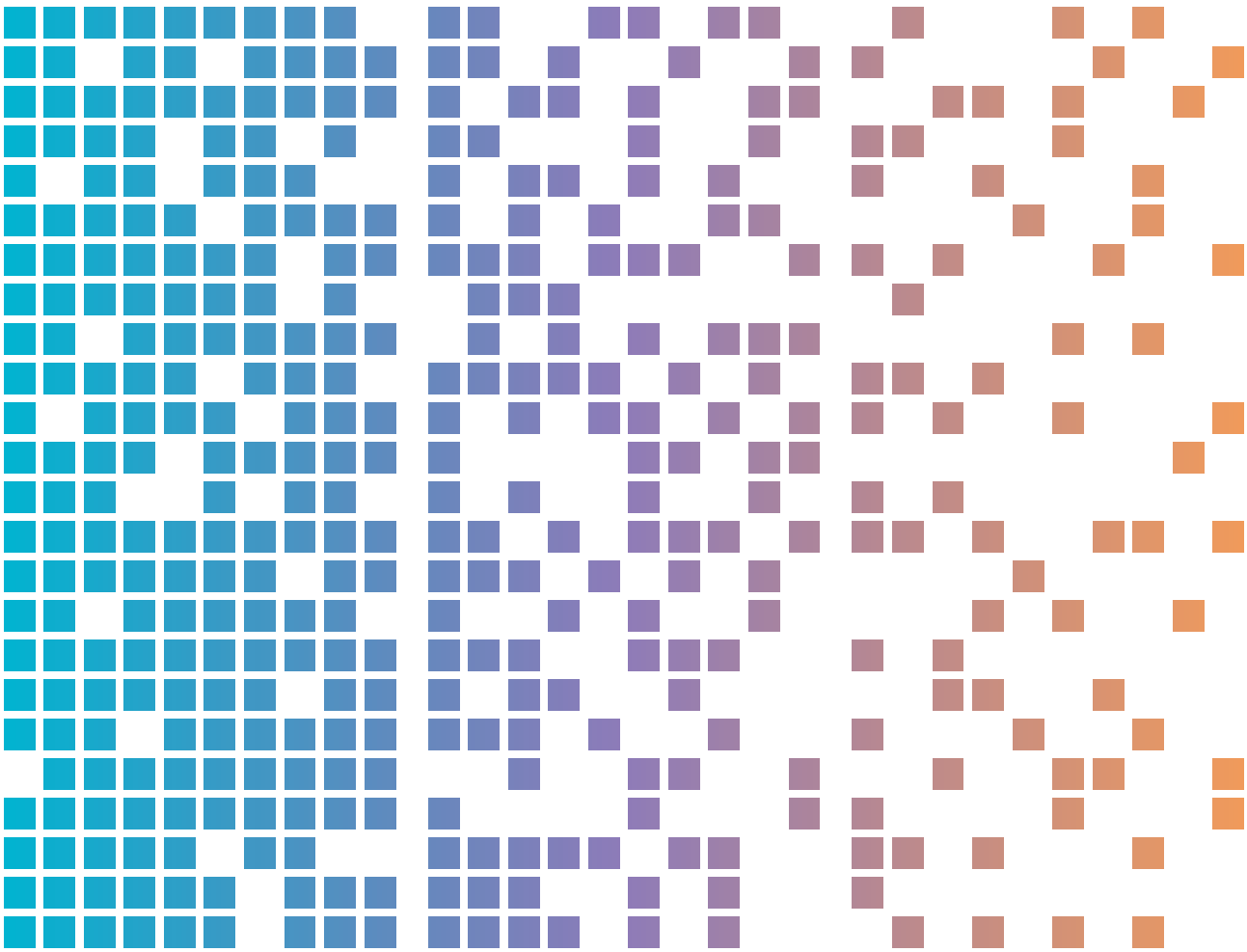
Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

O ataque silencioso: os cibercriminosos utilizam malware de roubo de informações para comprometer redes empresariais



Complexidade do Conteúdo
MODERADA

Índice

Contexto

O malware de roubo de informações rouba as credenciais dos utilizadores e informação do sistema que os cibercriminosos exploram, predominantemente para ganhos monetários. Os ladrões de informações têm sido observados em ciberataques contra várias organizações e setores em todo o mundo, incluindo a Austrália. Esta publicação dá aos leitores orientações de segurança cibernética sobre o malware de roubo de informações, incluindo atividade de ameaça e conselhos de mitigação para as organizações e os seus funcionários.

