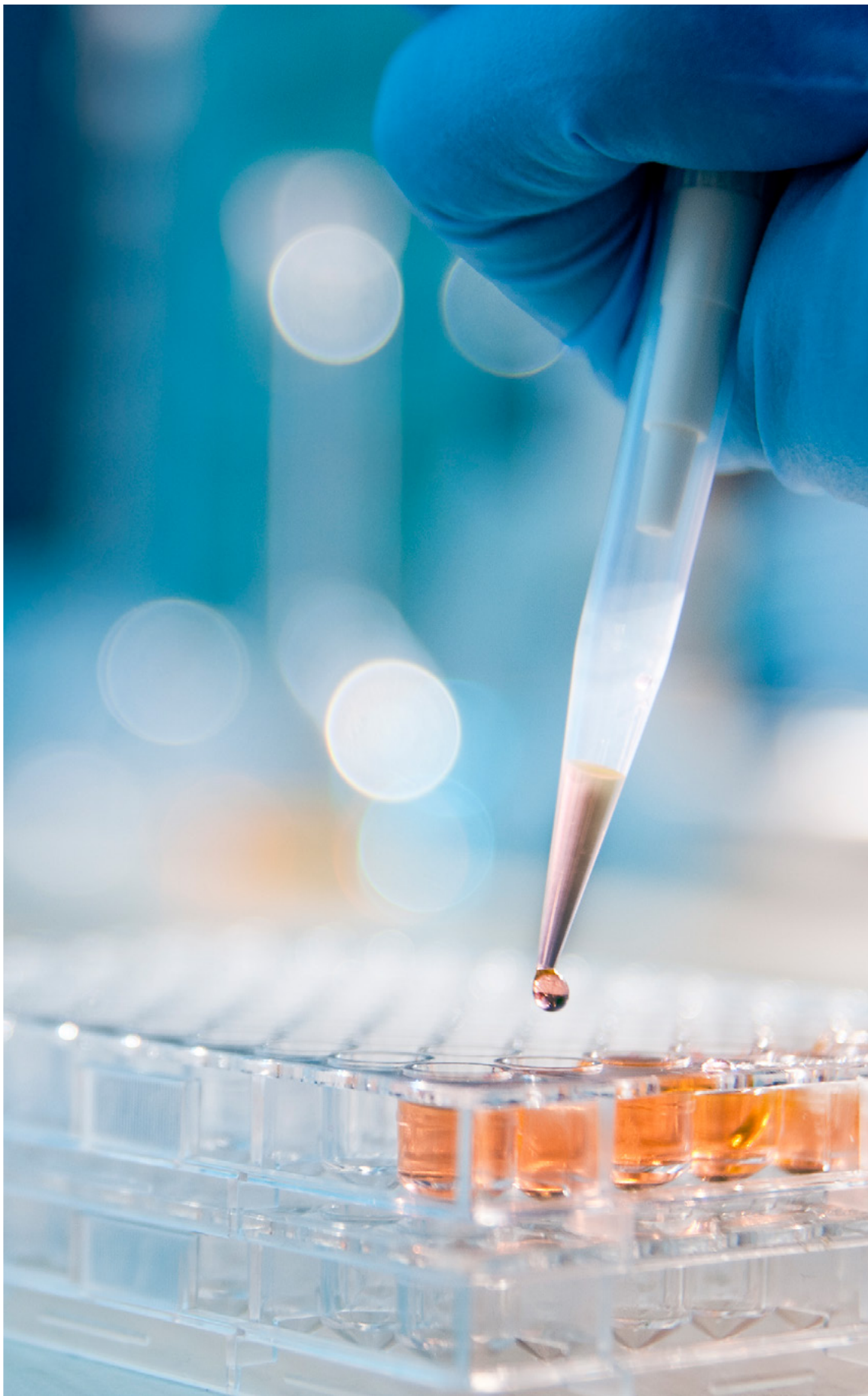
Ameaças cibernéticas no setor farmacêutico

PwC Threat Intelligence
2023



pwc

Conteúdo

Introdução 3

Cronologia dos ataques 5

Temas de incidentes 7

- Espionagem 8
- Motivações criminosas 11
- Hacktivismo 16
- Sabotagem 16

Cenário de ameaças 17

Estudos de caso 18

Considerações finais 22

Apêndice 1: Metodologia de análise 23

Apêndice 2: PwC Threat Intelligence 26

Contatos 28

Introdução

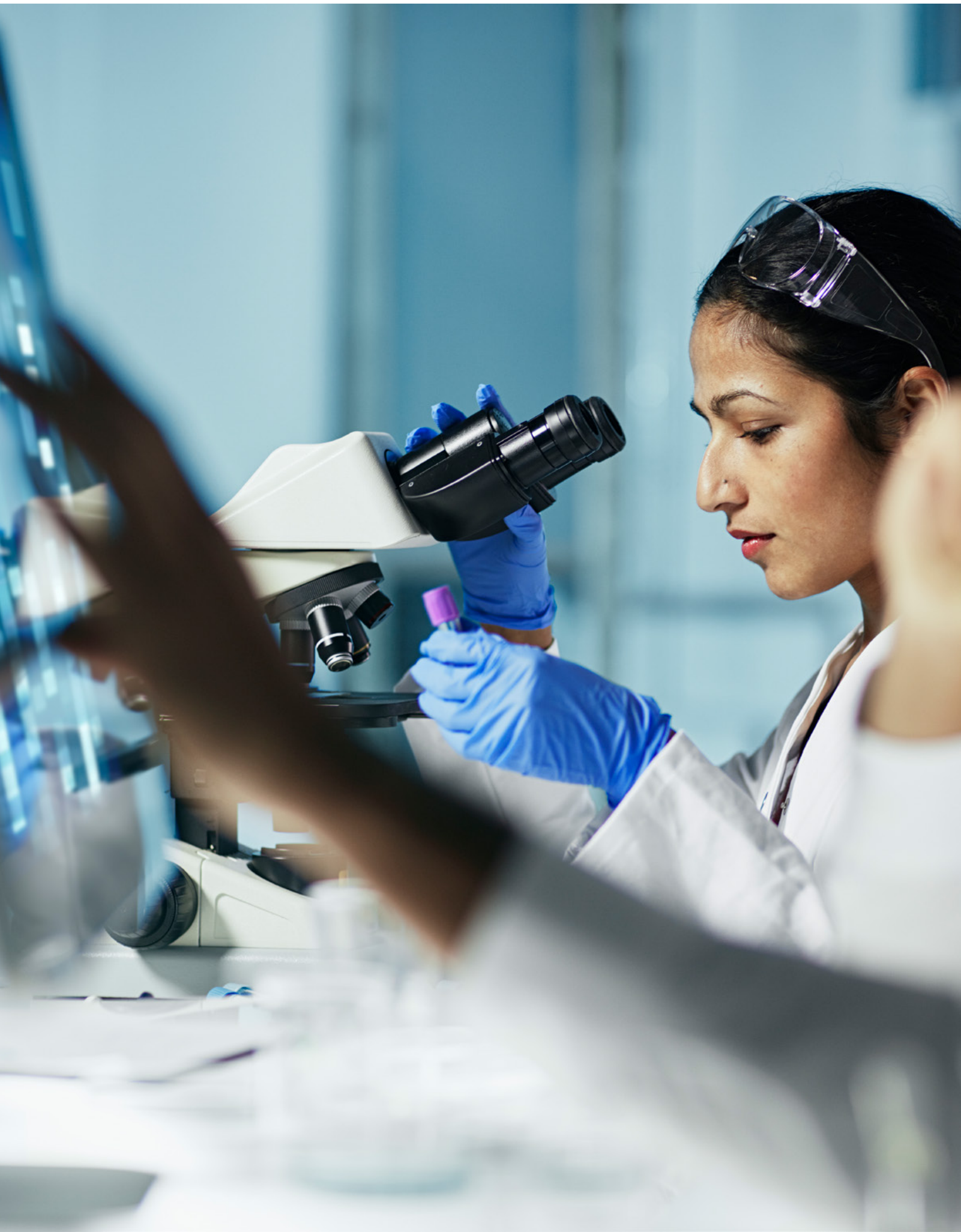
O setor farmacêutico está em constante transformação e enfrenta novos desafios cibernéticos à medida que surgem novas tecnologias e processos digitais orientados por dados e robotização. O que está em jogo são as pesquisas sobre tratamentos que salvam vidas, patentes, inovação de ponta e propriedade intelectual. Como ocorreu em outros setores, a pandemia da covid-19 impactou a área acelerando a digitização do local de trabalho. Com essa disrupção - e o importante papel do setor na resposta global à doença - vários cibercriminosos aproveitaram o momento para realizar atividades de espionagem e obter ganhos financeiros.

