Enfrentando a complexidade

Como lidar com cyberincidentes complexos causados por ameaças sofisticadas modernas

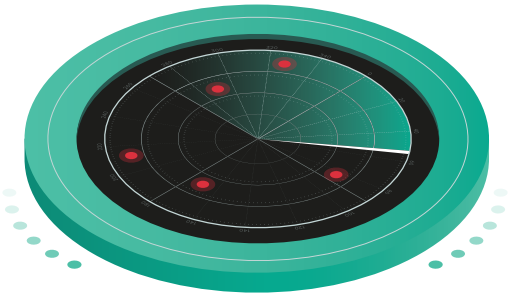
kaspersky BRING ON THE FUTURE

Nem sempre é possível parar uma ameaça antes que ela penetre no perímetro de segurança, mas está totalmente dentro do nosso poder prevenir que o ataque se espalhe e limitar ou excluir os possíveis danos resultantes. Quando se trata de ataques complexos ou direcionados, a velocidade da resolução do incidente é crucial.

No entanto, os incidentes complexos apresentam desafios muito específicos, pois geralmente envolvem muitos aspectos da infraestrutura da organização que está sob ataque. De certa forma, isso apresenta o dilema: como saber por onde começar quando tudo parece ser o mais importante?

Neste artigo, vamos examinar as cinco principais barreiras para alcançar uma solução de incidentes complexos bem-sucedida. Mas, primeiro, vamos começar questionando a própria ideia de complexidade e o que isso significa para os profissionais de cibersegurança.

O que é, exatamente, um incidente complexo?



Um incidente complexo pode ser definido com mais precisão em oposição a um incidente simples. Seria uma negligência não mencionar que a pandemia mundial da COVID-19 é o resumo de um incidente complexo; ela envolve vários sistemas: países, organizações (governamentais e corporativas), comunidades, escolas, setores, famílias e seres humanos individuais. Sem falar que o vírus age como um incidente complexo dentro do corpo das pessoas que são infectadas; seus efeitos vão além do sistema respiratório, incluindo os sistemas cardiovascular, renal, dermatológico, neurológico, imunológico e até psiquiátrico.

Ciberespaço complexo, cenário de ameaças complexo, incidentes cibernéticos complexos: uma progressão natural?

Vale a pena destacar que a crescente complexidade dos incidentes cibernéticos está diretamente relacionada ao aumento da complexidade dos sistemas corporativos de TI em expansão e, na verdade, do próprio ciberespaço. Na realidade, de acordo com o relatório Emerging Trends January 2019 to April 2020 Threat Landscape Report da *ENISA* (Agência Europeia para a Segurança das Redes e da Informação), "a interconectividade de diversos sistemas e redes permite que os incidentes cibernéticos se espalhem rapidamente e de maneira mais ampla, tornando mais difícil avaliar e atenuar os riscos cibernéticos". Em outras palavras, quanto mais complexa a infraestrutura de TI corporativa, mais ela estará sob risco de sofrer ataques cibernéticos complexos, o que torna o desafio de incidentes complexos ainda mais grave para grandes organizações inerentemente complexas.

Porém, a correlação natural entre ambientes complexos e os incidentes complexos se estende para além do sistema corporativo complexo específico. O próprio ciberespaço é definido pela ISO/IEC 27032:2012 como um "ambiente complexo resultante da interação de pessoas, software e serviços na Internet por meio de dispositivos e redes de tecnologia conectados a ele, que não existe em uma forma física". Em outras palavras, o que enfrentamos tem três camadas de complexidade: o ciberespaço, o ambiente de TI corporativo e os incidentes cibernéticos. Complicando ainda

mais esse cenário está o fato de que essas três camadas estão interconectadas e são interdependentes, cada uma se tornando cada vez mais complexa para alcançar seus objetivos:

Ciberespaço – aumento da dependência em dispositivos, sistemas e processos interconectados a fim de dar suporte aos negócios diários e ao lazer, levando ao aumento da complexidade do ambiente

Ambiente de TI corporativo – enfrenta uma superfície de ataque em expansão resultante do aumento no número de dispositivos, sistemas e processos interconectados (incluindo a cadeia de fornecimento) e, simultaneamente, do forte crescimento na complexidade de incidentes cibernéticos que sofridos por ela, bem como das configurações de cibersegurança necessárias para defender-se deles.

Cenário de ameaças e seus agentes – de um lado, responder ao aumento da complexidade do ciberespaço e do ambiente corporativo e, do outro lado, utilizar especificamente essa complexidade para lançar ataques avançados altamente sofisticados (envolvendo movimento lateral de um pedido que não seja possível nos dias de sistemas de destino mais simples).

