ZEROFOX | Whitepaper

A Taxonomy of Digital Threats

A framework for understanding digital threat types, attack tactics, and risk protection strategies

Why a Taxonomy of Digital Threats?

For most organizations, digital engagement means business. Customers expect to interact online with organizations through online portals, social media, and mobile apps. Today's institutions invest in digital platforms to compete for customers and maintain high levels of satisfaction.

However, law-abiding organizations are not the only ones that recognize the value of digital platforms. Cybercriminals exploit this new and expanding attack surface, deploying spoofed domains, bogus social media accounts, and fraudulent mobile applications to engage with the same customers. Hacktivists and malicious state actors spread false and misleading information through social media, web forums, and review sites.

These attacks are facilitated by a no-cost social landscape, low technical barriers, ease of target acquisition and payload delivery, and broad access to potential victims through these platforms. These factors have created new categories of digital risk, many of which were barely imagined ten years ago.

Leading industry analyst firms and security-conscious enterprises have recognized the seriousness of these risks and have given the name "Digital Risk Protection (DRP)" to the programs and technologies designed to address them. They now view DRP as a key element of information security and cyber risk management.

Unfortunately, the definitions and descriptions of the digital risk landscape and DRP offered so far are vague. They characterize digital risks as those related to "digital business processes," or define DRP as products and services to "reduce risks that emerge from digital transformation," or "secure your brand against digital security risks." These descriptions are not wrong, but they aren't much help if someone wants to understand the range of digital threats and the options available for protecting against them.

To provide greater clarity, ZeroFOX developed a taxonomy that provides a high-level view of four major categories of digital risks. This paper presents the taxonomy, drills down into specific threats in each category, and suggests DRP activities available to detect and neutralize those threats.

We believe that by reviewing this taxonomy, both technical and business-oriented readers will obtain a solid understanding of:

- Types of digital risk
- The impacts of each type
- Detection techniques
- Remediation options

The High-Level View: Four Broad Threat Categories

Our taxonomy of digital risk is based on four broad categories. Those categories, together with some of their key characteristics, are summarized in Table 1. (Those who wish to review the complete digital risk taxonomy before reading this section can turn to the end of this paper.)

Theft and financial fraud targeting customers and third parties involves cybercriminals motivated by financial gain who in some way impersonate the company, its brand, or its employees. The impacts on the enterprise are mostly indirect: no money comes out of the enterprise's budget. The indirect costs are very real, however, including loss of current and future revenue because of damage to reputation and trust. Also, financial institutions and others sometimes feel compelled to restore lost funds, even if they have no role in the fraud.

Attacks on reputation usually involve hacktivists motivated by ideological and political factors, or disgruntled customers or employees eager to disparage the enterprise. Impact is usually indirect, such as lost revenue from damage to reputation and expenses to counter misinformation.

Attacks against the enterprise and employees may involve cybercriminals motivated by financial gain, as well as state actors and business competitors seeking intellectual property (IP) or embarrassing information. They typically cause direct costs, such as funds siphoned from bank accounts, costs to notify customers of breaches, and fines for regulatory failures. But indirect costs can also be substantial, including lost revenue from damaged reputation and loss of competitive position stemming from stolen IP.

Emerging threats represent attacks that are in the discussion or planning stages. These include potential fraud schemes, cyberattacks, and attacks on reputation. They may also involve threats of protests and physical attacks against the enterprise's locations and employees.

The main difference between emerging threats and the other three categories is the threats have not yet been put into action, or are in the very early planning stages. That means they cannot be detected though direct evidence of ongoing or successful attacks like spear phishing emails, spoofed domains, or stolen data posted to the web. Instead, defenders must find statements of intention and evidence of preparations, such as disclosures of vulnerabilities, "attack chatter" on dark websites, or exploit kits for sale.

Obviously, there are overlaps between these four categories, and examples of threats that don't fit neatly in any of them. However, they illustrate the range of digital risks we face and help us think about how different types of threats can be detected and remediated.

Table 1. Summary of threat types, actors and motivations, and impacts

Threat Category	Threat actors and motivations	Impacts
Theft and financial fraud targeting customers and third parties	**Cybercriminals:** Financial gain	**Indirect:** Damage to reputation; Loss of sales **Direct:** Resolution of disputes
Attacks on reputation	**Hacktivists:** Ideology or politics **Disgruntled customers and employees:** Anger or revenge	**Indirect:** Damage to reputation; Loss of revenue **Direct:** Costs to counter misinformation
Attacks against the enterprise and employees	**Cybercriminals:** Financial gain **Competitors and state actors:** IP and embarrassing information	**Indirect:** Damage to brand; Loss of competitive position **Direct:** Breach notification costs; regulatory fines; disruption of operations
Emerging threats	Various	Indirect and direct costs in the future

Theft and Financial Fraud Targeting Customers and Third Parties

The taxonomy's first threat category, "Theft and financial fraud targeting customers and third parties," breaks down into three specific types of threat:

- Financial fraud
- Counterfeiting and piracy
- Identity theft and credential stealing

Table 2 lists examples of tactics used in each threat, impacts on the business and its customers, examples of how they can be detected, and some of the ways they can be blocked and remediated.

I Want My Discount! Fake Coupons Cost Retailer $1.5 Million

The Threat

In a case of brand impersonation, a major online retailer was victimized when cybercriminals blasted thousands of fake coupons across Facebook and Twitter. Customer dissatisfaction, loss of reputation, and operational issues resulted in the loss of over $1.5 million in revenue.

What Can Be Done?

Use scam classifiers and machine learning to identify fake coupons on social media sites like Instagram and Twitter, so the malicious posts can be taken down. Identify and remove fraudulent Facebook accounts that promote the scams.

Table 2: Details of threat types in the "Theft and financial fraud targeting customers and third parties" category

Threat Type	Examples of Tactics	Impacts	Examples of Detection Techniques	Examples of Remediation
Financial fraud	Spoofed websites and social media accounts; Phishing campaigns; Social media account takeover; Fake mobile apps; Spoofed domains (i.e. typosquatting)	Loss of trust; Loss of revenue; Damage to brand	Monitor domain registries; Scan social media sites for names and logos; Monitor app stores; Check owned social media accounts for unauthorized changes	Take down fraudulent websites and social media accounts; Notify app stores of fake mobile apps; Freeze owned accounts and delete harmful content
Counterfeiting and piracy	Counterfeit goods in online marketplaces; Fraudulent coupons; Spoofed websites and social media accounts; Phishing campaigns	Resolution and liability costs; Loss of revenue; Damage to brand	Scan social media sites and online marketplaces for fraudulent goods, ads and coupons; Investigate claims and bad reviews	Take down fraudulent websites and ads; Notify hosts and law enforcement of counterfeiting and piracy
Identity theft and credential stealing	Impersonating social media accounts and account takeover; Information-stealing malware; Phishing campaigns	Cost of credit reporting for customers and other resolution costs; Loss of trust; Damage to brand	Monitor dark web for "sales chatter"; Scan web and social media for evidence of credential harvesting attacks	Take down fraudulent ads, websites, and social media accounts

Financial fraud

Financial fraud targeting customers and third parties usually involves impersonating the company, brand, or employees to convince customers or third parties to divulge account credentials or send money, without providing any goods or services in return.

Examples are:

- Spoofed websites that resemble the enterprise's actual website
- Spoofed domains that employ "typosquatting"; that is, URLs that look like the enterprise's URL but differ by one or two characters
- Spoofed social media accounts that resemble actual accounts of the enterprise on Facebook, Twitter, and other social media platforms
- Enterprise social media accounts that have been "taken over" (compromised) by an attacker
- Emails and social media messages that appear to come from the enterprise
- Fake mobile apps purportedly from the enterprise

These tools are often mixed and matched. For example, an email phishing campaign or a compromised social media account might send customers to a spoofed website that takes credit card payments for non-existent merchandise.

Unfortunately, customers and others often hold the enterprise responsible for their losses, even if the fraud was perpetrated without ever touching the enterprise's applications or social media accounts. The impacts include damage to reputation and loss of trust, which result in lost revenue when customers turn to competitors.

Detection

Frauds and scams against customers and third parties can be detected through techniques such as:

- Monitoring domain registries for new domains that resemble the enterprise's
- Monitoring domain registries owned by the enterprise for modifications of account contact details (for example, a new admin email) or transfer of ownership
- Scanning social media sites for the enterprise's name, keywords, trademarks and logo and the names and photos of executives
- Checking the enterprise's social media accounts to detect account take-overs
- Scanning app stores to find bogus mobile apps

Remediation

If taken over enterprises can reclaim their owned social media accounts. They can also send requests web hosting companies, social media platforms, and app stores to take down fraudulent websites, spoofed social media accounts, and fake mobile apps.

Taking down fraudulent websites and social media accounts is extremely labor-intensive work, especially at scale. Every service provider has its own request and removal process, and requirements for evidence vary widely. One option is to use automated services from DRP solution providers such as ZeroFOX that leverage API-based connections to hundreds of hosting and social network platforms.

Counterfeiting and piracy

Counterfeiting and piracy represent special cases of financial fraud against customers with a few unique twists. For example, retailers and entertainment companies are plagued by spoofed websites that sell knockoffs of clothing and merchandise and pirated content such as software, games, movies, music, and other streaming content. Another major problem is fake coupons, often distributed on Twitter, Instagram, and other social media platforms.

Counterfeit goods and fake coupons can have a devastating effect on company reputation and revenue, because many victims are unaware that they have been scammed and believe the merchant has defrauded them through incompetence or malice.

Detection

Detection techniques are very similar to ones enumerated above for financial fraud, but there are some variations. For example, it is possible to:

- Search social media sites for product names and images
- Search web and social media sites for fraudulent coupons on the web and social media sites
- Scan online forums, review services, and social media sites for complaints and bad reviews of products

Remediation

When counterfeiting and piracy are detected, remediation options include:

- Taking down fraudulent ads and websites
- Taking down fraudulent postings on social media
- Notifying hosts and law enforcement agencies of counterfeiting
- Educating customers on how to identify and avoid knock-offs and fraudulent coupons

Identity theft and credential stealing

Today cybercriminals can easily profit from stolen credit card numbers, account numbers, login credentials, and other forms of personal information. They can use the data for identity theft and impersonation scams, or sell the personal information to other cybercriminals and hackers on dark web sites.

These attacks can target any enterprise that collects confidential personal information. For example, there have been examples of cybercriminals:

- Impersonating the social media accounts and websites of staff recruiting firms, posting fake jobs (or reposting the descriptions of real jobs on the real recruiter's site), and harvesting the personal information of job applicants to use for identity theft
- Running phishing campaigns to send victims to a website resembling that of a well-known law firm and gathering personal and financial information

Detection

In addition to using the detection methods listed above for financial fraud, enterprises can uncover identity theft and credential stealing by:

- Monitoring the open web and social media for ads, offers, and emails that appear to come from the enterprise but are in fact being used by threat actors to harvest personal information and credentials
- Monitoring hacker forums and other dark web locations for "sales chatter" about customer data, credit cards and credentials for sale

Remediation

When searches detect activity on the web and social media designed to acquire or market stolen information and credentials, enterprises can act to take down those websites and postings.

In addition, when searching uncovers customer and employee data and credentials for sale, it may be possible to trace that data back to its source, such as:

- A phishing campaign
- Information-stealing malware
- Fraudulent mobile applications
- Spoofed (typosquatting) domains
- A vulnerability or exposed system on the enterprise's network

In addition to taking down fraudulent websites and postings, enterprises can use this information to:

- Provide information to malware reporting forums and cybersecurity product vendors so they can distribute malware signatures and IP addresses used in attacks and block attacker profiles
- Contact web stores and download sites so they can remove fraudulent mobile applications
- Harden their own infrastructure by eliminating vulnerabilities and adding monitoring and security controls to systems to defeat future attacks

There Are Not Enough Hours In The Day

The Threat

A major financial services provider knew that cybercriminals were continuously launching phishing campaigns against its customers, pointing them to look-alike web pages impersonating the company's website. They were also seeing suspicious activity around their owned social media accounts. Unfortunately, using simple keyword searches to find evidence of these attacks generated tens of thousands of unfiltered alerts each week. There simply weren't enough hours in the day to investigate all the alerts.

What Can Be Done?

Identify a list of unique entities, names, images, hashtags, key phrases, and other data that need to be protected. Use advanced search technology and machine learning to automate the search process, incorporate context, and flag a small number of alerts that represent real priority threats to the company and its customers.

Attacks on Reputation

Attacks on reputation are usually perpetrated by ideologically or politically-driven hacktivists, disgruntled customers, competitors, or nation state organizations targeting an industry or trying to undermine the economy and political stability of other countries. An organization's reputation can also be damaged by employees and other insiders posting controversial opinions, offensive content, and confidential information. Table 3 summarizes some of their key characteristics.

Today, Anything Can Be Controversial

The Threat

A prestigious Ivy League university is constantly at risk from malicious attacks on its reputation by outsiders – sometimes inflamed by controversial statements and activities within its own community. Offensive or just insensitive social media posts by students and faculty, the announcement of new research findings, admissions policies, fake diploma scams, even athletic events, can generate adverse publicity and threats of violence and damage the university's standing in the eyes of students, faculty, alumni, donors, and other key constituencies.

What Can Be Done?

Search the very wide range of social media platforms and web forums used by students and faculty and alert administrators to threats and problematic statements. Use natural language processors and machine learning to find potential threats in dozens of languages (because the university has students and faculty from all over the world). Create a system that can rapidly escalate violence-related alerts to the campus security team or authorities.

Table 3: Details of attacks on reputation

Threat Type	Examples of Tactics	Impacts	Examples of Detection Techniques	Examples of Remediation
Attacks on reputation	Posting fake or negative reviews; Posting false information in online forums; Account take-overs where attacker slanders the brand, org, employees, or 3rd parties. Creating social media accounts to disseminate misleading information; Insiders posting offensive content	Loss of revenue; Damage to re-lationships with business partners and government agencies; Ill-will within customer or constituent base. Costs to counter misinformation	Monitor review websites; Scan the web for product names, logos, and images; Scan social media for imper-sonations of the company and executives and for insiders violating company policies	Take down fraudulent websites and social media accounts; Noti-fy review sites, online forums, and social media platforms; Counter or moderate false and offensive information

These actors may disparage or disseminate misinformation about the enterprise, specific products, and executives and other employees. They may also impersonate the enterprise or its executives to distribute misinformation or portray executives as having controversial or morally repugnant views. Methods to perpetrate attacks on reputation include:

- Posting false, offensive, or misleading information on product review websites
- Posting false, offensive, or misleading information on legitimate social media accounts and online forums
- Creating fraudulent websites and social media accounts spoofing those of the enterprise, an executive, a news organization, a government agency, or an independent expert, and using those as platforms to disseminate false or offensive information
- Taking over social media accounts of the enterprise or its executives to post false or misleading information or controversial or abhorrent opinions

The impact of attacks on reputation can include loss of revenue and damage to relationships with suppliers, business partners, government agencies, and regulatory agencies. Enterprises can also be compelled to spend money on public relations crisis management activities and generally countering misinformation.

Of course, attacks on the reputation of an enterprise and its products can be factually correct or expressions of opinion that represent free speech. What we are talking about in this section is countering false and deliberately misleading information.

Detection

Techniques to detect attacks on reputation include:

- Scanning review websites, social media sites, and online forums for the enterprise's name, keywords, trademarks and logo, product names and images, and the names, profiles and photos of executives
- Monitoring the web and social media for sites and accounts impersonating the enterprise and its executives
- Searching for postings by insiders that contain confidential information or violate company policies
- Monitoring the enterprise's own websites and social media accounts for false and misleading information posted in reviews, online forums, and comments areas
- Monitoring for unauthorized changes to admin permissions that may indicate attempted account takeover
- Monitoring the enterprise's own websites and social media accounts to detect account takeovers

Remediation

Steps to remediate attacks on reputation include:

- Taking down fraudulent websites and social media accounts
- Notifying review sites, online forums, and social media platforms about phony reviews, false and misleading information, abusive and politically-motivated attacks, and other violations of their service terms policies
- Removing false, offensive, and misleading information from the enterprise's social media accounts and websites
- Reclaiming the enterprises social media accounts that have been taken over

Free speech and appropriate response

Many posts that attack enterprises are factually accurate or protected by free speech (as defined by the laws of the country and the policies of the platform provider). Usually these cannot be removed if they don't violate the terms of service of the platform. However, identifying and analyzing reputational attacks and criticism gives enterprises an opportunity to:

- Clarify misunderstandings
- Respond to misleading criticisms
- Remedy legitimate complaints
- Obtain intelligence on customer and community perceptions (i.e., sentiment analysis)
- Gather data to improve public relations and marketing activities, service delivery, and product planning

Attacks Against the Enterprise and Employees

The taxonomy's third threat category, "Attacks Against the Enterprise and Employees," breaks down into four types of threats, as shown in Table 4.

Table 4: Details of threat types in the "Cyberattacks against the enterprise and employees" category

Threat Type	Examples of Tactics	Impacts	Examples of Detection Techniques	Examples of Remediation
Theft of employee data and credentials	Spoofed websites and social media accounts; Phishing campaigns; Social media account takeover; Information-stealing malware; Fake mobile apps; Spoofed domains (typosquatting)	Loss of trust; Increased exposure to additional attacks	Monitor dark web for "sales chatter"; Monitor forums for related ads	Deactivate impacted accounts; Revoke compromised credentials; Strengthen security controls; Block phishing attacks; Improve employee training
Theft of customer data (including credit card and financial account data)		Loss of trust; Damage to brand; Regulatory fines; Cost of credit reporting for customers	Monitor dark web for "sales chatter" and card dumps; Scan web and social media for evidence of credential harvesting attacks	Deactivate impacted accounts; Revoke compromised credentials; Strengthen security controls; Provide credit monitoring
Theft of IP, media content, and software		Loss of revenue; Damage to brand; Loss of competitive position	Monitor dark web for "sales chatter"; Monitor online marketplaces for product listings and ads; Monitor code sharing sites	Remove counterfeit and pirated media content from marketplaces and websites; Remove IP and code from forums and code sharing sites; Notify law enforcement of piracy and copyright infringement; Strengthen security controls
Capture of infrastructure information		Increased exposure to additional attacks	Monitor dark web for "sales chatter" and discussions of vulnerabilities	Prioritize patching and elimination of vulnerabilities on targeted infrastructure; Strengthen security controls

Because these threat types will be all too familiar to our readers, we will not discuss them in detail here. Instead, we will outline some of the detection and remediation activities that can be performed outside of the enterprise's network.

Detection

Several types of evidence on the web can point toward ongoing cyberattacks against the enterprise and its employees:

- Fraudulent websites, social media accounts, and online ads used in phishing and other attacks to lure employees and customers and harvest their confidential data and credentials
- Websites, hacker forums, card dumps, and "chatter" on the dark web selling customer and employee data, credit card and financial account numbers and data, or discussing vulnerabilities in the infrastructure of the enterprise
- IP and pirated news and media content (including games, music, movies, and copyrighted books and articles) for sale on the open and dark web
- Stolen or inadvertently disclosed software in paste bins and public software repositories like GitHub

Enterprises can monitor these locations, searching for indicators such as company, product, employee, and customer names, account numbers and other data associated with the enterprise, keyword text strings and images from IP and proprietary content, and code snippets.

Remediation on the web

Remediation for this category of cyberattacks mostly involves eliminating vulnerabilities, educating employees, and improving security controls on the enterprise's network and systems.

However, most of these activities take time. Also, improving security controls won't protect information and IP already loose on the web (although finding such information may provide advance warning of pending attacks). There are many situations where enterprises can staunch the bleeding by:

- Taking down fraudulent websites, social media accounts, and online ads used to perpetrate and monetize the attacks
- Notifying forums and ISPs of fraudulent activities, copyright infringements, stolen IP, and other violations of their policies, so they can remove offending materials and shut down websites involved in selling stolen data, content, and software

Emerging Threats

Our final category is emerging threats, meaning threats that are being discussed or planned but have not yet been employed in actual attacks. These overlap with the other three threat categories, but there is an important difference: evidence such as fraudulent websites, spoofed social media accounts, and stolen information have not yet appeared. Enterprises must search for statements of intention or attack tools still under development.

Evidence of emerging threats can be divided into two types:

- Statements of intention and evidence of attack planning targeting the enterprise or its executives, industry, or locations
- Discussions of vulnerabilities and the development and sale of tools to exploit them

These are summarized in Table 5.

Situational awareness

The first type, evidence of attack planning, includes information important to a topic we have not yet discussed: physical security and what is often called "situational awareness." Many physical threats first manifest on social forums. For example, web forums might include threats against an executive, or warn about a protest march targeting one of the enterprise's sites.

These early warnings are invaluable for corporate security staffs. They allow them to take protective measures, including avoidance, which are far more safe and effective than reacting to crises as they happen.

Detection

Attack planning can be monitored by scanning forums on the dark web used by hackers and hacktivists and for references to the enterprise and its products, executives, industry, locations, and other relevant terms.

The same forums can also be monitored for discussions of vulnerabilities and the exploits and zero-day attacks that might affect the enterprise based on the software applications it uses and the servers, networking equipment, and cloud platforms that make up its infrastructure. This type of searching can also be extended to development and code sharing sites where malware and exploit kits are developed and sold.

Remediation

Early warning allows enterprises to take protective measures against physical threats, and to prioritize activities for hardening systems and infrastructure.

The Difference Between Concerns And Crises

The Threat

A major media company was tired of crisis management. It's goal was to identify risks proactively and head them off before an attack was launched, a brand crisis snowballed, content was pirated and sold on the web, a technical vulnerability was exploited, or a threat of physical violence was carried out.

What Can Be Done?

Monitor the widest possible range of social media platforms and dark web sites to find "chatter" mentioning the company and its business units, shows, broadcast and online channels, executives, and locations. Cross-reference data against information from other business units and cyber threat intelligence. User artificial intelligence to highlight alerts with the highest immediacy and risk.

Table 5: Details of threats in the "Emerging threats" category

Threat Type	Examples of Tactics	Impacts	Examples of Detection Techniques	Examples of Remediation
Statements of intent and attack planning	Threats against enterprises and industries; Efforts to recruit participants for cyberattacks; Discussion of protests and physical attacks	Potential for damage to brand, damage to personnel and facilities, loss of revenue, etc.	Monitor attacker discussion forums and public social posts for mentions of the enterprise, brands, and executives	Prioritize activities to strengthen security controls; Prepare for or avoid physical threats
Discussions of vulnerabilities and attack tools	Forum discussions of attack techniques and tools; Sales of exploit kits; Offers for infrastructure or services used in attacks	Increased risk of all types of cyberattacks	Monitor attacker discussion forums; Monitor development and code sharing sites	Prioritize activities to harden systems, accelerate patching, and strengthen other security controls

The ZeroFOX Digital Risk Taxonomy Summary

Threat Category	Threat Type	Examples of Tactics	Impacts	Examples of Detection
Theft and financial fraud targeting customers and third parties	Financial fraud	Spoofed websites and social media accounts; Phishing campaigns; Social media account takeover; Fake mobile apps; Spoofed domains (i.e. typosquatting)	Loss of trust; Loss of revenue; Damage to brand	Monitor domain registries; Scan social media sites for names and logos; Monitor app stores; Check owned social media accounts for unauthorized changes
	Counterfeiting and piracy	Counterfeit goods in online marketplaces; Fraudulent coupons; Spoofed websites and social media accounts; Phishing campaigns	Resolution and liability costs; Loss of revenue; Damage to brand	Scan social media sites and online marketplaces for fraudulent goods, ads and coupons; Investigate claims and bad reviews
	Identity theft and credential stealing	Impersonating social media accounts and account takeover; Information-stealing malware; Phishing campaigns	Cost of credit reporting for customers and other resolution costs; Loss of trust; Damage to brand	Monitor dark web for "sales chatter"; Scan web and social media for evidence of credential harvesting attacks
Attacks on reputation	Attacks on reputation	Posting fake or negative reviews; Posting false information in online forums; Account takeovers where attacker slanders the brand, org, employees, or 3rd parties; Creating social media accounts to disseminate misleading information; Insiders posting offensive content	Loss of revenue; Damage to relationships with business partners and government agencies; Ill-will within customer or constituent base. Costs to counter misinformation	Monitor review websites; Scan the web for product names, logos, and images; Scan social media for impersonations of the company and executives and for insiders violating company policies; Monitor owned-domains for attempted takeovers

The ZeroFOX Digital Risk Taxonomy Summary

Threat Category	Threat Type	Examples of Tactics	Impacts	Examples of Detection
Attacks against the enterprise and employees	Theft of employee data and credentials	Spoofed websites and social media accounts; Phishing campaigns; Social media account takeover; Information-stealing malware; Fake mobile apps; Spoofed domains	Loss of trust; Increased exposure to additional attacks	Monitor dark web for "sales chatter"; Monitor forums for related ads
	Theft of customer data (including credit card and financial account data)		Loss of trust; Damage to brand; Regulatory fines; Cost of credit reporting for customers	Monitor dark web for "sales chatter" and card dumps; Scan web and social media for evidence of credential harvesting attacks
	Theft of IP, media content, and software		Loss of revenue; Damage to brand; Loss of competitive position	Monitor dark web for "sales chatter"; Monitor online marketplaces for product listings and ads; Monitor code sharing sites
	Capture of infrastructure information		Increased exposure to additional attacks	Monitor dark web for "sales chatter" and discussions of vulnerabilities
Emerging threats	Statements of intent and attack planning	Threats against enterprises and industries; Efforts to recruit participants for cyberattacks; Discussion of protests and physical attacks	Potential for damage to brand, damage to personnel and facilities, loss of revenue, etc.	Monitor attacker discussion forums and public social posts for mentions of the enterprise, brands, and executives; Monitor for look-alike domain registrations and changes to owned-domain contacts
	Discussions of vulnerabilities and attack tools	Forum discussions of attack techniques and tools; Sales of exploit kits; Offers for infrastructure or services used in attacks	Increased risk of all types of cyberattacks	Monitor attacker discussion forums; Monitor development and code sharing sites

About ZeroFOX

ZeroFOX, the market leader in social media & digital protection, safeguards modern organizations from dynamic security, brand and physical risks across social, mobile, web and collaboration platforms. Using diverse data sources and artificial intelligence-based analysis, the ZeroFOX Platform identifies and remediates targeted phishing attacks, credential compromise, data exfiltration, brand hijacking, executive and location threats and more.

The patented ZeroFOX SaaS technology processes and protects millions of posts, messages and accounts daily across the social and digital landscape, spanning LinkedIn, Facebook, Slack, Twitter, Instagram, Pastebin, YouTube, mobile app stores, the deep & dark web, domains and more.