Imagem: iStock/NicoElNino

2018 O ano da cibersegurança

Como estão a evoluir as ciberameaças e como está a indústria a responder? E qual o verdadeiro efeito do "sismo" WannaCry na perceção das organizações quanto à importância de não negligenciar esta área do IT? Cisco, F5, Fortinet, GMV, Kaspersky Lab, Layer 8, Microsoft, Multicert e Palo Alto juntaram-se ao IT Channel e a um leitor convidado, o CIO da Lusitania, para debater o atual contexto da cibersegurança

Vânia Penedo

O ano de 2017 foi o ano do ransomware - WannaCry e Petya/Not Petya, em maio e junho, e Bad Rabbit, em outubro, deixaram o Mundo e a Europa em estado de alerta. Apesar de este tipo de malware estar em expansão e de ter sido o rosto mais visível do cibercrime no ano passado, não é a única ameaça a suscitar preocupações em 2018, já que estamos perante um panorama de elevada diversidade, povoado por ameaças cada vez mais complexas e sofisticadas. A crescente popularização do ransomware resultou, porém, num efeito positivo: demonstrou, aos que ainda tinham dúvidas, que num mundo em que o digital é o paradigma, os dados o novo petróleo e a conetividade ubíqua, o cibercrime é uma inevitabilidade à qual ninguém escapa.

"O mediatismo dos ataques em 2017 colocou a segurança e a gestão dos dados no centro das discussões", confirmou Pedro Lopes Vieira, responsável pelo Desenvolvimento de Negócio Secure eSolutions da GMV. "Acaba por ser um fator de sensibilização acrescido. O aspeto positivo dos ataques foi esse - recentrar e reposicionar a discussão em torno da segurança". Em 2018, existe uma única certeza: "Os ataques vão acontecer", disse.

Este ano, a Cisco prevê que continuem a verificar-se investidas de ransomware cada vez mais complexas e com algumas variações. "As ameaças do ano passado trouxeram alguma consciencialização para o que é a segurança da informação", revelou Luís Ramos, consulting systems engineer do fabricante. "Acredito que já fosse uma prioridade para muitas organizações, mas para muitos clientes, por um diverso conjunto de limitações, inclusive de budget, não o seria assim tanto".

O benefício, de acordo com João Abreu, system engineer da Fortinet, reflete-se numa mudança fundamental: "As abordagens deixaram de ser tão reativas para passarem a ser mais preventivas". Aliás, recordou, foi por demais evidente, aquando do WannaCry, que as empresas que já tinham implementado medidas precaucionais "não tiveram tanto impacto e que aquelas que não estavam preparadas sofreram mais". Ainda assim, observou, o WannaCry teve um "final feliz", por ter sido contido em tão pouco tempo. "Podia ter sido muito mais devastador".

Investimentos dependem da perceção de valor

Se a consciencialização do risco já começa a existir, podemos em 2018 esperar mais orçamento para a cibersegurança?

Paulo Vieira, sales manager da Palo Alto Networks, reconheceu que, no decorrer de 2017, as empresas começaram a olhar de forma diferente para a segurança e, finalmente, a operar gestão de risco. "Os orçamentos de cibersegurança não vão baixar, pelo contrário, vão até aumentar. E começa-se a

olhar para o que é ou não necessário em termos tecnológicos".

A intenção de investir é uma realidade desde há dois anos, segundo Fernando Simões, responsável pela área de enterprise business na Kaspersky Lab. Porém, continua a existir um problema: "O desafio dos investimentos em cibersegurança continua a ser a ausência de um ROI (retorno sobre o investimento) taxativo para o gestor". Por outras palavras, quando alguém do IT diz ao conselho de administração que é necessário investir em soluções de cibersegurança, não encontra do outro lado "a perceção de qual o impacto desses investimentos nos resultados globais do negócio". Esta distância entre negócio e IT, dentro das organizações, continua a ser um dos maiores entraves sentidos por este mercado. "Sim, há mais budget, não há é mais despesa", frisou o representante da Kaspersky Lab.

