilang ang:

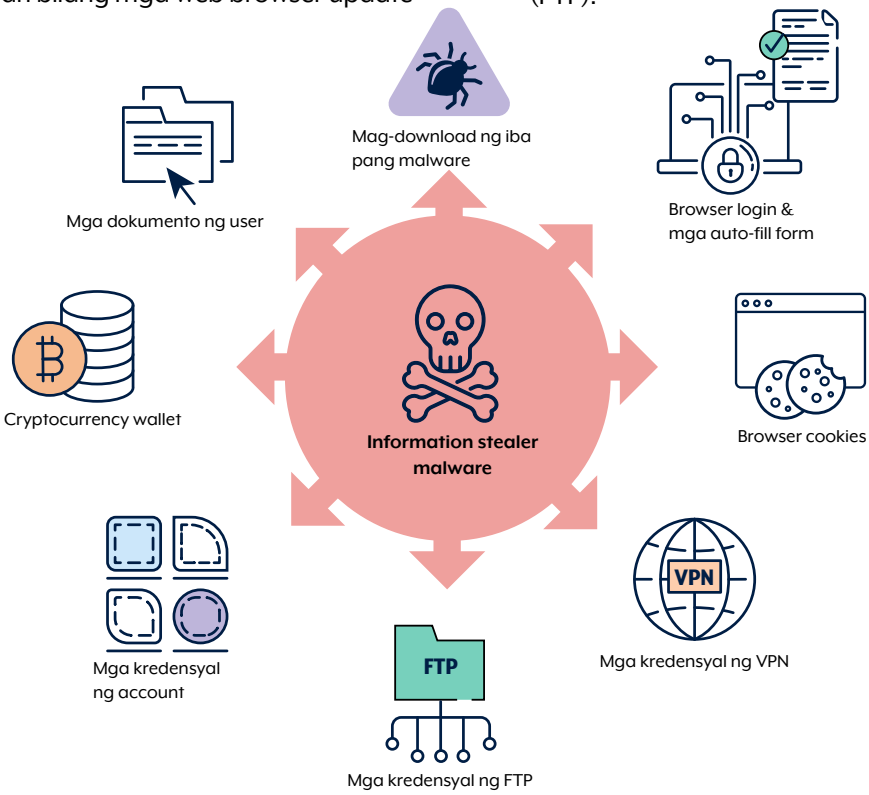
- **botnets**: mga network ng mga nakompromisong computer system na kinokontrol ng mga cybercriminal upang magsagawa ng mga malicious na aksyon, gaya ng paghahatid ng mga phishing message o malware

- **phishing**: mga pagtatangka na makakuha ng sensitibong impormasyon sa pamamagitan ng panlilinlang, kabilang dito ang mga email o direktang mensahe sa social media, mga forum at mga messaging app, na mga karaniwang paraan ng pamamahagi na nagbaba ng harang para makapasok ang mga cybercriminal:
  - Ang mga mensaheng ito ay karaniwang naglalaman ng malicious link, sa halip na mag-attach ng mga malicious file sa mismong email.
- **mga malicious search result**: inihatid sa pamamagitan ng mga teknik ng search engine optimization (SEO) na nagdidirekta ng mga target sa mga website na naghahatid ng malware na itinago bilang lehitimong software o iba pang content
- **malvertising**: ang paggamit ng mapaminsalang code na isinisingit sa mga lehitimong online advertisement, upang ipamahagi ang malware
- **crack o pirated software**: mga pag-download, kabilang ang mga video game, na ibinahagi sa pamamagitan ng mga video sa YouTube, na may mga malicious link sa video description o sa mga komento, o mula sa hindi mapagkakatiwalaang mga download site
- **mga social media advertisement at post**: nagdidirekta sa mga target papunta sa mga nagkukubling (disguised) malware file
- **mga malicious software update**: karaniwang nagkukunwari bilang mga web browser update

