2023

White paper series
Publicação 10

# Desafios e estratégias:

*Considerações sobre os ataques de ransomware nas Américas*

OEA | Mais direitos para mais pessoas

aws

# Créditos

Luis Almagro
**Secretário-Geral da Organização dos Estados Americanos (OEA)**

**Equipe técnica da OEA**
Luis Fernando Lima Oliveira
Alison August Treppel
Kerry-Ann Barrett
Mariana Jaramillo

**Equipe técnica de AWS**
Abby Daniell
Melanie Kaplan
Camilo Gonzalez
Arturo Cabañas
Jordana Siegel

**Editor**
Jeimy Cano

# Sumário

# Definições

**Botnet (A palavra "botnet" vem de "robot network")**
É uma rede de computadores infectados (via código malicioso), que são controlados remotamente e podem ser forçados a enviar spam, espalhar malware ou realizar ataques DDoS, tudo sem a autorização do proprietário do dispositivo[1].

**Carga útil (Payload)**
Parte de um malware (código malicioso) que executa a ação adversa ou prejudicial no sistema de destino depois de ter feito uma invasão bem-sucedida.

**Ciberhigiene**
É a adoção de uma mentalidade focada em segurança e hábitos de uso diário que ajudam os indivíduos e as organizações a mitigarem possíveis violações on-line[2].

**Cópia de backup**
Uma cópia dos arquivos e dos programas feita para facilitar sua recuperação, quando necessário[3].

**DDos**
Uma técnica de bloqueio de serviço que utiliza numerosos equipamentos para realizar o ataque[4].

**Doxing**
Ação ou processo de buscar e publicar na Internet informações privadas ou identificáveis sobre uma pessoa específica, geralmente com má intenção[5].

**Encriptação de dados**
Qualquer procedimento utilizado em criptografia para converter texto plano em texto cifrado a fim de impedir que qualquer pessoa, a não ser o destinatário previsto, possa ler esses dados[6].

**Link malicioso**
Link malicioso é um link que direciona para um site fraudulento. De maneira geral, consiste em uma conexão que parece levar a um site legítimo que, na realidade, é um site falso[7].

**Exfiltração ou vazamento de informações**
É a cópia, transferência ou recuperação ilegais de dados ou informações de um servidor que acaba nas mãos de um terceiro não autorizado.

**Malware**
Programa que se insere em um sistema, normalmente de forma encoberta, com a intenção de comprometer a confidencialidade, a integridade ou a disponibilidade dos dados, dos programas ou do sistema operacional da vítima, ou de causar disrupções de qualquer outra natureza à vítima[8].

**Ransomware**
Tipo de malware que geralmente sequestra e criptografa arquivos em um sistema de armazenamento e, em seguida, pede um resgate, geralmente mediante pagamento em criptomoedas, sem a garantia de que todos os arquivos possam ser descriptografados ou devolvidos com as mesmas condições iniciais.

1 https://www.avast.com/es-es/c-botnet
2 https://www.kaspersky.es/resource-center/preemptive-safety/cyber-hygiene-habits
3 https://csrc.nist.gov/glossary/term/backup
4 https://csrc.nist.gov/glossary/term/ddos
5 Tavella, F. (2021). Ransomware Conti: principales características y cómo operan sus afiliados. ESET. https://www.welivesecurity.com/la-es/2021/11/29/ransomware-conti-principales-caracteristicas/
6 https://csrc.nist.gov/glossary/term/encryption
7 https://www.mundopc.es/links-maliciosos-como-detectar-una-url-fraudulenta-484.html
8 https://csrc.nist.gov/glossary/term/malware

# Introdução

Notícias recentes em diferentes relatórios, tanto de fornecedores de tecnologias de segurança empresarial quanto de autoridades policiais, relatam que o **"ransomware"**[4] se tornou um dos riscos e ameaças mais importantes para a segurança global, não apenas por sua versatilidade e capacidade de ação, mas também por sua expansão e pelo impacto nas finanças e na reputação em nível organizacional (Interpol, 2020). Neste contexto, essa ameaça digital se torna um ponto de reflexão relevante para os setores público e privado.

Quando uma organização é afetada por ransomware, surge a pergunta-chave: ***"Como responder a um evento de segurança de ransomware e mitigá-lo?*** [5] Essa pergunta gera, nos setores público e privado, tensões de diferentes magnitudes e implicações de atribuição de responsabilidade dentro de uma organização, como considerações sobre como revelar detratores do investimento em segurança cibernética, além de uma série de implicações colaterais que normalmente atendem aos propósitos do adversário: gerar confusão, confronto e jogo de responsabilidades que lhe dão mais tempo para agir e se posicionar na busca do pagamento, que é o seu propósito final. Portanto, os setores público e privado têm todo interesse em mitigar o impacto nos dados e na reputação proveniente de um evento de ransomware, que pode gerar incertezas sobre como lidar com a situação e se se deve atender ao resgate ou não.

Quando uma organização é informada, em seus níveis executivos, da ocorrência de um ransomware, a reação comum é, em primeiro lugar, tentar entender que tipo de informação está comprometida e, depois, solicitar as explicações técnicas de como esse evento de segurança afeta as operações e quais são as suas potenciais implicações legais, bem como se as informações estão sujeitas a alguma proteção jurídica especial. Com esses dados, as organizações normalmente tentam esboçar, com todos os envolvidos internos, uma visão geral do que aconteceu e definir uma posição de base para agir contra o ransomware.

