Foto de Arian Darvishi na Unsplash

Pirataria Audiovisual: Um Panorama Técnico das Ameaças Cibernéticas e Seus Impactos

Por Danilo Almeida

A pirataria audiovisual se apresenta como um fenômeno complexo que explora vulnerabilidades técnicas e legais, revelando um cenário preocupante para a segurança da informação. Este artigo/tutorial é resultado de um estudo realizado pelo GT de Segurança da Informação da SET, composto por profissionais da indústria audiovisual que participam do GT. A análise aborda as principais formas de ataque e os quatro pilares que sustentam essa prática ilícita, destacando os riscos cibernéticos enfrentados pelos consumidores e os prejuízos financeiros causados à indústria.

Analisando as formas de ataque, técnicas utilizadas e principais tecnologias exploradas pelos hackers e piratas para obter acesso ilegal aos conteúdos audiovisuais (ao vivo ou sob demanda) podemos identificar duas afirmações:

- Toda a pirataria tem origem em um acesso legal, ou seja, em quaisquer modalidades de ação pirata. Quando analisada friamente, o primeiro elemento da corrente é uma assinatura legal do serviço.
- Ainda que se utilizem métodos, ferramentas e tecnologias variadas, é possível classificar todas as atividades piratas em quatro (4) pilares:

- Compartilhamento de conteúdos; Compartilhamento de serviços; Compartilhamento de credenciais; Compartilhamento de chaves.

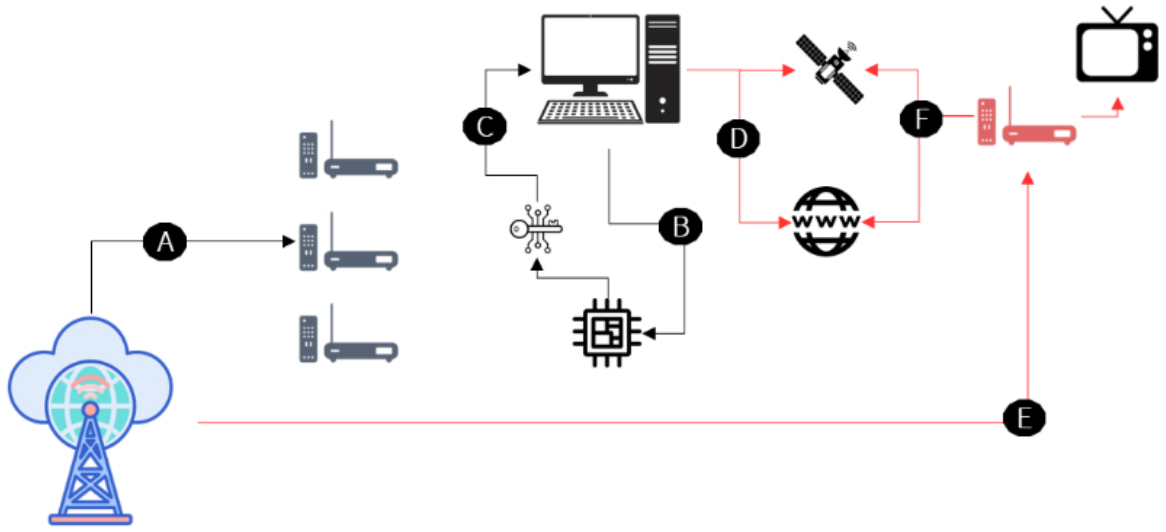
- Quais as formas de consumo de conteúdo pirata audiovisual e os seus principais riscos cibernéticos?

- TV Boxes; Listas de IPTV; Apps; Web-sites; Sistemas de download: Web lockers e P2P.

Compartilhamento de Chaves

A figura abaixo e a sua tabela adjacente ilustram e exemplificam o funcionamento do modelo de pirataria de compartilhamento de chaves.

Este modelo é mais comumente aplicado a distribuições de TV por assinatura tradicionais (cabo, satélite).