## Yugto 3: Pag-harvest ng data (Data harvesting)

Kapag na-execute na ang info stealer sa device ng biktima, magsisimula na itong mangolekta ng sensitibong data mula sa nakompromisong device. Bukod sa pagnanakaw ng mga kredensyal ng user, sa mga kaso kung saan ang mga info stealer ay bahagi ng isang botnet, maaaring malayuang kontrolin ng mga cybercriminal ang nakompromisong device sa pamamagitan ng pagpapadala ng mga configuration command upang i-activate ang mga karagdagang kakayahan (capabilities) o maghatid ng iba pang malware. Sa pangkalahatan, ang mga info stealer ay may kakayahang magnakaw ng:

- mga user name at password, lalo na ang mga nakaimbak sa mga multi-factor authentication (MFA) user sessions / tokens ng mga web browser
- authentication cookies
- impormasyon sa autofill form ng web browser
- mga kredensyal sa email, nilalaman at mga contact
- kasaysayan ng pagba-browse sa web (web browsing history)
- mga dokumento ng user
- mga detalye ng credit card
- mga chat log mula sa mga desktop messaging app
- system information
- mga cryptocurrency wallet
- Mga kredensyal ng VPN o File Transfer Protocol (FTP).




**Larawan 1. Kakayahan (Capability) ng info stealer**

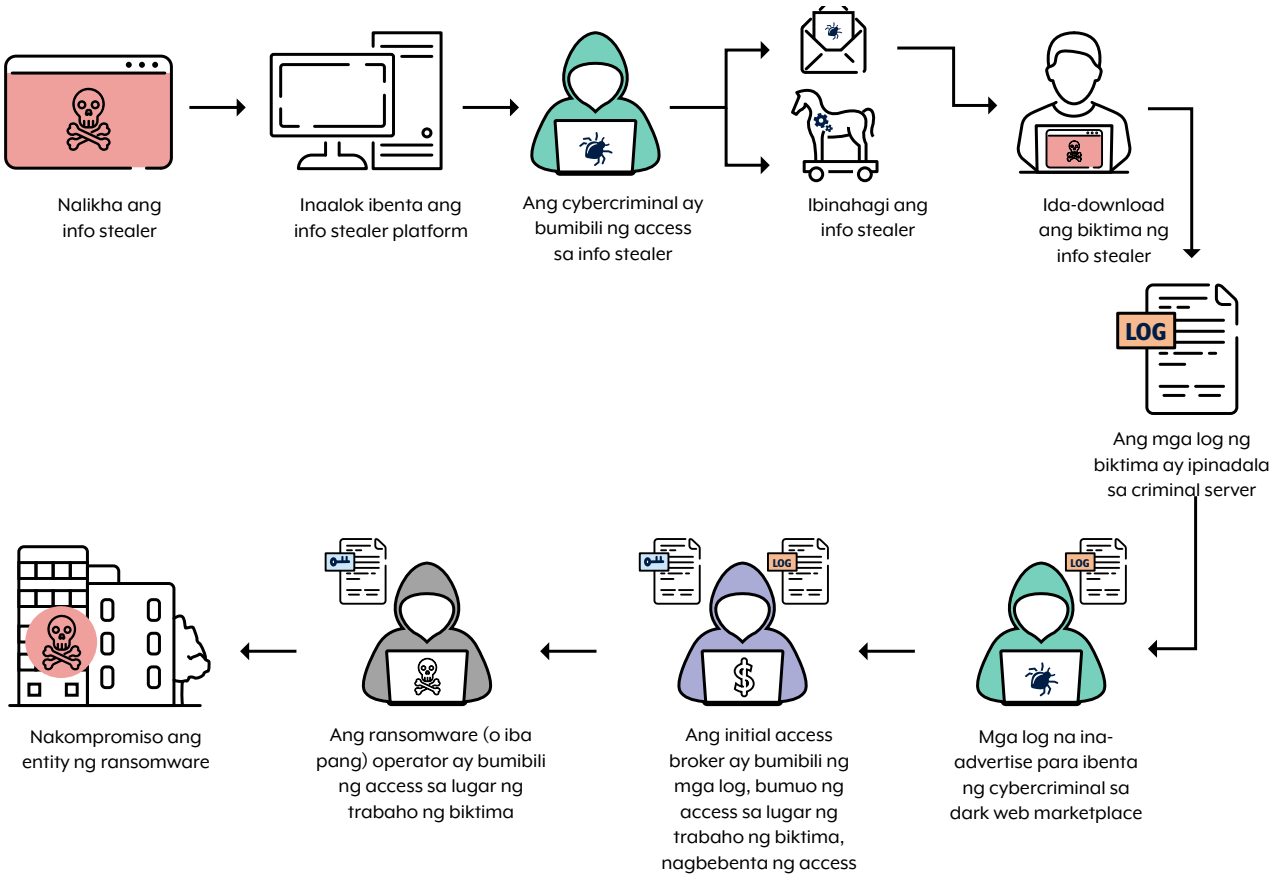
Ang ilang web browser authentication cookies ay nagpapanatili sa isang user na naka-log in sa isang account o serbisyo sa loob ng maraming araw sa isang pagkakataon, upang ang mga user ay hindi na kailangang muling mag-authenticate. Kung nanakaw, ang mga authentication cookies na ito ay maaaring epektibong lampasan ang mga hinihingi ng MFA at magbigay ng access sa mga cybercriminal para mapasok ang mga account ng biktima, mga corporate network at mga enterprise system.

