Proteção contra WannaCry e Petya

Um grande ataque cibernético, baseado na família de malware WannaCry, foi lançado em maio de 2017. O WannaCry explorou uma vulnerabilidade em algumas versões do Microsoft Windows. Estima-se que mais de 300.000 computadores em 150 países foram infectados durante o ataque principal, cada qual exigindo o pagamento de um resgate.

Não está claro qual foi o vetor de ataque inicial, mas um worm agressivo ajuda a disseminar o malware. Um patch crítico foi lançado pela Microsoft em março para eliminar a vulnerabilidade subjacente em versões suportadas do Windows, mas muitas organizações ainda não aplicaram esse patch.

Para computadores com versões não suportadas do Windows (Windows XP, Windows Server 2003), nenhum patch foi disponibilizado. A Microsoft lançou um patch de segurança especial para Windows XP e Windows Server 2003 após o ataque do WannaCry.

Aproximadamente seis semanas depois, um outro ataque cibernético explorou a mesma vulnerabilidade. O Petya não teve tanto impacto quanto o WannaCry, mas esses dois ataques expuseram o uso continuado de sistemas operacionais antigos e sem suporte em áreas críticas, bem como os processos deficientes de aplicação de patches seguidos por algumas empresas. Leia uma análise detalhada sobre esses ataques no *Relatório do McAfee Labs sobre ameaças: setembro de 2017*.

Políticas e procedimentos para proteção contra o WannaCry e o Petya

- **Faça backup dos arquivos:** o procedimento mais eficaz para evitar o ransomware é fazer backups regulares dos arquivos de dados e verificar os procedimentos de restauração da rede.
- **Conscientize os usuários da rede:** como outros tipos de malware, o ransomware costuma infectar sistemas através de ataques de phishing utilizando anexos de e-mail, downloads ou Cross-site scripting (XSS) através de navegação na Web.
- **Monitore e inspecione o tráfego de rede:** essa etapa ajudará a identificar tráfego anormal associado a comportamentos de ransomware.
- **Use canais de dados de inteligência sobre ameaças:** essa prática pode ajudar a detectar ameaças mais rapidamente.
- **Restrinja a execução de código:** o ransomware é frequentemente desenvolvido para ser executado em pastas bem conhecidas do sistema operacional. Se ele não puder alcançar essas pastas devido ao controle de acessos, isso pode bloquear a criptografia maliciosa dos dados.
- **Restrinja o acesso administrativo e de sistema:** alguns tipos de ransomware são feitos para utilizar contas padrão na realização de suas operações. Com esse tipo de ransomware, renomear as contas de usuário padrão e desativar todas as contas desnecessárias, com ou sem privilégios pode criar uma proteção adicional.
- **Remova direitos de administrador local:** evite que o ransomware seja executado em um sistema local e detenha sua disseminação com base em privilégios administrativos. A remoção de direitos administrativos locais também bloqueia o acesso a quaisquer arquivos e recursos críticos do sistema que o ransomware visa para criptografar.
- **Outras práticas relacionadas a permissões:** considere restringir as capacidade de gravação pelo usuário, impedir execução a partir de diretórios de usuários, criar uma lista branca de aplicativos permitidos e limitar o acesso a compartilhamentos ou armazenamentos de rede. Alguns tipos de ransomware exigem acesso de gravação a caminhos de arquivo específicos para serem instalados ou executados. Limitar a permissão de gravação a um pequeno número de diretórios (por exemplo, Meus documentos e Meus downloads) pode deter algumas variantes de ransomware. Os executáveis de ransomware também podem ser impedidos por meio da remoção da permissão de execução nesses diretórios. Muitas organizações utilizam um conjunto limitado de aplicativos para realizar seus negócios. É possível bloquear a execução de aplicativos que não constem em uma lista branca, como o ransomware, adotando-se uma política de utilizar somente aplicativos aprovados. Uma prática adicional em termos de permissões é exigir um login em recursos compartilhados, como pastas de rede.
- **Faça manutenção e atualização do software:** uma outra regra básica importante para proteção contra ransomware é manter e atualizar o software, particularmente as correções do sistema operacional, bem como o software de segurança e antimalware.