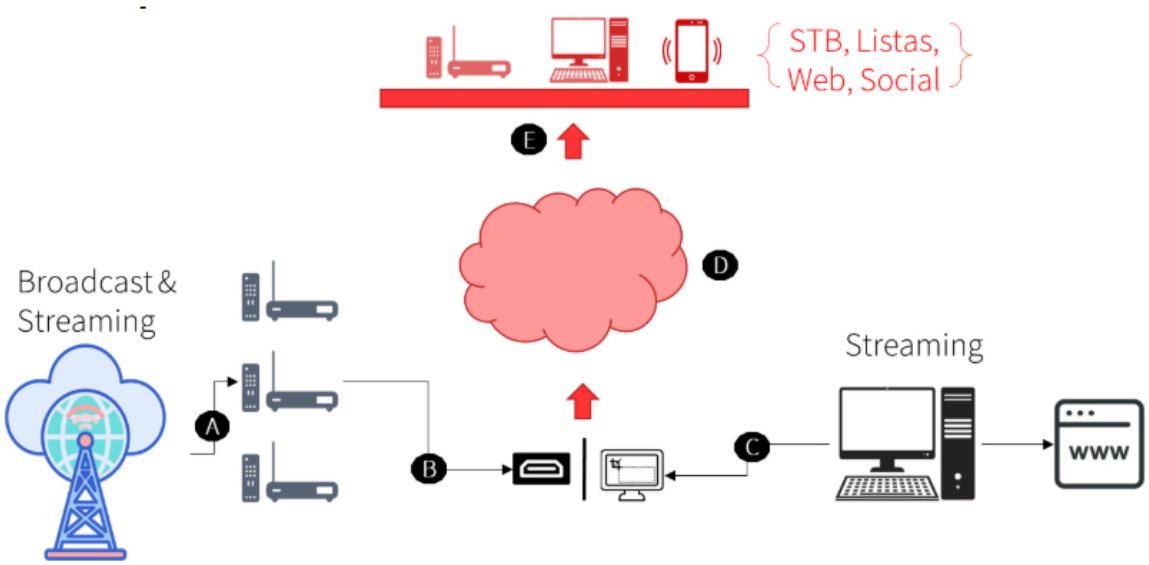


Fonte: Autor

Item/Fluxo	Descrição
A	Este fluxo indica um processo normal de transmissão em uma operação tradicional de TV por assinatura, onde a operadora de TV por assinatura envia o seu conteúdo completo para todos os seus clientes. Este sinal é normalmente codificado e criptografado, e chega até os aparelhos receptores, onde o sinal é decodificado e descriptografado para ser consumido. Sistemas de CAS garantem que cada assinante acesse somente os canais aos quais ele/ela assina. Devido a tecnologia utilizada neste tipo de transmissão, as chaves de criptografia (geradas por um equipamento chamado multiplexador) são enviadas junto com o conteúdo e são protegidas por sistemas de controle de acesso condicional (CAS).
B	Neste fluxo, identificamos um agente ilegal - pirata - agindo diretamente no hardware do decodificador para conseguir obter acesso ilegal a estas chaves de criptografia. Este acesso ilegal é realizado com explorações de baixo nível no hardware se valendo de zonas cinzentas e brechas em especificações técnicas, bem como falhas nos processos de ***sandboxing*** e ***hardening***. Não é uma tarefa trivial, mas para alguns equipamentos, os hackers conseguiram executar este procedimento obtendo acesso às chaves de criptografia utilizadas na transmissão.
C	Uma vez obtidas as chaves, os piratas rapidamente as transferem para sistemas de computação para que elas possam ser redistribuídas para a sua rede de aparelhos consumirem os serviços de TV por assinatura de forma ilegal.
D	Neste ponto o pirata distribui esta chave através de uma rede para os seus dispositivos. É possível utilizar dois modos de distribuição: (1) por satélite - modalidade conhecida por SKS (***Satellite Key Sharing***) ou (2) por internet - modalidade conhecida por IKS (***Internet Key Sharing***).
E	Os consumidores desta modalidade de pirataria precisam ter acesso à distribuição oficial da operadora de TV por assinatura (seja cabo, satélite ou micro-ondas). Contudo, como não são assinantes legais do serviço, todos os canais chegam ao seu dispositivo codificados e este consumidor não consegue ter acesso ao conteúdo (áudio e vídeo).
F	Quando este mesmo dispositivo - que já está conectado à rede de distribuição oficial de uma operadora de TV por assinatura - também se conecta à fonte de transmissão das chaves de criptografia furtadas de um dispositivo legal (item B), então consegue com sucesso ter acesso ilegal a todo o conteúdo linear transmitido pela operadora de TV por assinatura.

Compartilhamento de Conteúdos

A figura abaixo e a sua tabela adjacente ilustram e exemplificam o funcionamento do modelo de pirataria de compartilhamento de conteúdo. Este modelo pode ser aplicado tanto às distribuições de TV por assinatura tradicionais (cabo, satélite) quanto à distribuição de streaming.