Por outro lado, também cresceu a dependência de fornecedores terceirizados; a adoção da digitização e de tecnologias industriais da Internet das Coisas (IoT, na sigla em inglês); e a transição para ambientes híbridos e “multinuvem”. Essa evolução gerou uma lista crescente de preocupações cibernéticas, como ataques à cadeia de suprimentos, violações de terceiros e configurações incorretas que levam a vazamentos de dados.

Ciberespiões focaram em pesquisas médicas e desenvolvimento de vacinas relacionadas à covid-19, cruzando facilmente as fronteiras de diferentes jurisdições e países. O *ransomware*, por exemplo, tornou-se mais sofisticado e, de certa forma, “mais industrializado” devido à disponibilidade de *malware* como *commodity*, surgimento de novos mercados clandestinos e a ampliação do ecossistema de contratação de cibercriminosos.

É vital que as organizações não apenas desenvolvam um ambiente seguro, mas fiquem atentas ao atual cenário de ameaças, criando meios para detectar e responder aos potenciais incidentes cibernéticos. A segurança cibernética está associada a riscos que devem ser avaliados pela alta administração, e as organizações, como resultado, devem tomar medidas para priorizá-la.

Este relatório fornece uma visão geral dos riscos mais comuns enfrentados atualmente pelo setor, bem como informações para apoiar sua empresa em estratégias de defesa baseadas em inteligência. A análise se baseia em nosso próprio conjunto de dados de inteligência sobre ataques cibernéticos realizados nos últimos anos. São conhecimentos acumulados em nossos trabalhos de resposta a incidentes em todo o mundo e extraídos de relatórios disponíveis publicamente.



Cronologia dos ataques

Os cibercriminosos que atuam no setor variam em termos de motivação e sofisticação, executando desde ataques oportunistas com *ransomware* até atos de espionagem persistentes e altamente direcionados. Em 2020, por exemplo, os agentes de ameaças focaram primeiro nas pesquisas, depois no desenvolvimento e na distribuição de vacinas, à medida que a estratégia de contenção da pandemia foi mudando. No Apêndice 1, apresentamos uma explicação detalhada sobre as categorias de agentes de ameaças por motivação.

> "As violações relacionadas à indústria farmacêutica estão em terceiro lugar em termos de custo, com um preço médio de 5 milhões de dólares…"
>
> SC Media,[1] no Relatório de Custo de Violação de Dados da IBM 2022[2]

1. SC Media, "Healthcare data breaches cost an average of $10.1M, more than any other industry", 29/7/2022. Disponível em: https://www.scmagazine.com/analysis/breach/healthcare-data-breaches-cost-an-average-of-10-1m-more-than-any-other-industry
2. IBM, "Cost of a data breach 2022", 2022. Disponível em: https://www.ibm.com/reports/data-breach

2020

A ExecuPharm, com sede nos EUA, sofreu um ataque de *ransomware* com vazamento de dados, que levou ao roubo de informações de identificação pessoal (PII, na sigla em inglês) de funcionários.

2020

A Gilead Sciences, com sede nos EUA, foi alvo do Yellow Garuda em uma campanha de *spear phishing* de executivos da companhia, que visavam ganhar acesso a informações farmacêuticas sobre a covid-19.

2020

Vários governos alertaram sobre ataques do Blue Kitsune, com uso do WellMess, contra pesquisas acadêmicas e farmacêuticas sobre a covid-19.

2020

O governo dos Estados Unidos acusou dois chineses de conduzir vários ataques, alguns deles relacionados à covid-19.

2020

Black Artemis e Black Banshee atacaram organizações envolvidas em pesquisas sobre a covid-19. Agentes de ameaças norte-coreanos elegeram alvos semelhantes com o *ransomware* Maui.

2021

O White Ursia atacou a empresa francesa Pierre Fabre com *ransomware*, impactando a maioria da produção enquanto a organização tentava conter o avanço da ameaça.

2021

O ACSC emitiu um aviso sobre ataques de *ransomware* do White Dev 70 a vários países e setores, incluindo o farmacêutico.

2021

O White Bennu usou *ransomware* em ataque contra a empresa Supernus Pharmaceuticals, nos EUA.

2022

A empresa francesa Clarins sofreu uma violação de dados causada por um agente de ameaças não divulgado, que aproveitou a vulnerabilidade do Log4j.

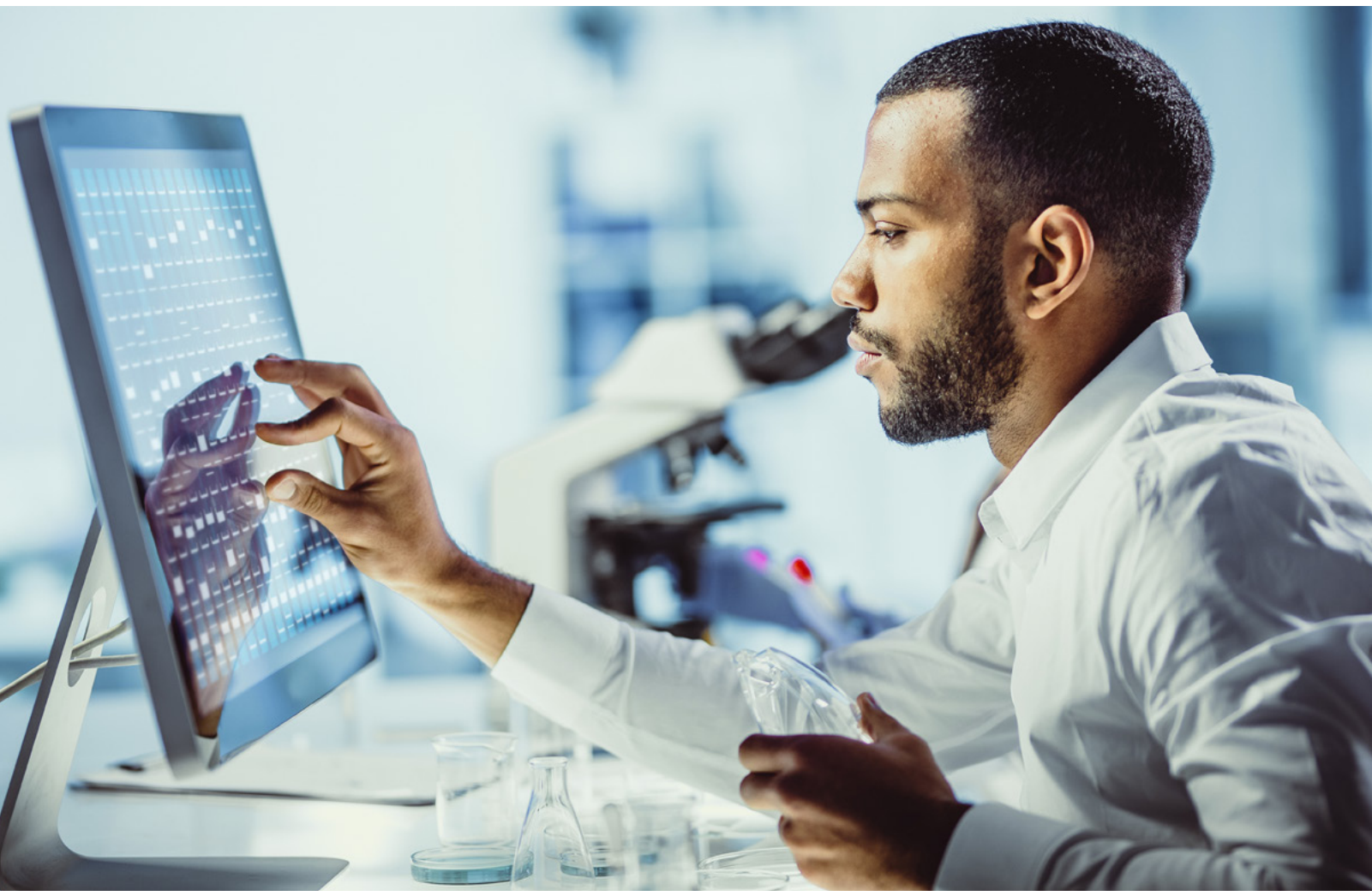
2022

O grupo Industrial Spy alegou ter roubado dados confidenciais da empresa suíça Novartis e os divulgou em seu *marketplace*.