Existem situações em que esses eventos de segurança podem afetar severamente as organizações – por exemplo, a extorsão com dados é uma forma de cibercrime que se baseia na inteligência, no chamariz e na distração desenvolvidos pelo adversário, com um padrão de comportamento baseado nas necessidades e expectativas dos indivíduos. Neste sentido, ao se identificar o que pode ser de interesse do usuário-alvo (por exemplo, a expectativa de uma promoção, a entrega de um bônus, o pagamento de uma multa, a intimação de uma instituição policial etc.), e vincular isso à dinâmica do contexto atual (o momento específico que a pessoa está vivendo com suas expectativas), os adversários conseguem mimetizar suas ações em um tecido social concreto para abordar suas vítimas potenciais sem que elas percebam.

4 Definição página 1.
5 As boas práticas internacionais desenvolvidas até o momento sugerem não pagar. Ver The European Union Agency for Cybersecurity (ENISA) Landscape for ransomware attacks: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks

A falta de compreensão dos controles de segurança para os serviços técnicos contribui para o sucesso de usuários não autorizados. Se, além do exposto acima, os agressores identificarem a baixa higiene informática (comumente chamada de *higiene cibernética*) em que as pessoas se movem no contexto digital, a confiança ingênua nos meios e nas tecnologias disponíveis e o aumento de produtos e serviços digitais implantados com medidas limitadas de segurança e controle, eles terão o cenário ideal para se mobilizar e executar suas ações e planos com pouco espaço para reação.

Esta publicação busca fornecer recomendações e reflexões baseadas em boas práticas internacionais para tomadores de decisão de organizações dos setores público e privado, em torno da realidade de um ataque de ransomware e de suas implicações, para ilustrar o processo que ocorre neste evento e, assim, propiciar espaços para se examinar como enfrentar esse desafio, que margem de ação se pode ter e como detectar alguns padrões de alerta sobre o avanço dessa ameaça em uma organização.

# Sequestro de dados: O que acontece em uma organização?

O sequestro de dados priva a pessoa ou a organização de um de seus bens mais importantes, que são seus dados e informações, e é de fato uma afronta direta que coloca em risco os direitos e as prerrogativas das organizações e das pessoas em sua liberdade na dinâmica social. O sequestro de dados e a posterior extorsão por terceiros configuram uma ação penal que, no devido tempo, será abordada por diferentes jurisdições e ações legislativas e incorporada aos sistemas jurídicos nacionais e internacionais (Grimes, 2022).


Quando uma organização é afetada por um evento de ransomware, surgem dilemas e geralmente são poucas manobras legais que podem ser ativadas para tentar conter os seus possíveis efeitos adversos (Leo et al., 2022).

Por um lado, a organização pode utilizar políticas de cibersegurança, que, de acordo com o seu âmbito e exclusões, podem apoiar as entidades na gestão desse desafio. Por outro lado, pode-se negociar com o agressor que capturou os dados, com a clareza de que, mesmo tendo maneiras de restaurar as informações, é provável que você não consiga fazê-lo completamente. No entanto, é importante ressaltar que as boas práticas e recomendações internacionais não recomendam a negociação com o agressor.[6] A alternativa de pagamento não é uma opção sustentada pelas boas práticas para se lidar com ransomware (e é abertamente ilegal em diferentes jurisdições nacionais e internacionais). Qualquer das ações convencionais tomadas tornará a organização mais resistente à materialização do ransomware, sem prejuízo do fato de que em algum momento o adversário poderá ter sucesso. Além disso, esse tipo de ação deverá se ajustar ao sistema legal (com exceção do pagamento de extorsão), o que dará tranquilidade aos executivos em suas estruturas de *compliance* e relatórios às entidades de controle.

Finalmente, informar e envolver a autoridade competente[7] em uma investigação pode ajudar a fornecer informações sobre o agente da ameaça com a utilização de diferentes estratégias para se encontrar o agressor, desativar o mecanismo de encriptação e usar canais diplomáticos,[8] se for o caso. Portanto, em conformidade com os cânones estabelecidos pela Constituição e pela lei, essas são algumas das maneiras pelas quais você pode optar na abordagem a um sequestro de dados.

6 https://www.nomoreransom.org/en/ransomware-qa.html
7 Les superviseurs d'un secteur particulier, la police ou les forces de l'ordre.
8 Lorsque les données compromises se trouvent dans d'autres pays ou juridictions ou y sont transférées, et qu'il devient nécessaire d'utiliser les voies diplomatiques pour coordonner l'action des services répressifs et judiciaires afin de prendre des mesures pour récupérer ou supprimer les informations.

*O* ransomware tira da zona de conforto os profissionais de segurança da informação, os advogados corporativos e os tomadores de decisão, levando-se em conta que, se as informações ou os dados comprometidos estiverem sujeitos a condições particulares de proteção e devido cuidado, eles deverão estabelecer claramente como responder à situação das diferentes partes interessadas afetadas. Consequentemente, a organização afetada estará em uma encruzilhada onde será avaliada em relação a suas práticas de segurança, privacidade e controle, e em relação a como estas vêm sendo desenvolvidas e aplicadas, gerando tensões legais com suas respectivas sanções (geralmente econômicas), que podem acabar impactando sua reputação no setor.

A abordagem a um ataque de ransomware é um tema que vai além do fenômeno tecnológico que o materializa, e possibilita um exame sistêmico do problema que conecta práticas de segurança, relações institucionais, marcos legais, seguradoras, vulnerabilidades tecnológicas e, sobretudo, comportamentos humanos (Sittig & Singh, 2016).

O *ransomware* tira da zona de conforto os profissionais de segurança da informação, a área jurídica das instituições e os tomadores de decisão. Para ser resiliente, é importante que cada organização tenha um plano proativo para responder à situação – por exemplo, seguindo o processo de preparação do NIST.[9]

9 Ransomware | NIST

# Ocorrência do ransomware: Dois lados da mesma equação

As ações que ocorrem após um sequestro de dados têm algum tipo de motivação (nem sempre econômica) e levam ao contato direto ou indireto com os grupos de interesse da vítima, a fim de se iniciar um jogo de pressões e tensões que buscam quebrar a vontade da parte impactada. Para isso, testes de sobrevivência, chamadas ameaçadoras e manifestações tangíveis que geram incerteza (fotos, símbolos ou pertences) são peças fundamentais para a criação da necessidade e das ações requeridas que levam ao cumprimento do objetivo do agressor.


