www.pwc.com.br

Ransomware Petya

pwc

Ransomware Petya

Uma nova onda do *ransomware* Petya tem afetado um número grande de organizações em diferentes setores desde 27 de junho de 2017. Muitas empresas foram atingidas, entre elas, entidades na Ucrânia, Espanha, Holanda, Reino Unido e Brasil. Trata-se de um *malware* similar ao do surto WannaCry de maio de 2017, que também teve alcance mundial e comprometeu uma ampla gama de organizações rapidamente.

O *ransomware* dessa nova onda é um pouco diferente, pois aplica uma abordagem em vários níveis, na qual criptografa o Master Boot Record (MBR) da máquina quando ele é executado por um administrador. Quando a execução é feita por um usuário normal, são criptografados arquivos específicos do sistema. O Petya também usa diferentes métodos para afetar o maior número possível de máquinas.

Ransomware é um nome dado ao *malware* que impede ou limita o acesso dos usuários a sistemas ou arquivos de computador, normalmente exigindo o pagamento de um resgate em troca de uma chave para ter acesso aos arquivos sequestrados. O comportamento moderno do *ransomware* geralmente envolve a criptografia de arquivos de usuários finais com algoritmos fortes, o que torna impossível a recuperação dos arquivos das vítimas. A chave de descriptografia é fornecida às vítimas em troca de algum tipo de moeda, normalmente as digitais (ex.: *bitcoin*). Diversas variantes de *ransomware* foram observadas em todo o mundo ao longo dos últimos anos. Elas são distribuídas regularmente, mas apresentam comportamentos diferentes. Por causa dessas diferenças, é fundamental compreender o comportamento de cada variante para se preparar para um ataque de *ransomware*, responder a ele e se recuperar.

Por exemplo, algumas variantes do *ransomware* implementaram mecanismos de criptografia mal projetados e, assim, permitiram que pesquisadores de segurança desenvolvessem ferramentas para descriptografá-las.

O *ransomware* é uma ameaça cada vez mais comum, com um número crescente de variantes projetadas para atacar redes corporativas. A fim de se proteger contra essa praga, existem várias medidas práticas que as organizações podem tomar para reduzir a probabilidade de incidentes, limitar seu impacto em caso de ocorrência e se recuperar de forma rápida e eficaz. Essas medidas abrangem vários aspectos das operações e da segurança de TI, como:

- ***Inteligência de* cyber**
  Coleta, correlação, análise e monitoramento de informações de diversas fontes externas, como novas ameaças globais (WannaCry, Petya), novas vulnerabilidades críticas (MS17-010), modalidades de ataque, notícias sobre o setor em que a organização atua etc.

- ***Planejamento e exercício de resposta a incidentes e crises***
  Procedimentos formais nos quais os funcionários e os responsáveis pelo gerenciamento de incidentes de alta prioridade estejam bem treinados para agilizar a reação da organização aos eventos do *ransomware* e a restauração do serviço.

- ***Planejamento robusto de continuidade de negócios***
  Planejamento e exercício permanente de continuidade de negócios para garantir que os sistemas dos usuários e os servidores principais possam ser restaurados rapidamente a partir de backups. Assegurar também que a frequência de backups esteja de acordo com o período dos dados que sua organização está preparada para perder no caso de inutilização de algum sistema.

- ***Política de segurança coerente e conscientização do usuário***
  Ações para prevenir que o *ransomware* entre no seu ambiente de TI usando o vetor mais comum – o *phishing* – por meio da aplicação de controles fortes em seus *gateways* de e-mail e perímetros de rede e da conscientização de funcionários por meio de fortes campanhas de conscientização.

- ***Gestão de* patches *e gerenciamento de vulnerabilidades***
  As vulnerabilidades exploradas nesse ataque já foram solucionadas pelos *patches* críticos da Microsoft lançados em março. Um programa forte de gerenciamento de vulnerabilidades ajudará a reduzir a probabilidade de exploração.

O vetor de infecção inicial da última onda de *ransomware* não é conhecido até o momento. Esse *malware* é uma combinação das variantes Petya e Mischa. Quando executado como administrador, ele criptografa o Master Boot Record (MBR), mas não os arquivos no disco.

A criptografia do MBR significa que o usuário não pode reiniciar o sistema de forma normal. Em vez disso, é exibida uma mensagem do *ransomware*.

No entanto, se o *malware* for executado sem privilégios de administrador, serão criptografados arquivos com extensões específicas (identificados no fim desta publicação). Isso também é conhecido como a combinação "Goldeneye".

O NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF) foi projetado para auxiliar as organizações na estruturação do seu programa de segurança cibernética em cinco funções: **Identificar**, **Proteger**, **Detectar**, **Responder** e **Recuperar**.

Identificar

Desenvolva o entendimento organizacional para gerenciar riscos de segurança cibernética relacionados a sistemas, ativos, dados e capacidades.

Ação:

I. Os executivos devem fazer um esforço para identificar os ativos da organização que são vulneráveis a essa variante de *ransomware*, especificamente os vulneráveis à exploração de EternalBlue e DoublePulsar SMB. Isso inclui todos os sistemas Microsoft Windows que ainda não têm o *patch* Microsoft MS17-010 instalado.

II. Conheça, compreenda e aprimore seus procedimentos corporativos de recuperação de desastres. Faça backup dos dados críticos da empresa e armazene-os de forma segura.

Proteger

Desenvolva e implemente as proteções adequadas para garantir a prestação de serviços de infraestrutura essenciais.

Ação:

I. Os executivos também precisam entender que as equipes de operações de TI, por recomendação de sua equipe de segurança, talvez precisem interromper de forma temporária alguns serviços de TI para implementação de controles adicionais e desativação de serviços vulneráveis.

II. Verifique se suas equipes de TI agiram ou elaboraram planos para:

a) Desativar todo o acesso SMB externo (bloqueando as portas 137, 139 e 445 para/da Internet).

b) Desativar o uso do protocolo de compartilhamento de arquivos de rede SMBv1 em todo o ambiente de TI.

c) Desativar a capacidade de executar macros não assinadas em documentos do Office, usando GPO (e assinar macros legítimas da sua própria organização).

d) Garantir que a autenticação de dois fatores esteja instalada para todo acesso externo necessário aos sistemas (por exemplo, VPN e RDP).

e) Identificar e evitar que todos os sistemas sem a atualização de segurança MS17-010 se conectem às principais redes corporativas e segregar as redes convidadas de todas as capacidades para acessar as principais redes corporativas.

f) Forçar uma atualização total das assinaturas de antivírus da empresa.

g) Isolar rapidamente todos os sistemas infectados da sua rede corporativa para limitar a disseminação para outros sistemas.

Detectar

Desenvolva e implemente as atividades apropriadas para identificar a ocorrência de um evento de segurança cibernética.

Ação:

As organizações devem aproveitar todas as fontes de inteligência disponíveis para construir uma biblioteca abrangente de indicadores a fim de melhorar seus recursos de detecção. Para apoiar essa fase, foram observados Indicadores de Comprometimento (IOCs) relacionados a essa campanha, que são listados no fim desta publicação. Esses IOCs são fornecidos com confiança média, podem não ser abrangentes para todas as variantes do *ransomware* Petya e devem ser avaliados de forma adequada pela organização.

Responder

Desenvolva e implemente as atividades apropriadas para agir em relação a um evento de segurança cibernética detectado.

Ação:

I. Se um evento de *ransomware* Petya for detectado, sua organização deverá estar preparada para acionar o plano de resposta a incidentes. Como o *ransomware* consegue se espalhar rapidamente em um ambiente suscetível, as ações de contenção devem ser tomadas com urgência. Além disso, a PwC não recomenda pagar resgate. Uma organização vítima de ataque deverá estar preparada para entender e quantificar o impacto de uma infecção e tomar as medidas adequadas para limitar esse impacto de forma mais eficaz.

II. Para organizações que atuam em indústrias reguladas (como serviços de saúde ou financeiros) nas quais informações privadas sejam afetadas pelo *ransomware*, é importante se familiarizar com as orientações divulgadas pelos órgãos reguladores locais sobre possíveis impactos do *ransomware*

Realize uma análise de impacto para quantificar os transtornos para os negócios e use essa análise para tomar decisões apropriadas baseadas em riscos.

Recuperar

Desenvolva e implemente as atividades apropriadas para manter planos de resiliência e para restaurar recursos ou serviços que tenham sido prejudicados por um evento de segurança cibernética.

Ação:

Use os atuais programas e processos de recuperação de desastres da sua organização para permitir operações de "*back to business*". Identifique se a sua organização é obrigada a notificar os órgãos reguladores, parceiros ou clientes em casos de comprometimento ou interrupção de negócios e adote as medidas adequadas. Faça uma análise de incidentes para garantir que as lições sejam incorporadas ao seu Programa de Segurança Cibernética.

A PwC conta com uma equipe global de com mais de 3.300 profissionais, incluindo consultores especializados, investigadores de *cyber-forensics*, analistas de inteligência, tecnólogos, advogados e líderes da indústria em segurança cibernética e privacidade.

Saiba mais em ***www.pwc.com.br/pt/imperativos-negocios/proteger-ativos.html***.

Rede diversificada de recursos

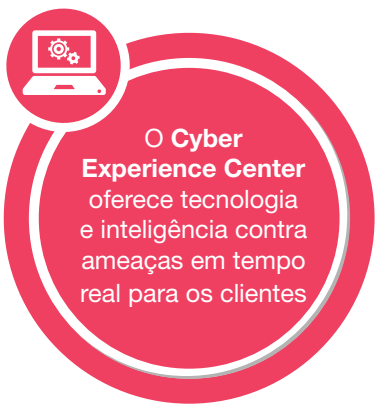
Nossa equipe tem ampla experiência em ajudar organizações globais a avaliar, projetar, implementar e melhorar estrategicamente programas de segurança cibernética. Também temos um longo histórico de construção de relacionamentos profissionais com líderes empresariais em todos os níveis.

Experiência

Nossos serviços se baseiam em décadas de conhecimento tático sobre projetos em diferentes indústrias, localidades e tecnologias.

Centros de análise global e de segurança

Nossos Impact Centers oferecem às empresas e organizações de todo o mundo acesso a especialistas e à experiência de toda a rede global da PwC para ajudá-las a acompanhar o ritmo acelerado de mudanças da era digital e se preparar para o futuro.



Indicadores de Comprometimento (IOC)

Hash

- 027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745
- 078de2dc59ce59f503c63bd61f1ef8353dc7cf5f
- 0ff07caedad54c9b65e5873ac2d81b3126754aac
- 1b83c00143a1bb2bf16b46c01f36d53fb66f82b5
- 26b4699a7b9eeb16e76305d843d4ab05e94d43f3201436927e13b3ebafa90739
- 2bc182f04b935c7e358ed9c9e6df09ae6af47168
- 34f917aaba5684fbe56d3c57d48ef2a1aa7cf06d
- 51eafbb626103765d3aedfd098b94d0e77de1196
- 71b6a493388e7d0b40c83ce903bc6b04
- 7ca37b86f4acc702f108449c391dd2485b5ca18c
- 82920a2ad0138a2a8efc744ae5849c6dde6b435d
- a809a63bc5e31670ff117d838522dec433f74bee
- aba7aa41057c8a6b184ba5776c20f7e8fc97c657
- af2379cc4d607a45ac44d62135fb7015
- bec678164cedea578a7aff4589018fa41551c27f
- d5bf3f100e7dbcc434d7c58ebf64052329a60fc2
- 71b6a493388e7d0b40c83ce903bc6b04
- 7e37ab34ecdcc3e77e24522ddfd4852d
- a1d5895f85751dfe67d19cccb51b051a
- e285b6ce047015943e685e6638bd837e
- e595c02185d8e12be347915865270cca
- fe2c47fbb22139f790287272e9a9e365

URL

- http://mischapuk6hyrn72.onion/
- http://petya3jxfp2f7g3i.onion/
- http://petya3sen7dyko2n.onion/
- http://mischa5xyix2mrhd.onion/MZ2MMJ
- http://mischapuk6hyrn72.onion/MZ2MMJ
- http://petya3jxfp2f7g3i.onion/MZ2MMJ
- http://petya3sen7dyko2n.onion/MZ2MMJ

E-mail

- wowsmith123456@posteo.net

Endereços IP

- 95.141.115.108
- 111.90.139.247
- 185.165.29.78
- 84.200.16.242

Regras de IPS

- alert http any any -> any any (msg:"[PwC] Crimeware - Petya Ransomware - OPTIONS /"; flow:established,from_client; urilen:1; content:"OPTIONS"; http_method; content:"DavClnt"; http_user_agent; content:"translate: f|0d 0a|"; http_header; pcre:"/^[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}$/W"; reference:md5,07250ff40d5f112217a0f7831379f54c3daff24bd628d06b046b21b038d683c9; classtype:trojan-activity; metadata:copyright,Copyright PwC 2017; metadata:tlp amber; metadata:confidence High; metadata:efficacy Unknown; sid:9000199; rev:2017062701;)

- alert http any any -> any any (msg:"[PwC] Crimeware - Petya Ransomware - OPTIONS /admin$"; flow:established,from_client; urilen:7; content:"/admin$"; http_uri; content:"OPTIONS"; http_method; content:"Microsoft-WebDAV-MiniRedir"; http_user_agent; content:"translate: f|0d 0a|"; http_header; pcre:"/^[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}$/W"; reference:md5,07250ff40d5f112217a0f7831379f54c3daff24bd628d06b046b21b038d683c9; classtype:trojan-activity; metadata:copyright,Copyright PwC 2017; metadata:tlp amber; metadata:confidence High; metadata:efficacy Unknown; sid:9000200; rev:2017062701;)

- alert http any any -> any any (msg:"[PwC] Crimeware - Petya Ransomware - PROPFIND /admin$"; flow:established,from_client; urilen:7; content:"/admin$"; http_uri; content:"PROPFIND"; http_method; content:"Microsoft-WebDAV-MiniRedir"; http_user_agent; content:"translate: f|0d 0a|"; http_header; content:"Depth: 0|0d 0a|"; http_header; content:"Content-Length: 0|0d 0a|"; http_header; pcre:"/^[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}$/W"; reference:md5,07250ff40d5f112217a0f7831379f54c3daff24bd628d06b046b21b038d683c9; classtype:trojan-activity; metadata:copyright,Copyright PwC 2017; metadata:tlp amber; metadata:confidence High; metadata:efficacy Unknown; sid:9000201; rev:2017062701;) Petya - the latest wave

Para saber como se prevenir contra ataques ou esclarecer dúvidas sobre *ransomware* e ameaças cibernéticas, envie um e-mail para **br_cyberintelligence@pwc.com** ou entre em contato com um dos nossos líderes.

Contatos

Edgar D'Andrea
Sócio
edgar.dandrea@pwc.com

Fernando Mitre
Diretor
fernando.mitre@pwc.com

Eduardo Batista
Sócio
eduardo.batista@pwc.com

Rafael Cortes
Gerente
cortes.rafael@pwc.com

www.pwc.com.br

PwC Brasil @PwCBrasil @PwCBrasil PwC Brasil PwC Brasil PwC Brasil

(DC0) Informação Pública
Versão: Julho/2017 | [F235]