Resumo de solução

Proteção contra o Pinkslipbot

O W32/Pinkslipbot é uma família de malware autopropagável criada para roubar dados pessoais e financeiros de suas vítimas. Esse malware permite total controle sobre os sistemas infectados através de um backdoor com base em comandos operado pelo servidor de controle, bem como um backdoor com base em computação de rede virtual. O Pinkslipbot também pode se espalhar por outros sistemas do ambiente através de compartilhamentos de rede e pode se comunicar com seu servidor de controle para fazer download de versões atualizadas de si próprio.

O Pinkslipbot foi identificado inicialmente em 2007, mas o grupo que o criou vem fazendo manutenção de sua base de código adicionando atualizações incrementais antes de colocar uma nova versão à solta em intervalos de alguns meses.

Os dados roubados pelo Pinkslipbot permitem que o atacante determine a localização, a organização e o proprietário do sistema infectado. O atacante pode vender essas informações (especialmente quando oriundas de uma organização de destaque) para terceiros e distribuir malware direcionado no sistema comprometido após o pagamento ser efetuado.

Para uma visão técnica aprofundada sobre o Pinkslipbot, consulte o *Relatório do McAfee Labs sobre ameaças: junho de 2016*. O relatório discute o processo de infecção inicial, mecanismos de propagação, detalhes técnicos e métodos gerais de proteção.

Políticas e procedimentos para proteção contra o Pinkslipbot

Seguem alguns procedimentos e políticas gerais que podem ajudá-lo a se proteger contra o Pinkslipbot.

Para proteger o perímetro, você deve bloquear as portas não utilizadas em todos os pontos de saída da rede, solicitações de conexão de/para endereços IP associados que sejam sabidamente maliciosos e o uso de compartilhamentos de rede para deter o movimento lateral do Pinkslipbot. Na maioria dos ambientes, você também deve desativar o recurso AutoRun do Microsoft Windows. É fundamental atualizar aplicativos e sistemas operacionais Windows aos níveis de patch mais recentes, bem como atualizar o software antimalware com a versão mais recente.

Sistemas não corrigidos permitem que vulnerabilidades sejam exploradas. Um gerenciamento bem-sucedido de patches é necessário para qualquer ambiente. Quando os patches são lançados pelo fornecedor, eles devem ser imediatamente testados, verificados e implementados. Quando a aplicação de patches não for possível devido a dependências de uma versão antiga, deverá haver um outro mecanismo disponível para minimizar a exploração de vulnerabilidades conhecidas. O gerenciamento agressivo de patches é, comprovadamente, um dos métodos mais eficazes para minimizar os efeitos do Pinkslipbot e de outros tipos de malware.

intel Security

Embora o Pinkslipbot seja entregue principalmente por downloads de passagem em sites comprometidos por kits de exploração, as vítimas normalmente são direcionadas para esses sites a partir de e-mails de phishing. Com os e-mails marcados como “internos” ou “externos”, os usuários têm mais chances de identificar e-mails de phishing ou falsificados e reconsiderar sua intenção de clicar em links maliciosos desconhecidos.

O Pinkslipbot é executado parcialmente na memória, portanto, não basta simplesmente aplicar patches nos sistemas, realizar uma varredura completa e executar uma ferramenta de remoção de malware. Os sistemas infectados precisam de uma reinicialização para remover o malware da memória e de uma nova varredura para assegurar que o sistema está limpo. Também recomendamos utilizar senhas fortes para deter violações por ataques de dicionário, desativar o AutoRun e colocar em prática o princípio de “privilégio mínimo”.

O Pinkslipbot é uma evolução agressiva do notório cavalo de Troia Zeus. Basta uma senha de login fraca para que um sistema Windows seja infectado pelo Pinkslipbot, mesmo sem exposição a um kit de exploração ou interação com usuários. A partir do momento em que o sistema é infectado, qualquer atividade realizada no sistema é registrada e enviada aos atacantes. Com a introdução de comunicação segura e personalizada com os servidores de controle, o Pinkslipbot está se tornando mais difícil de detectar e analisar. Seu histórico sugere que ele se tornará mais perigoso a cada nova iteração. Compreendendo seu ambiente e implementando as políticas e os procedimentos que recomendamos, você pode minimizar os danos que o Pinkslipbot pode causar.

Como a Intel Security pode ajudá-lo a se proteger contra o Pinkslipbot

McAfee VirusScan Enterprise (VSE) e McAfee Endpoint Security (ENS) 10

O McAfee VirusScan Enterprise e o McAfee Endpoint Security 10 oferecem proteção antimalware avançada para sistemas de endpoint. O McAfee VirusScan Enterprise foi substituído pelo McAfee Endpoint Security 10, que proporciona um desempenho mais rápido em uma plataforma otimizada. Os DATs da Intel Security para o McAfee VirusScan Enterprise e para o McAfee Endpoint Security 10 contêm capacidades de detecção e limpeza para componentes do Pinkslipbot. O McAfee VirusScan Enterprise e o McAfee Endpoint Security 10 oferecem vários níveis de proteção através de mecanismos de detecção de memória, antirrootkit, comportamentais e estáticos. Para camadas adicionais de proteção contra novas variantes, você pode implementar regras de proteção de acesso para evitar que o Pinkslipbot infecte sistemas.

- Crie e teste uma regra de proteção de acesso para impedir a execução de quaisquer arquivos executáveis em C:\Users*\AppData\Roaming\Microsoft**.exe.
- Crie e teste uma regra de proteção de acesso para evitar que os processos cscrpit.exe e wscript.exe leiam, executem e criem arquivos WPL na pasta %LOCALAPPDATA%\Microsoft\. Estes normalmente são arquivos JavaScript. Bloquear esses arquivos pode impedir que o malware faça download de novas versões.
- Crie e teste uma regra de proteção de acesso para evitar que os processos cscrpit.exe e wscript.exe leiam e executem arquivos na pasta %UserProfile%, supondo que seja viável.
- Crie e teste uma regra de proteção de acesso para evitar que “updates_*new.cb”, “upd_*.cb” e “updates*_new.cb” sejam executados ou criem novos arquivos. Estes costumam ser utilizados por arquivos de configuração do Pinkslipbot. Bloquear esses arquivos pode impedir que o malware se atualize.
- Crie e teste uma regra de proteção de acesso nas portas de 65200 a 65400 para os processos iexplorer.exe e explorer.exe. Como o Pinkslipbot injeta a si próprio nesses processos, impedir que essas portas sejam utilizadas por esses processos evita que o Pinkslipbot se comunique com seu servidor de controle.
- Implemente e teste regras de proteção de acesso para evitar a execução remota de arquivos autorun.inf.

McAfee Host Intrusion Prevention (HIPS)
O McAfee Host Intrusion Prevention protege sistemas contra ameaças de dia zero combinando um sistema de prevenção de intrusões comportamental e por assinaturas com um firewall dinâmico com monitoramento de estado. Atualizações de conteúdo programadas protegem sistemas contra vulnerabilidades em aplicativos e no sistema operacional, mesmo antes que patches estejam disponíveis. Reforce a segurança do ambiente ativando assinaturas para prevenir muitos dos métodos frequentemente empregados pelo malware para explorar o software comum.

- Teste e ative a assinatura McAfee HIPS 6010 (proteção genérica contra interceptação de aplicativos) incorporada no McAfee Host Intrusion Prevention.
- Teste e ative a assinatura McAfee HIPS 6011 (proteção genérica contra chamadas de aplicativos) incorporada no McAfee Host Intrusion Prevention.
- Isole os sistemas infectados pelo Pinkslipbot atribuindo a eles uma política na qual a regra de firewall bloqueie todas as portas que não sejam de administração.

O McAfee Endpoint Security 10 e o McAfee Host Intrusion Prevention estão incluídos no McAfee Complete Endpoint Protection.

McAfee Web Gateway (MWG)
Downloads de passagem e links de e-mails são maneiras comuns pelas quais o Pinkslipbot se dissemina. O McAfee Web Gateway proporciona uma segurança de Web de alto desempenho, protegendo sistemas contra sites maliciosos. Ele pode ser distribuído como um appliance de hardware dedicado ou como uma imagem de máquina virtual.

- Configure o McAfee Web Gateway para filtragem de spam.
  - A filtragem de spam pode protegê-lo contra:
    - IPs maliciosos
    - URLs maliciosos
    - Spam de e-mail
- Ative a inspeção GAM.
- Ative o McAfee GTI para reputação de URL e de arquivo.
- Integre-se com o McAfee Advanced Threat Defense para análises em área restrita (sandbox) e detecção de ameaças de dia zero.

McAfee Active Response (MAR)
O McAfee Active Response oferece detecção e resposta contínuas para sistemas visados por ameaças avançadas como o Pinkslipbot. O monitoramento automatizado de eventos permite encontrar indicadores de comprometimento que indicam se um sistema está infectado por malware.

- A presença dos seguintes domínios em um cache de DNS pode ser indício de uma infecção pelo Pinkslipbot:
  - gpfbvtuz.org
  - hsdmoyrkeqpcyrtw.biz
  - lgzmtkvnijeaj.biz
  - mfrlilcumtwieyzbfdmpdd.biz
  - hogfpicpoxnp.org
  - qrogmwmahgcwil.com
  - enwgzzthfwhdm.org

  - vksslxpxaoql.com
  - dxmhcvxcmdewthfbnaspnu.org
  - mwtfngzkadeviqtlfrrio.org
  - jynsrklhmaqirhjrtygjx.biz
  - uuwgdehizcuuucast.com
  - gyvwkxfxqdargdooqql.net
  - xwcjchzq.com
  - tqxllcfn.com
  - feqsrxswnumbkh.com
  - nykhliicqv.org
  - ivalhlotxdyvzyxrb.net
  - bbxrsgsuwksogpktqydlkh.net
  - rudjqypvucwwpfejdxqsv.org
- Execute a seguinte consulta ao cache de DNS para determinar se algum sistema se comunicou com algum dos domínios conhecidos do Pinkslipbot listados acima.
  - DNSCache where DNSCache hostname equals “[domínio do Pinkslipbot]”
- Essa consulta retornará uma lista de comunicações estabelecidas com domínios do Pinkslipbot a partir de sistemas dentro do ambiente. Você pode identificar facilmente quais sistemas estão se comunicando com quais domínios clicando na entrada e exibindo os sistemas relacionados.
- Use um firewall local, como o McAfee ENS 10 ou o McAfee HIPS, para colocar em quarentena os sistemas afetados pelo Pinkslipbot. Para colocar um sistema em quarentena, atribua uma política de bloqueio de firewall ao sistema, dentro do McAfee ePO.
- Execute uma varredura solicitada completa do sistema no McAfee ENS 10 ou no McAfee VSE designando uma tarefa de varredura por solicitação para executar imediatamente, dentro do McAfee ePO. Acorde o agente para iniciar a varredura.

Para leitura adicional

Consultoria de ameaças do McAfee Labs: W32/Pinkslipbot

Esse parecer consultivo oferece uma análise técnica detalhada do Pinkslipbot.

Série de webinars da Intel Secutiry sobre malware: Pinkslipbot

Esse vídeo proporciona uma visão geral do Pinkslipbot, categorizações regionais e setoriais, características e sintomas, bem como recomendações para prevenção.

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