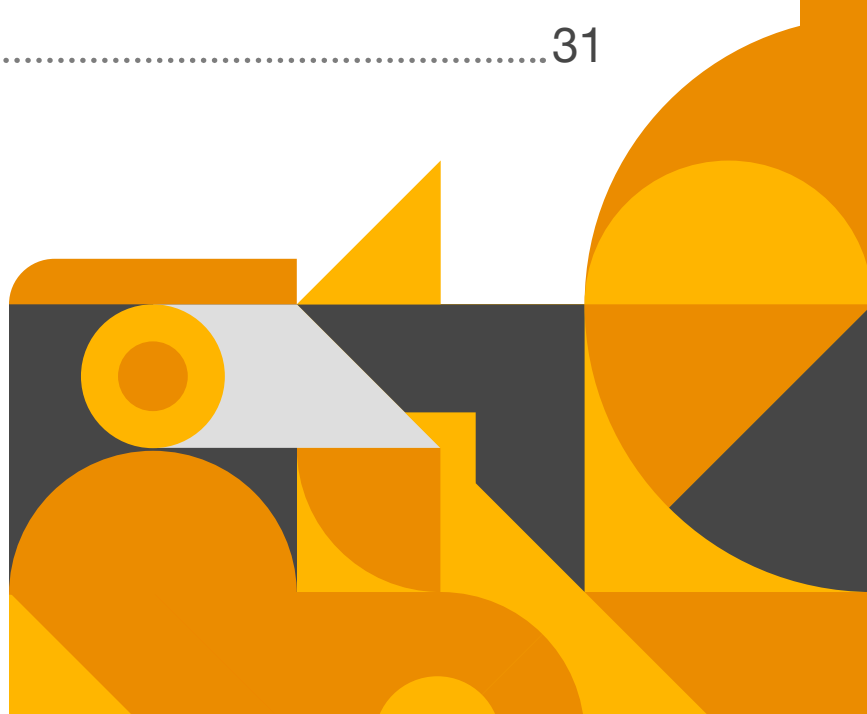
Ameaças cibernéticas ao setor da manufatura

PwC Threat Intelligence
2024

pwc

Conteúdo



Introdução

O setor de manufatura tem enfrentado um número crescente de ameaças cibernéticas cada vez mais sofisticadas causadas, majoritariamente, por atores de *ransomware*, à medida que as empresas continuam a integrar seus ambientes de tecnologia operacional (OT, na sigla em inglês), historicamente isolados, a sistemas cada vez mais conectados. Este setor dá suporte a um amplo conjunto de outras indústrias, e incidentes que envolvem organizações do setor têm efeitos que se desdobram a outros, o que aprofunda os desafios das cadeias de suprimento em todo o mundo desde 2020.

Vários setores industriais e de mercado interdependentes, como a indústria automotiva, estão experimentando os efeitos cascata de ataques de *ransomware* a terceiros (por exemplo, a seus fornecedores), que muitas vezes podem resultar em interrupções operacionais, parciais ou totais. Esses ataques cibernéticos variam em sofisticação, motivação e impacto.

Os atores de ameaça de *ransomware* têm se aproveitado de ambientes com segurança com baixa maturidade, criando operações de infecção generalizada e ataques oportunistas, que tentam extorquir as vítimas com sequestro dos ambientes de tecnologia e vazamentos de dados. Os criminosos roubam credenciais e as comercializam, juntamente com outras informações sensíveis, em mercados ilícitos.

Atores de ameaça motivados por espionagem miram empresas de manufatura para comprometer suas cadeias de suprimento, sabotar e roubar propriedade intelectual. Por causa das interseções significativas entre a manufatura e outros setores, como construção civil, semicondutores, aeroespacial, defesa e telecomunicações, o comprometimento de uma empresa do ramo manufatureiro pode ter consequências significativas para a infraestrutura crítica e defesa de um país.

Há também *insiders* maliciosos e atores motivados por sabotagem ou hacktivismo – como aqueles por trás do ressurgimento dos ataques DDoS (negação distribuída de serviço), vistos em todo o mundo – que seguem como uma preocupação significativa para o setor. Certamente, esses criminosos estão cientes de como interrupções operacionais e violações de alto perfil podem afetar a reputação de suas vítimas do ramo manufatureiro, assim como seus resultados.

É vital que as organizações não apenas desenvolvam um ambiente seguro, mas se mantenham informadas sobre o atual cenário de ameaças e desenvolvam meios para detectar e responder a incidentes cibernéticos rapidamente, de modo que qualquer impacto possa ser minimizado. É da Alta Administração a responsabilidade sobre o risco da cibersegurança, e as empresas devem tomar medidas ativas para priorizá-la como resultado.

Este relatório fornece uma visão geral das ameaças cibernéticas mais comuns atualmente enfrentadas pelo setor da manufatura. Buscamos conscientizar e esclarecer as motivações por trás desses ataques, além de apoiar você em suas estratégias de defesa. A análise é orientada por nossos próprios dados de inteligência em ataques cibernéticos e seus alvos, a partir do registro de uma variedade de atores de ameaça – inteligência que é obtida por meio de respostas a incidentes em todo o mundo e de relatórios disponíveis publicamente sobre ataques ao setor.

Cronologia dos ataques

Os atores de ameaça que miram o setor de manufatura variam em suas motivações, assim como em sofisticação – desde ataques oportunistas em processo de aprimoramento contínuo de suas operações, por meio de modelos baseados em serviços (por exemplo, *ransomware-as-a-Service* ou RaaS), até atores patrocinados por governos, altamente persistentes e com alvos previamente determinados, que visam obter informações de empresas específicas. O primeiro tipo tem recebido atenção significativa por parte da indústria e da mídia, onde há mais exemplos de ataques de *ransomware* em 2022 e no primeiro trimestre de 2023. No entanto, os atores motivados por espionagem continuam a ser uma importante preocupação.

