Guia de Resposta a Ransomware

SERVIÇOS DE RESPOSTA IBM A INCIDENTES

DATA DA LIBERAÇÃO: MAIO DE 2016

IBM

Copyright

As metodologias e os processos usados na condução deste compromisso são considerados propriedade intelectual da IBM e não podem ser divulgados sem permissão por escrito da mesma. A IBM autoriza a cópia deste relatório pelo cliente para o propósito de divulgar as informações dentro da organização ou de qualquer agência regulatória.

Renúncia de Responsabilidade

Novas tecnologias, mudanças na configuração, upgrades de software e manutenção de rotina, entre outros itens, podem criar riscos de segurança novos e desconhecidos. Além disso, “hackers” de computador e outros terceiros continuam a empregar técnicas e ferramentas cada vez mais sofisticadas, que resultam em desafios cada vez maiores para a segurança do sistema de TI e redes. O Relatório e as recomendações aqui contidas não constituem nenhuma declaração ou garantia da IBM sobre a segurança dos sistemas de computador e/ou de rede de uma empresa, incluindo, sem limitação, qualquer indicação de que os sistemas de tecnologia da empresa estejam protegidos contra intrusões, vírus ou quaisquer outros riscos de segurança.

Índice

Resumo Executivo

Contexto

Se no momento você estiver experimentando um incidente de ransomware, revise imediatamente a seção de restrição na página 17.

O documento é considerado um guia para as organizações que enfrentam uma infecção por ransomware[1]. Este guia é dividido em várias seções, com a mais crítica e urgente estando na seção de resposta inicial. **Se você estiver experimentando um incidente de ransomware no momento, é altamente recomendável revisar imediatamente a seção de restrição abaixo** e retornar a essa seção posteriormente para ter uma noção geral sobre ransomware.

Para o propósito deste guia, os termos 'versão' e 'variante' são usados com significados diferentes. O termo versão se refere ao mesmo programa de malware que inclui versões mais novas ou mais antigas do mesmo programa com recursos variados. O termo variante é usado para descrever uma 'família' de ransomware. Por exemplo, há diferentes variantes de ransomware que criptografam os arquivos de um usuário e, em seguida, exigem um resgate. Essas variantes geralmente são criadas por pessoas diferentes, conhecidas por nomes diferentes pelas empresas de antivírus e funcionam de modo diferente com o mesmo objetivo..

Nos últimos meses, a organização de Serviços de Resposta a Emergências, da IBM, tem percebido um aumento no número de clientes que relataram ser vítimas de ransomware. O ransomware geralmente é recebido pela vítima por meio de um e-mail não solicitado de um remetente desconhecido como um anexo e/ou injetado na sessão do navegador do usuário por meio de uma vulnerabilidade do navegador da web, como muitas das recentes vulnerabilidades do Adobe Flash que foram publicadas em 2015[2]. No início de 2016, uma nova abordagem foi usada para implementar outra variante de ransomware; ela é conhecida como SamSam ou SamAs. Essa nova ameaça usa vulnerabilidades conhecidas (principalmente no JBoss atualmente). Essas vulnerabilidades são exploradas por agentes de ameaça que usam ferramentas para comprometer sistemas e plantar "webshells" ou "backdoors" (cavalos de Tróia de acesso remoto (RATs)) para permitir maior comprometimento dos sistemas e da infraestrutura de rede da vítima. Uma vez que isso é conseguido, a carga útil/o pacote do ransomware é implementado em todos os sistemas Windows de destino. O hacker usa PSEXEC para prover o ransomware para cada sistema de destino. Assim que ele é entregue, inicia-se a criptografia de arquivos que correspondem à lista de 'correspondências'.

1 ***https://en.wikipedia.org/wiki/Ransomware*** — "um tipo de software malicioso desenvolvido para bloquear o acesso a um sistema de computador até que uma quantia em dinheiro seja paga."

2 ***https://helpx.adobe.com/security.html#flashplayer***

Desde o início de 2016, há inúmeras variantes diferentes de ransomware em uso. Alguns são muito eficientes e bem-sucedidos em tornar arquivos inacessíveis até que o resgate seja pago, enquanto outras variantes tentam alcançar o mesmo objetivo, mas implementam o processo de criptografia de modo ineficiente. Dependendo da variante e da versão do ransomware, essa implementação ineficiente pode permitir que um usuário decriptografe seus arquivos sem pagar um resgate.

No entanto, isso tem se tornado menos provável uma vez que a técnica de implementação e de gerenciamento de chave tem melhorado significativamente.

Quando um computador é infectado com ransomware, o malware geralmente gera uma quantidade muito pequena de tráfego de rede externo. Durante a infecção, a maioria das versões/variantes de ransomware utiliza um Algoritmo de Geração de Domínio (DGA)[3] para randomizar a solicitação de DNS feita ao servidor de comando e controle (C&C). Isso torna a geração da lista de bloqueio dos domínios conhecidos muito mais difícil pois o malware usará o DGA para gerar milhares de nomes de domínios randomizados, onde um domínio legítimo pode ser usado para conectar-se ao servidor C&C. Esse contato inicial com o servidor C&C serve para registrar o computador no servidor C&C e para obter as chaves de criptografia públicas que ele usa para criptografar todos os arquivos do usuário. Portanto, um dump de memória ou uma captura de tráfego de rede ajudará muito pouco na obtenção das informações necessárias para restaurar os arquivos, pois a chave privada necessária para decriptografar os arquivos não existirá no computador da vítima.