## Yugto 4: Pagsasama-sama ng data at monetisation

Ang mga info stealer ay na-configure upang i-exfiltrate ang impormasyon ng biktima, na kilala bilang 'mga log', sa mga malicious command-and-control server. Sa pangkalahatan, ginagamit ng mga info stealer ang mga popular na messaging app, gaya ng Telegram at Discord, upang magbahagi ng feed ng mga log sa mga cybercriminal.

Ang mga espesyal na marketplace ay umiiral sa Telegram at sa buong dark web para sa pagbebenta at pag-trade ng mga log. Pinagkakakitaan ng mga cybercriminal ang mga log sa iba't ibang paraan, kabilang ang:

- pagbebenta ng mga log sa mga criminal marketplace, kasama ang mga initial access broker
- direktang pagsasamantala sa biktima, sa pamamagitan ng pagnanakaw ng pagkakakilanlan (identity theft) at pangingikil
- paggamit ng impormasyon para sa paunang pag-access sa mga corporate network para sa ransomware activity.




**Larawan 2. Info stealer ecosystem at posibleng epekto sa isang organisasyon**

# Mga implikasyon

Ang mga info stealer ay maaaring magkaroon ng matinding epekto para sa mga indibidwal at organisasyon. Kung nakakolekta ang info stealer ng mga kredensyal ng user, maaaring gamitin ng mga cybercriminal ang mga kredensyal ng user na ito upang ma-access ang mga corporate network o enterprise system gamit ang balidong mga user account, na kadalasang magpapaantala sa pagtuklas sa mga may-ari ng system.

Para sa **mga organisasyon** na apektado ng mga info stealer, maaaring kabilang sa mga kahihinatnan ang:

- ransomware
- data breach
- Nakompromisong business email
- pagnanakaw ng intelektwal na ari-arian (theft of intellectual property)
- pagnanakaw ng sensitibong impormasyon.

Para sa isang **indibidwal** na apektado ng mga info stealer, maaaring kabilang sa mga kahihinatnan ang:

- hindi awtorisadong pag-access sa personal email o mga social media account
- tumaas na panganib ng pagnanakaw ng pagkakakilanlan (identity theft)
- tumaas na panganib ng mga phishing attack
- Pagkaluging pinansyal o hindi awtorisadong pag-access sa mga financial account
- pagkawala ng pribasya.

