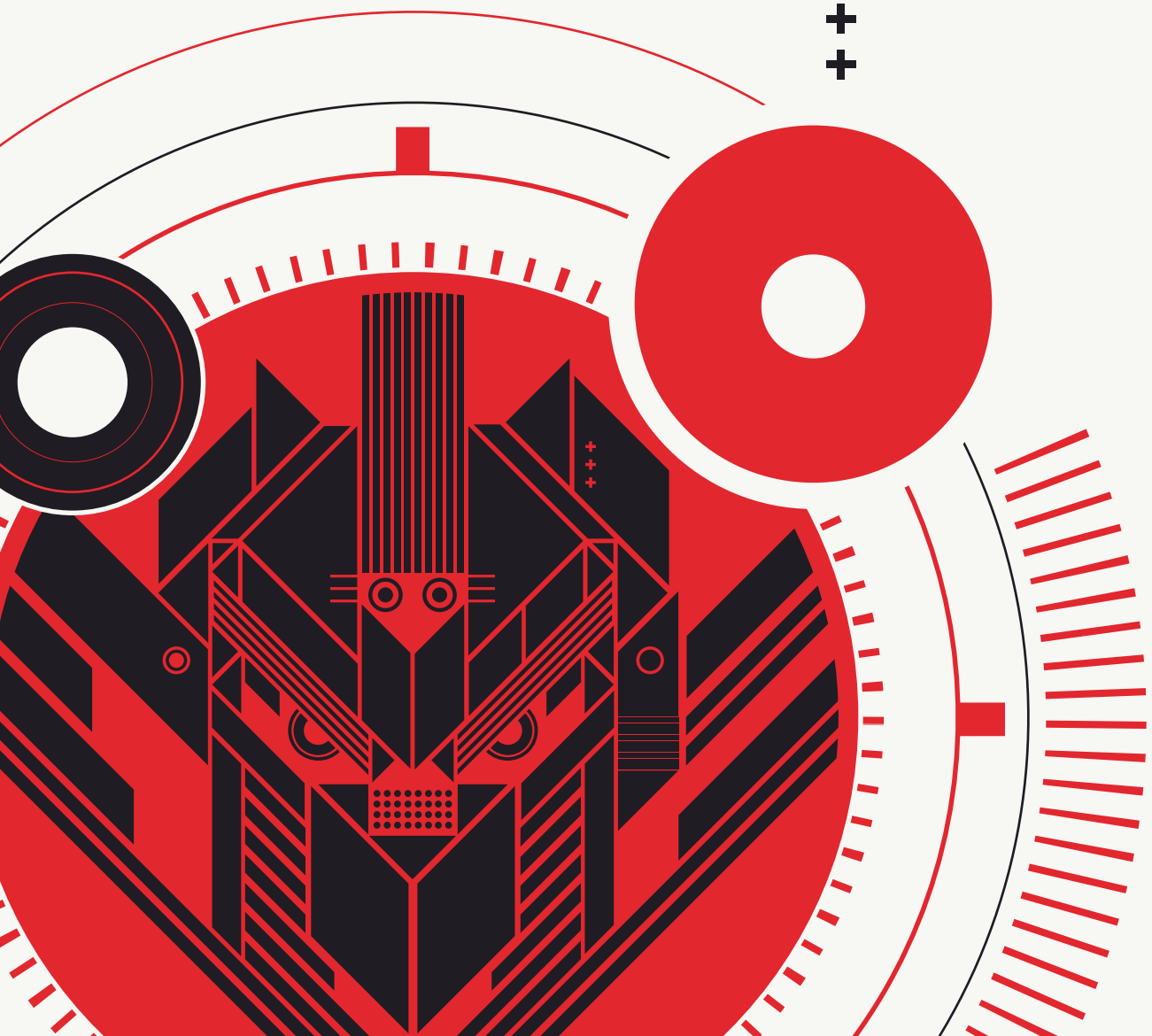
CROWDSTRIKE

2020

RELATÓRIO GLOBAL DE AMEAÇAS

RESUMO EXECUTIVO



FOI MAIS UM ANO ATIVO NA CIBERSEGURANÇA,

ameaças de nível nacional e e-crimes sustentados mirando organizações de praticamente todas as áreas. A CrowdStrike® observou incidentes direcionados a entidades nos setores acadêmico, governamental, de saúde, hospitalidade, tecnologia, energia, serviços financeiros e manufatura em todo o mundo, com diversos tamanho, de pequenas empresas a conglomerados da Global 1000.

No Relatório Global de Ameaças de 2020, a equipe de Inteligência CrowdStrike, a equipe de investigação gerenciada de ameaças Falcon OverWatch™ e a equipe de resposta a incidentes dos Serviços CrowdStrike destacam os eventos e tendências mais significativos das atividades de ciberameaças do ano passado.