No caso do SamSam, não há troca de chave, pois a chave pública (usada para criptografar arquivos) está incluída no pacote implementado. No entanto, como o SamSam é introduzido via atividades de hackeamento tradicionais, outros indicadores de comprometimento devem ficar visíveis e aplicáveis.

3 ***https://en.wikipedia.org/wiki/DGA***

A maioria dos ransomwares visa arquivos comuns criados e utilizados pelos usuários, não arquivos do sistema operacional.

A maioria dos ransomwares visa arquivos comuns criados e utilizados pelos usuários, não arquivos do sistema operacional. Os arquivos de destino variam entre variantes de ransomware e, em alguns casos, em diferentes versões da mesma variante de ransomware, mas eles geralmente incluem, mas não estão limitados a:

- Arquivos Microsoft Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx, .rtf)
- Arquivos Open Office (.odt, .ods, .odp)
- Arquivos Adobe PDF
- Arquivos de imagem populares (.JPG, .PNG, arquivos de câmera raw, etc.)
- Arquivos de texto (.txt, .RTF, etc.)
- Arquivo de banco de dados (.sql, .dba, .mdb, .odb,. db3, .sqlite3, etc.)
- Arquivo compactado (.zip, .rar, .7z, etc.)
- Arquivos de correio (.pst)
- Arquivos de chave (.pem, .crt, etc.)

Para demonstrar a amplitude dos arquivos criptografados por uma variante de ransomware, mais de 150 extensões diferentes são destinadas à criptografia. Dependendo da variante e da versão do ransomware, extensões de arquivo adicionais podem ser atingidas.

A decisão de pagar um resgate na esperança de obter os dados de volta é complicada. A IBM não defende a posição de pagar um resgate para decriptografar os arquivos. Qualquer decisão de pagar um resgate deve ser baseada em uma análise do risco em comparação ao benefício e com o entendimento de que, embora muitos usuários tenham relatado êxito em obter seus arquivos de volta após o pagamento de um resgate, não há garantias de que uma organização receberá as chaves necessárias para decriptografar os arquivos afetados caso o resgate seja pago. A IBM recomenda que uma organização primeiro considere sua infraestrutura de backup interna como uma maneira de recuperar arquivos importantes antes de pagar um resgate. Se os backups não estiverem disponíveis, as partes interessadas relevantes dentro da organização deverão estar envolvidas em qualquer decisão de pagar um resgate.

O grande sucesso do ransomware se deve em grande parte ao fato de que o ransomware não requer privilégios administrativos como outro malware. Em vez disso, ele se vale especificamente das permissões que uma vítima tem em seu computador designado e dentro de uma organização para criptografar os arquivos aos quais o usuário específico tem acesso, localmente ou em seu próprio computador e/ou na rede da organização nos servidores de compartilhamento de arquivos corporativos.

Ciclo de Vida do Incidente

Este documento descreve a resposta a um incidente de ransomware usando o Ciclo de Vida de Resposta a Incidentes do National Institute of Standards and Technology (NIST), conforme descrito no Guia de Manipulação de Incidentes de Segurança do Computador do NIST.[4]

Figua 1. Ciclo de Vida de Resposta a Incidentes

Preparação

Esta fase envolve preparar uma organização para os tipos de eventos e incidentes que ela irá encontrar. O detalhamento de todos os aspectos de uma resposta a incidente vai além do propósito deste documento, mas as recomendações a seguir são fornecidas como etapas que uma organização pode executar para ajudar a se preparar e evitar um incidente de ransomware. Devido à rápida evolução do ransomware, a IBM observa que a fase de preparação do Ciclo de Vida de Resposta a Incidentes do NIST é a mais importante. Quando os arquivos de ransomware maliciosos forem detectados, provavelmente será tarde e seus arquivos já terão sido criptografados. É importante utilizar uma estratégia abrangente de defesa; vários pontos preparatórios são essenciais para combater o ransomware e assegurar que ele nunca tenha a oportunidade de infectar seu ambiente.

4 ***http://www.nist.gov/customcf/get_pdf.cfm?pub_id=911736***

TREINAMENTO DO USUÁRIO FINAL

A educação e o treinamento proativos do usuário final continuam sendo essenciais para ajudar a evitar incidentes de ransomware e malware em geral, uma vez que não é incomum que usuários finais sejam os primeiros a encontrar incidentes de segurança. Por causa disso, é altamente recomendável realizar o treinamento periódico dos usuários finais sobre os tipos de ameaças que provavelmente encontrarão e quais ações eles devem ou não tomar em um sistema de informações enquanto realizam seus trabalhos. No final das contas, uma força de trabalho consciente da segurança é um ativo cultural raro que serve como um multiplicador econômico para a postura de segurança da organização.

