UNIVERSIDADE
FEDERAL DO CEARÁ

AUDITORIA E SEGURANÇA DE SISTEMAS DE INFORMAÇÃO

Guia de boas práticas: Ransomware

Contexto

O ransomware faz parte da família dos códigos maliciosos, ou seja, ele se enquadra na classificação de Malware que é resultado da combinação das palavras inglesas “malicious” e “software”, esses programas são desenvolvidos com intuito de infectar equipamentos e realizar ações danosas ao mesmo e ao usuário, praticamente qualquer dispositivo que possua conexão com a internet pode ser alvo desse tipo de código como por exemplo: computadores, modems, switches, roteadores, celulares e tablets, o principal objetivo do desenvolvimento desse tipo de programa é a obtenção de vantagens financeira, coleta de informações confidenciais, prática de golpes e spam. Analisando a forma de ataque do ransomware percebemos que ele executa uma espécie de *“Sequestro”* da máquina ou de dados e informações da vítima, utilizando-se de criptografia.

História

O primeiro ransomware foi criado em 1989 pelo biólogo evolucionário de Harvard, Joseph L. Popp (que hoje é conhecido como o 'pai do ransomware'). Seu malware foi batizado de AIDS Trojan, também conhecido como PC Cyborg. Popp enviou 20.000 disquetes infectados com o rótulo “Informações sobre AIDS - Disquetes introdutórios” aos participantes da conferência internacional sobre AIDS da Organização Mundial da Saúde em Estocolmo. Os discos continham código malicioso que ocultava diretórios, bloqueia nomes de arquivos e exigia que as vítimas enviassem US $189 para uma caixa postal no Panamá se quisessem seus dados de volta.

Tipos

Ransomware de bloqueio: Este tipo de malware bloqueia as funções básicas do computador. Por exemplo, o acesso à área de trabalho pode ser bloqueado e o mouse e o teclado são parcialmente desativados. Isso permite que você continue a interagir com a janela que contém o pedido de resgate, de modo que possa fazer o pagamento. Fora isso, o computador fica inoperável. Mas a boa notícia é que o malware de bloqueio não costuma ter como alvo arquivos críticos; ele geralmente só quer bloquear o seu acesso. Por isso, a destruição completa dos seus dados é improvável.

Ransomware de criptografia: O objetivo deste ransomware é criptografar seus dados importantes, como documentos, imagens e vídeos, mas não interferir nas funções básicas do computador. Isso gera pânico, pois os usuários podem ver seus arquivos, mas não podem acessá-los. Os desenvolvedores de criptografia muitas vezes adicionam uma contagem regressiva ao seu pedido de resgate: "Se você não pagar o resgate até o prazo,

todos os seus arquivos serão excluídos". E devido ao número de usuários que não sabem da necessidade de fazer backups na nuvem ou em dispositivos externos de armazenamento físico, o ransomware de criptografia pode ter um impacto devastador. Consequentemente, muitas vítimas pagam o resgate simplesmente para obter seus arquivos de volta.

Exemplos

Locky: é um ransomware que foi usado pela primeira vez para um ataque em 2016 por um grupo organizado de hackers. O Locky criptografou mais de 160 tipos de arquivos e foi espalhado por meio de e-mails falsos com anexos infectados. Os usuários caíram no truque do e-mail e instalaram o ransomware em seus computadores. Esse método de propagação é chamado phishing, e é uma forma de engenharia social. O ransomware Locky é direcionado a tipos de arquivos frequentemente usados por designers, desenvolvedores, engenheiros e testadores.

WannaCry: foi um ataque de ransomware que se espalhou por mais de 150 países em 2017. Ele foi projetado para explorar uma vulnerabilidade de segurança no Windows que foi criada pela NSA e vazada pelo grupo de hackers Shadow Brokers. O WannaCry afetou 230 mil computadores em todo o mundo. O ataque atingiu um terço de todos os hospitais do Serviço Nacional de Saúde (NHS, National Health Service) do Reino Unido, causando danos estimados em 92 milhões de libras. Os usuários foram bloqueados e foi exigido um resgate em bitcoins. O ataque expôs o problema de sistemas desatualizados, pois o hacker explorou uma vulnerabilidade do sistema operacional para a qual já existia um patch há muito tempo. O prejuízo financeiro mundial causado pelo WannaCry foi de, aproximadamente, US $4 bilhões.

Bad Rabbit: foi um ataque de ransomware de 2017 que se espalhou por meio dos chamados ataques de execução. Sites inseguros foram usados para realizar os ataques. Em um ataque de ransomware de execução, o usuário visita um site real, sem saber que ele foi comprometido por hackers. Na maioria dos ataques de execução, tudo o que é necessário é que um usuário abra uma página que tenha sido comprometida dessa forma. Nesse caso, entretanto, a execução de um instalador que continha malware disfarçado levou à infecção. Isso é chamado de dropper de malware. O Bad Rabbit solicitava ao usuário que ele executasse uma instalação falsa do Adobe Flash, infectando o computador com o malware.

Ryuk: é um cavalo de Tróia de criptografia que se espalhou em agosto de 2018 e desabilitou a função de recuperação dos sistemas operacionais Windows. Isso tornou impossível restaurar os dados criptografados sem um backup externo. O Ryuk também criptografou discos rígidos de rede. O impacto foi enorme, e muitas das organizações

norte-americanas que foram alvo pagaram as quantias de resgate exigidas. Estima-se que o total de danos seja de mais de US $640.000.

Shade/Troldesh: O ataque do ransomware Shade ou Troldesh ocorreu em 2015 e se espalhou por meio de e-mails de spam com links ou anexos de arquivos infectados. Curiosamente, os invasores do Troldesh se comunicavam diretamente com suas vítimas via e-mail. E as vítimas com quem construíam uma "boa relação" recebiam descontos. No entanto, esse tipo de comportamento é uma exceção à regra.

Jigsaw: é um ataque de ransomware que começou em 2016. Ele recebeu esse nome por causa de uma imagem que exibia do famoso fantoche da franquia do filme Jogos Mortais. A cada hora adicional que o resgate permanecia sem pagamento, o ransomware Jigsaw apagava mais arquivos. O uso da imagem do filme de terror causou estresse adicional entre os usuários.

CryptoLocker: é um ransomware que foi visto pela primeira vez em 2007 e que se disseminou por meio de anexos de e-mail infectados. Ele buscava dados importantes em computadores infectados e os criptografava. Estima-se que 500.000 computadores foram afetados. Autoridades legais e empresas de segurança conseguiram, eventualmente, controlar uma rede global de computadores domésticos hackeados que eram usados para espalhar o CryptoLocker. Isso permitiu às autoridades e às empresas interceptar os dados enviados pela rede sem que os criminosos percebessem. No fim, isso resultou na criação de um portal online onde as vítimas podiam obter uma chave para desbloquear seus dados. Dessa maneira, os dados puderam ser liberados sem precisar pagar um resgate aos criminosos.

Como ocorre a infecção?

Ocorre pela execução de arquivos infectados, estes arquivos podem chegar a suas vitimas de varias formas, como:

- Links em emails e redes sociais.
- Baixando arquivos em sites não confiáveis.
- Acessando Páginas infectadas com navegadores vulneráveis.
- Explorando a vulnerabilidade de sistemas sem as devidas atualizações de segurança.
- Mídias infectadas

Como se Proteger?

A melhor maneira de lidar com Ransomware é se prevenindo, ou seja, não abrir links suspeitos em emails e redes sociais, evitar realizar download de softwares piratas ou de fontes não oficiais.

Outras formas de garantir a proteção contra esse tipo de ataque é realizar Backups regularmente, como esse ataque consiste em realizar um sequestro de dados e informações através de encriptação, os backups garantem que seus dados não sejam perdidos, assim possibilitando uma saída caso aconteça uma infecção, para garantir a real efetividade desse método é necessário que o usuário mantenha os backups atualizados, automatizados, de fácil recuperação e verificar se eles realmente estão sendo feitos, outro passo importante é que os backups estejam desconectados do sistema principal, garantindo que em caso de ataque ele não seja afetado, é necessário também garantir a redundância das informações mais importantes.

Outra forma de se proteger e garantir que os softwares e o sistema estejam atualizados, programas ou softwares constantemente tem falhas de segurança que são corrigidas em atualizações recorrentes, caso o sistema operacional ou programas utilizados estejam desatualizados, em especial os navegadores, é muito provável a abertura de vulnerabilidades a ataques, além disso é essencial garantir a autenticidade desses softwares, apenas baixando-os de fontes oficiais.

Referências

SEYTONIC, **The Crazy Origins Of Ransomware.** Disponível em: <https://www.youtube.com/watch?v=qFX8ywAb0e0>. Acesso em: 12 maio. 2023.

CERT.BR. **Você sabe o que é ransomware?** Disponível em: <https://cartilha.cert.br/ransomware/>.

OTW. **Ransomware: Build Your Own Ransomware, Part 1.** Disponível em: <https://www.hackers-arise.com/post/ransomware-build-your-own-ransomware-part-1>.

IT, I. **Ransomware: O que é? Como funciona? E outras perguntas frequentes.** Disponível em: <https://www.internationalit.com/post/ransomware-o-que-%C3%A9-como-funciona-e-outras-perguntas-frequentes>.

DIGITAL, O. **WannaCry: Entenda o ciberataque que afetou mais de 200 mil PCs em 150 países.** Disponível em: <https://olhardigital.com.br/especial/wannacry/>.

The Biggest Ransomware Attacks in History. Disponível em: <https://www.youtube.com/watch?v=9T8El6dEr3U>. Acesso em: 18 maio. 2023.

WANNACRY: The World's Largest Ransomware Attack (Documentary). Disponível em: <https://www.youtube.com/watch?v=PKHH_gvJ_hA>.

A Brief History of Ransomware | CrowdStrike. Disponível em: <https://www.crowdstrike.com/cybersecurity-101/ransomware/history-of-ransomware/>.

A Brief History of Ransomware. Disponível em: <https://www.varonis.com/blog/a-brief-history-of-ransomware>.

Reconhecendo um ransomware – diferenças entre cavalos de Tróia de criptografia. Disponível em: <https://www.kaspersky.com.br/resource-center/threats/ransomware-attacks-and-types>.