# Análise da Ferramenta RITA (Real Intelligence Threat Analytics) na Detecção de APTs: Um Mapeamento aos Controles do PPSI 2.0

Plínio Andrade Passos[1], Éder Souza Gualberto[2]

[1]Banco Central do Brasil — Brasília-DF, Brasil [2]Universidade de Brasília (UnB) — Brasília-DF, Brasil

[1]*plinio.passos@bcb.gov.br*, [2]*eder.gualberto@redes.unb.br*

**Resumo.** *Este artigo investiga as capacidades da ferramenta de código aberto RITA (Real Intelligence Threat Analytics) para detecção de comunicação de Comando e Controle (C2) associada a Ameaças Persistentes Avançadas (APTs), e propõe um mapeamento sistemático de suas evidências aos controles do Programa de Privacidade e Segurança da Informação (PPSI) 2.0, utilizando o MITRE ATT&CK como camada intermediária de interpretação. O estudo foi conduzido em ambiente virtualizado sobre tráfego real de uma infecção por Win32/Koi Stealer. Os resultados demonstram que o RITA detectou comunicação C2 ativa com score de beaconing de 96.90%, classificado como Critical, sem conhecimento prévio de assinatura, sustentando empiricamente o subcontrole 13.3 do Controle 13 (Monitoramento e Defesa de Rede) do PPSI 2.0. O subcontrole 13.6 pode ser atendido de forma integrada pelo pipeline Zeek + RITA. Discutem-se ainda as implicações operacionais para equipes de SOC e CTIR de órgãos do SISP e as limitações técnicas da ferramenta.*

**Palavras-chave:** RITA; APT; Comando e Controle (C2); PPSI 2.0; MITRE ATT&CK; Detecção de ameaças.

## 1. Introdução

Ameaças Persistentes Avançadas (APTs — *Advanced Persistent Threats*) constituem uma categoria de ataque cibernético caracterizada pela combinação de sofisticação técnica, direcionamento a alvos específicos e persistência prolongada dentro do ambiente comprometido. Diferentemente de ataques baseados em malware genérico, as APTs envolvem atores com recursos significativos, frequentemente associados a grupos patrocinados por Estados ou organizações criminosas estruturadas, que planejam e executam campanhas de múltiplas etapas, podendo permanecer não detectados por meses [Al Lelah et al. 2023]. Um aspecto fundamental desse tipo de ameaça é a dependência de canais de Comando e Controle (C2), que permitem ao atacante manter comunicação contínua com os sistemas comprometidos.

Esses canais são essenciais para que o invasor monitore e controle o ambiente, e ao mesmo tempo representam o ponto mais favorável para que o defensor identifique a atividade maliciosa [Comprehensive Survey 2024].

O panorama de ameaças cibernéticas atual evidencia a relevância crescente desse problema. O relatório anual *Data Breach Investigations Report* (DBIR) da Verizon, em sua edição de 2024, analisou mais de dez mil violações confirmadas e constatou que o elemento humano esteve presente em 68% delas, com o *phishing* permanecendo como vetor relevante de obtenção de credenciais e ponto de entrada típico para campanhas subsequentes de instalação de malware e estabelecimento de C2. No âmbito europeu, o relatório *ENISA Threat Landscape* 2024, da Agência da União Europeia para a Cibersegurança, documentou a intensificação de técnicas de evasão por meio do abuso de serviços legítimos em nuvem, uma prática denominada *Living Off Trusted Sites* (LOTS) , na qual o tráfego de Comando e Controle é deliberadamente camuflado em plataformas como Slack e Telegram para se confundir com tráfego corporativo normal [ENISA 2024]. O mesmo relatório, em sua edição setorial voltada à administração pública, identificou grupos de ameaça persistente como APT28 e APT29 como atores recorrentes contra órgãos governamentais europeus, frequentemente utilizando técnicas de *spearphishing* para implantação de *backdoors* [ENISA 2025].

No Brasil, o reconhecimento institucional dessa ameaça tem se traduzido em política pública. O Programa de Privacidade e Segurança da Informação (PPSI), inicialmente lançado em 2023 e revisado em sua versão 2.0, em 2025, orienta os órgãos do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) quanto à implantação de práticas de segurança alinhadas a *frameworks* internacionais consolidados [MGI 2024]. A reformulação recente do programa, formalizada pela Portaria SGD/MGI nº 9.511, reposiciona o PPSI como uma política de governança e resiliência digital de Estado, ampliando o envolvimento da alta administração dos órgãos na gestão de riscos cibernéticos.

Esse movimento institucional dialoga diretamente com o conceito de soberania digital, definido na literatura como a capacidade de uma nação controlar sua própria infraestrutura digital, seus dados e suas tecnologias, de forma independente de influência ou controle externo [Katsikas 2025]. Katsikas argumenta que a cibersegurança constitui um dos pilares centrais dessa capacidade, na medida em que ameaças cibernéticas comprometem diretamente sua autoridade sobre a própria infraestrutura, sendo o fortalecimento da resiliência de setores, processos e dados críticos um requisito central para sustentar a soberania digital na prática

[Katsikas 2025]. Sob essa ótica, a capacidade de monitoramento e detecção de incidentes em órgãos federais brasileiros deixa de ser uma questão estritamente técnica e operacional, e passa a integrar a noção mais ampla de capacidade estatal de proteger seus próprios ativos de informação frente a atores adversos. É esse vínculo com a soberania digital que confere às ferramentas de detecção de APT, no contexto de órgãos do SISP, relevância estratégica, e não meramente tática.

Entre os controles tecnicamente mais relevantes do PPSI 2.0 para essa finalidade está o Controle 13 (Monitoramento e Defesa de Rede), que demanda capacidade de análise comportamental de tráfego de rede para identificação de atividade maliciosa, exatamente o domínio de atuação de ferramentas de código aberto voltadas à detecção de comportamento anômalo em rede. Esse ponto evidencia uma lacuna de pesquisa relevante para o setor público brasileiro: órgãos do SISP frequentemente operam sob restrições orçamentárias significativas, o que limita a aquisição de soluções comerciais de NDR, ao mesmo tempo em que a necessidade de detectar comportamentos sofisticados de C2 associados a APTs é crescente e documentada pelos relatórios internacionais citados. Ferramentas de detecção comportamental de código aberto, como o RITA, surgem como uma alternativa que ajuda a equilibrar a limitação de recursos com a necessidade de segurança, pois oferecem capacidade de análise estatística de tráfego sem custo de licenciamento e sem depender de assinaturas proprietárias que exigem atualização constante.

Nesse sentido, este trabalho tem por objetivo avaliar a capacidade do RITA na detecção de comportamentos associados a APTs, com foco na comunicação C2, e correlacionar seus achados com os controles do PPSI 2.0, utilizando como evidência empírica tráfego malicioso real processado em ambiente de laboratório controlado.

O artigo está organizado da seguinte forma: a Seção 2 apresenta a fundamentação teórica sobre o ciclo de vida das APTs, as técnicas de comunicação C2 e os *frameworks* de segurança correlatos; a Seção 3 descreve a ferramenta RITA e seus módulos; a Seção 4 detalha a metodologia experimental, o protocolo de mapeamento e os resultados obtidos, incluindo evidências práticas e implicações operacionais; e a Seção 5 conclui o trabalho e aponta direções futuras.

## 2. Fundamentação Teórica

### *2.1. Ciclo de Vida das APTs*

O NIST define formalmente a Ameaça Persistente Avançada como um adversário com elevado nível de especialização e recursos significativos, capaz de combinar múltiplos vetores de ataque para se estabelecer e expandir na infraestrutura de TI da organização-alvo. Seu objetivo é manter presença prolongada para exfiltrar informações de forma contínua ou comprometer ativos críticos, perseguindo seus fins de modo reiterado e adaptando-se às defesas ao longo do tempo [Comprehensive Survey 2024]. Uma revisão sistemática da literatura publicada no Journal of Cybersecurity (Oxford Academic), fundamentada nas diretrizes PRISMA e analisando 45 estudos entre academia e indústria, reforça essa definição ao caracterizar as APTs por sua natureza multi-estágio, na qual técnicas, táticas e procedimentos (TTPs) se sobrepõem entre fases e nem sempre seguem uma ordem rígida e previsível [Oxford SLR APT 2024].

A literatura propõe diferentes modelos para descrever o ciclo de vida das APTs, com variações de granularidade entre autores. O modelo de Cyber Kill Chain, originalmente proposto pela Lockheed Martin, descreve a progressão do ataque em sete etapas: reconhecimento, armamento (weaponization), entrega, exploração, instalação, comando e controle e ações sobre os objetivos [Exabeam 2025]. Um levantamento abrangente sobre técnicas de detecção de APT propõe um modelo mais sintético, de cinco etapas: reconhecimento, comprometimento inicial, estabelecimento de C2, movimentação lateral e exfiltração de dados e ação sobre os objetivos. Nesse modelo, o estabelecimento de C2 representa o ponto de maior oportunidade de detecção, dado que o atacante precisa necessariamente gerar tráfego de rede observável para manter comunicação com os sistemas comprometidos [Comprehensive Survey 2024]. Outros trabalhos, como o modelo de sete fases aplicado à análise do incidente SolarWinds/SUNBURST, acrescentam etapas intermediárias como estabelecimento de persistência e reconhecimento interno, evidenciando que a comunicação com a infraestrutura do atacante ocorre de forma recorrente ao longo de múltiplas fases, não apenas em um momento isolado [ANUBIS 2021].

Este trabalho adota como referência o modelo de cinco etapas do levantamento de 2024, concentrando-se na Etapa 3 (estabelecimento de C2), por ser o estágio de maior aderência funcional aos módulos de detecção comportamental do RITA, conforme detalhado na Seção 3.

### *2.2. Comunicação de Comando e Controle (C2)*

O canal C2 é o mecanismo por meio do qual o atacante mantém comunicação bidirecional com os hosts comprometidos, enviando comandos e recebendo dados exfiltrados. A natureza dessa comunicação exige técnicas de detecção comportamentais, em contraposição a abordagens tradicionais baseadas em assinaturas. Na prática, os agentes maliciosos empregam diferentes técnicas para estabelecer e manter esses canais de forma encoberta, sendo as mais documentadas na literatura o *beaconing*, o tunelamento DNS e o abuso de serviços legítimos em nuvem, cada uma explorando características distintas do tráfego de rede para evadir a detecção.

***Beaconing.*** O *beaconing* consiste no contato periódico e regular de um host comprometido com seu servidor C2, geralmente em intervalos fixos ou aleatórios (*jitter*) para dificultar a detecção. Mahboubi et al., em estudo publicado no *Journal of Network and Computer Applications*, distinguem o *beaconing* **determinístico** (usado por malware que precisa manter conexão estável, como ransomware aguardando instruções de pagamento) do *beaconing* **estocástico**, no qual a variação proposital dos intervalos visa evadir ferramentas de detecção baseadas em periodicidade fixa [Mahboubi et al. 2025]. Esse mesmo trabalho avalia explicitamente o RITA como ferramenta de referência para detecção de *beaconing*, utilizando dados de tráfego de rede derivados de capturas do repositório malware-traffic-analysis.net, o que reforça a adequação metodológica da escolha de dataset deste estudo (detalhada na Seção 4.1). Além disso, estudos voltados a ambientes de infraestrutura crítica, como o de detecção de *beaconing* em redes SCADA via metadados Zeek e Isolation Forest, reforçam que a análise estatística de periodicidade de conexões, sem necessidade de inspeção de payload, permanece eficaz mesmo sob tráfego criptografado, por depender apenas de metadados de conexão [*Beaconing* SCADA 2025].

**Tunelamento DNS.** O tunelamento DNS explora a confiança depositada no protocolo DNS para encapsular dados de exfiltração ou comandos C2 dentro de consultas e respostas DNS aparentemente legítimas. Pesquisas recentes destacam que essa técnica tem sido adotada por famílias de malware diversas e por campanhas de APT documentadas, como APT32 e APT34, que utilizam o DNS tanto para troca de mensagens de C2 quanto para exfiltração de dados sensíveis [DNS-HyXNet 2025]. A detecção tradicionalmente se apoia em duas estratégias complementares: análise de payload, que inspeciona características de uma consulta DNS isolada (como comprimento excessivo de subdomínios e alta entropia de caracteres,

indicativa de dados codificados ) e análise de tráfego, que examina volume e frequência de requisições ao longo do tempo [GIAC DNS Tunneling].

**Abuso de Serviços Legítimos em Nuvem.** Uma tendência consolidada na literatura recente é o uso de serviços de nuvem públicos e legítimos (exemplo Dropbox, OneDrive, Slack, Pastebin e Google Drive) como infraestrutura de C2. Al Lelah et al., em revisão sistemática da literatura, demonstram que essa prática mistura deliberadamente tráfego malicioso com tráfego legítimo gerado por aplicações corporativas amplamente utilizadas, dificultando significativamente a detecção baseada em reputação de domínio ou bloqueio de IP, já que os domínios envolvidos pertencem a provedores confiáveis e amplamente permitidos em políticas de *firewall* corporativas [Al Lelah et al. 2023]. O relatório ENISA Threat Landscape 2024 corrobora essa tendência ao documentar a técnica de *Living Off Trusted Sites* como uma das principais formas de evasão observadas no cenário europeu em 2023-2024, com atores estatais utilizando plataformas de mensageria como Telegram e Slack para mascarar comunicações C2 como tráfego corporativo rotineiro [ENISA 2024].

### *2.3. Frameworks de Segurança e o Alinhamento Internacional do PPSI 2.0*

O PPSI 2.0 não constitui um *framework* de controles originalmente formulado, mas sim uma adaptação nacional de referências internacionais já consolidadas [MGI 2024]. O documento-base do programa declara explicitamente correspondência direta entre seus controles de Detecção e Resposta e os controles equivalentes do CIS Controls versão 8 (CIS v8.1), publicado pelo Center for Internet Security, que organiza dezoito famílias de controles técnicos e organizacionais de segurança da informação [CIS 2024]. Por sua vez, os controles do CIS v8.1 são mapeados, dentro do próprio *framework*, às funções do NIST Cybersecurity *Framework* (CSF) 2.0, Identificar, Proteger, Detectar, Responder, Recuperar e Governar, publicado pelo National Institute of Standards and Technology dos Estados Unidos [NIST 2024].

Essa cadeia de correspondências (PPSI 2.0 → CIS v8.1 → NIST CSF 2.0) demonstra que a aderência do programa brasileiro a boas práticas internacionais não é apenas declarativa, mas estrutural. O Controle 13 (Monitoramento e Defesa de Rede) do PPSI 2.0, central para este trabalho, corresponde a controle homônimo do CIS v8.1 e à função Detectar do NIST CSF 2.0. Essa convergência indica que soluções tecnológicas capazes de evidenciar conformidade com um desses três *frameworks* tendem a oferecer evidência transferível para os demais, o que reforça o valor prático do mapeamento proposto neste trabalho: uma ferramenta validada contra

os controles do PPSI 2.0 simultaneamente demonstra aderência implícita a referências internacionais amplamente reconhecidas pela comunidade de segurança da informação.

Adicionalmente, o próprio MITRE ATT&CK funciona como uma camada complementar de granularidade sobre esses *frameworks* de controle. Enquanto o CIS v8.1, o NIST CSF 2.0 e o PPSI 2.0 definem *o que* deve ser implementado em termos de capacidade defensiva, o MITRE ATT&CK descreve *como* os adversários efetivamente operam, por meio de táticas, técnicas e procedimentos (TTPs) derivados de observações reais de incidentes [MITRE ATT&CK Survey 2023]. A tática de Comando e Controle do ATT&CK Enterprise cataloga especificamente técnicas como uso de protocolos de aplicação padrão (T1071), tunelamento de protocolo (T1572) e uso de serviços web legítimos (T1102), que correspondem diretamente às técnicas de *beaconing*, tunelamento DNS e abuso de serviços em nuvem discutidas na Seção 2.2. Essa correspondência fundamenta o uso do ATT&CK como base teórica para o protocolo de mapeamento adotado neste trabalho, detalhado na Seção 4.2.

## 3. A Ferramenta RITA

O RITA (*Real Intelligence Threat Analytics*) é um *framework* de código aberto para análise comportamental de tráfego de rede, desenvolvido pela Active Countermeasures e distribuído sob licença GPL, listada pela CISA como uma das ferramentas gratuitas de cibersegurança [CISA 2024; RITA GitHub 2024]. A ferramenta processa logs gerados pelo Zeek, sensor de monitoramento de rede de código aberto, aplicando algoritmos estatísticos para identificar padrões de comportamento característicos de comunicação C2, sem depender de assinaturas de payload.

O RITA é organizado em módulos funcionais, descritos na Tabela 1, cada um endereçando uma das técnicas de C2 discutidas na Seção 2.2.

**Tabela 1.** Módulos do RITA

| Módulo | O que detecta | Como detecta | Indicador gerado | Relação com C2 |
|---|---|---|---|---|
| Beaconing | Conexões periódicas de host interno para destino externo | Analisa intervalos entre conexões; calcula score de periodicidade. | Score por par origem-destino | Comportamento central de C2: o host infectado contata o servidor do atacante em intervalos regulares ou levemente dinâmicos para receber comandos |
| Long Connections | Sessões TCP/UDP com duração anormalmente longa | Calcula duração total; filtra sessões acima de limiar definido | Lista de conexões longas por duração | Canais C2 abertos (reverse shells, RATs) geram sessões persistentes fora do padrão normal |
| DNS Tunneling | Uso abusivo do DNS para exfiltração ou C2 | Mede entropia, comprimento médio e volume de subdomínios por domínio | Score de suspeita de tunneling DNS por domínio | Malware encoda dados C2 em queries DNS para contornar firewalls que liberam tráfego DNS |
| Strobe | Alto volume de conexões de um host para um único destino em curto período | Conta conexões por origem-destino; sinaliza quando ultrapassa limiar | Pares origem-destino com contagem elevada | Indica polling intensivo a servidor C2 ou força bruta em porta única |
| Threat Intel | Comunicação com IPs ou domínios em listas de ameaças | Cruza destinos observados com threat intel feeds configurados | Hosts internos que se comunicaram com entradas da blacklist | Identificação direta de servidores C2 conhecidos, mesmo quando o padrão de tráfego não é suficientemente anômalo |

## 4. Metodologia e Resultados

### *4.1. Ambiente Experimental e Dataset Utilizado*

O laboratório experimental foi construído em uma máquina virtual dedicada, executada no Oracle VirtualBox versão 7.2.6, configurada com 4 vCPUs, 8 GB de memória RAM e 40 GB de armazenamento em disco, em conformidade com as recomendações de implantação publicadas pela documentação oficial do projeto. A VM utilizou o sistema operacional Ubuntu Server 22.04 LTS. Sobre essa base, foram implantados contêineres Docker responsáveis pela geração e análise dos dados: o Zeek, versão 6.2.1, empregado para produzir os logs de tráfego, e o RITA, versão 5.1.1, instalado a partir do pacote oficial da Active Countermeasures. O repositório oficial do RITA disponibiliza um arquivo docker-compose contendo os componentes nativos do projeto, incluindo o próprio RITA, o ClickHouse como *backend* de armazenamento e o Syslog-NG para ingestão de logs em modo *inline*. O mesmo repositório também fornece instruções para a instalação e utilização do Zeek nos cenários em que o tráfego a ser analisado é importado a partir de arquivos PCAP, que é exatamente o caso deste estudo.

Os arquivos PCAP utilizados como insumo foram processados pelo Zeek para geração dos logs, posteriormente importados no RITA por meio do comando *import*, para análise.

Os experimentos foram conduzidos sobre arquivo PCAP proveniente dos Traffic Analysis Exercises do repositório malware-traffic-analysis.net, mantido por Bradley Duncan, Principal Threat Researcher da Unit 42 (Palo Alto Networks), com especialização em análise de tráfego de malware em ambientes Windows [Duncan 2024a]. Essa escolha tem respaldo tanto na comunidade de segurança quanto na literatura acadêmica: trata-se de uma fonte amplamente utilizada em pesquisas formais sobre detecção de C2 e *beaconing*. Em particular, Mahboubi et al., em artigo publicado no *Journal of Network and Computer Applications* (Elsevier) sobre decodificação de comunicação de *beaconing*, constroem explicitamente um de seus datasets de avaliação a partir de logs Zeek derivados de capturas do malware-traffic-analysis.net, posicionando esse repositório como base de comparação válida frente a técnicas estatísticas de detecção de *beaconing*, e citando o próprio RITA como ferramenta de referência [Mahboubi et al. 2025]. Adicionalmente, a comunidade de resposta a incidentes utiliza rotineiramente o mesmo repositório como prova de conceito para validação de ferramentas de monitoramento de rede: a plataforma Security Onion, por exemplo, mantém uma série pública e contínua de análises técnicas (*Quick Malware Analysis*) fundamentadas em PCAPs do mesmo

repositório malware-traffic-analysis.net, processados via Zeek e Suricata, prática que se estende por dezenas de publicações técnicas datadas desde 2021 [Security Onion 2021; Security Onion 2025]. Esses precedentes sustentam a adequação metodológica do repositório como prova de conceito para este trabalho.

O PCAP selecionado para este estudo é proveniente do exercício de análise de tráfego de 4 de setembro de 2024, disponibilizado publicamente no repositório malware-traffic-analysis.net [Duncan 2024b]. O cenário documentado registra a detecção de atividade suspeita em um host interno, identificado como infectado pelo malware Win32/Koi Stealer. A infecção foi caracterizada por comunicação de Comando e Controle (C2) com um endereço IP externo, acompanhada de atividade anormal e métodos de ofuscação de tráfego HTTP, padrões que configuram uma ameaça de exfiltração ativa e que, em um ambiente de produção, demandariam isolamento imediato do sistema, investigação forense e implementação de medidas de mitigação. Esse cenário reproduz, em escala laboratorial, o contexto típico de redes corporativas e governamentais que constituem o universo de aplicação do PPSI 2.0, tornando-o adequado para avaliar a capacidade de detecção comportamental do RITA sobre tráfego malicioso real.

### *4.2. Protocolo de Mapeamento RITA × PPSI 2.0*

O protocolo de mapeamento adotado neste trabalho baseia-se nas boas práticas formalizadas pela CISA no documento Best Practices for MITRE ATT&CK Mapping [CISA 2023], que consolida diretrizes amplamente aceitas pela comunidade de segurança para qualquer processo de mapeamento que utilize o MITRE ATT&CK como referência. Essas práticas orientam que evidências técnicas observáveis sejam primeiro interpretadas à luz das táticas e técnicas do ATT&CK e, somente então, associadas aos controles do *framework* de destino, evitando mapeamentos superficiais que associem diretamente saídas de ferramenta a nomes de controle sem fundamento técnico e adversarial claro.

O protocolo foi estruturado em quatro etapas:

> Etapa 1 — Execução do RITA: os logs Zeek gerados a partir do PCAP selecionado foram importados no RITA.
>
> Etapa 2 — Coleta de Evidências: foram coletados os artefatos de saída por meio do comando rita view no terminal, constituindo as evidências empíricas do estudo.

Etapa 3 — Classificação ATT&CK: cada evidência coletada foi classificada quanto à técnica do MITRE ATT&CK Enterprise que ela representa, como T1071 para *beaconing* via protocolo de aplicação.

Etapa 4 — Mapeamento ao PPSI: cada evidência, já interpretada à luz de sua técnica ATT&CK correspondente, foi associada ao controle do PPSI 2.0 pertinente, seguindo a lógica: evidência gerada → técnica ATT&CK → controle PPSI 2.0.

### *4.3. Resultados Práticos por Módulo*

A análise do PCAP referente à infecção por Win32/Koi Stealer de 4 de setembro de 2024 [Duncan 2024b] foi conduzida com todos os módulos do RITA ativos. A saída da ferramenta é exibida em uma única tela integrada, conforme ilustrado na Figura 1, que consolida em colunas as informações de todos os módulos analisados: score de *beaconing*, duração das conexões, subdomínios DNS e inteligência de ameaças. Os resultados são apresentados a seguir, organizados por módulo.

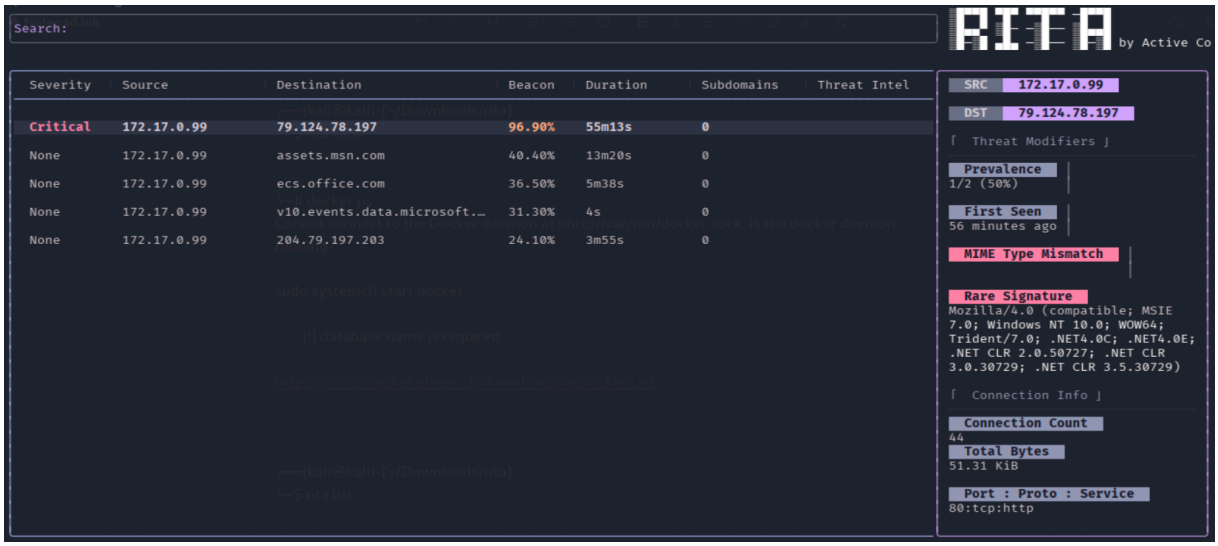


*Figura 1 - Saída do RITA — detecção Critical de beaconing no host 172.17.0.99 (score 96.90%).*

### *Beaconing*

O módulo de *Beaconing* gerou o achado mais relevante da análise. O RITA classificou como Critical a comunicação entre o host interno 172.17.0.99 e o endereço IP externo 79.124.78.197, atribuindo um score de *beaconing* de 96.90%, o valor mais elevado entre todos os pares origem-destino identificados na sessão. Esse score indica altíssima regularidade

temporal nas conexões, padrão estatisticamente improvável em tráfego legítimo e característico de um canal de Comando e Controle ativo. A comunicação ocorreu por HTTP na porta 80, totalizando 44 conexões e 51.31 KiB transferidos. A prevalência de 1/2 (50%) indica que apenas o host comprometido estabeleceu comunicação com esse destino dentro do conjunto analisado, reforçando o caráter anômalo da atividade.

Dois indicadores adicionais presentes na saída elevam a confiança na classificação. O primeiro é o alerta de MIME Type Mismatch, que sinaliza inconsistência entre o tipo de conteúdo declarado no cabeçalho HTTP e o conteúdo efetivamente transmitido, técnica utilizada por malware para disfarçar tráfego de C2 como navegação web comum. O segundo é a Rare Signature, identificada pelo User-Agent presente nas requisições: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64), que simula um Internet Explorer 7 rodando em Windows 10, combinação tecnicamente incoerente e raramente observada em tráfego legítimo moderno, configurando uma tentativa deliberada de ofuscação da identidade do cliente HTTP. Esse comportamento é consistente com a técnica ATT&CK T1071.001 (Application Layer Protocol: Web Protocols).

Os demais destinos observados na saída, como assets.msn.com (40.40%), ecs.office.com (36.50%) e v10.events.data.microsoft.com (31.30%), apresentaram scores inferiores e severidade classificada como None, refletindo tráfego legítimo de serviços Microsoft. Esse resultado demonstra a capacidade do RITA de separar comunicações suspeitas do ruído de fundo típico de um ambiente Windows corporativo, aspecto relevante para a operação prática da ferramenta em redes de órgãos do SISP.

**Long Connections**

A coluna Duration da saída do RITA registrou 55 minutos e 13 segundos de duração para a comunicação entre 172.17.0.99 e 79.124.78.197, o mesmo par identificado como Critical no módulo de *Beaconing*. Uma sessão HTTP de quase uma hora para um IP externo desconhecido, sem subdomínios associados e com apenas 51.31 KiB transferidos, é incompatível com padrões normais de navegação web ou transferência de arquivos legítimos.

Esse padrão é consistente com a manutenção de um canal de acesso remoto persistente aguardando comandos do operador, correspondendo à técnica ATT&CK T1071.001 e

reforçando o achado do módulo de *Beaconing* com uma segunda dimensão de evidência independente.

**Threat Intel**

A coluna Threat Intel da saída do RITA não apresentou valores aos destinos analisados, incluindo o IP 79.124.78.197, classificado como Critical. Esse resultado indica que o endereço não constava em nenhuma lista de ameaças configurada na ferramenta no momento da análise. Esse resultado evidencia uma das principais vantagens do RITA: a capacidade de detectar comunicações maliciosas ativas com base exclusivamente em análise comportamental, sem depender de inteligência de ameaças prévia.

Vale destacar que o módulo de Threat Intel do RITA é configurável: a ferramenta permite a integração de feeds externos de inteligência de ameaças, que podem ser substituídos ou complementados por listas mantidas pela própria organização ou por entidades governamentais. No contexto da Administração Pública Federal brasileira, isso abre a possibilidade de integração com bases de indicadores de comprometimento (IoCs) mantidas pelo CTIR Gov e pelo Serpro (reputation.serpro.gov.br), ampliando significativamente a capacidade de detecção de infraestruturas C2 já conhecidas no cenário nacional. Em um cenário real, o IP 79.124.78.197 poderia tratar-se de infraestrutura C2 recém-criada, ainda não catalogada por feeds públicos de threat intelligence, situação comum em campanhas de APT que renovam sua infraestrutura regularmente para evitar bloqueios baseados em reputação.

**DNS Tunneling e Strobe**

Os módulos de DNS Tunneling e Strobe não geraram alertas relevantes para o PCAP analisado. Esse resultado é esperado e coerente com o perfil do Win32/Koi Stealer, cujo mecanismo de C2 documentado opera via HTTP sobre porta 80, sem utilizar DNS como canal de exfiltração ou estabelecer padrões de tráfego intensivo característicos de strobe. A ausência de alertas nesses módulos não representa uma limitação do RITA, mas sim um comportamento correto da ferramenta ao não gerar falsos positivos para técnicas que o malware em questão não emprega.

### *4.4. Implicações Operacionais para Equipes de Segurança*

A operacionalização do RITA no cotidiano de um SOC (Security Operations Center) ou de um CTIR (Centro de Tratamento e Resposta a Incidentes Cibernéticos) de um órgão do SISP não substitui, mas complementa, o fluxo tradicional de monitoramento baseado em SIEM. Na prática, o RITA é mais eficaz como ferramenta de triagem e enriquecimento dentro do processo de threat hunting: analistas de blue team podem programar a importação periódica dos logs Zeek das redes monitoradas e revisar os scores mais elevados de *beaconing* como ponto de partida para investigações dirigidas por hipótese, em vez de depender exclusivamente de alertas reativos gerados por assinaturas conhecidas.

Para equipes de Red Team, os módulos do RITA oferecem um critério objetivo de validação durante exercícios de simulação adversarial. Ao emular comportamento de C2, a equipe ofensiva pode verificar empiricamente se a infraestrutura de monitoramento do órgão, instrumentada com Zeek e RITA, é capaz de detectar o padrão simulado, fornecendo métricas concretas de cobertura de detecção alinhadas ao MITRE ATT&CK. Essa prática se aproxima do conceito de purple teaming, no qual equipes ofensivas e defensivas colaboram continuamente para fortalecer a postura de segurança da organização frente a adversários sofisticados [Mettu 2025].

Para o CTIR, os resultados do RITA podem alimentar diretamente a fase de detecção e análise do ciclo de resposta a incidentes. A evidência gerada pela ferramenta, como o score de *beaconing* de 96.90% identificado na análise do Koi Stealer, fornece documentação técnica objetiva que sustenta decisões de contenção, isolamento de hosts e escalonamento para investigação forense, conforme previsto nos controles de resposta a incidentes do PPSI 2.0.

### *4.5. Resultados do Mapeamento e Limitações*

A Tabela 2 apresenta o mapeamento intermediário entre as evidências reais geradas pelo RITA na análise do PCAP do Win32/Koi Stealer, as técnicas do MITRE ATT&CK correspondentes e o controle do PPSI 2.0 sustentado por cada achado.

**Tabela 2.** Mapeamento Evidência RITA → MITRE ATT&CK → PPSI 2.0.

| Evidência (RITA) | Técnica ATT&CK | Controle PPSI | Subcontrole |
|---|---|---|---|
| Beaconing 96.90%, HTTP porta 80, 44 conexões | T1071.001 — Application Layer Protocol: Web Protocols | C13 | 13.3 |
| Long Connection de 55m13s para IP desconhecido | | | |
| MIME Type Mismatch | T1001 — Data Obfuscation | | |
| Rare Signature — User-Agent forjado (MSIE 7.0) | T1036 — Masquerading | | |
| Threat Intel = 0 — IP não catalogado em feeds | T1583 — Acquire Infrastructure | | |

O Controle 13 (Monitoramento e Defesa de Rede) orienta os órgãos a implantar e operar soluções de monitoramento e defesa do tráfego de rede, com foco na detecção de comportamentos anômalos. O **subcontrole 13.3** pergunta se o órgão implanta soluções de detecção de intrusão de rede, e é sustentado por cinco evidências empíricas convergentes geradas pelo RITA a partir da análise do tráfego do Win32/Koi Stealer.

O achado central é o score de *beaconing* de 96.90%, classificado como Critical, que evidencia comunicação C2 ativa entre o host comprometido e o IP externo 79.124.78.197 via HTTP na porta 80, mapeado à técnica T1071.001 (Application Layer Protocol: Web Protocols). A duração da sessão de 55 minutos e 13 segundos reforça esse mesmo achado, sendo incompatível com padrões normais de tráfego legítimo e consistente com a manutenção de um canal de acesso remoto persistente. O MIME Type Mismatch, mapeado à técnica T1001 (Data Obfuscation), e a Rare Signature com User-Agent forjado, mapeada à técnica T1036 (Masquerading), são evidências adicionais detectadas pelo RITA na camada de rede, indicando tentativas deliberadas de ofuscação do tráfego C2. Por fim, o resultado do módulo Threat Intel reforça o subcontrole 13.3 de forma complementar: a ausência de correspondência com feeds de ameaças conhecidos demonstra que o RITA detectou a ameaça puramente por análise comportamental, sem depender de inteligência prévia, o que é justamente o valor de uma solução de detecção de intrusão de rede baseada em comportamento.

Vale observar que o **subcontrole 13.6**, que pergunta se o órgão coleta logs de fluxo de tráfego de rede, também é atendido no contexto deste estudo, ainda que por meio do pipeline como um todo e não por um resultado direto do RITA. O uso do Zeek como coletor dos logs que alimentaram a análise demonstra que a combinação Zeek + RITA viabiliza o cumprimento desse subcontrole de forma integrada.

Entre as limitações técnicas identificadas, a principal é a incapacidade do RITA de inspecionar tráfego cifrado por TLS sem decodificação prévia. Isso restringe a visibilidade da ferramenta a metadados de conexão, abordagem que ainda é eficaz para detecção de *beaconing* por depender apenas de periodicidade temporal, mas é insuficiente para inspeção de conteúdo de payload exfiltrado. No caso específico do Win32/Koi Stealer, a comunicação ocorreu via HTTP na porta 80, o que permitiu a detecção plena. Em um cenário onde o mesmo malware utilizasse HTTPS, o score de *beaconing* ainda seria detectável, mas os indicadores de MIME Type Mismatch e Rare Signature não seriam observáveis sem inspeção TLS. Adicionalmente, o RITA depende do posicionamento do sensor Zeek na rede. Em implantações típicas, o Zeek é posicionado no perímetro, monitorando o tráfego que entra e sai da rede. Caso o atacante estabeleça um canal C2 inteiramente dentro do perímetro, utilizando infraestrutura implantada na própria rede interna, esse tráfego leste-oeste não passaria pelo sensor e não seria capturado nem analisado pelo RITA. Por fim, o RITA não substitui um SIEM para correlação multi-fonte entre logs de rede, eventos de endpoint e registros de autenticação, podendo atuar, pelo contrário, como elemento adicional de enriquecimento integrado ao SIEM.

## 5. Conclusão e Trabalhos Futuros

Este trabalho demonstrou que o RITA oferece suporte empírico e documentável ao **subcontrole 13.3** do Controle 13 (Monitoramento e Defesa de Rede) do PPSI 2.0, sustentado por cinco evidências convergentes obtidas a partir da análise do tráfego real do Win32/Koi Stealer: score de *beaconing* de 96.90% classificado como Critical, sessão de longa duração de 55 minutos e 13 segundos para IP externo desconhecido, MIME Type Mismatch, Rare Signature com User-Agent forjado e ausência de correspondência em feeds de threat intelligence. Todas as evidências foram classificadas segundo as técnicas correspondentes do MITRE ATT&CK (T1071.001, T1001 e T1036) antes de serem associadas ao controle do PPSI 2.0, seguindo o protocolo de mapeamento baseado nas boas práticas da CISA. O **subcontrole 13.6**, relacionado à coleta de logs de fluxo de tráfego de rede, é atendido de forma integrada pelo pipeline Zeek + RITA como um todo.

Um resultado igualmente relevante é que a detecção ocorreu sem qualquer conhecimento prévio da assinatura do malware analisado. Isso evidencia o principal diferencial do RITA para o atendimento do subcontrole 13.3 do PPSI 2.0: a capacidade de identificar comunicação C2 ativa por análise comportamental de tráfego de rede, sem depender de bases de assinaturas atualizadas continuamente. Essa abordagem é especialmente adequada ao contexto de órgãos do SISP, que precisam fortalecer sua capacidade de detecção de APTs sem dispor de orçamento para soluções comerciais de NDR, tensão que se mostra particularmente urgente diante do cenário nacional: segundo dados do CTIR Gov, o ano de 2024 registrou 14.921 incidentes cibernéticos em sistemas do governo federal, o maior volume desde o início do monitoramento pelo órgão [CTIR Gov 2024].

Contudo, o RITA deve ser adotado como componente de uma estratégia de defesa em profundidade. Como discutido na Seção 4.5, a ferramenta possui limitações com tráfego cifrado por TLS sem decodificação prévia, não cobre tráfego leste-oeste quando o canal C2 é estabelecido inteiramente dentro do perímetro da rede, e não substitui um SIEM para correlação multi-fonte. O modelo de implantação recomendado é um pipeline integrado de coleta (Zeek), análise comportamental (RITA) e correlação (SIEM), no qual o RITA atua como elemento de enriquecimento e triagem, reduzindo o volume de eventos que demandam investigação manual pelas equipes de SOC e CTIR. Adicionalmente, o módulo de Threat Intel da ferramenta suporta a integração com feeds externos de indicadores de comprometimento, como os disponibilizados no âmbito governamental pelo CTIR Gov, o que permite ampliar a capacidade de detecção de infraestruturas C2 conhecidas no contexto nacional.

Como trabalhos futuros, propõe-se: (i) a realização de uma Prova de Conceito do RITA em ambiente organizacional real de um órgão do SISP, avaliando seu impacto na redução do tempo médio de detecção (MTTD) de incidentes envolvendo APTs; (ii) o desenvolvimento de scripts em Python para automação da extração periódica dos resultados do RITA e geração automática de alertas via integração com webhooks de mensageria corporativa, quando scores de *beaconing* excederem limiares, reduzindo a dependência de revisão manual; e (iii) o desenvolvimento de um dashboard personalizado em Grafana, consumindo os dados indexados no ClickHouse utilizado pelo RITA como *backend*, de modo a oferecer visualização consolidada e histórica dos indicadores gerados pelos módulos da ferramenta, facilitando sua incorporação à rotina operacional de SOCs e CTIRs com recursos limitados.

## Referências


Al Lelah, T., Theodorakopoulos, G., Reinecke, P., Javed, A., and Anthi, E. (2023). Abuse of Cloud-Based and Public Legitimate Services as Command-and-Control (C&C) Infrastructure: A Systematic Literature Review. Computers. MDPI. https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf. Acesso em: jan. 2026.

ANUBIS (2021). A Provenance Graph-Based Framework for Advanced Persistent Threat Detection. https://dl.acm.org/doi/epdf/10.1145/3477314.3507097. Acesso em: jun. 2026.

Beaconing SCADA (2025). Beaconing Detection in Encrypted Traffic: A SCADA-Based Hybrid Approach Using Zeek Metadata and Isolation Forest. Research Square preprint. https://www.researchsquare.com/article/rs-8244495/v1. Acesso em: maio. 2026.

Center for Internet Security — CIS (2024). CIS Controls Version 8.1. https://www.cisecurity.org/controls/v8-1. Acesso em: jan. 2025.

CISA (2023). Best Practices for MITRE ATT&CK Mapping. Cybersecurity and Infrastructure Security Agency. Technical Report. https://www.cisa.gov/sites/default/files/publications/Best%20Practices%20for%20MITRE%20ATTCK%20Mapping.pdf. Acesso em: jan. 2025.

CISA (2024). Free Cybersecurity Services and Tools — RITA. https://www.cisa.gov/resources-tools/services/rita. Acesso em: jan. 2025.

Comprehensive Survey (2024). A Comprehensive Survey on Advanced Persistent Threat (APT) Detection Techniques. Computers, Materials & Continua. https://doi.org/10.32604/cmc.2024.057619. Acesso em: maio. 2026.

CTIR Gov (2024). CTIR Gov em Números. Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo. https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros. Acesso em: jun. 2026.

DNS-HyXNet (2025). From Graphs to Gates: DNS-HyXNet, A Lightweight and Deployable Sequential Model for Real-Time DNS Tunnel Detection https://arxiv.org/html/2512.09565v1. Acesso em: jun. 2026.

Duncan, B. (2024a). Bradley Duncan — Author Profile. Unit 42, Palo Alto Networks. https://unit42.paloaltonetworks.com/author/bduncan/. Acesso em: jan. 2026.

Duncan, B. (2024b). Traffic Analysis Exercise — 2024-09-04: Win32/Koi Stealer infection. Malware-Traffic-Analysis.net. https://www.malware-traffic-analysis.net/2024/09/04/index.html. Acesso em: jan. 2026.

ENISA (2024). ENISA Threat Landscape 2024. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape. Acesso em: jun. 2026.

ENISA (2025). ENISA Threat Landscape — Public Administration Sectorial Report. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Public%20Administration%20TL%202024%20-%20v1.2.pdf. Acesso em: jun. 2026.

Exabeam (2025). Cyber Kill Chain: Understanding and Mitigating Advanced Threats. https://www.exabeam.com/explainers/information-security/cyber-kill-chain-understanding-and-mitigating-advanced-threats/. Acesso em: jun. 2026.

GIAC DNS Tunneling. Detecting DNS Tunneling. SANS Institute, GIAC Gold Certification Paper. https://www.giac.org/paper/gcia/1116/detecting-dns-tunneling/108367. Acesso em: jun. 2026.

Katsikas, S. K. (2025). Towards a Cybersecurity-Oriented Research Agenda for Digital Sovereignty. Procedia Computer Science. Elsevier. https://www.sciencedirect.com/science/article/pii/S1877050925004375. Acesso em: jan. 2026.

Mahboubi, A., Luong, K., Jarrad, G., Camtepe, S., Bewong, M., Bahutair, M., and Pogrebna, G. (2025). Lurking in the shadows: Unsupervised decoding of beaconing communication for enhanced cyber threat hunting. Journal of Network and Computer Applications. Elsevier. https://www.sciencedirect.com/science/article/pii/S1084804525000244?via%3Dihub. Acesso em: maio. 2026.

Mettu, B. P. R. (2025). Collaborative Cyber Defense: A Framework for Purple Team Integration in Countering Sophisticated Adversaries. Journal of Computer Science and Technology Studies. https://al-kindipublishers.org/index.php/jcsts/article/view/9928/8618. Acesso em: jun. 2026.

Ministério de Gestão e Inovação — MGI (2024). Guia Framework do Programa de Privacidade e Segurança da Informação (PPSI) 2.0. https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi-2.0/. Acesso em: jan. 2026.

MITRE ATT&CK Survey (2023). MITRE ATT&CK: State of the Art and Way Forward. https://arxiv.org/abs/2308.14016. Acesso em: jan. 2026.

National Institute of Standards and Technology — NIST (2024). The NIST Cybersecurity Framework (CSF) 2.0. Technical Report. NIST. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf. Acesso em: jan. 2026.

Oxford SLR APT (2024). A Systematic Literature Review on Advanced Persistent Threat Behaviors and its Detection Strategy. Journal of Cybersecurity.Oxford Academic. https://academic.oup.com/cybersecurity/article/10/1/tyad023/7504935. Acesso em: jan. 2026.

RITA GitHub (2024). RITA — Real Intelligence Threat Analytics. Active Countermeasures. https://github.com/activecm/rita. Acesso em: jan. 2026.

Security Onion (2021). Quick Malware Analysis: Traffic Analysis Exercise pcap from 2021-02-08. https://blog.securityonion.net/2021/11/quick-malware-analysis-traffic-analysis.html. Acesso em: jun. 2026.

Security Onion (2025). Quick Malware Analysis: NETSUPPORT RAT pcap from 2025-08-20. https://blog.securityonion.net/2025/08/quick-malware-analysis-netsupport-rat.html. Acesso em: jun. 2026.

Verizon (2024). 2024 Data Breach Investigations Report (DBIR). https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf. Acesso em: jun. 2026.