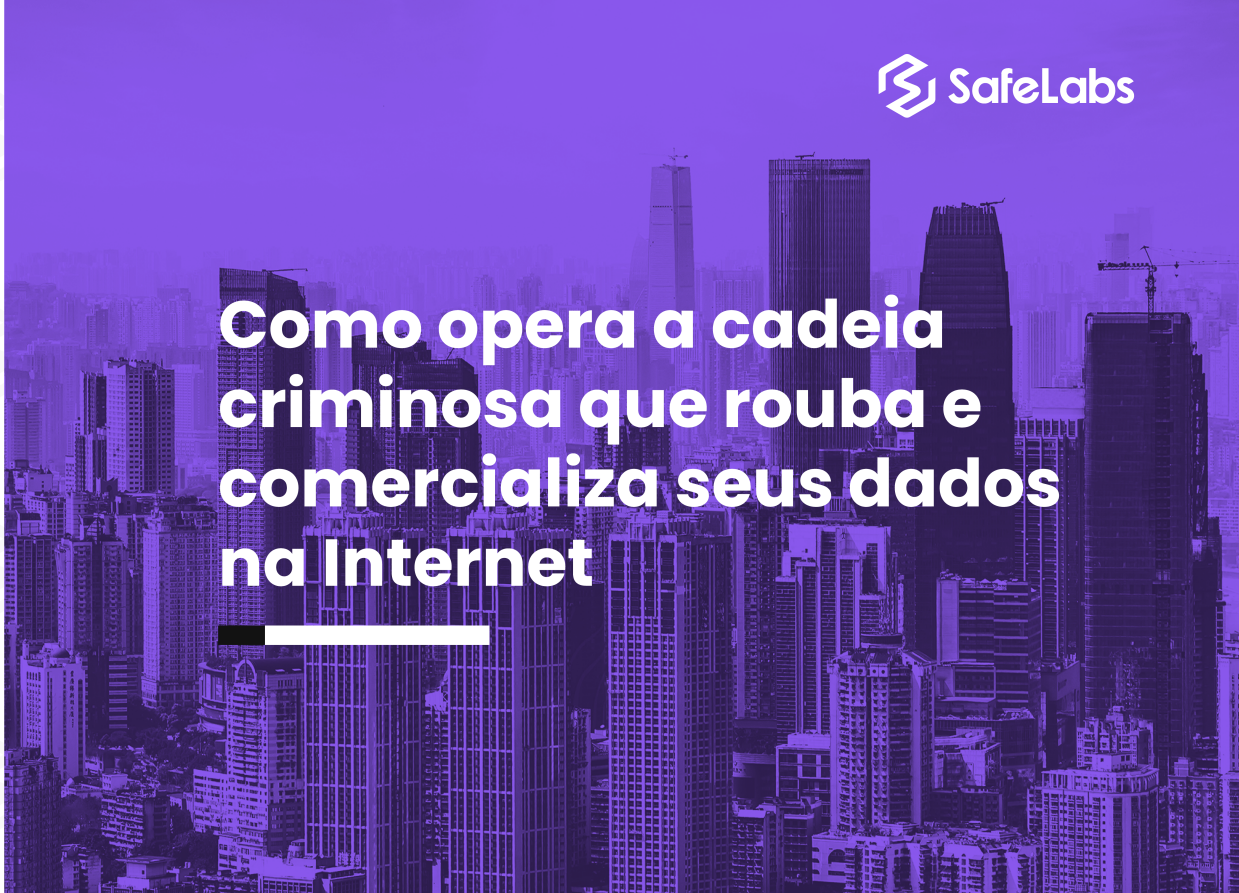
SafeLabs

Como opera a cadeia criminosa que rouba e comercializa seus dados na Internet



Sumário

1. Introdução

Antes de falar sobre a comercialização de credenciais no mundo do cibercrime, é importante termos um entendimento básico sobre o que é a impressão digital de dispositivo (em inglês, Device Fingerprint), como ela é importante para a proteção de sistemas de autenticação, como de fato essa impressão digital funciona e quais seus usos potenciais para o crime digital.

Device Fingerprint são informações coletadas sobre um dispositivo de computação para fins de identificação. Elas podem ser utilizadas para identificar usuários ou dispositivos na rede, e esse reconhecimento não ocorre necessariamente através de algum tipo de credencial específico. A coleta e o armazenamento desses dados são fundamentais para a segurança. Permitem, por exemplo, que bancos e varejistas online evitem que fraudadores tentem burlar sistemas de segurança durante o processo de autenticação.

Apenas sistemas modernos que trabalham com Device Fingerprint conseguem garantir que dois computadores idênticos sejam vendidos no mesmo dia, na mesma loja de uma cidade, instalados e configurados por empresas diferentes, e ainda assim sejam discernidos no ambiente online com uma precisão de 98%, uma leitura feita com base em todos os parâmetros possíveis coletados através da impressão digital.

Normalmente, as soluções de antifraude utilizam as próprias técnicas conhecidas aplicadas por fraudadores para bloquear transações que tenham impressões digitais semelhantes. E por algum tempo, isso foi suficiente. Porém, hoje criminosos já encontraram novas formas de randomizar impressões digitais (uma das principais iremos abordar neste relatório) para burlar o Device Fingerprint.

Por isso, nesse relatório, iremos apresentar de forma detalhada como funciona uma cadeia de operação comercial de credenciais e impressões digitais, como funciona cada etapa dessa rede criminosa e a ligação da operação, ponto a ponto.

Em resumo, **o que você irá encontrar nesse documento é**:

- Breve introdução sobre impressões digitais;
- Conceitos técnicos, benefícios e malefícios desta tecnologia;
- O funcionamento do processo de roubo destas impressões digitais por cibercriminosos;
- Como fraudadores burlam sistemas avançados de proteção contra Malwares e Trojans;
- A estruturação da cadeia criminosa e como os dados roubados são comercializados em redes de marketplaces pela internet.