No mundo digital, o ransomware tem hoje pelo menos duas visões: sequestro de informações ou dados (geralmente sensíveis) pelos quais se exige um pagamento de resgate (com a ameaça de que o não pagamento acarretará sua destruição ou desaparecimento); ou acesso a informações sensíveis ou comprometedoras que possam ser expostas (com possíveis danos à reputação) se não houver pagamento ao criminoso digital (Baykara & Sekin, 2018). Em ambos os casos, os criminosos procurarão fornecer evidências às suas vítimas de que qualquer dessas ameaças é real e grave e que as ações são realizadas para intimidar e gerar pressão, incluindo contagens regressivas visíveis, mensagens de voz modificadas para intimidar as organizações ou pessoas e contatos baseados em contas de e-mail anônimas ou descartáveis. Na análise da ocorrência de um evento como o ransomware, é necessário avaliar os dois lados da equação: a organização (ou a pessoa) e o atacante.

Do lado da pessoa ou da organização, a análise sobre a possível ocorrência e extensão dos danos por conta de um ransomware pode incluir os seguintes aspectos:

- Nível de garantia das práticas de segurança e controle
- Nível de ajuste fino e uso das tecnologias de segurança e controle disponíveis
- Evidências e lições aprendidas com a avaliação e o monitoramento dos planos de recuperação e continuidade de negócios
- Análise do comportamento de navegação e uso da internet
- Nível de desenvolvimento da cultura de segurança da informação (incluindo a higiene pessoal cibernética)
- Análise prospectiva de riscos latentes e emergentes para a indústria da organização no contexto das operações e estratégias da organização
- Definição de apetite ao risco[10] empresarial (ou pessoal) (Herrera Silva, Barona López, Valdivieso Caraguay & Hernández-Álvarez, 2019)

10 A cota de riscos que uma organização está disposta a aceitar e suportar na realização da sua missão/visão. Fonte: Quinn et al. (2021 Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management. NIST. NISTIR 8286A. https://doi.org/10.6028/NIST.IR.8286A

Qualquer falha ou resultado que não corresponda ao que se espera em cada um dos elementos mencionados está associado a uma capacidade limitada de gestão de risco por parte da organização ou da pessoa, frente aos devidos cuidados que devem ser tomados na proteção das informações ou dos dados de sua propriedade ou pelos quais é responsável, o que se pode caracterizar como como negligência comprovável por meio de auditoria ou verificação independente.

Do ponto de vista do agressor, a análise das capacidades e dos apoios disponíveis para atingir os seus objetivos pode incluir, entre outros aspectos, os seguintes:

- Nível de especialização e capacidade de desenvolver inteligência
- Motivações específicas que levam à ação
- Uso de ferramentas conhecidas ou especializadas
- Conexões com outros grupos criminosos
- Pagamentos baseados em criptomoedas ou outros tipos de monetização
- Padrões de ação anteriores
- Antecedentes disponíveis em nível nacional ou internacional (Cano, 2020)

Qualquer informação que se considere, com base na lista acima, oferecerá orientação e pistas para seguir o rastro do invasor. Cada uma delas ajudará a formar o quebra-cabeça que envolve a conexão das diferentes ações do agressor, com vistas a se encontrar padrões consistentes que deem clareza à reconstrução da sua ação criminosa e que levem, no melhor dos cenários, a encontrar sua localização e a capturá-lo. Isso nem sempre é possível; porém, quanto mais confiável e relevante for a informação obtida, melhores serão os mapas que podem ser traçados no território de natureza incerta plantado pelo adversário (El-Kosairy & Azer, 2018).

No mundo digital, o ransomware tem hoje pelo menos duas visões: *sequestro* de informações ou dados (geralmente sensíveis), para os quais se exige um resgate (com a ameaça de que o não pagamento acarretará sua destruição ou desaparecimento); ou *acesso a informações sensíveis ou comprometedoras* que possam ser expostas (com possível impacto na reputação) se não houver pagamento ao criminoso digital.

# Recomendações/Boas práticas face a um ataque de ransomware: *Ideias convencionais*

Ao constatar a ocorrência de um ransomware, a organização deverá considerar os dois lados da equação, e não apenas se concentrar nos danos que o ataque gera internamente, com as consequências naturais geradas pelo fato do ponto de vista das responsabilidades individuais e coletivas, além de considerar o possível impacto sobre os indivíduos dentro da organização.

Várias agências fornecem informações sobre como equipar melhor as organizações para lidarem com esses incidentes. Neste sentido, propõem-se aqui algumas ações convencionais que as organizações ou os indivíduos podem aplicar no caso da ocorrência de sequestro de dados e extorsão. Por exemplo, nos Estados Unidos o Federal Bureau of Investigation (FBI) incentiva as organizações a relatarem incidentes de resgate às autoridades policiais. O Internet Crime Complaint Center (IC3) aceita relatórios de crimes on-line na internet da vítima real ou de terceiros ao denunciante, e trabalha com eles para determinar o melhor curso de ação no futuro. Neste caso, as seguintes informações são essenciais para se dar prosseguimento à ação:

1. Qualquer informação relevante que se considere necessária para apoiar a queixa
2. Cabeçalho(s) de e-mail
3. Informações de transações financeiras (informações sobre conta, data e valor da transação, detalhes do destinatário)
4. Nome do denunciante, endereço, telefone, e-mail, site e endereço IP
5. Detalhes específicos sobre como a vítima foi afetada
6. Nome, endereço, telefone e e-mail da vítima

As seguintes recomendações são fornecidas com base nas boas práticas internacionais disponíveis até à data:[11]

• Contratar ou procurar serviços especializados para restaurar dados comprometidos. Esse tipo de serviço é caro e envolve o uso de ferramentas específicas que tentam encontrar padrões e estabelecer formas alternativas de acessar dados, o que nem sempre se consegue.