Uma explicação detalhada sobre como categorizamos os atores de ameaça por motivação está localizada no Apêndice 1 deste relatório.

A estrutura de Threat Intelligence da PwC tem analisado dados de sites de vazamento de *ransomware* desde 2019 e, daquele momento até março de 2023, a manufatura tem liderado a lista dos setores mais impactados. Ao longo de 2022, especificamente, esse setor reuniu 15% de todas as vítimas de sites de vazamentos e, quando somado à construção civil, esse porcentual sobe para 25%.

Janeiro de 2022

A KP Snacks, de propriedade alemã, foi vítima de um ataque de *ransomware* que interrompeu temporariamente a produção, o processamento e envio de pedidos. A empresa estimou inicialmente que os desafios persistiram por dois meses.

Fevereiro de 2022

O White Janus (também conhecido como LockBit) realizou um ataque de *ransomware* contra a subsidiária americana da Bridgestone Corp., desconectando suas instalações de produção e recauchutagem nas Américas Latina e do Norte da rede para remediação.

Fevereiro de 2022

Um ataque do *ransomware* Blue Cronus (também conhecido como Conti) na Kojima Industries, fabricante de componentes plásticos para empresas do setor automotivo, forçou a Toyota Motors a suspender linhas de produção em 14 fábricas no Japão.

Março de 2022

O Blue Cronus realizou um ataque de *ransomware* contra a Nordex, fabricante alemã de turbinas eólicas, forçando a empresa a desligar os sistemas de TI para remediação, embora as operações não tenham sido afetadas.

Março a junho de 2022

O ator de ameaça baseado na China Red Ladon (também conhecido como TA423) conduziu uma campanha de espionagem cibernética contra entidades do governo e da mídia australiana, bem como contra grandes fabricantes da indústria pesada global que fazem a manutenção de frotas de turbinas eólicas no Mar da China Meridional.

Maio de 2022

AGCO, fabricante e distribuidora global de equipamentos agrícolas, anunciou que foi vítima de um ataque do *ransomware* Blue Cronus (também conhecido como BlackBasta), que afetou algumas de suas instalações industriais.

Julho a outubro de 2022

A empresa de manufatura alemã Semikron foi vítima de um ataque do *ransomware* White Dev 136 (também conhecido como LV), o que impactou seus sistemas de TI e parou temporariamente a maior parte de sua operação. Ela foi forçada a reconstruir seus sistemas de comunicação e TI, e suas linhas de produção não foram retomadas até outubro de 2022.

Fevereiro de 2023

A empresa de semicondutores MKS Instruments sofreu um ataque de *ransomware* que a impediu de processar ou enviar pedidos. Segundo a companhia, isso lhe custará uma perda de receita de mais de US$ 200 milhões.

Março de 2023

Até o final de 2022, atores de ameaça de *ransomware* vazaram dados de 365 organizações no setor da manufatura, tornando-o o mais impactado do ano, representando 15% de todas as vítimas.

No primeiro trimestre de 2023, essa tendência continuou com a manufatura representando 14% (116 organizações) de todas as vítimas desses sites – quase o dobro em relação ao segundo setor, que é o de serviços profissionais (8%, ou 68 organizações).

Temas de incidentes

Com base nos últimos incidentes e nas tendências do setor, avaliamos que a manufatura tem sido impactada principalmente por atores com motivações financeiras. No entanto, outros tipos de criminosos e ataques cibernéticos preocupam o setor, especialmente com incidentes relacionados à espionagem e sabotagem. Sistemas legados estão sendo cada vez mais atualizados e integrados nas operações de manufatura, as quais também estão mais interconectadas do que nunca com operações de outros segmentos e indústrias.

Embora ataques cibernéticos direcionados a *operational technology* (OT, na sigla em inglês) e sistemas de controle industrial (ICS)[1] possam comprometer operações e segurança, criminosos que visam dados sensíveis das redes corporativas do setor podem causar consequências graves às vítimas, como a perda de informações proprietárias e pessoalmente identificáveis (PII) de funcionários e clientes, além de credenciais e dados de acesso que eles podem usar para ataques futuros. Além disso, em 2022, a IBM descobriu que 61% dos incidentes que impactaram empresas conectadas a OT ocorreram no setor de manufatura.[2] Já em um exemplo de maio de 2023, a fabricante global de eletrônicos Lacroix foi vítima de um ataque que resultou no desligamento das operações de três fábricas na França, Alemanha e Tunísia por uma semana.[3]

Motivações criminosas

Modelos de crimes cibernéticos baseados em serviços, como *Ransomware-as-a-Service* (RaaS) e *Access-as-a-Service* (AaaS), facilitam a monetização das atividades ilícitas dos criminosos. Esses ataques são disruptivos e custosos, e mesmo que nem sempre impactem operações específicas de OT ou manufatura, ainda podem causar danos à reputação e outros prejuízos a uma indústria já com muitos problemas. Ainda que os incidentes relacionados a *ransomware* sejam uma ameaça significativa, também identificamos casos em que criminosos roubaram credenciais e outras informações sensíveis para extorsão de dados ou para vender a clientes de mercados clandestinos.

