Resumo de solução

Proteção contra manipulação de BIOS e firmware

No ***Relatório do McAfee Labs sobre ameaças: maio de 2015***, examinamos em detalhes o Equation Group e seus ataques contra firmware de discos rígidos e unidades de estado sólido. O "Equation Group" (em português, grupo da equação), cujo nome foi derivado de sua afinidade por esquemas de criptografia ultrassofisticados e do malware associado ao grupo, está entre os exemplos mais visíveis e avançados de ataque de firmware já vistos.

Uma das descobertas mais importantes da pesquisa são os módulos de reprogramação do firmware de unidades de risco rígido (HDD) e de estado sólido (SSD). As unidades HDD/SSD cujo firmware foi reprogramado podem recarregar o malware associado a cada inicialização do sistema infectado. O malware persiste mesmo que as unidades sejam reformatadas ou que o sistema operacional seja reinstalado. Além disso, assim que a unidade é infectada, o firmware reprogramado e o malware associado ficam indetectáveis pelo software de segurança.

Nos últimos anos, a Intel Security tem estudado diversos exemplos de malware com recursos de manipulação de BIOS ou firmware. Eles foram observados em cenários acadêmicos ou de prova de conceito e em cenários reais, incluindo **CIH/Chernobyl**, Mebromi e **BIOSkit**. Nós também prevemos esse tipo específico de ataque no *Relatório do McAfee Labs sobre previsões sobre ameaças em 2012*. Com a descoberta de amostras características do Equation Group, elas agora são, para nós, um dos exemplos mais visíveis e avançados de ataque de firmware já antes visto.

Proteção contra ataques Equation Group

Apresentamos a seguir políticas e procedimentos recomendados para proteção contra ataques no estilo do Equation Group:

- Instale um software de segurança de endpoint em todos os endpoints.
- Ative as atualizações automáticas dos sistemas operacionais ou faça download das atualizações dos sistemas operacionais regularmente, para mantê-los protegidos contra vulnerabilidades conhecidas.
- Instale patches de outros fabricantes de software tão logo eles sejam distribuídos.
- Criptografe discos rígidos e dados importantes.
- Elimine campanhas de phishing em massa com filtragem de e-mails no gateway seguro.
- Implemente verificação da identidade do remetente para reduzir o risco de que criminosos cibernéticos sejam inadvertidamente considerados confiáveis.

intel Security

- Detecte e elimine anexos maliciosos com antimalware avançado.
- Faça uma varredura de URLs nos e-mails quando recebidos e novamente quando clicados.
- Faça uma varredura do tráfego da Web quanto à presença de malware quando o phishing conduz o usuário em uma jornada de cliques até a infecção.
- Conscientize os usuários sobre as práticas recomendadas para detectar e agir em relação a e-mails suspeitos.
- Implemente a prevenção de perda de dados para deter o vazamento no caso de uma violação.

Como a Intel Security pode ajudá-lo a se proteger contra ataques no estilo do Equation Group

A proteção contra ataques de manipulação de BIOS e firmware deve fazer parte da estratégia de segurança de todas as empresas. Para tanto, elas devem priorizar duas frentes de atuação:

- Estabelecer formas de detectar a entrega inicial do malware do Equation Group. Os vetores de ataque conhecidos são phishing, CDs e unidades USB. Atente especialmente para essas áreas.
- Proteger os sistemas contra vazamento de dados. Embora hoje não seja possível detectar o módulo de reprogramação de firmware, é altamente provável que o objetivo geral do ataque seja o reconhecimento. Como o reconhecimento depende da comunicação sistemática e do vazamento de dados com um servidor de controle, é extremamente importante impedi-lo.

McAfee Advanced Threat Defense

O **McAfee Advanced Threat Defense** é uma solução de detecção de malware multicamada que reúne múltiplos mecanismos de inspeção que aplicam inspeção com base em assinatura e em reputação, emulação em tempo real, análise completa de código estático e área restrita dinâmica. O McAfee Advanced Threat Defense ajuda a proteger contra malware avançado que tenha sido instruído a recarregar pelo firmware reprogramado do Equation Group.

- **Detecção com base em assinatura:** detecta vírus, worms, spyware, bots, cavalos de Troia, estouros de buffer e ataques combinados. Sua abrangente base de conhecimentos é criada e mantida pelo McAfee Labs, e 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 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:** 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 Windows 7 (32/64 bits), Windows XP, Windows Server 2003, Windows Server 2008 (64 bits) e Android.

McAfee Threat Intelligence Exchange
É imprescindível dispor de uma plataforma de inteligência capaz de se adaptar 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.

- **Inteligência abrangente 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 momento presente, permite mais rapidez na resposta e na correção.
- **Indicadores de comprometimento (IoCs):** importe hashes de arquivos nocivos conhecidos para que o McAfee Threat Intelligence Exchange imunize o seu ambiente contra esses arquivos notoriamente nocivos através da imposição de políticas. Caso algum dos indicadores de comprometimento (IoCs) seja acionado no ambiente, o McAfee TIE pode eliminar todos os processos e aplicativos associados com o IoC.

McAfee VirusScan Enterprise
O **McAfee VirusScan® Enterprise** utiliza o premiado mecanismo de varredura da McAfee 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 técnicas, como bloqueio de portas, nomes de arquivos, pastas/diretórios e compartilhamento 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 Network Security Platform
O **McAfee Network Security Platform** foi desenvolvido para realizar inspeções profundas no tráfego de rede. Ele reúne técnicas de inspeção avançadas, que incluem análise completa de protocolo, reputação de ameaças, análise de comportamento e análise avançada de malware para detectar e impedir ataques conhecidos e de dia zero na rede.

- **Defesa abrangente contra malware:** reúne reputação de arquivos do McAfee GTI, análise profunda de arquivos com detecção de JavaScript e análise avançada de malware, sem assinaturas, para detectar e deter ameaças de dia zero, malware personalizado e outros ataques furtivos.

- **Utiliza técnicas avançadas de detecção:** inclui análise completa de protocolo, reputação de ameaças e análise de comportamento para detectar e prevenir ataques conhecidos e de dia zero na rede.
- **Integração com o McAfee Global Threat Intelligence:** combina canais de geolocalização, reputação de IP e reputação de arquivos em tempo real com dados contextuais detalhados sobre usuários, dispositivos e aplicativos para respostas rápidas e precisas a ataques via rede.
- **Security Connected:** uma integração decisiva com o McAfee Advanced Threat Defense permite ao McAfee Network Security Platform enviar para o McAfee Advanced Threat Defense aquivos suspeitos encontrados no tráfego monitorado e permiti-los ou proibi-los, com base em descobertas do McAfee Advanced Threat Defense.

McAfee DLP Monitor

O **McAfee Data Loss Prevention (DLP) Monitor** coleta, rastreia e gera relatórios sobre dados transmitidos em toda a rede. Descubra com facilidade ameaças aos dados desconhecidas para protegê-los e garantir que sua empresa não sofra uma grande violação.

- **Examine o tráfego de rede:** os recursos de análise e varredura de dados do McAfee DLP Monitor são líderes no setor e examinam o tráfego de rede em um nível profundo.
- **Identifique os dados rapidamente:** os recursos de descoberta em tempo real oferecem com rapidez detalhes sobre a forma como os dados estão sendo usados, quem os está usando e o destino deles, fornecendo informações suficientes para que você possa tomar uma atitude. O McAfee DLP Monitor identifica com rapidez mais de 300 tipos de conteúdo sendo transportados por qualquer porta ou protocolo, garantindo visibilidade para a sua empresa.
- **Análise forense detalhada:** realize análises forenses para correlacionar eventos de risco atuais e passados, detectar tendências de risco e identificar ameaças. Permite que você entenda a situação rapidamente e desenvolva regras e políticas para lidar com o problema.

McAfee DLP Prevent

O **McAfee Data Loss Prevention (DLP) Prevent** protege contra a perda de dados garantindo que os dados deixem a rede apenas quando for apropriado, seja por e-mail, Webmail, mensagens instantâneas, wikis, blogs, portais, HTTP/HTTPS ou transferências FTP. A capacidade de identificar e mitigar tentativas de vazamento com rapidez é essencial para manter seus valiosos dados seguros e evitar o próximo grande escândalo.

- **Visibilidade para incidentes de segurança:** visualizações personalizadas e relatórios de incidente fornecem informações resumidas e detalhadas sobre incidentes de segurança e suas ações corretivas.
- **Imponha proativamente o cumprimento das políticas para todos os tipos de informações:** imponha políticas para informações reconhecidamente confidenciais e também para informações não tão óbvias que você talvez desconheça. Com uma ampla gama de políticas internas, que incluem desde a conformidade e o uso aceitável até a propriedade intelectual, você pode fazer a correspondência de documentos parciais ou integrais com um conjunto de regras para proteger todas as suas informações confidenciais.

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