A verdade indesejável é que, dentre esses três, os agentes de ameaças são os que encontraram meios de reduzir a barreira de complexidade mais rapidamente, ao recorrer ao malware como serviço, entre outras coisas:

> "Hoje em dia, as barreiras de entrada para os aspirantes a cibercriminosos estão caindo rapidamente porque os invasores têm diversas funcionalidades e recursos substanciais (técnicos) à disposição, uma vez que o malware e o malware como serviço são disponibilizados de modo mais fácil e mais barato em vários meios e fontes (como a Dark Web e a Deep Web). Como resultado, uma grande variedade de técnicas e ferramentas avançadas (por exemplo, técnicas de engenharia social e programas de exploit de "dia zero") está disponível e pode ser usada por cibercriminosos para iniciar ataques direcionados avançados."
>
> Papastergiou, S., Mouratidis, H. & Kalogeraki, EM. **Handling of advanced persistent threats and complex incidents in healthcare, transportation and energy ICT infrastructures.** Evolving Systems (2020).

A boa notícia é que há maneiras para que as empresas possam diminuir a barreira da complexidade de modo significativo, eficaz e decisivo, e vamos abordar isso mais adiante neste artigo. Antes de fazer isso, vamos examinar as cinco principais barreiras para alcançar uma resolução bem-sucedida de incidentes complexos.

As cinco barreiras para a resolução bem-sucedida de incidentes complexos

Sabemos que nós temos total capacidade de interromper o progresso das ameaças complexas, bem como limitar os danos causados por elas, mesmo quando já penetraram no perímetro corporativo. Para os iniciantes, vale a pena lembrar que a maioria das táticas de acesso inicial na estrutura corporativa MITRE ATT&CK ainda são relativamente tradicionais.

Entretanto, saber que o spearphishing ainda pode ser uma importante tática de acesso inicial, até para APTs, dentro do contexto caótico da pandemia mundial, deveria nos fazer parar para pensar. Primeiro, nós devemos considerar quantos ataques poderiam ser evitados ao automatizar tarefas de rotina de cibersegurança que bloqueiam o acesso inicial. Mas isso também realça o fato de que a penetração de ataque (com exceções como exploits de "dia zero") não é o que torna um incidente *complexo*.

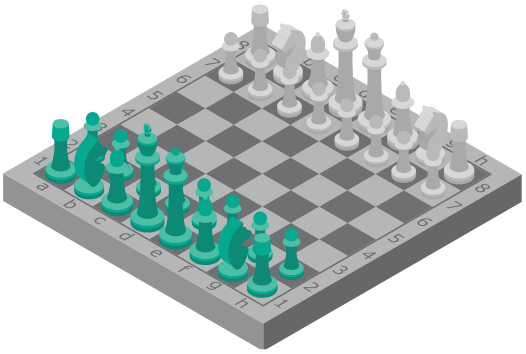
A complexidade começa com táticas como o movimento lateral e o estabelecimento de backdoors, bem como com diversos modos de entrega e ocultação de cargas. Então, o que impede que as equipes de segurança de TI consigam exercer seu poder e expertise para impedir que um incidentes se torne complexo? E depois que o incidente se torna complexo, por que é frequentemente tão difícil atenuar e resolvê-lo com êxito?

Barreira nº 1: A complexidade dos sistemas de cibersegurança por si só

Para uma pessoa que não é da área, uma configuração de cibersegurança corporativa média é tão confusa quanto o cockpit de um avião a jato. Não que exista realmente algo como uma empresa média ou uma configuração de cibersegurança média, é claro. Várias ferramentas, lidar com tarefas de segurança específicas altamente especializadas, diversos consoles de controle e enormes quantidades de alertas constantemente. Nós já vimos como essa complexidade surgiu; é, por um lado, uma evolução óbvia em resposta à crescente complexidade da infraestrutura de segurança de TI corporativa e, por outro lado, ao cenário de ameaças.

