New Financial Malware Targets Brazilian Banking Customers

securityintelligence.com/camubot-new-financial-malware-targets-brazilian-banking-customers/

September 4, 2018

Home / Banking & Finance
CamuBot: New Financial Malware Targets Brazilian Banking Customers

Banking & Finance September 4, 2018
By Limor Kessem co-authored by Maor Wiesen 4 min read
Leia o artigo em Português - Read this article in Portuguese

Novo malware, denominado CamuBot, visa clientes corporativos dos bancos brasileiros

Pesquisadores do IBM X-Force analisaram um novo malware que visa os principais bancos brasileiros, por meio de seus clientes corporativos. O malware foi apelidado de CamuBot uma vez que se camufla como um módulo de segurança exigido pelos bancos. O CamuBot surgiu no Brasil em agosto de 2018, no que pareciam ser ataques direcionados a usuários de bancos comerciais. De acordo com as pesquisas do X-Force, os autores deste malware estão visando empresas e organizações do setor público, usando uma combinação de engenharia social e táticas de malware para driblar a autenticação e os controles de segurança. Ao contrário de outros malwares operados no Brasil, o CamuBot foi definido como um novo código. Muito diferente dos típicos Trojans, o CamuBot não se esconde; pelo contrário, é muito visível, usando logotipos dos bancos e a mesma aparência de um internet banking, por exemplo, para se passar por um aplicativo de segurança. Assim, ganha a confiança da vítima e leva-a a instalá-la sem perceber que está executando um assistente de instalação para um cavalo de Tróia. O CamuBot é mais sofisticado do que os típicos malwares de ataque remoto e táticas de fraude usados no Brasil. Em vez de simples telas falsas e uma ferramenta de acesso remoto, as táticas do CamuBot se assemelham àquelas usadas por malwares fabricados na Europa Oriental, como TrickBot, Dridex ou QakBot, todos focados em bancos comerciais e combinando engenharia social com controle de conta / dispositivo auxiliado por malware.

Um Telefonema seguido do Phishing

O método de fraude do CamuBot é uma mistura de elementos projetados para atrair uma vítima para instalar o malware em seu dispositivo e, em seguida, guiá-la inconscientemente, autorizando uma transação fraudulenta. Para efetivar os ataques, os operadores do CamuBot começam com uma pesquisa básica de empresas que façam negócios com uma determinada instituição financeira. Em seguida, ligam para a pessoa que provavelmente teria as credenciais da conta bancária da empresa. Os invasores se identificam como funcionários do banco e instruem a vítima a entrar em um site com o objetivo de verificar se o módulo de segurança está atualizado. Obviamente, a verificação de validade aparece negativa, então os invasores usam este pretexto para que a vítima instale um "novo" módulo de segurança para continuar usando o internet banking. Os usuários que baixam o módulo são aconselhados a fechar todos os programas em execução e a executar a instalação com um perfil de administrador do Windows.

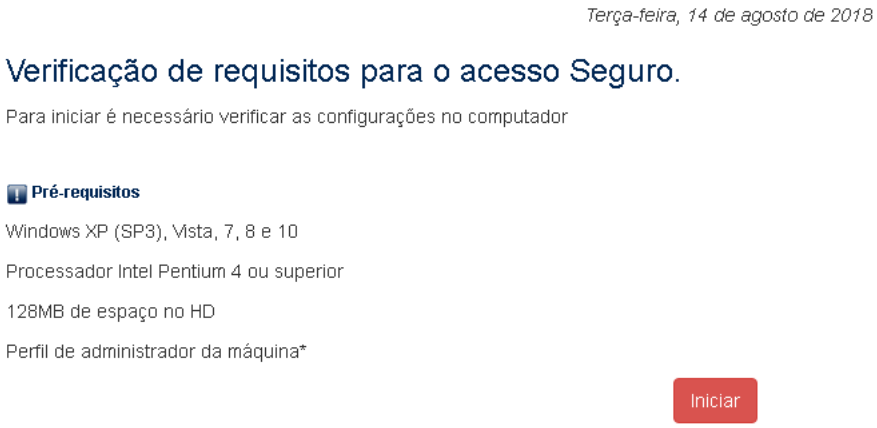

Figura 1: O CamuBot, disfarçado de aplicativo falso, pede requisitos mínimos antes da instalação Neste ponto, um aplicativo falso com os logotipos do banco começa a ser baixado. Por trás da interface, o CamuBot é executado no dispositivo da vítima. O nome do arquivo e a URL a partir da qual é feito o download muda a cada novo ataque.

