BOLETIM DE SEGURANÇA

Trojan bancário Coyote visando instituições financeiras na América Latina, com foco no Brasil

heimdall
security research
A DIVISION OF ISH

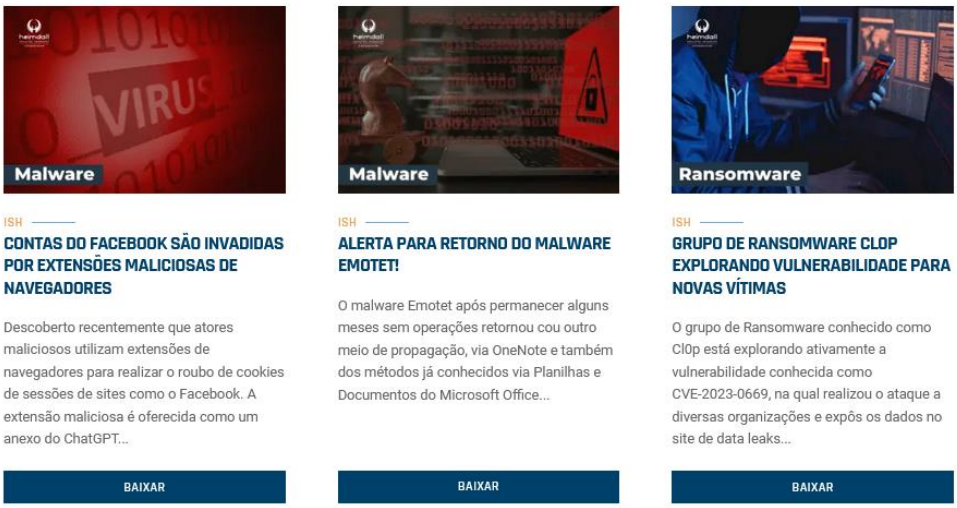
TLP: CLEAR

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso **X**.

[Heimdall Security Research]

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

[Boletins de Segurança – Heimdall]



SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

O crescimento do comércio mundial e a expansão do mercado na América Latina (LATAM) têm transformado a região em um alvo cada vez mais atrativo para criminosos cibernéticos nos últimos anos. O Trojan bancário chamado Coyote, desenvolvido em .NET, tem como principal alvo instituições financeiras brasileiras, especialmente bancos. Ele normalmente se espalha através de e-mails de phishing, sites comprometidos ou downloads maliciosos disfarçados de software legítimo.

2 VETOR DE ATAQUE OBSERVADO

Este malware é distribuído principalmente através de campanhas de phishing e e-mails maliciosos, onde os usuários são enganados a baixar e executar arquivos infectados. Uma vez instalado no sistema da vítima, o Coyote tem a capacidade de capturar credenciais bancárias, registrar pressionamentos de teclas e interceptar dados sensíveis. Ele também utiliza técnicas de evasão para evitar detecção por softwares antivírus e análises de segurança. Além disso, o Coyote pode se atualizar automaticamente, baixando novas funcionalidades e correções de bugs. O Coyote pode executar um total de 24 comandos e funções, incluindo tirar capturas de tela da atividade de um usuário, mostrar janelas de sobreposição em tela cheia (incluindo uma sobreposição de um aplicativo bancário falso), fazer alterações no registro, mover o mouse do usuário, desligar a máquina e registrar teclas.

```
if (tnjtyggq[0].Length == 31)
{
    try
    {
        if (tnjtyggq[1] == Program.dtgmwiuxtypja(132))
        {
            Program.bzbsbdclzomzay = true;
            Program.wyimrnrcvvkjbu = new Thread(delegate()
            {
                try
                {
                    while (Program.bzbsbdclzomzay)
                    {
                        for (int k = 0; k < 256; k++)
                        {
                            if (Program.GetAsyncKeyState(k) == -32767)
                            {
                                Keys keys = (Keys)k;
                                try
                                {
                                    Program.mvfptxhvrmzomc += keys.ToString();
                                }
                                catch (Exception)
                                {
                                }
                            }
                        }
                    }
                }
                catch (Exception)
                {
                }
            });
            Program.wyimrnrcvvkjbu.Start();
```

Figura 1 – Comando do keylogger Coyote..