No entanto, é irônico e uma terrível tragédia que a complexidade da configuração de cibersegurança com frequência se torne uma barreira real para a resolução bem-sucedida dos incidentes muito complexos que ela deveria resolver. Essa complexidade impede a atenuação e a resolução bem-sucedidas das seguintes maneiras:

- As equipes estão se afogando em ferramentas, investindo seu tempo precioso agindo como "intérpretes" entre soluções distintas. As pilhas de tecnologia de cibersegurança (e as pilhas de tecnologia em geral) com frequência se transformam em Torres de Babel virtuais, com a operação contínua e perfeita sendo impedida porque as diferentes ferramentas falam "linguagens" distintas.
- Quando os dados de incidentes cibernéticos são coletados em pequenas amostras de uma grande variedade da sensores de dados não integrados em potenciais pontos de penetração, as equipes geralmente não conseguem ter uma visão geral e, por isso, são incapazes de perceber que um incidente complexo está ocorrendo antes que aparecem sinais de entrada óbvios. Em outras palavras, o incidente não é totalmente compreendido e isso pode, no fim, levar a danos.
- A necessidade de processamento manual constante que surge ao lidar com alertas e processos de resposta a incidentes inconsistentes e não sistemáticos drena uma energia valiosa, fazendo com que alertas cruciais não sejam notados e seja dedicada atenção em excesso a falsos positivos.



Barreira nº 2: Inteligência de ameaças deficiente ou irrelevante

A inteligência de ameaças deve passar por um teste rigoroso de três partes se ela pretender começar a atender sua promessa de entregar visibilidade profunda sobre as ameaças cibernéticas direcionadas à sua organização:

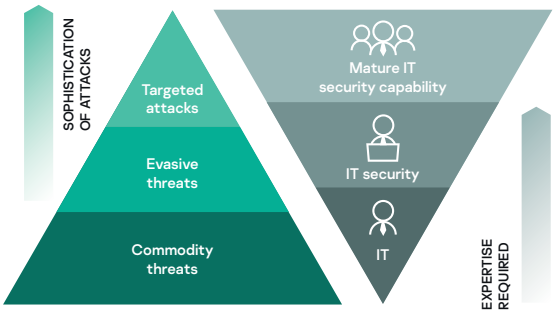
- Ela é abrangente?
- Ela é precisa?
- Ela está atualizada?

Entretanto, passar nesse teste é apenas a primeira etapa. A barreira que muitas organizações de nível corporativo enfrentam atualmente é que, embora tenham acesso a uma inteligência de ameaças abrangente, precisa e atualizada, elas estão perdendo uma parte essencial: a relevância. Qualquer profissional de segurança de TI familiarizado com a variedade de feeds de inteligência de ameaças disponíveis atualmente está mais do que cientes disso.

A relevância talvez seja uma forma de dizer que a qualidade é mais importante do que a quantidade, mas isso é apenas parcialmente verdadeiro. A inteligência de ameaças deve vir de uma fonte que ofereça as duas coisas e deve ser canalizada ou processada por meio de um sistema holístico de cibersegurança que faz a curadoria e define a relevância para aquela organização específica, para aquele momento específico e para aquele ambiente específico. A relevância não é um esforço isolado, ela é um processo contínuo que envolve um ciclo de feedbacks entre os elementos integrados em uma configuração de cibersegurança.

A inteligência de ameaças com relevância de contexto, integrada a outros mecanismos de detecção e busca de ameaças, encontra o significado e o contexto automaticamente, poupando um valioso tempo ao fornecer clareza desde o início.

Barreira nº3: Uma tendência histórica de se concentrar em excesso em ameaças de comodities simples

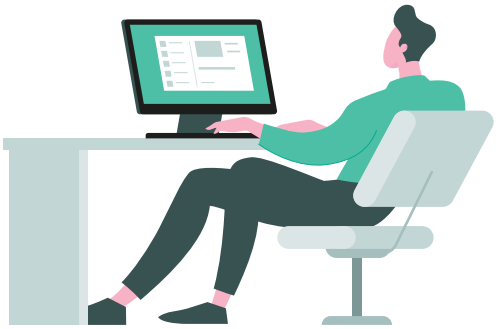


As ameaças a comodities simples ainda representam uma porcentagem bastante alta de todas as ameaças que qualquer organização enfrentará. Sendo assim, não surpreende que a tendência de se concentrar em excesso nessas ameaças ainda seja endêmica, mesmo em grandes organizações com segurança de TI madura.

No entanto, o custo dos incidentes associados a essas ameaças é insignificante comparado ao do dano potencial causado pela porcentagem restante, que inclui ataques complexos devastadores, como ataques direcionados e de APTs.

O outro motivo pelo qual algumas equipes de segurança de TI ainda se concentram muito em ameaças simples (em detrimento de incidentes complexos) é mais óbvio. É natural querer se dedicar a um problema simples que seja fácil de solucionar. Além disso, um dos motivos pelos quais as ameaças elementares são tão simples é que até a configuração de cibersegurança mais básica e com estrutura deficiente pode fazer um trabalho razoável de detecção automática delas e, ao mesmo tempo, não oferecer automação suficiente quando se trata de resolvê-las. Portanto, as ameaças simples podem ocupar muito espaço, demandando atenção que talvez não precisem, às custas de se concentrar em incidentes complexos que são muito mais letais.

Barreira nº 4: A crise de talentos de cibersegurança



Uma olhada rápida no Cyberseek Heat Map, uma iniciativa da US National Initiative for Cybersecurity Education (NICE), revela a extensão da crise de talentos de cibersegurança. Embora o Cyberseek aborde apenas as lacunas relacionadas à América do Norte, ele funciona como uma visão rápida muito útil (e moderada) sobre a escassez global.

Desde 30 de janeiro de 2021, foram abertas 521.617 ofertas de trabalho para profissionais de cibersegurança nos EUA, em relação a uma força de trabalho de cibersegurança empregada de 941.904 profissionais no total. Isso indica uma taxa média de oferta/procura nacional de 1,8.

Embora seja uma boa notícia para os profissionais de cibersegurança em termos de estabilidade no trabalho (e agora seria um bom momento para incentivar os jovens no ensino médio a perseguir uma carreira semelhante), ela não é uma boa notícia quando se trata de qualidade e eficácia na vida profissional.

A maioria dos analistas conclui que a crise de talentos de cibersegurança é devida a falhas em educação e treinamento, mas essa informação não ajuda as organizações de maneira prática. Até que essas falhas sejam abordadas e remediadas (em parte por iniciativas como o Cyberseek), as organizações precisarão lidar com essa barreira maximizando o poder de suas equipes de segurança de TI existentes, fornecendo as ferramentas, o suporte, a orientação e o apoio de que elas necessitam para conseguir resolver os incidentes complexos com êxito.

Barreira nº 5: O problema da velocidade

A última barreira para a resolução bem-sucedida de incidentes complexos está vinculada às quatro barreiras anteriores. Ao enfrentar desafios complexos, como os exploits de "dia zero", os ataques não relacionados a malware, os ataques sem arquivo e os ataques de subsistência, a velocidade é tudo.

Um incidente não começa necessariamente de maneira complexa, como vimos na continuidade da prevalência do spearphishing como uma tática para obter acesso inicial. As consequências devastadoras (e custosas) da enorme quantidade de incidentes complexos poderiam ser evitadas se a equipe responsável fosse capaz de responder com rapidez.

É claro que isso não deve sugerir que há um ponto na evolução de um incidente complexo em que passa a ser "tarde demais", pois como o tempo, o nível de complexidade também avança. Pode soar muito simplificado declarar que, quando se trata de incidentes complexos, a velocidade é tudo. Mas considerando que nós qualificamos o que queremos dizer com velocidade, isso é absolutamente verdadeiro.

Velocidade não significa combater incêndios constantemente nem ser um gatilho muito sensível e responder rapidamente a qualquer alerta que exija atenção. Significa a velocidade de execução com precisão de todos os processos de detecção e resposta essenciais de maneira decisiva e consistente. Isso inclui busca proativa de ameaças, análise de retrospectiva e causa básica, neutralização, atenuação, resposta a incidentes, entre outros.

O que o futuro reserva para as organizações ao enfrentar incidentes complexos?

O início de 2021 parece ser o pior momento da história recente para tentar responder qualquer pergunta sobre o futuro. Afinal, a pandemia já é, por si só, um incidente complexo para o qual nossas ferramentas, sistemas e profissionais não estão preparados. Mas ainda há algumas coisas das quais temos certeza. Por exemplo, sabemos que as APTs e outros ataques complexos continuarão a evoluir e também sabemos que o **trabalho à distância provavelmente continuará a crescer**, mesmo após a pandemia ser resolvida. Nossa Equipe de Pesquisa e Análise Global (GReAT), com os melhores pesquisadores de cibersegurança do mundo, fez as seguintes **previsões sobre APTs em 2021:**

- Os ataques de bandeiras falsas (como o Olympic Destroyer) alcançarão um novo nível
- O ransomware será cada vez mais direcionado
- Surgirão novos vetores de pagamento e banco on-line
- Ocorrerão mais ataques à infraestrutura e ataques contra alvos que não sejam PCs
- Aumento de ataques em regiões localizadas nas rotas de comércio entre Ásia e Europa
- Crescente sofisticação dos métodos de ataque
- Mais uma mudança de foco em relação aos ataques a dispositivos móveis
- Abuso de informações pessoais: desde deep fakes até vazamentos de DNA

A perspectiva desses incidentes complexos pairando sobre as cabeças dos profissionais de segurança de TI não precisa ser um sinal de algo terrível.

Voltando ao relatório Research Topics January 2019 to April 2020 da ENISA, nós encontramos um fio de esperança e uma dica de onde concentrar nossos esforços ao tentar solucionar com êxito os incidentes complexos: a dimensão humana:

"A cibersegurança ainda é vista como a prática de proteger redes, sistemas de informações e dados (NIS). Essa definição precisa ser expandida para além das questões técnicas a fim de incluir as preocupações sociais, comportamentais e econômicas e as diferentes funções executadas pelas partes envolvidas. Isso deve ser uma prioridade nas discussões futuras sobre pesquisa e inovação de cibersegurança. Uma compreensão melhor da dimensão humana é essencial para definir qualquer estratégia de cibersegurança, de modo que as decisões de segurança sejam tomadas para atender suas necessidades, habilidades e expectativas."

Para os nossos propósitos, as "partes" mencionadas acima referem-se aos profissionais de segurança de TI, bem como aos líderes corporativos, pelos quais eles são responsáveis. Talvez não seja possível recrutar todos os talentos de cibersegurança de que nós precisamos e, por isso, nos questionamos: como podemos estimular o que já temos?

Expert tech in expert hands

O primeiro passo é compreender que até as organizações com maior maturidade de TI não estão preparadas para enfrentar ameaças complexas e ataques de APTs. Isso é um problema global, com mudanças constantes de regiões e setores, e muitas equipes estão concentradas em seus esforços para resolver os incidentes complexos com êxito, tudo isso por causa das barreiras que analisamos neste artigo.

Por isso que nós incentivamos todos os nossos clientes corporativos a assegurar que eles abordem com empenho o que consideramos ser os três pilares de qualquer estratégia de incidente complexo. Ou seja, as equipes de segurança devem estar:

- **Equipadas:**
  A cibersegurança é uma área de especialização em que até um profissional qualificado pode culpar legitimamente suas ferramentas. A proteção contra ataques multivetoriais e outros incidentes complexos exige uma plataforma consolidada unificada que forneça visibilidade total, eliminando silos obstrutivos e evitando o excesso de alertas e outras tarefas de rotina dentro do processo de resposta a incidentes.

- **Informadas:**
  A especialização avançada existente das organizações com maturidade de TI nunca deve ser considerada como certa. Afinal de contas, o horizonte de crimes cibernéticos está em constante mudança e expansão. A educação contínua e a inteligência de ameaças robusta de um parceiro de cibersegurança confiável são essenciais.

- **Reforçadas:**
  Quando um incidente complexo ou uma APT é descoberta, até os analistas de segurança de TI mais avançados deveriam ter acesso a suporte externo para obter opinião de terceiros, avaliação de segurança, busca de ameaças gerenciada e resposta a incidentes. Embora os incidentes complexos resultantes de APTs sejam altamente direcionados, eles raramente visam apenas uma vítima. Especialistas externos podem lançar uma luz global de vários setores sobre os prováveis caminhos de uma APT e fornecer conselhos práticos sobre a melhor maneira de eliminá-la do sistema.

Revolucione a maneira como seus especialistas em segurança de TI controlam os incidentes complexos

Revolucione a maneira como seus especialistas em segurança de TI controlam os incidentes complexos com o Kaspersky Expert Security: um conceito de defensa abrangente que equipa, informa e orienta a equipe na luta contra os ataques cibernéticos mais sofisticados e direcionados. Ele é uma plataforma de XDR (Extended Detection and Response) com uma combinação perfeita de tecnologia líder do setor, inteligência de elite contra ameaças, experiência humana, treinamento e serviços, tudo isso com o apoio das maiores mentes em cibersegurança. Nossa abordagem holística estimula o poder de cibersegurança da sua equipe em relação à descoberta de ameaças multidimensionais, investigações eficazes e busca proativa de ameaças, oferecendo uma resposta rápida e centralizada a todo o espectro de ameaças modernas

Saiba mais em **https://go.kaspersky.com/expert-pt-br.html**

Notícias sobre ameaças cibernéticas: www.securelist.com
Notícias sobre segurança de TI: www.kaspersky.com/blog
Threat Intelligence Portal: opentip.kaspersky.com
Um olhar sobre as tecnologias: www.kaspersky.com/TechnoWiki
Prêmios e reconhecimentos: media.kaspersky.com/en/awards
Ferramenta de portfólio interativo: kaspersky.com/int_portfolio

www.kaspersky.com.br

kaspersky BRING ON THE FUTURE