Proteja seus negócios com a McAfee.

Night Dragon - O que você precisa saber

Prezado Cliente,

Como você já deve ter lido em sites de notícias, como Wall Street Journal, New York Times, Financial Times, Reuters, entre outros, a McAfee descobriu uma grande sequência de ataques (batizada de "Night Dragon" ou "Dragão Noturno"), criada para roubar dados confidenciais de organizações específicas. A McAfee vem acompanhando esse ataque há algum tempo e **já incluimos proteção contra o "Night Dragon"** (e proteção contra ameaças semelhantes) **às soluções de segurança da McAfee**. Para obter a melhor defesa contra o Night Dragon e outros ataques, como sempre, recomendamos o uso de versões atualizadas e mais recentes das soluções da McAfee para terminais e redes, com assinaturas atualizadas e com o Global Threat Intelligence ativado.

Sumarizamos algumas informações e ferramentas importantes sobre esses ataques para que você seja capaz de proteger sua organização de maneira mais eficiente e eficaz.

Faça o download agora **whitepaper "Ciberataques ao setor energético mundial: Night Dragon (Dragão Noturno)" (em português)**

Night Dragon (Dragão Noturno)

Os ataques do Night Dragon são semelhantes à Operação Aurora (embora não estejam ligados à Operação Aurora) e outras ameaças avançadas persistentes (APTs - Advanced Persistent Threats), pois trata-se de uma combinação de engenharia social e ciberataques bem coordenados e dirigidos, utilizando cavalos de Troia, software de controle remoto e outros tipos de malware. Embora os ataques Night Dragon só tenham se intensificado recentemente, a McAfee associou esses ataques às invasões iniciadas em novembro de 2009 que podem estar aproveitando técnicas detectadas já em 2008. Agora, novos ataques Night Dragon estão sendo identificados a cada dia.

A McAfee tem provas de infecções pelo malware Night Dragon nas Américas, na Europa e na Ásia, bem como em países do Oriente Médio e do Norte da África. A McAfee também identificou as ferramentas, as técnicas e as atividades de rede utilizadas durante estes ataques contínuos, que podem ter sido originados na China.

Atualmente, os atacantes que usam o Night Dragon estão focando em empresas globais de petróleo, energia e petroquímica com a aparente intenção de roubar informações sigilosas, tais como detalhes de operação, pesquisas de exploração e dados financeiros. Embora a McAfee esteja trabalhando em estreita colaboração com muitas dessas empresas e órgãos policiais, nossa intenção com este comunicado é alertar as organizações que talvez não tenham as defesas mais recentes instaladas ou que possam se beneficiar de informações adicionais. E embora tenhamos confirmado que o Night Dragon está atualmente voltado para organizações dos setores de petróleo/ gás/ petroquímica/ energia, APTs semelhantes podem ser (e são) dirigidas a organizações de praticamente todos os setores de atividade econômica. Ao contrário do Stuxnet, os ataques Night Dragon não são voltados necessariamente a um setor específico.

Detalhes do ataque

Os ataques Night Dragon utilizam ciberataques coordenados, disfarçados e dirigidos, aproveitando de engenharia social, spearphishing, explorações de vulnerabilidades do sistema operacional Windows, comprometimentos do Active Directory e ferramentas de administração remota (RATs). A sequência do ataque é a seguinte:

1. Servidores da Web voltados para o público são comprometidos através de injeção de SQL; malwares e RATs são instalados
2. Os servidores da Web comprometidos são utilizados para comandar ataques contra alvos internos
3. Ataques de spearphishing a profissionais que utilizam celulares conectados a VPNs são utilizados para aumentar os direitos de acesso interno
4. Os atacantes utilizam ferramentas de roubo de senhas para acessar outros sistemas – instalando RATs e malware à medida que prosseguem
5. Sistemas pertencentes a executivos são atacados em busca de e-mails e arquivos que são capturados pelos atacantes

Para mais informações, **leia o whitepaper** **"Ciberataques ao setor energético mundial: Night Dragon (Dragão Noturno)" (em português)**, escrito pelos especialistas em segurança da McAfee, faça o download de uma apresentação sobre o Night Dragon, acesse o post sobre Night Dragon no blog do CTO da McAfee, George Kurtz, e visite o site do Night Dragon (em inglês).

Perguntas e respostas sobre o Night Dragon

P: Como posso saber se a minha empresa está infectada?
R: Atualize os DATs do seu antivírus ao menos na versão 6232 e verifique se as varreduras sob demanda estão funcionando corretamente; execute uma varredura completa de vírus no sistema de arquivos. Avalie o ePO e leia os alertas de antivírus e os logs de rede para identificar os sistemas comprometidos.

A McAfee oferece ferramentas para ajudá-lo:

- Utilitário de Detecção de Remoção do Night Dragon (Stinger)
- Varredura de Vulnerabilidade do Night Dragon

Se você descobriu a presença do Night Dragon na sua empresa e gostaria de reagir ao incidente ou de obter assistência pericial, envie amostras para Virus_Research@avertlabs.com ou pelo site McAfee Labs WebImmune.

P: Existe alguma detecção de rede/IDS disponível?
R: Sim. Nas comunicações de rede, preste atenção ao string que indica um computador infectado enviando um "guia" para um servidor de comando e controle: "\x01\x50\x00\x00\x00\x00\x00\x00\x00\x00\x01\x68\x57\x24\x13". Entre em contato com a McAfee para obter mais suporte sobre informações de rede.

P: É possível encontrar o Night Dragon sem perícia de informática?
R: Sim. A DLL é simplesmente um atributo de arquivo Oculto ou Sistema e pode ser encontrada pelo tamanho (19-23kb), geralmente na pasta C:\Windows\System32 ou C:\Windows\SysWow64. Existem outros artefatos no sistema de arquivos que podem identificar quando o dropper instalou a DLL de backdoor, bem como os tipos de atividades realizadas pelo atacante (Área de Trabalho Remota, Command Shell, etc).

P: Se encontrarmos o Night Dragon, precisamos nos preocupar com a infecção de outros computadores?
R: Não. O Night Dragon não tem os recursos de infecção de um worm e não se propaga. O Night Dragon é um cavalo de Troia instalado em um sistema através de um arquivo dropper de cavalo de Troia (.exe) que é copiado nos computadores por um atacante - geralmente através de compartilhamentos do Windows.

Soluções da McAfee para combater o Night Dragon

APTs são ataques sofisticados e multifacetados que exigem uma defesa coordenada e bem arquitetada. Estamos confiantes de que a McAfee é a única capaz de lidar com as APTs (inclusive o Night Dragon) e outros ataques direcionados. **A McAfee já adicionou a proteção contra o Night Dragon em suas tecnologias de segurança mais recentes**. Confira abaixo algumas soluções da McAfee que, operando juntas, ajudam a combater ataques como o Night Dragon:

- McAfee Host Intrusion Prevention conta com um recurso de detecção de APTs para correlacionar e detectar RATs e vazamento de dados
- McAfee Application Control (MAC) impede o malware por não permitir a execução de software que não seja aprovado
- McAfee Configuration Control (MCC) proíbe alterações de configuração que não sejam aprovadas
- McAfee Vulnerability Manager (MVM) detecta sistemas infectados e os pontos fracos de segurança nesses sistemas
- McAfee VirusScan Enterprise (VSE) oferece proteção com os DATs antivírus 6263 e posteriores
- McAfee Policy Auditor detecta pontos fracos de segurança em sistemas comprometidos
- McAfee Risk Advisory (MRA) permite ver os erros de configuração e as falhas de segurança que permitem explorações
- McAfee Network Threat Response (NTR) detecta tráfego de comando e controle
- McAfee Network Security Manager (NSM) detecta tráfegos mal-intencionados na rede e alertas, permitindo uma reação rápida
- McAfee Firewall Enterprise atenua as penetrações na rede e pode ser instalado em níveis para reduzir os ataques internos à rede
- McAfee Web Gateway atenua as operações de RAT
- McAfee Endpoint Encryption reduz a possibilidade de uso de informações sigilosas específicas

- McAfee Data Loss Protection (DLP) impede e detecta a extração de dados sigilosos

Os últimos anos foram turbulentos: os ataques ao Google e muitas outras empresas com a Operação Aurora, ataques a infra-estruturas críticas com o Stuxnet, pessoas com acesso privilegiado roubando informações que levaram à divulgação de documentos pelo Wikileaks, e assim por diante. Agora, o "Night Dragon" está prestes a entrar na disputa pelas manchetes.

O compromisso da McAfee é fazer tudo que estiver ao nosso alcance para proteger você e a sua empresa desses ataques. Se você gostaria de obter mais informações sobre o Night Dragon ou qualquer coisa que ameace a sua segurança virtual:

whitepaper "Ciberataques ao setor energético mundial: Night Dragon (Dragão Noturno)" (em português)

Ou entre em contato conosco

Atenciosamente,

Robert Dyer
Vice Presidente
McAfee América Latina