Pontos principais

- O malware de roubo de informações, também conhecido como ladrões de informações, é um tipo de malware concebido para recolher informações do dispositivo da vítima. Isto pode incluir nomes de utilizadores e palavras-passe dados de cartões de crédito, carteiras de criptomoedas, ficheiros locais, e dados do navegador incluindo cookies, histórico do utilizador e detalhes de preenchimento automático de formulário.
- Os cibercriminosos podem tentar comprar e usar as credenciais roubadas de utilizadores associadas às contas empresariais para obter acesso inicial aos dispositivos do empregador da vítima, aos seus clientes e outros sistemas empresariais. O impacto subsequente para estas organizações pode incluir ransomware, extorsão, compromisso de e-mails da empresa e roubo de propriedade intelectual.
- O Centro Australiano de Segurança Cibernética da Direção Australiana de Sinais (ACSC da ASD) identificou violações de redes corporativas que foram originadas pelo acesso aos recursos de trabalho pelos funcionários a partir de dispositivos pessoais comprometidos. Em várias instâncias, os cibercriminosos obtiveram acesso inicial às redes corporativas através do uso de credenciais de utilizador válidas roubadas. As nossas investigações mostraram que compromissos extensivos geralmente ocorreram depois dos cibercriminosos terem tido acesso bem-sucedido às contas privilegiadas dos utilizadores.
- As organizações que facilitam o acesso remoto à sua rede pelos funcionários, empreiteiros, fornecedores de serviços geridos ou outras entidades, incluindo através do hardware Traga Seu Próprio Dispositivo (BYOD), devem estar cientes do risco de ladrões de informação e protegerem-se contra essa ameaça. Os cibercriminosos implantam ladrões de informações nos dispositivos das vítimas utilizando uma vasta gama de técnicas, incluindo e-mails de phishing, downloads de software pirateado, otimização para motores de busca (SEO), anúncios ou links maliciosos publicados em plataformas de redes sociais. Em geral, os dispositivos que são utilizados tanto para fins de trabalho como para fins pessoais correm alto risco de infecção através destas técnicas devido ao comportamento do utilizador e aos controlos de segurança reduzidos.
- Os ladrões de informações oferecem um modelo atraente aos cibercriminosos para monetizar a atividade cibercriminosa, principalmente para cibercriminosos iniciantes e aqueles com proficiência técnica limitada. Alguns cibercriminosos comercializarão produtos de roubo de informação sob um programa de tipo Malware como Serviço (MaaS), cobrando uma taxa de assinatura mensal para seu uso.

Antecedentes

O uso de ladrões de informações pelos cibercriminosos representa uma ameaça à segurança e ao bem-estar das organizações australianas. As infecções dos ladrões de informações geralmente apresentam-se como atividade percursora aos grandes incidentes de segurança cibernética, pois os cibercriminosos usam-nas para obter credenciais de utilizadores. Estas credenciais de utilizadores, especialmente aquelas que fornecem acesso aos serviços remotos ou contas privilegiadas digitais, são em seguida exploradas a fim de permitir acesso inicial aos sistemas e dados corporativos.

Nota: Os corretores de acesso inicial desempenham um papel especializado no âmbito do ecosistema do cibercrime, através da compra e validação de credenciais de utilizadores roubadas. Em seguida, eles leiloam as credenciais de utilizadores de alta qualidade, de ambientes corporativos procurados, aos cibercriminosos que usarão as credenciais de utilizadores para explorar a rede corporativa da organização.

Credenciais de utilizadores válidas roubadas são muito valiosas para os cibercriminosos porque elas aceleram o acesso inicial às redes corporativas e aos sistemas empresariais. Com credenciais de utilizadores válidas roubadas, os cibercriminosos podem contornar várias táticas e técnicas típicas, incluindo:

- identificar e pesquisar um alvo
- enumerar a rede do alvo para achar vulnerabilidades
- desenvolver vetores para acesso inicial, tais como:
  - material de phishing
  - exploração de vulnerabilidades de software
  - almejar serviços remotos, incluindo o Protocolo de Área de Trabalho Remota (RDP) ou serviços de Rede Virtual Privada (VPN)
  - ataques de força bruta contra as credenciais de utilizadores (adivinhar a palavra-passe).

Estes passos necessitam investimento de tempo e um nível de aptidão técnica que constituem uma barreira para alguns cibercriminosos. Em particular, os cibercriminosos que não conseguem penetrar as defesas de redes corporativas podem beneficiar diretamente das infecções do ladrão de informações, pois essas infecções podem fornecer acesso rápido e fácil às credenciais de utilizadores das redes corporativas desejadas.