1. CTO-SIB-20230105-01A – *The OT threat landscape*
2. *"X-Force Threat Intelligence Index 2022,"* IBM, https://www.ibm.com/downloads/cas/ADLMYLAZ (fevereiro de 2023)
3. *"Lacroix Shuts Three Factories For a Week After Cyber-Attack,"* Infosecurity Magazine, https://www.infosecurity- magazine.com/news/lacroix-shuts-three-factories-week/ (16 de maio de 2023)

Ransomware

Ao longo de 2022, os sites de vazamento de *ransomware* postaram vítimas do ramo de manufatura mais do que de qualquer outro setor ou indústria – elas representam 15% do total que rastreamos no período. Essa tendência se manteve até março de 2023. 14% de todas as vítimas eram do segmento de manufatura no primeiro trimestre do ano.[4] O setor também havia liderado essa lista em 2020 e 2021. Quando avaliamos conjuntamente ao setor de construção civil, percebe-se que ambos respondem por 25% de todas as vítimas desses sites em 2022.[5] Além disso, a IBM descobriu que 36% dos ataques que impactaram organizações conectadas a OT neste ano envolveram *ransomware*.[6]

Olhando além dos números, ataques de *ransomware* causaram inúmeros prejuízos a organizações de manufatura, desde danos à reputação até interrupções operacionais e em cascata nas cadeias de suprimentos. Isso foi especialmente identificado em 2022 na cadeia global de suprimentos automotivos. Em fevereiro daquele ano, o ator de ameaça RaaS White Janus (conhecido como LockBit) conduziu um ataque de *ransomware* contra a subsidiária americana da Bridgestone Corp. Como resultado, a empresa teve de se desconectar da rede para remediação das suas plantas industriais e de recauchutagem na América Latina e América do Norte.[7] No mesmo mês, um outro ataque do Blue Cronus (Conti) na Kojima Industries, fabricante de componentes plásticos para o setor automotivo, forçou a Toyota Motors a suspender suas linhas de produção em 14 fábricas no Japão.[8]

---

4. CTO-SRT-20230417-01A – *Ransomware report for March 2023*
5. "Ameaças cibernéticas: 2022 em retrospectiva" PwC Brasil, https://www.pwc.com.br/pt/estudos/servicos/consultoria-negocios/2023/ameacas-ciberneticas-2022-em-retrospectiva.html
6. *"X-Force Threat Intelligence Index 2022,"* IBM, https://www.ibm.com/downloads/cas/ADLMYLAZ (fevereiro de 2023)
7. *"Bridgestone Hit as Ransomware Torches Toyota Supply Chain,"* Threat Post, https://threatpost.com/bridgestone-hit-as- ransomwaretorches-toyota-supply-chain/178998/ (21 de março de 2022)
8. *"Ransomware: The #1 Threat Targeting Manufacturers Worldwide,"* Dragos, https://hub.dragos.com/hubfs/312-Year-in- Review/2022/Dragos_Year-In-Review-Infographic-2022-Ransomware-Targeting-Manufacturers.pdf?hsLang=en (fevereiro de 2023)

Em março de 2022, a subsidiária alemã da japonesa Denso Corporation, que é uma fornecedora da indústria automotiva,[9] reportou ter sido vítima de um grupo de *ransomware* chamado Pandora. Este afirmou ter exfiltrado 1,4 TB de dados, incluindo informações supostamente ligadas à gigante japonesa Toyota Motor, e ameaçou vazar dados financeiros, de propriedade intelectual, esquemas e comunicações internas.[10] A rápida sucessão desses ataques de *ransomware* nas empresas manufatureiras resultaram em paralisações operacionais e complicaram ainda mais os problemas da cadeia de suprimentos automotivos em 2022.[11]

Em um outro incidente no mesmo mês deste ano, a Parker-Hannifin Corporation, com sede nos EUA, foi vítima de um ataque do *ransomware* Conti, o que impactou um grande número de indivíduos e afetou informações relacionadas a empregados atuais e ex-empregados e dependentes e membros dos planos de saúde do grupo.[12] Quatro meses depois, a empresa alemã de manufatura Semikron foi vítima de um ataque do White Dev 136 (também conhecido como LV), que impactou seus sistemas de TI e parou temporariamente a maior parte de sua operação. A empresa teve de reconstruir seus sistemas de comunicação e TI, e suas linhas de produção não foram retomadas até outubro de 2022.[13]

---

9. *Analyst Note: Denso Corporation supplies to a variety of companies, including Toyota, Honda, Fiat, Mercedes-Benz, Volvo, Ford, and General Motors.*
10. *"Pandora Ransomware Hits Giant Automotive Supplier Denso,"* Threat Post, https://threatpost.com/pandora-ransomware-hits- giantautomotive-supplier-denso/178911/ (15 de março de 2022)
11. CTO-QRT-20220407-01A – *Ransomware report for March 2022*
12. *"Manufacturing Company Parker-Hannifin Suffers Health Plan Cyberattack, 120K Impacted"*, TechTarget, https://healthitsecurity.com/news/manufacturing-company-parker-hannifin-suffers-health-plan-cyberattack-120k-impacted (19 de maio de 2022)
13. *"Semiconductor manufacturer Semikron hit by LV ransomware attack"*, Bleeping Computer, https://www.bleepingcomputer.com/news/security/semiconductor-manufacturer-semikron-hit-by-lv-ransomware-attack/ (2 de agosto de 2022)

Em maio de 2023, o *ransomware* BlackBasta, que atribuímos ao Blue Cronus, atacou a empresa global de automação ABB, que possui ampla carteira de clientes em vários setores e comercializa soluções ICS e SCADA para fornecedores da manufatura e do setor de energia. O ataque interrompeu as operações comerciais da companhia, afetando o Diretor Ativo do Windows (*Windows Active Director*) e se espalhando a centenas de dispositivos em sua rede. Ela então teve de encerrar conexões VPN (rede privada virtual) "com seus clientes para evitar a propagação do *ransomware* para outras redes".[14]

Roubo de dados

Embora agora seja comum que os criminosos não apenas criptografem dados de vítimas, mas também roubem informações em ataques que chamamos de "extorsão dupla", esses atores também fazem isso fora das operações de *ransomware*. Eles aproveitam oportunidades para explorar dados desprotegidos ou expostos, fazer novas vítimas (por meio de *social engineering*) ao mirar nos funcionários ou lançar *malwares* de roubo de informação para obter acesso ilícito a sistemas ou dados e monetizar em cima disso. Mesmo que nenhum setor esteja imune, a manufatura tem sido um alvo significativo, o que se evidencia pelos inúmeros incidentes e perda de grande número de credenciais. Em 2022, por exemplo, a Flashpoint identificou 800 milhões de credenciais e registros pessoais roubados somente de organizações da área.[15]

