CG//One

CASOS DE SUCESSO

Resposta a Incidentes:

como a CG One mitigou ataques de ransomware em tempo recorde

Sumário

3	Introdução: chamadas de emergência
4	CASE 1 - Uma aula de resiliência: como a CG One mitigou um ataque de ransomware em um cliente do setor educacional em apenas 27 horas
4	O caso – linha do tempo
7	Resultado
8	CASE 2 - Linha de defesa: como a CG One restaurou a operação de uma indústria têxtil em menos de 4 dias
8	O caso – linha do tempo
10	O ataque: táticas e técnicas utilizadas pelo grupo
12	Resultado
13	A importância de contar com um parceiro preparado para tudo – incluindo ransomware e incidentes cibernéticos críticos

Introdução:
chamadas de emergência

Imagine receber uma ligação informando que os sistemas da sua empresa estão indisponíveis e os dados foram criptografados, reféns do talvez mais temido dentre os incidentes cibernéticos – o famigerado ataque de ransomware. Este foi o pesadelo vivido por dois clientes da CG One, em setores distintos: o educacional e o industrial.

Em um cenário onde tempo é dinheiro – **e ataques cibernéticos superaram prejuízos na ordem de R$ 2,3 trilhões em 2024** – cada minuto de inatividade nas operações de uma empresa pode representar enormes prejuízos financeiros, além dos danos à reputação. Por isso, a velocidade na resposta é, sem dúvida, um dos fatores mais importantes para mitigar um incidente de cibersegurança. No caso desses clientes, a rapidez e a precisão da nossa intervenção foram cruciais para evitar perdas significativas e garantir a continuidade dos negócios.

Este documento vai apresentar, em detalhes, como a CG One atuou para mitigar os ataques de ransomware enfrentados pelos nossos clientes, destacando as estratégias e soluções empregadas para mitigar as ameaças em tempo recorde.

CASE 1 – Uma aula de resiliência: como a CG One mitigou um ataque de ransomware em um cliente do setor educacional em apenas 27 horas

Quando um cliente do setor educacional sofreu um ataque de ransomware, ele se viu diante de um cenário crítico: sistemas indisponíveis, dados criptografados e a ameaça de grandes prejuízos financeiros e reputacionais. Foi nesse momento que a CG One entrou em ação. Com uma resposta ágil e coordenada, a equipe isolou e restaurou as máquinas infectadas em apenas 27 horas após o chamado inicial do cliente. Em somente três dias, todo o processo de recuperação e mitigação estava completo, permitindo ao cliente retomar suas atividades sem os prejuízos devastadores que costumam acompanhar ataques desse tipo. Levando em consideração que o tempo médio de inatividade em consequência de um ataque é de 21 dias, **segundo dados divulgados pela McKinsey**, nosso cliente se recuperou cerca de sete vezes mais rápido que o habitual nesse tipo de ataque - graças a uma atuação conjunta muito bem orquestrada e executada.

O caso - linha do tempo

Domingo

16h21 - Alerta máximo
Recebemos o chamado do cliente relatando o ataque de ransomware. A situação exigia uma resposta rápida e uma consultoria avançada. O relógio começa a correr.

16h32 – Equipe mobilizada
Em apenas 11 minutos, mobilizamos nossa equipe especializada para atender o cliente. Especialistas escalados e prontos para agir.

16h33 - A "War Room" é ativada
Em um ambiente virtual seguro, iniciamos a coordenação estratégica, definindo os próximos passos e analisando a extensão do ataque. Cada segundo conta.

17h20 - O time de resposta a incidentes da CG One entra em ação
Nossa equipe foi composta por especialistas de diversas áreas. Com foco total na missão, eles iniciam o processo de isolamento das máquinas infectadas para impedir a propagação do ataque.

17h37 - Nosso parceiro tecnológico Akamai entra no jogo
Após uma análise criteriosa do cenário e das necessidades do cliente, identificamos que a solução Guardicore, da Akamai, seria essencial para a contenção do ataque, atuando como uma peça chave na estratégia de resposta ao incidente.

O Guardicore, uma tecnologia de micros-segmentação, foi essencial para controlar a propagação do ransomware dentro da rede do cliente. Ao aplicar políticas de segmentação, a solução isolou rapidamente as áreas infectadas, impedindo que o malware se espalhasse para outros sistemas críticos. Esse nível de controle granular proporcionou visibilidade detalhada e controle sobre o tráfego lateral, reduzindo drasticamente a superfície de ataque e facilitando a contenção.

Segunda-feira

7h00 – Início intensivo da restauração de sistemas críticos.
Ao longo do dia, nossa equipe focou na reativação de:

- *20 servidores*
- *150 desktops*
- *Três máquinas, consideradas de missão crítica, precisavam permanecer em operação contínua, exigindo uma abordagem de recuperação ainda mais cuidadosa.*

20h40 - Finalizado com sucesso o processo de restauração completo das máquinas comprometidas.
Cerca de 27 horas desde a primeira ligação recebida pela CG One, o cliente pôde retomar suas operações de maneira 100% estabilizada.