Nas configurações de trabalho remoto, alguns funcionários usaram os dispositivos pessoais para navegar na internet tanto para fins de trabalho quanto pessoais. Quando fazem isso, os funcionários podem optar por armazenar as suas credenciais de utilizadores nos repositórios de palavras-passe e extensões dos seus navegadores da web, ou podem utilizar os recursos de preenchimento automático do navegador da web. Os ladrões de informações visam os dados destes armazéns de dados juntamente com os cookies de autenticação e outros dados pessoais no navegador da web.

Ao contrário dos dispositivos corporativos, os dispositivos pessoais nem sempre têm políticas de segurança empresarial aplicadas, o que representa um risco maior para as organizações. Por exemplo, os funcionários podem envolver-se em atividades como baixar software pirata e navegar em sites de alto risco, aumentando a sua exposição a ameaças cibernéticos e infecções por malware.

Os ladrões de informações, distribuidores, corretores de acesso inicial e afiliados de ransomware constituem agora uma parte importante do ecossistema cibercriminoso motivado pelo lucro financeiro. O ecossistema cresce com mais eficiência quando os cibercriminosos se especializam e desenvolvem capacidades que visam fases particulares de um ataque, e depois vendem essa capacidade como um serviço a outros afiliados criminosos.

Atividade de ameaça

A ACSC da ASD está a rastrear e monitorizar um aumento de atividade de roubo de informações globalmente, que representa uma ameaça crescente para as redes australianas. Os relatórios da indústria indicam que os ladrões de informações são a variante de malware mais popular na atividade cibercriminosa no decorrer de 2023. O volume crescente de dados roubados para venda nos mercados da dark web e um aumento na atividade de corretores de acesso inicial que aproveitam estes dados, é reflexo desta tendência crescente, que acelerou em 2024.

Ecossistema de roubo de informação

Fase 1: Comprar o malware

Os ladrões de informações são geralmente oferecidos nos mercados cibercriminosos como MaaS ou Stealer-as-a-Service, ou vendidos como código fonte. MaaS refere-se a um modelo de negócio por meio do qual um desenvolvedor de malware vende uma assinatura para o seu software malicioso a indivíduos através de uma plataforma baseada na web, semelhante a ofertas legítimas de Software-as-a-Service. O modelo MaaS reduziu a barreira de entrada para os cibercriminosos, pois permite que indivíduos sem competências técnicas extensas distribuam malware e recolham informação roubada para uso em ataques cibernéticos.

Os ladrões de informações oferecidos como MaaS são geralmente anunciadas por um preço mensal relativamente barato, e dão acesso aos cibercriminosos a um painel de ladrões de informações. O painel facilita a criação de malware para roubo de informação, organiza os dados roubados e localiza o número de sistemas comprometidos. Os operadores de MaaS oferecem atualizações de recursos, ferramentas e apoio técnico para evitar a detecção por software antivírus e para atrair e reter assinantes. Muitos ladrões de informações têm a capacidade de se removerem do dispositivo da vítima depois de efetuar a exfiltração de dados.

Fase 2: Distribuição

Os cibercriminosos que distribuem ladrões de informações e recolhem informação de dispositivos comprometidos são chamados 'Traffers' (distribuidores de tráfego). Os traffers encaminham as vítimas para os links maliciosos, facilitando a disseminação dos ladrões de informações como parte de campanhas amplas. A maioria das campanhas são indiscriminadas, confiando nas infecções oportunistas. No entanto, algumas campanhas são adaptadas para indústrias específicas e envolvem spear-phishing direcionado a vítimas específicas. Os traffers efetuam estas campanhas mais direcionadas em resposta à demanda do cliente; por exemplo, quando os compradores estão à procura de acesso a organizações ou sectores específicos de alto valor.

Os traffers implantam ladrões de informações nos dispositivos das vítimas utilizando uma ampla gama de técnicas, incluindo:

- **botnets**: redes de sistemas de computadores comprometidos controladas por cibercriminosos para efetuar atos maliciosos como enviar mensagens de phishing ou malware

- **phishing**: tentativas de obter informação confidencial através de decepção, incluindo através de e-mails ou mensagens diretas nas redes sociais, fóruns ou aplicações de mensagens, que são métodos de distribuição comuns que reduziram a barreira de entrada para os cibercriminosos:
  - Estas mensagens geralmente contêm um link malicioso, em vez de anexar ficheiros maliciosos ao próprio e-mail.
- **resultados de busca maliciosos**: entregues por meio de técnicas de otimização para motores de busca (SEO) que direcionam alvos para sites distribuindo malware disfarçado de software legítimo ou outro conteúdo
- **publicidade maliciosa**: a utilização de código prejudicial, injectado em anúncios online legítimos, para distribuir malware
- **software crackeado ou pirateado**: downloads, incluindo videojogos, partilhados através de vídeos de YouTube, com links maliciosos na descrição ou comentários do vídeo, ou de sites de download não confiáveis
- **anúncios e posts na rede social**: direcionando alvos para ficheiros de malware disfarçados
- **atualizações de software malicioso**: normalmente disfarçadas como atualizações do navegador da web