• Entrar em contato com os provedores de ferramentas de segurança e controle, ou seus contatos, a fim de estabelecer alternativas para encontrar maneiras de recuperar as informações ou parte delas. Essa ação costuma gerar resultados discretos, e existem centros de pesquisa associados que podem contribuir neste sentido.

• Usar o backup das informações da organização ou da pessoa, que geralmente não responde a uma prática sistemática e validada. Em geral, essa estratégia funciona parcialmente, uma vez que a atualização das informações suportadas define o nível de escopo e manobra que a organização ou pessoa pode ter. O uso dessas informações como forma de recuperação pode gerar deficiências e diferenças quando utilizadas, uma vez que depende da confiabilidade da mídia de armazenamento utilizada, da tecnologia de suporte usada no backup e da estratégia implementada: backup diário, incremental ou total, ou armazenamento em nuvem.

• Desenvolver e atualizar o plano de continuidade das atividades que considera as informações sujeitas a proteção jurídica (tendo como primeira prioridade, por exemplo, bases de dados com informações pessoais) a fim de manter o devido cuidado e a *compliance* regulatória frente aos supervisores do seu setor nos níveis nacional e internacional.

• Manter os dados criptografados (codificados em trânsito e quando não estiverem em uso) na mídia de armazenamento estabelecida pela organização/pessoa (para casos de dupla extorsão: exfiltração e criptografia).

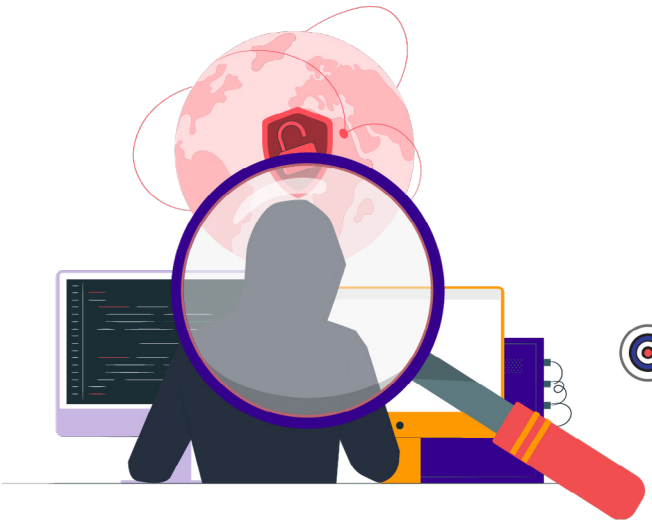
• Aplicar patches ou ajustes críticos, liberados por fornecedores, a programas ou sistemas operacionais disponíveis para a organização/indivíduo.

• Garantir treinamento e simulação periódicos aos indivíduos contra as estratégias utilizadas pelos invasores na implementação de chamarizes e na motivação de ações que possibilitam a materialização de ransomware.

• Motivar as pessoas a denunciarem comportamentos suspeitos dos dispositivos que utilizam (como desativação de serviços, reinicialização, alertas do sistema antivírus, entre outros).

11 U.S. Cybersecurity & Infrastructure Security Agency - https://www.cisa.gov/stopransomware/ransomware-guide
The European Union Agency for Cybersecurity (ENISA) Landscape for ransomware attacks - https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks
Australian Cyber Security Centre (ACSC) – Ransomware Attacks Emergency Response Guide - https://www.cyber.gov.au/sites/default/files/2021-07/11515_ACSC_Emergency-Response-Guide_Accessible_08.12.20.pdf

# Estudos de caso – Guacamaya e Conti: *Ameaças presentes na região*



Considerando as análises anteriores em torno do ransomware, é importante reconhecer e examinar os possíveis adversários por trás dessas ações. Neste sentido, desenvolve-se a seguir uma breve caracterização de dois estudos de casos e dos impactos de suas ações na região.

## GUACAMAYA

Segundo Vicens (2022), Guacamaya é um grupo de ativistas centro-americanos cujo principal objetivo é se infiltrar em mineradoras e petroleiras, polícias e diferentes agências reguladoras latino-americanas, a fim de revelar injustiças em geral, ofensas penais contra a população, o território local e o planeta. Ele critica abertamente o "imperialismo dos EUA" e sua agressão aos povos da América.

Este grupo hacktivista tem como alvo governos, entidades estatais, militares e extrativistas, a fim de supostamente motivar maior transparência nas informações sobre iniciativas dos Estados ou das instituições mencionadas e, assim, dar aos cidadãos detalhes que não são se observam diretamente.

O modo de funcionamento deste grupo consiste em identificar vulnerabilidades comuns ou típicas nas infraestruturas das instituições-alvo, tais como falhas na atualização ou configuração do sistema operacional ou de aplicativos específicos, que são exploradas para a obtenção de acesso privilegiado às informações residentes em dispositivos tecnológicos e, em seguida, revelar a informação e publicá-la em diferentes meios de acesso público. Além disso, mantém um portal[12] onde acompanha suas ações e declarações.

Entre suas ações mais direcionadas estão os ataques ao setor público de Chile, México, Peru, El Salvador e Colômbia, nos quais, devido a essas ações de ransomware, foram reveladas informações confidenciais de governos, instituições militares e empresas do setor extrativo.