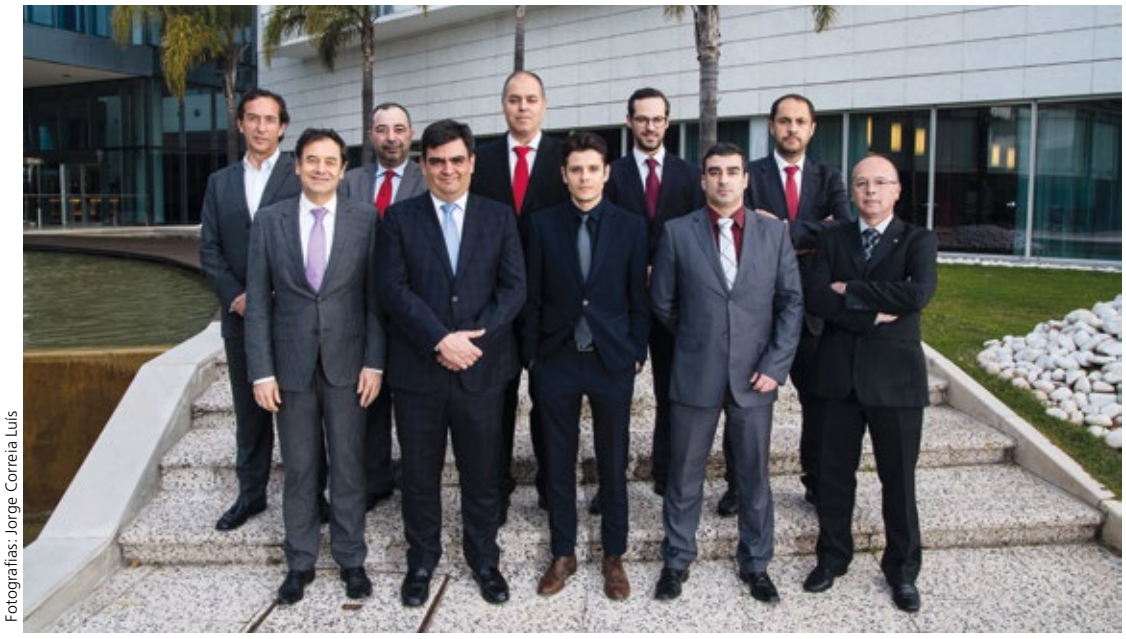
Este aspeto, o da "ausência de perceção do valor", nas palavras de Fernando Cardoso, CTO da Layer 8, "é um problema para fabricantes e integradores, e também para o CIO, que sente a dificuldade de, internamente, 'vender' essa necessidade". Deste modo, acrescentou, "a perceção do valor passa muito por que os gestores tenham a consciência

"Não tenho orçamento de segurança. Mas tenho segurança no orçamento"

Sérgio Martinho

CIO, Lusitania Seguros

de que, ao investirem em cibersegurança, estão a minimizar riscos e a aumentar o valor das empresas". Carlos Faria, responsável por Modern Workplace na área de segurança da Microsoft, apontou outro fator igualmente crítico: "Este tema não está na agenda de um CEO. Em Portugal não se tem sentido que as organizações tenham uma cultura centrada na cibersegurança". Esta, sobretudo, já não é somente da responsabilidade do IT. "A transformação digital dos processos de negócio amplia as superfícies de ataque - mais dados significam mais oportunidades para os atacantes. Além do mais, as organizações estão cada vez mais expostas nas redes sociais, o



Fotografias: Jorge Correia Luís

que pode comprometer uma marca. Isso significa que a segurança passa a ser uma responsabilidade do negócio".

Sérgio Martinho, CIO da Lusitania, disse não ter orçamento de segurança. "Mas tenho segurança no orçamento", disse. "A segurança não é um vertical, é horizontal a tudo o que se faz. A mensagem que o IT leva ao board está intimamente relacionado com o negócio".

A responsabilidade dos fornecedores

Nos conselhos de administração das maiores empresas do país, assegurou Jorge Alcobia, CEO da Multicert, "não existe nenhuma pessoa que domine minimamente o tema, e isso é um problema", referiu. "É difícil que exista alguma sensibilidade para

"A ausência da perceção de valor dos investimentos em cibersegurança é um problema para fabricantes e integradores"