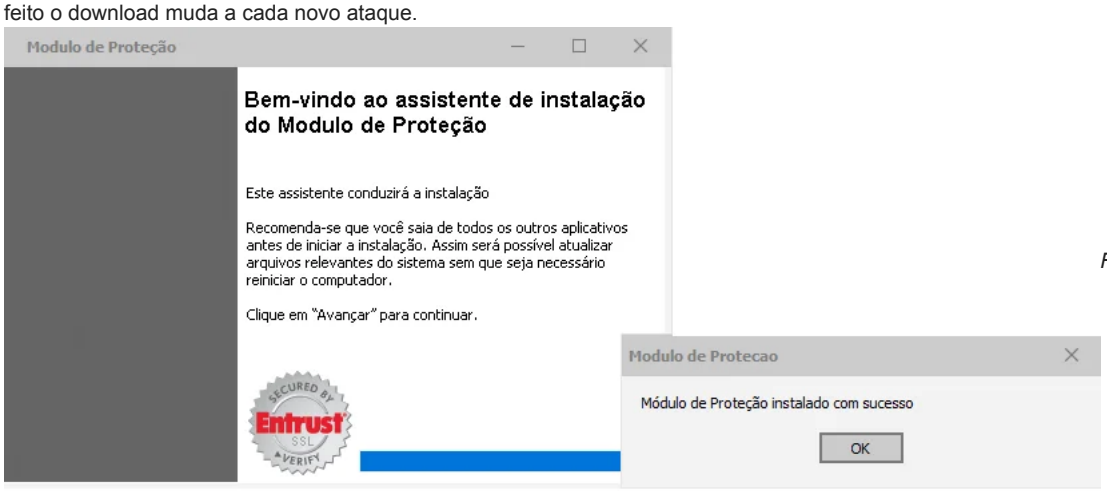

Figura 2: CamuBot, disfarçado como aplicativo falso, completa a instalação Como parte destas simples etapas da instalação, o CamuBot:

1. Grava dois arquivos na pasta {30bfbf8d9f2833f0337133e196b4dc87825dfb7d33a3602d05ee876ecd6f1178}ProgramData{30bfbf8d9f2833f0337133e196b4dc87825dfb7d3 Windows para estabelecer um módulo proxy no dispositivo. O nome do executável não é estático e muda a cada ataque.
2. Adiciona-se às regras do Firewall para parecer confiável. E faz o mesmo com o antivírus:

C:WindowsSystem32netsh.exe" firewall add allowedprogram "" Anti-Virus ENABLE

```
00AA93B6        push        0
00AA93B8        push        0
00AA93BA        push        0AA95BC;'firewall add allowedprogram "'
00AA93BF        lea         edx,[ebp-0C]
00AA93C2        mov         eax,[0B320DC];^Application:TApplication
00AA93C7        mov         eax,dword ptr [eax]
00AA93C9        call        005E7CD0
00AA93CE        push        dword ptr [ebp-0C]
00AA93D1        push        0AA9604;'" Anti-Virus ENABLE'
00AA93D6        lea         eax,[ebp-8]
00AA93D9        mov         edx,3
00AA93DE        call        @UStrCatN
00AA93E3        mov         eax,dword ptr [ebp-8]
00AA93E6        call        @UStrToPWChar
00AA93EB        push        eax
00AA93EC        push        0AA962C
00AA93F1        push        0
```