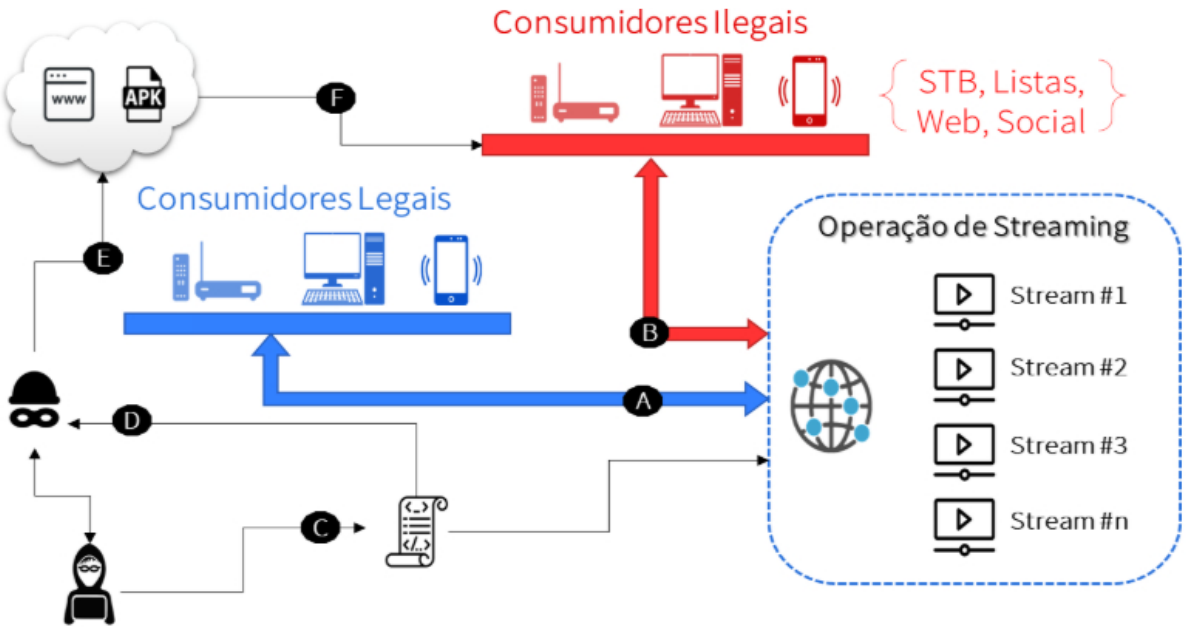
Fonte: Autor

Item/Fluxo	Descrição
A	Este fluxo indica um processo normal de transmissão em uma operação tradicional de TV por assinatura ou de uma operação de streaming de vídeo, onde o operador envia o seu conteúdo para todos os seus clientes ou via ***broadcast/multicast*** ou via ***unicast***. Este sinal é normalmente codificado e criptografado, e chega até os aparelhos receptores, onde o sinal é decodificado e descriptografado para ser consumido. Em transmissões do tipo ***broadcas***t ou multicast o sistema de segurança é o CAS já mencionado na tabela anterior, já para as transmissões do tipo unicast o sistema de segurança aplicado pode ser: (1) baseado somente em tokens de autenticação, ou (2) baseados em sistemas de criptografia conhecidos como DRM (***Digital Rights Management***).
B	Neste fluxo, identificamos um agente malicioso, que através de um acesso legal à plataforma de vídeo, faz uso de equipamentos externos de gravação e/ou captura de conteúdo pela porta HDMI. Por exemplo: um assinante malicioso utiliza um decodificador original e oficial da operação de vídeo para acessar os conteúdos (ao vivo ou por demanda) e, em lugar de conectar a saída HDMI do decodificador na entrada de um aparelho de TV, ele utiliza um dispositivo de captura e ***streaming*** de conteúdo.
C	Neste fluxo, identificamos um agente malicioso, que através de um acesso legal à plataforma de vídeo, faz uso de tecnologia de captura de tela para extraviar o conteúdo de vídeo. Por exemplo: um assinante malicioso utiliza um acesso regular ao aplicativo ou ao website da operação e inicia uma sessão de streaming de vídeo. Depois utiliza ferramentas de captura de tela e de áudio para extraviar o conteúdo. Uma outra vertente deste modelo de ataque são piratas utilizando navegadores de internet com vulnerabilidades e conseguindo acessar diretamente os arquivos de streaming (manifesto e arquivos de mídia) baixados pelo navegador para a operação normal de ***streaming***. Este último modelo é mais praticado quando a segurança é baseada em tokens, já que desta forma os arquivos de mídia não são encriptados.