2. O algoritimo da similaridade

2.1. O benefício que traz um risco

Como qualquer tecnologia de rastreamento e identificação, o Device Fingerprint também é um benefício que carrega um risco. As impressões digitais podem ser usadas de forma construtiva para combater fraudes online ou roubo de credenciais, verificando se um usuário que faz autenticação em um site específico é de fato o usuário legitimo da conta informada. Mas, enquanto criam essa vantagem, geram ameaças ao possibilitarem o rastreio de usuários em sites e a coleta de informações sobre hábitos e gostos sem que eles saibam. Em um cenário mais preocupante, as impressões digitais também ajudam a burlar sistemas de antifraude online, utilizando os mesmos dados da impressão digital para autenticar um cibercriminoso que obteve credenciais ilegalmente, permitindo que ele acesse sistemas como se fosse o usuário legítimo da conta.

Pense na loja online em que você costuma fazer compras. Em algumas ocasiões, a loja exige que você prove que você é você mesmo. Para isso, envia um código de verificação para seu e-mail ou uma mensagem SMS com o intuito de confirmar a identidade. Este procedimento é chamado de Challenge (Desafio), e é aplicado em cenários em que o padrão de uso ou de hábito estão diferentes do de costume reconhecidos pelo sistema da loja.

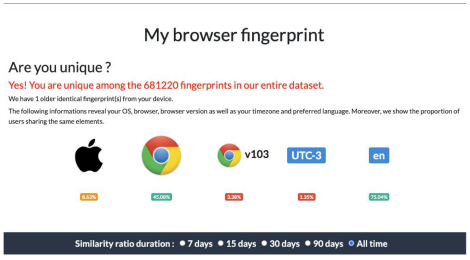
Esse padrão de uso funciona com a impressão digital do usuário, coletada todas as vezes que ele acessa e faz o uso da loja online. Garante a segurança, mas também gera uma fragilidade. Afinal, um cadeado só protege uma porta se a chave que o abre estiver em mãos confiáveis. Ou seja, da mesma forma que a loja utiliza os dados para identificar o cliente e, assim, protegê-lo, limita todo o processo de segurança ao portador dos dados. Se as informações forem roubadas, a porta sequer precisará ser arrombada. Usando dados legítimos, os cibercriminosos terão acesso livre a informações de pagamentos e todo o histórico da loja online.

2.2. Quantitativo de conexões bloqueadas

Mesmo que existam dois computadores idênticos na internet, ainda assim serão únicos. A distinção desses computadores possíveis é possível graças a tecnologias que permitem acessar praticamente qualquer informação do dispositivo do usuário sem a necessidade de instalação de um agente ou software adicional.

Essas tecnologias são desenvolvidas pela linguagem de programação JavaScript. E no navegador instalado no dispositivo do usuário, acessa dezenas de informações técnicas. Há também o componente Canvas do HTML5, que ajuda no acesso a dados importantes para a formação da impressão digital. Facilita a coleta de pequenas variações e configurações de um mesmo hardware, ainda que os dispositivos sejam quase idênticos. A menor diferença no processamento de um pixel é detectada.

Existem alguns sites que ajudam curiosos a atestar se o seu usuário é realmente único, e se não há pessoas se passando por eles na internet. As informações são coletadas e comparadas a impressões digitais de um banco de dados interno. Um dos sites mais famosos que fazem esse trabalho é o amiunique.org. Ele funciona a partir de técnicas modernas de identificação e algoritmo de similaridade.



Na imagem acima, vemos que um dos principais elementos que compõem a impressão digital é o Sistema Operacional, seguido por navegador, versão do navegador, fuso horário do usuário e a linguagem padrão do sistema. Existem centenas de outros elementos considerados na hora de se determinar o quão único alguém é na rede. Rolando a página, há detalhes mais avançados que também foram coletados e utilizados na identificação.

Lembrando que, apesar de o site ser considerado confiável, ele não abrange a imensidão da internet, portanto o resultado que ele mostra não pode ser compreendido como a verdade absoluta sobre o sigilo e a segurança dos seus dados.

3. Roubando seus dados

3.1. O que é um Stealer

Agora que já explicamos o que é o Device Fingerprint, como elas são importantes para o combate a fraudes digitais, e como também podem acabar se tornando um risco enquanto garantem segurança, iremos entender melhor como funciona toda a rede de operação dos cibercriminosos para roubar dados e de que maneira credenciais e impressões digitais são obtidas por meio de engenharias sociais simples para a disseminação de trojans do tipo Stealer.

Um Stealer é um tipo de malware focado em coletar informações confidenciais e condicionais de um sistema comprometido, como credenciais de usuários e dados financeiros e pessoais.

O caminho para se obter credenciais e fingerprints de forma massiva é o trojan do tipo Stealer. O malware consiste em executáveis com funções complexas, que acessam informações pessoais armazenadas nos dispositivos das vítimas depois de instalar um acesso persistente na máquina. Mantém comunicação contínua com um servidor malicioso, conhecido como C2 (Command & Control), para atualizar o roubo de dados e garantir que ele seja constante.

Os Stealer são vendidos em fóruns hackers por alguns dólares e, embora tenham como alvo informações de alto valor, não são sofisticados. A variação de preço no mercado ilegal online pode se referir à duração da assinatura e/ou à robustez de seus recursos.

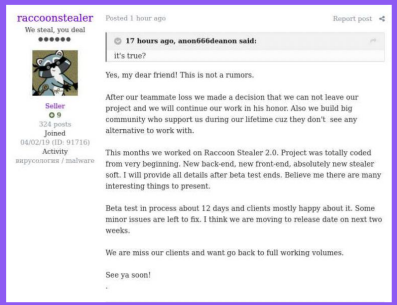
A maioria dos Stealers é vendido como Malware-As-A-Service (MaaS), em que os autores de malware incluem acesso a uma equipe de suporte técnico e atualizações (correções de bugs e novos recursos), além de um login em um painel administrativo em que o invasor pode personalizar a funcionalidade do malware, visualizar todas as credenciais/impressões digitais roubadas e baixar compilações atualizadas do malware.

3.2. O guaxinim

Existem dezenas de trojans do tipo Stealer. Aqui, iremos nos dedicar ao Raccoon Stealer. É um dos mais conhecidos, completos e modernos que existem.

