LogRhythm®

A Empresa de Inteligência de Segurança

COMO O RANSOMWARE FUNCIONA

Ransomware está ganhando força!
Nos últimos três anos, o ransomware saltou aos holofotes do cenário de ameaças cibernéticas. O FBI estima que os ataques ransomware renderam mais de $1B em 2016.[1]

O que é um ransomware?
Ransomware é um software malicioso que permite a um hacker restringir o acesso a uma informação vital da empresa ou do indivíduo e depois exige alguma forma de pagamento (geralmente Bitcoins) para suspender a restrição.

209 milhões Valor pago no 1º trimestre de 2016 aos cibercriminosos usando o ransomware[1]

1 bilhão Estimativa do FBI para perdas a serem incorridas em 2016 devido ao ransomware[1]

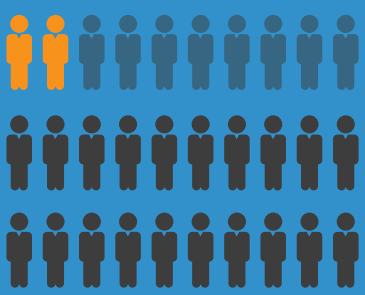
Tempo da infecção inicial até um pedido de resgate

$ 10–$ 50 milhões
Renda mensal estimada dos cibercriminosos a partir do ransomware[3]

72%
Porcentagem das empresas afetadas pelo ransomware que não puderam acessar os dados por pelo menos 2 dias após a ataque[4]

32%
Porcentagem que perdeu o acesso aos seus dados por 5 dias ou mais[4]

86%
Ataques que afetaram **2** ou mais trabalhadores[4]



47%
Ataques que afetaram mais de **20** trabalhadores[4]

$ 17,000
Valor pago pelo Centro Médico Presbiteriano de Hollywood em 2016 para desbloquear arquivos e voltar aos negócios como de costume[5]

$ 100,000
Montante que o hospital estava perdendo **POR DIA** pela incapacidade de realizar tomografias de pacientes[5]

[1]CNN-Money, http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/, 15 de abril de 2016
[2]Security Magazine (Revista de Segurança), "Os ataques 'ransomware' aumentam em 2016", 23 de novembro de 2016
[3]David Common, CBC News, "Ransomware: O que você precisa saber", 11 de março de 2015
[4]Post no blog Intermedia: "Se o ransomware atacar seus negócios, você estará preparado? Nossas novas conclusões sobre o estudo podem surpreendê-lo.", 17 de março de 2016
[5]PYMNTS.com, "City Held Hostage – Via bitcoin ransomware", 22 de março de 2016

AS 5 FASES
de um ataque ransomware

Existem 5 fases distintas de um ataque ransomware. Entender o que acontece em cada fase e reconhecer os indicadores de compromisso (IOCs) pode aumentar a probabilidade de se defender com sucesso contra, ou pelo menos mitigar os efeitos de, um ataque.

A cronologia de um ataque é muito comprimida. Muitas vezes você tem apenas 15 minutos de exploração e infecção até receber a nota de resgate. Reconhecer os primeiros indicadores é fundamental para seu sucesso em parar um ataque.

1

Fase 1: Exploração e infecção (T -00:00)

Para que um ataque seja bem sucedido, o arquivo ransomware malicioso precisa ser executado em um computador. Isso é frequentemente feito através de um e-mail de phishing ou um exploit kit. No caso do malware CryptoLocker, o Angler Exploit Kit é um método preferível para obter a execução.

2

Fase 2: Entrega e execução (T -00:05)

Durante esta fase, os executáveis ransomware atuais são enviados ao sistema da vítima. Após a execução, mecanismos de persistência são colocados em prática.

3

Fase 3: Espoliação de backup (T -00:10)

Alguns segundos depois, o ransomware tem como alvo as pastas e os arquivos de backup no sistema da vítima e os remove para evitar a restauração do backup. Isso é exclusivo do ransomware–outros tipos de crimeware não se preocupam em excluir arquivos de backup.

4

Fase 4: Criptografia de arquivos (T -02:00)

Assim que os backups forem completamente removidos, o malware executará uma troca de chaves seguras com o servidor de comando e controle (C2), estabelecendo essas chaves de criptografia que serão usadas no sistema local.

5

Fase 5: Limpeza e notificação de usuário (T -15:00)

Com os arquivos de backup removidos e o trabalho sujo de criptografia feito, são apresentadas instruções para extorsão e pagamento. Muitas vezes, a vítima tem alguns dias para pagar. Após esse tempo, o resgate aumenta.

Finalmente, como as gravações Mission Impossible que se autodestroem, o malware se limpa do sistema, de modo a não deixar provas forenses significativas que ajudariam a criar melhores defesas contra o malware.

Os ataques ransomware estão apenas começando a se intensificar. Como esses ataques são muito lucrativos para os criminosos, eles certamente se tornarão mais comuns, mais prejudiciais e mais caros.

O sucesso da sua organização na defesa contra um ataque ransomware é largamente dependente do seu nível de preparação e das ferramentas que você implanta para monitorar que seus sistemas detectem, respondam e neutralizem a atividade suspeita.

Saiba como você pode rapidamente detectar e neutralizar um ataque ransomware em **https://logrhythm.com/the-ransomware-threat-ebook/**

LogRhythm®

A Empresa de Inteligência de Segurança