RECONHECENDO UM EVENTO DE RANSOMWARE

Quando executado, o ransomware cria vários indicadores de que um sistema da informação foi comprometido (consulte a seção Detecção). Os usuários finais devem saber como e quem contatar para relatar rapidamente essas anomalias. Por exemplo, se um funcionário se deparar com um arquivo que foi criptografado por ransomware, ou se um arquivo HTML/TXT foi deixado para informar as instruções de pagamento ao usuário, esse funcionário foi educado sobre o comportamento do ransomware, sobre o significado da mensagem e sobre quem avisar imediatamente para ajudar a minimizar o impacto geral na organização? Se os usuários finais não conseguirem reconhecer um evento de segurança e relatá-lo por meio dos canais adequados, a organização nunca sequer poderá reconhecer que esse evento de segurança ocorreu.

E-MAIL COMO UM VETOR DE INFECÇÃO

Considere executar exercícios periódicos de phishing simulado sem aviso prévio nos quais os usuários recebem e-mails ou anexos que simulam um comportamento malicioso. Durante essas campanhas, gerar métricas sobre o número de usuários que clicam nos anexos ou links suspeitos é essencial para demonstrar progressos. Uma campanha bem-sucedida requer a geração de um número base de usuários que clicam em anexos ou links suspeitos, seguida pela educação da força de trabalho e, então, de uma campanha de acompanhamento para quantificar o aumento do conhecimento dentro da organização.

Os formatos de arquivo comuns (extensões) usados em e-mails para anexos maliciosos incluem: ZIP, RAR, JS, PDF, DOC, XLS, CHM, HTML. Outras extensões duplas - às vezes com muito preenchimento por espaços - são usadas para ocultar o formato ‘real’ do arquivo e fazer a vítima acreditar que o arquivo é seguro para abrir. Geralmente, os anexos de e-mail que são arquivos .ZIP ou .RAR conterão arquivos .JS, .DOC, .XLS, .HTML, .PDF maliciosos.

MACROS COMO UM VETOR DE INFECÇÃO

O ransomware geralmente também é distribuído como um documento Word do Office contendo uma macro. Quando o usuário abre o documento, ele é orientado a “ativar a macro para obter mais informações”. Caso isso seja feito, a macro buscará uma carga útil adicional que poderá driblar as ferramentas de segurança tradicionais fazendo download dos dados que são criptografados e, em seguida, decriptografando-os no computador infectado, evitando, assim, a inspeção da ferramenta de segurança durante a transição. Distribuir malware via macros é uma técnica muito antiga, datada de meados de 1990 que, provavelmente, muitos programas de segurança não tratam por não terem sido populares durante anos. Este método de ataque antigo e a falta de conhecimento pelos usuários podem levá-los a ativar uma macro em um documento do Office protegido simplesmente porque eles não entendem os riscos envolvidos e não foram informados dos perigos.

SEPARE/PROÍBA ANEXOS COM EXECUTÁVEIS A PARTIR DO E-MAIL

A maioria das organizações configura seus servidores de e-mail para proibir o envio ou o recebimento de e-mails com arquivos executáveis como um anexo. Também é muito comum que hackers enviem um e-mail com um anexo de archive ZIP contendo malware executável. As organizações geralmente configuram seus gateways de e-mail para varrer dentro do anexo de archive ZIP, mas não para separar/remover os executáveis. Se a varredura antivírus não detectar o executável como uma ameaça, eventualmente ela o fará na caixa de correio ou no terminal do usuário.

Quando possível, é recomendável configurar o servidor de e-mail para separar qualquer arquivo executável, incluindo arquivos dentro de archives (que não são protegidos por senha) que tenham uma extensão EXE, COM ou SCR e, desde 2016, considerar também a separação de extensões .JS. Esses arquivos devem ser separados antes de permitir a entrega na caixa de correio do usuário.

Dependendo de quais ferramentas de segurança estão ativas na organização, esta também pode considerar colocar os anexos do documento do Office que contêm macros em quarentena automaticamente, porque esse também é um método de distribuição comum. Algumas organizações têm realizado essa etapa de um modo mais rigoroso, realizando a quarentena de todos os anexos, independentemente da aprovação ou da liberação para o destinatário final.

Para algumas organizações, uma solução melhor para documentos do Office é criar uma lista de desbloqueio das macros confiáveis (assinadas) e bloquear todas as outras; caso novas macros do documento de negócios precisem ser liberadas, deve ser realizado o gerenciamento da mudança para assegurar que a trilha de auditoria completa exista (para minimizar o risco de ela ser usada indevidamente por intrusos maliciosos).

Novas versões de ransomware estão aparecendo a cada dia e geralmente não são detectadas pelos antivírus corporativos populares durante muitos dias.

MANTENHA O ANTIVÍRUS E/OU A PROTEÇÃO DO DISPOSITIVO ATUALIZADOS

As soluções de antivírus de terminal nunca devem contar apenas com mecanismos de proteção contra ameaças, mas eles são o mecanismo de detecção inicial mais comuns. É recomendável que as organizações assegurem que suas soluções de antivírus estejam atualizadas com as definições de antivírus mais recentes para maximizar sua eficácia. O ransomware está evoluindo e mudando constantemente no esforço de evitar a detecção. Novas versões estão aparecendo a cada dia e geralmente não são detectadas pelos antivírus corporativos populares durante muitos dias.

