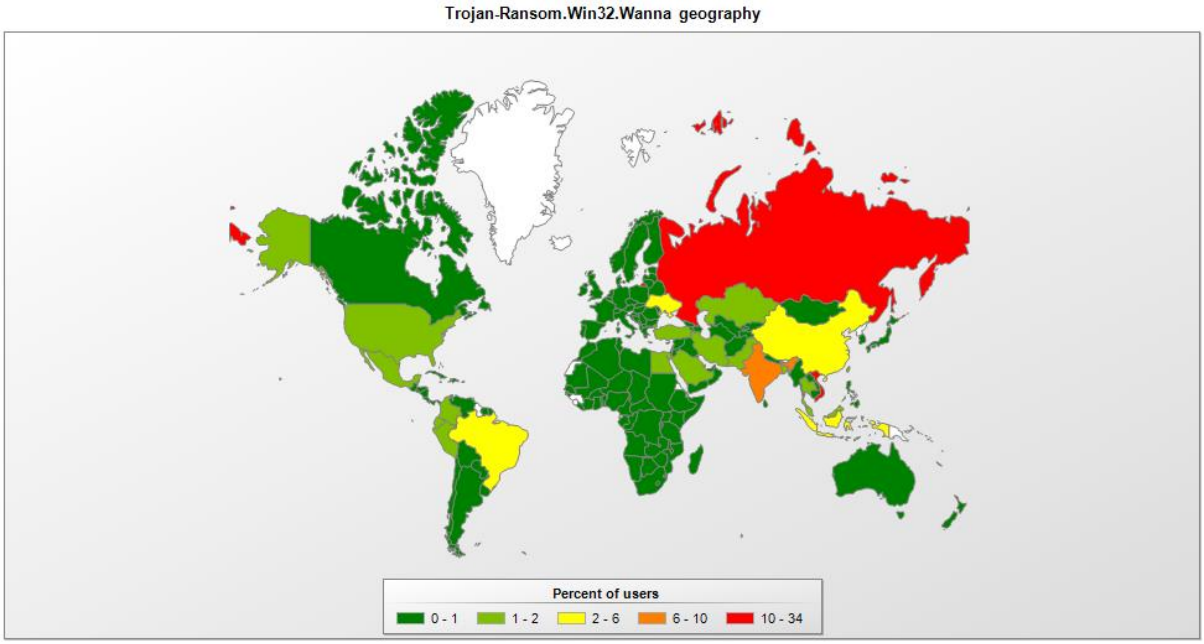
Depois de um ano de WannaCry, o EternalBlue ainda é um vetor de infecção

A maior infecção de ransomware da história afetou mais de 200 mil sistemas em 150 países

São Paulo, 10 de maio de 2018

Na sexta-feira, 12 de maio de 2017, a comunidade global testemunhou o início da maior infecção de ransomware da história. Este ataque conseguiu afetar mais de 200 mil sistemas em 150 países. A montadora Renault teve que fechar sua maior fábrica na França e os hospitais do Reino Unido tiveram que rejeitar pacientes. Já no Brasil, o ataque causou a interrupção do atendimento do INSS, instituto responsável pelo pagamento da aposentadoria e demais benefícios aos trabalhadores brasileiros, além de afetar empresas e órgãos públicos de 14 estados brasileiros mais o Distrito Federal.

Nos dias após o ataque, as empresas afetadas estavam sendo percebidas por diferentes países ao redor do mundo. Por fim, o país mais afetado foi a Rússia, com 33,64% das empresas afetadas, seguido do Vietnã (12,45%) e da Índia (6,95%). A região da América Latina também foi uma das mais afetadas, com o Brasil ocupando a sexta posição (4,06%) e o México a décima primeira (1,59%).



Mapa dos países infectados pelo Wannacry

A novidade deste ataque foi sua forma de propagação. Usando a exploração EternalBlue - vulnerabilidade no protocolo PMEs, divulgado semanas antes pelo grupo Shadowbrokers - que instalou o backdoor DoublePulsar, usado para injetar código maliciosos sem exigir qualquer interação com os usuários. Uma vez que os computadores foram infectados, o WannaCry criptografou as informações e extorquiu as vítimas, pedindo-lhes que pagassem um resgate para recuperar suas informações.

O WannaCry mostrou como era fácil explorar uma vulnerabilidade conhecida para o sistema operacional Microsoft Windows. Embora o patch já estivesse disponível, muitos administradores de sistemas perceberam que sua rede estava exposta quando já estava atrasada.

"*Embora ainda haja dúvidas sobre as motivações por trás do ataque em 12 de maio de 2017, as lições aprendidas pela indústria têm sido de grande valor e levaram a uma melhoria progressiva das medidas de segurança aplicadas em ambientes corporativos. O WannaCry deixou claro que a segurança de computadores deve ser um processo proativo e constante, com o pilar fundamental da aplicação dos patches do sistema operacional e a configuração correta das soluções antimalware*", reforça **Dmitry Bestuzhev, diretor da Equipe de Análise e Pesquisa da Kaspersky Lab para a América Latina.**

Meses após a contenção do surto inicial, WannaCry ainda estava reivindicando vítimas, incluindo a Honda, que foi forçada a fechar uma de suas instalações de produção. Apesar da disseminação do ataque, um ano depois, a exploração do EternalBlue ainda é um vetor de infecção, não apenas para ransomware, mas também para outras infecções por malware. Isso se deve à falta de instalação dos patches correspondentes da Microsoft para fechar essas vulnerabilidades.

"*A vulnerabilidade do EternalBlue ainda está sendo explorada por criminosos para distribuir malware e obter infecções maciçamente. Em alguns casos, é ransomware, mas em outros temos visto a proliferação de cryptominers, ou seja, um tipo de aplicativo cujo único objetivo é gerar moedas digitais como Bitcoin ou Monero. É interessante observar como, após um ano, ainda existem sistemas que não aplicaram as atualizações e ainda estão vulneráveis a esse tipo de ameaça*", acrescenta **Santiago Pontiroli, analista de segurança da Equipe de Pesquisa e Análise Global da Kaspersky Lab.**

De acordo com dados da Kasperksy Lab, aproximadamente 65% das empresas afetadas pelo ransomware durante o ano passado disseram que perderam acesso a uma quantidade significativa de dados ou até mesmo a todos os dados. Um em cada seis daqueles que pagaram o resgate nunca recuperou seus dados.

A fim de abordar a crescente ameaça representada pelo ransomware em todo o mundo, especialistas da Kaspersky Lab recomendam que as empresas sigam as seguintes medidas:

1. Verifique se o patch da Microsoft que fecha esta vulnerabilidade específica foi instalado e certifique-se de instalar atualizações de segurança, pois elas irão resolver as vulnerabilidades no futuro;
2. Instale uma solução de endpoint como o Kaspersky Endpoint Security que, graças à sua Endpoint de Detecção e Resposta (EDR), é uma ferramenta que pesquisa e bloqueia de maneira proativa ameaças antes que elas causem danos custosos, responde de maneira rápida e eficaz aos incidentes de brechas de segurança, sem afetar a produtividade ou incorrer em grandes investimentos;
3. Faça backup de seus dados com frequência. Mesmo se você estiver em uma situação em que seus arquivos foram criptografados, faça backup desses dados, pois a chave para descriptografá-los pode estar disponível por alguns dias e você poderá recuperá-los;
4. Em caso de infecção no seu equipamento, a recomendação é não pagar o resgate. Em vez disso, as empresas são aconselhadas a consultar a página da iniciativa No More Ransom de um computador limpo. O projeto reúne fornecedores de segurança e agentes policiais para rastrear e interromper as atividades de grandes famílias de ransomware a fim de ajudar as pessoas a recuperar seus dados e minar o lucrativo modelo de negócios dos criminosos.

Além disso, a Kaspersky Lab oferece dois tipos de soluções que ajudam as empresas a lutarem contra esse tipo de ameaça:

- **Kaspersky Anti-Ransomware Tool** para empresas é uma ferramenta gratuita que ofrece segurança completa para proteger seus usuários corporativos de contra ransomware. A ferramenta identifica os padrões de comportamento do ransomware e protege terminais baseados no Windows e utiliza duas tecnologias inovadoras: Kaspersky Security Network e System Watcher. Os recursos exclusivos do System Watcher incluem a capacidade de bloquear e restaurar alterações prejudiciais. Baixe a ferramenta grátis aqui.
- **Kaspersky Cloud Sandbox** é um serviço de assinatura que permite os clientes a acabarem com arquivos suspeitos em um ambiente virtual com um relatório completo sobre as atividades do arquivo. O serviço é projetado para aumentar a eficiência da resposta a incidentes e da cibersegurança forense, sem qualquer risco para os sistemas corporativos de TI. Para mais informações, visite https://www.kaspersky.com/blog/cloud-sandbox/22010/.

Sobre a Kaspersky Lab

A Kaspersky Lab é uma empresa internacional de cibersegurança que tem mais de 20 anos de operações no mercado. A detalhada inteligência de ameaças e a especialização em segurança da Kaspersky Lab se transformam continuamente em soluções e serviços de segurança da próxima geração para proteger empresas, infraestruturas críticas, governos e consumidores finais do mundo inteiro. O abrangente portfólio de segurança da empresa inclui excelentes soluções de proteção de endpoints e muitas soluções e serviços de segurança especializada para combater ameaças digitais sofisticadas e em evolução. Mais de 400 milhões de usuários são protegidos pelas tecnologias da Kaspersky Lab, e ajudamos 270.000 clientes corporativos a proteger o que é mais importante para eles. Saiba mais em www.kaspersky.com.br.