Item/Fluxo	Descrição
D	Todo o conteúdo extraviado é então transcodificado e disponibilizado na nuvem ou por ***web-lockers*** (ou ***web-drives***) ou por plataformas de ***streaming*** de vídeo.
E	Na fase final do ciclo de vida deste modelo de pirataria, os consumidores ilegais acessam este conteúdo extraviado é disponibilizado na nuvem através de aplicativos ilegais (executados em PCs, Tablets, celulares, etc), listas de ***playback*** - que podem ser carregadas em qualquer aplicativo regular tocador de mídia, como pode exemplo o VLC, mídias sociais como Youtube, IGTV, Facebook (entre outros) e diretamente através de sites na internet indexada.

Compartilhamento de Serviços

A figura abaixo e a sua tabela adjacente ilustram e exemplificam o funcionamento do modelo de pirataria de compartilhamento de serviços. Este é aplicado em distribuições de ***streaming***.



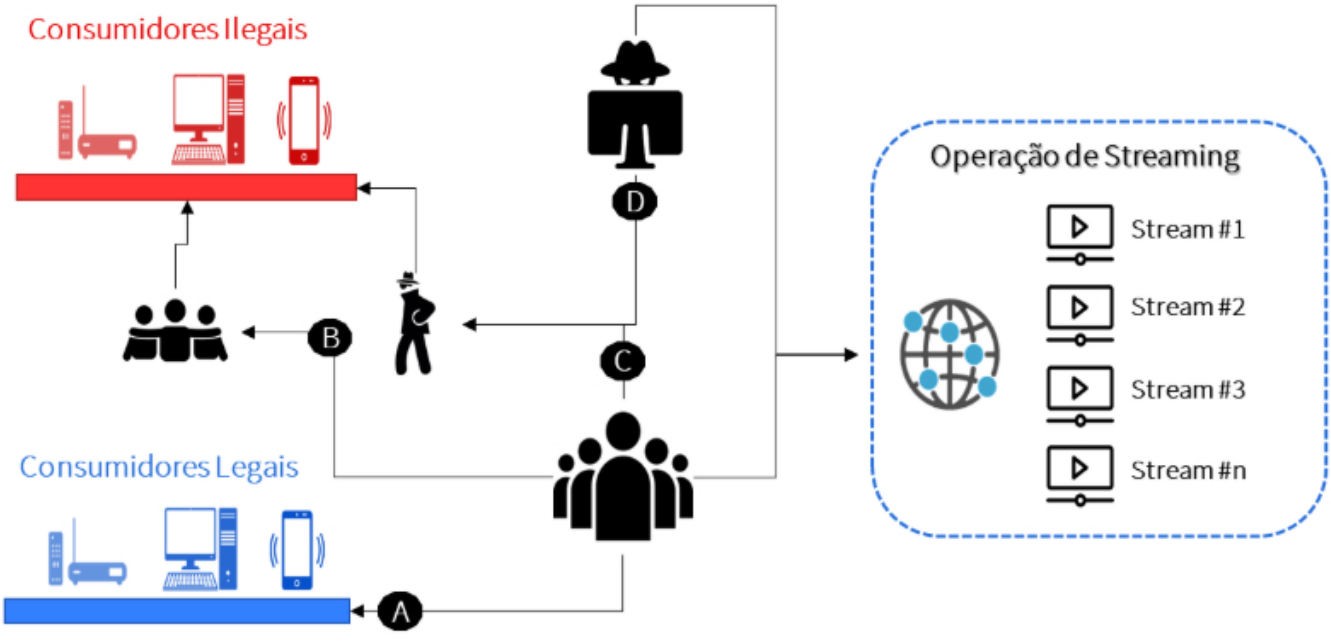
Fonte: Autor

Item/Fluxo	Descrição
A	Este fluxo indica um processo normal de transmissão em uma operação de ***streaming*** de vídeo, no qual um usuário regular acessa a plataforma de vídeo, navega e tem acesso aos conteúdos que estão disponíveis (ao vivo ou por demanda). Normalmente os conteúdos de vídeo são acessados através de uma estrutura de distribuição de conteúdos (CDN).
B	O fluxo "B" mostra um usuário ilegal, consumindo o conteúdo de forma ilegal diretamente da infra-estrutura do operador de ***streaming.*** Ou seja, neste modelo de pirataria o operador de streaming é duplamente lesado: (1) tem consumidores acessando o seu conteúdo premium sem ter pago por este acesso e (2) ainda está pagando sua infraestrutura de tecnologia de informação com sistemas e hardware para entregar o conteúdo da melhor forma possível para este consumidor ilegal. Mas como isso acontece?