O Coyote usa a biblioteca WatsonTCP para comunicação com C2s.

Figura 2 – Conexões do Coyote com diferentes servidores C2..

3 ALVOS DO MALWARE

O Trojan bancário Coyote possui um extensa lista de instituições financeiras brasileiras, bem como a Binance, uma empresa global que opera uma exchange de criptomoedas com o maior volume diário de negociação de criptomoedas.

- Bancobrasil.com.br
- Bb.com.br
- internetbanking.caixa.gov.br
- loginx.caixa.gov.br
- banco.bradesco
- cidadetran.bradesco
- ne12.bradesconetempresa.b.br
- binance.com
- mercadobitcoin.com.br
- bitcointrade.com.br
- foxbit.com.br
- blockchain.com
- accounts.binance.com
- pf.santandernet.com.br
- pj.santandernetibe.com.br
- itau.com.br
- meu.original.com.br
- empresas.origina
- ibpj.original.com.br
- banrisul.com.br
- internetbanking.banpara.b.br
- ib.banpara.b.br
- www2s.bancoamazonia.com.br
- ecode.daycoval.com.br

- mercantildobrasi
- stone.com.br
- bancopan.com.br
- unicred.com.br
- safra.com.br
- safraempresas.com.br
- ib.brde.com.br
- banese.com.br
- bancobmg.com.br
- brbbanknet.brb.com.br
- internetbanking.confesol.com.br
- tribanco.com.br
- credisisbank.com.br
- credisan.com.br
- bancobs2.com.br
- bancofibra.com.br
- uniprimebr.com.br
- uniprime.com.br
- bancotopazio.com.br
- btgmais.com
- citidirect.com
- banestes.b.br
- zeitbank.com.br
- cora.com.br
- sofisa.com.br
- sofisadireto.com.br
- www.banestes.com.br
- banestes.com.br
- wwws.uniprimedobrasil.com.br
- www.rendimento.com.br
- rendimento.com.br
- contaonline.viacredi.coop.br
- sicredi.com.br
- nel.bnb.gov.br
- mercadopago.com.br

4 MITRE ATT&CK - TTPs

Tática	Técnica	Detalhes
Execution	T1059.007 Command and Scripting Interpreter: JavaScript T1204.002 User Execution: Malicious File	Após a execução do Squirrel, um aplicativo NodeJS é executado e executa código JavaScript ofuscado. O carregador inicial é disfarçado como um atualizador Squirrel.
Persistence	T1547.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	O valor do registro é adicionado à chave HKCU\Environment\UserInitMprLogonScript (antes de verificar sua existência). O valor adicionado no caso que observamos: “obs-browser-page.exe” é para estabelecer persistência.
Privilege Escalation	T1574.002 Hijack Execution Flow: DLL Side-Loading	O Trojan é carregado por meio do carregamento lateral de DLL de uma dependência dos executáveis do Chrome e do OBS Studio (libcef.dll).
Defense Evasion	T1218 System Binary Proxy Execution T1027 Obfuscated Files or Information T1620 Reflective Code Loading T11036.001 Masquerading: Match Legitimate Name or Location T1553.002 Code Signing T1480.001 Execution Guardrails	Uso do Squirrel para criar pacotes de instalação e atualizações que ocultam o vetor de infecção em um atualizador. Trojan utiliza ofuscação de string com criptografia AES. O aplicativo NodeJS executa e executa código JavaScript ofuscado. O NIM é usado para carregar o estágio final, que descompacta o executável .NET e o executa na memória usando o CLR. O Coyote oculta seu carregador inicial apresentando-o como um empacotador de atualização. Uso de aplicativo assinado com biblioteca legítima. Depois que o malware verifica que a conexão é realmente com o invasor, ele envia as informações coletadas da máquina infectada e dos aplicativos bancários para o servidor.
Discovery	T1082 System Information Discovery T1010 Application Windows Discovery	O C2 coleta informaçãoes da máquina. O Trojan monitora todos os aplicativos abertos no sistema da vítima e aguarda o acesso ao aplicativo ou site bancário específico.
Collection	T1056.001 Input Capture: Keylogging T1113 Screen Capture	O Trojan tem a capacidade de realizar keylogging, tem a capacidade de fazer capturas de tela.
Command and Control	T1573 Encrypted Channel T1205 Traffic Signaling	O invasor envia um pacote de resposta que contém ações específicas. Para processar essas ações, o invasor transmite uma string com um delimitador aleatório. Cada

		posição da string é então convertida em uma lista, com a primeira entrada representando o tipo de comando.
Impact	T1529 System Shutdown/Reboot	O Trojan tem capacidade de desligar o sistema comprometido.

