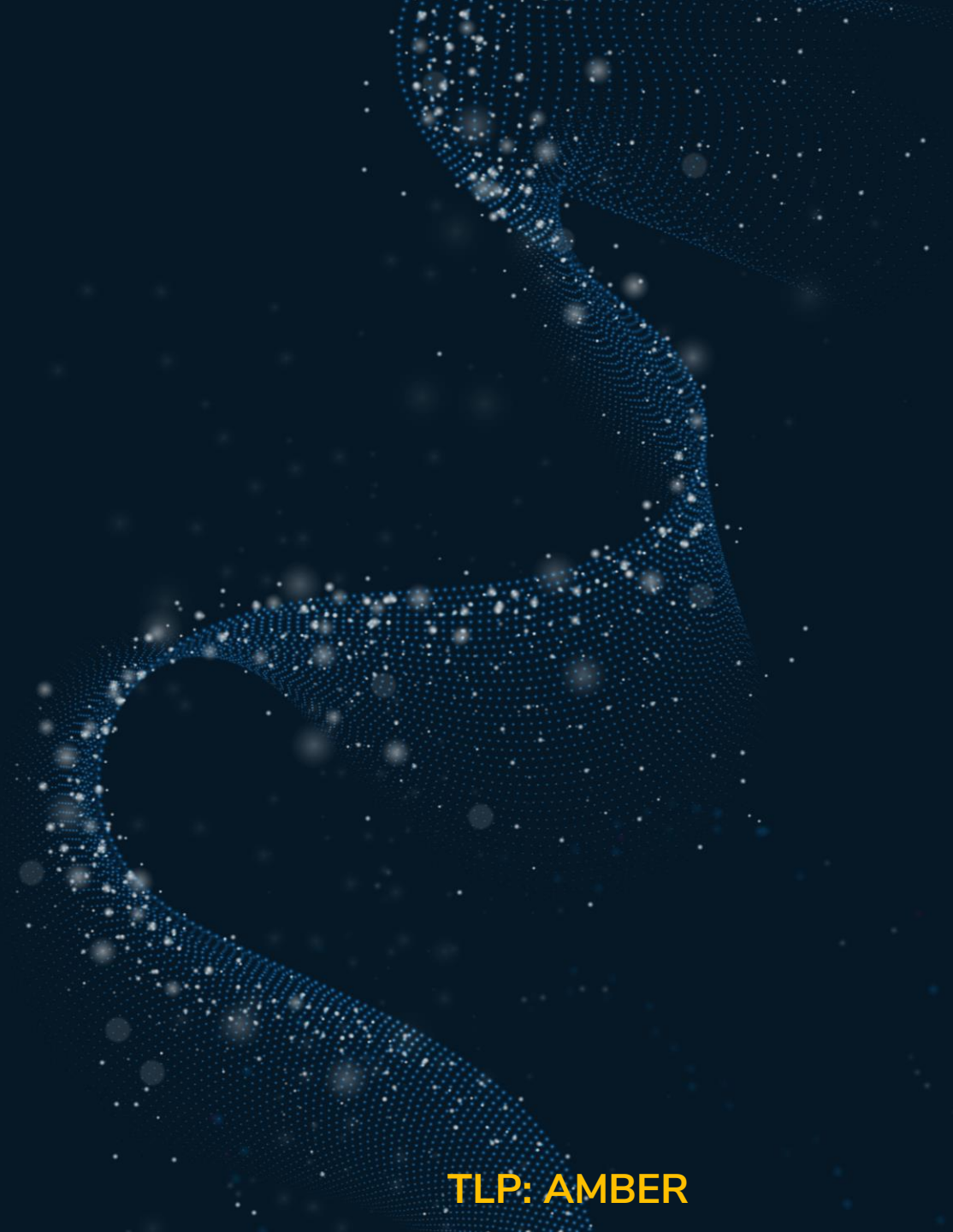
KROLL

CTI Spotlight Trends Report

December 2023 and Year End



TLP: AMBER

Methodology

- Kroll CTI monthly spotlights are based on intelligence from Kroll's cyber incident response engagements where we are engaged to respond, manage, or mitigate a cybersecurity incident. Kroll's incident response work is informed by intelligence gained from the 3,000+ engagements handled per year by the Kroll Cyber Risk team.
- Data is collected and processed by the Kroll Cyber Threat Intelligence team during the initial scoping intake as well as during the lifecycle of a Kroll engagement.
- Kroll currently reports on data on a monthly and quarterly basis through the monthly spotlights and Quarterly Threat Landscape reports.

December 2023 Spotlight Trends Report

TLP: AMBER

Key Takeaways

Initial Access Methods

- **Phishing - Link** (44%)
- **Valid Accounts - Insider** (15%)
- **Valid Accounts - Externally Exposed** (12%)
- **Phishing - Attachment** (12%)

Most Impacted Sectors

- **Professional Services** (21%)
- **Healthcare** (14%)
- **Manufacturing** (13%)
- **Financial Services** (12%)

Top Ransomware Variants

- **LOCKBIT** (28%)
- **AKIRA** (17%)
- **PLAY** (11%)

Top Threat Incident Types

- **Email Compromise** (50%)
- **Ransomware** (22%)
- **Insider Threat** (8%)

Sector Analysis

December 2023

PROFESSIONAL SERVICES IS THE MOST IMPACTED INDUSTRY SECTOR THROUGHOUT DECEMBER 2023

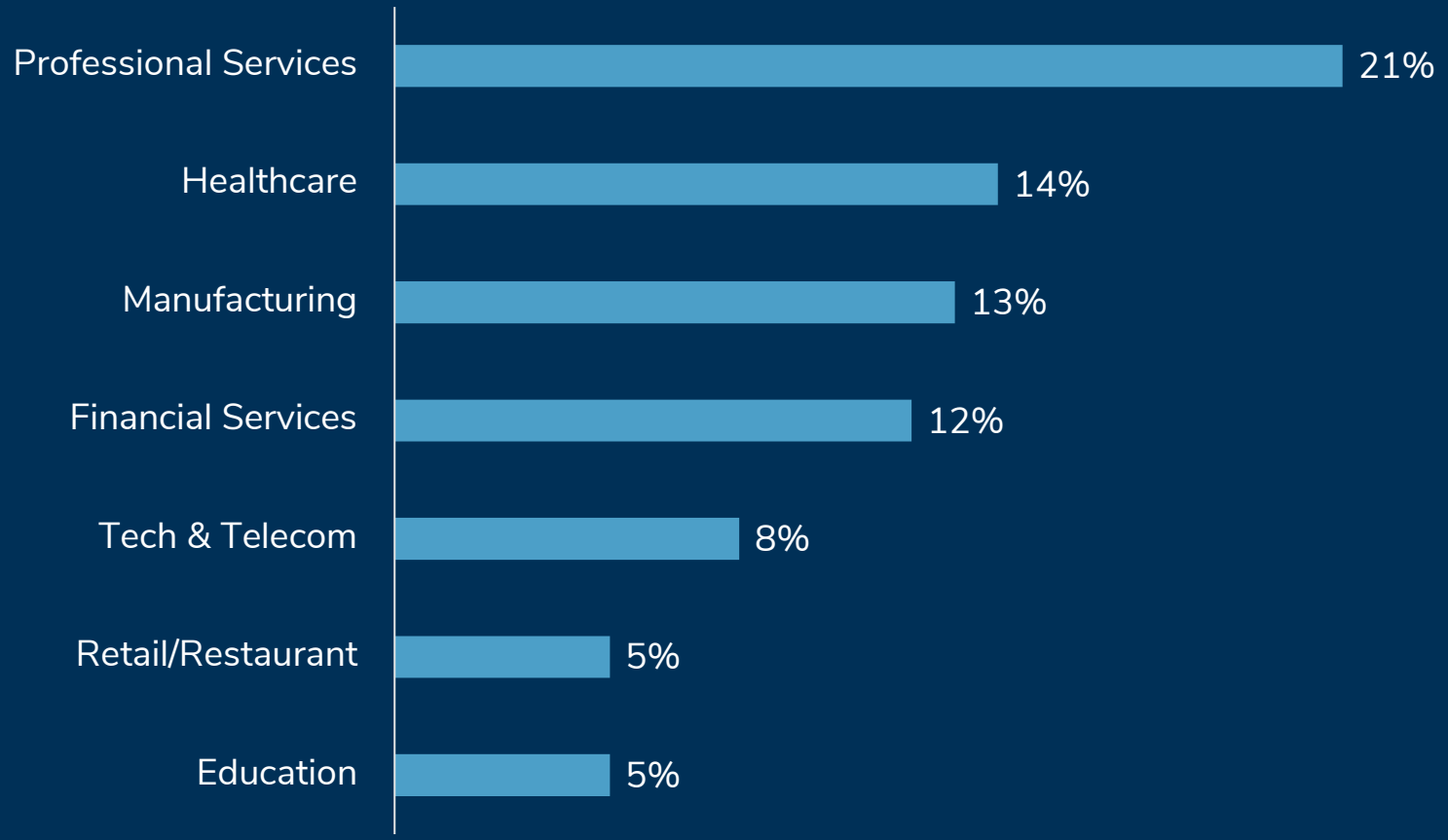
- **Email Compromise** was the top threat incident type impacting the professional services sector.
- In December, threats against the professional services sector most often involved **Phishing - Link** as the initial access method.

HEALTHCARE AND MANUFACTURING WERE THE 2nd and 3rd MOST IMPACTED SECTORS IN DECEMBER 2023

- **Email Compromise** was the top reported threat incident type impacting the Healthcare sector.
- **Ransomware** and **Email Compromise** were tied for the top reported threat incident type impacting the Manufacturing sector.

Incidents by Sector

Top 7 impacted industries

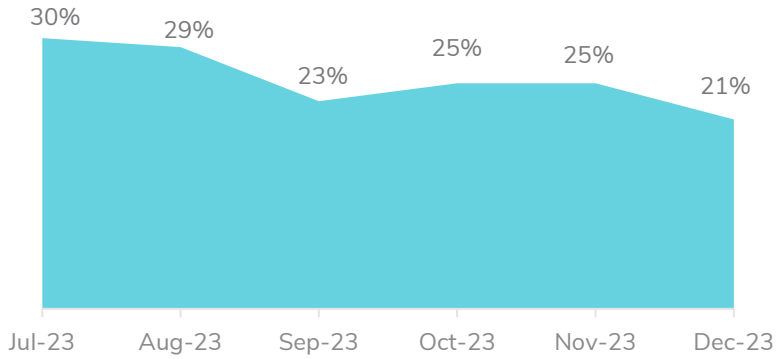


TLP: AMBER

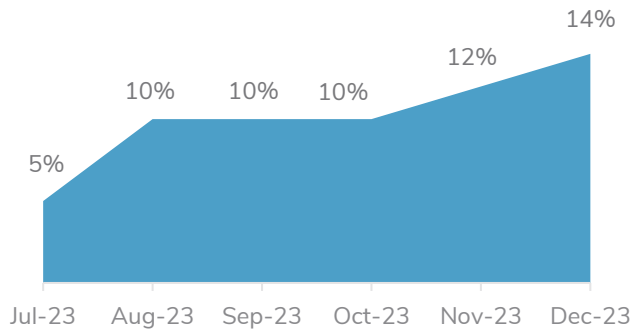
Most Impacted Sectors

Previous 6 Months

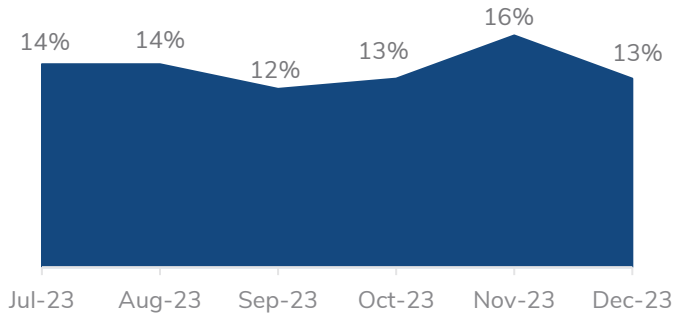
Professional Services



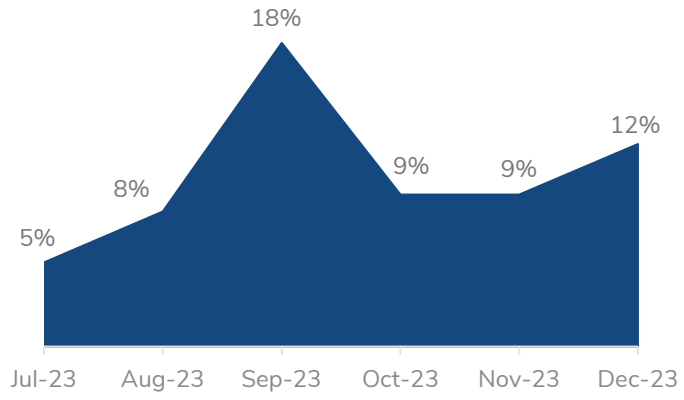
Healthcare



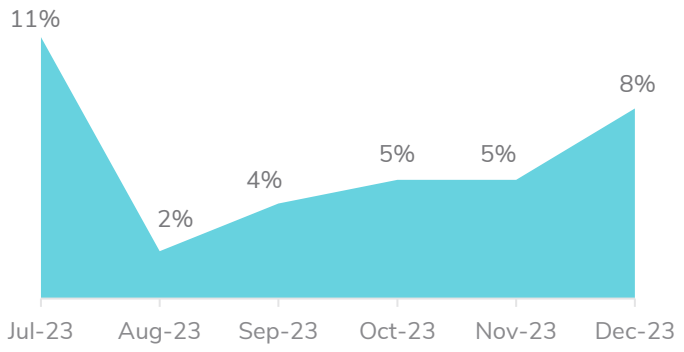
Manufacturing



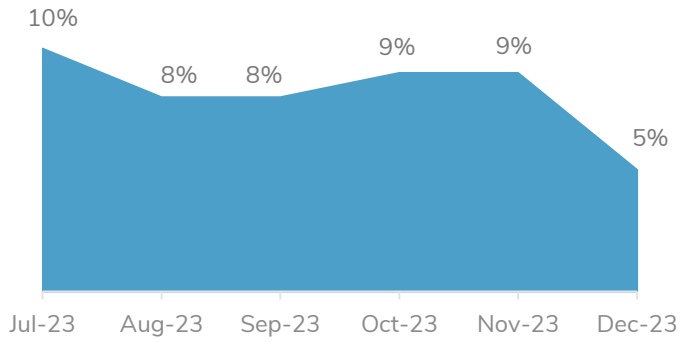
Financial Services



Tech & Telecom

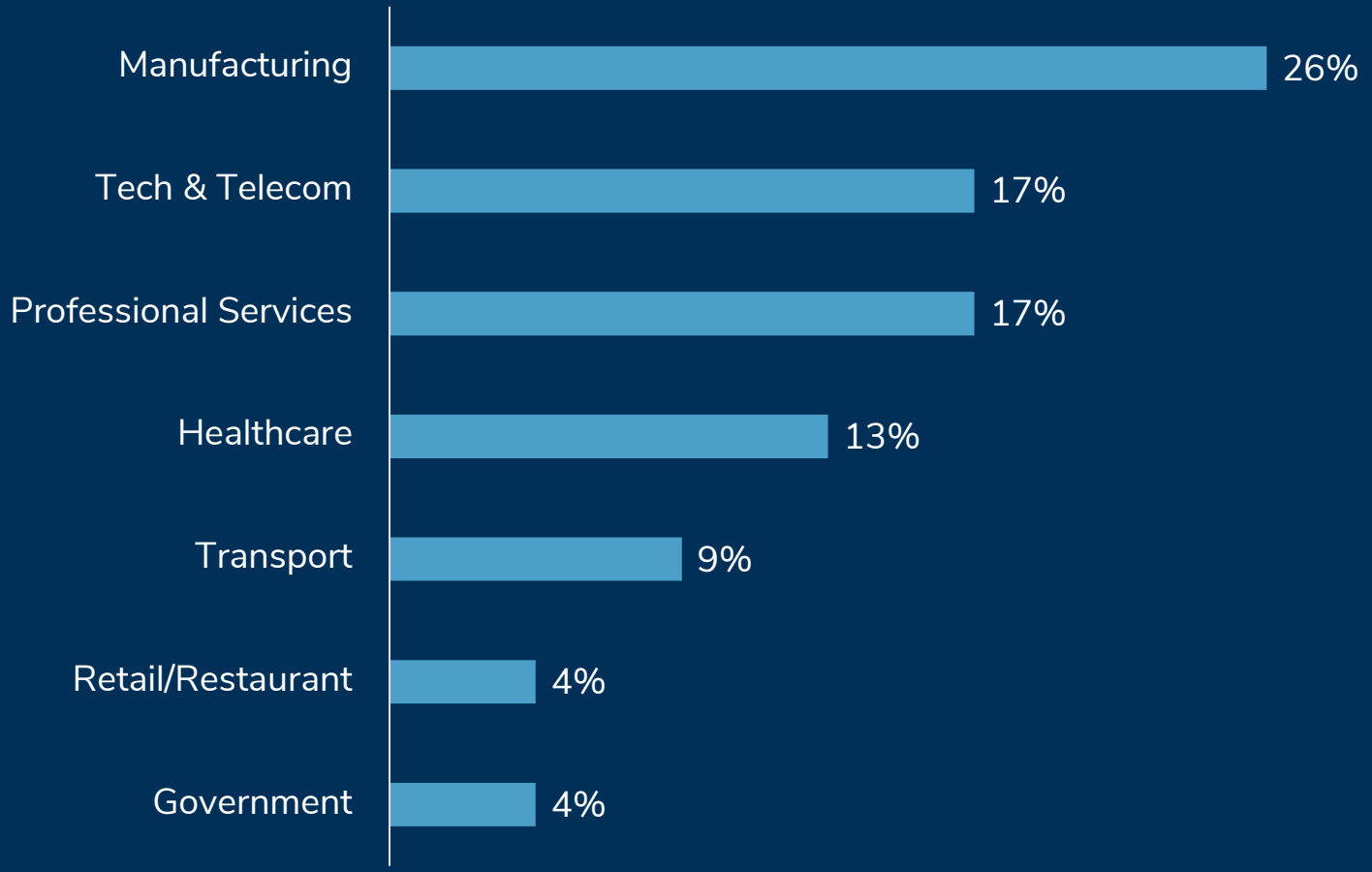


Retail/Restaurant



Ransomware – Top Impacted Sectors

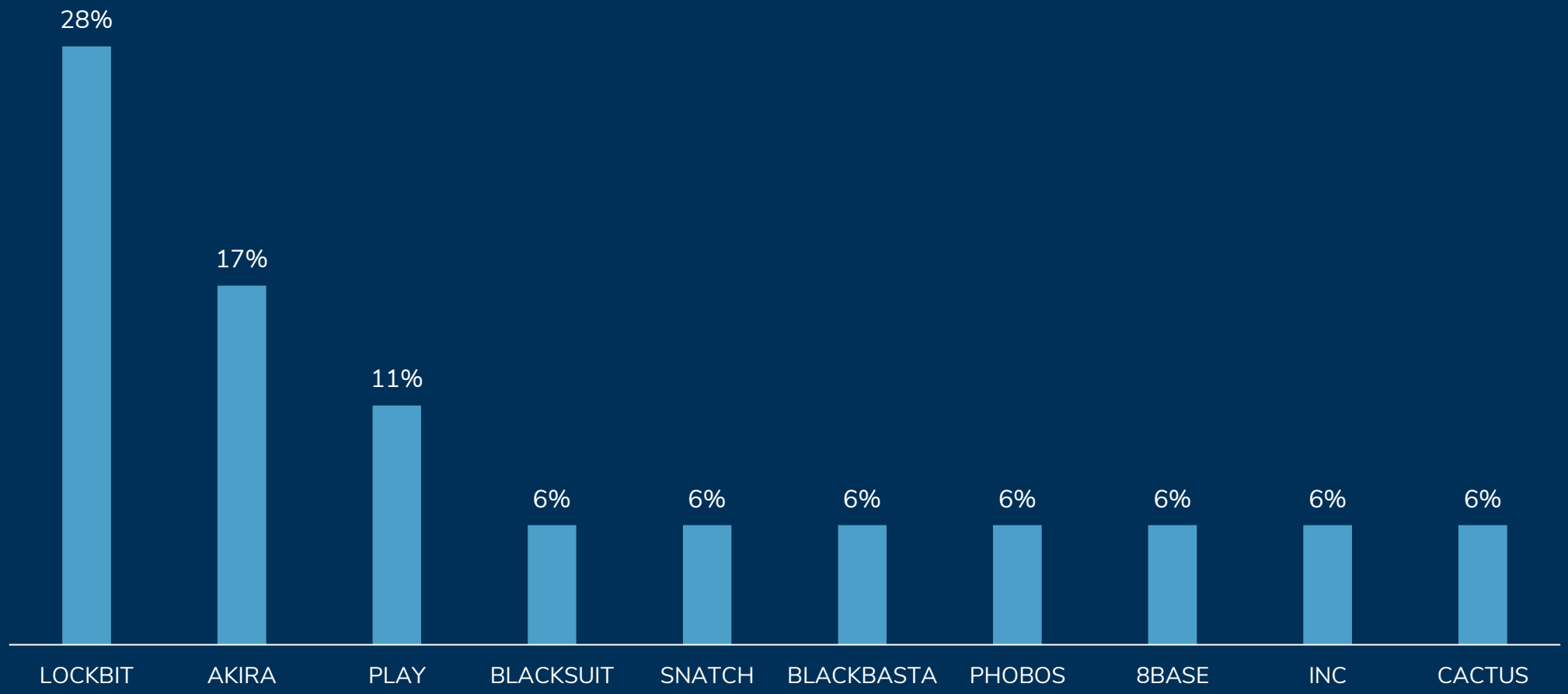
December 2023



TLP: AMBER

Top Ransomware Variants

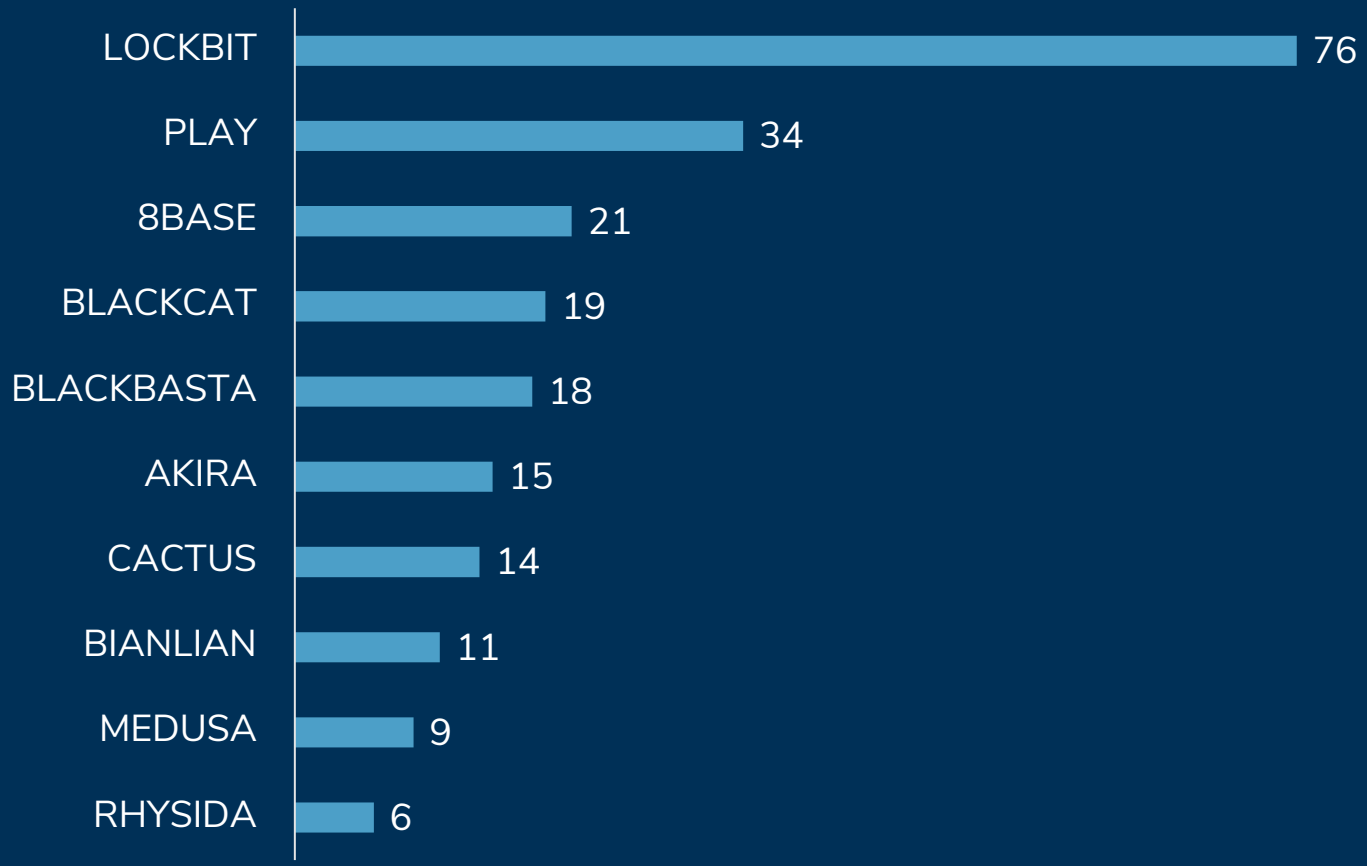
December 2023



TLP: AMBER

Ransomware – Actor-Controlled Site Listings

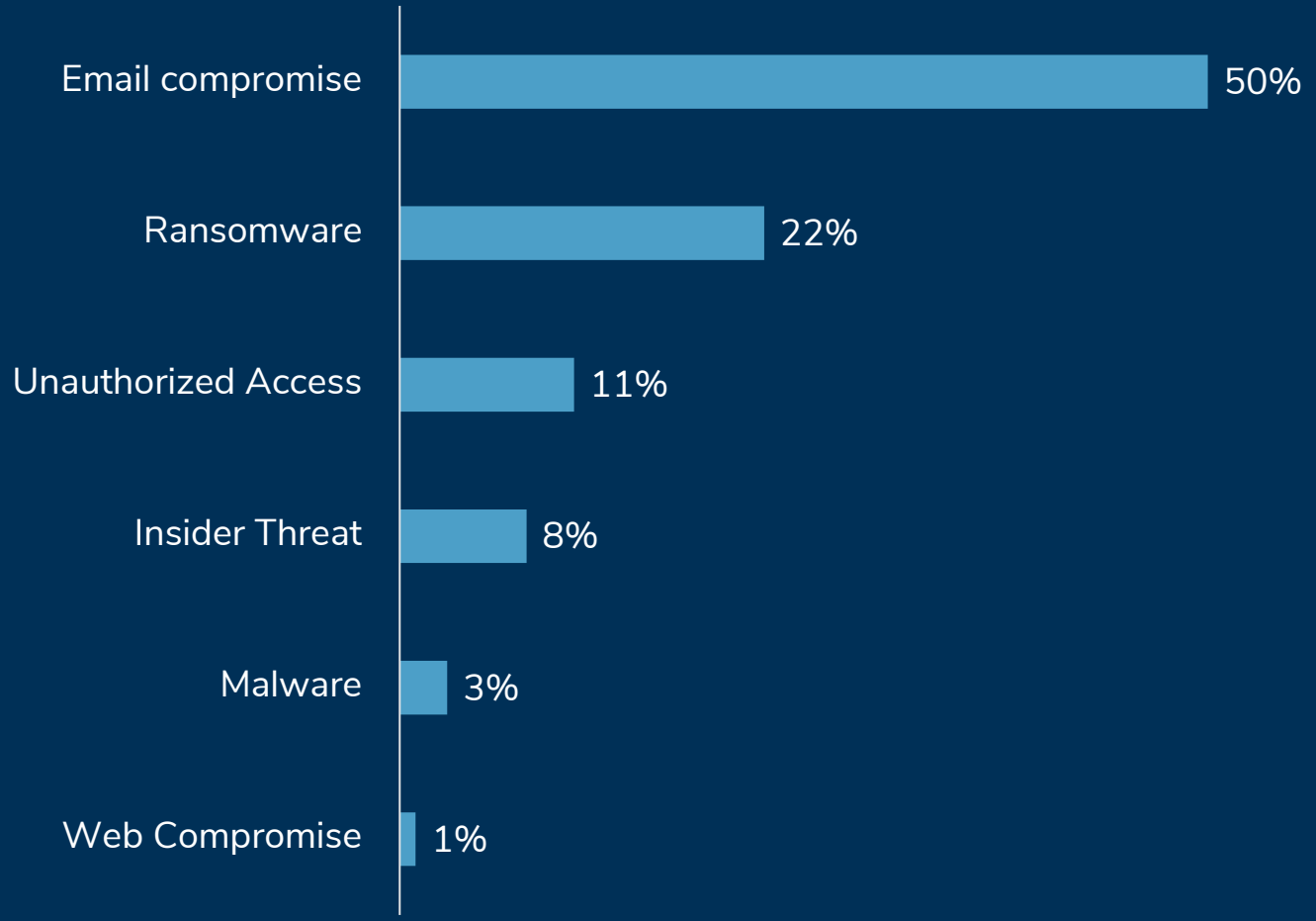
December 2023



TLP: AMBER

Incidents by Threat Type

December 2023



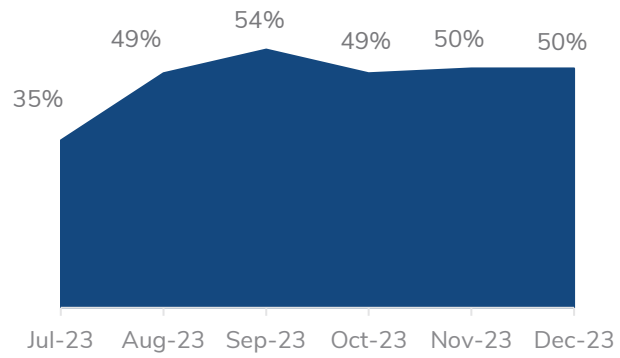
*Unauthorized Access represents a summation of Unauthorized Access - Network and Unauthorized Access - Cloud / Repository Access

TLP: AMBER

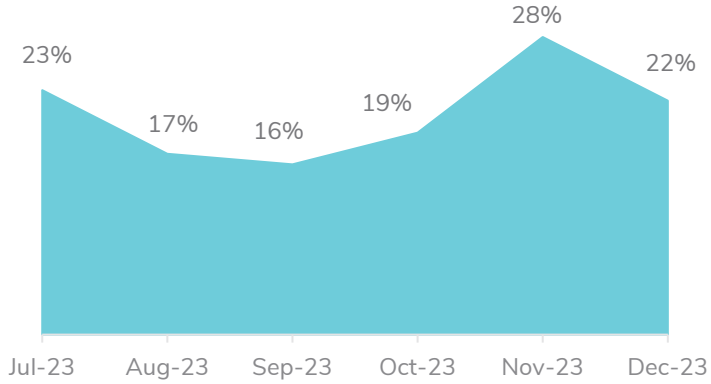
Threat Type Trends

Previous 6 Months

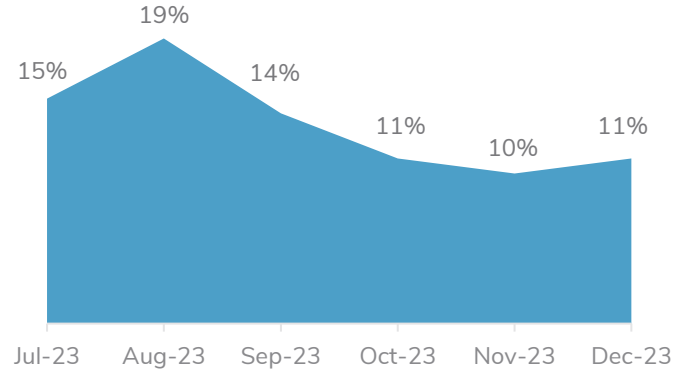
Email Compromise



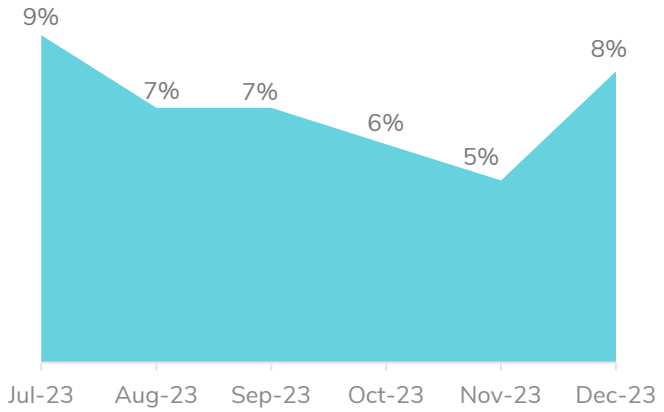
Ransomware



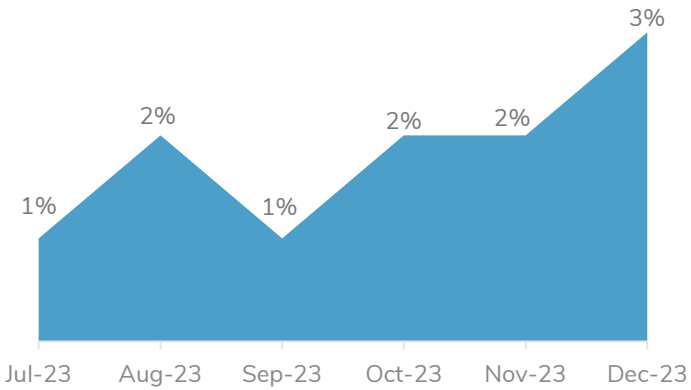
Unauthorized Access



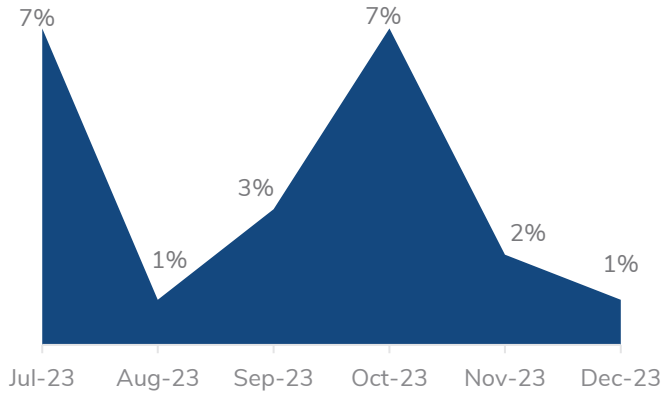
Insider Threat



Malware - Other



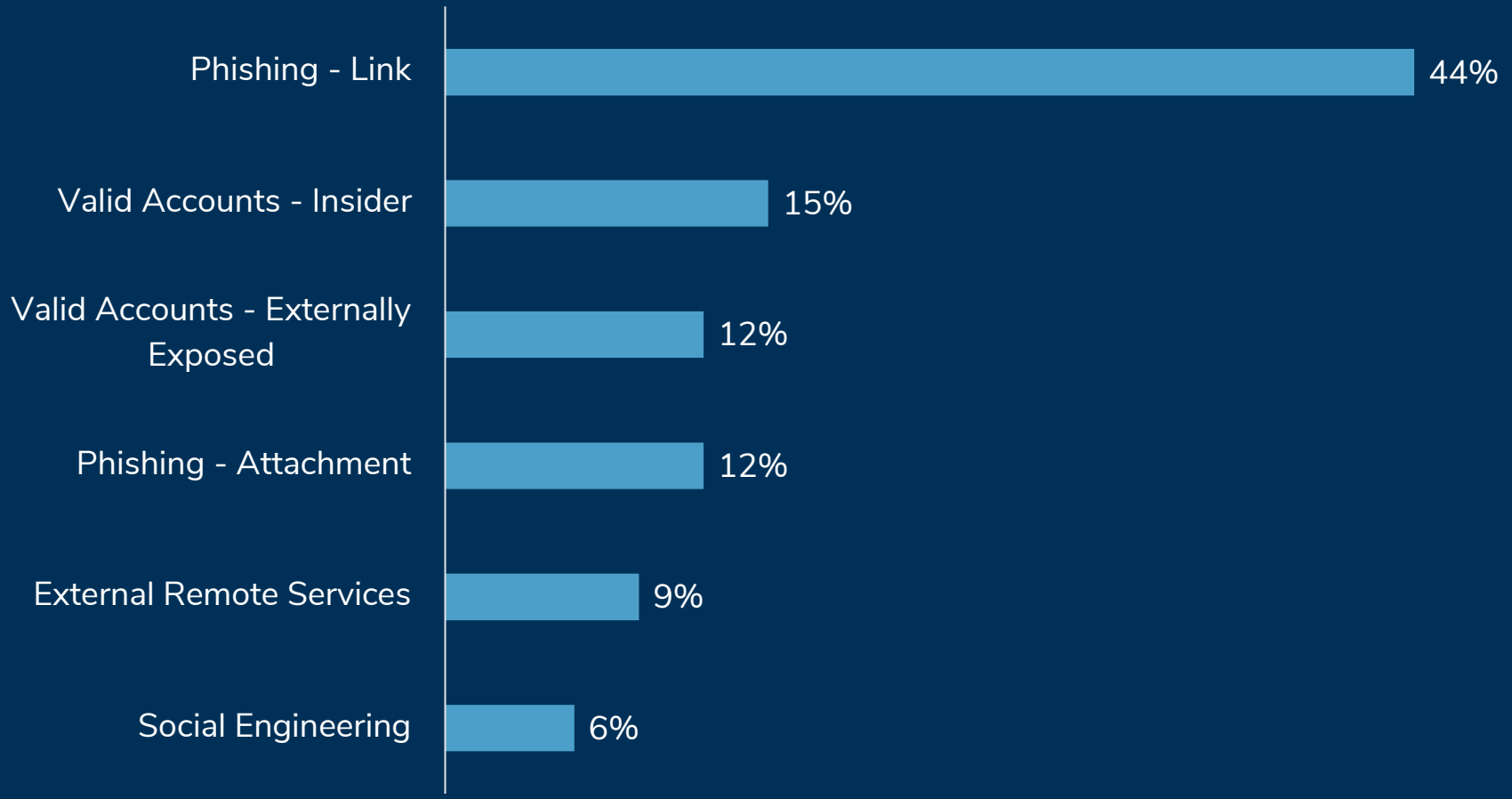
Web Compromise



*Unauthorized Access represents a summation of Unauthorized Access - Network and Unauthorized Access - Cloud / Repository Access

Initial Access Methods

December 2023



TLP: AMBER

Most Frequently Observed Malware

Malware variants/threat actor groups observed in active Kroll cases in December 2023

Malware	Definition
BLACKBYTE	Ransomware Variant
COBALTSTRIKE	Command & Control
AKIRA	Ransomware Variant
CACTUS	Ransomware Variant

*Word font size denotes frequency

Most Frequently Observed Threat Actor Tools

Tools observed in active Kroll cases in December 2023

Tool	Definition
MEGASYNC	Data Exfiltration
PSEXEC	Execution
ANYDESK	Remote Access
ACCOUNTRESTORE	Credential Bruteforce

*Word font size denotes frequency

Trending Vulnerabilities

December 2023

CVE	Vendor/Software	Advisory
CVE-2023-4966	Citrix NetScaler	https://nvd.nist.gov/vuln/detail/CVE-2023-4966
CVE-2023-3519	Cisco NetScaler	https://nvd.nist.gov/vuln/detail/CVE-2023-3519
CVE-2023-48365	Qlik Sense Enterprise	https://nvd.nist.gov/vuln/detail/CVE-2023-48365
CVE-2023-41265	Qlik Sense Enterprise	https://nvd.nist.gov/vuln/detail/CVE-2023-41265

Year End Spotlight Trends Report

TLP: AMBER

Key Takeaways

Initial Access Methods

- **Phishing - Link** (32%)
- **External Remote Services** (16%)
- **CVE / Exploit** (15%)
- **Phishing - Attachment** (12%)

Most Impacted Sectors

- **Professional Services** (24%)
- **Manufacturing** (13%)
- **Financial Services** (10%)
- **Healthcare** (9%)

Top Ransomware Variants

- **LOCKBIT** (23%)
- **CLOP** (13%)
- **AKIRA** (9%)

Top Threat Incident Types

- **Email Compromise** (40%)
- **Ransomware** (25%)
- **Unauthorized Access – Network** (8%)

Key Takeaways

2022-2023 Comparison

Top Initial Access Methods

2022

- Phishing (link and attachment) (51%)
- CVE Exploitation (15%)

2023

- Phishing – Link (32%)
- External Remote services (16%) ↑
- CVE Exploitation (15%)
- Phishing – Attachment (12%)

Top Threat Incident Type

2022

- Email Compromise (33%)
- Ransomware (32%)
- Unauthorized Access (25%)

2023

- Email Compromise (40%) ↑
- Ransomware (25%)
- Unauthorized Access (8%)

Most Impacted Sector

2022

- Professional Services (16%)
- Healthcare (13%)
- Manufacturing (11%)

2023

- Professional Services (24%) ↑
- Manufacturing (13%) ↑
- Financial Services (10%)
- Healthcare (9%)

Top Observed Ransomware Variant

2022

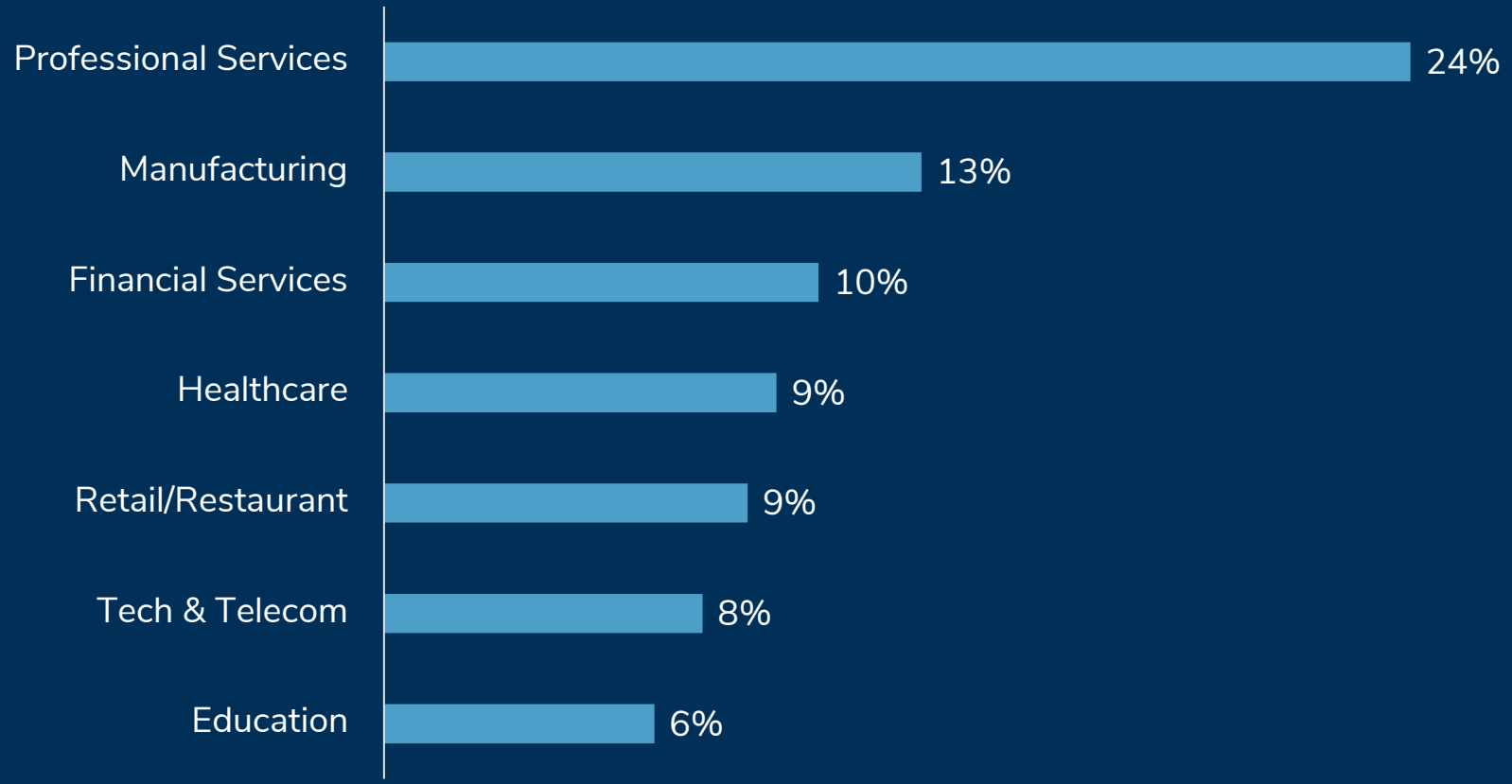
- LOCKBIT (18%)
- CONTI (7%)
- BLACKCAT (7%)
- BLACK BASTA (6%)

2023

- LOCKBIT (23%) ↑
- CLOP (13%) ↑
- AKIRA (9%)

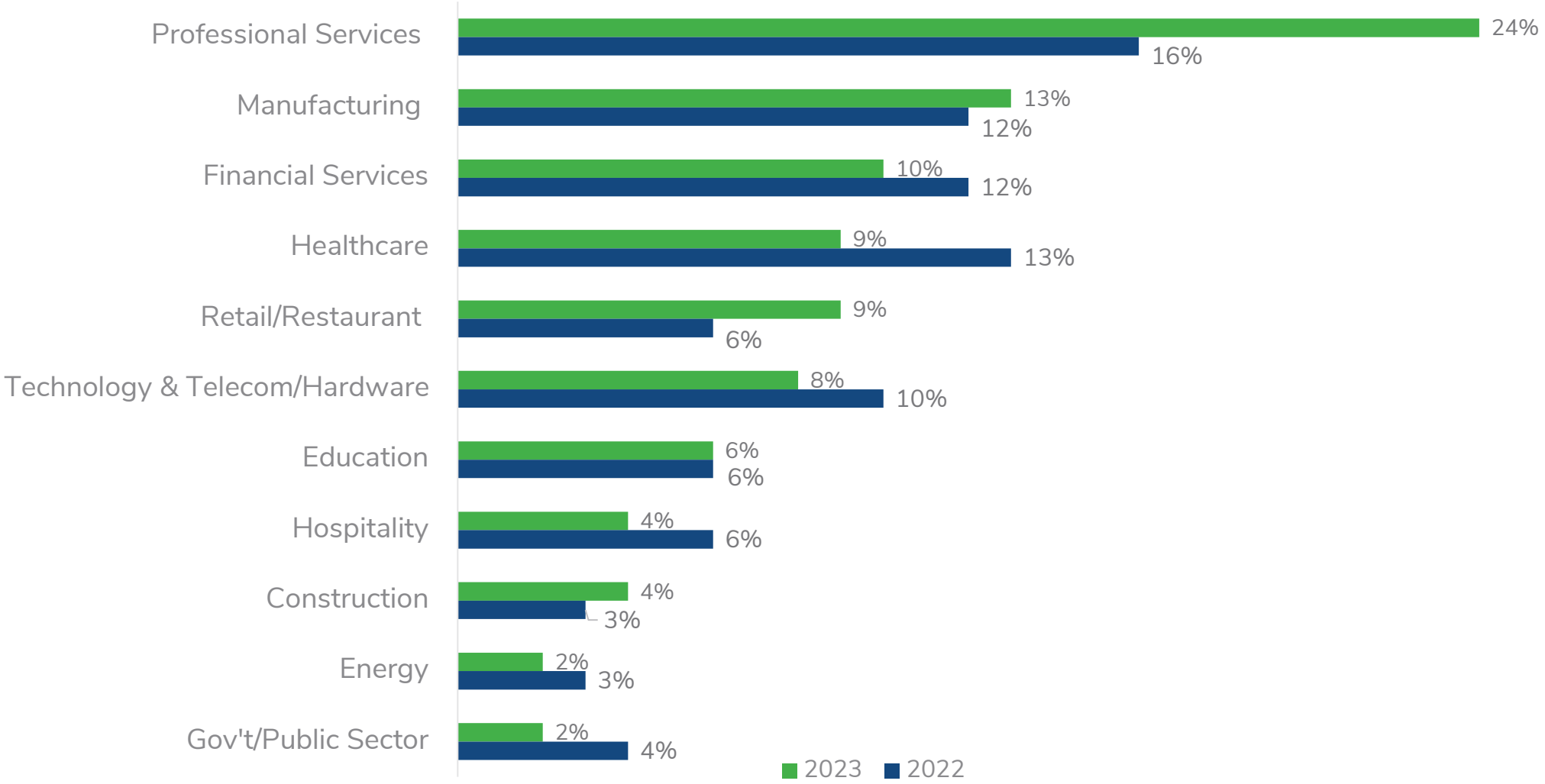
Incidents by Sector

Top 7 impacted industries for 2023



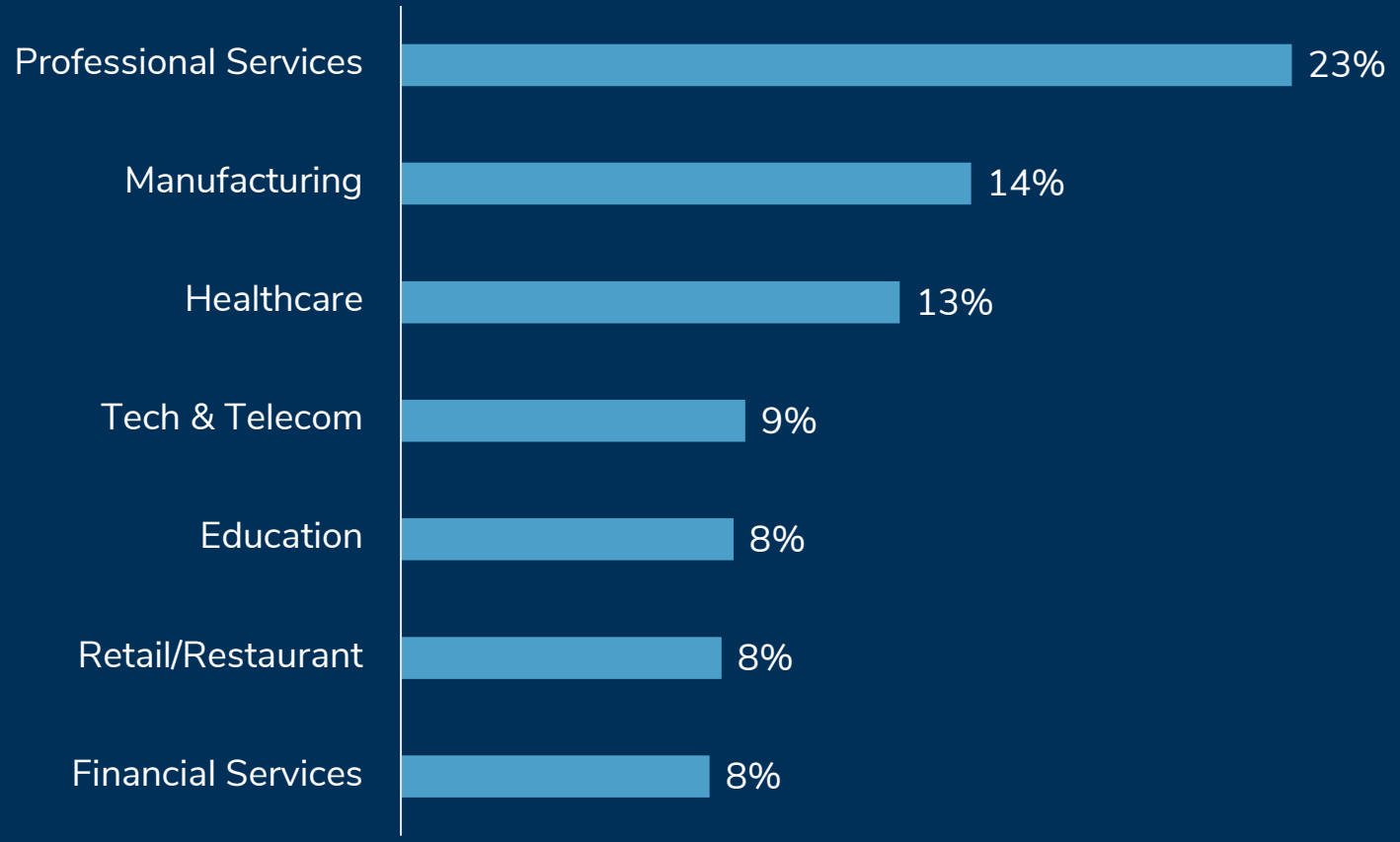
Incidents by Sector

2022-2023 Comparison



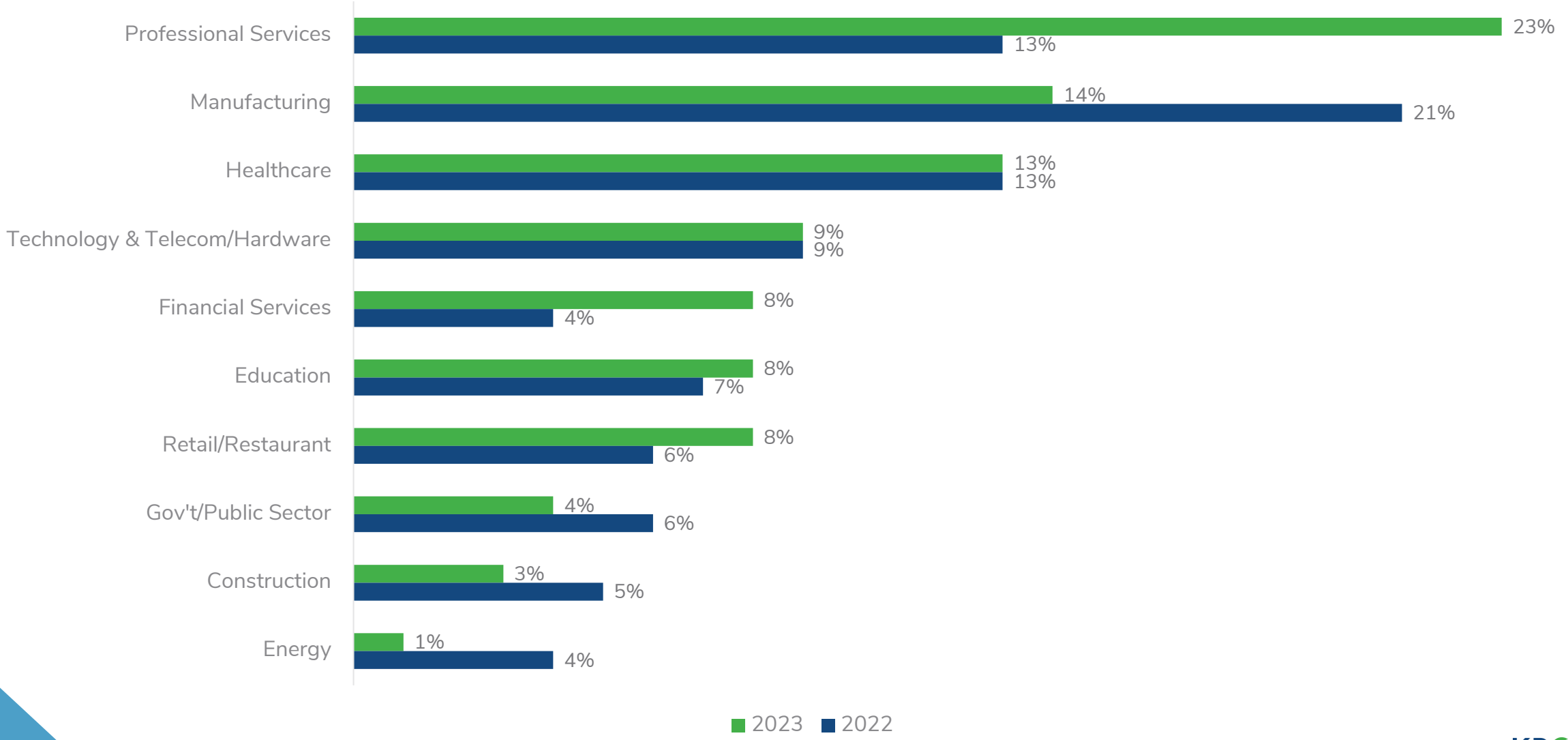
Ransomware – Top Impacted Sectors

Year End 2023



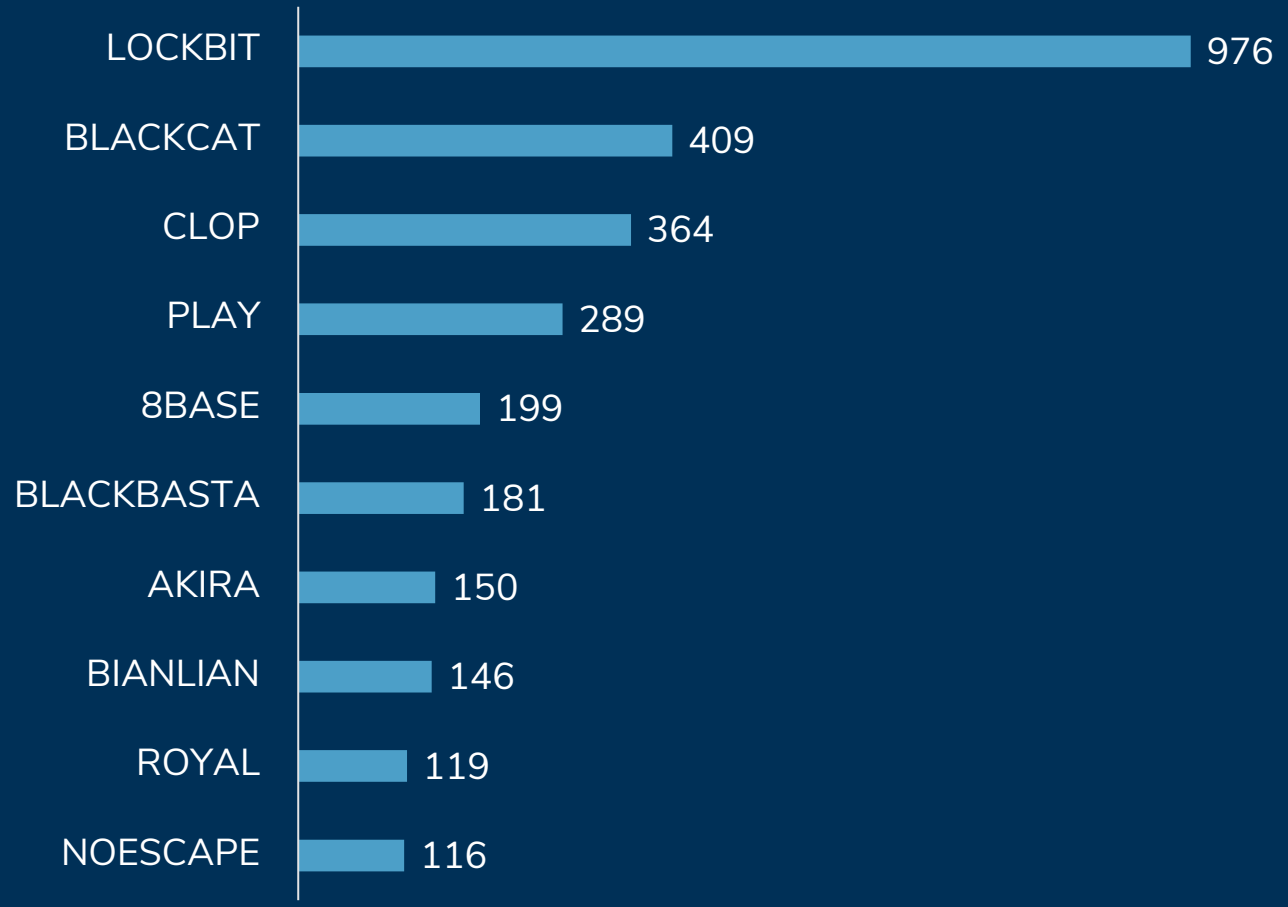
Ransomware – Top Impacted Sectors

2022-2023 Comparison



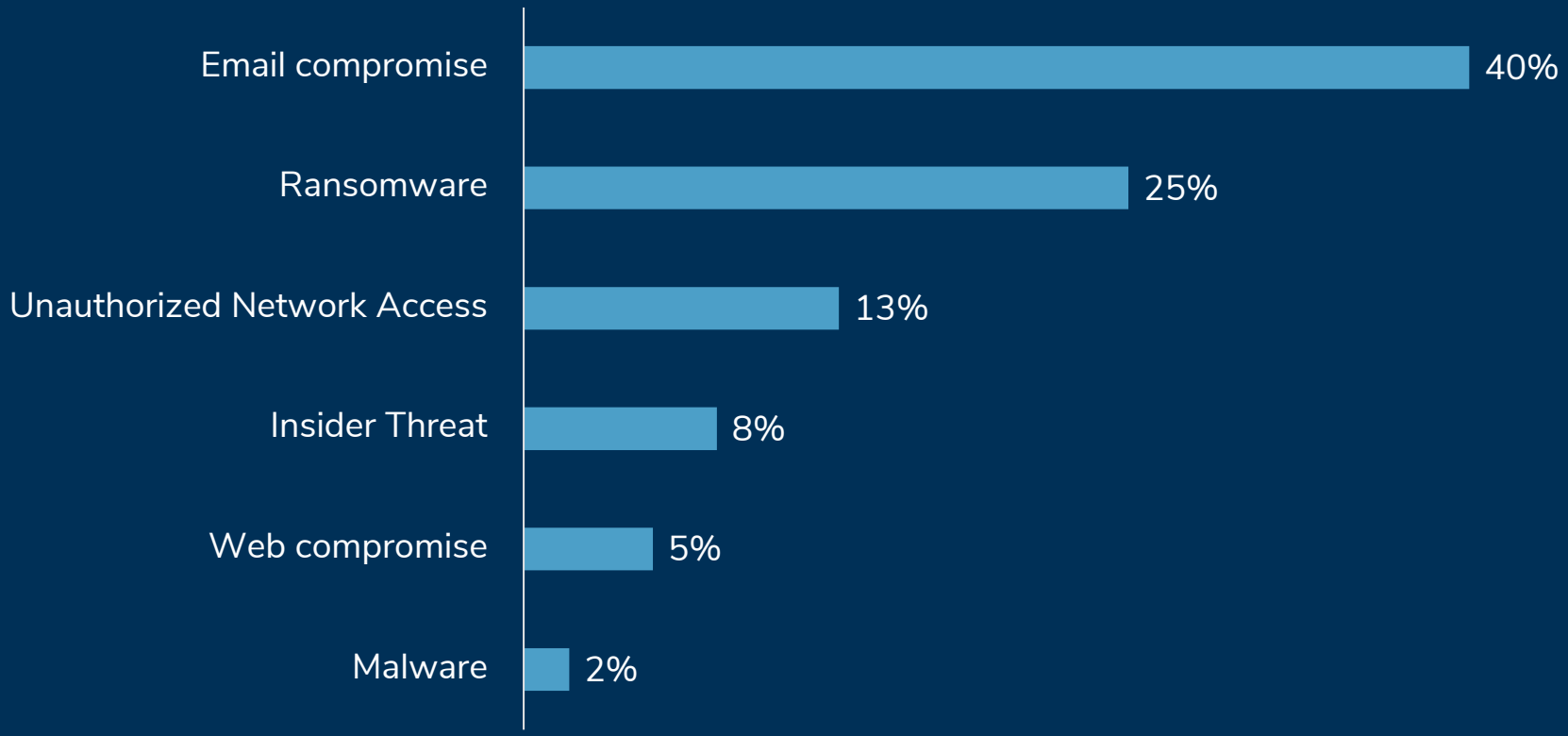
Ransomware – Actor-Controlled Site Listings

Year End 2023



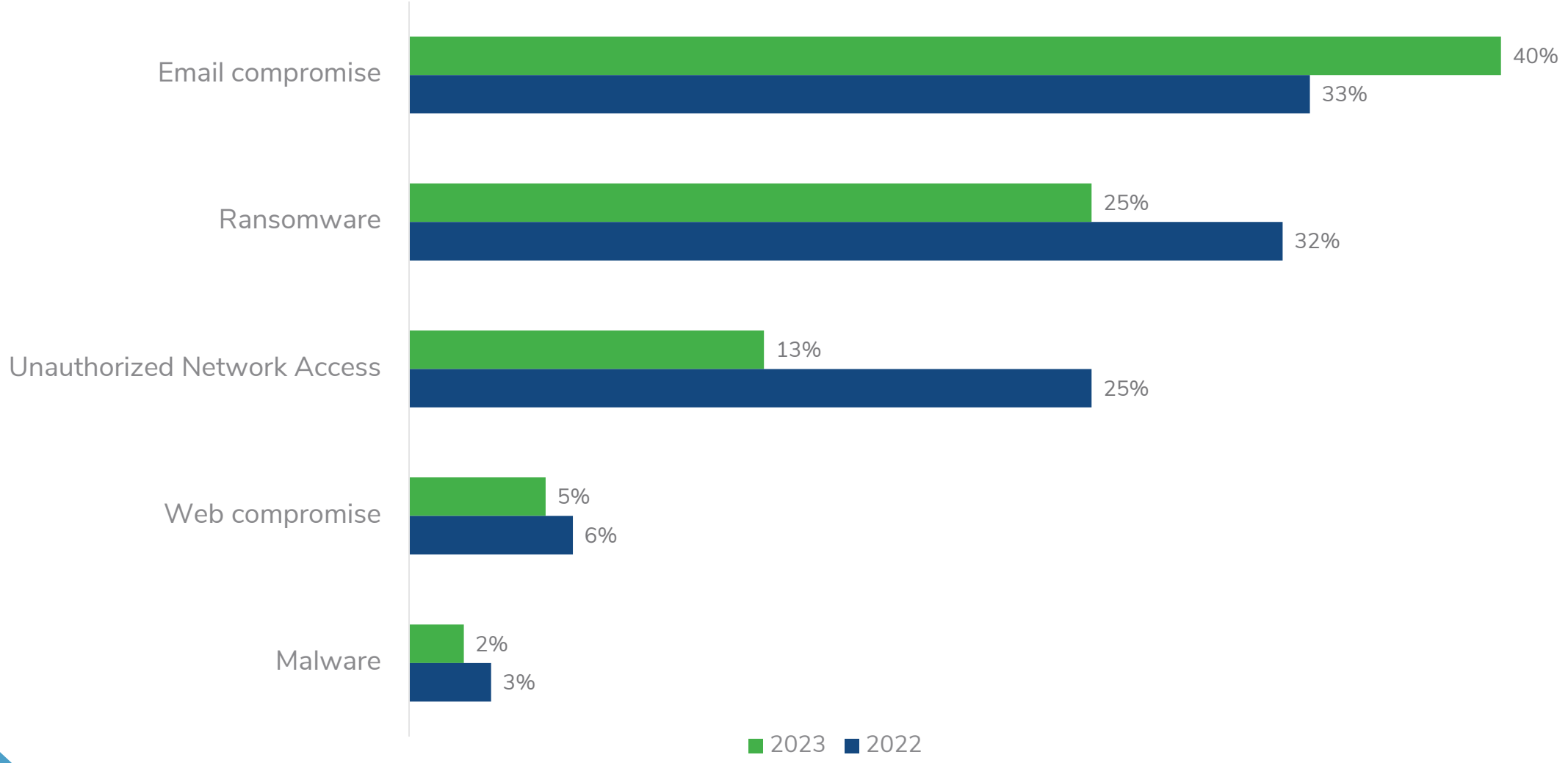
Incidents by Threat Type

Year End 2023



Incident by Threat Type

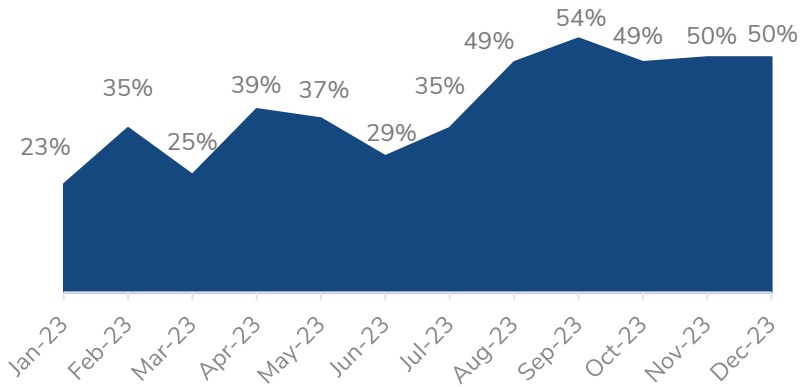
2022-2023 Comparison



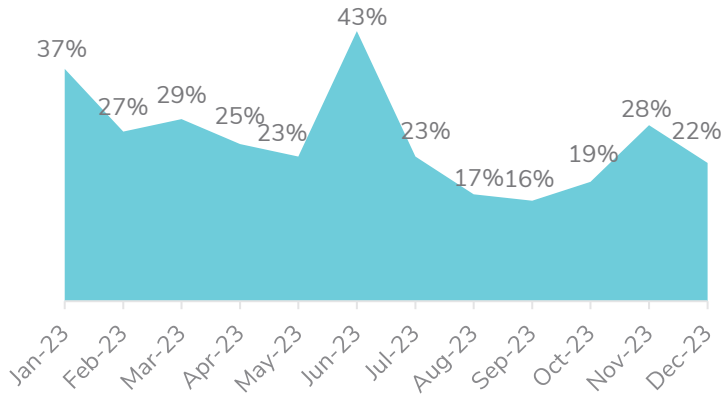
Threat Type Trends

2023 Monthly Breakdown

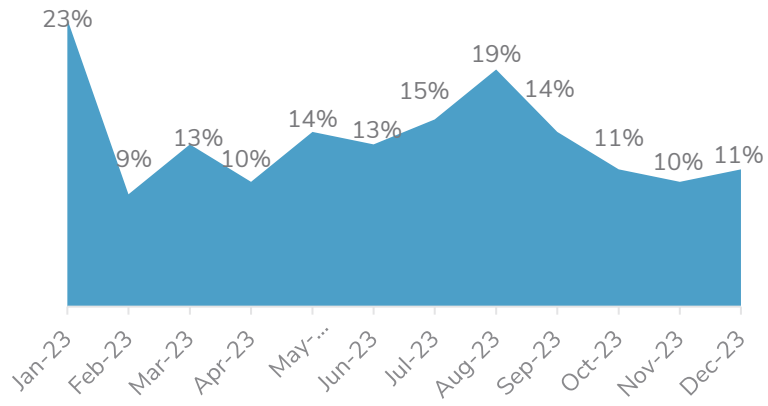
Email Compromise



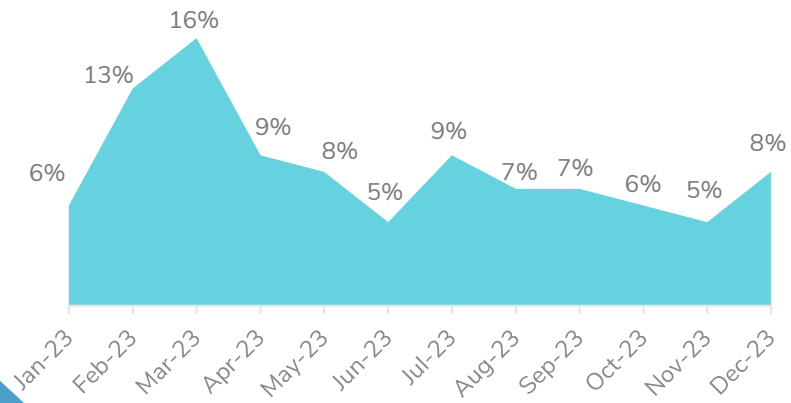
Ransomware



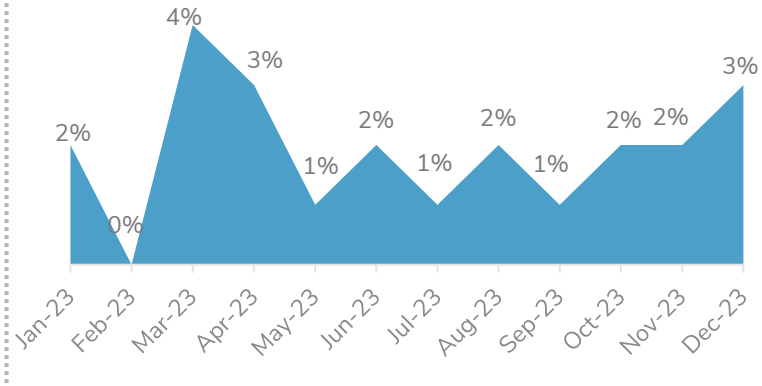
Unauthorized Access



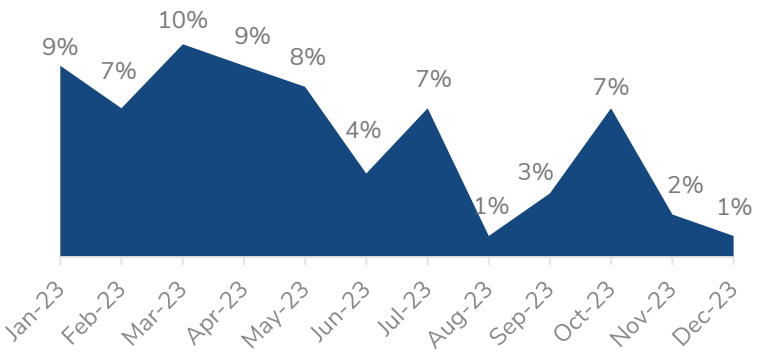
Insider Threat



Malware - Other



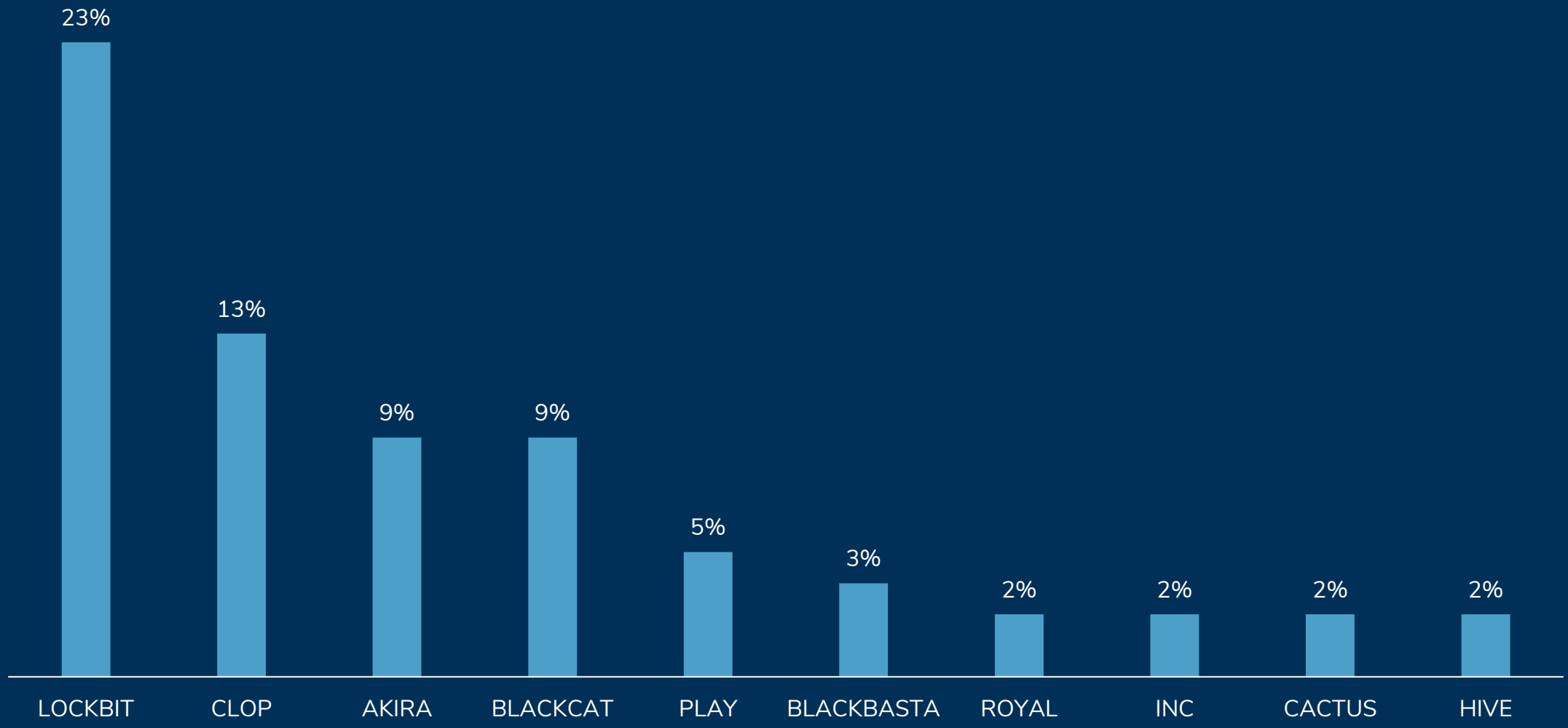
Web Compromise



*Unauthorized Access represents a summation of Unauthorized Access - Network and Unauthorized Access - Cloud / Repository Access

Top Ransomware Variants

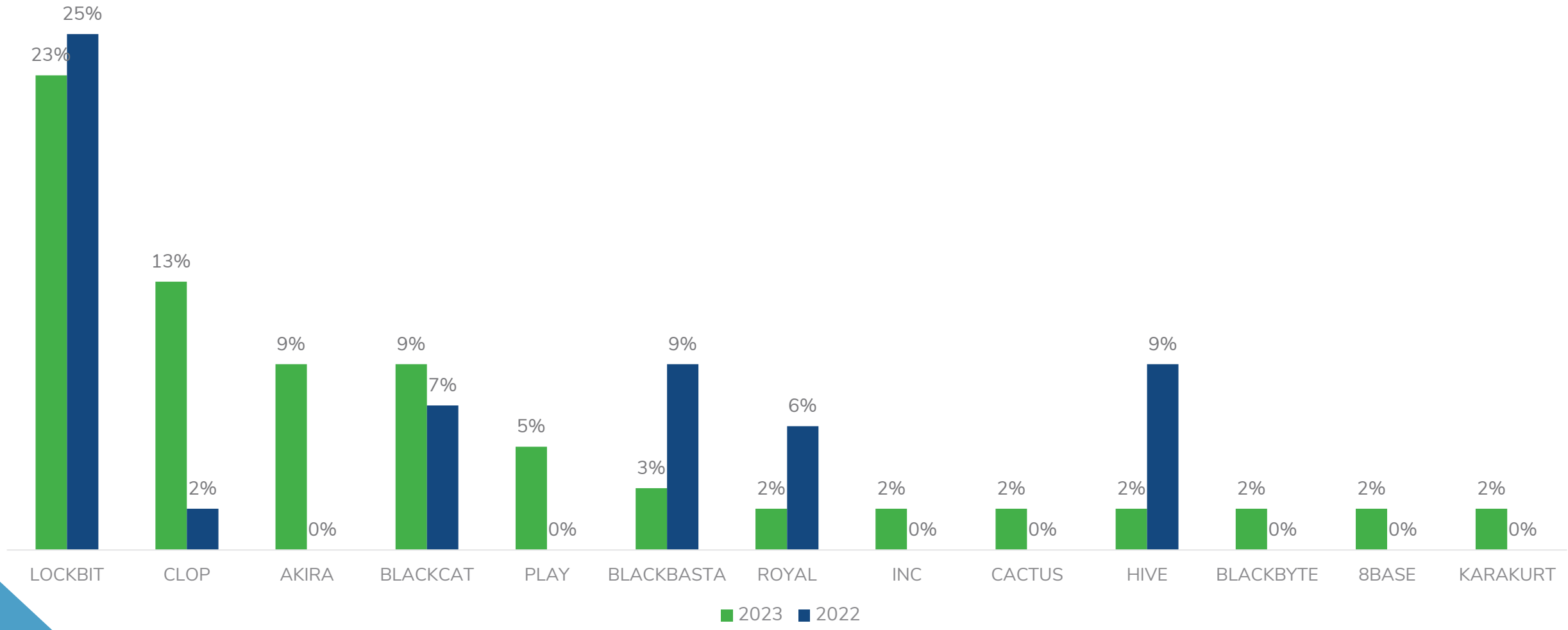
Year End 2023



TLP: AMBER

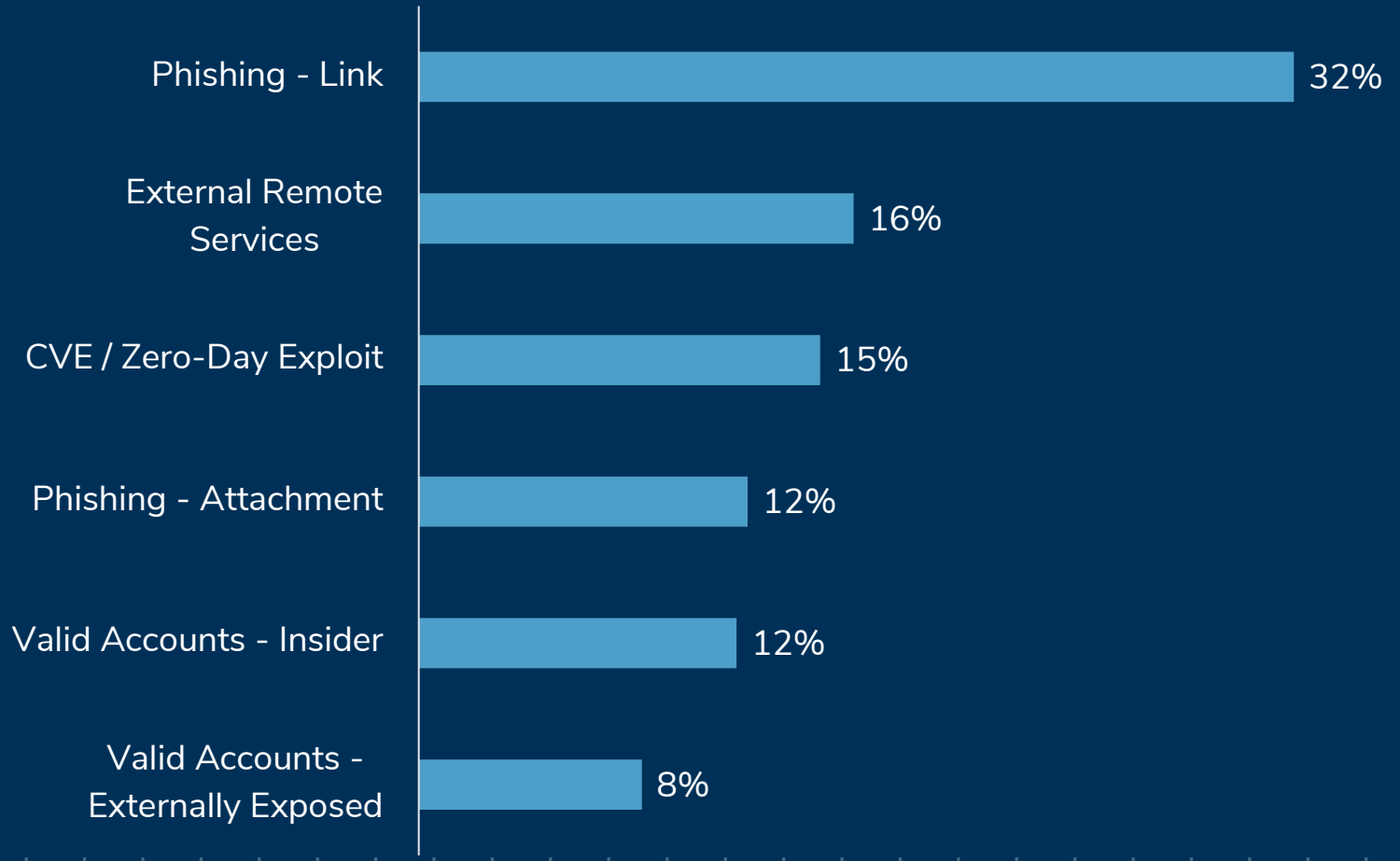
Top Ransomware Variants

2022-2023 Comparison



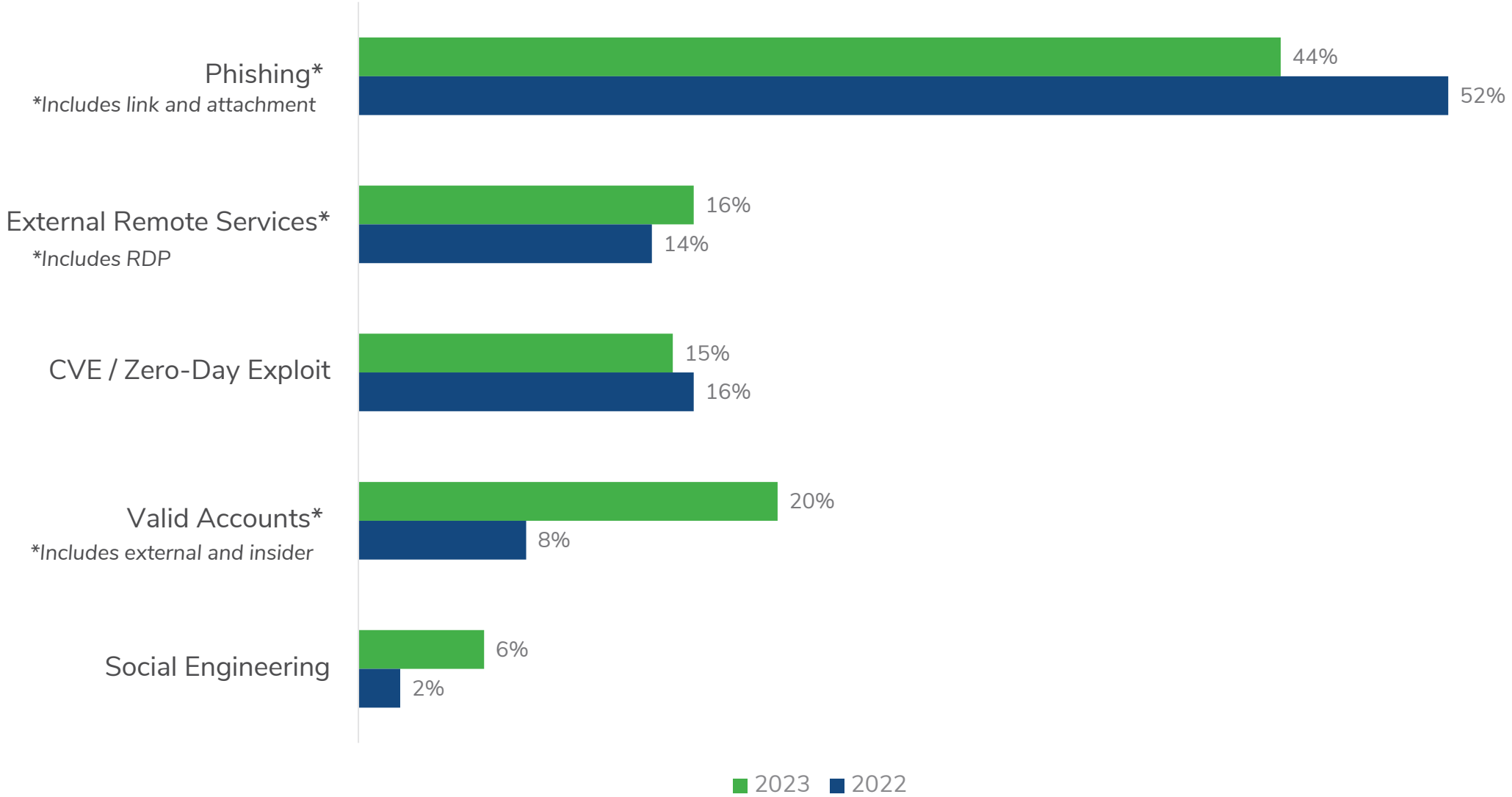
Initial Access Methods

Year End 2023



Top Initial Access Methods

2022-2023 Comparison



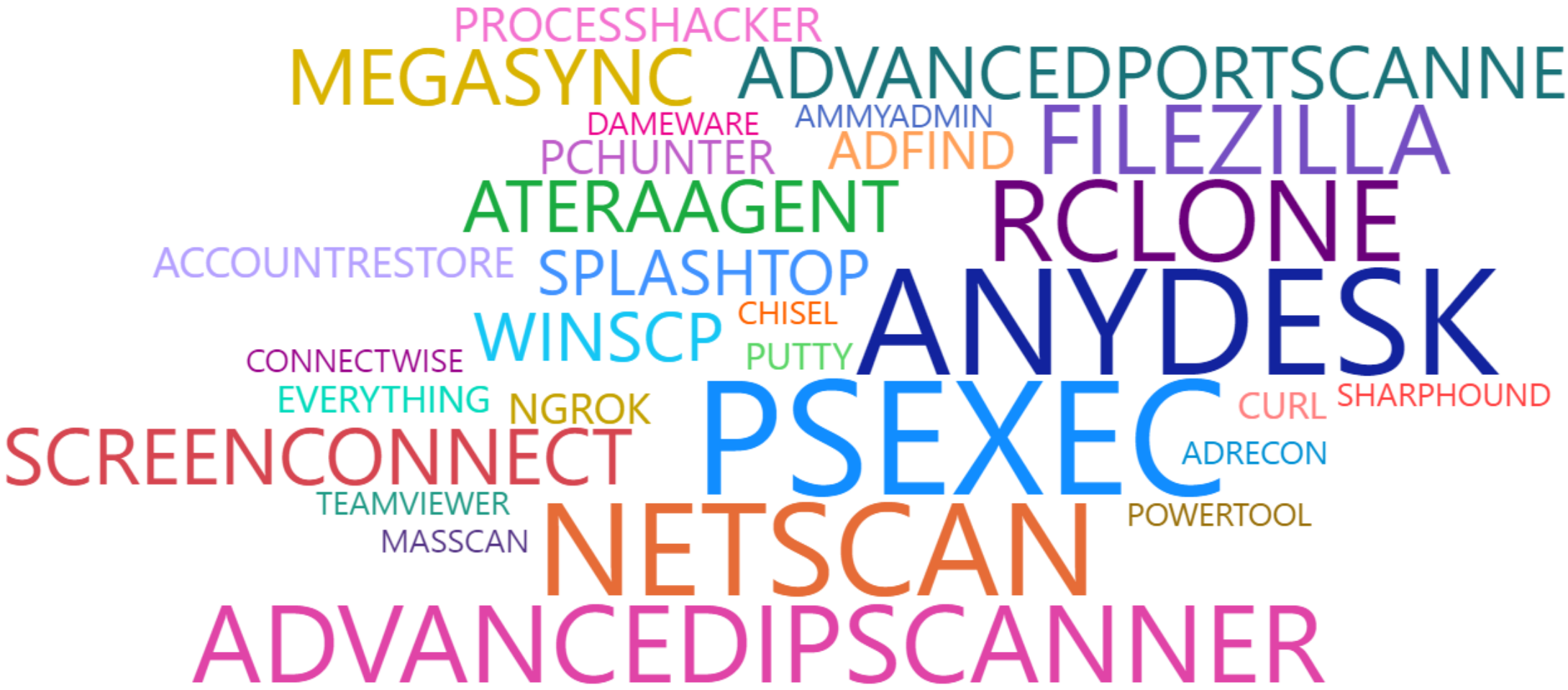
Most Frequently Observed Malware

Malware variants/threat actor groups observed in active Kroll cases in 2023

*Word font size denotes frequency

Most Frequently Observed Threat Actor Tools

Tools observed in active Kroll cases in 2023



*Word font size denotes frequency

Trending Vulnerabilities

Year End 2023

CVE	Vendor/Software	Advisory
CVE-2023-34362	Progress MOVEit Transfer	https://nvd.nist.gov/vuln/detail/CVE-2023-34362
CVE-2023-0669	Fortra GoAnywhere MFT	https://nvd.nist.gov/vuln/detail/CVE-2023-0669
CVE-2021-44228	Apache Log4j	https://nvd.nist.gov/vuln/detail/CVE-2021-44228
CVE-2023-25610	Ghost Security	https://nvd.nist.gov/vuln/detail/CVE-2023-26510
CVE-2022-41040	Microsoft Exchange	https://nvd.nist.gov/vuln/detail/cve-2022-41040
CVE-2023-3519	Citrix NetScaler ADC and NetScaler Gateway	https://nvd.nist.gov/vuln/detail/CVE-2023-3519
CVE-2023-27350	PaperCut NG	https://nvd.nist.gov/vuln/detail/CVE-2023-27350
CVE-2023-27351	PaperCut NG	https://nvd.nist.gov/vuln/detail/CVE-2023-27351
CVE-2022-40684	Fortinet FortiOS, FortiProxy, and FortiSwitchManager	https://nvd.nist.gov/vuln/detail/CVE-2022-40684
CVE-2023-27997	Fortinet FortiOS, FortiProxy, and SSL-VPN	https://nvd.nist.gov/vuln/detail/CVE-2023-27997

Threat Incident Types

Email Compromise: An event where email accounts are accessed maliciously by a third party (e.g., account takeover), a phishing email/campaign is identified, or an organization's email is used or compromised in a fraud scheme, such as a business email compromise.

Ransomware: An event where threat actors conduct malicious activity within a network followed by a demand for a financial ransom. Typically includes some combination of data exfiltration, data encryption, and extortion.

Malware – Other: An organization is impacted by a malware or virus where no financial demand is made. Examples include pre-ransomware activity (e.g., QakBot, Emotet) or information stealers (e.g., Vidar, Raccoon).

Unauthorized Access: An unauthorized actor has inadvertently or maliciously accessed a network.

Web Compromise: An actor has gained unauthorized access to web application or website code to conduct malicious activity. Examples include SQL injections to steal credit card data or website defacement.

Initial Access Methods

Drive-By Compromise: Compromise via a legitimate website.

External Remote Services: Compromise via remote access services such as VPNs.

Hardware Additions: Addition of computing device to gain access.

CVE / Zero-Day Exploit: Exploitation of a known or previously unknown vulnerability in an existing software.

Phishing – Attachment: Use of malware attached to an email.

Phishing – Link: Use of links in an email that lead to credential loss and/or downloading malware.

Supply Chain Compromise: Attack on weak links within an organization's supply chain (e.g., third-party vulnerability).

Social Engineering: Attempt to gain access to someone's personal or financial information via manipulation (e.g., Vishing, email impersonation).

Valid Accounts – Insider: The use of known credentials/legitimate or unrevoked access by an insider.

Valid Accounts – Externally Exposed: Account takeover via use of known credentials by external actor.

Additional Resources

See below for recent publications and upcoming events from Kroll's cyber threat intelligence team

CVE-2024-0204: Authentication Bypass Vulnerability in Fortra GoAnywhere MFT - A critical vulnerability, tracked as CVE-2024-0204, has been discovered in Fortra's GoAnywhere MFT versions prior to 7.4.1 that could allow an unauthorized user to create an admin user via the admin portal.

Inside the SYSTEMBC Command-and-Control Server - Throughout Q2 and Q3 2023, Kroll observed an increased use of the malicious SYSTEMBC tool to maintain access in a compromised network. Our experts conducted research into the SYSTEMBC command and control (C2) server.

Open the DARKGATE – Brute Forcing DARKGATE Encodings - Kroll recently analyzed newer versions of DARKGATE, a Windows-based malware sold on the dark web, which randomly shuffles the non-standard alphabet in use. Kroll identified a weakness in this shuffling.

Q4 2023 Threat Landscape Briefing

February 15, 2024 11:00 am – 11:45 am ET

Kroll's cyber threat intelligence leaders will explore key insights and trends drawn from over 3,000 cyber incidents handled worldwide each year. They will discuss the overarching trends of 2023 and highlight some of the trends likely to have an impact in 2024, as well as diving into detail on the fourth quarter of the year.

Register here

Definitions

Traffic Light Protocol (TLP)

Color	When should it be used?	How may it be shared?
TLP:RED **Not for disclosure, restricted to participants only.**	Sources may use **TLP:RED** when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share **TLP:RED** information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, **TLP:RED** information is limited to those present at the meeting. In most circumstances, **TLP:RED** should be exchanged verbally or in person.
TLP:AMBER+STRICT **Limited disclosure, restricted to participants' organization only.**	Sources may use **TLP:AMBER+STRICT** when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share **TLP:AMBER+STRICT** information with members of their own ***organization*** who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
TLP:AMBER **Limited disclosure, restricted to participants' organizations and clients.**	Sources may use **TLP:AMBER** when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share **TLP:AMBER** information with members of their own ***organization and with clients or customers*** who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
TLP:GREEN **Limited disclosure, restricted to the community.**	Sources may use **TLP:GREEN** when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share **TLP:GREEN** information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. **TLP:GREEN** information may not be released outside of the community.
TLP:CLEAR **Disclosure is not limited.**	Sources may use **TLP:CLEAR** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, **TLP:CLEAR** information may be distributed without restriction.

KROLL

For more information, please contact:

Keith Wojcieszek
Managing Director, Cyber Risk
1 443 295 5082
keith.wojcieszek@kroll.com

Laurie Iacono
Associate Managing Director, Cyber Risk
1 412 588 4337
laurie.iacono@kroll.com

About Kroll

As the leading independent provider of risk and financial advisory solutions, Kroll leverages our unique insights, data and technology to help clients stay ahead of complex demands. Kroll's global team continues the firm's nearly 100-year history of trusted expertise spanning risk, governance, transactions and valuation. Our advanced solutions and intelligence provide clients the foresight they need to create an enduring competitive advantage. At Kroll, our values define who we are and how we partner with clients and communities. Learn more at www.kroll.com.

TLP: AMBER