Rootkits-SI-2022/2023

Carlos Palma(46520) e Manuel Cunha(48482)

Licenciatura em Engenharia Informática, Universidade de Évora

17 de junho de 2023

Resumo

Um rootkit é um pacote de software projetado para oferecer acesso não autorizado a um computador ou software. Os rootkits são difíceis de detetar e podem ficar ocultos num sistema infetado, são usados para aceder manipular e roubar dados. Quando um rootkit assume o controlo, o atacante pode exercer controlo absoluto do dispositivo por acesso remoto. Por vezes estes podem parecer legítimos e contornar os antivírus e sistemas de segurança. Este trabalho de pesquisa aborda a natureza dos rootkits, as suas técnicas de ocultação e o impacto que podem ter na segurança da informação. (Referência: [1])

1 Introdução

A criação e o uso generalizado da Internet trouxeram benefícios significativos para a sociedade, porém também trouxeram desvantagens, como o surgimento de novos crimes e a prática de crimes convencionais por meio do uso da tecnologia. O crescimento exponencial e a dependência das Tecnologias de Informação e Comunicação (TICs) nos diversos setores económicos e governamentais tornam estas entidades vulneráveis a ataques informáticos, colocando em risco a segurança de uma nação. Diante desta emergente ameaça informática, é crucial o estabelecimento de medidas e estratégias de segurança. (Referência: [2])

Os rootkits estão entre as ameaças à segurança, tanto a nível pessoal quanto governamental, uma vez que permitem ao atacante obter acesso não autorizado a um dispositivo. Considerando esses dois aspetos, decidimos, no âmbito da disciplina de Segurança Informática da Universidade de Évora, elaborar o nosso trabalho final de pesquisa sobre estes pacotes de software maliciosos.

Neste trabalho, abordaremos separadamente as diferentes características dos rootkits, como os tipos existentes, as técnicas de ocultação, deteção e prevenção. O nosso objetivo é obter uma compreensão mais abrangente de seu funcionamento e aprender como nos podemos proteger dos ataques que utilizam estes recursos.

Através desta pesquisa, esperamos contribuir para o avanço do conhecimento e fornecer insights relevantes para a segurança informática. Estamos confiantes

de que esta investigação irá ajudar-nos a aprimorar as nossas habilidades e a desenvolver estratégias mais eficazes para enfrentar os desafios da segurança no mundo digital.

2 Fundamentação Teórica

Tal como mencionado anteriormente, um rootkit é um pacote de software projetado para proporcionar acesso não autorizado a um computador ou software. Este tipo de malware permite obter acesso remoto ao dispositivo da vítima, sem ser detetado, ganhando privilégios de administrador no sistema operativo. Desta forma, o rootkit pode executar uma série de ações maliciosas, alterando ou modificando o sistema da vítima.

O funcionamento de um rootkit baseia-se na inserção de código malicioso no dispositivo da vítima, de forma oculta e persistente. Ele age de maneira furtiva, evitando ser detectado por ferramentas de segurança convencionais. Ao obter controlo privilegiado, um rootkit pode realizar diversas ações prejudiciais, como ocultar outros tipos de malware, desativar ou violar programas de segurança, roubar dados sensíveis, espiar a vítima invadindo a sua privacidade, entre outros.

Esta capacidade de manipulação e controlo absoluto oferecida por um rootkit representa uma grave ameaça à segurança da vítima e pode ter impactos significativos tanto a nível pessoal quanto organizacional. Através do acesso não autorizado, os atacantes podem explorar vulnerabilidades, comprometer a integridade e a confidencialidade dos dados, além de violar a privacidade das vítimas.

Para combater efetivamente os rootkits, é essencial entender as técnicas de ocultação dos mesmos e as possíveis consequências da sua presença. A deteção precoce e a implementação de medidas preventivas são fundamentais para mitigar os riscos associados a esta ameaça.

3 História dos rootkits

1. 1990: Lane Davis e Steven Dake criam o primeiro rootkit conhecido na Sun Microsystems para o SunOS Unix OS.

2. 1999: Greg Hoglund publica um artigo que descreve a criação de um cavalo de Tróia chamado NTRootkit, o primeiro rootkit para Windows. É um exemplo de vírus rootkit que funciona no modo kernel.

3. 2003: o rootkit de modo de utilizador HackerDefender surge para Windows 2000 e Windows XP. O surgimento do HackerDefender desencadeou um jogo de gato e rato entre ele e a ferramenta anti-rootkit RootkitRevealer.

4. 2004: um rootkit é usado para aceder a mais de 100 telefones na rede da Vodafone na Grécia, incluindo o telefone usado pelo primeiro-ministro do país, num ataque que ficou conhecido como o Watergate grego.

5. 2005: a Sony BMG é atingida por um enorme escândalo depois de distribuir CDs que instalam rootkits como uma ferramenta anti pirataria, sem o consentimento dos consumidores.

6. 2008: o bootkit TDL-4, conhecido na época como TDL-1, alimenta o infame cavalo de Troia Alureon, usado para criar e manter botnets.

7. 2009: o rootkit Machiavelli, que é uma prova de conceito, tem como alvo o macOS (então chamado Mac OS X)e mostra que os Macs também são vulneráveis a malwares, como rootkits.

8. 2010: o worm Stuxnet, supostamente desenvolvido em conjunto por EUA e Israel, usou um rootkit para ocultar a sua presença ao atacar o programa nuclear iraniano.

9. 2012: um malware conhecido como Flame, modular e com 20 MB, é relativamente grande, já que muitos malwares têm menos de 1 MB e causou estragos em toda a infraestrutura no Oriente Médio e no norte da África.

10. 2018: LoJax é o primeiro rootkit que infecta o UEFI do computador, o firmware que controla a placa-mãe, permitindo que o LoJax sobreviva à reinstalação do sistema operativo.

11. 2019: ataque de rootkit recente vem do Scranos, um rootkit que rouba passwords e dados de pagamento armazenados no navegador. Notavelmente, transforma o computador em um farm de cliques para gerar secretamente receita de vídeo e subscritores do YouTube.

História realizada com base na história apresentada no site da avast (Referência: [1]).

4 Tipos de Rootkits

Existem várias classificações para rootkits dependendo se o malware sobrevive a um reboot e se o mesmo é executado em modo de utilizador ou kernel:

- Rootkits no modo de utilizador

  Um roorkit no modo de utilizador infeta a conta administrativa de um sistema operativo obtendo privilégios de nível superior necessários para alterar protocolos num computador enquanto se oculta a ele mesmo e outros malwares que utiliza. Este tipo de rootkit é iniciado automaticamente quando o computador é ligado.

- Rootkits no modo de kernel

  Este tipo de rootkit existe no computador ao nível do sistema operativo e como resultado compromete todo o sistema. O atacante intercepta as chamadas do sistema podendo adicionar os seus próprios dados, filtrando qualquer outro dado retornado pelo malware que possa levar a que este seja reconhecido. Este tipo de rootkit é muito difícil de desenvolver corretamente pois causa frequentes falhas no sistema.

- Rootkits híbridos

  Rootkits hibridos colocam componentes tanto a nível do utilizador como do kernel, isto permite que o rootkit tenha a estabilidade dos rootkits de modo de utilizador com a discrição aprimorada dos rootkits de kernel. A presença de componentes no nível do utilizador permite que o rootkit seja iniciado automaticamente quando o sistema é ligado, fornecendo acesso privilegiado e a capacidade de ocultar as suas atividades maliciosas. Já os componentes no nível do kernel permitem um controlo mais profundo sobre o sistema operativo, possibilitando manipulações de baixo nível. Esta combinação de recursos confere aos rootkits híbridos uma vantagem significativa em relação a outros tipos de rootkits pelo que são um dos tipos mais utilizados pelos criminosos.

- Rootkits de firmware

  Os rootkits de firmware representam uma ameaça avançada e preocupante, pois aproveitam o firmware, que é um software de baixo nível que controla componentes de hardware de um computador. Estes rootkits podem infectar o firmware, ocultando-se de forma persistente mesmo quando o sistema é desligado e reiniciado. O rootkit é reinstalado automaticamente a cada reinicialização, garantindo o seu funcionamento contínuo e a capacidade de realizar ações maliciosas no sistema. Os rootkits de firmware têm o potencial de causar danos significativos, uma vez que podem comprometer componentes críticos do hardware, como a BIOS (Basic Input/Output System) ou UEFI (Unified Extensible Firmware Interface), que são responsáveis por inicializar o sistema operativo.

- Bootkits

  Os bootkits, também conhecidos como rootkits bootloader, representam uma variante de rootkit no modo kernel que infecta o MBR (Master Boot Record) de um computador. O MBR é responsável por fornecer instruções sobre como iniciar o sistema operativo quando o computador é ligado. Portanto, sempre que o computador consulta o MBR, o bootkit também é carregado, permitindo que o malware persista e opere no sistema. Este tipo de rootkits tornaram-se obsoletos em muitos sistemas operativos modernos, como o Windows 8 e o Windows 10, que introduziram o recurso de Inicialização Segura (Secure Boot). A Inicialização Segura verifica a integridade do código de inicialização, incluindo o MBR, antes de carregar o sistema operativo. Isto ajuda a prevenir a execução de bootkits e outros malwares durante o processo de inicialização do sistema.

- Rootkits virtuais

  Os rootkits virtuais, também conhecidos como rootkits baseados em máquina virtual (VMBRs), representam uma forma avançada de rootkit que aproveita o uso de máquinas virtuais para ocultar as suas atividades. Uma máquina virtual é uma emulação baseada em software de um computador hospedado em um computador físico, permitindo a execução de múltiplos sistemas operativos ou a criação de ambientes isolados para testes. Os VMBRs carregam-se a si mesmos sob o sistema operativo original, agindo como uma camada intermediária entre o sistema operativo e o hardware real do computador, criando uma máquina virtual, onde o sistema operativo original é colocado e executado, isolado do host. A principal vantagem dos rootkits virtuais é que são executados separadamente do sistema operativo do computador, o que torna extremamente difícil a sua detecção.

5 Técnicas de Ocultação

Nesta secção iremos abordar as principais técnicas utilizadas pelos rootkits de forma a permanecerem ocultos no sistema:

- Injeção de código

  A injeção de código é uma técnica usada por rootkits para se ocultarem no sistema. Nesta técnica, o rootkit injeta o seu próprio código malicioso em processos legítimos do sistema operativo, aproveitando vulnerabilidades ou explorando mecanismos de execução de código. Ao injetar o código num processo legítimo, o rootkit pode camuflar-se e evitar a deteção por ferramentas de segurança convencionais, beneficia da confiança que os sistemas operativos e aplicações têm nestes processos, tornando a sua presença menos suspeita.

- Hooking de funções

  O hooking de funções é uma técnica utilizada por rootkits para se ocultarem no sistema, alterando o comportamento de funções legítimas do sistema operativo ou de aplicações. Esta técnica permite que o rootkit intercete chamadas de funções específicas e substitua o seu comportamento original por código malicioso. O rootkit aproveita-se de privilégios de administrador ou vulnerabilidades para modificar a estrutura de execução do sistema e garantir que as suas ações passem despercebidas.

- Manipulação de estruturas internas

  A manipulação de estruturas internas é uma técnica utilizada por rootkits para ocultação no sistema, alterando ou corrompendo estruturas de dados internas do sistema operativo. Estas estruturas de dados são utilizadas pelo sistema operativo para armazenar informações críticas sobre processos, arquivos, dispositivos e outras entidades do sistema. Ao manipular estas estruturas internas, o rootkit pode ocultar a sua presença e atividades maliciosas, interferir na funcionalidade normal do sistema operativo e enganar as ferramentas de segurança. Esta técnica requer um conhecimento profundo das estruturas internas do sistema operativo e, frequentemente, é específica para uma determinada versão do mesmo. Ao explorar vulnerabilidades ou fraquezas nestas estruturas, o rootkit consegue esconder a sua presença de forma eficaz.

6 Prevenção e Deteção

Muitas das estratégias para escapar a rootkits também são boas práticas e podem proteger o utilizador contra todo o tipo de ameaças, estas práticas passam por não abrir anexos de e-mails enviados por remetentes desconhecidos, não fazer download de arquivos desconhecidos, ter o sistema operativo e respetiva firewall atualizada e por fim ter um sistema de vigilancia instalado verificando se o mesmo é legítimo. (Referência: [4])

E se porventura acreditar que o meu sistema já foi infetado com um rootkit? De que forma o posso detetar? A verdade é que detetar um rootkit não é fácil pois o mesmo é projectado de forma a manter-se oculto, no entanto existem algumas ocasiões que podem indicar a presença de um rootkit tais como:

Aquilo que um utilizador comum pode verificar:

- Ecrã azul - Em computadores Windows a constante presença de um ecrã azul que force a reinicialização pode indicar a existência de um rootkit.
- Comportamento incomum do browser - Quando um rootkit é instalado, o browser pode apresentar um comportamento estranho, exibindo favoritos desconhecidos e redirecionado constantemente para url's não pretendidos.
- Baixo desempenho - O computador demora muito tempo a iniciar e quando liga funciona de forma lenta.
- Configurações mudam sem permissão (Windows) - Alterações como mudança do protector de ecrã e barra de tarefas oculta.
- Páginas da web não funcionam como deveriam - O carregamento de páginas é interrompido e o tráfego de rede é excessivo.

Utilizadores avançados:

- Pesquisa por caracteres – A pesquisa por caracteres conhecidos, como nomes de ficheiros de configuração, utilizadores, palavras passe, endereços IP, entre outros, em binários trojaned, pode indicar a presença de um rootkit no sistema;
- Verificação de integridade – A verificação e comparação periódica de hashes de programas e ficheiros contra hashes geradas após uma instalação inicial do sistema, pode indicar a presença de alterações maliciosas em ficheiros, causadas por rootkits;
- Verificação de processos do sistema e bibliotecas – pode indicar acessos indevidos a ficheiros de configuração utilizados por rootkits;
- Análise de MAC times – MAC times de programas e ficheiros pode auxiliar no isolamento de possíveis alterações feitas após um ataque;

- Análise de Ligações de rede – A verificação por portas abertas e ligações suspeitas pode indicar a presença de um backdoor remoto no sistema;
- Analise processos do sistema e símbolos do kernel –símbolos incomuns no kernel podem indicar a presença de um rootkit em nível de kernel;

7 Conclusão

Em suma, ao longo deste trabalho, tivemos a oportunidade de aprofundar os nossos conhecimentos em segurança informática, explorando especificamente o tema dos rootkits. Ao compreender a natureza dos rootkits e suas capacidades ocultas, percebemos a necessidade crítica de proteger os nossos sistemas e redes contra estas ameaças, a segurança informática tornou-se uma preocupação fundamental, tanto para utilizadores domésticos quanto para organizações de todos os tamanhos. Foi um trabalho muito interessante de desenvolver que nos deu um pequeno vislumbre daquilo que é a segurança informática e que nos faz considerar a possibilidade de seguir carreira neste campo desafiador e em constante mudança. Em resumo, esta pesquisa sobre rootkits serviu como um ponto de partida para nossa jornada em direção a um futuro promissor no campo da segurança informática, com novos desafios pela frente, estamos entusiasmados para continuar aprendendo e contribuindo para tornar o mundo digital um lugar mais seguro.

Referências

[1] BURDOVA, Carly. O que é um rootkit e como removê-lo?. 2021. Disponível em: https://www.avast.com/pt-br/c-rootkit. Acesso em: 17/06/2023.

[2] Santos, Patrícia Isabel Pinho. Segurança informática: a importância para a segurança interna. 2016. Disponível em: https://comum.rcaap.pt/handle/10400.26/24845. Acesso em: 17/06/2023.

[3] Russinovich, Mark. RootkitRevealer v1.71. 2006. Disponível em: https://learn.microsoft.com/en-us/sysinternals/downloads/rootkit-revealer. Acesso em: 17/06/2023.

[4] AVG Signal Team. Tudo o que você precisa saber sobre rootkits e como se proteger contra essas ameaças . 2020. Disponível em: https://www.avg.com/pt/signal/what-is-rootkit. Acesso em: 17/06/2023.

[5] Wagner, Pedro. Como identificar um rootkit . 2022. Disponível em: https://tecnoblog.net/responde/como-detectar-e-remover-um-rootkit-windows-mac/. Acesso em: 17/06/2023.

[6] Pinto, Pedro. Sabe o que são Rootkits? Saiba como detectar . 2016. Disponível em: https://pplware.sapo.pt/internet/sabe-sao-rootkits-saiba-detectar/. Acesso em: 17/06/2023.