Exposição de falhas de gigantes de tecnologia continuará em 2018 [1]

Recomendadas

Problema está centrado na falta de atualização de computadores, que deve ser feito pelo usuário.

É preciso estar antenado com as novas práticas dos cibercriminosos, entender os ataques e conseguir reagir às suas ameaças, protegendo as empresas desses perigos digitais. Confira neste material um guia prático sobre ataques criptor e entenda como se defender.

Logo nos primeiros dias do ano, vulnerabilidades como Meltdown e Spectre foram descobertas em todos os processadores utilizados no planeta. Profissionais de segurança revelaram a existência dessas falhas gravíssimas de segurança, que afetam inúmeros processadores fabricados ou que embarcam tecnologias da Intel, AMD e ARM nos últimos 20 anos.

Em 2018, segundo estimativa da consultoria Gartner, o investimento global na segurança da informação deverá ser de US$ 93 bilhões, o que representa aumento de 12% em relação ao ano passado. Contudo, na visão de Prado, mesmo com as altas cifras, o setor se mostra vulnerável e coloca em risco os dados dos usuários, sejam eles empresariais ou não, por meio de falhas como a Meltdown e a Spectre..

O especialista lembrou que as duas falhas foram capazes de atingir os principais fabricantes de processadores, Intel, AMD e ARM, envolvendo sistemas operacionais da Microsoft, Apple e Google. O primeiro, Meltdown, é uma lacuna de segurança em hardware de chips Intel que explora a comunicação entre os núcleos de processamento para interceptar as informações que ali trafegam. Essa brecha não possibilita que ocorram alterações ou a exclusão dos dados, porém coloca em risco a integridade de itens tais como nomes de usuário, senha e informações bancárias.

O Spectre, por sua vez, é uma vulnerabilidade capaz de atacar diversos modelos e marcas de processadores. Pode ser executado por meio dos navegadores web com a

[1] Bruno Prado *é CEO da UPX Technologies* - 19 de Janeiro de 2018

execução de um código em Java, o que coloca em risco os usuários de todos os tipos de dispositivos que possuam acesso à rede mundial de computadores.

Além dessa falha identificada nos processadores, Prado faz alerta para outras ameaças. Uma delas, diz o especialista, é um botnet chamado Reaper, que tem se propagado rapidamente e já infecta diversas organizações por meio de dispositivos internet das coisas (IoT), computadores e roteadores desprotegidos. "A qualquer momento, poderá haver um ataque de negação de serviço (DDoS) em larga escala, provavelmente o maior já registrado, superando o Mirai, que tirou do ar diversos servidores em 2016", alerta o especialista.

Falta de atualizações

O cenário traz um alerta para os CIO: assim como na maioria dos ataques, diz Prado, os danos são provenientes de atrasos em atualizações. "Ao utilizar softwares desatualizados, os usuários se expõem aos riscos de brechas de segurança, que são aproveitadas pelos cibercriminosos como forma de abrir caminho para o roubo de informações", alerta.

As empresas, por sua vez, são testadas em tempo integral por criminosos virtuais, que buscam por oportunidades de realizar malfeitos. "Para equilibrar a balança, é fundamental atuar em conjunto com um PenTest – método cuja finalidade é avaliar a segurança de um sistema de computador, tanto desktop quanto mobile, seus softwares, redes, sites, servidores, aplicativos e até hardwares, simulando um ataque malicioso para identificar possíveis vulnerabilidades nos sistemas", afirma.

Desse modo, prossegue Prado, os gestores ficam cientes de quais são os pontos frágeis que podem ser explorados e conseguem realizar um investimento mais preciso e garantir sua proteção contra toda a diversidade de ameaças presentes na rede, mitigando a exposição e, consequentemente, os riscos corporativos.

Mesmo que o tenha ano começado movimentado na segurança digital, o especialista em segurança digital, diz que há pontos positivos nesse cenário. "O início de um novo ciclo é o melhor momento para que haja a conscientização, planejamento e execução de ações em prol da proteção das informações". "Com os riscos, exposições e recuperações de 2017, é essencial que os gestores aumentem o foco e a importância na defesa de suas instituições, afinal, os criminosos e as ameaças não esperam", complementa.

Intel alerta que patches contra Spectre podem reiniciar PCs[2]

Fabricante diz que usuários devem instalar os updates mesmo assim, já que eles protegem as máquinas contra falha de CPU.

[2] 18/01/2018 - PC World / EUA

Os patches de firmware feitos para proteger os processadores da Intel contra a falha de CPU Spectre possuem um ponto negativo e tanto: estão forçando mais reinicializações frequentes em alguns sistemas, incluindo PCs lançados em 2017.

No último dia 11 de janeiro, a Intel disse que os patches causavam reboots mais frequentes em sistemas com os processadores Haswell (2013) e Broadwell (2014). No dia 17/1, o VP executivo da empresa, Navin Shenoy, revelou que muitas outras gerações de processadores também sofrem com esse bug que reinicia as máquinas, incluindo os seguintes chips: Sandy Bridge (2011), Ivy Bridge (2012), Skylake (2015) e Kaby Lake (2017).

Os únicos processadores dos últimos cinco anos que rodam sem problemas com os patches – até o momento, pelo menos – parecem ser os mais recentes chips Intel Core de oitava geração, chamados de Coffee Lake.

A PC World / EUA "Reproduzimos esses problemas internamente e estão fazendo progresso no sentido de identificar a causa disso. Em paralelo, na próxima semana deve ser liberado microcódigo beta para as fabricantes validarem", afirma o executivo.

Mesmo com esse problema que reinicia os PCs, os updates atuais de firmware ainda entregam proteção valiosa contra potenciais ataques por meio da vulnerabilidade Spectre. "A Intel recomenda que os parceiros mantenham a disponibilidade dos updates de microcódigo já lançados para os usuários finais", destaca o aviso da companhia. "A Intel não recomenda a retirada de qualquer update que já tenha sido disponibilizado para os usuários finais."

Em outras palavras: instale os patches, viva algum tempo com esses reboots (reinicializações) indesejados e fique de olho nas próximas atualizações de segurança que serão liberadas pelas empresas.

Google detalha como protegeu seus serviços das falhas Spectre e Meltdown[3]

Correções para as falhas Spectre e Meltdown reveladas recentemente podem prejudicar o desempenho de processadores e serviços de internet, mas o Google diz que conseguiu uma maneira de minimizar o impacto disso em seus serviços.

Em um post em seu blog oficial, o Google comenta que seus serviços já estão protegidos da falha, mas não foi fácil chegar a uma saída. Em um primeiro momento apenas o Meltdown e uma das variações do Spectre foram corrigidos, enquanto a segunda versão exigiu mais esforço por parte dos seus engenheiros.

Inicialmente, única forma que os engenheiros do Google tinham encontrado prejudicava demais o desempenho dos serviços da empresa, mas depois de alguns meses eles acabaram chegando a uma correção que mantinha tudo funcionando do jeito que devia. Enquanto o Meltdown e uma variação do Spectre já não ameaçavam mais seus serviços em setembro, a segunda versão da falha só foi consertada em dezembro.

De acordo com o Google, essas vulnerabilidades foram as "mais desafiadoras e difíceis de corrigir" dos últimos dez anos. Agora, diz a empresa, tudo está sob controle, e seus serviços não tiveram queda de desempenho por causa das correções.

Saiba como se proteger contra o "Meltdown", a grave falha em chips da Intel[4]

Mais uma vez falando do "Meltdown" e complementando informação sobre o assunto a falha de segurança encontrada por pesquisadores em chips Intel ter mostrado que é possível acessar praticamente qualquer dado de um PC que esteja na memória do chip, a indústria vem se debatendo para correr atrás do possível prejuízo. Milhões de clientes estariam vulneráveis, mas algumas empresas já estão trabalhando em soluções definitivas e temporárias para o problema. Por isso, nós trouxemos algumas dicas que podem deixar seu computador livre do "Meltdown", pelo menos por enquanto.

---

[3] Redação Olhar Digital 12/01/2018 - Google Internet Segurança

[4] By Rogerinho Freitas - Janeiro 4th, 2018 - *Fonte: THEVERGE - https://hack4fun.club/2018/01/04/saiba-como-se-proteger-contra-o-meltdown-a-grave-falha-em-chips-da-intel/*

Ataques explorando a falha em questão podem ser feitos na memória do processador por conta da forma como os chips atuais fazem diversos núcleos "conversarem" entre si. Dessa maneira, um hacker com conhecimento suficiente consegue interceptar praticamente toda a informação que estiver armazenada por ali. Felizmente, não há a possibilidade de fazer alterações ou excluir os dados através do Meltdown.

Não há a possibilidade de fazer alterações ou excluir os dados através do Meltdown

Para proteger seu computador, você deve tomar pelo menos duas ações diferentes: atualizar seu navegador para a versão mais recente disponível e buscar e instalar todas as atualizações do Windows 10.

A versão 57 do Firefox já oferece uma solução temporária, bem como as novas do Microsoft Edge e do Internet Explorer. A Google informou que o próximo Google Chrome, o 64, vai trazer um elemento de segurança similar no dia 23 de janeiro.

No Windows 10, é necessário abrir a central de atualizações e baixar todos os pacotes disponíveis. Você deve se certificar de que a atualização **"KB4056892"** está devidamente instalada. Caso contrário, force o Windows a buscar atualizações. A Apple ainda não se pronunciou sobre o problema, não tendo previsões para aplicar correções ao Safari ou ainda ao macOS.

Nas próximas semanas os fabricantes de processadores como: Intel; AMD; ARM; Qualcomm e outros devem liberar uma atualização de firmware, que é o sistema do hardware, capaz de definitivamente eliminar o problema do Meltdown. Há previsões, contudo, de que isso afete o desempenho dos chips atualizados, conforme foi comentado anteriormente, mas a Intel espera resolver isso posteriormente. Além disso, a distribuição vai depender das fabricantes desses aparelhos (computadores e smartphones) e não da Intel e suas rivais no segmento.