ATIVIDADES DE ECRIMES

A maior parte dos lucros de ransomware parece destinada àqueles que são capazes de dominar vários métodos de monetizar suas habilidades e ferramentas.

- **Observou-se uma escalada em big game hunting (BGH)**, ou seja, ataques de ramsomware com motivação criminosa direcionados a organizações de porte empresarial. BGH foi a atividade mais lucrativa para o eCrime - as demandas de resgate chegaram aos milhões, causando disrupções sem precedente. Atualmente, não há indicações de que os perpetradores de BGH pretendam desacelerar suas operações.
- **Cibercriminosos estão transformando dados confidenciais em armas para aumentar a pressão sobre as vítimas de ransomware.** Foram observados casos de adversários ameaçando vazar dados confidenciais e, algumas vezes, cumprindo a ameaça, como meio de obter pagamentos de resgate de vítimas que optaram por restaurar suas redes usando cópias de segurança.
- **O ecossistema do eCrime continua a evoluir, amadurecer e desenvolver uma crescente especialização.** Organizações criminosas estabelecidas continuaram a expandir, trocando Trojans bancários por:
  - Desenvolvedores de Ransomware como Serviço **(RaaS)** que adotam ataques BGH
  - Desenvolvedores de Malware como Serviço **(MaaS)** trazendo módulos de ransomware
  - Operações de Download como Serviço **(DaaS)** que distribuem malware de terceiros

  Esses esforços para habilitar campanhas de **BGH** enfatizam o enorme efeito cascata que o ransomware direcionado causou no ecossistema do crime.
- Além do **BGH**, foi observado um aumento nas campanhas de eCrime direcionadas às instituições financeiras por meio de fraudes em transferências ou saques em caixas eletrônicos, com a atividade se expandindo para além dos EUA, Canadá e Europa, afetando as América do Sul e Central e a África.

- **Os ataques sem malware aumentaram, ultrapassando o volume de ataques com malware.** Em 2018, 40% dos ataques usaram técnicas livres de malware, em 2019, este número aumentou para 51%. Isso ressalta a necessidade de avançar além das soluções de antivírus básicas.

- **Os adversários continuam a evoluir e a atualizar suas táticas, técnicas e procedimentos (TTPs) com atividades sofisticadas**, incluindo a inutilização de produtos de segurança, encapsulamento de DNS, uso de sites comprometidos hospedando o sistema de gerenciamento de conteúdo WordPress (CMS), sequestro de correntes de email, comprometimentos 2FA e criadores de documentos dropper e serviços de distribuição.

ATAQUES DIRECIONADOS PATROCINADOS PELO ESTADO

A publicação de táticas, técnicas e procedimentos associados às operações de nível nacional observadas em 2019 pode levar a métodos menos óbvios no próximo ano, mas a intenção permanecerá a mesma - coletar inteligência e promover divisão dentro das comunidades.

A CrowdStrike rastreia, em todo o mundo, vários adversários de intrusão direcionada patrocinados pelo Estado, incluindo grupos de agentes de ameaças atribuídos à República Popular Democrática da Coréia (RPDC ou Coréia do Norte), China, Rússia e Irã. Como em anos anteriores, a maioria das invasões direcionadas conduzidas por esses agentes parece motivada pelo objetivo clássico de coletar inteligência. A CrowdStrike Intelligence também está investigando a possível colaboração entre adversários sofisticados do crime eletrônico e intrusões direcionadas patrocinadas por Estados. Evidências iniciais sugerem que algumas ferramentas criminais se sobrepõem e/ou cooperam com serviços de inteligência na RPDC e na Rússia.

RPDC: O Chollima

As intrusões direcionadas com base na RPDC representam algumas das operações mais ativas em 2019.
As entidades na Coréia do Sul continuaram sendo de interesse estratégico para os adversários afiliados à RPDC. Além disso, vários incidentes tiveram como alvo a Índia e um adversário também atacou os EUA e o Japão com operações de coleta de inteligência focadas em questões nucleares e de sanções.

China: O Panda

A atividade dos adversários chineses manteve-se estável ao longo de 2019, com destaque para o setor de telecomunicações.
O alvo no setor de telecomunicações - especialmente na Ásia Central e no Sudeste Asiático - complementa o plano da China de desenvolver uma "Rota da Seda Digital", incluindo o desenvolvimento de redes móveis 5G. Vários governos observaram isso e recusaram oportunidades de trabalhar com a gigante chinesa das telecomunicações Huawei, citando preocupações sobre as associações da empresa a serviços militares e de inteligência na China, Rússia e RPDC. O alvo em empresas dos EUA envolvidas em indústrias chave consideradas vitais para os interesses estratégicos da China - incluindo energia limpa, saúde, biotecnologia e área farmacêutica - provavelmente vai continuar.

Rússia: O Bear (The Bear)

Ao longo de 2019, a CrowdStrike Intelligence observou atividades de intrusão direcionadas da Rússia contra a Ucrânia.