# Case study

Ang case study na ito ay hindi nagpapakilala upang maibahagi sa publiko. Halaw ito sa maraming insidente ng cyber security na nakaapekto sa mga entity sa Australya na nag-report sa ACSC ng ASD. Ang naapektuhang entity ay tinutukoy dito bilang 'ang organisasyon'. Ang mga pangalan ng mga indibidwal sa case study na ito ay kathang-isip lamang at tinanggal ang mga detalye upang maprotektahan ang pagkakakilanlan ng mga biktima.

Ang organisasyon ay isang negosyo sa Australya na nagpapahintulot sa mga kawani na ma-access ang mga corporate system mula sa mga personal device. Si Alice ay isang empleyado sa organisasyon na malayuang nagtatrabaho.

Kapag nagtatrabaho mula sa bahay, malayuang ina-access ni Alice ang corporate network ng kanyang organisasyon gamit ang kanyang personal laptop. **Nag-download** si Alice, sa kanyang **personal laptop**, ng isang bersyon ng Notepad++ (na isang uri ng software sa pagkuha ng tala) mula sa isang website na pinaniniwalaan niyang lehitimo. Ang **info stealer** ay nagkukunwaring installer para sa Notepad++ software.

Nang sinubukan ni Alice na i-install ang software, na-activate ang info stealer at nagsimulang **mag-harvest ng mga kredensyal ng user** mula sa kanyang laptop. Kasama rito ang kanyang username at password sa trabaho, na na-save niya sa login feature ng kanyang web browser. Pagkatapos ay ipinadala ng info stealer ang mga kredensyal ng user na ito sa isang remote command-and-control server na kinokontrol ng isang cybercriminal group.

Ang mga ninakaw na log ay naka-package kasama ng iba at pagkatapos ay **ibebenta sa mga cybercriminal** sa dark web marketplace.

Isang cybercriminal na nagngangalang Bob ang bumili ng mga kredensyal ng user ni Alice, na tinutukoy ang mga kredensyal ng user para sa mga serbisyo sa network ng kanyang organisasyon. **Hindi na-configure ng organisasyon ni Alice ang MFA** para sa mga serbisyong ito, na nangangahulugang magagamit ni Bob ang mga ninakaw na kredensyal ng user nang mag-isa upang matagumpay na **i-authenticate at i-access** ang corporate network.

Na-access ni Bob ang corporate network ng organisasyon ni Alice nang hindi natuklasan gamit ang ninakaw na **mga balidong kredensyal ng user**. Nagawa ni Bob na mag-pivot sa corporate network, matukoy ang sensitibong data na pagmamay-ari ng organisasyon at ma-exfiltrate ito para makapangikil sa kumpanya.

Sa pagnakaw ng sensitibong data, **na-encrypt** ni Bob ang **mga database at file system** ng organisasyon upang gawin itong di-maa-access.

# Mga mitigasyon

Maaaring hindi maipatupad ng mga organisasyon ang mga kontrol sa mga device na kumokonekta sa kanilang corporate network, lalo na sa mga personal device na ginagamit ng mga empleyadong nagtatrabaho nang malayuan. Inirerekomenda ng ACSC ng ASD na tumuon ang mga organisasyon sa pagpapatupad ng mga kontrol upang protektahan ang kanilang sarili laban sa panganib ng mga info stealer na nagta-target sa mga kredensyal ng user. Kabilang sa mga mitigasyon na ito ang:

**Magbigay ng pagsasanay sa mga kawani tungkol sa kaalaman sa cyber security**

- Pigilan ang matagumpay na naka-target na social engineering at pag-download ng malicious file sa pamamagitan ng pagbibigay ng epektibong pagsasanay sa mga kawani.
- Itaas ang kaalaman tungkol sa mga info stealer, sa kanilang mga paraan ng paghahatid at mga phishing threat sa inyong organisasyon.