Tabela 1 – Tabela MITRE ATT&CK.

5 RECOMENDAÇÕES

Além dos indicadores de comprometimento elencados abaixo pela ISH, poderão ser adotadas medidas visando a mitigação da infecção do referido *malware*, como por exemplo:

Educação e treinamento de funcionários

- **Treinamento de conscientização**: Proporcione treinamento regular para funcionários sobre como reconhecer e evitar e-mails de phishing e outros métodos comuns de engenharia social.
- **Política de negação**: Implementar políticas que restrinjam o acesso a recursos da web apenas a sites legítimos, especialmente para perfis de usuários críticos, como aqueles no departamento financeiro.

Uso de ferramentas e tecnologias de segurança

- Soluções de segurança confiáveis: Utilize soluções de segurança abrangentes que ofereçam proteção contra uma ampla gama de ameaças cibernéticas financeiras, incluindo antivírus e anti-malware atualizados.
- Sistemas de Detecção e Resposta a Endpoints (EDR): Implemente sistemas de EDR para monitorar e responder a atividades suspeitas em tempo real.
- Autenticação multifatorial (MFA): Adote MFA para sistemas internos e aplicações bancárias para adicionar uma camada extra de segurança.

Manutenção e atualizações regulares

- Atualizações de software: Certifique-se de que todos os sistemas operacionais, aplicativos e softwares de segurança estejam sempre atualizados com os últimos patches e correções.
- Segmentação de redes: Segmente a rede para limitar o acesso a dados críticos apenas aos usuários que realmente precisam dessas informações.

Monitoramento e análise contínua

- Análise comportamental: Use ferramentas de análise comportamental para identificar e responder rapidamente a atividades anormais que possam indicar a presença de malware.
- Comunicação segura: Monitore e analise a comunicação de rede para identificar e bloquear comunicações suspeitas com servidores de comando e controle (C2) usados por malware como o Coyote.

6 INDICADORES DE COMPROMISSOS

A ISH Tecnologia realiza o tratamento de diversos indicadores de compromissos coletados por meio de fontes abertas, fechadas e também de análises realizadas pela equipe de segurança Heimdall. Diante disto, abaixo listamos todos os Indicadores de Compromissos (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