Item/Fluxo	Descrição
C	Para que isso seja possível, o fluxo "C" introduz a figura de um ***hacker*** (ou ***cracker***) que vende em mercados paralelos um serviço no qual ele analisa e explora vulnerabilidades cibernéticas na estrutura do operador de ***streaming*** alvo. Essas vulnerabilidades variam de estrutura para estrutura e podem se apresentar nos sistemas de gerenciamento de tokens de autenticação, de tokens de autorização, ou ainda em sistemas de Control Plane, CDN e sistemas de DRM (ou multi-DRM, mais comuns). Uma vez analisadas as vulnerabilidades, este ***hacker*** cria um ***script*** que vai iterar sobre os conteúdos disponíveis na plataforma (normalmente conteúdos ao vivo) e gerar uma URL que pode ser utilizada em qualquer aplicativo ou navegador de internet sem que seja necessário fornecer nenhum tipo de credenciais ou quaisquer informações extras.
D	Neste fluxo, identificamos um agente pirata que encomenda e adquire estes scripts dos ***hackers*** e os executam frequentemente, gerando e renovando as URLs "tocáveis". Uma vez em posse dessas URLs este pirata faz uso de múltiplos mecanismos para vender o acesso ilegal a consumidores piratas.
E	Neste fluxo, o agente pirata cria listas, aplicativos e websites que apresentam o serviço como um serviço de TV legalizado. Contudo, consumindo os acessos ilegais gerados pelo processo descrito nos passos anteriores.
F	A última etapa deste modelo é quando os piratas utilizam as URLs tocáveis extraídas no passo D e através dos meios descritos no passo E disponibilizam acesso aos consumidores ilegais nos conteúdos furtados.

Compartilhamento de Credenciais

A figura abaixo e a sua tabela adjacente ilustram e exemplificam o funcionamento do modelo de pirataria de compartilhamento de credenciais. Este é aplicado em distribuições de ***streaming***.



Fonte: Autor

Item/Fluxo	Descrição
A	Este fluxo indica um processo normal de transmissão em uma operação de ***streaming*** de vídeo, no qual um usuário regular acessa a plataforma de vídeo, navega e tem acesso aos conteúdos que estão disponíveis (ao vivo ou por demanda). Normalmente os conteúdos de vídeo são acessados através de uma estrutura de distribuição de conteúdos (CDN).
B	Este fluxo identifica o modelo conhecido no mercado como compartilhamento casual, sob o controle do assinante regular do serviço. Neste caso, o mais comum são casos: pais que assinam o serviço de ***streaming*** e "fornecem" as suas credenciais para os filhos. Ou ainda amigos que fazem uma espécie de consórcio onde cada um assina um serviço de ***streaming*** e compartilham as credenciais entre si, potencializando o acesso individual. Estes exemplos não são exaustivos e existem muitas outras "razões/justificativas" para o compartilhamento. Nesta modalidade, não existe a figura da compensação financeira ao "pirata". Apesar de parecer uma ação inofensiva está nominalmente proibida no(s) acordo(s) de serviço aceitos e/ou assinados com o provedor de serviço de streaming e também contribui para um processo de perdas operacionais ao provedor de serviço de ***streaming*** uma vez que este provedor precisa investir em infra-estrutura para atender à demanda de consumo que além de mais extensa do que um cenário normal, pode envolver acessos simultâneos e de posições geográficas diferentes e não esperadas.
C	Este fluxo, começa a demonstrar um problema de código civil, ainda em baixa escala, mas igualmente ruim para o provedor de serviço de ***streaming***. O assinante legal faz a assinatura de planos que permitem um número maior de acessos simultâneos, e explora esta configuração, oferecendo os acessos "excedentes" da sua assinatura por preços baixos em mercados paralelos. Aqui já existe a ação e pagamento para o "pirata", portanto, caracterizando uma venda fruto de um furto. Este modelo não escala muito pois fica limitado pela configuração de simultaneidade do provedor de serviços de ***streaming***.
D	Este último fluxo já demonstra um problema maior - especialmente para o provedor de serviço de ***streaming*** - de roubo/extravio de credenciais. Os crimes cibernéticos são - infelizmente - bastante comuns no mundo atual e normalmente a principal motivação para ataques e exfiltração de dados pessoais (que incluem credenciais em geral) são adquirir acesso a sistemas financeiros e sistemas corporativos, porém, muitos acessos a serviços on-line como ***streaming***, jogos, plataformas sociais, etc. são extraviados de forma colateral e são indiscriminadamente ofertados e comercializados em mercados paralelos.

Formas de consumo de conteúdo pirata audiovisual

Explicaremos abaixo quais as formas de consumo de conteúdo audiovisual de forma pirata e os seus riscos cibernéticos - quando houver.

TV Boxes

Os dispositivos chamados TV Boxes são set-top boxes, ou seja, aparelhos que estão conectados à uma fonte de conteúdo (ao vivo e on demand) e que transmite este conteúdo para um aparelho de TV ou monitor através de cabo HDMI. Estes set-top boxes são normalmente baseados em sistemas AOSP - Android Open-Source Project e tem como fonte de conteúdo:

- **Ao Vivo:** Satélite; e SKS: Conteúdo e chaves de criptografia compartilhados por Satélite. Em algumas ocasiões o mesmo Satélite, em outras Satélites diferentes - um para conteúdo, outro para as chaves.
- **IKS:** Conteúdo compartilhado por Satélite; e Chaves de criptografia compartilhadas por Internet.
- **Streaming:** Podem vir de estruturas próprias ou podem vir de estruturas compartilhadas. Assim, compartilhamento entre operações piratas "associadas"; ou Compartilhamento entre modos

de pirataria, onde o mesmo conteúdo pode ser distribuído em TV Boxes, Listas IPTV, Apps etc.

É cada vez mais comum observar o uso de técnicas P2P - peer-to-peer na redistribuição de conteúdo ilegal, aparentemente visando reduzir a carga de acessos nos servidores da infraestrutura pirata. Neste modelo, um TV Box procurará o conteúdo primeiramente em outro TV Box antes de tentar buscar este conteúdo nos servidores pirata.

Os TV Boxes podem variar nas suas especificações técnicas, possuindo desde configurações/ funcionalidades mais básicas até configurações/ funcionalidades bastante avançadas de hardware e periféricos. Alguns deles permanecem funcionando por alguns anos sem necessidade de troca de aparelho, contudo, é relativamente comum se identificar marcas que forçam que os seus consumidores comprem versões mais novas do seu TV Box, outros solicitam uma assinatura anual, através de processos de autenticação durante o boot do dispositivo.

É importante ressaltar que - isolados - os TV Boxes são apenas dispositivos Set-Top Boxs genéricos, contudo, quase a totalidade dos TV Boxes são comercializados com os "serviços" de vídeo ao vivo e on demand ilegais, isto é, são comercializados em mercados paralelos (físicos e digitais). Alguns oferecem certas funcionalidades que podem ser avaliadas como vantagens, porém, potencializam bastante os riscos cibernéticos, tais como: projetor e roteador mesh integrado, roteador Wi-Fi e extensor de Wi-Fi.

Riscos cibernéticos dos TV Boxes

Como explicado acima, a grande maioria dos fabricantes de TV Box fazem uso do sistema Android (AOSP) e, ainda que não atuem diretamente e pró-ativamente incluindo ***trojans, worms*** e vírus em seus ***firmwares***, não possuem nenhum investimento em segurança da informação.

Praticamente todos os modelos de TV Box são muito vulneráveis, podem ser facilmente comprometidos e fazer parte de vetores de ataque. Devido a quantidade estimada de TV Boxes em uso no Brasil, representa um risco muito alto para a infraestrutura de telecomunicações do país.

Para os dispositivos TV Box que possuem funcionalidades extra de roteador (Wi-FI/Mesh) ou de extensores de rede doméstica, os riscos cibernéticos são ainda maiores e podem envolver técnica de ataque cibernético conhecidos como "***men-in-the-middle***" ou homem/agente-no-meio, que consiste em utilizar um software malicioso entre a comunicação de um dispositivo e a saída da rede doméstica para internet, quando esta técnica é aplicada, todas as comunicações entre os dispositivos da rede doméstica - que eventualmente estiverem conectados com o roteador ou extensor oferecidos pelo pirata, por exemplo, conectar celulares, computadores, IoT no access point do TV Box em vez do roteador específico - podem potencialmente ser copiadas digitalmente e exploradas de forma maliciosa.

- **Exemplos de TV Box:** BTV; HTV; e InXPlus.

Faixa de preço praticada (ref. 2024): R$ 400,00 a R$ 1.200,00

Foto de Panos Sakalakis na Unsplash

Listas IPTV

As listas de IPTV ou playlists são arquivos de texto que contém instruções para que um software gerenciador de mídias possa criar um lineup (ao vivo) ou catálogo (on demand) com conteúdos retransmitidos ilegalmente.

Os softwares onde se consomem as listas de conteúdo ilegal são em sua grande maioria softwares perfeitamente legais, desenhados originalmente para consumo de mídia em ambiente centralizado e consumo de conteúdo (gratuito ou pago) distribuido de forma legal através da internet. Contudo, algumas organizações piratas fazem "parcerias" ou lançam seus próprios "***branded***" software. Que em princípio não contém conteúdo ilegal - sem que o usuário pague uma assinatura mensal -, portanto, estão regulares e presentes nas lojas de aplicativos de todas as TVs conectadas, de tablets/ celulares e de computadores.

Um detalhe técnico: muito embora o nome IPTV tenha se popularizado para o modelo de comercialização

pirata, em realidade se trata de streaming, ou OTT (*Over the Top*). Não são conhecidos piratas que desenvolveram e implementaram suas próprias redes *multicast* de distribuição.

São comercializadas principalmente em fóruns fechados e grupos especializados de redes sociais e/ou aplicativos de mensageria.

Riscos cibernéticos das Listas IPTV

Trackers maliciosos, dependendo do player IPTV que se utiliza, este player poderá ofereçer os mesmos riscos de um aplicativo malicioso para TVs conectadas, celulares, tablets e computadores.

- **Exemplos de Software para consumo de Listas IPTV:** VLC Media Player; e Aplicativos genéricos como XCIPTV, IPTV Smarters, IBO Player.
- **Exemplos de Listas IPTV:** ClubTV; Zeus; LifeTV; e ClienteTV.

Faixa de preço praticada (ref. 2024): R$ 20,00 a R$ 45,00

Apps

Aplicativos são softwares comuns, que fornecem acesso à conteúdo ilegal, neste caso normalmente não mesclam conteúdo ao vivo e on demand no mesmo aplicativo. Não são raros os casos onde estes aplicativos tentam simular marcas de operações legais e regulares de *streaming* e TV. Estes aplicativos específicos de distribuição ilegal de conteúdo são facilmente identificáveis e constantemente monitorados nas lojas oficiais de aplicativos tanto de Android como de iOS, por esse motivo são encontrados mais facilmente em lojas paralelas de aplicativos ou para download em sites específicos.

Uma vez baixados, estes aplicativos podem ser instalados em tablets, celulares ou em TV Box (AOSP), se valendo do acesso como desenvolvedor no caso dos dispositivos Android e de técnicas de *Jailbreak* no caso dos dispositivos iOS.

São comercializados normalmente em conjunto ou como opção para os TV Boxes, ou ainda em fóruns fechados e grupos especializados de redes sociais e/ou aplicativos de mensageria.

Riscos cibernéticos dos Apps

Malware, Backdoors, Extravio de dados.

- **Exemplos de Apps:** MyFamilyCinema; TVExpress; e RedPlay.

Faixa de preço praticada (ref. 2024): R$ 20,00 a R$ 35,00

Websites

São sites web específicos para a distribuição de conteúdo ilegal. Focados em conteúdo ao vivo. Fazem parte e se valem da internet indexada para conseguir chegar até os consumidores finais. Em linhas gerais é um modo pirata mais utilizado para eventos de grande audiência como eventos esportivos ou grandes lançamentos de séries/novelas/filmes.