A grande maioria dessas operações parece ter como alvo diplomatas ucranianos e oficiais de segurança nacional, provavelmente coletando informações políticas e militares relacionadas ao conflito ucraniano. Parece que os adversários russos podem ter tentado influenciar o resultado da eleição presidencial ucraniana em março de 2019, com vários relatos de campanhas de desinformação, ataques distribuídos de negação de serviço (DDoS) e comprometimentos das mídias sociais. À medida que o conflito entre a Ucrânia e a Rússia continua, é provável que as operações de coleta de inteligência afiliadas à Rússia continuem - ou aumentem - no futuro.

Irã: O Gatinho (The Kitten)

Em meio à crescente tensão entre o Irã e os EUA, a atividade adversária iraniana sugere um foco crescente no governo tendo o setor de defesa como alvo.

Embora a atividade no início do ano tenha se concentrado em países do Oriente Médio e Norte da África (MENA, na sigla em inglês), no segundo semestre de 2019 houve uma mudança significativa dos adversários iranianos em direção a entidades nos EUA, provavelmente em resposta às tensões entre o Irã e os EUA. que começaram em maio de 2019. A CrowdStrike Intelligence avalia com alta confiança que os adversários iranianos continuarão usando ciberespionagem para dar suporte a coleta de inteligência tradicional, com ênfase particular na região MENA e na América do Norte.

Com base na atividade observada em 2019, organizações de defesa, marítimas, de telecomunicações e tecnologia da informação na região MENA provavelmente serão de particular interesse para os adversários iranianos em 2020.

RECOMENDAÇÕES DA CROWDSTRIKE

A CrowdStrike faz as seguintes recomendações para ajudar a proteger sua organização e fortalecer suas defesas contra os adversários em constante evolução de hoje - e de amanhã:

Tire o maior proveito possível da proteção que você possui. A proliferação de BGH aumentou drasticamente o impacto nas organizações que não implementam proteções adequadas. As organizações inteligentes gastam o tempo necessário para maximizar os controles de segurança que elas possuem no momento.

Proteja identidades. No ano passado, houve uma tendência crescente para técnicas de ataque sem malware. Como linha de base, a autenticação de dois fatores (2FA) deve ser estabelecida para todos os usuários, porque os atacantes de hoje são hábeis em acessar e usar credenciais válidas, levando rapidamente a um comprometimento mais profundo. Além disso, um processo robusto de gerenciamento de acesso a privilégios limitará o dano que os adversários podem causar se entrarem.

As organizações que atendem à meta 1-10-60 têm muito mais probabilidade de expulsar adversários antes que um ataque se espalhe do seu ponto de entrada inicial, minimizando a escala e o impacto.

Relacione seus usuários na luta. Embora a tecnologia seja claramente crítica na luta para impedir os invasores, o usuário final continua sendo um elo crítico na cadeia. Programas de conscientização do usuário devem ser iniciados para combater a ameaça contínua de phishing e técnicas de engenharia social relacionadas.

Atinja o benchmark 1-10-60. A CrowdStrike pede às organizações que adotem a "regra 1-10-60" para combater efetivamente ameaças cibernéticas sofisticadas: Detecte invasões em menos de um minuto, investigue e compreenda ameaças em menos de 10 minutos, e contenha e elimine o adversário do ambiente em menos de 60 minutos.

Procure parceiros para ajudar a preencher a lacuna de talentos. Operar na velocidade 1-10-60 requer mais do que tecnologia. A defesa contra ameaças sofisticadas, no final das contas, exige processos maduros e profissionais de segurança eficazes e dedicados 24 horas por dia, 7 dias por semana. As empresas de sucesso geralmente fazem parceria com os melhores fornecedores de soluções da categoria para ajudar a preencher as lacunas críticas de talentos de maneira custo-eficaz.

Faça o download da sua cópia GRATUITA do **Relatório Global de Ameaças 2020 da CrowdStrike®** para obter mais informações e insights derivados de incidentes observados em todo o mundo em 2019 - e aprenda os caminhos recomendados para neutralizar os ciberataques em constante avanço em 2020: **http://crowdstrike.com/gtr.**

SOBRE A CROWDSTRIKE

A CrowdStrike® Inc. (Nasdaq: CRWD), líder global em segurança cibernética, está redefinindo a segurança para a era da nuvem com uma plataforma de proteção de endpoint criada do zero para impedir ataques. Utilizando inteligência artificial (IA), a plataforma CrowdStrike Falcon® oferece visibilidade e proteção instantâneas de toda a empresa, evitando ataques a endpoints dentro ou fora da rede. Alimentado pelo patenteado CrowdStrike Threat Graph™, o CrowdStrike Falcon correlaciona em tempo real mais de 3 trilhões de eventos relacionados a endpoints de todo o mundo por semana, abastecendo uma das plataformas de dados para segurança mais avançadas do mundo.