INTEL471

BRAND GUIDE

TABLE OF CONTENT

BRAND

6 Mission
Vision
Tagline
Differentiation
7 Our Characteristics
8 Demographics
9 Our Audience

IDENTITY

12 Logo Usages
Logo Elements
Clear Space
Minimum Size
13 Other Logo Usage
14 Logo Positioning
15 Logo Placement Examples
16 Logo Don’ts
Logo Typography
Typography for Marketing
Subsitiute Typography
17 Typography Examples
18 Primary and Accent Colors
Colors for Print
Colors for Digital
19 Color Use Examples
20 Texture Backgrounds
22 Marketing Images

MARKETING

26 Branding
27 Branding Examples
28 Collateral
29 Collateral Examples
30 Internet and Social Media
32 Events
35 Conclusion

BRAND

OUR STORY

Intel 471 provides an unparalleled threat intelligence solutions. Whether scaling your digital security presence or just starting to build your team, we can help you fight cyber threats. Intel 471 empowers security teams to be proactive with our relevant and timely insights into the cyber underground.

MISSION

Become essential to our clients by providing unique intelligence and support that allows them to counter the threat of cybercrime.

Partner with our clients to grow and mature their intelligence capabilities so they can better counter the threat of cybercrime.

VISION

To be the premier, most respected and most called on cyber threat intelligence company and to be best in class in all that we provide.

Unlock the power of cyber threat intelligence to support all aspects of the business and across the range of maturity levels.

TAGLINE

Your Voice of Reason & Truth.

DIFFERENTIATION

Timeliness: ability to identify near real-time identification and indication tactics, techniques, and procedures.

Relevance: Surfacing the most relevant intelligence, which is mapped to specific customer needs in a GIR (General Intelligence Requirements) framework.

Operationalization:

- Ease of integration or structured and actionable data exposed on our TITAN platform or via RESTful API and third-party tools.
- Clean data that translates into zero false-positive results and minimizes both analyst fatigue and the need for additional resources.

OUR CULTURE

HUMBLE EXPERT

We impart our knowledge and expertise with the ultimate goal of sharing what we know - not trying to inflate our ego or look superior.

OPERATE WITH INTEGRITY

Our company culture emphasizes ethical conduct and upholds the highest standards of honesty and transparency in all that we do. We always seek to do the right thing, even when it hurts.

CELEBRATE COLLABORATION AND CAMARADERIE

We foster a culture that thrives on teamwork, mutual support, and a strong sense of camaraderie, valuing collaboration as a catalyst for success.

TACKLE PROBLEMS HEAD ON & EMBRACE ACCOUNTABILITY

We encourage a proactive approach to problem-solving, promoting a culture of accountability where individuals take ownership of challenges and work together to find effective solutions.

IDEAL CUSTOMER PROFILE (ICP)

Cyber hreat Intelligence Market
~15,000 target orgs globally $2.2B TAM

Tier1: ICP 1,000 orgs:

- Organizations with annual revenue of $5B or greater
- High level of CTI maturity; executing against multiple use cases with specialized teams; has executive and/or Board level support

Tier2: ICP 3,000 orgs:

- Organizations with annual revenue of $1B or greater, but less than $5B
- Mid-level CTI maturity; often a single team handling all aspects of cybersecurity led by an experienced senior level professional

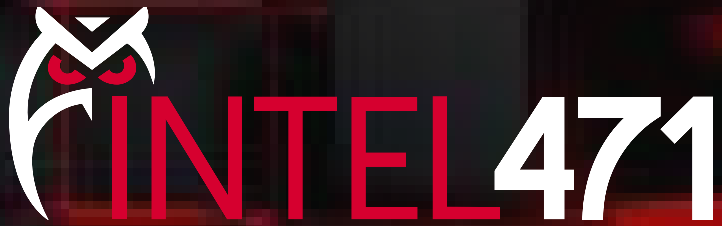
Tier3: ICP 11,000 orgs:

- Organizations with annual revenue of $500M, but less than $1B
- Low level of CTI maturity; minimal staff with little connection to the corporate goals

OUR AUDIENCE

IDENTITY

OUR LOGO



Intel 471 logo is bold and serious in color choices with a clean and elegant style/font. The Owl reflects wisdom and exemplifies our tagline, "Voice of Reason & Truth." The wise old owl lived in an oak; The more she saw, the less she spoke; The less she spoke, the more she heard; Why can't we all be more like that wise old bird?

LOGO USAGE

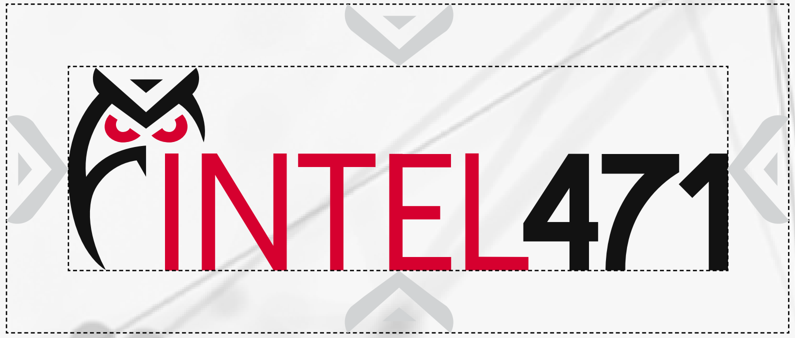
The primary logo contains red and monochromatic hues. Version with dark hues should be used on light backgrounds, and light version on dark backgrounds. The logo should be legible regardless of background.

