



BLACK KITE

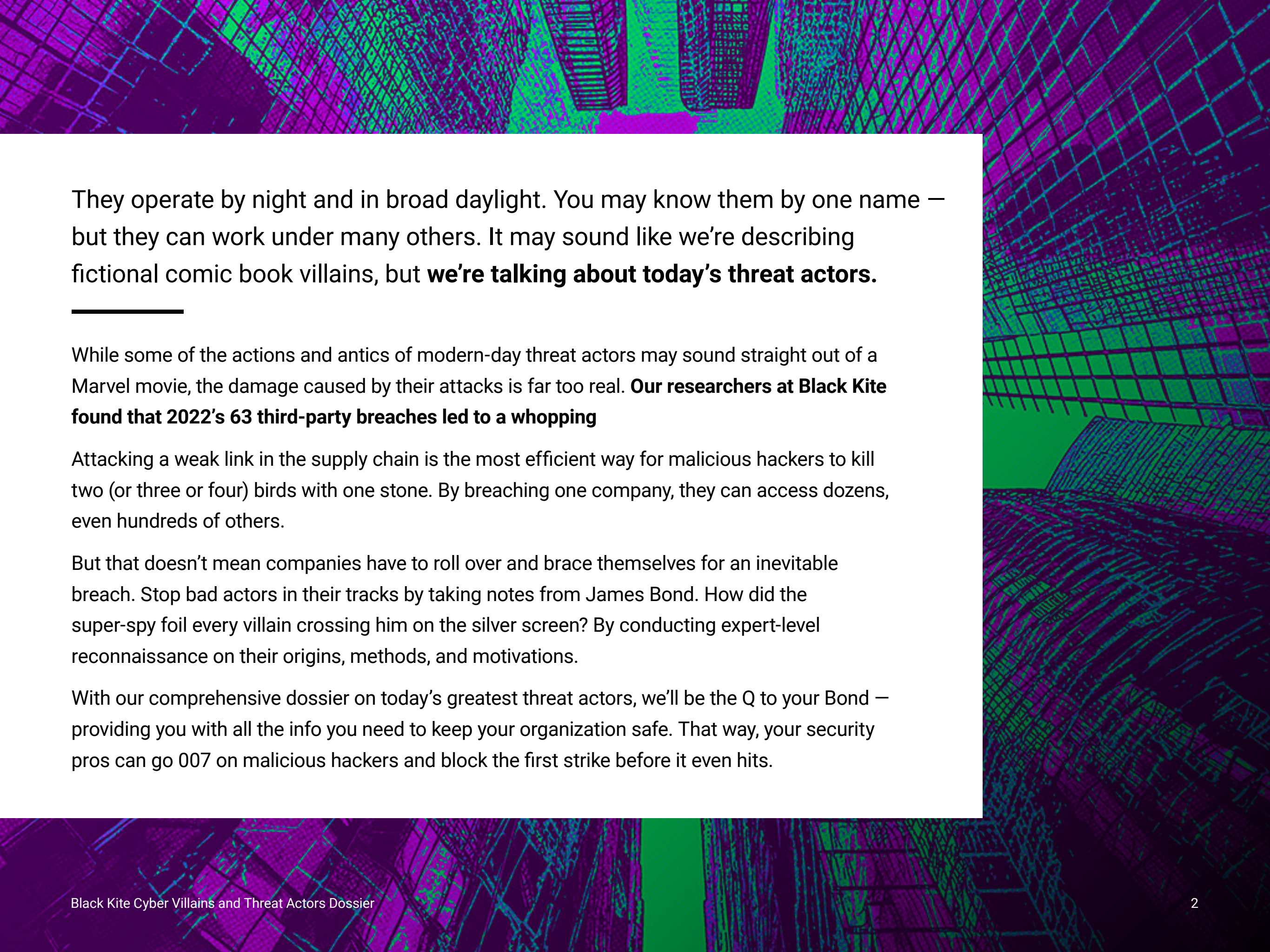
CYBER

VILLAINS

and Threat Actors Dossier







They operate by night and in broad daylight. You may know them by one name — but they can work under many others. It may sound like we’re describing fictional comic book villains, but **we’re talking about today’s threat actors.**

---

While some of the actions and antics of modern-day threat actors may sound straight out of a Marvel movie, the damage caused by their attacks is far too real. **Our researchers at Black Kite found that 2022’s 63 third-party breaches led to a whopping**

Attacking a weak link in the supply chain is the most efficient way for malicious hackers to kill two (or three or four) birds with one stone. By breaching one company, they can access dozens, even hundreds of others.