O conteúdo ilegal é acessado de forma “gratuita”, ou melhor, sem a figura do pagamento. Este sistema se torna rentável através de publicidade. O pirata controla o website e portanto, controla o inventário, ou as oportunidades de anúncio digital, forçando o usuário do website a assistir uma quantidade grande de anúncios durante a transmissão do conteúdo ilegal. Os ***cookies, tokens*** e dados gerados pelos usuários destes websites são normalmente (re)utilizados para fraude em anúncios, onde o site simula visualizações inexistentes, veiculando uma certa quantidade de anúncios para uma audiência “virtual”, mas que digitalmente se parece com uma audiência real, gerando uma quantidade de impressões muito acima das reais. Alguns destes websites também reconhecem plugins e ferramentas de bloqueio de publicidade - chamados de ***ad-blockers*** - e não permitem que o usuário ilegal assista o conteúdo sem que antes estas ferramentas sejam desabilitadas.

Riscos cibernéticos dos websites

Malware, Fraudes em Publicidade, Trackers maliciosos.

- **Exemplos de Websites:** redecanaistv.dev; futemax. ma; e multicanais.fi

Faixa de preço praticada (ref. 2024): Acesso gratuito pela internet.

Sistemas de Download

Os sistemas de download de conteúdo são focados em conteúdo on demand, normalmente: filmes, séries, desenhos e animes. Livros, revistas, músicas e software (incluindo jogos) distribuídos ilegalmente também fazem uso deste modelo. Em resumo o conteúdo é furtado e/ou copiado de forma ilegal e depois disponibilizado para download.

Podem ser classificados em dois modelos:

- **Web-lockers ou Web-drives:** Neste modelo o conteúdo ilegal é distribuído de forma paga ou gratuíta atraves de sites ou foruns especializados, links especiais - públicos ou privados - de serviços como: Google Drive, Mega Upload, Dropbox, Rapid Share, SugarSynnc, Onedrive etc.
- **P2P:** Neste modelo os usuários trocam conteúdo distribuído ilegalmente através de softwares baseados no protocolo *Peer-to-peer*, uma forma de rede distribuída na qual os computadores/dispositivos conectados ao sistema atuam como clientes e também como servidores. Os arquivos grandes são divididos em pacotes menores, ordenados, os computadores/dispositivos que já possuem uma determinada parte do todo atuam como servidores destas partes, enquanto são clientes das partes que ainda não possuem, fazendo o download de algum outro computador/dispositivo. Este protocolo ainda utiliza técnicas de análise de latência, priorizando o download de locais mais próximos ou com uma conexão melhor.

Riscos cibernéticos dos websites

Em linhas gerais o principal risco é o de perpetuação de ameaças do tipo trojans, worms e vírus, que podem abrir caminho para ataques de data exploitation e sequestro de dados/infraestrutura (*ransom*).

- **Exemplos de Websites:** Google Drive, Mega Upload, Dropbox, RapidShare, Sugarsync, Onedrive etc. uTorrent, Bittorrent, eMule, Soulseek, Ares etc.

Faixa de preço praticada: normalmente gratuitos para conteúdo audiovisual.

Conclusões

Este estudo demonstra que os criadores - ou agregadores - de conteúdo que desejam vender o acesso a estes conteúdos podem sofrer ataques de formas diferentes para extravio deste conteúdo. Mostra também que o efeito "***Robin Hood***" não é mais válido (isso se algum dia já foi considerado válido no passado. Significa que as pessoas envolvidas no furto, extravio, distribuição e empacotamento de conteúdo audio-visual pirata lucram – muito – com essas operações ilegais.

Por último, demonstra que todos os modelos de distribuição de conteúdo pirata oferecem algum tipo de exposição a riscos ciberneticos por parte dos consumidores, que, ou desconhecem estes riscos, ou não acreditam que ataques poderão acontecer com eles/elas, ou não se importam em correr esses riscos.

No final a indústria audiovisual inteira perde receita, os usuários precisam pagar de qualquer forma pelo acesso ao conteúdo, existem riscos cibernéticos latentes – inclusive à própria infraestrutura de telecomunicações do país, e os "piratas" enriquecem vendendo um produto que não produziram e nem contribuíram com a produção.

Danilo Almeida

é diretor técnico de engenharia de soluções e Engenheiro de soluções SaaS na Synamedia, graduado em Sistemas de Informação pela FIAP, com especialização em gestão de operações pela POLI-USP e Inovações/Transformação Digital pela FIAP. Atua há mais de 20 anos no mercado de tecnologia e há 12 anos no mercado de TV digital. Palestra sobre tecnologia, ad-tech, broadcast & streaming e combate a pirataria no mercado audiovisual. Guitarrista e churrasqueiro ocasional.

Contato: daniloalmeida@gmail.com