O Stealer Raccoon, visto pela primeira vez em abril de 2019, continua popular por causa dos recursos avançados e do baixo preço. A antiga versão tinha assinaturas comercializadas por US$ 75 por semana e US$ 200 por mês. É capaz de roubar informações confidenciais de quase 60 aplicativos em sua versão mais recente, entre credenciais de login, impressões digitais, informações de cartão de crédito, carteiras de criptomoedas e informações do navegador (cookies, histórico, preenchimento automático).

A operação comercial do Raccoon Stealer foi encerrada em março de 2022, quando seus operadores anunciaram que um dos principais desenvolvedores foi morto durante a invasão da Ucrânia pela Rússia. A equipe restante prometeu retornar com uma segunda versão, relançando o projeto Malware-As-A-Service (MaaS), em infraestrutura atualizada e com mais recursos.



Para conhecimento, outros Stealers que se destacam: Redline, Azorult e Taurus, sendo o Azorult um dos mais antigos, e que vem causando certo estrago na rede até os dias de hoje.

Nesta nova versão 2.0, o Raccoon foi reescrito puramente em C++. Embora não tenha sofisticação nenhuma em seu código fonte, compila vários métodos e recursos de roubo de dados de navegadores populares, clientes de e-mail e carteiras de criptomoedas.

Dentre as principais características do Trojan, estão:

- Completamente reescrito do zero (também em C++);
- Tamanho executável 55 Kbytes (anteriormente 580 Kbytes);
- Importação dinâmica de todas as funções;
- Suporte para conexão SSL;
- Descriptografia de senhas, cookies e dados (AES GCM) no navegador.

Na nova versão 2.0, o desenvolvedor do Raccoon garante ainda alguns pontos importantes sobre o sistema que sustenta o novo Stealer:

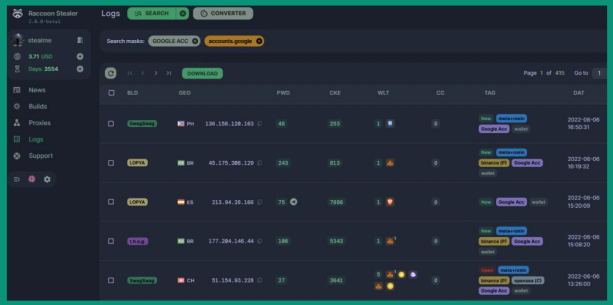
- Sistema descentralizado;
- Backups regulares;
- Alertas sobre o status dos nós principais para manter alto uptime;
- Sistema de busca rápido e outros.

A dedicação no desenvolvimento e sustentação do Raccoon 2.0 é tão grande que o responsável pelo Stealer garante atenção até na experiência da interface gráfica do trojan. Praticamente um trabalho de UX/UI.

A maioria dos malwares, particularmente os do tipo MaaS, tem um servidor C&C para que possa obter informações sobre as opções e recursos ativados pelo cibercriminoso e enviar de volta todos os dados roubados da vítima.

A saída do Raccoon Stealer do mercado foi curta, o que demonstra que nem sua reputação nem o interesse dos cibercriminosos desapareceram. Prova disso é que, durante o hiato do Raccoon, outros Stealers apareceram, como Mars Stealer e Jester Stealer, porém, nenhum teve a chance de alcançar as mesmas notoriedade e reputação.

A segunda versão principal do Raccoon Stealer está disponível apenas para um número limitado de cibercriminosos, provavelmente clientes anteriores. O custo é definido como US$ 275/mês ou US$ 125/semana.



3.3. E lá se foram seus dados

Sempre que a vítima é infectada pelo Stealer, o que costuma acontecer por meio de uma engenharia social, baixa e executa o arquivo malicioso com os breakpoint (códigos maliciosos que iniciam com um cabeçalho programado para passar confiança e burlar programas de Antivírus). Assim, é iniciada a tarefa do Stealer, que, por padrão, é quase sempre a de atribuir um serviço no sistema de tarefas do Windows, criar a persistência no sistema e, assim, se manter ativo mesmo que o usuário reinicie o computador.

Logo que a persistência é concluída, a maioria dos trojans do tipo Stealer fazem uma comunicação com seu endpoint de C2 (Command & Control) para receber algum comando específico, validar conectividade com a internet e por fim iniciar o roubo de dados.

Estes trojans são desenvolvidos para procurar e roubar dados de forma paragramática, pesquisando em pastas específicas do sistema. Quando encontradas as pastas e os arquivos, tudo é copiado para uma outra pasta temporária, criptografado e enviado para o C2 que gerencia o Stealer.

As pastas e arquivos que os Stealers procuram são:

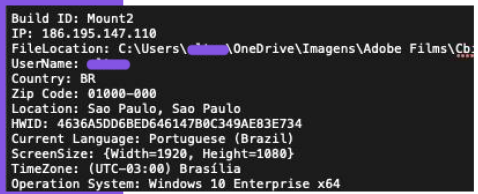
- Senhas salvas no navegador;
- Cookies;
- Tokens de aplicações de mensageria;
- Tokens de aplicações bancárias;
- Textos de Autofills (autopreenchimento) de navegadores;
- Softwares instalados na máquina;
- Dados de carteiras Bitcoin.

Estes são os principais dados que um Stealer geralmente busca nas máquinas das vítimas (lembrando que isso pode variar muito de um Stealer para outro). Compartilhamos abaixo um exemplo de pastas com os arquivos roubados pelo Stealer:

Todos os arquivos são organizados por tipo e fonte, sendo que a disposição depende do tipo e versão do Stealer. Alguns mais simples coletam apenas as senhas salvas no navegador, e outros mais complexos conseguem até mesmo gravar alguns segundos da área de trabalho da vítima quando uma ação monitorada é identificada.

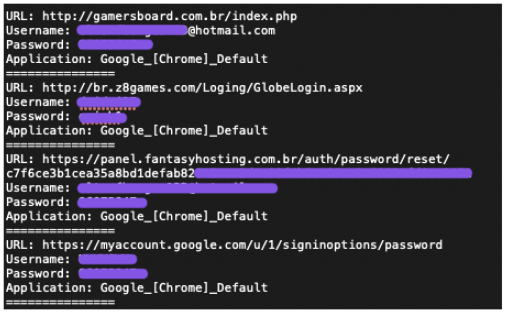
No arquivo UserInformation.txt podemos encontrar diversas informações sensíveis relacionadas ao computador da vítima. Elas podem ser utilizadas para montar uma estrutura falsa de Device Fingerprint (impressão digital) quando o cibercrimonoso for acessar sistemas online com as credenciais da vítima, conforme já explicado no início deste relatório.

Informações como endereço IP, localização, Hardware ID e resolução do sistema são informações críticas para burlar sistemas com proteção baseados em impressão digital.



Um dos arquivos fundamentais é de fato o Passwords.txt, que contém todas as credenciais da vítima encontradas pelo Stealer. Afinal, de nada adianta acesso aos dados de impressão digital da vítima sem ter as credenciais reais do usuário.

Quando vamos acessar sistemas com baixa maturidade de segurança ou sem nenhum controle de identicidade apenas as credenciais são suficientes, contudo, para sistemas robustos, é necessária a combinação dos dois.



Estes dois arquivos, UserInformation.txt e Passwords.txt, são importantes para nosso entendimento do relatório.

Existem outros arquivos críticos, como o Autofills, que trazem tudo o que foi salvo como autopreenchimento no navegador da vítima, pois pode contar informações importantes do usuário; ou a pasta de Tokens bancários, que nos leva diretamente ao impacto financeiro da vítima. Contudo, geralmente as senhas e impressões digitais são os principais procurados nos resultados de uma contaminação de Stealer.

4. A engenharia

4.1. A isca

Muitas questões influenciam na elaboração de uma estratégia de engenharia social. Perfil de consumo, faixa etária, cultura (países latino-americanos, por exemplo, sofrem mais com distribuição de Trojans através de engenharia social com foco jogos online, os famosos "hack"). O que torna o assunto desafiador de ser abordado.

Da mesma forma, quando cibercriminosos desenvolvem alguma engenharia social para roubar credenciais de colaboradores de grandes corporações, discutem o que precisa ser levado em consideração para aumentar a probabilidade de o usuário baixar e executar o arquivo malicioso. Além disso, direcionar um golpe diretamente para o alvo está mais difícil devido ao amadurecimento da cultura de cibersegurança dos usuários, introduzida pelas empresas em que trabalham.

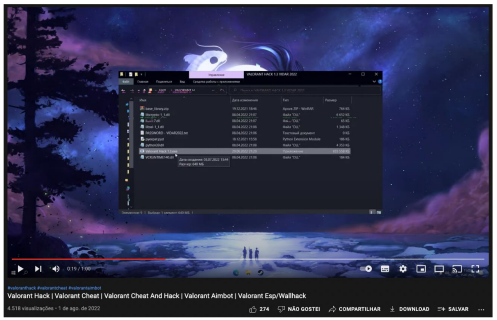
As campanhas de conscientização durante o uso do computador de trabalho, a educação sobre noções de segurança da informação, novas tecnologias de proteção e meios de comunicação protegidas, como VPN, cresceu no mundo corporativo. Assim, não é mais tão fácil fazer com que um colaborador morda uma isca. Isso exige que os cibercriminosos criem formas de atingir suas vítimas.

4.2. Crianças e os jogos online são a nova engenharia social

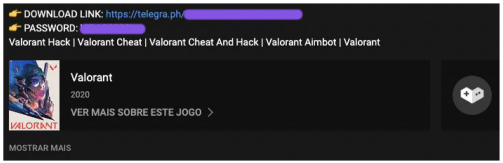
Então, se os colaboradores estão melhor preparados para identificar uma tentativa de golpe, um novo alvo fácil é discutido nas comunidades de Trojans: as crianças e os filhos desses colaboradores.

E o Home Office é a realidade em que a família do colaborador pode ter contato com o computador de trabalho que, antes, ficava somente no escritório. Em muitas situações, aquele computador doméstico, que era compartilhando por todos da casa, passou a ser a mesma máquina que os trabalhadores acessam dados da empresa. Se os filhos gostam de jogar online, vão preferir o computador corporativo caso a máquina tenha um hardware mais potente.

Se os pais autorizam, a criança acessa o jogo, interage em comunidades gamers, descobre ferramentas para facilitarem desempenho e experiência, e talvez cheguem aos famosos "Hacks", que prometem vantagens desleais durante a partida. No YouTube, há milhares de vídeos com links de download do facilitador, junto com passo a passo de instalação.

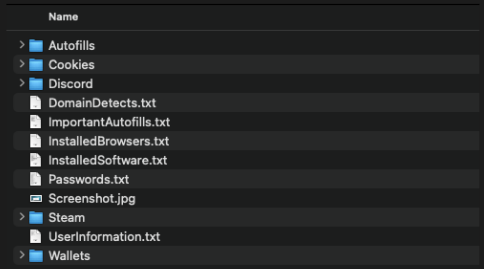


Assim que o executável é baixado, informando algum tipo de senha para extrair o suposto Hack, começa o processo de distribuição do Stealer na máquina da vítima, assim como a persistência no computador para que, mesmo que os arquivos baixados sejam deletados e o sistema reiniciado, o Stealer permaneça ativo.



A máquina que executou o suposto Hack já está infectada e o malware vai precisar de poucos minutos para copiar os arquivos da vítima e enviá-los de forma criptografada para uma nuvem do cibercriminoso, organizados como apresentamos na Figura 4 deste relatório.

Como exemplo e forma de demonstrar um caso real, identificamos uma vítima que teve dados obtidos através da mesma engenharia social, utilizando o Stealer Redline, com operação e funcionalidades muito próximas do Raccoon:

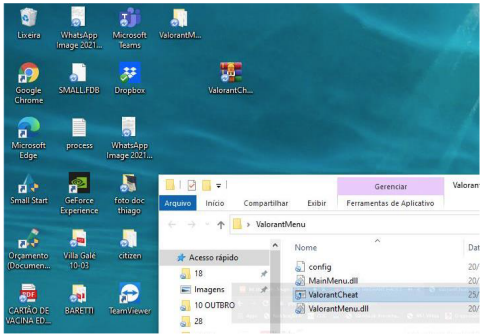


A vítima desse exemplo foi atraída pela engenharia social de Hack para jogos online. E podemos confirmar que se tratava do filho de um colaborador de alguma empresa pela análise das impressões digitais (Device Fingerprint) dos dados coletados na máquina. Tratava-se de um computador corporativo. O Hack online do jogo baixado foi o com nome de Valorant.

```
Build ID: @m[redacted]
IP: 143.255.111.24
FileLocation: C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
UserName: [redacted]corporate
Country: BR
Zip Code: 72910-[redacted]
Location: Aguas Lindas de Goias, Goias
HWID: DAB11827C21[redacted]
Current Language: Portuguese (Brazil)
ScreenSize: {Width=1600, Height=900}
TimeZone: (UTC-03:00) Brasilia
Operation System: Windows 10 Enterprise x64
UAC: AllowAll
Process Elevation: False
```

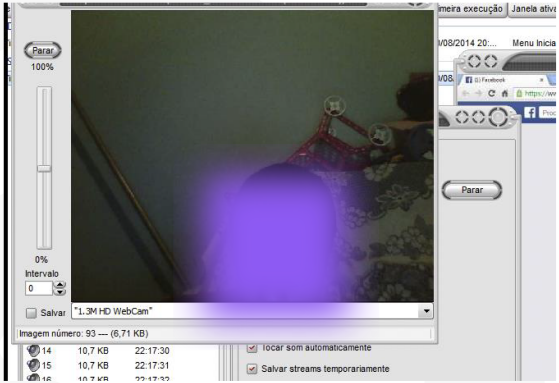
Podemos identificar o domínio corporativo no Username, como também é possível validar que se trata de um Windows 10 Enterprise, exclusivo para computadores corporativos.

Alguns Stealers também conseguem capturar uma foto da tela da área de trabalho assim que o Trojan é executado, como aconteceu neste exemplo que nos auxiliou a evidenciar que se tratava mesmo de um dispositivo de trabalho.

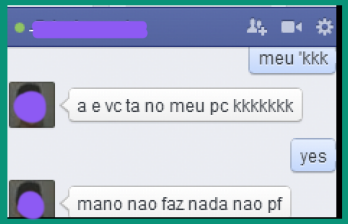


No corte da tela capturada, é possível ver o aplicativo malicioso com nome de "ValorantCheat" sendo executado. Uma demonstração do que vem sendo discutido nos últimos meses nas comunidades de Stealers e desenvolvimento de trojans. A engenharia social se torna mais eficaz quando a distribuição é focada em conteúdo infantil, principalmente jogos online.

Durante as discussões dos cibercriminosos em como melhorar e desenvolver novas engenharias sociais, alguns membros da comunidade até evidenciam, com ironia, como é fácil direcionar o foco para o público infantil, postando fotos de câmeras de vítimas ligadas.



Para os cibercriminosos a facilidade é tanta que eles chegam a mandar mensagens no perfil de redes sociais da vítima com o intuito de provocar essas crianças, incentivando que elas chamem o responsável pelo computador, reiniciem a máquina ou utilizem algum tipo de antivírus. O acesso ilícito ainda vai persistir.



Neste caso a criança seguiu um tutorial de como desativar alguns elementos de segurança do computador corporativo, baixar e executar arquivos maliciosos. E, assim, abriu a porta para o cibercriminoso acessar dezenas de credenciais corporativas e dados de impressão digital.

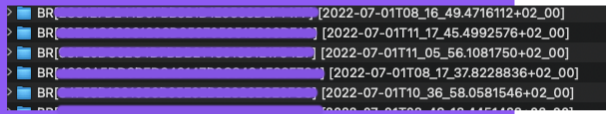
5. Oito senhas, um real

8D5AF30

5.1. Seus dados organizados

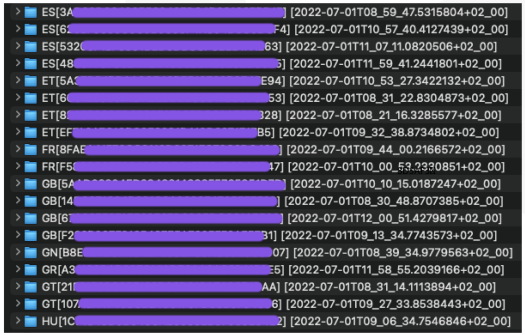
É comum que um único trojan, de um simples vídeo no YouTube, chegue a fazer; milhares de vítimas em poucas horas. A atração e a facilidade que o vídeo passa para a vítima, prometendo poucos passos para a trapaça que irá garantir a vitória no jogo, faz que com milhares de crianças caiam na engenharia social.

No servidor do cibercriminoso dezenas de pastas com os arquivos das vítimas vão se acumulando a cada minuto enquanto o vídeo está no ar. As pastas são todas organizadas pelo nome do país da vítima, seguido por um ID de identificação e por final a data de infecção da vítima.



Uma curiosidade importante é que a sigla do país de origem da vítima é crucial durante a comercialização distribuição dos dados. Isso porque é comum que compradores interessados peçam dados de um país específico, afinal, as credenciais e informações vão ser utilizadas para um novo ataque, personalizado para habitantes de um local específico.

Como o alcance de divulgação do vídeo pode ir além de um território somente, as campanhas de Stealers acabam coletando vítimas de variadas regiões do mundo. O que é vantajoso para o cibercriminoso, que ganha mais mercadoria para comercializar. Alguns países como China ou Rússia tem pouca relevância no mercado negro, enquanto dados de corporações norte-americanas ou da Europa Ocidental são valorizadas por compradores.



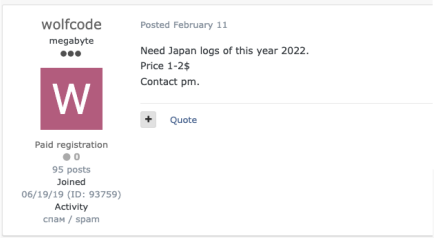
5.2. Credenciais a venda

Agora vamos falar a respeito do destino desses arquivos que contêm dados pessoais e credenciais das vítimas, de que modo são comercializados, os valores, principais compradores e como acontece a distribuição dos dados no mercado negro. Importante: arquivos roubados são chamados de “Logs” pelos cibercriminosos e é esse nome que vamos utilizar daqui para a frente.

Assim que as informações das vítimas são roubadas e copiadas para a nuvem do cibercriminoso, costumam ter pelo menos um de três destinos possíveis, sendo eles:

1. Venda direcionada no fórum / comunidade que compra de regiões específicas;
2. Venda direcionada a empresas e marcas;
3. Venda para lojas de varejo, compras e pagamentos feitos no atacado.

A primeira possibilidade é quando o dono dos logs (resultados da campanha de Trojan) separa os arquivos das vítimas por país e vende a criminosos que já têm alguma técnica de monetização específica para vítimas daquela região. Aqui, os preços praticados são os mais baixos, variando entre USD 1$ a USD 5$.

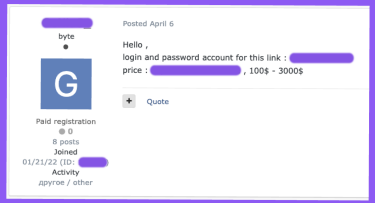


Os arquivos costumam ser usados para crimes de extorsão, com foco em vítimas que tenham algum tipo de relação extraconjugal. Assim, o criminoso entra em contato com a vítima após vasculhar e-mails pessoais atrás de fatos comprometedores.

Outro cenário bem comum são logs que contêm algum tipo de dado bancário, usados por criminosos que já tem um método para como conseguir sacar o dinheiro das contas de vítimas daquele país.

No caso de vendas direcionadas a empresas e marcas, talvez um dos mais perigosos, o cibercriminoso busca compradores que estão atrás de dados de organizações específicas. A negociação acontece por meio de fóruns, em que há anúncios que tratam de um o interesse em uma marca ou empresa, com valor determinado. Para fazer a oferta, o criminoso que possui milhares de logs, pesquisa o que é pedido no anúncio, geralmente priorizando arquivo com credenciais de acesso.

Na grande maioria das vezes o comprador utiliza estes dados para acessar o ambiente computacional da empresa e instalar um ransomware, roubar dados da organização e cometer extorsão após o vazamento. Os preços praticados neste cenário são os maiores, chegando a 20 mil dólares dependendo do tamanho da empresa.



O terceiro caso é o mais famoso e procurado, que são as vendas feitas na modalidade de varejo. O cibercriminoso entra em contato com o proprietário da loja e vende todos os seus logs. Recebe um valor que varia de acordo com a qualidade dos arquivos, medida através da data dos arquivos, do trojan utilizado para obtê-los e se eles são de fato únicos.

Assim que o criminoso entra em contato com o lojista, é utilizada uma ferramenta que checa a duplicidade desses Logs. Há situações em que a mesma vítima teve seus dados roubados por mais de um Stealer, por exemplo, então não é incomum que dois cibercriminosos consigam os mesmos dados através de trojans diferentes.

Quando o Log recebe a tag de "único", o preço dele aumenta, e a quantidade de credenciais contidas no arquivo Passwords.txt também faz o preço pago pelo lojista aumentar exponencialmente. Não é costume checar se os Logs contêm dados de grandes empresas ou acessos críticos, como uma VPN, por exemplo. Os fatores de avaliação são sempre bem simples até pela quantidade de logs que transaciona diariamente neste tipo de loja online criminosa.

5.3. Aceitamos apenas bitcoin

Como forma de detalhar um pouco mais sobre o caso 3 do tópico anterior, trazemos capturas de tela que mostram como a operação de uma loja funciona, as formas de pesquisas e os preços praticados.

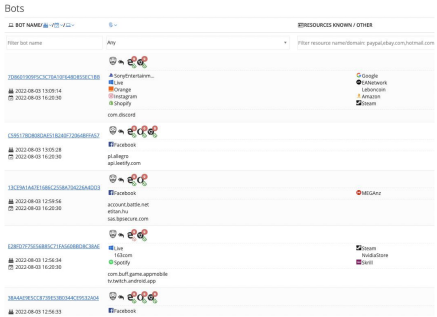
A loja escolhida chama Genesis e talvez seja a mais conhecida no submundo online, com o maior volume de Logs ofertados no varejo criminoso.

A loja tem um Dashboard que traz a quantidade de logs organizados por país e separados por uma tabela com colunas para as últimas 24 horas, última semana e último mês. No final, aparece o total de logs disponíveis para cada região.

Available Bots

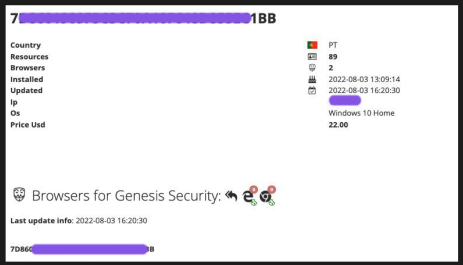
COUNTRY	LAST 24H	LAST WEEK	LAST MONTH	AVAILABLE
Overall				
226	+751	+3080	+16396	439394
Groupped by				
PL	+164	+673	+3386	24820
RO	+126	+450	+2294	28319
PT	+47	+180	+983	27801
HU	+53	+189	+829	15228
ES	+30	+158	+737	33957
US	+15	+52	+654	7639
CZ	+42	+145	+635	3477
LT	+23	+122	+582	1566
TR	+17	+145	+501	23262
IT	+19	+110	+499	56760

Ao acessar a opção de bots (a loja utiliza o nome de bots no lugar de logs), o comprador tem acesso a um campo de busca que levanta endereços web, nome ou ID do bot, e filtra as informações por aplicativos que a vítima tinha instalado no computador. Outro filtro é o endereço IP da vítima.