But that doesn’t mean companies have to roll over and brace themselves for an inevitable breach. Stop bad actors in their tracks by taking notes from James Bond. How did the super-spy foil every villain crossing him on the silver screen? By conducting expert-level reconnaissance on their origins, methods, and motivations.

With our comprehensive dossier on today’s greatest threat actors, we’ll be the Q to your Bond — providing you with all the info you need to keep your organization safe. That way, your security pros can go 007 on malicious hackers and block the first strike before it even hits.





# Our Villain Dossier

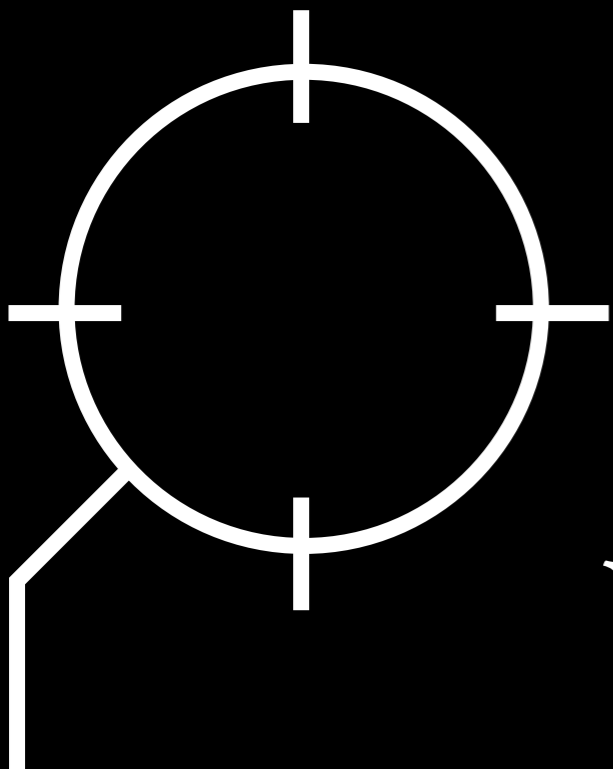
Our teams lurk in the shadows of the dark web.

They read every headline and take extensive notes on the latest villains populating the threat landscape.





# Evil org



**BEWARE THE  
ORGANIZED IRE  
OF RANSOMWARE  
GANGS**



## Calling Cards

Ransomware gangs are the most common type of villain organizations you can expect to encounter in the threat landscape – and they’re usually the heaviest hitters.

Think of ransomware groups as “evil organizations.” They’re the most coordinated villain in our dossier. Ransomware groups form and function like legitimate corporate entities – except they operate by conducting illegal activities. Malicious cyber actors working for a ransomware group work as a cohesive unit with a level of communication and collaboration on par (or even better!) than the average businesses.

A central image of a laptop with a red screen displaying '27%' in white, surrounded by various playing cards scattered around it. The background is dark with a grid pattern.

**IN 2022, RANSOMWARE ATTACKS ACCOUNTED FOR 27% OF ALL THIRD-PARTY BREACHES.**





Like legitimate organizations, ransomware groups can have a hierarchical structure with C-level leaders, business development departments, finance departments, research and development departments, and even OSINT teams. Some ransomware groups even have branding – which helps entice and recruit new bad actors to their gangs. They’re constantly seeking more information (and funding) to take their attacks to the next level.

Like the “evil orgs” common in spy movies, ransomware groups’ ability to work as a single unit and bring together the expertise of many bad actors in concert makes them dangerous. That expertise explains why **over 2,700 organizations** fell victim to ransomware attacks last year – they know how to hit an organization’s defenses where it hurts.

Ransomware gangs may also partner with other cybercriminals to conduct daily operations. For example, they may work with operators on the black market to mine the dark web for passwords or access codes that could help them break through their target systems.

**You read that right.** These ransomware groups have their own digital supply chains that enhance their business.

### **Ransomware Gangs’ Heavy-Hitter Weapon: RaaS**

Ransomware groups offer a popular product, and it’s known as [Ransomware-as-a-Service](#) (RaaS).

### **What is RaaS?**

It’s basically “pre-made” or “packaged” ransomware made by a cybercriminal developer. That means specialized hacking or coding expertise is no longer a prerequisite for launching a successful ransomware attack. Any average Joe can purchase RaaS from a ransomware group and unleash its power on unsuspecting target organizations.



## Motives

Like most corporate entities, ransomware gangs share one common goal: **Cold hard cash.**

Money is the biggest motivator for ransomware groups, and they're good at knowing how to get them.

[According to our 2023 Ransomware Threat Landscape Report,](#) ransomware groups tend to target companies with annual revenues of around \$50 million to \$60 million.

WITH **IBM** CLOCKING THE AVERAGE COST OF A RANSOMWARE ATTACK IN 2022 AT

\$44.5

Million

...it's no surprise why ransomware attacks are increasingly more popular by the minute.



Ransomware groups' obsession with money often proves to be a cyclical pattern. A successful ransom gives them a big lump sum of cash to reinvest into their business. **With that money, they can hire more employees, invest in more technology, and wreak havoc on unsuspecting targets.**

While most ransomware groups usually attack companies with money in the multi-millions, they're not necessarily ultra-picky. They'll go for any organization that has cash (or data of value) on its hands, which means that virtually all businesses are at some risk.

### TPRM Tip

Don't rely exclusively on questionnaires to get a pulse check on your third parties' security health. [This traditional method of TPRM](#) is ineffective at painting the full picture of risk because questionnaires are largely subjective — and usually too optimistic.

It's best to supplement questionnaires with risk tools that can give your organization an unbiased point of view of your vendors' risk profiles.





## An (In)Famous Example

Security pros should keep an eye on LockBit, one of the most prolific ransomware groups to date. According to [Black Kite research](#), LockBit was responsible for 29% of all ransomware attacks during the past year.

This group mainly targets companies with annual revenues between \$40 and \$80 million — primarily focusing on manufacturing and technical service organizations in the U.S. and Europe.

**[LockBit was responsible](#) for the record-breaking incident with U.K. Royal Mail in early 2023, the U.K.'s largest shipping organization. The ransomware group demanded an \$80 million ransom, which was promptly rejected. As a result, LockBit leaked several of the Royal Mail's files and negotiation chat history.**

### TPRM Tip

It's not enough to ensure that your vendors aren't making any political enemies. To defend against hacktivists, organizations must also keep tabs on even their vendors' partners — and stay vigilant of any potential ideological crossfire.





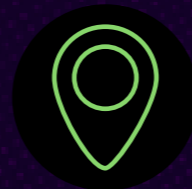
## Defenses are Forever

Organizations can boost their defense against ransomware gangs by keeping a pulse on the latest ransomware attacks.

**Here are some actionable steps your organization can take to defend against ransomware groups:**



- Stay on top of ransomware attacks hitting your specific industry — and make sure you don't have the same vulnerabilities as other victims.



- Conduct an organization-wide audit and pinpoint where you're holding your most sensitive and valuable data and resources — and secure them.



- Identify which of your vendors have access to or handle those resources — and establish them as priorities to track in your TPRM program.





# SELF- RIGHTEDOUS ROGUE

**KEEP AN  
EYE OUT FOR  
HACKTIVISTS**



## Calling Cards

Hacktivists are malicious cyber actors operating with a great sense of moral purpose. Think of them as “the self-righteous rogue” in our villain dossier. They launch attacks on organizations that they deem morally corrupt and are on the hunt for information that they believe should be exposed for the good of the public.

Hacktivists’ attacks can look very different, depending on the moral issue at stake. For example, a self-righteous rogue might be responsible for any of the following: blocking operations at an oil company to protest climate change, hacking a government site for perceived unjust practices, or even hacking a private organization for making a political statement they find disagreeable.

Hacktivists can operate both as organized groups or as solo bad actors. **Either way — more often than not, hacktivists will opt to take credit for what they’ve done.**





# Motives

Hactivists are motivated by their particular political or social beliefs – whether those are right-leaning, left-leaning, somewhere in the middle, or neither. Such a variety of beliefs can make it tough to pinpoint what exactly might motivate each hactivist attack.

**Still, a few common themes unify hactivists in their activities. When hactivists attack, they're looking to:**

- **Gain visibility for the cause they're promoting.** When hactivists hack, they don't do it quietly. Unlike with ransomware gangs, there's very little chance of hactivists giving data back once it's been stolen or quietly settling for a fee.
- **Gain recognition.** Let's be honest: Hactivists aren't acting purely out of the goodness of their hearts. They also want the public to know who is responsible for these hacks and why. So, a little hunger for fame (or more likely, notoriety) plays a role in determining their targets.





## An (In)Famous Example

For an example of just how far hacktivist attacks can go, look no further than [Julian Assange](#), who faces possible extradition to the U.S. for his actions.

Assange is the founder and face of [WikiLeaks](#), a hacktivist site famous for releasing several types of government documents, many of which have caused significant threats to U.S. national security. According to State Department spokesman [P.J. Crowley](#), a [2010 WikiLeaks](#) attack put Afghan and Iraqi citizens communicating with the U.S. military at high risk of physical harm.





## Defenses Are Forever

Organizations can strengthen their defenses against hackers by staying alert for any stories on hacking in the news.

It's best to study what's motivating those particular hackers and then scan your organization for any data or resources that might be valuable to their political causes. Organizations should be on high alert for any hacker attacks if they plan to put out any announcements on potentially controversial topics.

Hackers have a tendency to prefer distributed denial-of-service (DDoS) attacks to temporarily take down websites. In these cases, organizations must have a game plan for when DDoS attacks do occur. How will workflows change when critical sites are down? What contingency plans must be made in order to keep business going?

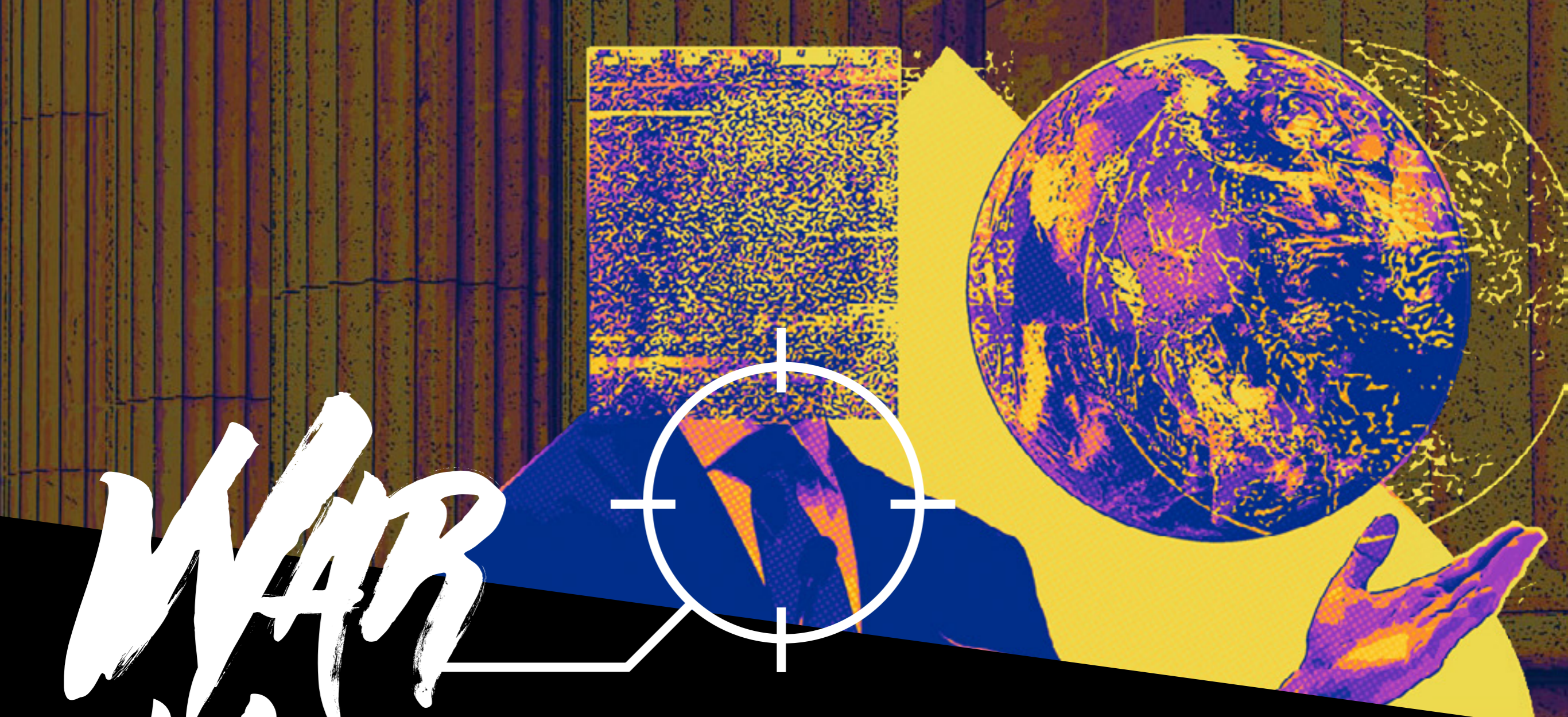
Luckily, security teams don't have to rely exclusively on disparate reports or word-of-mouth for their research. They can also keep tabs on FBI news alerts for the latest hacker developments.

The word "DDoS" is written in a large, white, stylized, brush-stroke font. It is set against a red background that features a pattern of binary code (0s and 1s) in a lighter shade of red. The overall aesthetic is digital and high-tech.

### TPRM Tip

It's not enough to ensure that your vendors aren't making any political enemies. To defend against hackers, organizations must also keep tabs on even their vendors' partners — and stay vigilant of any potential ideological crossfire.





# WAR MACHINE

**PREPARE  
FOR BATTLE  
WITH STATE-  
SPONSORED  
THREAT ACTORS**



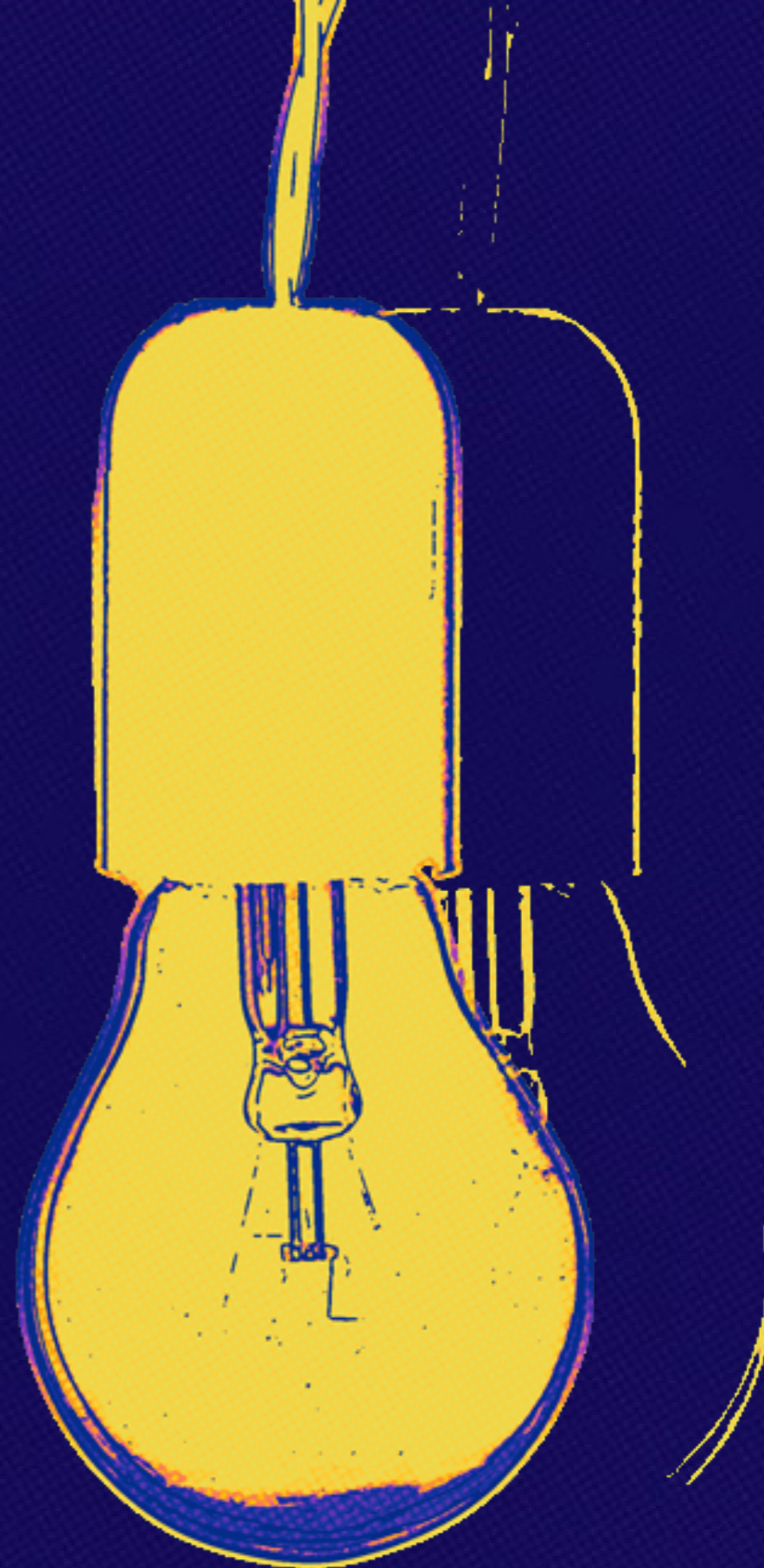
## Calling Cards

State-sponsored bad actors (APTs) are exactly what they sound like: malicious attackers working on behalf of government interests. We're calling APTs "*the war machine*" because they're so often leveraged during times of physical, economic, and cultural war.

Don't be fooled by the title, though. Just because these bad actors work for foreign governments doesn't mean that they're only looking at federal targets.

APTs may also attack critical infrastructure or private entities to disrupt the workflow, business, and lives of those living in the countries they target.

Look no further than [Russia's 2022 cyberattacks on Ukraine](#) for a prime example. Russian APTs attacked everything from banks to bridges, to electric grids and hospitals to gain leverage over Ukrainian forces.





# Motives

APTs are geopolitically motivated. That means all kinds of international tensions can motivate an attack. Most frequently, they'll launch an attack when there's the following:

- **War or military conflict:** Hacks and supply chain attacks are now a leading method of cyber warfare. APTs might launch assaults on financial institutions to put pressure on opposing governments — or they might even shut down operational technology (OT) like bridges or electrical grids to impair physical offenses.
- **A perceived insult to their nation:** If the insult is big enough (and if the government is sensitive enough), APTs might launch a cyber attack in retaliation.
- **Economic competition:** State-sponsored attacks motivated by economic competition are usually less flashy, but they still pack a financial and reputational punch. These state-sponsored hacks are usually a clandestine way of conducting reconnaissance on rival countries and their domestic economies. That's likely why **supply chain vendors** are particularly vulnerable; they're the easiest link to break that's connected to treasure troves of information.



## An (In)Famous Example

Organizations can learn a lot about state-sponsored attacks from the [Kremlin-linked Snake](#) espionage malware. **In 2023, U.S. and international authorities finally dismantled the malware implant that plagued unsuspecting organizations for nearly two decades.**

The FBI found that an APT utilized this particular malware to infect hundreds of computers across nearly 50 countries — in all different kinds of industries. It's a perfect example of why all types of organizations in any country should stay abreast of state-sponsored attacks. Even if they're not in direct conflict with a particular nation, they could still very well be a target.



## Defenses Are Forever

Organizations should stay in the know of large geopolitical events that might affect their industry. They should also develop contingency plans in case essential parts of their supply chain are interrupted.

Many nations had to rely on such contingency plans when the 2022 Russia-Ukraine War severely affected [diesel and gas supply chains](#). As Russia is a major supplier of the world's gas (and Russia and Ukraine are both major global suppliers of wheat and grain), many organizations based in the U.S. and the EU turned to resources in Asia and Africa to pick up the slack.

Another good tip is to diversify the types of vendors working with your organization to [mitigate concentration risk](#). Imagine if your company exclusively did business with Russia and Ukraine in 2022. If that were the case, you'd be suddenly out of luck pretty fast. Doing business with companies from different parts of the globe opens organizations up to new resources and mitigates the impact of state-sponsored supply chain attacks.

### TPRM Tip

Even if your organization isn't located in a state that's in conflict, it's possible that you might be doing business with a vendor that is. Your TPRM program should take into account the national stability of the states your third parties are based in — as well as keep tabs on their geopolitical developments





TALE

MOLE

**LOOK WITHIN  
FOR INSIDER  
THREATS**



## Calling Cards

**Insider threats — particularly malicious insiders — are on the rise as one of the most pervasive types of bad actors.**

What exactly is an insider threat? It's basically any type of security threat or risk that originates from within an organization as opposed to outside of it. That's exactly why we're calling malicious insiders "the mole" — they have the power to work right under your nose while planning devastating leaks, attacks, and breaches.

According to the [2022 Ponemon Cost of Insider Threats Global Report](#), malicious insider attacks have risen by 44% over the past two years. What makes them so dangerous? The fact that *they already have access to some of your most valuable and sensitive information*. Plus, security programs often put a heavy emphasis on defense against external threats, which can mean neglecting defense against internal threats.



# Motives

For insider threat actors, attacks are usually personal.

Malicious insiders are typically motivated by the following:

- **Financial gain:** Money talks, especially when it comes to disgruntled former (or even current) employees that feel their compensation doesn't match their worth – and they could stand more to gain through betrayal than loyalty. Organizations should keep tabs on company morale to ensure financial dissatisfaction isn't on the rise.
- **Espionage:** Sometimes, another organization (or government) might sway those closest to your organization to conduct a little spying on their behalf. Employees aren't immune to bribes, and the right offer may convince them to do some snooping.
- **Recognition:** Sometimes, hacks might simply be due to emotional distress. An insider threat might feel overlooked or tossed to the side, so launching a large-scale cyber-attack might be their cry for attention. There's also a chance that malicious insiders might launch attacks based on emotional distress or dissatisfaction. These "revenge" attacks are common from disconcerted former employees or contractors who either still have access to sensitive information or stole that information while they still had access.



## An (In)Famous Example

Insider threats can come from all kinds of experience, industries, and backgrounds. Real-life examples of malicious insiders include:

- [Jack Teixeira](#), a U.S. Air National guardsman who leaked Pentagon assets in 2023.
- [Anthony Levandowski](#), a former Google employee who sold trade secrets via acquisition to Uber in 2022.
- [Chelsea Manning](#), a former U.S. Army soldier who disclosed sensitive military documents to WikiLeaks in 2013.

In all of these cases, each malicious insider had legitimate access to the information and assets that they leaked.







## Defenses Are Forever

Here's the tricky part about handling insider threats: They might have authorized access (and actually need that authorized access for their job) to dozens upon dozens of sensitive servers and data points.

That's why it's key for organizations to have clear-cut processes for what authorized users can do with sensitive info — and implement security processes that prevent wrongful use.

### TPRM Tip

Here's a quick reality check about insider threats — they're not always intentional. In fact, a good number of leaks caused by insider threats often happen by accident, usually due to carelessness around passwords or other security settings.

In these cases, it's best to ensure that your vendors are also establishing clear boundaries and protocols for when their other partners might have access to their data. That way, you can safeguard your own organization from additional negligence.





The best way to defend an organization from insider threats is to establish clear onboarding and offboarding processes for vendors and contractors that must work with your systems and data. **When working with third parties, organizations should always:**



- Monitor vendor activity. Keep tabs on what your third parties and contractors are doing in your systems and note any anomalies.



- Communicate expectations around regulations with vendors. Lay clear ground rules for the compliance standard your organization requires its partners to meet.



- Establish a clear and air-tight method of offboarding. Sometimes partnerships end, and that's okay. Make sure to tie up all loose ends (i.e., fully remove access) when those relationships come to a close.



# Bad Actors Are Smart — But You're Smarter

The key to foiling these villains' dastardly plans is knowing their methods and motivations like the back of your hand. Knowing your enemies can give your security teams a better idea of who might be setting their sights on your organization, why they're targeting you, and how you can prepare proactively for different types of attacks.

Once your organization has a good grasp on what makes these villains tick, it's time to extend that knowledge to the rest of your supply chain. That intel can help your organization [build the right TPRM program](#) that'll save on dollars and reputation in the long run.

With our villain dossier, your teams can leverage the right intel and take down hackers with efficiency and swagger — like Daniel Craig. Or Sean Connery, if you're old school.

**Check out our [blog on the different types of hackers for more details.](#)**