Temas de incidentes

O setor farmacêutico é o alvo principal de espionagem e cibercriminosos com motivações financeiras. Enquanto o mundo lutava contra a crise sanitária, vários agentes de ameaças capitalizaram o medo, a incerteza e os esforços para combater o vírus por meio de campanhas de *phishing* e *malware* – ou seja, aproveitaram a forma de se comunicar dos órgãos oficiais, imitando até identidades visuais, para realizar ataques. Além disso, um dos tipos de ofensiva mais comuns foi o *ransomware*, que foi tanto utilizado por cibercriminosos convencionais quanto por APTs com origem na Coreia do Norte.

Os cibercriminosos provavelmente enxergam as organizações como alvos por causa do valor de resgate de informações pessoais dos pacientes e dados sensíveis em seus sistemas. Também identificamos casos extremos de sabotagem e hacktivismo, como o ocorrido com uma farmacêutica que relatou uma violação de dados em janeiro de 2022, causada por um agente de ameaça não divulgado que explorou a vulnerabilidade conhecida como Log4Shell (CVE-2021-44228).[3] [4]



3. Today Online, “Cosmetics company Clarins hit by data security incident, ‘may involve’ Singapore customers’ personal information”, 11/1/22. Disponível em: https://www.todayonline.com/singapore/cosmetics-company-clarins-hit-data-security-incident-may-involve-singapore-customers-personal-information-1788466

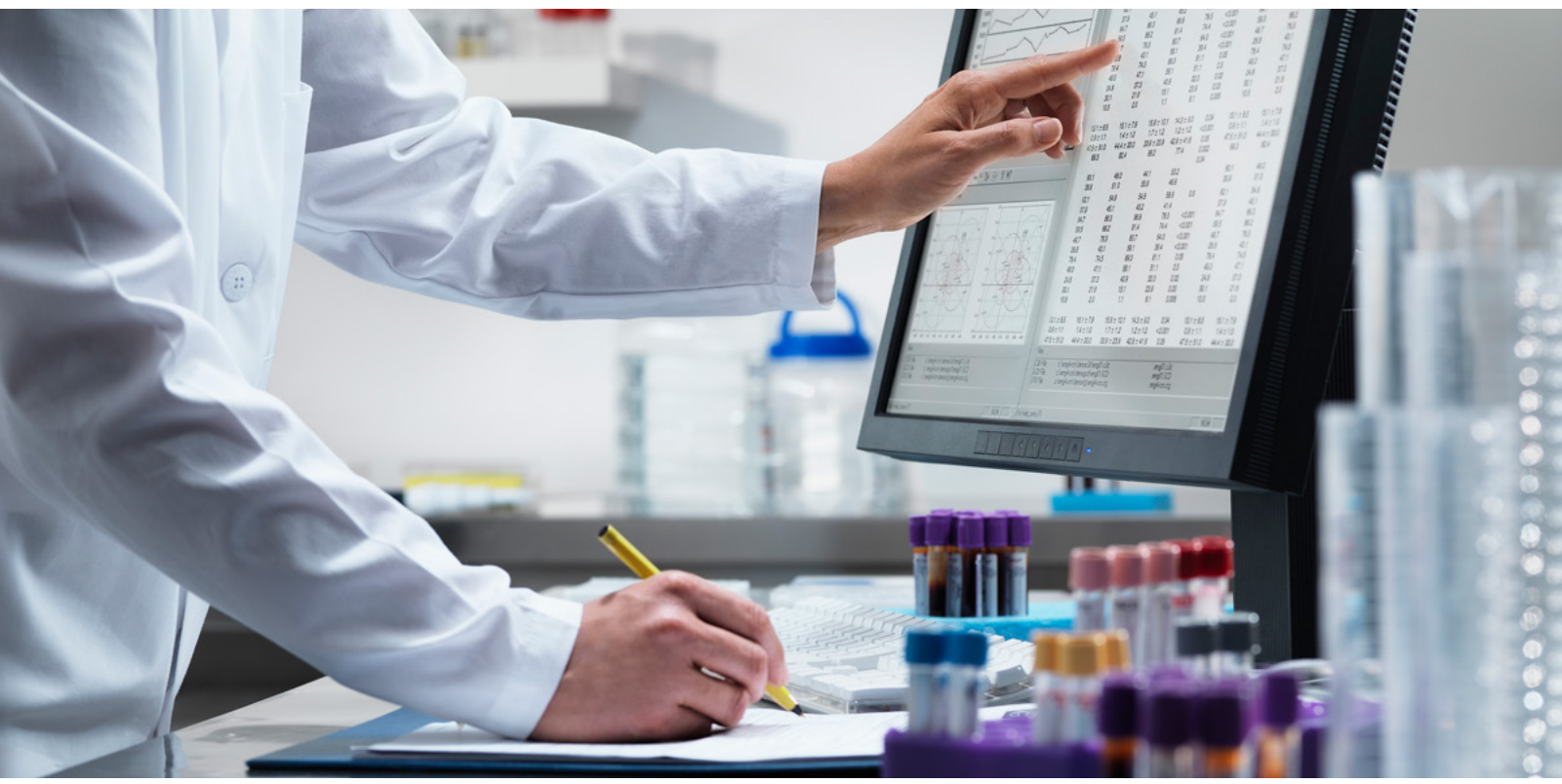
4. 4CTO-QRT-20211210-01A – Active scanning of CVE-2021-44228

Espionagem

O objetivo dos cibercriminosos é obter dados confidenciais e propriedade intelectual de pesquisas médicas por causa das vantagens econômicas que vacinas e medicamentos podem oferecer. Os ataques motivados por espionagem geralmente são causados por invasores patrocinados por nações ou por empresas concorrentes. Enquanto estas estão interessadas em coletar informações para alcançar maior vantagem competitiva, os primeiros têm escopo mais técnico, de acordo com a geopolítica e a economia de seus respectivos países ou organizações.

Como os principais componentes da indústria farmacêutica são baseados em inovação, direitos imateriais e patentes, um ataque pode resultar em perdas devastadoras que prejudicam a reputação de grandes organizações. A vacinação bem-sucedida se tornou uma das propriedades intelectuais mais valiosas para os invasores cibernéticos, com cibercriminosos na Coreia do Norte,[5] Rússia, China e Irã.[6]

Dado o aumento de ataques apoiados por nações com histórico de ataques cibernéticos, muitas organizações têm trabalhado com agências governamentais para proteger suas pesquisas. O diretor de Segurança da Informação da Johnson & Johnson, que foi alvo de cibercriminosos norte-coreanos em 2020, afirmou que a empresa estava sofrendo ataques patrocinados por nações “o tempo todo”.