As organizações devem considerar o uso de diferentes produtos antivírus para diferentes propósitos, ou seja, um antivírus para os desktops, um diferente para servidores e outro para o gateway de e-mail. Esta estratégia pode fornecer o máximo de cobertura para ameaças emergentes que podem não ser detectadas por uma das soluções antivírus, mas podem ser detectadas por outra.

Considere soluções adicionais de proteção do terminal como o IBM Security Trusteer APEX Advanced Malware Protection[5] ou soluções de integridade do terminal como o Carbon Black, que não dependem de assinaturas, mas do comportamento e de aplicativos confiáveis.

EXECUÇÃO RESTRITA DE PROGRAMAS A PARTIR DE PASTAS TEMPORÁRIAS

Geralmente o malware usa pastas temporárias como o ponto de execução inicial e o ransomware não é diferente. Quando possível, é recomendável usar Objetos de Política de Grupo (GPO) ou Políticas de Restrição de Software (SRP)[6] para restringir a execução de qualquer programa a partir de pastas temporárias genéricas e de dentro de pastas temporárias no perfil de um usuário, tal como “c:\users\<user>\appdata\temp”.

Por exemplo, quando a maioria dos ransomware é executada inicialmente, ela tenta copiar a carga útil maliciosa na pasta temporária do usuário para continuar a cadeia de execução. Se isso fosse bloqueado, a infecção inicial do malware seria bloqueada.

Uma solução mais robusta é utilizar o AppLocker para desativar a ativação de executáveis a partir não apenas das pastas temporárias, mas também de outras pastas não padrão, como em %AppData% ou %LocalAppData%, que a maioria dos softwares comerciais/profissionais não deve usar. Muitos ransomwares e outros malwares usarão essas pastas.

5 ***http://www-03.ibm.com/software/products/en/trusteer-apex-adv-malware***
6 ***https://technet.microsoft.com/en-us/library/cc759648%28v=ws.10%29.aspx***

MANTENHA UMA POLÍTICA DE GERENCIAMENTO DE CORREÇÃO AGRESSIVA E ATUAL

O ransomware (e o malware em geral) geralmente usa 7 vulnerabilidades de dia zero para avançar sua campanha. Este vetor de ataque também é um que não pode ser monitorado tão intensamente quanto mensagens de e-mail recebidas. A inteligência da ameaça revela que muitas versões diferentes de malwares, incluindo ransomware, são rápidas em implementar vulnerabilidades de dia zero em uma tentativa de aumentar sua receita.

As organizações devem adotar uma política de gerenciamento de correção agressiva, especialmente com vulnerabilidades do navegador tais como o Adobe Flash e o Java, que são usados por uma grande parte dos funcionários. As correções devem ser aplicadas em tempo hábil. A IBM observa que as correções recentes da Adobe para ransomware devem ser aplicadas “o mais breve possível” e a Adobe define este período de tempo como “dentro de 72 horas”[8].

AUMENTE A VISIBILIDADE DO DNS, OS RECURSOS DE SUMIDOURO E DE FILTRAGEM DA WEB

No caso do ransomware, a resolução de DNS inicial pelo malware depende do algoritmo de geração de domínio (DGA). Isso torna o bloqueio de domínios inválidos conhecidos muito mais difícil pois ele tem a capacidade de gerar e usar milhares de nomes de domínio diferentes para acessar o servidor de comando e controle.

Todavia, ter uma boa visibilidade dos servidores de nomes de domínio (DNS) corporativos pode ser extremamente útil ao trabalhar em um incidente e para fornecer um sistema de aviso antecipado. Estar apto a procurar e monitorar as solicitações de DNS que estão ocorrendo fornece a capacidade de ver padrões, tais como solicitações de DNS de estilo DGA frequentes. As organizações também devem considerar implementar um recurso de sumidouro de DNS[9] em vez de bloquear totalmente IPs ou domínios especificados no gateway egresso. O uso de um sumidouro permite que a organização redirecione domínios (e IPs) para um servidor interno específico que possa fornecer avisos aos usuários que tentam acessar sites bloqueados. O sumidouro também fornece recurso de notificação em tempo real quando os computadores estão tentando acessar sites específicos.

As organizações devem considerar implementar um recurso de filtragem da web baseado em reputação. O controle de IPs, domínios e sites bloqueados em geral é uma tarefa sem fim. Os firewalls e proxies da nova geração contam com feeds de reputação em tempo real que transmitem informações de inteligência de origem e ajudam a proteger as organizações implementando destinos inválidos conhecidos rapidamente, fornecendo recursos de bloqueio rápido quando descobre-se que os sites têm conteúdo malicioso.

7 ***https://en.wikipedia.org/wiki/Zero-day_%28computing%29***
8 ***https://helpx.adobe.com/security/severity-ratings.html***
9 ***https://en.wikipedia.org/wiki/DNS_sinkhole***

APLIQUE A METODOLOGIA DE MENOR PRIVILÉGIO

Como o ransomware visa arquivos de usuário comuns no sistema local, bem como compartilhamentos de rede, é recomendado pela equipe de Serviços de Respostas a Incidentes do IBM Security que as organizações usem a metodologia de menor privilégio e conceda apenas as permissões necessárias para as pastas para que cada usuário execute seu trabalho diário. Como um computador infectado opera com a permissão do usuário com login efetuado no momento, ele pode atravessar e criptografar apenas arquivos aos quais ele tem acesso de leitura e gravação. Se o usuário não precisa de acesso de leitura/gravação para vários compartilhamentos de rede, considere remover, no mínimo, as permissões de gravação dos locais que não precisam ser acessados pelos usuários para uma necessidade de negócios rotineira.

CONSIDERE DESATIVAR O FLASH

O Adobe Flash é considerado um grande vetor de infecção para ransomware. Em julho, o Mozilla utilizou uma etapa incomum de bloqueio do flash por padrão, devido às enormes falhas de segurança do Flash. Devido ao risco representado pelo Flash, os Serviços de Resposta de Emergência da IBM recomendam que as organizações considerem desativar o Flash dentro da organização por padrão. Caso exista um caso de negócios que requeira o uso do Flash pelos usuários, esses usuários poderão se beneficiar de proteções adicionais (por exemplo, rede de alto risco dedicada segmentada na organização). Embora a desativação do Flash não remova todos os riscos relacionados a atividades da Internet, ela diminuirá o número de vetores de infecção abertos aos atacantes.

CONSIDERE DESATIVAR O WINDOWS SCRIPTING HOST

O uso de JavaScript ou VCScript pelo ransomware (e outros malwares) aumentou nos últimos anos. Isso tem sido usado pelos autores de malware porque o Windows Scripting Host (WSH) está ativado em todos os sistemas Windows por padrão.

No entanto, muitas organizações não o usam ou o usam comedidamente. Isso permite que os autores de ransomware usem e abusem de um grande vetor de ataque, havendo uma grande chance de o script de dropper de malware ser bem-sucedido e começar a dinâmica do ransomware até a conclusão da criptografia do arquivo.

Isso pode ser evitado centralmente por meio da Política de Grupo. Crie a chave de registro e o valor a seguir:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Script Host\Settings\ Enabled e configure o campo ‘Value data’ de Enabled como ‘0’ (ou seja, um zero sem as aspas).

Isso deterá efetivamente qualquer ransomware ou outro malware que tente usar JavaScript ou VBScript para infectar um sistema. Em vez de executar o script, o seguinte será mostrado ao usuário:

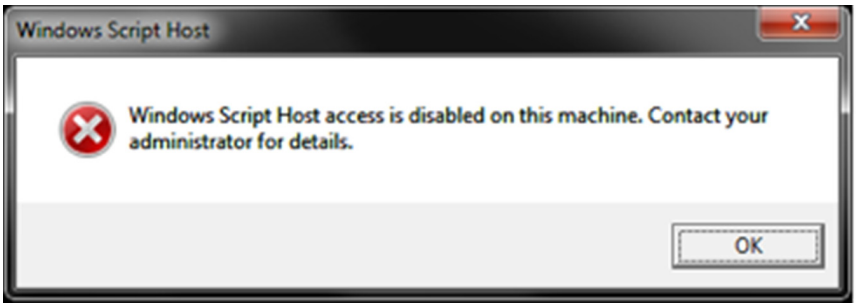

Figura 2. Mensagem desativada pelo Windows Script Host.

É preferível que seus usuários vejam essa caixa de mensagem de aviso a uma nota de resgate porque, então, será tarde demais. Observe apenas que a desativação do WSH impedirá que os usuários executem qualquer script (inclusive VBScript e JScript) que dependa de WSH.

CRIANDO UM PLANO

A resposta ao ransomware ou a outros tipos de malware pode requerer uma resposta de função cruzada dentro da organização. Ter um plano de resposta a incidentes definido e atualizado com funções e responsabilidades predefinidas é uma etapa preparatória essencial que permite que a organização tenha um processo de resposta organizado caso um ransomware seja detectado.

Detecção

A maneira como uma organização percebe que foi vítima de um ransomware pode variar. O problema mais urgente é identificar todo e qualquer sistema que foi (ou pode ter sido) infectado com o ransomware. Isso serve para ajudar a minimizar o risco para a organização isolando os sistemas infectados. Também ajuda a parar qualquer processo de criptografia que ainda possa estar ocorrendo, reduzindo, assim, o dano na organização e o esforço necessário para restaurar a organização para a operação normal.

A resposta ao ransomware ou a outros tipos de malware pode requerer uma resposta de função cruzada dentro da organização.

À medida que você lê os cenários abaixo, tenha em mente que, apesar de uma organização identificar um host que esteja infectado ou que seja responsável por criptografar arquivos, isso não significa que outros não sejam infectados. Se um host dentro da organização estiver infectado, há uma grande chance de haver vários hosts infectados porque a mesma vulnerabilidade pode existir dentro da empresa como um todo. A maioria dos ransomwares não criptografará novamente os arquivos que já foram criptografados. Portanto, se você identificar um host infectado responsável por criptografar arquivos, especialmente em um compartilhamento de rede, monitore os compartilhamentos de perto após colocar o host infectado off-line, caso haja outros hosts infectados, e continue o processo de criptografia.