14. *"Multinational tech firm ABB hit by Black Basta ransomware attack,"* Bleeping Computer, https://www.bleepingcomputer.com/news/security/multinational-tech-firm-abb-hit-by-black-basta-ransomware-attack/ (11 de maio de 2023)

15. *"State of Cyber Threat Intelligence 2023,"* Flashpoint, https://flashpoint.io/wp-content/uploads/State-of-Cyber-Threat-Intelligence- Report-2023.pdf (março de 2023)

Em janeiro de 2023, a Pepsi Bottling Ventures, com sede nos Estados Unidos, descobriu que seus sistemas de TI foram expostos por um ator de ameaça que não foi divulgado. Este havia atacado a empresa, em dezembro de 2022, com um *malware* de roubo de informação, que conseguiu roubar dados como a PII (*Personally Identifiable Information*, na sigla em inglês) de seus funcionários.[16] Em outro exemplo, em fevereiro de 2022, a fabricante americana de chips NVIDIA foi comprometida pelo White Dev 111 (também conhecido como LAPSUS$ Group) em um ataque de extorsão de dados, que envolveu vazamento de credenciais dos funcionários e informações proprietárias. Não bastasse o pedido de resgate, o ator fez mais demandas. Solicitou que fosse aumentado o limite da capacidade de mineração da GPU (unidade do processamento gráfico) e que a NVIDIA fizesse com que seus *drivers* GPU se tornassem de código aberto.[17]

Espionagem

Embora não tenham sido tão amplamente observados ou reportados publicamente em comparação aos atores de ameaça com motivações financeiras, os ataques de espionagem continuam a ser uma grande preocupação para as empresas de manufatura. Entre as tensões nas cadeias globais de suprimentos causadas pela pandemia de covid-19 e os desafios que surgiram após a invasão da Ucrânia pela Rússia em 2022, o setor tem enfrentado problemas com fornecedores, transporte, logística e terceiros. À medida que esses desafios globais são exacerbados, as organizações do ramo podem se encontrar na mira de espiões que tentam infiltrar ou interromper indústrias sensíveis.

16. *"Pepsi Bottling Ventures suffers data breach after malware attack,"* Bleeping Computer, https://www.bleepingcomputer.com/news/security/pepsi-bottling-ventures-suffers-data-breach-after-malware-attack/ (13 de fevereiro de 2023)

17. *"Cybercriminals who breached Nvidia issue one of the most unusual demands ever"*, Ars Technica, https://arstechnica.com/informationtechnology/2022/03/cybercriminals-who-breached-nvidia-issue-one-of-the-most-unusual- demands-ever/ (4 de março de 2022)

Uma das indústrias que dominou as manchetes em 2022, no contexto de tensões geopolíticas, é a de semicondutores. Em resposta às crescentes preocupações com a transferência de tecnologia, os Estados Unidos emitiram em 2022 um novo conjunto de controles de exportação com o intuito de restringir o acesso chinês a tecnologias, softwares e componentes relacionados a semicondutores.[18] Considerando que a massa crítica desta indústria está localizada em Taiwan e as tensões crescentes deste país com a China, vários governos e organizações internacionais estão se preparando para uma disrupção significativa nesse setor e para mudar ou mover suas operações, por exemplo, para a Índia.[19]

Os atores de ameaça baseados na China têm um histórico de ataques a indústrias de semicondutores e alta tecnologia, além de manufatura industrial pesada. Criminosos motivados por espionagem, como o Red Charon (conhecido como Chimera) e o Red Djinn (também identificado como BlackTech, Palmerworm, COBALT e Huapi), foram observados atacando empresas de eletrônicos e semicondutores em Taiwan em suas cadeias de suprimentos, incluindo subsidiárias, parceiros e concorrentes em 2018 e 2019.[20, 21] Mais recentemente, analisamos uma campanha, de abril a junho de 2022, atribuída ao ator de ameaça baseado na China Red Ladon (TA423, APT40 e Leviathan), que atacou entidades do governo e da mídia australiana, além de players globais da indústria pesada, que realizam a manutenção de frotas de turbinas eólicas no Mar da China Meridional.[22] Este padrão de direcionamento, alinhado a áreas-chave de interesse da China, conforme estipulado em seu 14º Plano Quinquenal, também esclarecem essas interseções adicionais com o ramo da manufatura, como nas áreas aeroespacial, de defesa, energia, saúde e outras tecnologias.[23]

18. CTO-SIB-20221117-01A – *US export controls on semiconductors*
19. CTO-SIB-20221214-01A – *APAC-origin forecast - Q3 2022 developments*
20. CTO-TIB-20200506-01A – *Supercomputers and TSCookies*
21. CTO-SIB-20221117-01A – *US export controls on semiconductors*
22. CTO-TIB-20220829-01A – *Rising tide*
23. CTO-SIB-20210423-01A – *China's 14th Five-Year Plan*

Em 2022, avaliamos outros casos de espionagem que se voltaram a organizações de manufatura em todo o mundo. No início de 2022, respondemos a um incidente que envolveu uma organização europeia de engenharia e manufatura, alvo do ator de ameaça baseado no Irã, Yellow Liderc (também conhecido como Tortoiseshell e TA456). Além disso, com base em nossa análise dos ataques cibernéticos e suas tendências em 2022, antecipamos que atores baseados na Rússia e China aumentarão o foco no setor manufatureiro, bem como em indústrias interconectadas ou dependentes, à medida que aumentam as tensões geopolíticas.[24]

Sabotagem

Ataques motivados por sabotagem contra empresas do setor de manufatura têm um potencial devastador sobre as vítimas, especialmente se forem perpetrados contra ambientes de tecnologia operacional (OT) – o que pode implicar riscos de segurança para empresas e períodos de inatividade operacional longos e custosos. Devido à natureza altamente especializada desses ambientes, atores de ameaça em busca de sabotagem normalmente desenvolvem *malwares* sob medida para atacar instalações específicas.[25] A invasão da Ucrânia pela Rússia, em fevereiro de 2022, é um exemplo recente de ataques e tentativas de sabotagem por atores de ameaça patrocinados pelo governo para implantar *malwares* específicos de OT e ICS.[26] Além disso, ainda neste ano, a empresa de cibersegurança Dragos "viu uma escalada revolucionária nas capacidades de um novo *malware* modular para sistemas de controle industrial (ICS), PIPEDREAM, desenvolvido pelo grupo CHERNOVITE".[27]

24. "Ameaças cibernéticas: 2022 em retrospectiva" PwC Brasil, https://www.pwc.com.br/pt/estudos/servicos/consultoria-negocios/2023/ameacas-ciberneticas-2022-em-retrospectiva.html
25. CTO-SIB-20230105-01A – *The OT threat landscape*
26. "Ameaças cibernéticas: 2022 em retrospectiva" PwC Brasil, https://www.pwc.com.br/pt/estudos/servicos/consultoria-negocios/2023/ameacas-ciberneticas-2022-em-retrospectiva.html
27. *"ICS/OT Cybersecurity Year in Review 2022,"* Dragos, https://www.dragos.com/year-in-review/ (fevereiro de 2023)

Hacktivismo

Ao mesmo tempo em que os ataques de sabotagem voltados a OT e ICS continuam a preocupar seriamente o setor de manufatura, vimos também, em 2022, um ressurgimento de ações de hacktivismo na forma de ataques DDoS contra várias vítimas.[28] Essa tendência permaneceu no ano seguinte com o aparecimento do ator de ameaça pró-Rússia e hacktivista NoName057(16), o qual foi visto atacando de forma generalizada com DDoS organizações ao redor do mundo e diversos setores, incluindo a manufatura.[29] Os DDoS, embora menos sofisticados, ainda são disruptivos e consomem energia e recursos para evitar preocupações mais urgentes.

28. "Ameaças cibernéticas: 2022 em retrospectiva" PwC Brasil, https://www.pwc.com.br/pt/estudos/servicos/consultoria-negocios/2023/ameacas-ciberneticas-2022-em-retrospectiva.html

29. *"Russia Affiliated NoName057[16] Hacktivist Group Puts 2023 Czech Presidential Election on the Spot,"* Check Point, https://blog.checkpoint.com/2023/01/19/russia-affiliated-noname05716-hacktivist-group-puts-2023-czech-presidential-election-on- the-spot/ (19 de janeiro de 2023)

Cenário de ameaças

Os atores de ameaça listados abaixo foram observados pela PwC ao atacarem o setor da manufatura. Seus alvos variam conforme regiões, tipos de organização, motivações e intenções. Este cenário de ameaças pode ser usado para ajudar a determinar e priorizar a cobertura de criminosos que se voltam contra organizações específicas.

	Ator de ameaça	Nomes	País de origem
Espionagem	Black Artemis	Lazarus Group, Hidden Cobra, ZINC	Coreia do Norte
	Black Banshee	Kimsuky, Velvet Chollima	Coreia do Norte
	Blue Kraken	Energetic Bear, DRAGONFLY	Rússia
	Red Apollo	APT10, Stone Panda, Menupass Team	China
	Red Charon	Chimera	China
	Red Djinn	BlackTech, Palmerworm, COBALT, Huapi	China
	Red Dev 24	Antlion	China
	Red Ladon	TA423, APT40, Leviathan	China
	Yellow Dev 29	TA457	Irã
	Yellow Dev 33	Moses Staff, Abraham's Ax	Irã
	Yellow Liderc	Tortoiseshell, TA456	Irã
	Yellow Nix	MuddyWater, MERCURY	Irã
	Yellow Orc	APT33, Refined Kitten, STONEDRILL	Irã

	Ator de ameaça	Nomes	País de origem
Criminal	Blue Cronus	Conti, BackBasta, Royal	Rússia
	Bronze Dev 2	Silver Terrier	Nigéria
	White Baku	Cuba, Coldraw	Em avaliação
	White Dev 101	ALPHV-ng, BlackCat	Em avaliação
	White Dev 136	LV	Em avaliação
	White Janus	LockBit	Em avaliação
	White Peryton	Play	Em avaliação
	White Pixie	RansomEXX, Defray777	Em avaliação
	White Sobek	Karakurt	Em avaliação
	White Veles	DEV-0504, Velvet Tempest	Em avaliação

Estudos de caso

Os estudos de caso abaixo fornecem uma visão geral dos ataques que ocorreram nos últimos anos. Esses exemplos também ilustram as motivações dos atores de ameaça que têm como alvo o setor da manufatura.

Motivação do ator de ameaça	Alvo	Ano
Espionagem	Manufatura, governo, mídia, energia	2021-2022

Sumário executivo

Em 2021 e 2022, o Red Ladon (também identificado como TA423, APT40 e Leviathan) mirou fabricantes globais da indústria que atuam na produção, instalação e manutenção de turbinas eólicas no Mar da China Meridional, além de empresas da mídia e órgãos governamentais da Austrália. Essa campanha usou a tática de *spear phishing* para entregar:

- Links maliciosos que hospedavam o *framework* ScanBox;
- Documentos RTF e de Word maliciosos.