Indicadores de URL, IPs e Domínios

Indicadores de Hashes e Domínios	
Hash	096d7765f278bb0de33fbfa0a15413a2432060d09c99f15c6ca900a6a8a46365 9c6fc9e0854eaf5a0720caab1646f48c7992f6f4051438004598af89102a49eb e0b65087cc83b899d53c153fcfd1420d15e369c3d196325396b50cb75681c27d 485c8bfae3e5c150012e1d630f5d9ae37b786d4b750a9a0adf2b174b7ab85c65 16cc13258a3e63be247c9adf18def0369bb72197bdb3668142bc50a6656047af 2bd6bbe48d0328e4011ce3053e616664a4eb2bf43bd5762cb03be297f786b068 287b39f40ed541585c968b6529c44e9ccdd899bca0b88457907d994c2b5013f4 341a1945f606bcf4c25bce9b850dbddc5125376156cb7f8d14c6ce6bc4b396c3 9160ca25889427b2c2da4d4b14c4a93a707efc2ce07a49d5b8ab1a7f9be8ab55 2d8b10e35c2c2d9675ec693558629450eeee2c8e38f491d38c42de96bddf317a 112edf53d4c560ab71f1b20856ec4d6096e0ea42b0271526b3415c3563300f06 3cbc282c6a51edff4e762267332e1ff2a503f7ba8a7b2a10c9ff404a7bda913b aedffb9cf780bb52c68586ceb238fcaf90253524f06a4a338edc6437409e51c5 2b428df6f76d36ceeebfd37df65ab7893cb6f526afeb9e4494829628f0b9cae8 ae6676ad5b8ba386e88ae045eacc05225a657360963844cdf18db6a45318ea89 ce07ef596772e9cfa6f41000f27244f6f750527639a26c6be0b73033a8e41883 c0833babb2982e36ac7646f7539f6a235a42bcf5375bc080d3ac9d031dc3b903 d44f4db6680d178437e9cfba010ac049f80e5eddf43b3977da819119bb6ca06d 504a5902f20d0a7e3968251849cd88acd31e7fc895fc18d5c82076c5388df5bd 8e614368f99f955c75752df597f97de1dd51b4f0dfeeadc76e1badcc7ca57fc2 3cc58b46d0babd561508d7b67c609e0e9be9a35db9425f1e8a29512a5229665a 5656501522adfe1b08f58cccc1e187cbb7099ef1193a62edd5dfe0d32da4cd7a fb8353e718397dcabd11d9bd8a500ffd54e2a57ac4722a34241757c60ba2bdff ae65738fa81be0b2cfe2f63209db9ed5b928b4b5a1a703ce2a89699a6f192f07 5b3421beb6aaf3fd16831e1456475acac4f8e7c863869fb4d5dc9b1ae0576ef3 6b7a014d0674fe5f145aa2c5dc7674d42e5306d82c3fe7ab0235dcbfd559725f d96c3e8dc899948bf92c377bb4872b19b5983b6eb2d59f00019345293601843c 2a54b7f1327398ccd1c538759201e8699dfad7c53e8e095ea782d862ec48cb92 90ffb18c9d05bf6a61d90c57f299b70702c0e65dac90349b06d5e6833d6d2612 4869fcfda9be32f3cdd48c21bda07aefde496c5f06f235f33ce948169e9744e5 3edcf6a6b6cb254f72f0f2607fa4bb2ecb604475b448c9487e89fc76eb8f896e a0d2c87f4ed6522fdcd8c8d234dca9c7e8831de5faa9445275405ddd0a9104cc 6da5f450f3124e30e8091fda443cb416d29eab4e166a777263e004758acf2e69 10af5c8950b8802851afe96b423d20408b618f80ab54c1a5aef0f1a04c36f331 f6ed73bed9e6b992dbfdee64ff8c9dfde5e3f12c3ec6bbb4e2367fbd2ce75b6f 1ba49976a6e596abb68e2f7ca37407930330a4bf0bd25207057c5a60cb3a4107 798fb8de9bb0434ee0b172793f5b68eb593054538cf5ec96e71a5a0759f6bcc5 c057145da9481a4fff50e69b7e746c19cc95e2d33331539b6b62077169bc4b42 fcb8f32502147dbf8ef44ad99a41d9eaf639bb3d22c4de92a3022f501c9d8cb6 0dea05062d6527ab03f80de87488d278dd333167cdabdf5ef28da760bf252863 3a14ab878697453832306a836e67915d7475481307c65268ceb1f900ff4ec25a eb615c093e9b52ed409f426764857e6e42aa85e02adef59d6f1457dcbb90bb40

	1bed3755276abd9b54db13882fcf29c543ebf604be3b7fcf060cbd6d68bcd23f 4806617bbc8187a89d5ed73cb818853e306d3699f87bd09940b0ecffdc96091d 1d59bc782e532780da0364b14a1b474a8cb8a5af50c8124159bf5d943bd050f7
Domínio	cloridatosys[.]com flogoral[.]com formitamina[.]com bilatex[.]com autoglobalcar[.]com atendesolucao[.]com angelcallcenter[.]com servicoasso[.]com dowfinanceiro[.]com centralsolucao[.]com gargamellojas[.]com carrodenatal[.]com marvelnatal[.]com nograusistema[.]com navegacaodura[.]com jogodequadra[.]com carrosantigo[.]com bermatechcliente[.]com

Tabela 2 – Indicadores de Compromissos de Rede.

Obs: Os *links* e endereços IP elencados acima podem estar ativos; cuidado ao realizar a manipulação dos referidos IoCs, evite realizar o clique e se tornar vítima do conteúdo malicioso hospedado no IoC.

7 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Blackberry**

8 AUTORES

- **Ismael Pereira Rocha**

heimdall
security research
A DIVISION OF ISH