**I-secure ang corporate account**

- Ipatupad ang MFA:
- Ipatupad ang MFA sa mga panlabas at panloob na serbisyo (external and internal services), mga system at mga imbakan ng sensitibong data, lalo na para sa webmail, mga VPN, at mga privileged user account na nag-a-access ng mga critical system. Ang pinakamahusay na kasanayan ay ang pagpapatupad ng phishing-resistant MFA sa lahat ng mga account.
- I-disable ang mga user account kapag hindi na kinakailangan ang mga ito.
- Limitahan ang mga pribilehiyo ng administrator:
- Magsagawa ng network administration at iba pang privileged na gawain gamit ang isang nakatalagang locked-down workstation lamang (ibig sabihin, isang secure na admin workstation).
- Sundin ang pinakamahuhusay na gawi sa hindi gaanong pribilehiyo (least-privilege best practice) sa pamamagitan ng pag-aatas sa mga administrator na gumamit ng mga privileged user account para sa pamamahala ng mga system at mga standard user account para sa mga hindi pang-administratibong gawain.
- Pigilan ang mga privileged user account (hindi kasama ang mga tahasang awtorisadong mag-access ng mga online na serbisyo) mula sa pag-access sa internet, email at mga serbisyo sa web.
- Isaalang-alang ang pagpapatupad ng just-in-time na pangangasiwa para sa mga system at application.
- Ipatupad ang pamamahala at pag-audit ng mga privileged user account.
- Pana-panahong i-update ang mga password, lalo na ang mga external-facing remote-access account.
- Ipatupad ang mga lifespan time out at mga sunset policy sa mga session token and cookies.

**Pagpatigas ang enterprise mobility**

- Magsagawa ng pagtatasa ng panganib sa enterprise mobility at ipatupad ang mga alituntunin sa pagpapatigas ng enterprise mobility.
- Magpatupad ng patakarang Bring Your Own Device (BYOD) kung papayagan mo ang mga empleyado na gumamit ng mga personal device para sa trabaho, dahil mas secure ang mga device na pinamamahalaan ng kumpanya kaysa sa hindi pinamamahalaang mga personal device.

**Suriin at tasahin ang mga panganib sa supply chain mula sa mga vendor na nag-a-access sa inyong mga network, kabilang ang mga vendor ng Software-as-a-Service (Saas) at Managed Service Provider.** Paano Pamahalaan ang Iyong Seguridad Kapag Nakikipag-ugnayan sa isang Managed Service Provider.

**Protektahan ang iyong corporate network**

- Panatilihing up-to-date ang mga application at operating system.
- Ilapat ang mga lokal na patakaran sa seguridad upang ipatupad ang application control na may mahigpit na listahan ng pinapayagan.
- Ipatupad ang network segmentation upang paghiwalayin ang mga segment ng network batay sa tungkulin at gamit (functionality).
- I-audit at i-monitor ang mga aktibidad ng user, lalo na para sa mga malayuang empleyado.
- Ang pag-monitor sa mga privileged account ay maaaring magbunyag ng hindi awtorisadong pag-access sa sensitibong data o hindi pangkaraniwang mga aktibidad sa paglilipat ng data, tulad ng malalaking volume ng data na na-upload sa isang panlabas na network.
- Ipatupad ang mga patakaran sa pag-iwas sa pagkawala ng data at mga tool upang maiwasan ang mga hindi awtorisadong paglilipat ng data.

**Maging isang ASD Cyber Security Network Partner at sumali sa serbisyo ng Cyber Threat Intelligence Sharing (CTIS) ng ASD**

- Ang CTIS ay isang two-way sharing platform na nagbibigay-daan sa gobyerno at mga kasosyo sa industriya na makatanggap at magbahagi ng impormasyon tungkol sa malicious cyber activity.
- Sinusubaybayan ng ACSC ng ASD ang aktibidad ng info stealer at nagbabahagi ng mga detalye ng aktibong imprastraktura ng command and control sa pamamagitan ng CTIS platform.
- Mag-sign up upang maging isang kasosyo at protektahan ang iyong organisasyon at customer data laban sa mga cybercriminal threat.

**Maghanda para sa isang kompromiso**

- Bumuo ng isang plano sa pagtugon sa insidente ng cyber security na gagamitin kung sakaling makompromiso ng info stealer. Tiyaking alam ng mga empleyado kung ano ang gagawin at kung sino ang dapat kontakin kung sa hinala nila ay naka-download sila ng kahina-hinalang file.