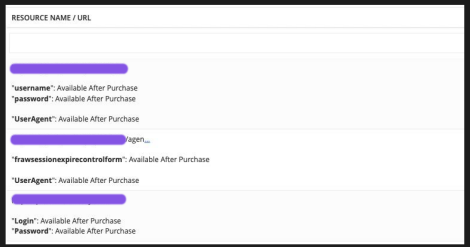


A busca por endereços web é importante porque permite que o cliente da loja faça pesquisas direcionadas para encontrar credenciais de acesso ligadas a empresas específicas. É possível pesquisar, por exemplo, entre arquivos Passwords.txt. O que quer dizer que, caso a empresa que sofreu o ataque do Stealer tenha alguma credencial disponível na loja online, o comprador consegue adquirir no varejo aquele acesso em particular. O que é matéria-prima para ataques hackers direcionados.

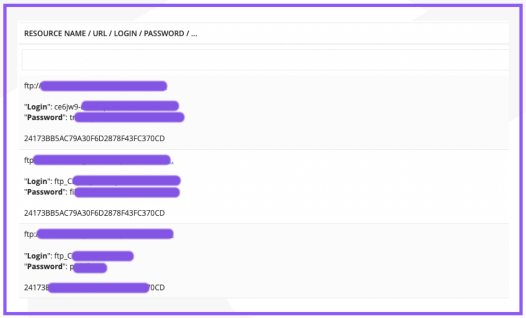
Assim que você clica em alguma das ofertas disponíveis na loja, uma nova página abre com todos os detalhes possíveis sobre o log e a vítima, como o país de origem, a quantidade de credenciais contidas na oferta, quando foi instalado o Stealer na máquina infectada e qual foi a última vez que o Stealer obteve atualizações (novos arquivos) do computador em que foi instalado.



Na parte de baixo do site é possível fazer pesquisas de endereços web em que a vítima tinha credenciais, sendo que não é possível visualizar as credenciais, a não ser que o usuário da loja finalize a compra.



Concluída a compra do bot (logs do Stealer), o cliente criminoso da loja tem acesso livre a todas as senhas e demais credenciais da vítima. O bot que estava à venda é retirado da “vitrine” da loja, para que o comprador tenha a garantia de exclusividade dos dados.



5.4. Cenário brasileiro de risco

Com o intuito de ilustrar o tipo de risco que essas lojas criminosas representam para segurança digital de empresas no nosso cenário brasileiro, o time de inteligência do Mantis desenvolveu uma ferramenta que obtém todos os possíveis endereços web das organizações citadas na lista "TOP 1500 MAIORES EMPRESAS DO BRASIL".

O algoritmo basicamente executa as seguintes funções sequenciais, sem entrar em detalhes técnicos e operacionais da ferramenta desenvolvida:

1. Obtém o nome da empresa contida na lista pública TOP 1500 do Estadão;
2. Pesquisa e valida o domínio principal da empresa em um site Whois público e Google para obter um endereço web válido;
3. Pesquisa o mesmo domínio no campo de filtro da loja Genesis, aguarda o resultado (que pode chegar a levar 1 minuto);
4. Analisa a quantidade de resultados retornados pela loja;
5. Salva o resultado em um arquivo tabulado.

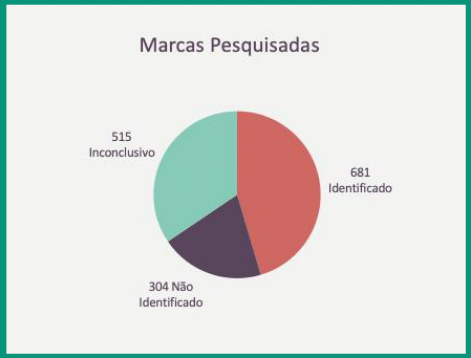
O resultado foi separado em três categorias, sendo elas **Identificado**, **Não Identificado** e **Inconclusivo**:

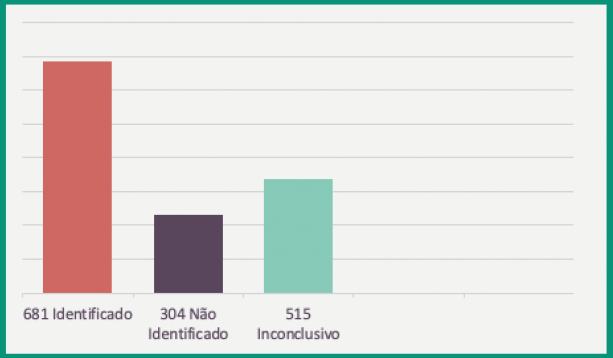
- **Identificado:** representa as empresas que, ao serem pesquisadas, tiveram Bots encontrados e, portanto, possuem supostas credenciais sendo comercializadas através do seu domínio principal;
- **Não identificado:** representa as empresas cujo domínio principal não constou nos resultados de pesquisa na loja;
- **Inconclusivo:** representa as empresas que não tiveram um endereço de web válido identificado pelo Mantis e, por isso, não chegou na etapa de ser pesquisada na loja.

Apesar de simples, o resultado da ferramenta nos trouxe alguns indicadores bem interessantes, como por exemplo:

- Em média, quando identificado o endereço da marca na loja, a média de Logs com credenciais sendo comercializados eram de 41;
- Grande parte do Sistema Operacional identificado nos detalhes das vítimas se tratava de fato de Windows 10 Enterprise;
- 23% dos Logs identificados continha algum tipo de credencial do tipo Remote Desktop ou FileZilla (FTP), tipo de conexão utilizada em ambiente corporativo;
- O valor médio dos logs comercializados é de 16 dólares por vítima.

Como forma de ilustrar o resultado obtido pela ferramenta, incluímos os dados em gráficos:





Finalizamos esse tópico trazendo o nível de risco que essas lojas representam para o mundo da segurança digital, e como comercializar tais credenciais e dados no formato de marketplace em varejo pode impactar diretamente na postura de cibersegurança das organizações.