O Red Ladon mira empresas com interesses na região e, nesta ação, concentrou-se em entidades envolvidas na fazenda eólica *offshore* de Yunlin e no campo de gás Kasawari. Embora o foco do Red Ladon se volte geralmente para a costa chinesa, o grupo também teve como alvo um fabricante europeu de equipamentos pesados usados na instalação dessas eólicas. Isso demonstra que cadeias de suprimentos e empresas relacionadas podem sofrer danos colaterais mesmo em ações de espionagem localizadas. Ao mesmo tempo, a Sapura Energy, entre outras companhias, retirou-se do projeto por causa de atrasos na construção.[30]

30. *"Sapura Energy pulls out from Taiwan offshore wind farm project,"* The Edge Markets, https://www.theedgemarkets.com/article/sapura-energy-pulls-out-taiwan-offshore-wind-farm-project (2 de fevereiro de 2022)

Ferramentas, Técnicas e Procedimentos (TTPs)

O Red Ladon tentou fazer vítimas via *spear phishing* com um e-mail que continha um link para um site criado para despertar o interesse das pessoas e com arquivos suspeitos disponíveis para download. Documentos do tipo RTF e de Word anexados aos e-mails usariam a vulnerabilidade de injeção de modelo para recuperar um *downloader* de um C2 e, quando o anexo era um arquivo ZIP, o ator de ameaça seduzia a vítima para extrair e executar os arquivos.

Em um caso, o ator usou como temas dos e-mails a “perfuração em águas profundas, petróleo e sua exploração”, além de outras questões relacionadas à Defesa Naval Australiana, a organizações de mídia e a empresas de fazendas eólicas.

Quando um link malicioso era usado no e-mail de *phishing*, o *framework* ScanBox então perfilava a vítima e entregava mais *malware*. Normalmente, as cargas úteis eram na forma de um par de DLL executável. Em campanhas anteriores a carga útil final foi uma do tipo Meterpreter.

Impacto

O impacto de uma invasão dessa natureza é difícil de calcular. Isso porque a coleta de inteligência realizada por esses atores de ameaça persistentes e avançados (*Advanced Persistent Threat*, em inglês) raramente é utilizada de imediato. Em geral, o criminoso exfiltra informações do ambiente de sua vítima por meses ou até anos. Além disso, elas raramente são usadas, se é que já aconteceu, pelo próprio ator, já que, muitas vezes, são repassadas a um terceiro que solicitou a informação.

Nossa avaliação é que, nos casos relatados, os dados coletados e convertidos em inteligência foram usados por organizações em negociações de fusão e aquisição (M&A) ou de parceria com a vítima, o que garantia vantagem nas negociações; como informações sobre a situação financeira da parte oposta, seus planos de investimento e objetivos.

Neste caso, há ainda a possibilidade de interferência de terceiros para atrasar, interromper ou impedir a realização de trabalhos de empresas que não concordassem com os objetivos declarados de governos. Embora não possamos estabelecer conexão direta entre os atrasos sofridos durante a construção da fazenda eólica *offshore* de Yunlin e as atividades do Red Ladon, essa é uma possibilidade sobre a qual as companhias devem estar cientes ao operar em áreas politicamente sensíveis.

Invasões por atores de ameaça persistentes e avançados (APTs) podem ser demoradas e difíceis de detectar, e suas atividades nem sempre resultam em um impacto imediato na entidade comprometida. Por outro lado, operadores de *ransomware* ou outros grupos de crime organizado (Organized Crime Groups, em inglês) causam um impacto mais imediato e direto na vítima e devem ser priorizados. No entanto, a equipe de Inteligência de Ameaças da PwC enfatiza que a coleta de informações no longo prazo pode impactar os negócios de organizações em qualquer setor. Operar ou negociar com um potencial parceiro comercial que possua uma posição de mercado injusta, graças a essas informações sensíveis obtidas ilicitamente, pode criar situações em que uma empresa é adquirida ou faz negócios com uma organização que está em uma vantagem competitiva distinta.

Mais informações

CTO-TIB-20220829-01A – *Rising Tide*

TA423/Red Ladon: Espionage in South China Sea

Scanbox: A Reconnaissance Framework Used with Watering Hole Attacks

Motivação do ator de ameaça	Alvo	Ano
Financeiro	Manufatura	2022

Sumário executivo

Em maio de 2022, a AGCO, uma fabricante de equipamentos agrícolas com sede nos EUA, foi atacada por *ransomware*. O Blue Cronus (conhecido como Black Basta e ex-operador do Conti) reivindicou a responsabilidade pelo ataque. Depois, postou os dados em seu site de vazamento. A AGCO declarou que "é de se esperar que as operações comerciais sejam afetadas negativamente por vários dias e levem mais tempo do que o previsto para retomar todos os serviços, dependendo do quão rápido a empresa consiga reparar seus sistemas."[31]

A AGCO também sentiu o golpe em suas finanças, uma vez que suas ações caíram 6% após o anúncio.[32] A imprensa destacou que, antes de ser comprometida, a companhia havia doado US$ 50.000 "para setores impactados pela guerra na Ucrânia"[33], o que poderia ter influenciado o grupo de *ransomware* a atacá-la.[34]

Ferramentas, Técnicas e Procedimentos (TTPs)

Como o Blue Cronus opera o Black Basta como um *Ransomware as a Service* (RaaS), com afiliados que realizam invasões reais contra as vítimas, os TTPs específicos para cada ação podem variar. A seguir, estão descritos os mais conhecidos que foram usados para implantar o Black Basta.

31. *"AGCO announces ransomware attack"*, AGCO, https://news.agcocorp.com/news/agco-announces-ransomware-attack (6 de maio de 2022)
32. *"AGCO ransomware attack disrupts tractor sales during U.S. planting season,"* Reuters, https://www.reuters.com/business/agco- says-some-production-facilities-hit-by-ransomware-attack-2022-05-06/ (6 de maio de 2022)
33. *"AGCO Agriculture Foundation Donates to Farmer-Focused Initiative 'BORSCH' in Ukraine"*, AGCO, https://news.agcocorp.com/news/agco-agriculture-foundation-donates-to-farmer-focused-initiative-borsch-in-ukraine (5 de maio de 2022)
34. *"US agricultural machinery maker AGCO hit by ransomware attack,"* Bleeping Computer, https://www.bleepingcomputer.com/news/security/us-agricultural-machinery-maker-agco-hit-by-ransomware-attack/ (6 de maio de 2022)

O acesso inicial é obtido por meio de infecções do trojan QakBot. Seus operadores procuram infectar as vítimas por meio de *spear phishing* com links para baixar arquivos ISO que carregam o binário QakBot. Outro método é o uso de arquivos OneNote que soltam *scripts* HTA, VBScript e Batch. Uma vez no ambiente da vítima, um afiliado procurará estabelecer persistência com *backdoors* ou ferramentas de administração remota. Isso inclui Brute Ratel e Cobalt Strike, assim como AnyDesk e Atera.

O Cobalt Strike e o Brute Ratel também possibilitam aos afiliados a capacidade de se mover lateralmente no ambiente da vítima via PsExec e WinRM. Eles também são conhecidos por empregar BITSAdmin, WMI e RDP para essa finalidade. Junto com a movimentação lateral, essas ferramentas também são capazes de permitir a escalada de privilégios tanto com o Mimikatz quanto via personificação de *token*.

Os dados são exfiltrados usando o Rclone, um utilitário de linha de comando que permite ao ator de ameaça carregar arquivos para armazenamento na nuvem. Neste estágio, os afiliados do Black Basta criptografam arquivos nos sistemas das vítimas com *ransomware* e ameaçam vazar dados em seu site de vazamento se elas não pagarem por uma ferramenta de descriptografia

Impacto

No caso da AGCO, o impacto foi comunicado 10 dias após o anúncio de que havia sofrido um ataque de *ransomware*. A empresa declarou que “a maioria dos locais de produção e operações de peças afetadas retomou as atividades operacionais na semana passada ou hoje. O restante deve começar a operar ao longo da semana, e todos estarão funcionando normalmente até o final desta semana.”[35] – isso significa que o impacto imediato da invasão durou pouco mais de duas semanas. A empresa disse ainda que sofreu uma queda na produção devido à invasão e que dados foram vazados. Afirmou também que esses dados não tinham privacidade protegida por natureza, pois não realizava “operações de varejo”. No entanto, conforme o comunicado, ainda haveria custos de remediação e investigação para verificar a extensão das ações realizadas contra a companhia.

35. *“AGCO Provides Update on Recovery from Ransomware Cyber Attack,”* AGCO, https://news.agcocorp.com/news/agco-provides- update-on-recovery-from-ransomware-cyber-attack (16 de maio de 2022)

Mais informações

CTO-TIB-20230419-01A – *The unfortunate return of Black Basta*

CTO-TIB-20230301-02A – *Backstabbing EDR's*

CTO-TIB-20220525-02A – *Behold: Black Basta's basic but bullish binary*

AGCO Provides Update on Recovery from Ransomware Cyber Attack

AGCO ransomware attack disrupts tractor sales during U.S. planting season

Recomendações para detecção

Técnicas comuns neste relatório

Dumping de Credenciais do Sistema Operacional (T1003)

Monitore controladores de domínio para solicitações de replicação inesperadas ou não programadas, especialmente de sistemas que não são controladores de domínio. Monitore sistemas para sinais de *dumping* de *hash* ou acesso ao SAM. Procure por processos incomuns que tentem interagir com o lsass.exe.

Descoberta Remota de Sistema (T1018)

Realize o monitoramento da rede interna para detectar varreduras e outras tentativas de descoberta, assim como atividades de movimentação lateral. Monitore a execução de comandos para detectar comandos que possam ser usados para essas finalidades.

Intérprete de Comando e *Script* (T1059)

Registre o uso do PowerShell e audite esses logs regularmente. Monitore *scripts* em execução em um sistema que normalmente não os executa, ou o carregamento de módulos para linguagens de *script* que normalmente não são usadas. Monitore ainda os argumentos de linha de comando por sinais de coleta ou descoberta de informações.

Exploração para Escalonamento de Privilégios (T1068)

Monitore sinais de injeção de processo e o carregamento de *drivers* vulneráveis, ou que ainda não tenham sido vistos anteriormente em seu ambiente. Procure por criações de processo incomuns, como aplicações que normalmente não rodam o PowerShell ao acionar seu executável. Da mesma forma, procure por quaisquer sinais de tentativa de elevação de privilégios.

Comprometimento da Cadeia de Suprimentos (T1195)

Realize verificações de hash ou integridade em softwares recebidos, além de os escanear com ferramentas *antimalware*. Realize atualizações em um ambiente monitorado de teste, antes de liberá-las amplamente.

Relacionamento Confiável (T1199)

Monitore o tráfego com terceiros para identificar padrões incomuns. Registre e audite qualquer atividade delegada.

Exploração para Execução do Cliente (T1203)

Procure por criações de processos pouco usuais, como aplicativos que normalmente não rodam o PowerShell ao acionar o seu executável.

Inibição da Recuperação do Sistema (T1490)

Monitore os *backups* por quaisquer sinais de tentativas de exclusão ou alteração nas políticas de retenção, bem como quaisquer mudanças em processos ou configurações envolvidas na recuperação do sistema.

Negação de Serviço na Rede (T1498)

Monitore a saúde de qualquer serviço exposto, incluindo os tempos de resposta e quaisquer erros ou avisos, além dos volumes de tráfego.

Comprometimento das Defesas (T1562)

Monitore todos os comandos que possam modificar qualquer ferramenta ou configuração relacionada à segurança – por exemplo, alterações nas regras do firewall ou sua parada no Windows. Isso incluirá a ausência de registros esperados. Monitore ainda mudanças nas contas dos usuários em que a alteração do acesso possa afetar a segurança.

Considerações finais

Ainda que seus objetivos sejam diferentes, vários criminosos têm aproveitado oportunidades para atacar empresas de manufatura e impactar setores e mercados interconectados. Os alvos e os ataques cibernéticos coincidiram com o aumento da digitalização do setor, a integração de OT e de redes de terceiros e os requisitos relativamente menores para impor controles de segurança nesses ambientes. Com base em tendências de incidentes, estudos de caso de ataques e em nossa própria análise interna, concluímos que atores de ameaça motivados financeiramente têm foco crescente em manufatura. As empresas enfrentaram um significativo número de ataques de *ransomware*, e o roubo de dados por cibercriminosos continua preocupante.