5. Wall Street Journal, “North Korean Hackers Are Said to Have Targeted Companies Working on Covid-19 Vaccines”, 2/12/2020. Disponível em: https://www.wsj.com/articles/north-korean-hackers-are-said-to-have-targeted-companies-working-on-covid-19-vaccines-11606895026

6. CTO-SIB-20200724-01A – Iran injects interest in healthcare

Informações e pesquisas relacionadas à covid-19

Em maio de 2020, o agente de ameaças iraniano Yellow Garuda[7] (também conhecido como Charming Kitten) visou o e-mail de um executivo de uma empresa farmacêutica americana envolvida na pesquisa e no desenvolvimento de tratamentos e vacinas contra a covid-19. Esse ataque foi confirmado como parte do rastreamento que realizamos da infraestrutura do infrator, quando a Reuters divulgou um relatório sobre atividades de hackers do Irã.

Em julho de 2020, o Departamento de Segurança Interna (DHS) dos EUA, o Centro Nacional de Segurança Cibernética (NCSC) do Reino Unido e o Serviço de Segurança de Comunicações (CSE) do Canadá afirmaram que um criminoso russo, que identificamos como Blue Kitsune (ou APT29), mirava instituições de pesquisa acadêmica e farmacêutica para obter informações de vacinas contra a covid-19.[8] Esse grupo usou um *malware* personalizado conhecido como WellMess, que permite que o criminoso interaja com as vítimas off-line e com um nível de abstração[9] entre o agente e o software malicioso. Essas organizações continuaram sendo alvo de ataques no decorrer de 2020.

Também em julho de 2020 o governo dos EUA acusou dois cidadãos chineses de conduzir ataques de espionagem cibernética em nome do governo chinês, bem como outros ataques com motivações financeiras pessoais contra vários setores. Além dos muitos alvos relacionados à covid-19, as atividades buscavam informações sobre medicamentos em desenvolvimento, equipamentos médicos, processos e mecanismos de fabricação, resultados de testes e tratamentos. Os ataques pareciam alinhados com a iniciativa do governo chinês “China Saudável 2020” e com seu foco na fabricação de equipamentos de ponta.[10]

7. CTO-QRT-20200511-01A – Yellow Garuda and COVID-19
8. PwC, “Cyber Threats 2020: A Year in Retrospect”, 2021. Disponível em: https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
9. CTO-TIB-20200807-01A – Controlling the (Well)Mess
10. CTO-SIB-20200811-01A – You fool, ufo0lxy

O agente de ameaças norte-coreano Black Artemis (também chamado de Lazarus) é conhecido por suas atividades de ataque com várias motivações, mas, no fim de 2020, ele conduziu dois ataques contra organizações envolvidas na pesquisa da doença. Em um caso diferente, outro agente norte-coreano, que mapeamos como Black Banshee (ou Kimsuky e Velvet Chollima), foi observado registrando vários novos domínios entre o final de agosto e outubro de 2020.[11] Eles estavam configurados, na maioria dos casos, para resolver IPs comumente utilizados pelo Black Banshee, para hospedar *phishings* e infraestrutura de Comando e Controle (C2) e provavelmente foram projetados para atingir entidades envolvidas na pesquisa de vacinas contra a covid e a Organização Mundial da Saúde (OMS).[12]

Outras propriedades intelectuais e dados sensíveis

A covid-19 pode ter atraído agentes de ameaças envolvidos com espionagem, mas esses grupos sempre visaram organizações do setor farmacêutico para roubo de propriedade intelectual e informações confidenciais. O objetivo das atividades variava entre a transferência de tecnologia, espionagem econômica e o avanço das iniciativas de saúde pública dos governos patrocinadores. Como essas atividades são abrangentes por natureza, os cibercriminosos costumam atacar várias vítimas ao mesmo tempo. Por exemplo, os chineses Wicked Panda (que mapeamos como Red Zhen e Red Kelpie) realizaram ataques usando o *malware* Winnti, o que resultou em muitas vítimas no setor farmacêutico, incluindo a Bayer, sediada na Alemanha, em 2018,[13] e a Roche em 2019.[14]

11. CTO-TIB-20201007-01A – Black Banshee targets COVID-19 research
12. CTO-QRT-20201113-02A – An AppleSeed a day keeps COVID-19 away
13. Cyber Scoop, “German drug giant Bayer breached by Chinese hacking group Wicked Panda: report”, 4/4/2019. Disponível em: https://www.cyberscoop.com/bayer-breached-china-wicked-panda/
14. Reuters, “BASF, Siemens, Henkel, Roche target of cyber attacks”, 24/7/2019. Disponível em: https://www.reuters.com/article/uk-germany-cyber-idUKKCN1UJ154

Motivações criminosas

Devido a ataques oportunistas, que afetam desde informações confidenciais a sistemas críticos, agentes de ameaças com motivação financeira continuam sendo a principal preocupação para o setor farmacêutico. Eles normalmente operam com risco muito menor, recompensa maior e um *modus operandi* variável. No entanto, alguns têm demonstrado técnicas mais sofisticadas, com envio de e-mails de *spear phishing* bem elaborados, além da capacidade de persistência e de se mover lateralmente pelas redes de vítimas. Essas atividades têm um custo maior em termos de tempo, o que significa que os ataques costumam ter um volume menor.

Os operadores de *ransomware* começaram a aparecer mais em 2019, ganharam evidência durante a pandemia e, provavelmente, continuarão a dominar as discussões sobre ameaças cibernéticas nos próximos anos. Esse ecossistema também desenvolveu mercados clandestinos para facilitar a compra e venda de acessos, seja por meio de *malware*, exploração de vulnerabilidades, exposição de credenciais ou outros.

Ataques de *ransomware* e extorsão dupla

O impacto do *Ransomware-as-a-Service* (*RaaS*) cresceu desde 2019, e os agentes por trás desses ataques dependem de operações de infecção prevalentes e indiscriminadas para criptografar os sistemas das vítimas. Os operadores de *ransomware* enxergam alto valor nas organizações do setor farmacêutico por causa do impacto operacional e reputacional que um ataque teria em informações e sistemas sensíveis, ou seja, uma dupla extorsão.

Com base em nossa análise e em dados de vazamento, verificamos que eles fizeram 145 vítimas no segmento entre maio de 2020 e novembro de 2022.[15] Foram vários casos de programas afiliados de *ransomware* fazendo vítimas no setor, como parte de operações de infecção, criptografia e extorsão.

15. Nota de análise: rastreamos as estatísticas de sites de vazamento de *ransomware* para analisar quais vítimas, de quais setores e países, estão sofrendo vazamento causado por agentes de ameaças. Essas estatísticas incluem apenas as vítimas que apareceram nesses sites, e algumas podem não aparecer por vários motivos, incluindo possível pagamento de resgate e negociações em andamento. Geralmente, não temos como confirmar esses fatos, a menos que estejamos auxiliando os clientes em uma função de resposta a incidentes ou que os incidentes sejam divulgados publicamente.

Após várias respostas a incidentes, apoiadas pela equipe da PwC em 2021, identificamos e analisamos durante seis meses um agente de ameaça que mapeamos como White Veles. Ele utilizou um *malware* associado a pelo menos quatro outros operadores *RaaS* de maior perfil (ou seja, White Janus, também chamado de LockBit 2.0, White Apep, ou BlackMatter, Blue Cronus, também chamado de Conti, e White Dev 101, ou BlackCat).