Fase 3: Recolha de dados

Uma vez que um ladrão de informações executa no dispositivo da vítima, ele começa a recolher dados confidenciais da máquina comprometida. Além de roubar credenciais de utilizadores, nos casos em que os ladrões de informações fazem parte de uma botnet, os cibercriminosos podem controlar remotamente o dispositivo comprometido enviando comandos de configuração para ativar outros recursos ou transferir outro malware. Em geral, os ladrão de informações conseguem roubar:

- nomes de utilizadores e palavras-passe, particularmente aqueles armazenados nas sessões/tokens de utilizador na autenticação multifator dos navegadores da web (MFA).
- cookies de autenticação
- formulário de preenchimento automático do navegador da web
- credenciais, conteúdo e contactos de e-mail
- histórico de navegação na web
- documentos do utilizador
- dados do cartão de crédito
- registos de conversas de aplicações de mensagens para desktop
- informação de sistemas
- carteiras de criptomoedas
- credenciais de VPN ou Protocolo de Transferência de Ficheiros (FTP).

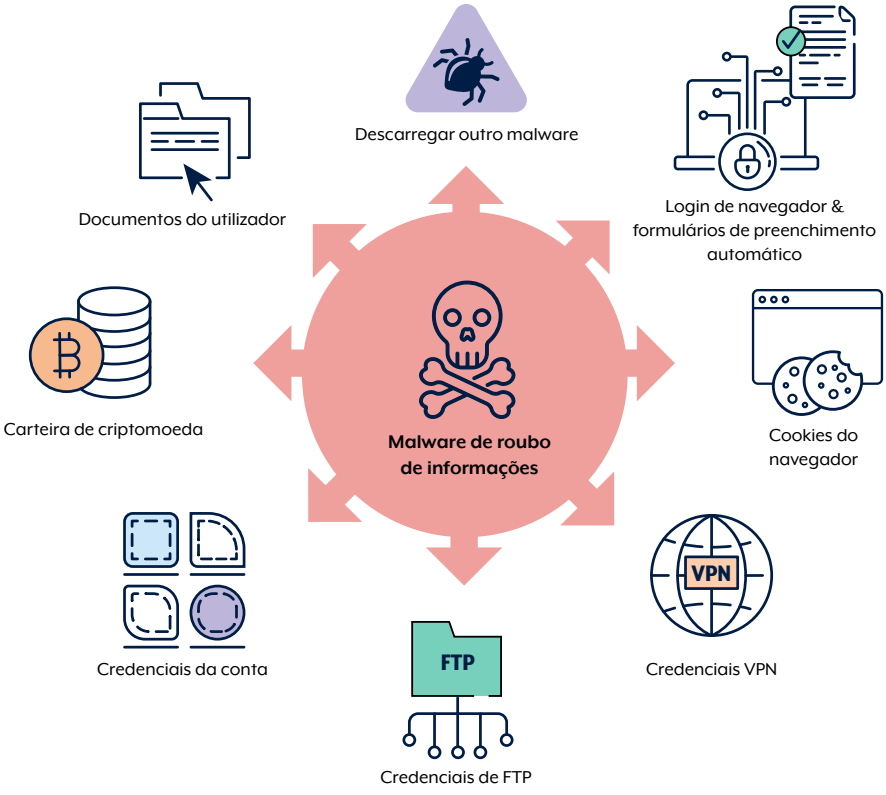


Figura 1. Capacidade de ladrões de informações

Alguns cookies de autenticação do navegador da web mantêm um utilizador ligado a uma conta ou serviço por vários dias de cada vez, para que os utilizadores não tenham de autenticar novamente. Se roubados, estes cookies de autenticação poderiam efetivamente contornar os requisitos do MFA e permitir acesso aos cibercriminosos às contas das vítimas, redes corporativas e sistemas empresariais.

Fase 4: Agregação e monetização de dados

Os ladrões de informações são configurados para exfiltrar as informações da vítima, conhecidas como 'logs' (registos), para servidores maliciosos de comando e controlo. Em geral, os ladrões de informações utilizam as aplicações populares de mensagens como Telegram e Discord para partilhar logs com cibercriminosos.

Existem mercados especializados no Telegram e em toda a dark web para a venda e troca de logs. Os cibercriminosos monetizam os logs de várias maneiras, incluindo:

- vendendo logs nos mercados criminosos, incluindo aos corretores de acesso inicial
- explorando as vítimas diretamente através de roubo de identidade e extorsão
- utilizando a informação para acesso inicial às redes corporativas para atividade de ransomware.