6. O acesso na prática

6.1. Controles de identidade

Iniciamos explicando conceitos básicos de impressão digital (Device Fingerprint), introduzimos em seguida o mundo dos Stealers para exemplificar como cibercriminosos conseguem as credenciais e os dados básicos de impressão digital, e no último tópico trouxemos etapas da operação no mundo da comercialização.

Mas onde entra a impressão digital?

Há diversos controles de identidade que protegem sistemas contra ataques de Account Takeover (Roubo de Contas), em que não basta o criminoso ter credenciais reais e ativas, ainda assim é possível identificar se o acesso é legítimo. Esses controles têm como base os dados de impressão digital do usuário, e são essenciais para esse processo.

Mas, existe uma técnica que cibercriminosos conseguem contornar controles e entrar em sistemas com proteção robusta na fase de autenticação de usuário.

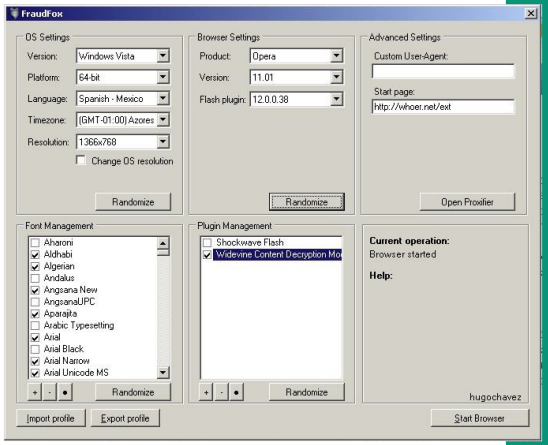
6.2. Fraudfox

Uma das principais técnicas que cibercriminosos utilizam para conseguir acessar sistemas protegidos com controles de identidade é a replicação de impressão digital. A ação consiste em remontar a estrutura de digital da vítima, copiando os dados da impressão para uma máquina virtual que vai simular o computador do usuário. Algumas ferramentas são famosas por automatizarem essa técnica, entre elas o FraudFox (o nome é uma sátira ao Firefox, navegador de internet da Mozilla Foundation).

A informação mais recente é que o FraudFox deixou de ser comercializado pelos desenvolvedores oficiais. Inclusive, uma parte dos cibercriminosos hoje utilizam uma alternativa popular chamada Kameleo. De qualquer forma o FraudFox ainda é o favorito de boa parte da comunidade criminosa, com uma versão "crackeada" que ainda funciona.

O FraudFox é um emulador feito para burlar os sistemas de monitoramento de impressão digital. Na época, era possível contratar mediante uma assinatura mensal no valor de 99 dólares, com direito a suporte por e-mail 24/7.

Ao abrir o FraudFox, o cibercriminoso consegue configurar diversos itens para a geração de uma nova impressão digital, como versão e plataforma do sistema operacional, idioma do sistema, fuso horário, tamanho da tela, versão do browser, tipo de fonte e tamanho. Ele também permite uma seleção randômica de itens.



Na prática, quando cibercriminosos adquirem arquivos no formato de Logs dos Stealers, seja em uma loja de marketplace igual ao Genesis ou até mesmo de uma campanha de distribuição massiva de Trojans aplicada por ele mesmo, muitas vezes sair acessando os sistemas das empresas diretamente não é eficaz e seguro pelos seguintes motivos:

- O acesso suspeito pode gerar "ruído" nas operações de SIEM, plataforma de monitoramento informático da empresa alvo;
- Um acesso inapropriado pode levar ao bloqueio do acesso por completo, e o time de tecnologia pode fazer o bloqueio de todas as credenciais corporativa da vítima;
- O acesso suspeito pode gerar um alerta de notificação para o e-mail da vítima, solicitando que revise seu acesso.

6.3. Eu sou seu vizinho

Você pode estar pensando: “ok, eles conseguem manipular os dados de impressão digital do dispositivo, mas isso não muda o fato de que o endereço IP ainda vai ser muito diferente ou distante do endereço real da vítima que esta habituada em acessar sistemas monitorados e protegidos”.

Sim, hoje em dia qualquer solução de SIEM ou produtos com proteção contra Account Takeover (Roubo de contas) conseguem analisar critérios em volta do endereço IP, em que até a distância de geolocalização entre a última autenticação e a atual, que está tentando ser feita, é analisada.

Para este tipo de desafio, cibercriminosos fazem a contratação de um serviço chamado Proxy Caseiro (Home Proxy), serviços que ofertam endereços IP domésticos, oriundos de máquinas infectadas por trojans.

Empresas que trabalham com produtos de Proxy Caseiro conseguem oferecer para o cliente uma lista de endereços IP que serão lidos como confiáveis. E, nesse caso, o cliente criminoso consegue escolher um IP a seu gosto, filtrando por cidade ou regiões, bairros e até a rua. Assim, o cibercriminoso monta um acesso muito próximo do real, com a geolocalização passando despercebida por operações e regras de monitoramento.

7. Conclusão

É necessário também compreender que hoje a comunidade de cibercriminosos também evolui na mesma velocidade que as tecnologias e soluções de cibersegurança. E a maior das vulnerabilidades é a falsa sensação de segurança. Sim, não devemos renunciar a nossos antivírus e VPN's, mas, quando falamos de uma postura de segurança madura, é imprescindível uma visão maior de risco. E de como se preparar para responder a ele.

Essa preparação passa por inteligência. É a solução que se mostra mais consistente e eficaz no monitoramento e análise das ameaças. É a inteligência, fortalecida por profissionais e tecnologia, que antecipa os passos da cibercriminalidade, que prevê estratégias montadas para atacar organizações, que desenha o cenário real de risco que irá embasar a melhor arquitetura de segurança para os negócios.

Por isso, conte com o time de inteligência do Mantis que, de forma contínua e proativa, acompanha e analisa a evolução dos ataques, para fornecer estratégicas informações para nossos clientes e ajudá-los na desafiadora tarefa de orientar os investimentos em cibersegurança na direção certa.

email@safelabs.com.br
www.safelabs.com.br