As vítimas estavam associadas a diferentes setores, e avaliamos que a ferramenta de exfiltração de dados conhecida como ExMatter pode estar associada exclusivamente ao White Veles.[16] Além disso, o agente Blue Cronus continuou suas operações de infecção usando o *malware* Emotet em 2022, apesar de ter sofrido com a paralisação das operações do Conti no mesmo ano.[17]

Em uma notícia de 2021, foi relatado que o REvil, um agente de *ransomware* que mapeamos como White Ursia, atingiu o grupo farmacêutico francês Pierre Fabre, que é considerado o segundo maior do país e o segundo maior laboratório de dermocosméticos do mundo. O ataque afetou a produção enquanto a organização tentava conter a disseminação, e o preço do resgate do White Ursia dobrou de US$ 25 milhões para US$ 50 milhões.[18] Em outra ocasião, o White Bennu (Hive) atacou a empresa norte-americana Supernus Pharmaceuticals em novembro de 2021. A organização divulgou o incidente em seu site e indicou que o ataque não teve impacto significativo em seus negócios, além de alegar não ter pago o resgate.[19]

16. CTO-TIB-20220211-01A – White Veles – a prolific criminal shapeshifter
17. CTO-QRT-20220824-01A – Recent Blue Cronus (in)activity
18. Bleeping Computer, “Leading cosmetics group Pierre Fabre hit with $25 million ransomware attack”, 9/4/2021. Disponível em: https://www.bleepingcomputer.com/news/security/leading-cosmetics-group-pierre-fabre-hit-with-25-million-ransomware-attack/
19. Supernus Pharmaceuticals, “Supernus Pharmaceuticals Targeted in Ransomware Incident”, 24/11/2021. Disponível em: https://www.globenewswire.com/en/news-release/2021/11/24/2340869/19871/en/Supernus-Pharmaceuticals-Targeted-in-Ransomware-Incident.html

Em outubro de 2020, o White Samyaza (Egregor) vitimou a empresa farmacêutica indiana Dr. Reddy's, que fechou várias fábricas em resposta ao ataque cibernético, que resultou na interrupção de suas operações.[20] No início de março de 2020, a empresa norte-americana ExecuPharm sofreu um ataque de *ransomware*, com violação de dados, do grupo White Austaras (também conhecido como TA505 e Cl0P). No ataque, foram roubados dados pessoais, incluindo números de previdência social, IDs de contribuinte, números de carteira de motorista, números de passaporte, detalhes de contas bancárias, números de cartão de crédito e informações de beneficiários[21] de seguridade social.

Relatórios adicionais identificaram várias vítimas de *ransomware* no setor farmacêutico, embora os cibercriminosos não tenham sido identificados:

- Em junho de 2020, um agente de *ransomware* desconhecido atacou a Universidade da Califórnia em São Francisco (UCSF), que não divulgou detalhes ou quais sistemas foram afetados. Na época, os pesquisadores estavam trabalhando em testes e ensaios clínicos relacionados aos tratamentos contra a covid-19.[22]
- Em agosto de 2021, outro agente de *ransomware* desconhecido atacou a Surecare Specialty Pharmacy, potencialmente expondo os dados de saúde de pacientes e informações pessoais para fins de dupla extorsão.[23]

20. Business Insider, "Another Indian pharmaceutical giant reports cybersecurity breach within two weeks of ransomware hack on Dr Reddy's", 5/11/2020. Disponível em: https://www.businessinsider.in/tech/enterprise/news/lupin-reports-cybersecurity-breach-within-two-weeks-of-ransomware-hack-on-dr-reddys/articleshow/79061065.cms
21. Infosecurity Magazine, "Pharma Giant ExecuPharm Suffers Data Breach/Ransomware Combo", 29/04/2020. Disponível em: https://www.infosecurity-magazine.com/news/execupharm-suffers-data/
22. Bloomberg, "Hackers Target California University Leading Covid Research,' Bloomberg", 3/6/2020. Disponível em: https://www.bloomberg.com/news/articles/2020-06-04/hackers-target-california-university-leading-covid-19-research#xj4y7vzkg
23. Calculated HIPAA, "Ransomware Attacks Reported by Surecare Specialty Pharmacy, Blue Shield of California, and Blue Cross of California", 9/11/2021. Disponível em: https://www.calhipaa.com/ransomware-attacks-reported-by-surecare-specialty-pharmacy-blue-shield-of-california-and-blue-cross-of-california/

Outros ataques com motivações financeiras

Além do desafio persistente dos agentes de *ransomware*, outros com mais recursos e sofisticação visam o setor com objetivos financeiros. Isso inclui incidentes envolvendo agentes da Coreia do Norte que atacaram organizações desde 2021. Em julho de 2022, o governo dos EUA divulgou informações sobre um criminoso norte-coreano por trás do *ransomware* Maui e o acusou de visar serviços de saúde privada e pública desde maio de 2021.[24] Além disso, foi noticiado que o agente por trás do *ransomware* GwisinLocker tinha como alvo organizações da Coreia do Sul em agosto de 2022. Alguns pesquisadores suspeitavam que um agente norte-coreano foi responsável por esses ataques, devido ao perfil das vítimas e ao domínio do idioma coreano, bem como aos feriados públicos e ao horário comercial típico[25] do país.

O comprometimento de e-mail comercial é uma preocupação que envolve outros agentes de ameaças com motivações financeiras. Em outubro de 2020, analisamos uma campanha de *phishing* prolongada que foi vista pela primeira vez em junho de 2020. Ela envolvia o que parecia ser um anexo do Excel, mas era na realidade um arquivo HTM que hospedava uma página de *phishing* para coletar credenciais. A distribuição foi generalizada, mas as caixas de correio visadas eram de natureza financeira, assim como as iscas do conteúdo de e-mail de *phishing*.[26]

24. US Cybersecurity & Infrastructure Security Agency (CISA), “Alert (AA22-187A): North Korea State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector”, 7/7/2022. Disponível em: https://www.cisa.gov/uscert/ncas/alerts/aa22-187a

25. Bleeping Computer, “New GwisinLocker ransomware encrypts Windows and Linux ESXi servers”, 6/8/2022. Disponível em: https://www.bleepingcomputer.com/news/security/new-gwisinlocker-ransomware-encrypts-windows-and-linux-esxi-servers/

26. CTO-TIB-20201012-01A – Be right BEC, checking the invoice

Mercados ilícitos e exposição de risco

As organizações do setor farmacêutico devem estar cientes de exposições intencionais ou não, diretas ou indiretas, de seus dados. *Insiders* mal-intencionados representam uma ameaça. Por exemplo, no início de julho de 2019, uma empresa australiana que fornecia serviços de correspondência para ensaios clínicos tinha um banco de dados exposto com informações pessoais de mais de 37 mil indivíduos. Um pesquisador descobriu, alertou a empresa e, por meio de um esforço coletivo, essa exposição foi mitigada até o final de julho de 2019.[27] Não foi relatado por quanto tempo os dados ficaram vulneráveis ou se outras pessoas tiveram acesso a eles além do que foi revelado pelo pesquisador.

Mercados clandestinos também prosperam no ecossistema de cibercrime, e agentes[28] de ameaças podem explorar livremente bancos de dados expostos, atuar na compra e venda de credenciais e acessos, medicamentos, pesquisas e outros itens relacionados à indústria farmacêutica. Em um estudo que realizamos em 2021, descobrimos que os *marketplaces* de cibercriminosos mais proeminentes da época (ou seja, RaidForums, XSS e Exploit) negociavam violações de dados, acesso a redes comprometidas e tinham listas postadas que estavam associadas a vítimas de 80 países e 27 setores. Embora o setor tenha aparecido pouco, a proeminência desses mercados é uma preocupação importante, já que indica um interesse contínuo desses cibercriminosos.