**Ipatupad ang Essential Eight ng ACSC ng ASD**

- Bilang karagdagan sa mga mitigasyon na binanggit sa itaas, mariing inirerekomenda ng ACSC ng ASD na ipatupad ang natitirang bahagi ng Essential Eight ng ACSC ng ASD.

**Payo para sa iyong mga empleyado kapag malayuang nagtatrabaho**

- Protektahan ang iyong impormasyon sa iyong mga personal device
  - Bumuo ng mahusay na cyber hygiene at huwag mag-click sa mga kahina-hinalang link o pop-up, o mag-download ng mga file o software mula sa hindi kilalao hindi pinagkakatiwalaang mga mapagkukunan.
  - Gumamit ng mga natatanging password para sa mga work at personal account. Gamitin ang MFA para sa mga personal account hangga't maaari.
  - Huwag iimbak ang iyong mga kredensyal sa trabaho sa isang personal password manager maliban kung tahasang inaprubahan ng iyong tagapag-empleyo. Kabilang dito ang password manager ng iyong web browser. **Kung may pagdududa, hilingin sa iyong tagapag-empleyo na magbigay ng isang password manager na sinusuportahan ng kumpanya.**
  - Huwag mag-log in sa iyong mga work account mula sa mga shared o communal workstation.
  - Magkaroon ng kamalayan kung ano ang iniimbak sa autofill feature ng iyong web browser. Tina-target ng mga info stealer ang data na isine-save ng mga browser sa mga autofill form. Kapag pinupunan ang mga web form, isaalang-alang ang manu-manong pag-enter ng sensitibong data, gaya ng mga numero ng credit card, sa halip na i-save ito sa autofill feature ng iyong web browser.
  - Mag-log out mula sa lahat ng online na serbisyo at i-clear ang cookies ng web browser pagkatapos ng pagba-browse upang mabawasan ang impormasyong magagamit sa mga info stealer.
  - Tiyaking naka-enable ang built in antivirus solution ng iyong operating system. Kung gumagamit ka ng third-party antivirus solution, tiyaking napapanatili itong up-to-date at mula sa isang mapagkakatiwalaang vendor.

# Tulong

Ang mga organisasyon sa Australya na naapektuhan o nangangailangan ng tulong hinggil sa isang kompromiso ng info stealer ay maaaring makipag-ugnayan sa ACSC ng ASD sa **1300 CYBER1 (1300 292 371)** o sa pamamagitan ng pagsusumite ng report sa cyber.gov.au/report.

Hinihikayat ng ACSC ng ASD ang mga entity na mag-report ng kahina-hinalang network activity at mga pahiwatig ng kompromiso na nauugnay sa mga info stealer, kahit na ang insidente ay itinuturing na napigilan. Ginagamit namin ang impormasyong ibinibigay mo upang pahusayin ang aming pag-unawa sa mga taktika, teknik at pamamaraan ng mga cyber threat actor, na tumutulong sa amin na bigyan ng babala ang iba pang organisasyon sa Australya na na-target sa parehong paraan.

**Pagtatatwa**

Ang materyal sa gabay na ito ay may pangkalahatang katangian at hindi dapat ituring bilang legal na payo o pagsalalayan para sa tulong sa anumang partikular na pangyayari o emerhensya. Sa anumang mahalagang bagay, dapat kang humingi ng naaangkop na independiyenteng propesyonal na payo kaugnay ng iyong sariling mga kalagayan.

Ang Commonwealth ay hindi tumatanggap ng responsibilidad o pananagutan para sa anumang pinsala, pagkawala o gastos na natamo bilang resulta ng pagsalalay sa impormasyong nakapaloob sa gabay na ito.



**Para sa higit pang impormasyon, o para mag-report ng insidente sa cyber security, makipag-ugnayan sa amin:**

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

Ang numerong ito ay magagamit lamang sa loob ng Australia.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre