Aluno: José Victor Medeiros Thomé da Silva
Instrutor: José Luís

TAG – Segurança Ofensiva - Relatório

1. Introdução:

O malware a ser descrito nesse relatório é o Ransomware, que é um tipo de software malicioso no qual tem como objetivo “sequestrar” os dados do computador da vítima com o objetivo de conseguir um dinheiro com o resgate dos mesmos. Suas primeiras variantes foram desenvolvidas no final da década de 80 e inicialmente o pagamento de resgate era feito por correio tradicional, enquanto hoje em dia são usadas as moedas virtuais, como bitcoin, para dificultar a exposição e rastreamento do cibercriminoso.

Devido ao alto índice de vítimas (No segundo semestre de 2016, a Trend Micro fez uma pesquisa sobre ataques de Ransomware e consultou mais de 500 empresas brasileiras e da América Latina. O resultado foi que 51% das empresas brasileiras tiveram algum tipo de incidente em 2015) e aos altos custos gerados nos últimos anos (segundo dados do FBI, nos Estados Unidos as empresas gastaram R$ 325 milhões com resgates de ransomware), esse malware é considerado um dos mais rentáveis da história.

Exemplos notáveis de ransomwares são: Reveton (2012), Cryptolocker (2013), CriptoWall (2014), Fusob (2015 – 2016), WannaCry (2017), Petya (2017) e Bad Rabbit (2017).

2. Como contrair um ransomware?

Há diversos vetores de ataques feitos por malwares para atacar aparelhos (sejam esses fixos como um desktop ou moveis como um celular), sendo uma das mais comuns é através de um e-mail spam contendo em anexo um arquivo malicioso (como um pdf infectado ou arquivos suspeitos passivos de serem abertos em programas que suportam execução de macros como .docx do Word e o .xlsm do Excel) ou links que direcionam para páginas maliciosas que executam download do malware. Outra forma muito comum de propagação de ransomware é através de pop-ups com propagandas.

Em ambos os métodos de propagação é usado uma estratégia de engenharia social para induzir a vítima de fazer o download do malware, seja por phishing (como um pop-up botar um aviso de que o PC foi infectado e para solucionar clicar num link), pretexting (como falsa informação de uma atualização de algum serviço do usuário ou mensagens vindas de alguma prestadora de serviço contratada) ou baiting (ofertas duvidosas).

No entanto, há ransomwares que se propagam/comportam como outros tipos de malwares. Um exemplo desse tipo de ransomware é o WannaCry que age como um worm, se propagando pela rede e chegando ao PC sem a necessidade de interação com o usuário. Com isso, tanto pessoas quanto organizações foram afetadas, gerando prejuízos de milhares de dólares.

3. Como funciona um ransomware?

A forma que um ransomware funciona depende da variante usada pelo criminoso e pela família do malware. As três variantes conhecidas são:

- Criptográficos: como o próprio nome diz, o seu payload é um código de criptografia no qual criptografa todos os arquivos do dispositivo da vítima, e o pagamento é

demandado para o envio da chave para descriptografar os mesmos (quando o ransomware é mal feito, dá para extrair a chave usando engenharia reversa).

- Lock-screen: já essa variante simplesmente trava o dispositivo do usuário, exigindo um valor de resgate para desfazer esse processo.

- Scareware: geram mensagens ao usuário indicando erroneamente que seu dispositivo está com problemas e exige um pagamento para solucioná-los. Mesmo que o PC continue funcionando, as mensagens continuarão aparecendo e o usuário fica impossibilitado de usar alguns programas.

O ataque acontece em três fazes geralmente:

- Na fase 1 o ataque é enviado na forma de um spam ou um anúncio no qual burla o filtro de spam do usuário e usa uma estratégia de engenharia social para induzir o usuário a baixar o arquivo malicioso;

- Na fase 2 o usuário clica/acessa o conteúdo malicioso e o mesmo é baixado o computador burlando o antivírus (principalmente se o mesmo estiver desatualizado). O processo é executado via cmd/powershell no caso do Windows junto com os programas para dar acesso root e o algoritmo de criptografia, e daí esse malware é copiado para as demais pastas do disco rígido.

- Na fase 3, depois de propagar o malware nas pastas, é feito uma conexão com o servidor do atacante para enviar os comandos e informações e o algoritmo de criptografia é executado. Depois disso é mandada uma mensagem ao cliente pedindo o resgate.

3. Meu código

Acompanhado desse relatório está um código escrito em C que, embora não seja um ransomware completo, poderia ser um payload de um do tipo criptográfico, pois esse programa acessa uma pasta (tentando ser a do usuário) e criptografa todos os arquivos dentro da mesma (usando uma símples Cifra XOR), sendo a chave passada no momento da execução do programa. Embora o código seja um símples algoritmo de criptografia, um ataque com o mesmo poderia ser feito a um PC executando o mesmo por meio de um acesso remoto via um reverse shell com acesso privilegiado fornecido por rootkits.

Supondo que o executável desse código esteja salvo em algum link da internet, então através de um e-mail com arquivos/links infectados ou um worm na rede consigamos ter acesso ao PC da vítima, transpassando a segurança fornecida pelo antivírus ou por um firewall fraco (podendo ser através de uma rootkit, por exemplo), e executemos um reverse shell no modo privilegiado. Baixamos então o executável para criptografar os arquivos e copiamos o mesmo para as pastas dos diversos usuários existentes e então o executamos usando uma mesma chave. Daí o restante a se fazer é mandar uma mensagem cobrando pelo resgate ao dono do dispositivo.

4. Conclusão

Obviamente as formas de ataque dos ransomwares de hoje são muito mais sofisticados, gerando mensagens com contadores para prazos, conexões com plataformas de bitcoin, estratégias de ataque através de propagação em redes (como citamos no caso do WannaCry). Por isso é necessário ter todo tipo de cuidado por parte do usuário para se proteger, como ficar atento aos detalhes das mensagens de e-mail,

não sair baixando qualquer coisa da internet, ficar alerta com propagandas maliciosas e, o mais óbvio, manter o antivírus e o firewall sempre atualizados.

Todo esse cuidado é necessário pois, como tudo na área da informática, malwares também tendem a evoluir tecnologicamente, e com os ransomwares as coisas não são diferentes.

5. Referências:

- https://www.proof.com.br/blog/ransomware/
- https://br.malwarebytes.com/ransomware/
- https://www.avast.com/pt-br/c-wannacry