Em junho de 2022, foi relatado que o agente de extorsão Industrial Spy comprometeu a empresa suíça Novartis. Ele é conhecido por roubar dados confidenciais e, em seguida, extorquir as vítimas com ameaças de venda. O criminoso alegou ter obtido dados relacionados ao trabalho da Novartis sobre "tecnologia e testes de medicamentos baseados em RNA e DNA" e faturado com a venda deles US$ 500 mil em bitcoin, mas a vítima refutou essas alegações.[29]

27. UpGuard, "Clinical Trials: How Personal Information for Thousands of Australians was Exposed", 7/8/2019. Disponível em: https://www.upguard.com/breaches/data-leak-neoclinical-australia-new-zealand

28. CTO-SIB-20211209-01A – A unique peek at 13 weeks of leaks – Part 1

29. Bleeping Computer, "Novartis says no sensitive data was compromised in cyberattack", 3/6/2022. Disponível em: https://www.bleepingcomputer.com/news/security/novartis-says-no-sensitive-data-was-compromised-in-cyberattack/

Hacktivismo

Embora não tenhamos observado uma tendência nos ataques hacktivistas ao setor farmacêutico nos últimos anos, as organizações devem estar cientes de possíveis motivações por trás desses agentes. As instalações de pesquisa médica e as empresas farmacêuticas periodicamente podem chamar a atenção de cibercriminosos que não acreditam na linha ou no método de pesquisa adotado por elas – por exemplo, o uso de testes em animais. O foco dos ataques pode ser o roubo de contas de mídias sociais, *defacement* de sites, ataques de negação de serviço (DoS) ou outras atividades perturbadoras, como obtenção e vazamento de e-mails comerciais. Em um caso descrito por um pesquisador de tecnologia e segurança cibernética em janeiro de 2019, um agente de ameaça executou um ataque distribuído (DDoS) contra uma organização de saúde devido a suas práticas de preços.[30]

Sabotagem

Essa categoria é motivada por ideologias políticas, econômicas ou religiosas, além de executar tarefas em ataques apoiados por nações. Como muitas empresas farmacêuticas usam tecnologia anterior à internet, elas podem permanecer na mira dos ataques, já que seus equipamentos foram originalmente projetados como sistemas isolados, e não construídos para enfrentar agentes altamente motivados e com infraestrutura robusta. Para as empresas farmacêuticas, qualquer ataque dessa natureza pode resultar em perda de produtividade e disponibilidade de dispositivos físicos e operações.[31]

30. Splunk, “Revenge Hacktivism: Is Your Company Vulnerable?”, 17/01/2019. Disponível em: https://www.splunk.com/en_us/blog/security/revenge-hacktivism-is-your-company-vulnerable.html

31. SCADAfence, “Cyber Threats To The Pharmaceutical Industry: Johnson & Johnson Experiencing OT and IT Attacks From Nation State Attackers”, 1/2020. Disponível em: https://blog.scadafence.com/pharmaceuticals-like-johnson-johnson-are-experiencing-daily-cyber-attacks-from-nation-state-attackers

Cenário de ameaças

A PwC observou que os cibercriminosos variam de acordo com regiões, tipos de organização, motivações e intenções. Este levantamento abaixo pode ser usado para ajudar a identificar e priorizar a cobertura da atuação de agentes que direcionam seu foco a organizações específicas do setor farmacêutico.

	Agente de ameaça	Nomes	País de origem
Espionagem	Red Kelpie	APT41, Wicked Panda	China
	Red Scylla	Aquatic Panda	China
	Red Zhen	APT22, Wicked Panda	China
	Yellow Nix	Static Kitten,MuddyWater	Irã
	Yellow Garuda	APT42, Charming Kitten	Irã
	Black Artemis	Lazarus Group	Coreia do Norte
	Black Banshee	Kimsuky	Coreia do Norte
	Black Echidna	Sandworm, Voodoo Bear	Rússia
	Black Kitsune	APT29, Cozy Bear	Rússia
Cunho criminal	Blue Cronus	Conti, Emotet, TrickBot, Diavol	Rússia
	Industrial Spy	N/A	TBD
	White Bennu	Hive	TBD
	White Dev 70	Avaddon	TBD
	White Samyaza	Egregor	TBD
	White Ursia	REvil, Sodinokibi	TBD
	White Veles	DEV-0504	TBD
	White Austaras	TA505, Cl0P	TBD

Estudos de caso

Os estudos de caso abaixo fornecem uma visão geral dos ataques que ocorreram nos últimos anos e ilustram as motivações dos cibercriminosos que têm como alvo o setor farmacêutico.

Motivação do agente de ameaça	Alvo	Ano
Cunho criminoso/financeiro	Indústria farmacêutica	2021

Sumário executivo

O agente de *ransomware* White Bennu (ou Hive) atacou a empresa americana Supernus Pharmaceuticals em novembro de 2021. O grupo alegou ter roubado 1,5 TB de dados referentes a mais de 1,2 milhão de arquivos e anunciou o vazamento em seu site.

Modus operandi

White Bennu é um agente de *ransomware* que realiza ataques de extorsão dupla, nos quais compromete uma vítima, rouba seus dados e ameaça vazá-los caso não receba o resgate. O grupo White Bennu opera o *ransomware* Hive como um modelo *RaaS*, em que vários afiliados usam o *ransomware* em seus ataques. Esses afiliados empregam vários métodos para obter acesso às redes das vítimas, principalmente os servidores RDP expostos e *spear phishing*. Depois que o acesso é concluído, podemos observar que as afiliadas distribuem o Cobalt Strike e, em alguns casos, a ferramenta de administração remota ConnectWise, para explorar ainda mais as máquinas e mover-se lateralmente pela rede da vítima. Uma vez que os agentes tenham acesso suficiente, eles tentarão exfiltrar os dados usando vários serviços disponíveis publicamente, como o provedor de armazenamento de arquivos AnonFiles.

Impacto

A empresa divulgou o incidente em seu site, informando que o ataque não teve impacto significativo em seus negócios e que ela não pagou o resgate. No entanto, o White Bennu afirmou que a vítima havia tentado negociações. A empresa disse que conseguiu recuperar os arquivos afetados e informou que o incidente permitiu a ela remediar o problema e melhorar sua segurança.

Mais informações

Supernus Pharmaceuticals Targeted in Ransomware Incident
https://www.globenewswire.com/news-release/2021/11/24/2340869/19871/en/Supernus-Pharmaceuticals-Targeted-in-Ransomware-Incident.html

Indicadores de Comprometimento (IoCs) associados ao Ransomware HIVE
https://www.ic3.gov/Media/News/2021/210825.pdf

CTO-TIB-20220208-01A – A Hive of scum and villainy

Motivação do agente de ameaça	Alvo	Ano
Espionagem	Indústria farmacêutica	2019

Sumário executivo

A empresa farmacêutica Bayer AG, a maior da Alemanha e a principal empresa de suprimentos agrícolas do mundo, foi alvo do Wicked Panda (que mapeamos como Red Zhen e Red Kelpie) no início de 2018. Depois de descobrir a violação, ela avaliou que não havia evidências de roubo ou vazamento de dados confidenciais. Em julho de 2019, outra empresa farmacêutica, a Roche, de origem suíça, foi atingida pelo mesmo *malware*.

Modus operandi

O Wicked Panda se infiltrou na rede, plantou o *backdoor* do Winnti, permitindo o acesso remoto ao sistema da Bayer AG, e, em seguida, buscou novas explorações. A Bayer encontrou o *malware* em sua rede em 2018, mas secretamente o monitorou e analisou até o final de março de 2019, com a intenção de rastrear os dados extraviados pelo *malware* de volta à fonte, antes de remover a ameaça do sistema. O *malware* era comumente usado por cibercriminosos chineses, que tinham como motivação provável a espionagem industrial de vários setores priorizados para o desenvolvimento econômico do país, bem como a espionagem de pessoas politicamente relevantes.

