Vírus Metamórficos e Vírus Polimórficos

Daniel Barreiros[48452] and Tomás Antunes[48511]

Universidade de Évora

Abstract. A elevada diversidade de vírus existentes na atualidade bem como a sua evolução representa uma grande preocupação, principalmente para as empresas. Neste shortpaper pretendemos detalhar no que consistem os vírus metamórficos e polimórficos, explorar o que os diferencia, as suas técnicas para sobreviver nos hospedeiros e por fim iremos dar alguns exemplos de vírus que utilizam estas técnicas.

Keywords: Metamórficos · Polimórficos · Técnicas · Exemplos

1 Vírus Metamórficos

Os vírus metamórficos consistem em códigos versáteis, caracterizados por terem a capacidade de se transformar a cada execução. Este malware consegue converter, reescrever e alterar o seu próprio código tornando-o altamente perigoso, visto que após cada infeção, realiza as alterações necessárias para não ser facilmente detetado nas próximas investidas. Quanto mais tempo o vírus permanece ativo, mais variações são criadas e maiores são os estragos causados, tornando difícil o processo de desinfeção do sistema.

O malware metamórfico muda o seu código a cada replicação e através do surgimento de mecanismos de mutação, a ocultação de código pode ser realizada de uma forma rápida e em grandes quantidades. Este tipo de malware não é fácil de detetar através de scanner antivírus pois através de cada iteração eles alteram estruturalmente, mas a níveis funcionais permanecem iguais. Duas propriedades importantes passam pela ocultação e pelo pequeno tamanho no seu mecanismo de mutação. [2][3]

2 Vírus Polimórficos

Os vírus polimórficos consistem em códigos versáteis, também particularizados por conseguirem alterar o seu código à medida que vão sendo executados. São caracterizados pelo seu código simples e pela capacidade de realizarem a encriptação do seu próprio código através de uma chave externa variável. Deste modo, a cada execução, o código é encriptado de uma forma diferente, tornando assim mais difícil a sua deteção. [1][2][3]

3 Metamórficos VS Polimórficos

Os vírus metamórficos e polimórficos são muitas vezes confundidos pois têm algumas funcionalidades em comum, contudo, existem algumas diferenças. Os vírus polimórficos têm a capacidade de se auto-encriptarem através de uma chave externa, já os vírus metamórficos não realizam qualquer tipo de encriptação. Outra das suas diferenças consiste na complexidade do código fonte, visto que os vírus metamórficos são compostos por um código bem mais extenso e complicado que o dos vírus polimórficos. [3]

4 Técnicas Metamórficas e Polimórficas

Como explicado acima, os vírus metamórficos e polimórficos utilizam diversas técnicas para conseguirem evoluir de geração em geração. Nesta secção iremos detalhar algumas destas técnicas. [3]

4.1 Permutação

Esta técnica consiste na divisão do código em vários blocos para posteriormente serem organizados por outra ordem (simulando assim ser um código diferente). Introduzindo simples instruções de "jump", este irá fazer sempre a mesma coisa, embora se encontre desordenado. Deste modo, o vírus tem a capacidade, de geração para geração, de realizar a divisão aleatória, levando a uma infinidade de gerações diferentes.

4.2 Substituição de Instruções

Esta técnica consiste na capacidade de o vírus substituir algumas das suas instruções por outras equivalentes, simulando assim não ser o mesmo código de geração para geração.

4.3 Integração no Código

De uma forma resumida, o ficheiro executável é descompilado em pequenos elementos, permitindo ao vírus mover alguns blocos de código do seu sítio inicial para um local temporário, insere o seu código no código do ficheiro e reconstrói o executável. Deste modo o vírus consegue integrar-se na perfeição ao código do seu alvo, tornando muito difícil obter a sua localização.

4.4 Código Desnecessário

Esta simples técnica consiste na introdução de blocos de código desnecessário no meio do corpo do vírus de modo a que este seja diferente de geração para geração, dificultando o trabalho aos antivírus. Este código é criado para parecer algo legítimo, contudo, não altera o funcionamento do código original.

5 Exemplos de Vírus Metamórficos

5.1 Win32/Evol

O vírus Evol (Criado em 2000) é um mecanismo metamórfico com capacidade para ser utilizado em plataforma de Win32. Uma das suas funcionalidades consistia em inserir instruções desnecessárias entre o código principal tornando mais difícil detetar a sua existência. [2]

5.2 Win95/Bistro

O vírus Bistro apareceu uns meses depois com uma forma mais avançada de inserir código desnecessário. Quando uma rotina é ativada, é criado de forma aleatória um bloco de código desnecessário no ponto de entrada do corpo do vírus, levando posteriormente a que este gere, quando ativado, milhões de iterações, desafiando assim as capacidades do emulador. [2]

5.3 Win32/Ghost e Win95/Zperm

Estes dois vírus foram responsáveis por introduzir um novo nível de metamorfismo. De uma forma simples, estes vírus dividem o seu código em várias partes e trocam a ordem com que estes blocos se organizam. De forma a garantir que o código é lido pela ordem certa, colocam por exemplo, instruções de "jump". Deste modo, é possível obter várias versões do código com a mesma finalidade. [2]

6 Exemplos de Vírus Polimórficos

6.1 Vírus 1260

Este vírus foi um dos primeiros a ser conhecido como polimórfico. Era caracterizado por utilizar uma rotina criptográfica que introduzia várias instruções desnecessárias pelo meio do código funcional. Através da introdução destas instruções, o processo de criptografia não era afetado e tornava quase impossível a extração de uma sequência legível. [2]

6.2 Win32/Mydoom

Surgiu em 2004 e conseguia propagar-se através de e-mails e arquivos compartilhados entre os utilizadores. Composto por técnicas de alteração do código a cada infeção, tornava uma vez mais o processo de deteção complicado. Este vírus ainda possuía um extra, pois detinha funcionalidades que permitiam o controlo por parte dos invasores de uma forma remota. [2]

6.3 Win32/Conficker

Este vírus surgiu em 2008 e utilizava principalmente as redes locais para se conseguir propagar. Como vírus polimórfico este conseguia alterar o seu próprio código, dificultando o processo de remoção e utilizava as suas capacidades para se auto replicar de uma forma rápida. [2]

References

1. Cabrera, A., Calix, R.A.: On the anatomy of the dynamic behavior of polymorphic viruses. In: 2016 international conference on collaboration technologies and systems (CTS). pp. 424–429. IEEE (2016)
2. Konstantinou, E., Wolthusen, S.: Metamorphic virus: Analysis and detection. Royal Holloway University of London **15**, 15 (2008)
3. Li, X., Loh, P.K., Tan, F.: Mechanisms of polymorphic and metamorphic viruses. In: 2011 European intelligence and security informatics conference. pp. 149–154. IEEE (2011)