CENÁRIO UM - UM USUÁRIO DE REDE TENTA ACESSAR UM ARQUIVO EM UM COMPARTILHAMENTO DE REDE E DESCOBRE QUE ELE ESTÁ CRIPTOGRAFADO

Este primeiro exemplo apresenta o maior risco para a organização. Neste caso, há um computador infectado em algum lugar na rede. O usuário que usa o computador tem acesso a compartilhamentos de rede e o ransomware, que está operando com as permissões do usuário, está acessando todo compartilhamento de rede e arquivos aos quais o usuário tem acesso.

Se a organização é grande, o número de arquivos que o usuário pode acessar pode chegar a centenas de milhares, o que poderia levar dias para o ransomware criptografar. Esse atraso pode contribuir com o fato de que o computador da vítima nunca exibe uma mensagem, pois ele ainda está percorrendo todos os arquivos e compartilhamentos de rede aos quais os usuários têm acesso.

Nesse caso, é extremamente importante e urgente determinar o computador da vítima. Isso normalmente é feito consultando as permissões de propriedade dos arquivos que foram criptografados e/ou as permissões de propriedade do novo arquivo que foi criado em cada pasta, notificando os usuários de que os arquivos foram criptografados. Esse novo arquivo normalmente herdará as permissões do usuário sob as quais o ransomware estava sendo executado, fazendo com que o proprietário do arquivo seja listado como a conta do usuário que foi infectada inicialmente com o ransomware.

CENÁRIO DOIS - O USUÁRIO TENTA ACESSAR UM ARQUIVO LOCAL E DESCOBRE QUE ELE ESTÁ CRIPTOGRAFADO

O segundo cenário possível é quando um computador é infectado e um usuário localiza arquivos no sistema local que estão criptografados e inacessíveis, mas ele ainda não recebeu uma mensagem pop-up. Neste cenário, é provável que o processo de criptografia esteja atualmente em progresso e que o usuário apenas tenha testado e acessado um arquivo que foi criptografado, mas o ransomware não concluiu sua atividade maliciosa. A maioria das variantes de malware deixa um arquivo de texto ou arquivo HTML em cada pasta que ela criptografa informando o usuário que os arquivos foram criptografados e estão sendo mantidos reféns.

Neste caso, o computador da vítima deve ser encerrado imediatamente pois a probabilidade é que o processo malicioso esteja ativo no momento, percorrendo as várias pastas nas unidades locais (e possivelmente na rede) e tornando-as inacessíveis. O sistema deve ser desativado imediatamente e a equipe de segurança de TI deve ser notificada. O sistema não deve ser ativado novamente, caso contrário o processo de criptografia continuará e poderá concluir, tornando todos os arquivos do usuário inacessíveis.

CENÁRIO TRÊS - USUÁRIO RECEBEU UMA MENSAGEM POP-UP EM SEU COMPUTADOR

Neste último cenário, o computador da vítima (ou computadores) dentro da organização será infectado silenciosamente e começará a criptografar todos os arquivos locais do usuário, bem como todos os arquivos aos quais o usuário possa ter acesso nos compartilhamentos de rede.

Quando o processo de criptografia for concluído, será exibida uma mensagem no computador infectado notificando ao usuário que seus arquivos foram criptografados e fornecendo um método para pagamento do resgate. O texto de uma mensagem exibido ao usuário pode variar e ser semelhante ou diferente do exemplo mostrado abaixo.

Figura 3. Mensagem pop-up de amostra do usuário final do Ransomware.

Cada variante de ransomware pode ter uma mensagem diferente exibida ao usuário e/ou o texto da mensagem em si pode variar. A mensagem exibida no computador infectado é muito útil na determinação de com qual variante de ransomware o computador da vítima foi infectado. Qualquer mensagem exibida deve ser capturada obtendo uma captura instantânea ou foto com um dispositivo móvel. Discutiremos a importância da determinação da variante do ransomware em uma seção posterior.

A fase de Análise foca basicamente duas áreas: 1) identificar a variante específica do ransomware e 2) determinar como o malware entrou na organização.

Análise

A fase de Análise foca basicamente duas áreas: 1) identificar a variante específica do ransomware e 2) determinar como o malware entrou na organização.

IDENTIFICAÇÃO DO MALWARE

Ao embarcar na fase de Análise do incidente, é essencial identificar a variante específica do ransomware dentro de seu ambiente. Como existem muitas variedades de ransomware, com novas surgindo frequentemente, cada uma com seus próprios recursos exclusivos, compreender a variante de ransomware é um pré-requisito para avançar à fase de Restrição. Algumas versões de ransomware, como o SamSam, têm a capacidade de utilizar o movimento lateral enquanto outras variantes podem não ter esta capacidade. As capacidades do ransomware influenciarão muito as etapas posteriores de restrição.

Determinar a variante pode ser complicado e a IBM recomenda que a organização busque a assistência de especialistas internos no assunto ou de profissionais externos, tal como um provedor de serviços de segurança, para ajudar a determinar a variante.