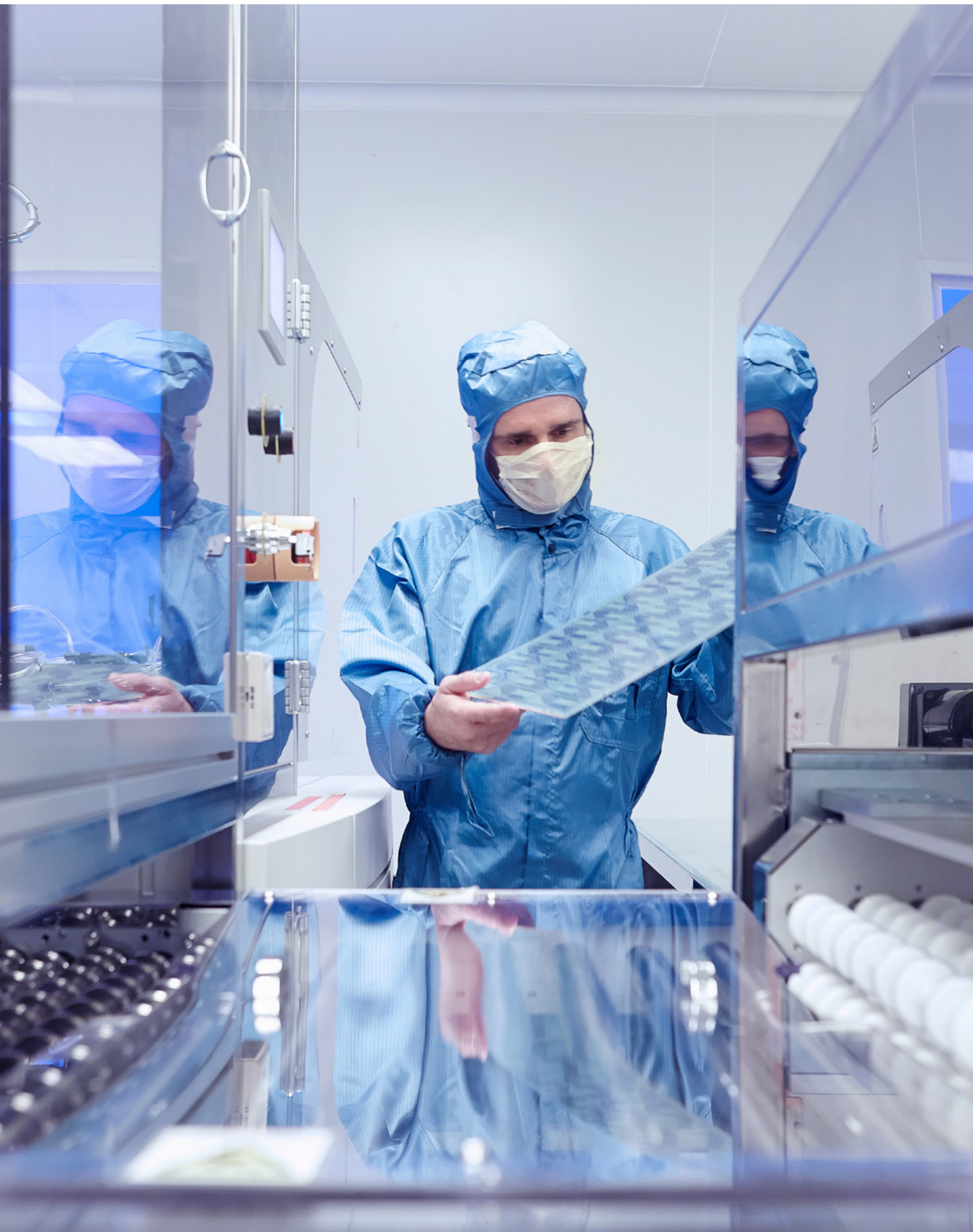
Impacto

Na época, um porta-voz da Bayer disse que não havia evidências de roubo ou vazamento de dados, mas acrescentou que o dano geral ainda estava sendo avaliado e que os promotores públicos alemães iniciaram uma investigação. Esse incidente foi parte de uma campanha de espionagem muito maior, que envolveu outras organizações, como a empresa farmacêutica suíça Roche, o grupo hoteleiro Marriott, a companhia aérea Lion Air, o conglomerado Sumitomo e o grupo químico Shin-Etsu. A longa campanha tornou-se pública depois que um relatório foi publicado pelas emissoras alemãs BR e NDR, segundo as quais os hackers vinham espionando empresas em todo o mundo há anos. As demais vítimas comentaram não ter conhecimento de um possível vazamento de dados.

Mais informações

Roche, like Bayer, was hit in Winnti cyberattack
https://www.fiercepharma.com/manufacturing/roche-like-bayer-was-targeted-winnti-cyber-attack

Attacking the Heart of the German Industry
https://interaktiv.br.de/winnti/english



Considerações finais

Vários agentes de ameaças visaram o setor farmacêutico nos últimos anos com diferentes métodos, motivações e alvos em diferentes países. Com base nas tendências, estudos de casos e nossa própria análise, identificamos que cibercriminosos envolvidos com espionagem aumentaram seu foco nesse setor, especialmente após o início da pandemia de covid-19. Embora possam ter objetivos diferentes, os cibercriminosos enxergam vantagens econômicas muito atraentes nessas empresas.

Com o avanço da crise sanitária, o setor passou a ser alvo de uma pressão crescente e com alta repercussão na mídia. Cibercriminosos voltaram sua atenção para empresas farmacêuticas, aproveitando ataques oportunistas para roubar dados confidenciais e propriedade intelectual. Enquanto isso, agentes envolvidos com espionagem intensificaram suas campanhas, visando à obtenção de informações privilegiadas sobre pesquisa e desenvolvimento de vacinas.

Saber quais agentes de ameaças são relevantes para um determinado setor é um passo importante para direcionar estrategicamente o investimento em controles de defesa apropriados. Entender como as ameaças caminham pela infraestrutura de sua organização pode ajudar a identificar os gaps existentes em seus controles de segurança.

Apêndice 1: Metodologia de análise

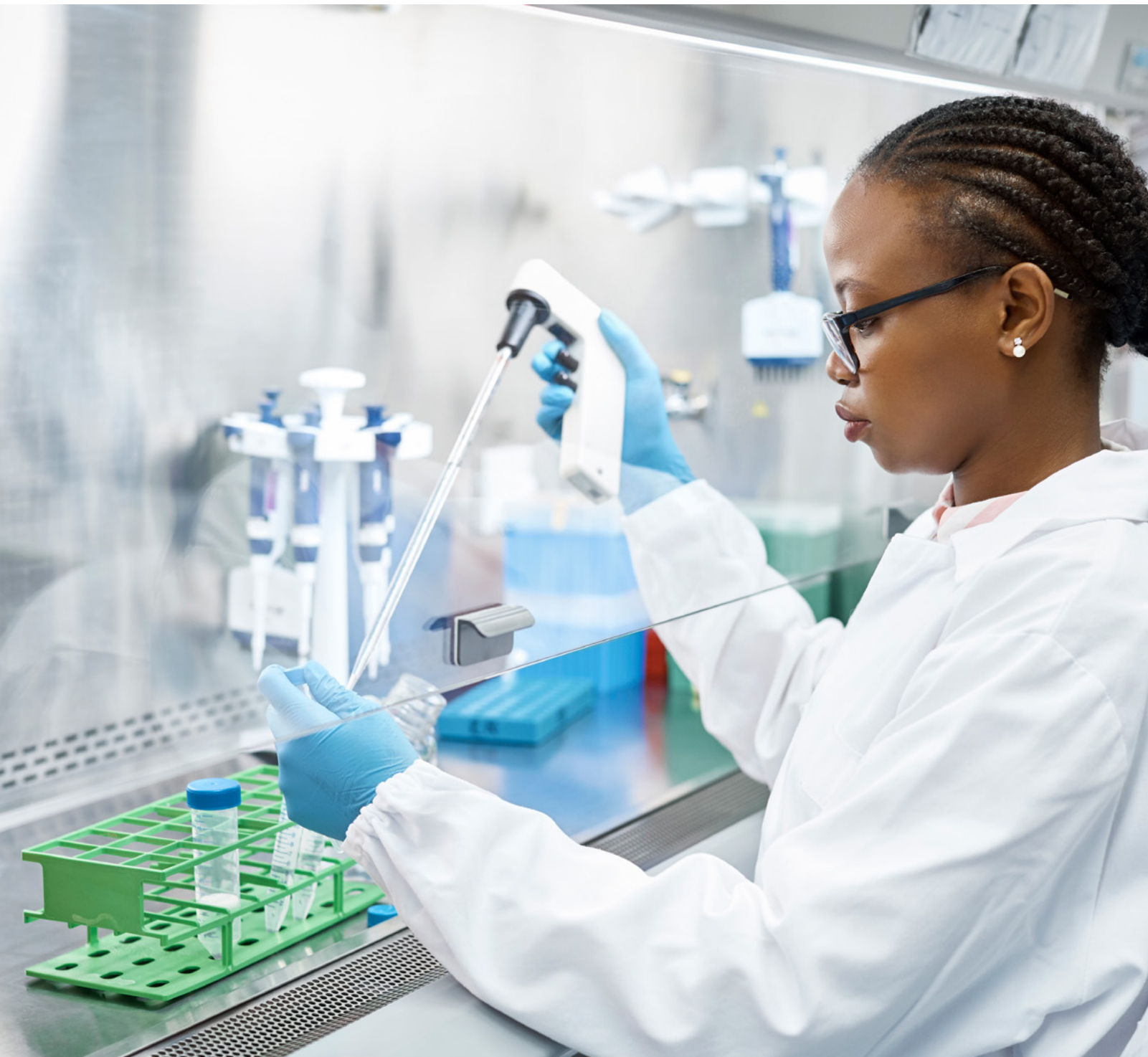
Embora possam compartilhar objetivos, os ataques de agentes de ameaças diferentes nem sempre compartilham a mesma motivação. Examinar o que motiva um ataque pode permitir a identificação da categoria do invasor.