Quarta-feira

Conclusão completa do processo com a mitigação total do ransomware, a restauração completa do ambiente à normalidade e as aplicações das proteções adequadas.
Ao longo do processo, foram aplicadas mais de:

- *79 regras de segurança*
- *19 etiquetas para segmentação e classificação*
- *Análise e categorização de mais de 700 ativos*

Esse esforço garantiu uma estrutura robusta, fortalecida contra futuras ameaças, e proporcionou ao cliente uma visão clara e segmentada de seus recursos críticos.

Resultado

Em tempo recorde – apenas três dias após ser acionada - a CG One conseguiu não apenas conter o ataque de ransomware, mas também restaurar completamente o ambiente do cliente, protegendo sua operação e ativos. Todo o trabalho foi realizado sem qualquer interrupção significativa nos sistemas críticos, garantindo que as atividades essenciais pudessem seguir normalmente.

Graças à rapidez e precisão na resposta, o cliente não sofreu danos e impactos à imagem de sua marca — uma conquista rara em casos de ataques cibernéticos dessa magnitude. Este case reforça a importância de contar com especialistas preparados, capazes de atuar com agilidade e inteligência estratégica para garantir uma recuperação segura e completa.

CASE 2 - Linha de defesa: como a CG One restaurou a operação de uma indústria têxtil em menos de 4 dias

Nesse segundo caso, uma indústria têxtil enfrentou um ataque de ransomware que comprometeu seus sistemas críticos, colocando a operação da empresa em risco. A CG One foi acionada para restaurar a operação e proteger os dados essenciais, mas o desafio era grande: a empresa enfrentava a interrupção de seus sistemas críticos, com o risco de paralisar a produção e causar impactos financeiros significativos. Em menos de quatro dias, também em um tempo recorde, nossa equipe conseguiu mitigar os danos, isolar as ameaças e restaurar a operação da indústria, permitindo que as atividades voltassem ao normal com a mínima interrupção e sem comprometer os dados.

O caso - linha do tempo

Quinta-feira: o primeiro contato

15h38 – Detecção da crise:
Recebemos o chamado urgente sobre um ataque de ransomware que comprometia operações críticas de uma indústria têxtil.

16h00 – Resposta imediata:
Em apenas 22 minutos, a equipe da CG One iniciou o atendimento, priorizando a contenção rápida para evitar a propagação do malware.

17h12 – Mobilização do time de resposta a incidentes:
O time de RI da CG One foi escalado, entrando em ação para avaliar o nível de comprometimento e formular o plano inicial de mitigação.

Sexta-feira: isolando a ameaça

07h às 22h (15 horas) - Iniciamos a restauração e o isolamento das máquinas infectadas para interromper o avanço do ransomware.

- *Ajustes nos firewalls: Reconfiguramos os firewalls para bloquear acessos não autorizados e evitar a movimentação lateral do malware.*
- *Correção de problemas de roteamento: Garantimos que o tráfego de rede fosse redirecionado de forma segura, evitando caminhos comprometidos.*
- *Criação de labels e instalação do Guardicore: a tecnologia de microssegmentação Guardicore novamente se mostrou crucial para conter o avanço da ameaça. Ao identificar rapidamente os pontos de comprometimento, aplicamos políticas precisas de segmentação, isolando as máquinas afetadas e protegendo os sistemas essenciais para a operação.*

Sábado: reconstruindo a infraestrutura

09h às 22h (13 horas) - Continuamos os esforços para reestabelecer a operação à normalidade e fortalecer as defesas da rede.

- *Restabelecimento da SD-WAN: recuperamos a conectividade para a continuidade operacional.*
- *Atualização do EMS: Asseguramos que os sistemas de gerenciamento estivessem atualizados para impedir vulnerabilidades exploradas pelo ransomware.*
- *Configuração de VPN para servidor IMP: Restabelecemos conexões seguras para o servidor, essencial para manter processos em andamento.*

Domingo: produção recuperada

07h às 17h53 (11 horas) - Finalizamos a restauração e o isolamento das máquinas infectadas, garantindo a segurança e integridade dos sistemas.

- *Ambiente de produção em operação: a empresa retomou suas atividades sem perda de dados críticos.*
- *Mais de 40 servidores e 500 estações monitoradas: garantimos o acompanhamento contínuo dos ativos para evitar reinfecções e reforçar a resiliência contra novos ataques.*

O ataque:
táticas e técnicas utilizadas pelo grupo

O grupo: Inc. Ransomware

O Inc. Ransomware é uma operação de extorsão digital que surgiu em julho de 2023. É um grupo cibercriminoso focado em ataques direcionados contra grandes organizações e empresas corporativas. Eles utilizam uma combinação de vetores de ataque, incluindo exploração de vulnerabilidades, campanhas de spear-phishing e implantação de ransomware.