ANÁLISE DA CAUSA RAIZ

Deve ser executado uma análise da causa raiz (RCA) para ajudar uma organização a entender como o ransomware entrou em seu ambiente. Enquanto uma análise de causa raiz formal pode esperar até a Atividade Pós-incidente, uma RCA resumida auxiliará a organização ao entrar na fase de Restrição. Sem esta análise, o ciclo de infecção provavelmente se repetirá. Também é importante realizar a RCA antes da fase de recuperação, pois uma organização pode gastar uma grande quantidade de tempo e esforço recuperando arquivos apenas para tê-los criptografados novamente logo depois.

Existem duas maneiras de o ransomware chegar a uma organização - por meio de um e-mail não solicitado com um anexo ou por meio de vulnerabilidades do navegador da web, tal como a vulnerabilidade recente do Flash que foi implementada no kit de exploração do Angler. Se um funcionário recebeu um e-mail não solicitado que continha ransomware, existe alto potencial de reinfecção. Se ficar determinado que o ransomware foi recebido por e-mail, deve ser conduzida uma procura no armazenamento de e-mail da organização rapidamente para identificar outros e-mails possivelmente não abertos nas caixas de correio do funcionário. Esses e-mails devem ser extraídos e excluídos imediatamente.

As vulnerabilidades do navegador da web são um pouco mais complicadas e difíceis de determinar, mas a RCA provavelmente contará com a estrutura de gerenciamento de correção da organização. Uma análise adequada ajudará a identificar qual website inicial causou a infecção, fornecendo à organização a capacidade de bloquear o acesso a esse website por todos os outros funcionários e ajudando a reduzir a chance de incidentes futuros semelhantes. A organização deve ter em mente que, embora bloquear os sites maliciosos identificados seja uma primeira etapa, isso pode não ser um controle de compensação adequado pois os funcionários remotos não serão bloqueados pelas regras de firewall da organização uma vez que não estão na rede local (LAN) da organização.

Um método mais recente é o ransomware ser introduzido por hackers que exploram vulnerabilidades conhecidas no JBoss e, em seguida, instalam webshells ou backdoors para permitir a implementação do ransomware manualmente nos sistemas identificados.

A IBM recomenda o uso de especialistas no assunto (SMEs) internos para resposta a incidentes ou um especialista externo para auxiliar na análise adequada da causa raiz.

Restrição

Quando um sistema tiver sido identificado como tendo potencialmente um ransomware, o computador potencialmente infectado deverá ser imediatamente removido de suas redes (inclusive Wifi) e desligado ou hibernado - o ideal - para ajudar na análise forense e de amostra, para minimizar o risco de o ransomware continuar o processo de criptografia.

A falha em isolar o sistema da rede rapidamente pode contribuir com o incidente, permitindo que o malware continue criptografando arquivos no sistema local e/ou nos compartilhamentos de rede, aumentando, assim, os esforços de recuperação realizados pela organização.

ÚLTIMO RECURSO DE RESTRIÇÃO

Se a organização não puder determinar rapidamente a origem do ransomware e do processo de criptografia, como último recurso a organização deve considerar colocar os compartilhamentos de arquivos off-line para ajudar a minimizar o risco e o impacto nos negócios. Os servidores de arquivos não precisam ser encerrados, mas todo o acesso aos compartilhamentos de arquivos deverá ser finalizado (remover o compartilhamento, restringir por ACL de rede ou de firewall baseado em host, etc.). Não é recomendável mudar as permissões nos arquivos dentro de um compartilhamento na tentativa de restringir o acesso pois, dependendo do número de arquivos, a propagação da permissão poderia levar horas e permitiria que o processo de criptografia continuasse durante esse tempo.

Se você usar CIFS/SMB em outros sistemas operacionais, incluindo UNIX, Linux, etc., lembre-se de protegê-los também. Isso reduzirá muito a chance de esses compartilhamentos serem criptografados porque para o ransomware eles parecerão compartilhamentos do Windows.

Erradicação

Esta fase envolve a remoção do ransomware dos sistemas infectados. A IBM recomenda que qualquer sistema que tenha sido identificado como estando infectado com o ransomware seja reconstruído a partir de uma origem confiável. Além disso, a RCA pode revelar que o ransomware veio para a organização por meio de um e-mail ou de outros mecanismos aos quais outros usuários têm acesso. Se a RCA revelou que o malware chegou inicialmente por meio de um e-mail, a organização deverá procurar e limpar todas as mensagens existentes ainda dentro do armazenamento de e-mail. Uma organização deve considerar isolar qualquer sistema que recebeu o e-mail e/ou abriu o e-mail até que seja verificado se o ransomware não foi executado nesses sistemas.

Se a RCA revelou que o ransomware chegou por meio de uma exploração do navegador da web, esses sites deverão ser bloqueados e monitorados. A organização deverá, então, avaliar a necessidade de atualizar/remover qualquer componente do navegador vulnerável.

As senhas para os usuários afetados devem ser alteradas como precaução.

Recuperação

Assim que uma organização tiver contido o ransomware e identificado a causa raiz da infecção, haverá várias considerações a serem examinadas ao iniciar a fase de recuperação. É muito importante que a organização determine quais hosts foram infectados e a causa raiz da infecção antes de iniciar o processo de recuperação.

RESTAURAÇÃO A PARTIR DO BACKUP

A IBM recomenda que uma organização conte inicialmente com sua infraestrutura de backup interna para restaurar os arquivos afetados, antes que qualquer outra opção seja considerada. Isso requer que um processo de backup já exista para os dados afetados e uma análise deve ser feita com relação à frequência e à integralidade dos backups para assegurar que os dados afetados serão completamente restaurados.

Uma organização deve ter em mente que, se um compartilhamento de rede esteve envolvido na criptografia, poderá haver uma chance de que vários dos últimos backups contenham arquivos parcialmente criptografados. Por exemplo, se o compartilhamento de arquivo de uma organização passa por backup diário, mas um computador da vítima é infectado e demora cinco dias para criptografar tudo no compartilhamento antes de notificar o usuário ou de alguém descobrir a infecção, os últimos cinco backups conterão arquivos que foram criptografados inicialmente.

A melhor solução é ter um bom processo de backup - um que utilize as melhores práticas do mercado, tal como assegurar que não apenas backups locais sejam feitos, mas que backups também sejam arquivados em mídia removível (fitas, discos óticos ou discos rígidos removíveis). Contar somente com imagens de disco local, replicação e outros backups de rede local pode não ser suficiente, pois eles também podem ser criptografados por ransomware ou o backup pode ser realizado após os arquivos terem sido criptografados pelo ransomware.

RECURSOS DA VARIANTE DE RANSOMWARE

Embora o ideal seja identificar a variante do ransomware na fase de Análise, saber a variante e a versão do ransomware pode ajudar na fase de recuperação, determinando se o processo de criptografia usado pelo ransomware é reversível sem a necessidade de pagar o resgate. Muitas variantes de ransomware atingem o objetivo de criptografar seus arquivos com segurança, enquanto outras não. A determinação da variante do ransomware com a qual sua organização foi infectada fornecerá uma opção de recuperação alternativa se uma restauração a partir do backup não for possível.

Informações de Contato para os Serviços de Resposta a Incidentes da IBM

América do Norte:
Canal de contato 24 horas por dia, 7 dias da semana: 1-888-241-9812

Europa, Oriente Médio, África, Ásia-Pacífico:
França (+33) 157327272
Espanha (+34) 910507799
Portugal (+351) 213665622
Finlândia (+358) 972522099
Alemanha (+49) 69380791120
Holanda (+31) 707709351
Letônia (+371) 66163849
Itália (+39) 299953631
Reino Unido (+44) 2036844872
Dinamarca (+45) 43314987
Suécia (+46) 850252313
Noruega (+47) 23024798
Suíça (+41) 227614228
Polônia (+48) 223062234
Emirados Árabes Unidos (+971) 4 80004442417
Austrália (+61) 1888637539

Tenha em mente que a criptografia usada pelo ransomware indicada pode não ser exata. Por exemplo, a IBM observou que a versão original do TeslaCrypt usava na verdade a criptografia AES Symmetric, embora ela indique o uso de chaves RSA Asymmetric (PKI). Isso é mostrado claramente na captura de tela a seguir de uma infecção de TeslaCrypt.

```
Seus arquivos foram criptografados com segurança no
PC: fotos, vídeos, documentos, etc. Clique no botão
"Mostrar arquivos criptografados" para visualizar
uma lista completa dos arquivos criptografados e você
poderá verificar isso pessoalmente.

A criptografia foi produzida usando uma chave pública
RSA- 2048 exclusiva gerada para este computador. Para
decriptografar os arquivos, é necessário obter a chave
privada.

A única cópia da chave privada que permitirá decrip-
tografar seus arquivos está localizada em um servidor
secreto na Internet; o servidor eliminará a chave após
um período de tempo especificado nessa janela.
Quando ele concluir, ninguém será capaz de restaurar os
arquivos...
```

Figura 4. Captura de tela de amostra do incidente de infecção.

PAGANDO O RESGATE

As organizações podem ser confrontadas com uma decisão de pagar o resgate para recuperar arquivos importantes que não podem ser recuperados por outros métodos. Conforme mencionado acima, cada organização deve considerar essa opção com cuidado e apenas após todas as outras opções de recuperação terem se esgotado. Uma organização que considera essa opção deve envolver todas as partes interessadas relevantes dentro da organização no processo de decisão e considerar todos os resultados possíveis.

A solução ideal é aquela em que os dados podem ser recuperados por meio de backups ou de outros armazenamentos de dados. Isso é preferível ao pagamento pois, de outra forma, você estará validando o modelo de negócios do autor do ransomware e provando que ele foi bem-sucedido em sua decisão. Além disso, isso apenas incentivará mais agentes mal-intencionados a tirem vantagem de uma situação específica.

Atividade Pós-incidente

A atividade pós-incidente deve incluir a revisão das lições aprendidas durante a resposta ao incidente, quais controles de detecção e segurança poderão ou não ser utilizados para ajudar a detectar e evitar um incidente semelhante no futuro. Cada organização é diferente e as recomendações apresentadas na fase de preparação deste documento poderão ou não se aplicar a uma organização específica. Portanto, é extremamente importante que a organização discuta as descobertas do incidente com o propósito de aprender novas técnicas para detectar, responder, analisar ou evitar incidentes semelhantes no futuro.