A PwC divide o cenário de ameaças de acordo com a motivação dos ataques cibernéticos. Para cada uma, são descritas ferramentas, técnicas e procedimentos comuns. As divisões são:

Motivação	Descrição
Espionagem (por informação)	Os agentes de ameaças envolvidos em espionagem (chamados de “ameaças persistentes avançadas” – APTs na sigla em inglês) geralmente procuram roubar informações que fornecerão uma vantagem econômica ou política a seu patrocinador. Os ataques motivados por espionagem geralmente se originam de concorrentes do setor ou de agentes de ameaças patrocinados por nações. Muitas vezes, o patrocinador é uma nação, e a atividade de espionagem alinhada aos objetivos dessa nação se refletirá na geopolítica e nos eventos do mundo real. Normalmente, as informações buscadas por espiões são encontradas apenas em organizações específicas. Isso significa que eles visam repetidamente a mesma organização e seus fornecedores até que concluam a missão.

Motivação	Descrição
Crime (por dinheiro)	Os cibercriminosos cibernéticos procuram um alvo de maneira indiscriminada, pois simplesmente buscam monetizar as atividades. A gama de sofisticação dos cibercriminosos cibernéticos é vasta e apresenta um conjunto muito diferente de ferramentas, técnicas e procedimentos. O crime cibernético inclui tanto esquemas diretos de saque, que levam a um ganho financeiro imediato – por exemplo, a violação de e-mails comerciais, sequestro de caixa eletrônico ou roubo de carteiras de criptomoedas – como atividades que buscam monetizar dados roubados – coleta de detalhes de cartões de pagamento ou outras informações pessoais. Muitos cibercriminososs são meros consumidores de dados roubados por agentes mais sofisticados. Esses dados são normalmente usados para cometer fraude ou roubo de identidade. O *ransomware* tornou-se motivo de preocupação especialmente prevalente, afetando grandes corporações do setor privado até instituições de caridade e governos locais.
Hacktivismo (pela causa)	Hacktivistas conduzem ataques para aumentar a visibilidade de seu perfil público e a conscientização sobre sua causa. Isso geralmente é feito por meio da interrupção de serviços, como ataques de negação de serviço (DoS) e descaracterização de sites. Em muitos casos, esses ataques são aleatórios. Os hacktivistas se importam pouco com a forma dos ataques ou quem é afetado, desde que sua mensagem seja promovida. Em alguns casos, no entanto, as ações atribuídas a uma organização ou um indivíduo, ou o apoio dado a um tema, tornam essa organização ou indivíduo alvo de ataque. Assim como a espionagem, os ataques de hacktivistas costumam ser influenciados por eventos do mundo real. Isso significa que o risco desses ataques está sujeito a mudanças.

Motivação	Descrição
Sabotagem (pelo impacto)	Sabotadores procuram danificar, destruir ou subverter a integridade de dados e sistemas. Os ataques maliciosos nem sempre são deliberados e têm sido usados para mascarar outras atividades maliciosas. As operações de sabotagem projetadas para desviar a atenção podem também resultar em danos colaterais significativos. Entre os exemplos de ataques estão o apagamento de discos rígidos, provocando o mau funcionamento dos sistemas de supervisão e aquisição de dados (SCADA, na sigla em inglês) ou alterando dados comerciais. Assim como os ataques de espionagem, os ataques de sabotadores tendem a ser influenciados por eventos do mundo real. Dependendo de determinados fatos ou questões políticas, o risco de ataques aumenta conforme a região onde a empresa atua e as ações que ela adota.



Apêndice 2: PwC Threat Intelligence

Quem somos

A PwC é reconhecida mundialmente como líder em segurança cibernética, uma firma capaz de atuar globalmente e apresentar soluções para os desafios de segurança e risco que seus clientes enfrentam. Nossos serviços de assessoria e estratégia em segurança voltados para o conselho se apoiam na experiência e no conhecimento que adquirimos com nossos serviços especializados em defesa cibernética, como Defesa Cibernética Gerenciada, *Red Teaming*, resposta a incidentes e inteligência de ameaças.

Nossa equipe de inteligência de ameaças é especializada em fornecer serviços que ajudam os clientes a resistir, detectar e responder a ataques cibernéticos avançados. Isso inclui eventos de crise, como violações de dados, espionagem econômica e invasões direcionadas, como aquelas chamadas de ameaças persistentes avançadas (APTs).

A capacidade de combinar profundo conhecimento técnico com pensamento estratégico são um dos nossos diferenciais, como também nossas pesquisas, conduzidas por especialistas com experiência principalmente em órgãos governamentais, círculos militares e serviços de segurança – o que nos dá uma perspectiva única e uma vasta gama de contatos. Tudo isso, aliado à inteligência em segurança, conhecimento técnico e compreensão do risco cibernético, ajuda nossos clientes a obter a clareza necessária para se adaptarem com confiança a um cenário de novos desafios e oportunidades.

Nossa pesquisa de inteligência de ameaças apoia todos os nossos serviços de segurança e é usada por organizações dos setores público e privado em todo o mundo para proteger, conhecer o entorno de atuação e apoiar estratégias.

Assinatura de inteligência contra ameaças cibernéticas

Acesso aos *feeds* de indicadores sobre ataques direcionados da PwC, assinaturas de rede e *endpoint* e relatórios táticos e estratégicos.

Investigações e avaliações direcionadas

Acesso direto à equipe de pesquisa de ameaças da PwC para tarefas relacionadas a consultas pontuais ou de longo prazo – tanto pesquisas táticas como estratégicas sobre amostras maliciosas, agentes de ameaças ou suporte em análises.

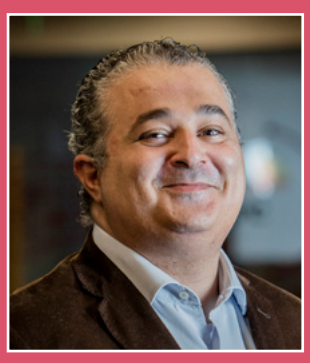
Monitoramento de inteligência de ameaças cibernéticas

Pesquisa contínua, sob medida e focada, em complemento aos nossos serviços de assinatura.

Consultoria e assessoria

Serviços de consultoria para ajudar as organizações a definir requisitos, além de consumir, aplicar e produzir inteligência de ameaças da maneira mais adequada à sua realidade.

Contatos



Eduardo Batista
Sócio e líder de *Cybersecurity* da PwC Brasil
eduardo.batista@pwc.com

Rafael Cortes
Sócio de *Cybersecurity* da PwC Brasil
cortes.rafael@pwc.com

Bruno Porto
Sócio e líder da indústria de Saúde
da PwC Brasil
bruno.porto@pwc.com

pwc

www.pwc.com.br

PwC Brasil @PwCBrasil PwC Brasil @PwCBrasil PwC Brasil @PwCBrasil