Observamos ainda que atividades de atores de ameaça motivados por espionagem buscaram obter insights sobre projetos sensíveis e informações que envolviam representantes do segmento. Porém, o foco estava em outros alvos ou inteligências cruciais, como construção civil, semicondutores, aeroespacial, defesa e telecomunicações. Isso resultou em *targeting* e roubos de dados de empresas, de suas redes corporativas e de outras organizações de sua cadeia de suprimentos. Criminosos motivados por espionagem e sabotagem também visaram organizações de manufatura com o intuito de impactar suas operações, como foi visto entre os atores baseados na Rússia, após a invasão da Ucrânia.

Saber quais atores são relevantes para um setor é um importante passo para direcionar estrategicamente o investimento em controles de defesas apropriados. No entanto, a visão geral apresentada neste relatório abarca todo o segmento da manufatura, suas indústrias e seus mercados interconectados. Uma análise mais setorizada das ameaças deve ser feita por cada organização. Por fim, um estudo de como as ameaças navegam na infraestrutura da sua organização pode ajudar a identificar os *gaps* existentes em seus controles de segurança e possibilitar uma rápida adequação.

Apêndice 1: Metodologia de análise

Embora possam compartilhar objetivos, os ataques dos atores de ameaça 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 pela informação	Os atores 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 atores 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 pelo dinheiro	Os cibercriminosos cibernéticos procuram um alvo de maneira indiscriminada, pois simplesmente buscam monetizar as atividades. A gama de sofisticação dos cibercriminosos cibernéticos é ampla 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 atores 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 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, ataques de *ransomware*, espionagem econômica e invasões direcionadas, incluindo 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 dos riscos cibernéticos, ajuda nossos clientes a obterem 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 do setor público e privado em todo o mundo para proteger, conhecer o entorno de atuação e apoiar estratégias.

Pesquisas e avaliações direcionadas

Acesso direto à equipe de pesquisa de ameaças da PwC para tarefas relacionadas a consultas *ad-hoc* ou de longo prazo – tanto pesquisas táticas quanto estratégicas sobre amostras maliciosas, atores de ameaça ou suporte à análise.

Monitoramento de inteligência de ameaças cibernéticas

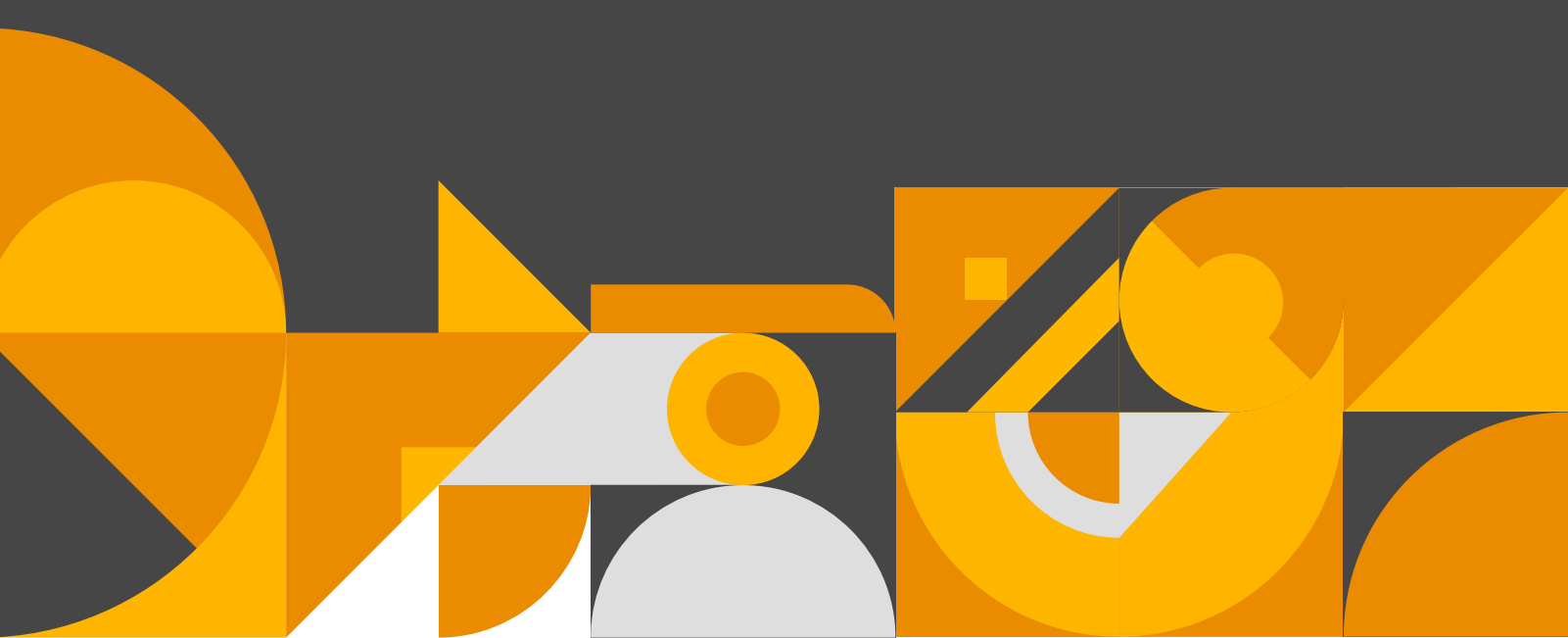
Pesquisa contínua, personalizada e focada em complementar nossos serviços de assinatura.

Consultoria e assessoria

Serviços de consultoria para ajudar empresas a definir requisitos e como consumir, aplicar e produzir inteligência de ameaças, da maneira que melhor se adapte à sua realidade organizacional.

Assinatura de inteligência de ameaças cibernéticas

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



Contato

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

pwc

Acesse o site:

www.pwc.com.br

Siga a PwC nas redes sociais