Figura 3: CamuBot modifica as configurações do Windows Firewall para parecer confiável Para comunicar-se através da máquina infectada , o CamuBot estabelece um proxy SOCKS baseado em SSH. De acordo com a análise da X-Force, a DLL do módulo SSH é uma ferramenta gratuita que foi obtida através do GitHub. A DLL é nomeada: "{30bfbf8d9f2833f0337133e196b4dc87825dfb7d33a3602d05ee876ecd6f1178}TEMP{30bfbf8d9f2833f0337133e196b4dc87825dfb7d33a3602d05e
O módulo proxy é então carregado e estabelece o encaminhamento de porta. Esse recurso geralmente é usado em um túnel bidirecional de portas de aplicativos do dispositivo do cliente para o servidor. No caso do CamuBot, o túnel permite que os invasores direcionem seu próprio tráfego através da máquina infectada e usem o endereço IP da vítima ao acessar a conta bancária comprometida. Uma vez que a instalação é concluída, uma tela pop-up redireciona a vítima para um site de phishing que simula o portal de internet banking. Eles são solicitados a fazer login em sua conta e, assim, inadvertidamente, enviar suas credenciais para o invasor. Nesse momento, se as credenciais forem suficientes para uma invasão de conta, o invasor se desconecta.

O Camubot consegue driblar a autenticação biométrica?

Nos casos em que os operadores do CamuBot invadem um dispositivo de autenticação forte conectado a máquina infectada, o malware pode buscar e instalar um driver para esse dispositivo. A vítima é então solicitada a ativar o compartilhamento remoto. Acreditando que estão falando com um representante do banco, a vítima pode autorizar o acesso, sem saber que, ao compartilhar o acesso ao dispositivo conectado, ele permitirá que o invasor intercepte senhas de uso único geradas para fins de autenticação.

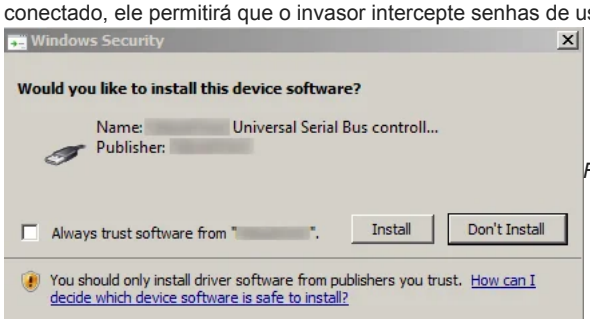

Figura 4: CamuBot solicita à vítima que instale o driver de acesso remoto a um dispositivo USB Com a senha do usuário em mãos , o criminoso pode tentar uma transação fraudulenta, abrindo caminho através de seu endereço IP, para fazer a sessão parecer legítima pelo lado do banco. Os pesquisadores do X-Force reforçam que uma possibilidade preocupante foi de que o driver de dispositivo implantado pelo CamuBot fosse similar a outros dispositivos fornecidos pelo mesmo fornecedor, alguns dos quais são usados para autenticação biométrica. Se o mesmo compartilhamento remoto for autorizado por um usuário, eles podem, sem saber, comprometer sua autenticação biométrica.

Distribuição

A distribuição do CamuBot é personalizada. Como os operadores de malware têm como alvo empresas no Brasil, é possível que eles coletem informações a partir de listas de telefones locais, mecanismos de pesquisa, ou redes sociais. Todo eso para chegar a pessoas que possuem uma empresa, ou que tenham as credenciais da conta bancária da empresa.

Alvos

Atualmente, o CamuBot tem como alvo os correntistas de empresas no Brasil. Os pesquisadores do X-Force não visualizaram o CamuBot sendo usado em outros países, porém isso pode mudar com o tempo. Mantenha-se atualizado sobre o CamuBot no X-Force Exchange.

Algumas amostras de Camubot que investigamos:

- 9eab7ea297ea71057691c09b485d646f
- a000fe90363517e0fc4c8d02f7830825
- 684AAA16C9B54E4645C8B5778DB7562F
- CD27C9FC659B50776E3BD208A42F1E3F
- 7D50411C9621F1AD00996C8CE0F1AC20

Close Translation

IBM X-Force researchers analyzed new financial malware that targets major Brazilian banks through their business banking customers. The malware was dubbed CamuBot because it attempts to camouflage itself as a security module required by the banks it targets.

CamuBot emerged in Brazil in August 2018 in what appeared to be targeted attacks against business banking users. According to X-Force's findings, the malware's operators are actively using it to target companies and public sector organizations, mixing social engineering and malware tactics to bypass strong authentication and security controls.

A Brazilian Standout

Unlike other malware operated in Brazil, CamuBot is a defined new code. Very different from typical banking Trojans, CamuBot does not hide its deployment. On the contrary, it is very visible, using bank logos and overall brand imaging to appear like a security application. It thus gains victims' trust and leads them to install it without realizing they are running an installation wizard for a Trojan horse.