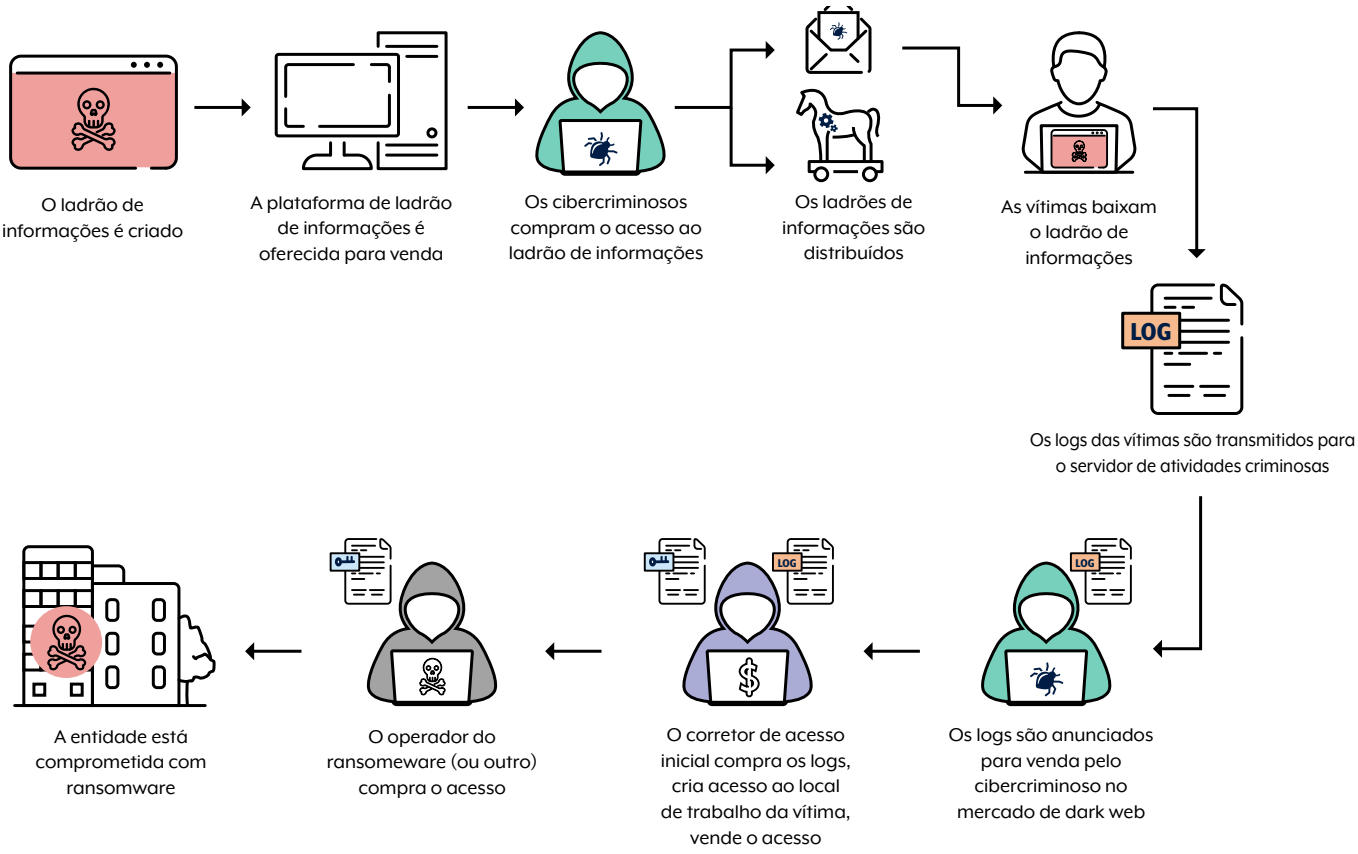


Figura 2. Ecossistema de ladrões de informações e possível impacto numa organização