12 https://enlacehacktivista.org

## CONTI

Ao contrário do grupo Guacamaya, o CONTI é uma organização transnacional do crime organizado, supostamente de origem russa. Foi detectado pela primeira vez em 2020 e acredita-se que seja o sucessor do grupo de ransomware Ryuk. De acordo com Chainalysis (2022), este grupo de ransomware foi o que mais arrecadou em 2021, com uma receita estimada de pelo menos US$ 180 milhões.

De acordo com Tavella (2021), o CONTI costuma utilizar a modalidade de dupla extorsão, também conhecida como *doxing*, que consiste em exfiltrar informações confidenciais de suas vítimas e criptografá-las e, em seguida, extorquir as vítimas ameaçando publicar as informações exfiltradas se não pagarem a quantia exigida. Dessa forma, eles aumentam a pressão, uma vez que não se trata apenas de recuperar os arquivos criptografados, mas também de evitar uma possível violação de informações que possa prejudicar a vítima de várias maneiras.

O *modus operandi* do CONTI engloba:

- Esquemas de phishing com anexos maliciosos;
- Recrutamento de pessoal interno da empresa-alvo para realizar e expandir sua atividade ilícita;
- Exploração de vulnerabilidades conhecidas em computadores expostos à internet;
- Ataques a computadores com o serviço RDP (Remote Desktop Protocol)[13].

O grupo criminoso CONTI opera como qualquer outra empresa no mundo. Possui vários departamentos, desde recursos humanos e administradores até codificadores e pesquisadores. Tem políticas próprias sobre como seus hackers devem processar seu código e, como contrapartida, adotam as melhores práticas para manter os membros do grupo escondidos das forças da ordem (Burguess, 2022).

O CONTI esteve envolvida em inúmeros ataques de alto perfil, incluindo aqueles contra a cidade de Tulsa, as escolas públicas do condado de Broward a Advantech nos Estados Unidos. No entanto, foi só depois de atacar o Health Service Executive (HSE) e o Department of Health (DoH) da Irlanda, deixando fora de serviço os sistemas de computadores do país por semanas, que eles ganharam notoriedade (Abrams, 2022).

Ultimamente, o CONTI vem atuando na América Latina, onde sua ação mais recente revelada pela mídia internacional foi o ataque contra os bancos de dados do Ministério das Finanças da Costa Rica e de outras instituições públicas do país, em 12 de abril de 2022, o que levou à declaração do "Estado de Emergência Nacional em todo o setor público do Estado da Costa Rica", de acordo com as disposições do decreto Nº 43542-MP-MICITT, de 8 de maio de 2022.

Como se vê, tanto o Guacamaya como o CONTI são ameaças concretas à estabilidade da região, uma vez que suas estratégias e métodos, embora diferentes na busca de seus objetivos, baseiam-se na aplicação limitada de boas práticas e padrões de cibersegurança /segurança nos níveis empresarial e estatal. A ameaça requer o desenvolvimento e a criação de capacidades conjuntas para fortalecer uma postura vigilante que possibilite, não apenas responder, mas dissuadir, atrasar ou confundir esses adversários.

13 Um protocolo que permite a um usuário remoto ter acesso total ao seu dispositivo, podendo mover o mouse e utilizar o teclado como se estivesse em frente ao computador.

Um resumo da caracterização desses dois grupos pode ser visto abaixo.

| Características | Guacamaya | Conti |
|---|---|---|
| Fundamento da sua ação | Hacktivista | Crime organizado |
| Procedência | Aparentemente América Central | Aparentemente Rússia |
| Técnicas utilizadas | Exploração de vulnerabilidades em equipamentos: falha na atualização ou configuração do sistema operacional ou de aplicativos específicos. | Phishing com documentos maliciosos anexados, exploração de vulnerabilidades conhecidas, ataque a equipamentos com exposição do protocolo de escritório remoto, decifração de senhas. |
| Setor-alvo | Inteligência militar, entidades estatais, segurança nacional, empresas de mineração e extração. | Entidades estatais ou empresas-chave que afetem os cidadãos e a dinâmica de um país. |
| Organização | Grupo organizado e centralizado em torno de uma causa comum: supostamente o bem-estar social e interesses nacionais. | Grupo de operação descentralizada em nível global, com fins econômicos e extorsivos. |
| Objetivo | Maior transparência da informação gerida pelos governos e pelas empresas de extração. | Incerteza, instabilidade, caos e ganhos econômicos. |
| Filosofía | Hacking com forma de resistência. | Hacking como forma de desestabilização política e geração de renda. |
| Resultado esperado | Exfiltração de dados sensíveis. | Retenção, exfiltração e encriptação de dados para garantir o pagamento. |

Tabela 1. Caracterização do Guacamaya e do Conti

# Conclusões

Ransomware é uma forma de crime organizado resultante da transformação digital da criminalidade há coisa de 10 a 15 anos, quando começava a questão dos *botnets* (ver definições). Conseguir controlar um computador sem que a vítima tenha conhecimento disso é uma das expressões e motivações mais fortes experimentadas pelos invasores: poder realizar ações criminosas, graças ao possível anonimato ou à total falta de rastreabilidade (Kardile, 2017).


Os aspetos atuais da criminalidade digital, como i) o máximo de anonimato com o mínimo de provas, ii) a máxima ambiguidade jurídica com o mínimo de conhecimentos tecnológicos disponíveis e iii) a máxima eficácia de suas ações com o mínimo de esforço, estabelecem uma economia do cibercrime que permite o desenvolvimento de capacidades técnicas, sociais e de inteligência sofisticadas o suficiente para aumentar o nível de incerteza nos indivíduos, nas organizações e nos países, e motiva ações ilegais lucrativas que podem passar despercebidas pelas autoridades oficiais (Interpol, 2020).