Métodos de Ataque (MITRE ATT&CK®)

O modus operandi do Inc. Ransom segue uma trajetória comum para invadir sistemas corporativos. **De acordo com dados de mercado**, as principais técnicas e táticas utilizadas pelo grupo são:

1. Acesso Inicial

- **Compra de credenciais válidas:** O Inc. Ransomware frequentemente utiliza credenciais adquiridas de Initial Access Brokers para acessar sistemas comprometidos.
- **Phishing (T1566):** O grupo realiza campanhas de phishing visando obter credenciais ou instalar malware em dispositivos das vítimas.
- **Exploração de vulnerabilidades (T1190):** Em novembro de 2023, o grupo explorou a vulnerabilidade CVE-2023-3519 no Citrix NetScaler para comprometer dispositivos de rede corporativos.

2. Evasão de defesas

- **Uso de ferramentas de terminação de processos (T1562.001):** Utilizam ferramentas como HackTool.ProcTerminator e ProcessHacker para encerrar processos e serviços, evitando detecção por soluções de segurança.

3. Acesso a credenciais

- **Dumping de credenciais (T1003):** Ferramentas são empregadas para capturar credenciais armazenadas em soluções de backup.

4. Discovery

- **Escaneamento de rede (T1046):** O grupo utiliza ferramentas como NetScan e Advanced IP Scanner para mapear a rede e identificar dispositivos e serviços vulneráveis.
- **Inspeção de arquivos com ferramentas legítimas (T1083):** Ferramentas padrão como Notepad, Wordpad e Paint são usadas para examinar dados e documentos sem levantar suspeitas.
- **Ferramentas adicionais para reconhecimento (T1580):** O grupo baixa ferramentas como Mimikatz para coleta de informações adicionais.

5. Movimentação Lateral

- **Ferramentas de administração remota (T1021.001):** Utilizam PSexec, AnyDesk e TightVNC para se mover lateralmente pela rede e comprometer outros sistemas.

6. Impacto

- **Exfiltração de dados (T1560.001):** Os dados são compactados com 7-Zip antes da exfiltração para serviços como MegaSync.
- **Criptografia de arquivos (T1486):** O ransomware utiliza o algoritmo AES para criptografia dos dados e arquivos.

Resultado

A CG One não apenas enfrentou o ataque de ransomware em menos de quatro dias, mas garantiu a completa restauração da operação da indústria, com mínimos prejuízos financeiros e sem impactos para a marca. A resposta foi ágil e precisa, com o isolamento e a recuperação das máquinas infectadas realizados de maneira eficaz, permitindo que a produção continuasse sem grandes interrupções nos processos críticos.

A empresa, que estava à beira de uma paralisação prolongada, conseguiu não apenas se recuperar rapidamente, mas também fortalecer sua infraestrutura contra ameaças futuras.

A importância de contar com um parceiro preparado para tudo – incluindo ransomware e incidentes cibernéticos críticos

No cenário atual de ameaças cibernéticas, um ataque pode acontecer a qualquer momento e com impactos devastadores. Ransomware, vazamentos de dados e outros incidentes de segurança cibernética não são mais uma questão de "se", mas "quando" vão acontecer.

NÃO TEMA A AMEAÇA. ESTEJA PREPARADO PARA LIDAR COM ELA.

Ter ao seu lado um fornecedor maduro e disponível para tudo – especialmente para ajudar a sua empresa a se preparar, bem como para responder a incidentes cibernéticos – é o que fará a diferença entre uma crise controlada rapidamente, e um prejuízo que pode ser irreparável.

Um parceiro experiente oferece:

- Agilidade para atuar nos momentos críticos;
- Expertise para conter a ameaça e minimizar danos;
- Confiança para restaurar suas operações com segurança;
- Amplo portfólio alinhado ao NIST® Cybersecurity Framework, com soluções best of breed do mercado;
- Robustez técnica obtida com mais de 4 décadas de atuação no mercado de tecnologia.

CG//One

Sua empresa está pronta para o inesperado?

Escolher o fornecedor certo hoje pode ser o fator decisivo para proteger seu negócio amanhã.

Sobre a CG One

Somos a evolução da marca Compugraf. Com mais de 40 anos de expertise no mercado de tecnologia, somos especializados em segurança cibernética para todo o ecossistema digital das empresas.

Desenvolvemos e gerenciamos soluções de Segurança da Informação, Proteção de Redes e Gerenciamento Integrado de Riscos, e nosso portfólio é orientado de acordo com as práticas e os padrões de segurança do NIST® Cybersecurity Framework.

Contamos com um time qualificado e certificado que já proporcionou operações seguras para mais de 500 empresas de diversos portes e setores, em todo o Brasil.