Implicações

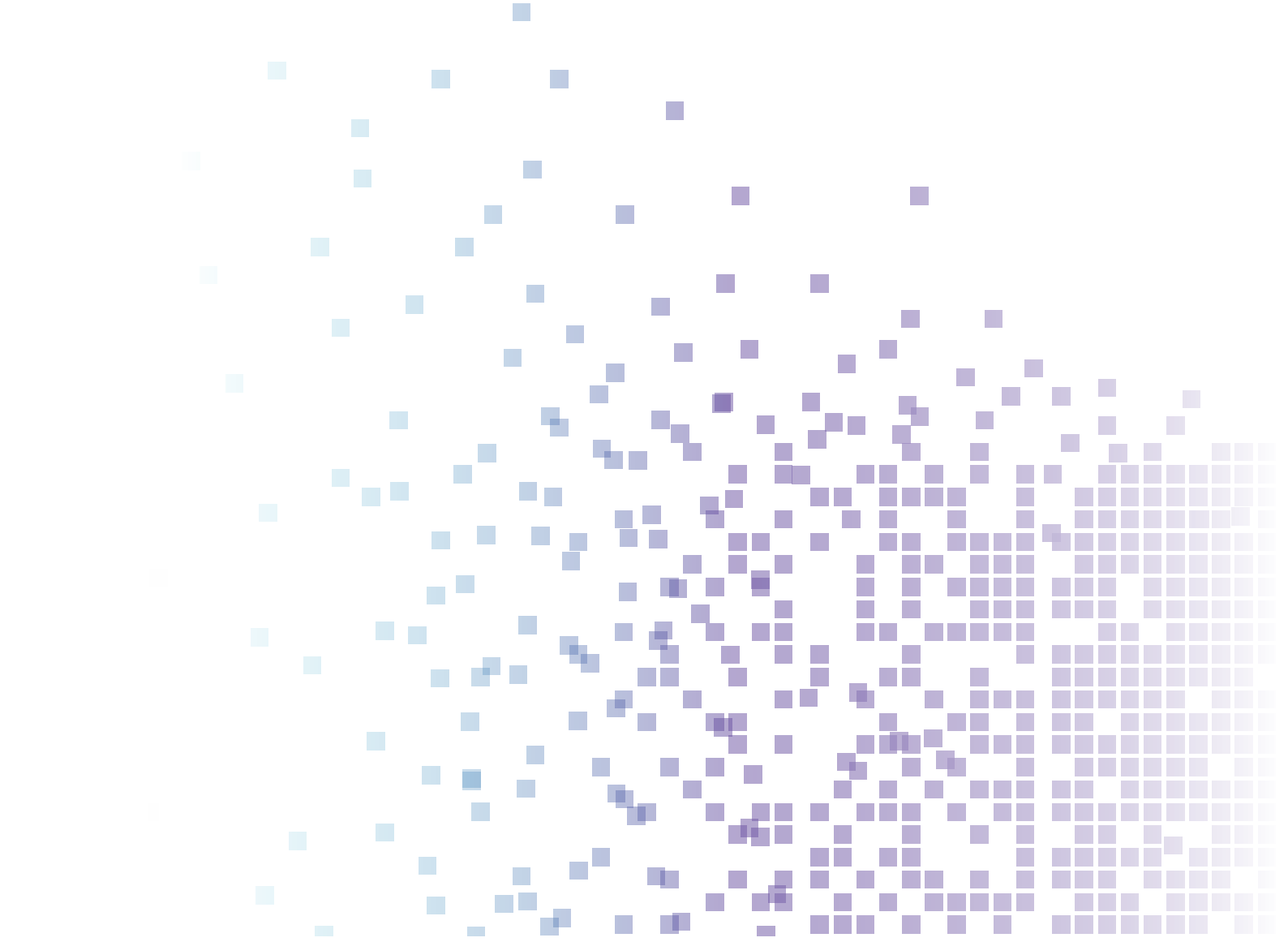
Os ladrões de informações podem ter implicações graves tanto para indivíduos quanto para organizações. Enquanto os ladrões de informações recolhem credenciais de utilizadores, os cibercriminosos podem usá-las para aceder redes corporativas ou sistemas empresariais com contas válidas de utilizadores, muitas vezes atrasando a deteção pelos proprietários do sistema.

Para as **organizações** afetadas pelos ladrões de informações, as consequências podem incluir:

- ransomware
- violação de dados
- comprometimento de e-mails empresariais
- roubo de propriedade intelectual
- roubo de informação confidencial.

Para um **indivíduo** afetado pelos ladrões de informações, as consequências podem incluir:

- acesso não autorizado a contas pessoais de e-mail ou de redes sociais
- risco acrescido de roubo de identidade
- risco acrescido de ataques de phishing
- perda financeira ou acesso não autorizado a contas financeiras
- perda de privacidade.



Estudo de caso

Este estudo de caso foi anonimizado para permitir a divulgação pública. Baseia-se em múltiplos incidentes de segurança cibernética que afetaram entidades australianas que os relataram à ACSC da ASD. A entidade afetada é doravante referida como 'a organização'. Os nomes dos indivíduos neste estudo de caso são fictícios e os detalhes foram removidos para proteger a identidade das vítimas.