Antes de uma pessoa ou organização se tornar vítima de ransomware, ela deve considerar suas estratégias de ação para estabelecer com clareza e visão holística a resposta mais apropriada no intuito de limitar o máximo possível os efeitos adversos dessa condição. Para isso se faz necessária a aplicação de boas práticas e a manutenção permanente de exercícios e simulações que gerem uma "memória procedimental e prática" e favoreçam uma atuação coordenada frente à agenda do adversário, que é gerar confusão, instabilidade e incerteza na vítima.

# Apêndice

## Lista de recursos on-line disponíveis para se lidar com o ransomware

Dada a evolução acelerada do ransomware no plano internacional, detalha-se a seguir um conjunto de recursos disponíveis na internet, que podem servir de apoio e orientação para os tomadores de decisão atuarem de forma coordenada e focada em meio às tensões geradas por esse evento.

- Allianz Global Corporate & Specialty (AGCS) (2021). Ransomware trends : Risks and Resilience - https://www.agcs.allianz.com/news-and-insights/reports/cyber-risk-trends-2021.html

- Cybereason (2022). Ransomware. The True Cost to Business 2022. A Global Study on Ransomware Business Impact - https://www.cybereason.com/ransomware-the-true-cost-to-business-2022

- Institute for Security and Technology (2022). Blueprint for Ransomware. Defense. An Action Plan for Ransomware Mitigation, Response, and Recovery for Small- and Medium-sized Enterprises - https://securityandtechnology.org/wp-content/uploads/2022/08/IST-Blueprint-for-Ransomware-Defense.pdf

- ThreatPost (2021). 2021: The Evolution of Ransomware - https://media.threatpost.com/wp-content/uploads/sites/103/2021/04/19080601/0354039421fd7c82eb4e1b4a7c90f98e.pdf

- NIST (2020). Data Integrity: Recovering from Ransomware and Other Destructive Events. NIST Special Publication 1800-11 - https://www.nist.gov/news-events/news/2020/09/data-integrity-recovering-ransomware-and-other-destructive-events-nist

## Estatísticas relevantes sobre o ransomware em nível global

Numerosos relatórios internacionais demonstram os desafios e as implicações da extorsão com dados, indicando a necessidade de se avançar e especificar estratégias para identificá-la e tratá-la da forma mais adequada com vistas a limitar os danos que a sua materialização pode causar. Nesse sentido, a Gartner,[14] em seus riscos emergentes para 2022 (Cohn, 2022), coloca o surgimento de novos modelos de ransomware como a tendência mais importante a ser mantida no radar corporativo, uma vez que sua evolução permanente e a capacidade dos invasores de transformar suas práticas de extorsão alertam para novas alternativas e adaptações dessa prática.

Por outro lado, o site *Cybersecurity Ventures* (2021), em seu mais recente relatório sobre extorsão com dados, apresenta uma estatística segundo a qual, até 2031 ocorrerá um ataque de ransomware uma empresa, em um consumidor ou em um dispositivo a cada dois segundos, o que implica uma aceleração em relação aos 11 segundos calculados em 2021. Esses dados representam um exercício de alerta e vigilância permanente que, correlacionado com a constatação da Gartner, requer um tratamento diferenciado e particular dada a elevada probabilidade de sucesso que se pode ter por conta dessa ameaça.

14 Société de recherche et de conseil en technologies de l'information basée à Stamford, Connecticut, États-Unis.

Outros relatórios recentes (Coverware, 2022) indicam vetores de ataque marcados usados por cibercriminosos, como phishing, vulnerabilidades de software (algumas conhecidas ou não corrigidas, como a associada ao WannaCry[15]) e o uso de protocolo de escritório remoto (em inglês, *Remote Desktop Protocol* (RDP)), que configuram a estratégia básica para o acesso não autorizado necessário para a implantação do código malicioso e o prosseguimento de sua execução. É importante notar que o atacante precisa da ação da vítima para iniciar o processo; portanto, na medida em que ela se torna mais resistente ao chamariz, mais tempo o adversário terá que investir para atingir seu fim.

Quando uma organização é vítima de ransomware, seus efeitos diretos se enquadram em pelo menos cinco temas (SpyCloud, 2022):

- Exposição de dados proprietários ou sensíveis
- Danos à reputação
- Alto esforço na recuperação e restauração das operações
- Perda de clientes ou satisfação por falhas operacionais
- Interrupção de serviços/infraestrutura crítica

Seja qual for o impacto que as organizações venham a sofrer, elas ficam expostas e afetadas na confiança do cliente, criando uma espiral de perda de credibilidade e controle que acabará impactando a dinâmica da entidade e suas iniciativas digitais no médio e no longo prazo.

Recentemente, foi relatada na América Latina e no Caribe uma importante atividade de exfiltração[16] e extorsão[17] com dados em nome de dois grupos particulares chamados "Guacamaya" e "Conti". Esses grupos, embora tenham objetivos e métodos diferentes, criaram instabilidade e perdas financeiras em muitos países da região. Suas ações, dirigidas contra entidades governamentais, entidades de defesa nacional, infraestruturas críticas e empresas do setor de mineração de energia respondem por uma agenda agressiva que busca, não apenas atrair a atenção, mas também realizar negócios lucrativos de extorsão para aumentar suas capacidades e lucros econômicos.

> Até 2031, ocorrerá um ataque de ransomware em uma empresa, consumidor ou dispositivo a cada dois segundos, em comparação com os 11 segundos calculados em 2021.