É extremamente importante reduzir a superfície de ataque, especialmente no que se refere ao phishing, uma das técnicas mais populares utilizadas pelo ransomware. Para o e-mail, considere as seguintes práticas:

- **Filtre o conteúdo do e-mail:** proteger as comunicações de e-mail é um procedimento fundamental. A possibilidade de um ataque bem-sucedido será reduzida se os usuários da rede receberem menos e-mails de spam com conteúdo potencialmente malicioso e inseguro.
- **Bloquear anexos:** a inspeção de anexos é uma etapa importante na redução da superfície de ataque. O ransomware costuma ser entregue na forma de um anexo executável. Implemente uma política segundo a qual arquivos com determinadas extensões não possam ser enviados por e-mail. Tais anexos podem ser analisados por uma solução de sandbox e removidos pelo appliance de segurança de e-mail.

Como os produtos da McAfee podem protegê-lo contra o WannaCry

McAfee Network Security Platform (NSP)

O McAfee NSP responde rapidamente para prevenir explorações e proteger ativos dentro de redes. A equipe do McAfee NSP trabalha com afinco para desenvolver e distribuir assinaturas definidas pelo usuário (UDS) para assuntos críticos. Em um período de 24 horas durante o ataque WannaCry, a McAfee criou e transferiu por upload várias UDS para os clientes distribuírem em seus sensores de rede. Nesse caso, a UDS visava explicitamente as ferramentas de exploração EternalBlue, Eternal Romance SMB Remote Code Execution e DoublePulsar. A McAfee também lançou indicadores de comprometimento relacionados que poderiam ser adicionados a uma blacklist para bloquear ameaças potenciais associadas ao cavalo de Troia original.

Leia mais sobre assinaturas NSP aqui.

McAfee Host Intrusion Prevention (HIPS)

O McAfee HIPS 8.0, com a assinatura NIPS 6095, oferece proteção contra todas as quatro variantes conhecidas do WannaCry. Consulte o artigo KB89335 para obter as informações mais recentes sobre essas configurações.

Assinatura personalizada 1: regra de bloqueio de Registro do WannaCry
Usar sub-regra padrão
Tipo de regra = Registro
Operações = Criar, modificar e alterar permissões, incluir chave do Registro
Chave do Registro = \REGISTRY\MACHINE\SOFTWARE\WanaCrypt0r
Executável = *

Assinatura personalizada 2: regra de bloqueio de arquivo/pasta do WannaCry
Usar sub-regra padrão
Tipo de regra = Arquivos
Operações = Criar, gravar, renomear, alterar atributos somente leitura/oculto, incluir arquivos
Arquivos = *.wnry
Executável = *

Configurações de proteção adaptável contra ameaças do McAfee Endpoint Protection (ENS) e do McAfee VirusScan Enterprise (VSE)

McAfee Endpoint Security 10.5 — Proteção adaptável contra ameaças

O McAfee Endpoint Security 10.5, com proteção adaptável contra ameaças, Real Protect e contenção dinâmica de aplicativos (DAC), proporciona proteção contra explorações conhecidas ou desconhecidas utilizadas pelo WannaCry.

- Configure os seguintes parâmetros na política de opções da proteção adaptável contra ameaças:
  - Rule Assignment (Atribuição de regra) = Security (Segurança). (A configuração padrão é Balanced (Balanceada)).
- Configure as seguintes regras na política de contenção dinâmica de aplicativos da proteção adaptável contra ameaças:
  - Dynamic Application Containment (Contenção dinâmica de aplicativos) — Containment Rules (Regras de contenção)

Consulte o artigo KB87843: Lista de regras de contenção dinâmica de aplicativos ENS e melhores práticas e configure as regras de DAC recomendadas para "Block" (Bloquear), conforme indicado.

McAfee Endpoint Security 10.1, 10.2 e 10.5 — Proteção contra ameaças

A proteção contra ameaças do McAfee Endpoint Security 10.x com conteúdo AMCore versão 2978 ou posterior oferece proteção contra todas as quatro variantes atualmente conhecidas do WannaCry.

McAfee VirusScan Enterprise 8.8

O McAfee VirusScan Enterprise 8.8 com conteúdo DAT versão 8527 ou posterior oferece proteção contra todas as quatro variantes atualmente conhecidas do WannaCry.

Medidas proativas de proteção do McAfee Endpoint Security (ENS) e de proteção de acessos do McAfee VirusScan Enterprise (VSE)

As regras de proteção do McAfee ENS e de proteção de acessos do McAfee VSE impedem a criação do arquivo .wnry. Essa regra interrompe a rotina de criptografia que cria arquivos criptografados com extensão .wncryt, .wncry ou .wcry. Com a implementação do bloqueio contra arquivos .wnry, outros bloqueios dos tipos de arquivo criptografados se tornam desnecessários.

Leia mais sobre configuração das regras de proteção de acessos do McAfee VSE.

Configure o sistema de segurança de endpoint para proteger contra criptografia de arquivo pelo WannaCry (e futuras variantes desconhecidas).

Os clientes que não utilizam a proteção adaptável contra ameaças do McAfee ENS podem não ter uma proteção de conteúdo definida pela McAfee contra variantes ainda não lançadas. Recomendamos configurar tarefas de atualização de repositório com um intervalo de atualização mínimo para assegurar que novos conteúdos sejam aplicados quando forem lançados pela McAfee.

Proteções adicionais contra a rotina de criptografia podem ser configuradas utilizando-se regras de proteção de acessos do McAfee VSE/ENS ou regras personalizadas do McAfee HIPS. Consulte o artigo KB89335 para obter as informações mais recentes sobre essas configurações.

As regras de proteção de acessos do McAfee VSE e do McAfee ENS, bem como as assinaturas personalizadas do McAfee HIPS, impedirão a criação do arquivo .wnry.

As regras interrompem a rotina de criptografia que cria arquivos criptografados com extensão .wncryt, .wncry ou .wcry.

Com a implementação do bloqueio contra .wnry, outros bloqueios dos tipos de arquivo criptografados se tornam desnecessários.

Consulte o artigo KB89335 (acessível para clientes registrados da McAfee) para obter as informações mais recentes sobre essas configurações.

McAfee Advanced Threat Defense (ATD)

A autoaprendizagem do McAfee ATD pode condenar uma amostra em uma análise de "gravidade média".

O McAfee ATD observou o seguinte:

Classificação do comportamento:

- Arquivo ocultado
- Disseminação
- Exploração por meio de código de shell
- Propagação pela rede

Análise dinâmica:

- Comportamento de ransomware demonstrado
- Criptografia de arquivos
- Criação e execução de conteúdo de script suspeito
- Comportamento característico de um instalador de macro de cavalo de Troia

Em relação ao WannaCry, o McAfee ATD observou, até hoje, 22 operações de processos, incluindo cinco DLLs de tempo de execução, 58 operações de arquivos, modificações do Registro, modificações de arquivos, criações de arquivos (dll.exe), injeções de DLL e 34 operações de rede.

McAfee Web Gateway (MWG)

McAfee Web Gateway (MWG) é uma família de produtos (appliance, nuvem e híbrido) de proxies Web que proporciona proteção imediata contra variantes do WannaCry entregues via Web (HTTP/HTTPS) utilizando múltiplos mecanismos de varredura em tempo real.

As variantes conhecidas são bloqueadas pela varredura antimalware e de reputação do McAfee Global Threat Intelligence (GTI) conforme o tráfego de Web é processado ao atravessar o proxy.

O mecanismo Gateway Anti-Malware (GAM) Engine dentro do MWG proporciona uma prevenção eficaz contra variantes ainda não identificadas com uma assinatura (ameaças de "dia zero") através de seu processo de emulação de comportamento — realizado em arquivos, HTML e JavaScript. Os emuladores são alimentados regularmente com inteligência por modelos de autoaprendizagem. O GAM é executado juntamente com a varredura antimalware e de reputação do GTI conforme o tráfego é processado.

A união do MWG com o ATD permite inspeções adicionais e uma abordagem eficaz de prevenção e detecção.

McAfee Threat Intelligence Exchange (TIE)

O McAfee Threat Intelligence Exchange (TIE) aprimora ainda mais a postura de segurança do cliente. Com a capacidade de agregar vereditos de reputação do ENS, do VSE, do MWG e do NSP, o TIE pode compartilhar rapidamente informações de reputação relacionadas ao WannaCry com qualquer vetor integrado. Ao oferecer a capacidade de usar o GTI para uma consulta de reputação global, o TIE também permite que produtos integrados tomem uma decisão imediata antes da execução da carga do ransomware, aproveitando a reputação armazenada temporariamente no banco de dados do TIE.

Conforme cada endpoint se protege, detecta quaisquer variantes relacionadas e ainda atualiza o índice de reputação enviado ao TIE, essa abordagem totalmente abrangente estende a proteção disseminando essas informações para todos os endpoints integrados com o TIE. Esse compartilhamento bidirecional de inteligência contra ameaças é duplicado em capacidade com o MWG e o NSP. Assim, conforme a ameaça potencial tenta se infiltrar pela rede ou pela Web, o MWG e o NSP oferecem proteção e detecção, e compartilham essa inteligência com o TIE para inocular os endpoints — protegendo imediatamente a empresa sem nenhuma execução adicional da variante condenada em um potencial "paciente zero" no ambiente.

Como os produtos da McAfee podem protegê-lo contra o Petya

A McAfee oferece proteção contra o ataque Petya inicial na forma de uma análise avançada do comportamento do malware com as técnicas de análise Real Protect Cloud e Dynamic Neural Network (DNN) disponíveis no McAfee Advanced Threat Defense.

O ATD 4.0 introduziu uma nova capacidade de detecção utilizando uma rede neural (DNN) multicamada com propagação retroativa, aplicando uma aprendizagem semisupervisionada. A DNN examina determinadas características demonstradas pelo malware para formular um veredito positivo ou negativo e, com isso, determinar se o código é malicioso.

Seja em modo autônomo ou conectado a sensores de rede ou de endpoint da McAfee, o ATD combina inteligência contra ameaças com análise comportamental em área restrita (sandbox) e autoaprendizagem avançada para proporcionar uma proteção de dia zero adaptável. O Real Protect, parte da solução Dynamic Endpoint, também utiliza autoaprendizagem e análise de vínculos para proporcionar proteção contra malware sem assinaturas e oferecer uma inteligência detalhada ao Dynamic Endpoint e ao restante do ecossistema McAfee. O Real Protect, combinado com a contenção dinâmica de aplicativos, proporcionou uma proteção prévia contra o Petya.

Vários produtos da McAfee oferecem proteção adicional para conter o ataque ou evitar execução adicional.

McAfee Endpoint Security

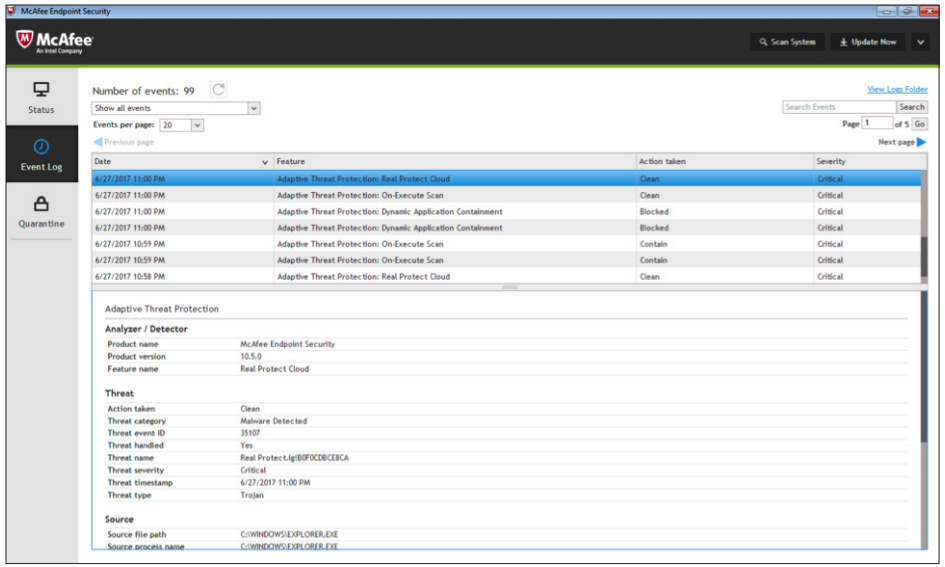
Prevenção de ameaças

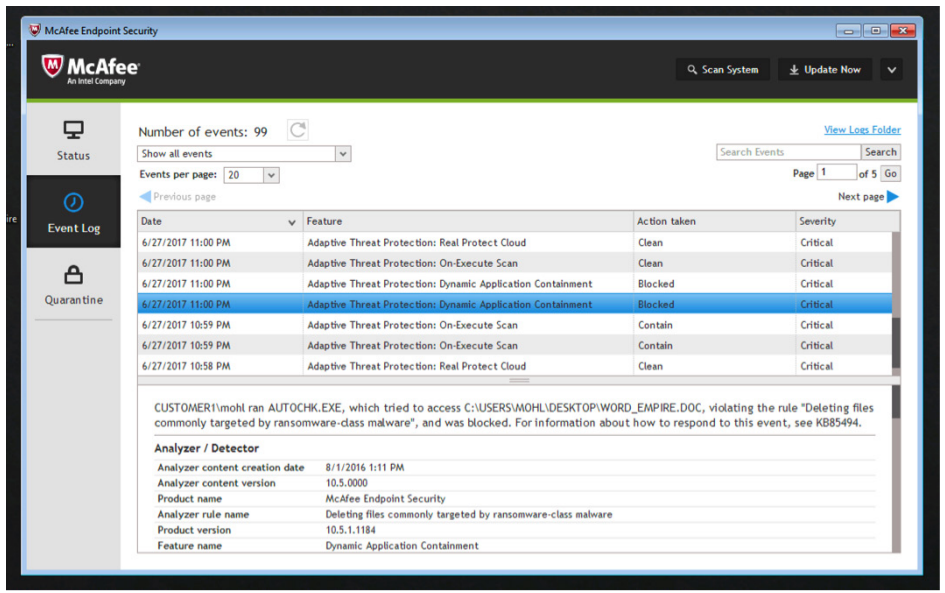
- O McAfee Endpoint Security, com o McAfee Global Threat Intelligence e a política de varredura ao acessar com o nível de sensibilidade definido como "Baixo", protege contra amostras e variantes conhecidas.
- Saiba mais sobre as configurações recomendadas de reputação de arquivo do McAfee GTI em KB74983, com informações adicionais em KB53735.
- O McAfee Threat Intelligence Exchange com GTI protege contra amostras e variantes conhecidas.

Os sistemas que utilizam o McAfee ENS 10 são protegidos contra amostras e variantes conhecidas, com assinaturas e com inteligência contra ameaças.

Proteção adaptável contra ameaças

- A proteção adaptável contra ameaças (ATP), com atribuição de regras configurada em "Modo balanceado" (configuração padrão em ATP\Opções\ Atribuição de regra), protege contra variantes conhecidas e desconhecidas do ransomware Petya.
- O módulo ATP protege contra essa ameaça desconhecida com várias camadas de contenção e proteção avançada:
  - O ATP Real Protect Static utiliza análise comportamental pré-execução no lado do cliente para monitorar ameaças maliciosas desconhecidas antes do lançamento.
  - O ATP Real Protect Cloud utiliza autoaprendizagem assistida pela nuvem para identificar e neutralizar a ameaça, conforme mostrado acima, à direita.
- A contenção dinâmica de aplicativos (DAC) do ATP contém com êxito a ameaça e evita a ocorrência de qualquer dano potencial (eventos de DAC indicado abaixo, à direita).





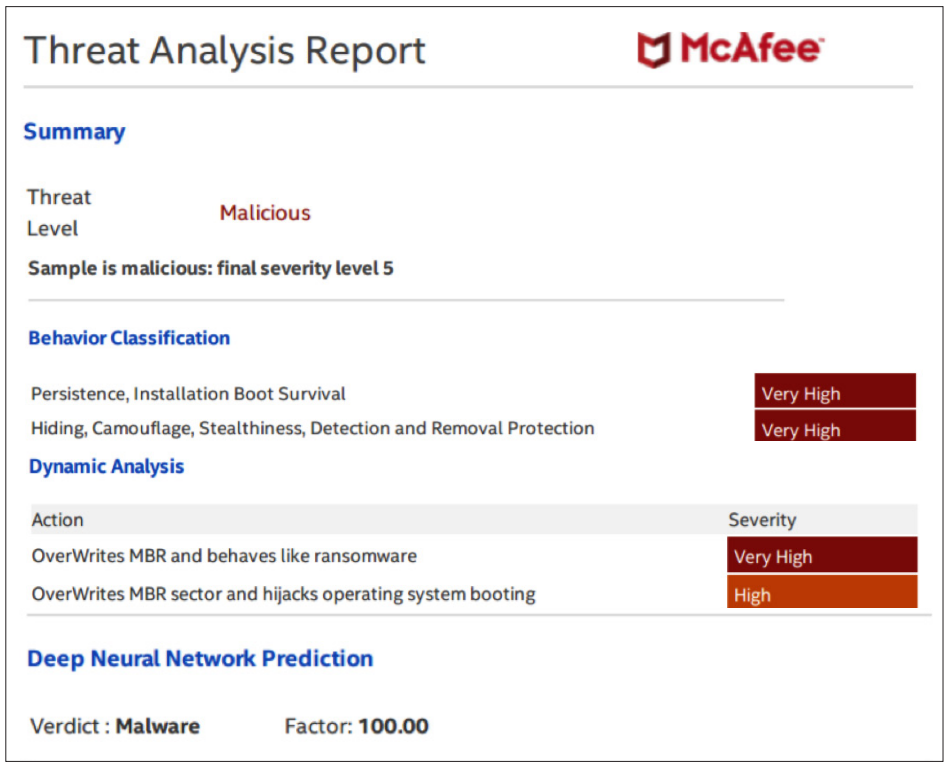
McAfee Advanced Threat Defense

- O McAfee Advanced Threat Defense 4.0 com rede neural profunda e área restrita (sandbox) dinâmica identificou a ameaça e atualizou proativamente o ecossistema de defesa cibernética. (Veja abaixo.)

McAfee Enterprise Security Manager

O McAfee Enterprise Security Manager (ESM) é uma solução de gerenciamento de eventos e informações de segurança que oferece inteligência decisiva e integrações para priorizar, investigar e responder a ameaças.

O Suspicious Activity Content Pack e o Exploit Content Pack do McAfee ESM foram atualizados com regras, alarmes e listas de observação específicos para o WannaCry, para que você possa localizar e identificar possíveis infecções. Essas atualizações também ajudam na proteção contra o Petya. Ambos os pacotes estão disponíveis para download no console do McAfee ESM sem custo adicional. As regras padrão de correlação do McAfee ESM também podem alertar os usuários sobre níveis mais altos de varredura de SMB horizontal.



O ataque Petya, semelhante ao WannaCry, constitui uma oportunidade de aprendizagem para analistas de centros de operações de segurança. A compreensão e a automação dessas melhores práticas ajudarão os profissionais de segurança a lidar com o próximo ataque rápido.

McAfee Web Gateway

O McAfee Web Gateway (MWG) é uma família de produtos (appliance, nuvem e híbrido) de proxies Web que proporciona mais uma camada potencial de proteção contra variantes do Petya entregues via Web (HTTP/HTTPS) utilizando múltiplos mecanismos de varredura em tempo real. As variantes conhecidas são bloqueadas pela varredura antimalware e de reputação do GTI conforme o tráfego de Web é processado ao atravessar o proxy.

O mecanismo Gateway Anti-Malware Engine dentro do MWG proporciona uma prevenção eficaz contra variantes de "dia zero" ainda não identificadas com uma assinatura através do processo de emulação de comportamento do GAM — realizado em arquivos, HTML e JavaScript. Os emuladores são alimentados regularmente com inteligência por modelos de autoaprendizagem. O GAM é executado juntamente com a varredura antimalware e de reputação do GTI conforme o tráfego é processado.

A união do MWG com o ATD permite inspeções adicionais e uma abordagem eficaz de prevenção e detecção.

Produtos da McAfee que utilizam arquivos DAT

A McAfee lançou um Extra.DAT para incluir a cobertura do Petya. A McAfee também lançou um DAT de emergência para incluir a cobertura dessa ameaça. DATs subsequentes incluirão essa cobertura. Os arquivos DAT mais recentes estão disponíveis no artigo KB89540 do Knowledge Center.

Para leitura adicional

Detalhes técnicos atualizados frequentemente podem ser encontrados nos artigos KB89335, KB87843, KB74983, KB53735 e KB89540 do McAfee Knowledge Center.

McAfee
Together is power.

Av. Nações Unidas, 8.501 – 16º andar
Pinheiros – São Paulo – SP
CEP 05425-070, Brasil
+(11) 3711-8200
www.mcafee.com/br

3530_0917
SETEMBRO DE 2017