A organização é uma empresa australiana que permite que o pessoal aceda aos sistemas empresariais a partir de dispositivos pessoais. A Alice é uma funcionária da organização que trabalha à distância.

Quando trabalha a partir de casa, a Alice acede remotamente a rede corporativa da sua organização utilizando o seu portátil pessoal. A Alice **baixou**, para o seu **portátil pessoal**, uma versão do Notepad++ (que é um softawe tipo bloco de notas) de um site que ela pensava que era legítimo. Um **ladrão de informações** fez-se passar pelo instalador de software do Notepad++.

Quando a Alice tentou instalar o software, o ladrão de informações foi ativado e começou a **recolher credenciais de utilizador** do seu portátil. Isto incluiu o nome de utilizador e palavra-passe do trabalho dela, que ela tinha gravado no recurso de logins gravados do seu navegador da web. Em seguida, o ladrão de informações enviou essas credenciais de utilizador para um servidor de comando e controlo remoto controlado por um grupo cibercriminoso.

Os logs roubados foram embalados juntamente com outros e depois **vendidos a cibercriminosos** através de um mercado da dark web.

Um cibercriminoso chamado Bob comprou as credenciais de utilizador da Alice, identificando as credenciais de utilizador para serviços na rede da sua organização. A organização da Alice **não tinha configurado MFA** para esses serviços, o que significa que Bob podia utilizar as credenciais de utilizador roubadas sozinhas para **autenticar e aceder** a rede corporativa com sucesso.

O Bob acedeu a rede corporativa da organização da Alice sem ser detectado utilizando as **credenciais de utilizador válidas** roubadas. O Bob foi capaz de se movimentar lateralmente através da rede corporativa, identificando dados confidenciais pertencentes à organização e exfiltrando os mesmo a fim de extorquir a empresa.

Depois de roubar dados confidenciais, o Bob **encriptou a base de dados e os sistemas de ficheiros** da organização para torná-los inacessíveis.

Mitigações

As organizações podem não ser capazes de aplicar controlos nos dispositivos ligados à sua rede corporativa, principalmente nos dispositivos pessoais usados pelos funcionários à distância. A ACSC da ASD recomenda que as organizações foquem na implementação de controlos para se protegerem do risco de ladrões de informação que visam as credenciais dos utilizadores. Estas mitigações incluem:

Fornecer capacidade de conscientização sobre segurança cibernética ao pessoal

- Impedir o sucesso da engenharia social direcionada e downloads de ficheiros maliciosos fornecendo formação eficaz ao pessoal.
- Aumentar a conscientização sobre ladrões de informações, seus métodos de entrega e as ameaças de phishing à sua organização.

Proteja as contas empresariais.

- Implemente MFA:
- Implemente MFA em todos os serviços externos e internos, sistemas e repositórios de dados confidenciais, principalmente para o webmail, VPNs, e contras de utilizadores privilegiadas com acesso a sistemas críticos. A melhor prática é aplicar MFA resistente a phishing em todas as contas.
- Desative contas de utilizadores quando elas já não forem precisas.
- Limite os privilégios de administradores:
- Execute administração de redes e outras tarefas privilegiadas usando apenas uma estação de trabalho dedicada e bloqueada (i.e. uma estação de trabalho segura).
- Siga a melhor prática do menor privilégio exigindo que os administradores utilizem contas de utilizador privilegiadas para gerir sistemas e contas de utilizador padrão para tarefas não-administrativas.
- Impeça que as contas de utilizador privilegiadas (excluindo aquelas explicitamente autorizadas para aceder a serviços online) tenham acesso aos serviços de internet, e-mail e web.
- Considere implementar a administração just-in-time para sistemas e aplicações.
- Imponha a gestão e auditoria de contas de utilizador privilegiadas.
- Atualize as palavras-passe periodicamente, principalmente das contas de acesso remoto voltadas para o exterior.
- Aplique políticas de tempo limite de vida útil e de encerramento aos tokens e cookies das sessões.

Fortaleça a mobilidade empresarial

- Realize uma avaliação de risco de mobilidade empresarial e implemente diretrizes de fortalecimento da mobilidade empressarial.
- Implemente uma política de Bring Your Own Device (BYOD) se você permite que os funcionários utilizem dispositivos pessoais para o trabalho, pois os dispositivos geridos pela empresa são mais seguros do que os dispositivos pessoais não geridos.

Reveja e avalie os riscos da cadeia de abastecimento dos fornecedores que acedem às suas redes, incluindo os fornecedores de Software-as-a-Service (Saas) e Provedores de Serviços Geridos. Como Gerir a sua Segurança ao Contratar um Provedor de Serviços Geridos.