15 Une vulnérabilité dans l'implémentation du protocole Server Message Block (SMB) de Microsoft est exploitée. Server Message Block (SMB) est un protocole réseau qui permet le partage de fichiers, d'imprimantes, etc., entre les terminaux d'un réseau d'ordinateurs utilisant le système d'exploitation Microsoft Windows. Source: https://www.avast.com/es-es/c-eternalblue

16 Ver a seção de definições.

17 Sequestro de dados ou informações para os quais um resgate é solicitado, geralmente com pagamento em criptomoedas.

## Anatomia de um ransomware: Nível de explorabilidade e etapas-chave

Do ponto de vista prático, a extorsão com dados requer a compreensão do nível de explorabilidade que a organização-alvo tem diante dessa ameaça. Isso significa conhecer e identificar (Stallings, 2019):

- **Vetor de ataque:** proximidade do invasor ao componente vulnerável
- **Complexidade do ataque:** dificuldade necessária para um invasor explorar uma vulnerabilidade uma vez identificado o componente-alvo
- **Privilégios requeridos:** para acessar, o invasor precisa explorar uma vulnerabilidade
- **Interação do usuário:** indicativo de se um usuário que não seja o invasor deve participar para o ataque ser bem-sucedido

Neste sentido, para que a extorsão de dados seja bem-sucedida, é necessário que a pessoa participe diretamente, ou seja, que um indivíduo realize uma ação específica em seu computador ou dispositivo, como um clique em um link malicioso (ver seção de definições), a fim de se ter um pivô básico onde iniciar as três principais etapas para a concretização da referida ameaça (Figura N° 1)

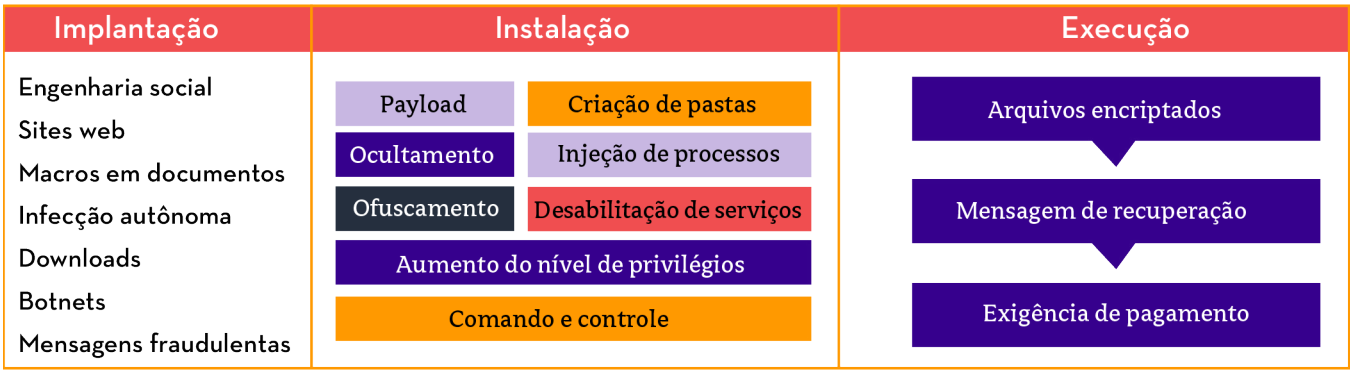



Figura 1. Anatomia de um ransomware (elaboração própria com ideias de Osorio et al., 2020)

O primeiro momento é a *implantação*, processo que se realiza por meio do esforço planejado e desenhado pelo atacante e que se inicia com a inteligência sobre as informações do indivíduo ou da comunidade-alvo para especificar os interesses e as questões relevantes na dinâmica social das possíveis vítimas. Em seguida, desenvolve-se o chamariz crível e confiável, que leva as pessoas a acessarem um site, baixarem documentos e lerem mensagens fraudulentas sem perceber o que estão fazendo. Por fim, a distração, que é o uso da perda de atenção pelas pessoas para realizar a ação que dá início ao download ou acesso do código malicioso ao celular, laptop ou computador desktop.

Após o download do malware, a *instalação* do ransomware será iniciada. É ativada a "carga útil" que aciona uma série de eventos de forma oculta no dispositivo, como a criação de pastas, ocultação e ofuscação de código malicioso, aumento do nível de privilégios no sistema de destino, injeção de processos que imitam o processo padrão do sistema operacional, desativação de serviços de monitoramento e proteção para, finalmente, preparar o sistema comprometido para a obtenção do comando e controle totais.

Após essa etapa, em que o dispositivo foi preparado para controle e manuseio pelo adversário, geralmente duas atividades ocorrem ao mesmo tempo. Inicia-se a exfiltração dos dados sensíveis que o adversário conseguiu obter e, posteriormente, a sua criptografia[18] no dispositivo, que é desenvolvida com algoritmos executados em paralelo para se alcançar a máxima eficiência no processo. Concluído esse passo, é gerada a mensagem de alerta sobre a nova condição da máquina e o pedido de pagamento para a recuperação das informações comprometidas.

A literatura estabelece pelo menos quatro tipos de extorsão que os invasores poderão desenvolver depois que os dados forem comprometidos (MunichRe, 2022):

- **Extorsão simples:** pedido de pagamento para devolver dados criptografados
- **Extorsão dupla:** roubo e ameaça de publicação de dados
- **Extorsão tripla:** ameaça de lançar um ataque de negação de serviço distribuído contra a vítima em caso de inadimplência de um pagamento
- **Extorsão quádrupla:** atacar os fornecedores, a cadeia de suprimentos e os clientes da vítima para expandir e promover a pressão pelo pagamento

Como esse tipo de atividade ilícita é um negócio altamente lucrativo, que gera a média de um bilhão de dólares por ano (Chainalysis, 2022), os ganhos econômicos de tal extorsão se baseiam em três aspectos fundamentais (Falco & Rosenbach, 2022, p. 24):

1. Tirar partido da venda de dados roubados a terceiros interessados
2. Ameaçar as organizações com o lançamento de um ataque cibernético ou com o vazamento de informações confidenciais
3. Pedir resgate impedindo a organização de acessar seus dados enquanto a extorsão não for paga

Seja qual for o tipo de extorsão que ocorra, a instituição terá pressões e exigências que a levarão a ser responsabilizada pelas consequências geradas em seus grupos de interesse e, ao mesmo tempo, reconhecerá as condições e capacidades do adversário para pôr em pratica a ameaça e alcançar seus propósitos: extorsão e/ou exfiltração.

