Resumo de solução

Proteção contra malware de GPU

No **Relatório do McAfee® Labs sobre ameaças: agosto de 2015**, examinamos de perto o malware que foge à regra de aproveitar a CPU ou a memória de sistema de um endpoint e que, em vez disso, ataca a unidade de processamento gráfico (GPU).

Malware que ataca ou se aproveita da GPU de um endpoint não é novidade. Cavalos de Troia mineradores de Bitcoins que aproveitam a capacidade de processamento da GPU para aumentar seus ganhos potenciais com o sistema comprometido já estão à solta (in the wild) há pelo menos quatro anos. No entanto, o lançamento de código de prova de conceito que alega aproveitar capacidades de GPU de maneiras nunca antes vistas colocou novamente em destaque o malware baseado em GPU. As alegações, discutidas amplamente no relatório, podem ser divididas em quatro pontos principais:

- Acesso à memória do host da CPU a partir da GPU.
- Subsequente exclusão de arquivos do host da CPU.
- Persistência entre reinicializações a quente.
- Ausência de ferramentas de análise de GPU.

As ameaças de GPU são um problema real, embora o malware que realize esse tipo de ataque ainda seja apenas uma prova de conceito. Ainda não vimos proliferação alguma à solta. A ausência de ferramentas que possam realizar análises forenses em GPUs resultou em uma situação na qual a engenharia reversa e a perícia são uma tarefa muito mais complexa e desafiadora do que analisar ataques que aproveitam memória ou CPUs. Os atacantes reduziram a superfície de detecção ao mover o código malicioso para fora da CPU e da memória, embora não por completo, pois elementos residuais de suas atividades costumam permanecer no endpoint.

Sem dúvida, os atacantes aprimorarão o malware baseado em GPU e só o tempo dirá o quanto esse tipo de ataque se tornará predominante.

Proteção contra malware de GPU

O McAfee Labs recomenda várias maneiras de proteger sistemas contra ataques de GPU:

- Ative as atualizações automáticas dos sistemas operacionais ou faça download das atualizações dos sistemas operacionais regularmente para manter os sistemas protegidos contra vulnerabilidades conhecidas.
- Instale patches de outros fabricantes de software tão logo eles sejam distribuídos.
- Instale software de segurança em todos os endpoints e mantenha atualizadas as assinaturas antimalware.

Intel Security

- Considere uma lista branca de aplicativos para proibir a execução de aplicativos não autorizados.
- Evite, sempre que possível, executar aplicativos em modo de administrador.

Como a Intel Security pode ajudá-lo a se proteger contra malware de GPU

McAfee Advanced Threat Defense

O **McAfee Advanced Threat Defense** é uma solução de detecção de malware em múltiplas camadas que combina vários mecanismos de inspeção. Ao combinar múltiplos mecanismos que aplicam inspeção com base em assinaturas e em reputação, emulação em tempo real, análise completa de código estático e análise dinâmica em área restrita (sandbox), o McAfee Advanced Threat Defense ajuda a proteger contra malware avançado.

- **Detecção com base em assinatura:** detecta vírus, worms, spyware, bots, cavalos de Troia, estouros de buffer e ataques combinados. O McAfee Advanced Threat Defense inclui uma base de conhecimentos abrangente, criada e mantida pelo McAfee Labs e que atualmente contém mais de 150 milhões de assinaturas.
- **Detecção com base em reputação:** consulta a reputação dos arquivos utilizando o serviço McAfee Global Threat Intelligence (McAfee GTI) para detectar ameaças recém-surgidas.
- **Análise estática e emulação em tempo real:** oferece emulação e análise estática em tempo real para localizar rapidamente malware e ameaças de dia zero não identificados por reputação ou técnicas com base em assinaturas.
- **Análise completa de código estático:** faz a engenharia reversa do código do arquivo para determinar todos os seus atributos e conjuntos de instruções, e analisar completamente o código-fonte sem execução. Seus recursos de descompactação abrangentes abrem todos os tipos de arquivos compactados para a análise completa e classificação do malware, permitindo que a sua empresa entenda a ameaça representada pelo malware em questão.
- **Análise dinâmica em área restrita (sandbox):** executa o código do arquivo em um ambiente de tempo de execução virtual e observa o comportamento resultante. Ambientes virtuais podem ser configurados conforme os ambientes de host da sua empresa, com suporte para imagens personalizadas de sistema operacional (SO) Microsoft Windows 7 (32/64 bits), Windows XP, Windows Server 2003, Windows Server 2008 (64 bits) e Android.

McAfee VirusScan Enterprise

O **McAfee VirusScan® Enterprise** utiliza o premiado mecanismo de varredura da Intel Security para proteger os seus arquivos contra vírus, worms, rootkits, cavalos de Troia e outras ameaças avançadas.

- **Proteção proativa contra ataques:** integra tecnologia antimalware com prevenção de intrusões para proteção contra ataques que utilizam explorações de estouro de buffer direcionadas contra vulnerabilidades em aplicativos.
- **Detecção e limpeza de malware imbatíveis:** protege contra ameaças, como rootkits e cavalos de Troia, com análise comportamental avançada. Detém o malware utilizando várias técnicas, como bloqueio de portas, nomes de arquivos, pastas/diretórios e compartilhamentos de arquivos, bem como rastreamento e bloqueio de infecções.
- **Segurança em tempo real com integração com o McAfee GTI:** protege contra ameaças conhecidas e emergentes em todos os vetores de ameaça — arquivos, Web, e-mail e rede — com o suporte da plataforma de inteligência sobre ameaças mais abrangente do mercado.

McAfee Threat Intelligence Exchange

É imprescindível dispor de uma plataforma de inteligência adaptável para atender às necessidades do seu ambiente. O **McAfee Threat Intelligence Exchange** reduz significativamente a exposição a ataques, graças à sua visibilidade sobre ameaças imediatas, como aplicativos ou arquivos desconhecidos.

- **Informações abrangentes sobre ameaças:** personalize facilmente informações abrangentes sobre ameaças obtidas de fontes de dados de inteligência global. Essas fontes podem ser o McAfee GTI ou canais de terceiros, com informações locais sobre ameaças obtidas de dados de eventos históricos e em tempo real fornecidos via endpoints, gateways e outros componentes de segurança.
- **Prevenção de execução e correção:** o McAfee Threat Intelligence Exchange pode intervir e impedir que aplicativos desconhecidos sejam executados no ambiente. Caso um aplicativo cuja execução tenha sido permitida seja posteriormente considerado malicioso, o McAfee Threat Intelligence Exchange pode desativar os processos em execução associados ao aplicativo em todo o ambiente, graças às suas poderosas capacidades de imposição de políticas e gerenciamento central.
- **Visibilidade:** o McAfee Threat Intelligence Exchange pode rastrear todos os arquivos executáveis compactados e sua execução inicial no ambiente, bem como todas as alterações ocorridas a partir de então. Essa visibilidade sobre as ações de um aplicativo ou processo, desde a instalação até o estado atual, permite mais rapidez na resposta e na correção.
- **Indicadores de comprometimento (IoCs):** os IoCs frequentemente importam hashes de arquivos nocivos. O McAfee Threat Intelligence Exchange pode imunizar o seu ambiente contra esses arquivos notoriamente nocivos através da imposição de políticas. Caso algum dos IoCs seja acionado no ambiente, o McAfee Threat Intelligence Exchange pode eliminar todos os processos e aplicativos associados com o IoC.

McAfee Application Control

O **McAfee Application Control** permite que a sua empresa controle quais aplicativos têm permissão para serem executados no seu ambiente através de listas brancas dinâmicas e imposição de políticas para endpoints conectados e desconectados — garantindo que a sua organização seja protegida contra aplicativos vulneráveis ou notoriamente maliciosos.

- **Listas brancas dinâmicas:** permitem que sua organização gerencie de forma eficiente os aplicativos relacionados em listas brancas, elaborando tais listas automaticamente conforme os sistemas são corrigidos e atualizados.
- **Reputação de arquivos:** a integração com o McAfee GTI permite que o McAfee Application Control consulte canais em tempo real sobre tipos de arquivos conhecidos como válidos, conhecidos como nocivos e desconhecidos, auxiliando a lista branca e mantendo a sua empresa ciente de vulnerabilidades ou ataques de aplicativos que podem ter sido alterados.
- **Mantenha-se protegido, conectado ou desconectado:** imponha controles a servidores conectados ou desconectados, máquinas virtuais, endpoints e dispositivos de função fixa, como terminais de ponto de venda.

McAfee. Part of Intel Security.
Av. das Nações Unidas, 8.501 - 16° andar
CEP 05425-070 - São Paulo - SP - Brasil
Telefone: +55 (11) 3711-8200
Fax: +55 (11) 3711-8286
www.intelsecurity.com