CamuBot is more sophisticated than the remote-overlay type malware commonly used in fraud schemes targeting users in Brazil. Instead of simplistic fake screens and a remote access tool, CamuBot tactics resemble those used by Eastern European-made malware such as TrickBot, Dridex and QakBot, each of which focuses on business banking and blends social engineering with malware-assisted account and device takeover.

Read the white paper: How Digital banking Is Transforming Fraud Detection

Hello, It's a Phish Calling

CamuBot's fraud method is a mix of elements that are designed to lure potential victims into installing the malware on their device and then walk them through unknowingly authorizing a fraudulent transaction.

To carry out their attacks, CamuBot operators begin with some basic reconnaissance to find businesses that bank with a certain financial institution. They then initiate a phone call to the person who would likely have the business's bank account credentials.

The attackers identify themselves as bank employees and instruct the victim to browse to a certain URL to check whether his or her security module is up to date. Of course, the validity check comes up negative, and the attackers trick the victim to install a "new" security module for his or her online banking activity.

Those lured into downloading the module are advised to close all running programs and run the installation with a Windows administrator profile.

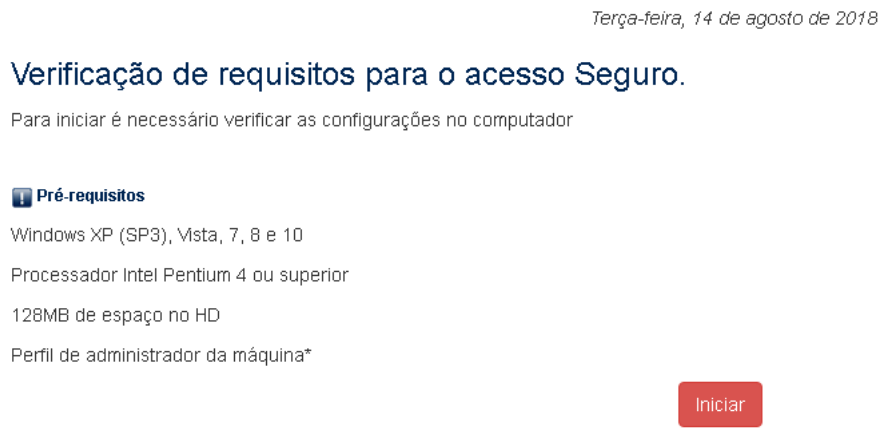

Figure 1: CamuBot, disguised as fake app, asks for minimum requirements before installation

At this point, a fake application that features the bank's logos starts downloading. Behind the scenes, CamuBot is fetched and executed on the victim's device. The name of the file and the URL from which it is downloaded change in every attack.

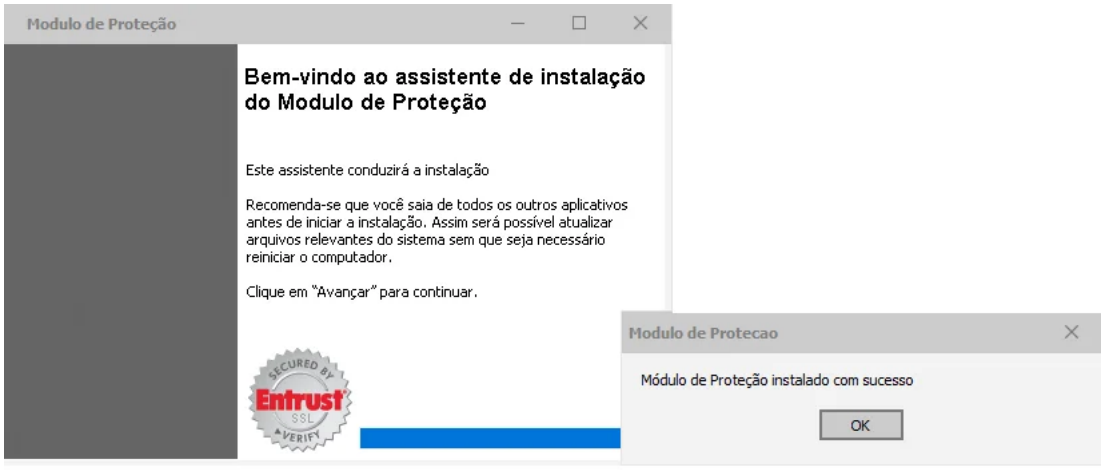

Figure 2: CamuBot, disguised as fake app, completes installation

As part of its simplistic infection routine, CamuBot writes two files to the %ProgramData% Windows folder to establish a proxy module on the device. The executable's name is not static and changes in every attack. Then it adds itself to the firewall's rules to appear trusted. It does the same for the antivirus:

C:\Windows\System32\netsh.exe" firewall add allowedprogram "<malware_dropper_directory>" Anti-Virus ENABLE

```
00AA93B6        push        0
00AA93B8        push        0
00AA93BA        push        0AA95BC;'firewall add allowedprogram "'
00AA93BF        lea         edx,[ebp-0C]
00AA93C2        mov         eax,[0B320DC];^Application:TApplication
00AA93C7        mov         eax,dword ptr [eax]
00AA93C9        call        005E7CD0
00AA93CE        push        dword ptr [ebp-0C]
00AA93D1        push        0AA9604;'" Anti-Virus ENABLE'
00AA93D6        lea         eax,[ebp-8]
00AA93D9        mov         edx,3
00AA93DE        call        @UStrCatN
00AA93E3        mov         eax,dword ptr [ebp-8]
00AA93E6        call        @UStrToPWChar
00AA93EB        push        eax
00AA93EC        push        0AA962C
00AA93F1        push        0
```

Figure 3: CamuBot edits Windows Firewall settings to appears trusted

To communicate with the infected device, CamuBot establishes a Secure Shell (SSH)-based SOCKS proxy. According to X-Force's analysis, the SSH module's dynamic link library (DLL) is a free tool that was obtained via GitHub. The DLL file is named "%TEMP%\Renci.SshNet.dll."

The proxy module is loaded and establishes port forwarding. This feature is generally used in a two-way tunneling of application ports from the client's device to the server. In CamuBot's case, the tunnel allows attackers to direct their own traffic through the infected machine and use the victim's IP address when accessing the compromised bank account.

After installation completes, a pop-up screen redirects the victim to a phishing site purporting to be their bank's online banking portal. The victim is asked to log into his or her account, thereby unknowingly sending the credentials to the attacker.

At this point, if the credentials are sufficient for an account takeover, the attacker hangs up.

Can CamuBot Beat Biometric Authentication?

In cases where CamuBot's operators run into a strong authentication device that's attached to the endpoint, the malware can fetch and install a driver for that device. The victim is then asked to enable sharing it remotely. Trusting that they are speaking to a bank representative, the victim may authorize the access, not knowing that by sharing access to the connected device, they can allow the attacker to intercept one-time passwords generated for authentication purposes.

Figure 4: CamuBot fetches and installs a driver for a connected device used in strong authentication

With the one-time code in hand, the criminals can attempt a fraudulent transaction, tunneling it through their IP address to make the session seem legitimate on the bank's side.

According to X-Force researchers, a more concerning possibility was that the device driver deployed by CamuBot was similar to other devices supplied by the same vendor, some of which are used for biometric authentication. If the same remote sharing is authorized by a duped user, he or she could unknowingly compromise the biometric authentication process.

Distribution and Targets

The delivery of CamuBot is personalized. Since the malware's operators target businesses in Brazil, it is very possible that they gather information from local phone books, search engines or professional social networks to get to people who own a business or would have the business's bank account credentials.

At this time, CamuBot targets business account holders in Brazil. X-Force researchers have not seen CamuBot used in other geographies, but that may change over time. Keep up to date on CamuBot on X-Force Exchange.

Some CamuBot Samples Observed

- 9eab7ea297ea71057691c09b485d646f
- a000fe90363517e0fc4c8d02f7830825
- 684AAA16C9B54E4645C8B5778DB7562F
- CD27C9FC659B50776E3BD208A42F1E3F
- 7D50411C9621F1AD00996C8CE0F1AC20

Read the white paper: How Digital banking Is Transforming Fraud Detection

Limor Kessem
Executive Security Advisor, IBM

Limor Kessem is an Executive Security Advisor at IBM Security. She is a widely sought-after security expert, speaker and author and a strong advocate for wom...