Os ganhos econômicos do ransomware se baseiam em três aspectos fundamentais:
- Aproveitar a venda de dados roubados a terceiros interessados;
- Ameaçar as organizações com o lançamento de um ataque cibernético ou com o vazamento de informações confidenciais;
- Pedir resgate impedindo a organização de acessar seus dados enquanto não pagar a extorsão.

18 Criptografia das informações feitas pelo adversário para impedir que seu proprietário tenha acesso a elas.

# Referências


Abrams, L. (2022). Conti ransomware finally shuts down data leak, negotiation sites. *Bleepingcomputer*. https://www.bleepingcomputer.com/news/security/conti-ransomware-finally-shuts-down-data-leak-negotiation-sites/

Baykara, M. & Sekin, B. (2018). A novel approach to ransomware: Designing a safe zone system. *2018 6th International Symposium on Digital Forensic and Security* (ISDFS), Antalya. 1-5. Doi: 10.1109/ISDFS.2018.8355317

Burgess, M. (2022). The Workaday Life of the World's Most Dangerous Ransomware Gang. *Wired*. https://www.wired.co.uk/article/conti-leaks-ransomware-work-life

Cano, J. (2020). Modelo SOCIA. Una reflexión conceptual y práctica desde la perspectiva del adversario. *Actas X Congreso Iberoamericano de Seguridad Informática 2020*. Universidad Politécnica de Madrid - Universidad del Rosario. Enero. Doi: 10.12804/si9789587844337.09

Chainalysis (2022). The 2022 crypto crime report. https://go.chainalysis.com/2022-Crypto-Crime-Report.html

Cohn, L. (2022). The Cutting Edge: 2Q22 Cool New Data Points. *Gartner Business Quarterly. Second Quarter*. 5-8. https://www.gartner.com/en/insights/gartner-business-quarterly

Coverware (2022). Fewer Ransomware Victims Pay, as Median Ransom Falls in Q2 2022. https://www.coveware.com/blog/2022/7/27/fewer-ransomware-victims-pay-as-medium-ransom-falls-in-q2-2022

El-Kosairy, A. & Azer, M. A. (2018). Intrusion and ransomware detection system. *2018 1st International Conference on Computer Applications & Information Security* (ICCAIS), Riyadh. 1-7, Doi: 10.1109/CAIS.2018.8471688

Falco, G. & Rosenbach, E. (2022). *Confronting cyber risk. An Embedded Endurance Strategy for Cybersecurity*. New York, NY. USA: Oxford University Press.

Herrera Silva, J. A.; Barona López, L. I.; Valdivieso Caraguay, A. L. & Hernández-Álvarez, M. (2019). A Survey on Situational Awareness of Ransomware Attacks—Detection and Prevention Parameters. *Remote Sens*. 11(10). 1-20. Doi: 10.3390/rs11101168

Interpol (2020). Cybercrimen: Covid-19 Impact. August. De: https://www.interpol.int/es/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf

Kardile, A. (2017). Crypto ransomware analysis and detection using process monitor. *Master Thesis*. University of Texas, Arlington. De: http://hdl.handle.net/10106/27184

MunichRe (2022). Global Cyber Risk and Insurance Survey 2022. *Global Report*. https://www.munichre.com/landingpage/en/global-cyber-risk-and-insurance-survey-2022.html

Osorio, A., Mateus, M. & Vargas, H. (2020). Proceso para la identificación, clasificación y control del comportamiento de familias Ransomware. *Revista UIS Ingenierías*. 13(3). 131-142. doi: 10.18273/revuin.v19n3-2020013

Richard, L. (2022). "LA LUCHA POR UN TERRITORIO ES LA LUCHA DE TODAS". Forbidden Stories. https://forbiddenstories.org/es/la-lucha-por-un-territorio-es-la-lucha-de-todas/

Saydjari, O. (2018). *Engineering trustworthy systems: get cybersecurity design right the first time*. New York, USA.: McGraw Hill

Sittig, D. F., & Singh, H. (2016). A Socio-Technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks. *Applied clinical informatics*, 7(2), 624–632. Doi: 10.4338/ACI-2016-04-SOA-0064

SpyCloud (2022). Ransomware defense report. https://spycloud.com/resource/ransomware-defense-report-2022

Stallings, W. (2019). *Effective cybersecurity. A guide to using best practices and standards*. USA: Addisson Wesley.

Tavella, F. (2021). Ransomware Conti: principales características y cómo operan sus afiliados. *ESET*. https://www.welivesecurity.com/la-es/2021/11/29/ransomware-conti-principales-caracteristicas/

Vicens, A. (2022). Hacking group focused on Central America dumps 10 terabytes of military emails, files. *CyberScoop*. https://www.cyberscoop.com/central-american-hacking-group-releases-emails/

Grimes, R. (2022). *Ransomware Protection Playbook*. Hoboken, NJ. USA: John Wiley & Sons.

Leo, P., Isik, O. & Muhly, F. (2022). The Ransomware Dilemma. *Sloan Management Review*. https://sloanreview.mit.edu/article/the-ransomware-dilemma/

2023

White paper series
Publicação 10

# Desafios e estratégias:

*Considerações sobre os ataques de ransomware nas Américas*

OEA | Mais direitos para mais pessoas

aws