Fernando Cardoso

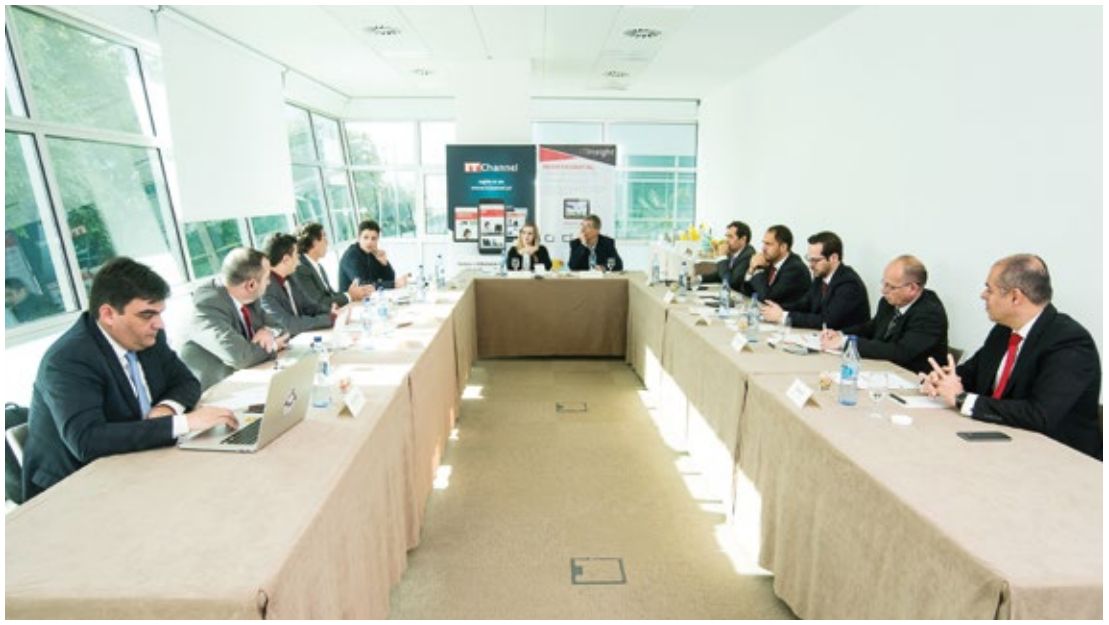
CTO, Layer 8

perceber os problemas que podem decorrer para o negócio. Porém, diria que parte da responsabilidade também está do nosso lado, dos fornecedores".

Sérgio Martinho, CIO da Lusitania, sublinhou a mensagem, identificando uma "profunda disrupção entre fornecedor, integrador e cliente". O chief information officer confessou que não discute tecnologia com o board da Lusitania. "Digo que temos de realizar determinado investimento, porque se não o fizermos o negócio será afetado de determinada forma". Olhar para o cliente como uma "entidade única foi o conselho deixado: "É fundamental perceber a área de atuação da empresa para conseguir acrescentar valor". Sérgio Martinho disse sentir, enquanto cliente, que existe uma "forte pressão por parte dos fornecedores para o atingimento de quotas", o que leva a que a abordagens comerciais "não sejam as mais indicadas". As empresas de IT devem começar por "fazer os impossíveis para falar com decisores", dado que muitas vezes as negociações ficam paradas no departamento de IT, porque se entende a cibersegurança como um tema somente de infraestruturas. "Isso é um problema, porque pode impedir que a proposta escale e suba na cadeia de valor da organização. Por vezes basta colocar a pergunta certa, como por exemplo, 'quem é o dono do orçamento'? Não tenham medo de colocar as perguntas mais elementares", aconselhou.

Manfred Ferreira (Westcon/F5) sublinhou que "é necessário entender os serviços críticos do cliente" e "aportar valor". Só assim será possível que as empresas do Canal se assumam como "um Parceiro que consegue realizar negócio hoje e nos próximos dez anos".

Paulo Vieira (Palo Alto Networks) aconselhou os Parceiros "a saber ouvir o cliente e utilizar uma linguagem minimamente simples e não tecnicista". Im-



porta veicular uma mensagem "não de produto, mas integradora, de uma solução end-to-end", realçou Carlos Faria (Microsoft). A necessidade de encontrar soluções transversais, "que abranjam vários vendors" também é uma preocupação para o CIO da Lusitania, Sérgio Martinho.

É tempo de ser um trusted advisor: "Quem está há mais tempo no mercado percebeu-o. Temos de ser o braço direto do cliente quando as coisas correm

"Dentro dos conselhos de administração não há quem domine minimamente o tema e isso é um problema"

Jorge Alcobia
CEO, Multicert

muito bem e quando correm muito mal", aconselhou Paulo Vieira (Palo Alto Networks).

Perceber as necessidades não apenas atuais, mas futuras é uma abordagem que deve estar no mindset do Canal. "Tem de haver um pensamento estratégico e uma abordagem mais consultiva", indicou Luís Ramos (Cisco).

O maior desafio do mercado da cibersegurança não é novo, mas está longe de ser solucionado. "Existe escassez de recursos humanos, falta de competências, o que torna o processo muito doloroso e difícil, tanto para os vendors como para os clientes finais", mencionou Carlos Faria (Microsoft).

No fundo, trata-se de ter a consciência de que, se o mercado mudou, a abordagem comercial também tem de mudar. "Quando se fala com o cliente deve perguntar-se se está pronto a mudar a infraestrutura de segurança para este paradigma de transformação digital. O que estamos a endereçar hoje no mercado não é o que endereçávamos há 20 anos. Nós somos os responsáveis pela transformação digital das empresas", disse, perentoriamente, Fernando Simões.

João Abreu (Fortinet) partilhou a visão de quem já vestiu a pele de cliente final, distribuidor, integrador e fabricante: "Todas estas experiências ofereceram-me uma visão end-to-end, porque consegui perceber todos os processos e dificuldades que cada um tem. Isso fez com que a minha abordagem fosse sempre no sentido de ser o mais claro possível. Do lado dos integradores, importa conhecer a dor do cliente e conseguir responder às suas necessidades. Do lado dos fabricantes, é preciso formar Parceiros e também os clientes, que têm de ter conhecimentos suficientes para saberem o que adquiriram".

Nesta cadeia de valor "muito importante", realçou, ninguém pode operar de forma isolada. "Não existem muitos Parceiros especializados em cibersegurança, mas os que existem são muito bons. Todos juntos devemos ajudá-los a aportar valor e a sentirem-se mais seguros".

Tecnologia ajuda na compliance do RGPD

O novo Regulamento Geral de Proteção de Dados, que será de cumprimento obrigatório a partir de 25 de maio, "é uma excelente oportunidade" para que as organizações percebam que "sem segurança não é possível garantir a privacidade dos dados", de acordo com Sérgio Martinho (Lusitania).

Pedro Lopes Vieira (GMV) referiu-se ao RGPD como "motivação induzida", por ter o mérito de "forçar alterações culturais na forma de olhar para a informação". A diretiva acaba por levar as organizações a olhar para a salvaguarda dos dados de um outro modo. A Multicert, que presta serviços nesta área, tem observado duas realidades. "Há empresas que estão a aproveitar este processo não tanto para efetuar uma operação de cosmética, mas para uma transformação mais profunda, no sentido inclusive de formar pessoas. Há outras que apenas procuram cumprir os requisitos mínimos, na eventualidade de uma auditoria", sublinhou Jorge Alcobia.

Para os vendors, a oportunidade está na "construção de uma framework que suporte todos os processos

"As abordagens à segurança deixaram de ser tão reativas para passarem a ser mais preventivas"

João Abreu
System Engineer, Fortinet

de negócio e ajude a obter conformidade", indicou Carlos Faria (Microsoft). "Vamos assistir provavelmente ainda este ano, no próximo certamente, a novas versões do RGPD. Para os vendors, a oportunidade é suportar as organizações e facilitar o pro-

cesso de compliance. A cloud, por exemplo, facilita, pela responsabilidade partilhada, retirando peso do lado do cliente", assinalou.

Assim, apesar de a tecnologia não ser a solução para o novo Regulamento, que é um tema de processos, este impõe a necessidade de identificar dados pessoais e de salvaguardar a privacidade. Por isso, para Luís Ramos (Cisco), irá materializar-se em tecnologia. "Estamos a observar que os clientes estão a aproveitar o RGPD como uma oportunidade para consolidar os sistemas".

Manfred Ferreira, business security developer da Westcon, em representação da F5, subscreveu este ponto, o dos dados. "O que fazemos é recolher os dados para que seja possível fazer uma análise. Existe a oportunidade para ser um enabler, para agilizar o processo de integração do RGPD nesta componente tecnológica".

"Serão mais frequentes os ataques direcionados e com objetivos específicos"

Carlos Faria

R.T. Modern Workplace na área da Segurança, Microsoft

Ataques sem ficheiros são tendência

À semelhança do que já aconteceu em 2017, este ano o malware deverá continuar a liderar ranking das ameaças mais prevalentes. Luís Ramos (Cisco) sublinhou que o ransomware, em concreto, continuará a vingar este ano "de forma ainda mais destrutiva" e que, devido à industrialização do próprio cibercrime, começa a assistir-se a uma evolução, do lado dos atacantes, para um cenário de ransomware-as-a--service. "Há plataformas disponíveis na dark web e muito facilmente se lançam ataques e se pedem resgates em bitcoins".

O ransomware, sendo a "ponta do iceberg", não deverá tardar em apontar armas também à cloud, segundo Fernando Cardoso (Layer 8). "Pela quantidade de dados que aí estamos a colocar, atrevo-me a dizer que irá atacar a cloud e também os providers de cloud pública".

Uma das principais tendências, do lado do malware, diz respeito à ausência de ficheiros para propagação de infeção. Os chamados ataques "fileless". "Por

"O roubo de dados e de identidade está presente em 27% dos ataques"

Manfred Ferreira

Solution Architect Westcon, F5

norma o malware recorre a um ficheiro para ser executado, mas a tendência será não para trabalhar com ficheiros, mas para ser residente na memória", referiu Luís Ramos (Cisco). Deste modo, os atacantes evitam a deteção por parte das soluções de endpoint security. "É outra forma de tornar o próprio ransomware mais eficaz — se não tivermos um ficheiro que infeta, ele vai à Internet buscar algo que se executa dentro de um flash, por exemplo", acrescentou Paulo Vieira (Palo Alto Networks). Este tipo de ataques já estão a acontecer, indicou, e tornam o processo mais ágil para os hackers, já que podem alterar o ficheiro no momento.

Pedro Lopes Vieira (GMV) antecipou um novo propósito do ransomware: "Mais do que capturar dados, o objetivo será cada vez mais criar disrupção no negócio, deitar redes abaixo, criar indisponibilidade de serviço".

APTs continuam a ser eficazes

Apesar de não serem uma novidade, as ameaças persistentes avançadas (APT - advanced persistent threats) continuarão a ser uma realidade e podem mesmo ser a principal intenção de um ataque de ransomware. "Numa infraestrutura, o ransomware é o ruído", frisou Fernando Simões (Kaspersky Lab). Por norma os criptolockers deixam pontos de falha que, na realidade, são ameaças avançadas. "O WannaCry, por exemplo, despoletou três APTs", declarou. Ainda de acordo com o responsável da Kaspersky Lab, "o WannaCry demonstrou que o objetivo do ransomware não é encriptar um ou dois PCs, mas fazer o sequestro de empresas inteiras".

A dedicação dos hackers tende a ser incansável, já o sabemos, e é por isso que os ataques avançados "não têm só uma componente tecnológica". O alerta foi deixado por Carlos Faria (Microsoft): "Serão mais frequentes os ataques direcionados e com objetivos específicos, e tem de existir uma preocupação a este respeito. Estes ataques obrigam a ter mecanismos de defesa muito mais avançados".
Porém, nem sempre os sistemas mais sofisticados são suficientes para proteger as empresas se estas descurarem o mais importante dos fatores: o humano. Não por acaso, os hackers continuam a recorrer à engenharia social, selecionando cuidadosamente as suas vítimas com o objetivo de conseguirem entrar nas empresas sem resistência. "Um perfil de Facebook vale 144 euros no mercado negro, e permite dar início a ataques muito específicos", partilhou

"Numa infraestutura, o ransomware é o ruído. O WannaCry despoletou três APTs"

Fernando Simões

Enterprise Business, Kaspersky Lab

Fernando Simões (Kaspersky Lab), como por exemplo campanhas de phishing "mais direcionadas e eficazes", complementou Fernando Cardoso (Layer 8).

O elo mais fraco nunca deixará de ser o comportamento humano quando o tema é a cibersegurança. "O nosso foco sempre foram os utilizadores, as pessoas. Muito do plano de cibersegurança assenta em

termos uma visão transversal de todo o serviço e negócio, mas também uma componente de ajuda ao utilizador", sublinhou Manfred Ferreira (Westcon/F5), que chamou a atenção para a prevalência do roubo de dados e de identidade. "De acordo com dados recolhidos pela F5 em 174 países, está presente em 27% dos ataques". A par do ransomware e do phishing, é uma "dor imediata". E, acrescentou, "44% dos ataques são ataques aplicacionais", já que "o centro das atenções são as aplicações que estão de uma forma transparente a enviar dados e a tomar ações sem que as pessoas se apercebam". O plano de cibersegurança da F5 Networks aposta por isso numa "defesa em profundidade, desde o cliente até às aplicações".

O roubo de computação para mineração de criptomoedas é outra clara tendência ao nível dos ciberataques, alertou Fernando Simões (Kaspersky Lab), que previu um aumento dos ataques a alvos físicos: "Infraestruturas críticas, smart grids e até mesmo aviões e automóveis". Para Luís Ramos (Cisco), o roubo de computação para minar criptomoedas "está a substituir o ransomware".

Inteligência artificial é arma dupla

O cibercrime é uma indústria e quem ataca não é (quase sempre) quem pensa e desenvolve as ferramentas de ataque, o que tem conduzido a uma

"Temos de trazer software para uma batalha de software"

Paulo Vieira

Sales Manager, Palo Alto Networks

democratização das investidas. Fernando Simões sublinhou que, do outro lado, nem sempre estão pessoas, já que podem ser "um ou vários dispositivos associados a uma ou mais pessoas".

Um dos fatores que mais tem contribuído para esta realidade é, de acordo com Paulo Vieira (Palo Alto Networks), a diminuição drástica dos custos da computação. "É uma equação matemática – se a capacidade de processamento está a aumentar e a ficar mais barata, está a tornar-se mais simples para os atacantes ter capacidade de processamento ao seu dispor". O ransomware "é um excelente exemplo", disse, porque já gera mais dinheiro do que o tráfico de estupefacientes.

O recurso a ferramentas de inteligência artificial (IA) e machine learning (ML) prometem facilitar ainda mais a vida dos hackers, ao dotar os ataques de um nível superior de agilidade e automatismo. "Já não são os humanos a lançar os ataques, há redes quase independentes a fazê-lo. Tratam-se de células terroristas com capacidades de processamento devastadoras", advertiu Jorge Alcobia (Multicert). "Estamos a falar de computação distribuída e quem está a defender-se não tem acesso a esses recursos. Dentro de pouco tempo teremos essencialmente

"Começa a falar-se de weaponização de IA. O botnet of things é uma tendência"

Pedro Lopes Vieira

Responsável Desenvolvimento de Negócio Secure e Solutions, GMV

máquinas contra máquinas. Estamos a entrar num paradigma totalmente novo". O CEO da Multicert sublinhou a importância da introdução do sandboxing, para efeitos de cyber threat intelligence, nos últimos anos, por permitir "compreender os ataques, perceber como acontecem e como arranjam mecanismos de ofuscação", técnica cada vez mais utilizada para limpar vestígios, disse.

Por esse motivo, explicou Paulo Vieira (Palo Alto Networks), "não é possível trazer pessoas para uma batalha de software — temos de trazer software". Do lado da defesa, IA e ML estão a ser utilizados para tornar a segurança mais proativa e preditiva, "para que se tomem ações mais rapidamente".
Não é difícil perceber porquê: "As pessoas têm sempre milésimos de segundo para tomar uma decisão. O tempo de reação é crucial e é aqui que entra o machine learning", reforçou. Carlos Faria (Microsoft) destacou, porém, que o ML só é bem-sucedido se for constantemente alimentado com dados que enriqueçam os algoritmos, do mais variado género – de contexto (identidade, rede, tipo dispositivo) computacionais (recolhidos dos dispositivos) ou relativos a critérios e controlos de segurança. Por este motivo, justificou, "players que nunca estiveram neste mercado, como a Microsoft ou a Google, começam a fazer sentido".

A este respeito, Fernando Cardoso (Layer 8) recordou que muitos fabricantes estão a desenvolver soluções de segurança "que utilizam modelos baseados numa enorme quantidade de informação recolhida junto das organizações para encontrar anomalias e agir em função disso". Do outro lado, os hackers estão a socorrer-se cada vez mais de algoritmos que permitam que determinado malware permaneça inativo e infete "apenas no momento em que pode despoletar um ransomware", explicou. Por este motivo, segundo Luís

"A tendência será para que o malware não trabalhe com ficheiros e seja, antes, residente na memória"

Luís Ramos

Consulting Systems Engineer, Cisco

Ramos (Cisco), ao nível de advanced malware protection, é fundamental não descurar a componente da deteção, e "olhar constantemente para todos e quaisquer processos que estejam a ocorrer".

Porém, o uso malicioso da IA não se fica somente pela automatização dos ataques. "Diz respeito também à diversificação, recorrendo a user behavioral analytics para imitar comportamento humano, o que é assustador", acrescentou Pedro Lopes Vieira (GMV). "Não é por acaso que se começa a falar de weaponização de IA. A questão do botnet of things, a diversificação da capacidade para produzir ataques com recurso a computação remota será uma tendência".