Proteja a sua rede corporativa

- Mantenha as aplicações e os sistemas operacionais atualizados.
- Aplique políticas de segurança local para impor o controlo de aplicações com listas de autorizações rigorosas.
- Implemente a segmentação da rede para separar segmentos da rede com base no desempenho e funcionalidade.
- Inspecione e monitorize as atividades dos utilizadores, especialmente dos funcionários à distância.
- Monitorizar contas privilegiadas pode revelar acesso não autorizado a dados confidenciais ou atividades de transferência de dados incomuns, tais como grandes volumes de dados baixados para uma rede externa.
- Implemente políticas e ferramentas de prevenção contra perda de dados para evitar transferência de dados não autorizada.

Torne-se um Parceiro da Rede de Segurança Cibernética da ASD e adira ao serviço de Partilha de Inteligência de Ameaças Cibernéticas (CTIS) da ASD

- O CTIS é uma plataforma de partilha bidirecional que permite que os parceiros governamentais e individuais recebem e partilhem informação sobre atividade cibernética maliciosa.
- A ACSC da ASD está rastreando a atividade de ladrões de informações e partilha os detalhes da infraestrutura ativa de comando e controlo através da plataforma do CTIS.
- Registe-se para se tornar um parceiro e proteja os dados da sua organização e dos clientes contra ameaças cibernéticas.

Prepare-se para um comprometimento

- Crie um plano de resposta a incidente de segurança cibernética para utilizar no caso de comprometimento de ladrão de informações. Assegure-se que os funcionários estão cientes daquilo que devem fazer e quem contactar se suspeitarem que baixaram um ficheiro suspeito.

Implemente os Oito Elementos Essenciais da ACSC da ASD

- Além das mitigações mencionadas acima, a ACSC da ASD recomenda fortemente a implementação dos restantes Oito Elementos Essenciais da ACSC da ASD.

Aconselhamento para os seus funcionários quando trabalharem à distância

- Protejam a sua informação nos seus dispositivos pessoais
  - Desenvolvam uma boa higiene cibernética e não clique em links suspeitos ou popups, nem baixe ficheiros ou software de fontes desconhecidas ou não confiáveis.
  - Utilize palavras-passe diferentes para contas de trabalho e pessoais. Utilize MFA para contas pessoais, sempre que possível.
  - Não armazene suas credenciais de trabalho num gestor de palavras-passe pessoais salvo explicitamente aprovado pelo seu empregador. Isto inclui o gestor de palavra-chave do seu navegador da web. **Se tiver dúvidas, peça ao seu empregador forneça um gestor de palavras-chave apoiado pela empresa.**
  - Não faça login nas suas contas de trabalho a partir de estações de trabalho partilhadas ou comunitárias.
  - Esteja ciente daquilo que está a ser armazenado no recurso de preenchimento automático do seu navegador da web. Os ladrões de informações direcionam os dados que os navegadores gravam para preencher formulários automaticamente. Quando preencher formulários da web, considere inserir manualmente dados confidenciais, tais como números de cartões de crédito, em vez de gravá-los no recurso de preenchimento automático do seu navegador da web.
  - Termine e saia de todos os serviços online e limpe os cookies do navegador da web quando terminar uma sessão de navegação de modo a reduzir a informação disponível aos ladrões de informações.
  - Assegure-se que a solução antivírus integrada no seu sistema operacional está ativada. Se você utiliza uma solução antivírus de terceiros, assegure-se que a mantém atualizada e que seja de um fornecedor de confiança.

Assistência

As organizações australianas que foram afetadas ou necessitam ajuda relativamente a um compromisso de ladrão de informações podem contactar a ACSC da ASD através de **1300 CYBER1 (1300 292 371)** ou enviando um relatório a cyber.gov.au/report.

A ACSC da ASD incentiva as entidades a relatar atividade de rede suspeita e indicadores de comprometimento associados aos ladrões de informações, mesmo que considerem que o incidente está controlado. Utilizamos a informação que você fornece para entendermos melhor as táticas, técnicas e procedimentos dos atores de ameaças cibernéticas, o que nos ajuda a avisar outras organizações australianas que foram visadas da mesma maneira.

Isenção de responsabilidade

O conteúdo deste guia é de natureza geral e não deve ser considerado como aconselhamento jurídico, nem utilizado como referência em circunstâncias específicas ou situações de emergência. Em qualquer assunto importante, deve procurar o aconselhamento profissional independente adequado em relação às suas circunstâncias pessoais.

A Commonwealth não se responsabiliza por quaisquer danos, perdas ou despesas incorridos como resultado da confiança nas informações contidas neste guia.

Para mais informação ou para relatar um incidente de segurança cibernética, contacte-nos:

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

Este número está disponível para uso apenas dentro da Austrália.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre