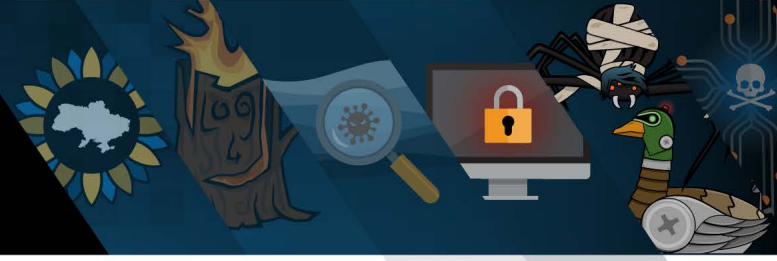
# RANSOMWARE E COMMODITY LOADERS



BAIXE O DOCUMENTO COMPLETO AQUI

## CENÁRIO DE AMEAÇAS DE RANSOMWARE

O espaço de ransomware é dinâmico, adaptando-se continuamente às mudanças no ambiente geopolítico, às ações dos defensores e aos esforços das autoridades policiais, cujo o escopo e a intensidade aumentaram em 2022. Isso leva os grupos a reformular a marca com nomes diferentes, encerrar operações e formar novas parcerias estratégicas. O Cisco Talos observou várias tendências relacionadas em 2022.

O Talos rastreia dezenas de grupos de ransomware como serviço (RaaS) **(Figura 1)**. De acordo com nossas descobertas, o LockBit foi o grupo mais ativo em 2022, respondendo por mais de 20% do número total de publicações de vítimas da Dark Web, seguido de perto pelo Hive e pelo Black Basta. Essas descobertas apontam para uma maior democratização dos opositores de ransomware, uma mudança geral em relação aos anos anteriores, em que alguns grupos selecionados monopolizaram o cenário. As afiliadas de ransomware também não têm mais estruturas isoladas e agora estão trabalhando em vários grupos, em que os agentes com conjuntos de habilidades exclusivas têm mais oportunidades de oferecer suporte a várias campanhas e empresas.

Também houve maiores complicações em toda a comunidade, pois a guerra na Ucrânia obrigou muitos agentes de ameaça a escolher um lado no conflito e direcionar suas operações contra alvos a favor da Rússia ou da Ucrânia. O grupo Conti RaaS estava entre os mais alarmantes, alertando que atacariam qualquer pessoa que tentasse interferir na invasão da Rússia. Um indivíduo ligado ao Conti se vingou da gangue de ransomware vazando informações, inclusive o código-fonte do malware e bate-papos internos entre as afiliadas. Em outro evento, o Talos tomou conhecimento da divulgação

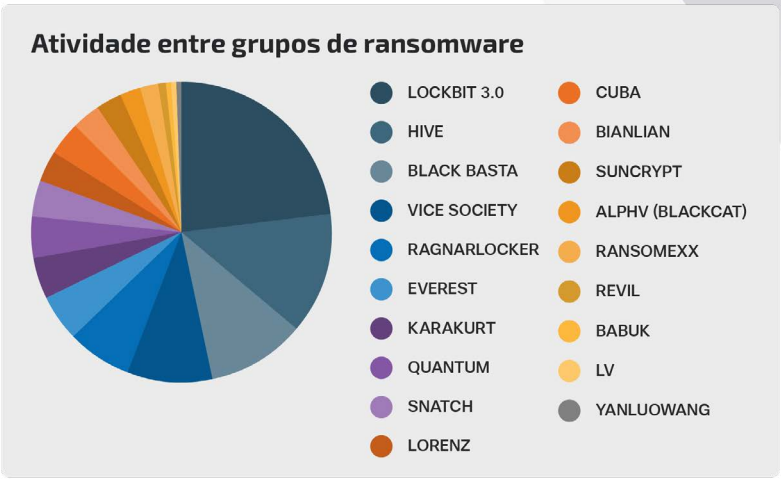



***Figura 1.*** *Número de publicações feitas em sites de vazamento de dados de ransomware rastreados pelo Talos, de janeiro a outubro.*

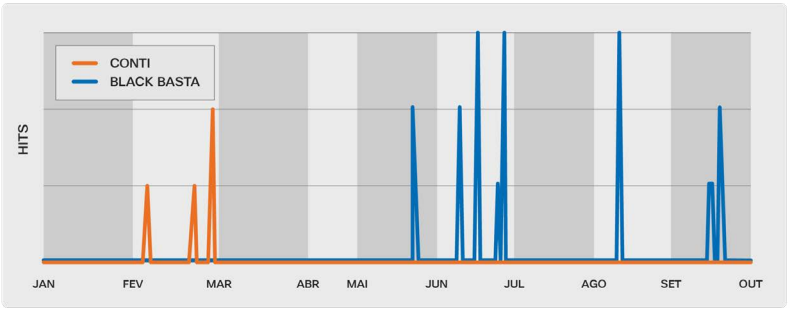



***Figura 2.*** *Detecções de indicadores comportamentais no ransomware Secure Malware Analytics for Conti e modificações de registro Black Basta.*

de um criador que vazou para o criptografador de ransomware LockBit 3.0 chamado de "LockBitBlack". O indivíduo que reivindica a responsabilidade é um suposto desenvolvedor do LockBit que, de acordo com o LockBit, afirmou estar insatisfeito com a estrutura de pagamento do grupo.

Esse tipo de conflito é o que geralmente leva à uma nova marca das gangues de ransomware ou ao surgimento de novos grupos. Quando o Conti encerrou as operações e colocou sua infraestrutura off-line, vimos uma queda geral nas detecções em nossa telemetria, mas, logo em seguida, surgiu uma nova marca do Conti denominada "Black Basta". Os pesquisadores sugerem que os dois grupos têm estilos de comunicação e sites de pagamentos e vazamento semelhantes **(Figura 2)**.

# RANSOMWARE E COMMODITY LOADERS

## COMMODITY LOADERS

Os commodity loaders, cavalos de Troia comerciais que implantam malware de segundo estágio, são uma ameaça constante que continua a ter um impacto global. Inicialmente desenvolvidos como cavalos de Troia bancários criados para comprometer entidades para ganho monetário, ao longo do tempo, eles se adaptaram a controles de segurança maiores e se transformaram em ameaças muito mais avançadas. Eles agora operam principalmente como loaders com funções modulares, permitindo que os criminosos cibernéticos tenham a flexibilidade de trabalhar com uma variedade de ferramentas de código aberto e malware recém-desenvolvido. Os quatro commodity loaders mais ativos em 2022 foram Qakbot, Emotet, IcedID e Trickbot, de acordo com nossa análise de vários conjuntos de telemetria de rede e endpoint **(Figura 3)**.

Embora nossa telemetria tenha detectado uma atividade associada ao Trickbot, avaliamos que grande parte dessa atividade provavelmente estava detectando endpoints antigos infectados, pois os operadores de malware estavam inativos desde o início de 2022. Da mesma forma, o Emotet, embora ainda operacional, permanece consideravelmente menos ativo do que antes do botnet ser suprimido pelas autoridades, no início de janeiro de 2021. Outros produtos de malware preencheram a lacuna ao se tornar mais populares, como Qakbot e IcedID.

Em uma tendência geral de 2022 que observamos, os operadores distribuíram com mais frequência o Qakbot, Emotet e IcedID usando os tipos de arquivo ISO, ZIP e LNK, provavelmente para contornar os esforços da Microsoft de bloquear documentos habilitados para macros. Em outra tendência, o Talos observou os operadores Qakbot, Emotet e IcedID que baixam e lançam cargas mal-intencionadas usando living-off-the-land binaries (LoLBins) encontrados nos ambientes de vítima. Em alguns casos, os afiliados do Qakbot e do Emotet refinaram a sequência de ataques, experimentando diferentes LoLBins para melhorar as chances de não serem detectados em uma empresa.

### Commodity Loaders

| | Qakbot | IcedID | Emotet | Trickbot |
|---|---|---|---|---|
| Aliases | Quackbot, Qbot, Pinkslipbot | BokBot | Geodo, Heodo | N/D |
| Afiliações | Malware de commodity provavelmente desenvolvido por criminosos cibernéticos eurasianos | Desconhecido | Malware de commodity desenvolvido pelo Mummy Spider, um grupo de crimes cibernéticos alinhado à Rússia | Malware de commodity desenvolvido pelo Mummy Spider, um grupo de crimes cibernéticos alinhado à Rússia |
| Active since | 2007 | 2014 | 2017 | 2016 |

**Metas**

- Obter acesso inicial e estabelecer persistência para facilitar outras atividades de invasão.
- Implantar malware na próxima fase, inclusive ransomware.

**Vitimologia**

- Direcionado para todos os setores em todo o mundo.
- Desde a guerra entre Rússia e Ucrânia, o Trickbot tem ameaçado retaliar contra o povo russo em relação aos ataques visíveis.

**TTPs notáveis**

- Phishing, malspam, engenharia social, exploração de vulnerabilidades, roubo de dados, como dados financeiros e credenciais, e propagação semelhante a worm.
- Altamente modular, permitindo que os operadores realizem uma ampla variedade de ataques.

**Malware e ferramentas**

- As variantes de malware implantam e são implantadas por várias outras famílias de malware, inclusive umas às outras.
- Usar ferramentas comerciais, como Cobalt Strike, bem como LoLbins em vários estágios do ciclo de vida do ataque.

***Figura 3.** Matriz de ameaças dos commodity loaders.*

Embora nossa telemetria tenha detectado uma atividade associada ao Trickbot, avaliamos que grande parte dessa atividade provavelmente estava detectando endpoints antigos infectados, pois os operadores de malware estavam inativos desde o início de 2022. Da mesma forma, o Emotet, embora ainda operacional, permanece consideravelmente menos ativo do que antes do botnet ser suprimido pelas autoridades, no início de janeiro de 2021. Outros produtos de malware preencheram a lacuna ao se tornar mais populares, como Qakbot e IcedID.

Uma análise detalhada de cada commodity loader está disponível no relatório completo.