LOGO ELEMENTS

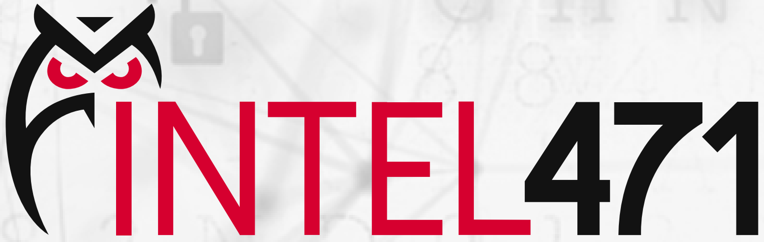
Intel 471 logo consist of an Owl icon that reflects knowledge and wisdom. These characteristics are the voice and tone of the company. The font Manun is used for the main name.

CLEAR SPACE

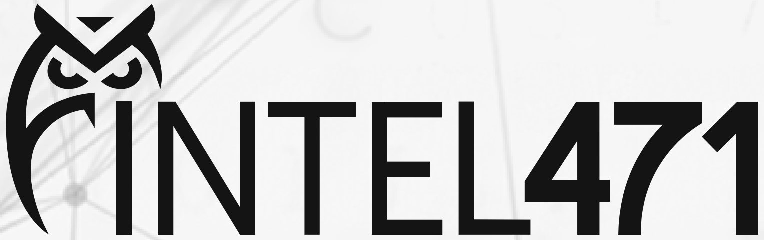
The amount of clear space around the logo is equal to the height of the owl's eyebrow in the logo image.



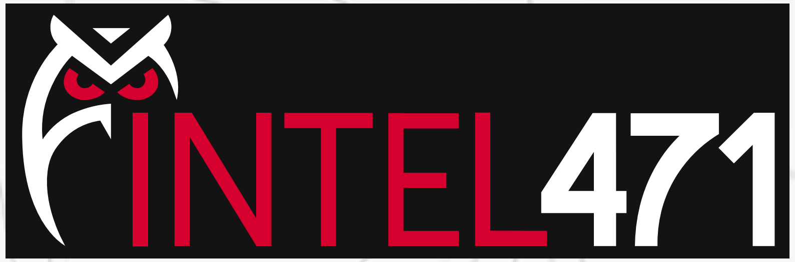
Main Logo



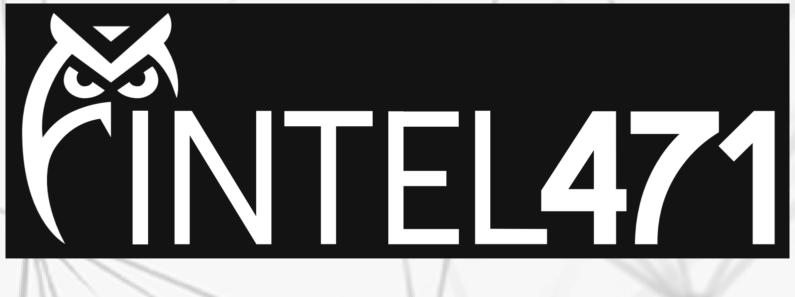
1-Color



Reverse Color



Reverse 1-Color

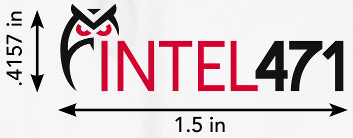


MINIMUM SIZE

It’s important that our logo is in our customer’s field of view, but we understand they are not going to our website or viewing our collaterals to look at our logo.

A larger-than-the-norm logo can get in the way of communicating our promises; and could accidently send a message that “we (the brand) is more important that our customers."

Using Intel 471 logo at a small size is feasible when necessary but should never be reduced below 1.5 in wide x .4157 in high.



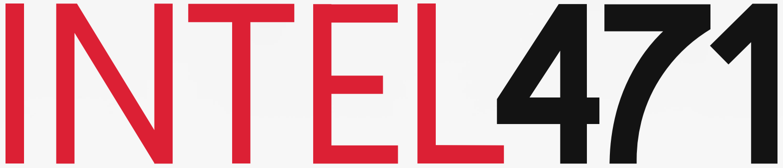
OTHER LOGO USAGE

For cases when primary logo can't be used, it is acceptable to use a monochrome version of the logo. Examples include black and white print advertising.

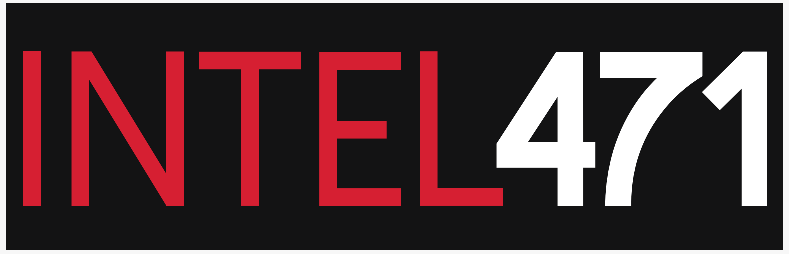
It is preferred to use two separate colors for logo elements. Preferred replacement for the brand red color is #707070 (C0 M0 Y0 K65). It is acceptable to use all-white and all black versions of the logo if no other version can be used.

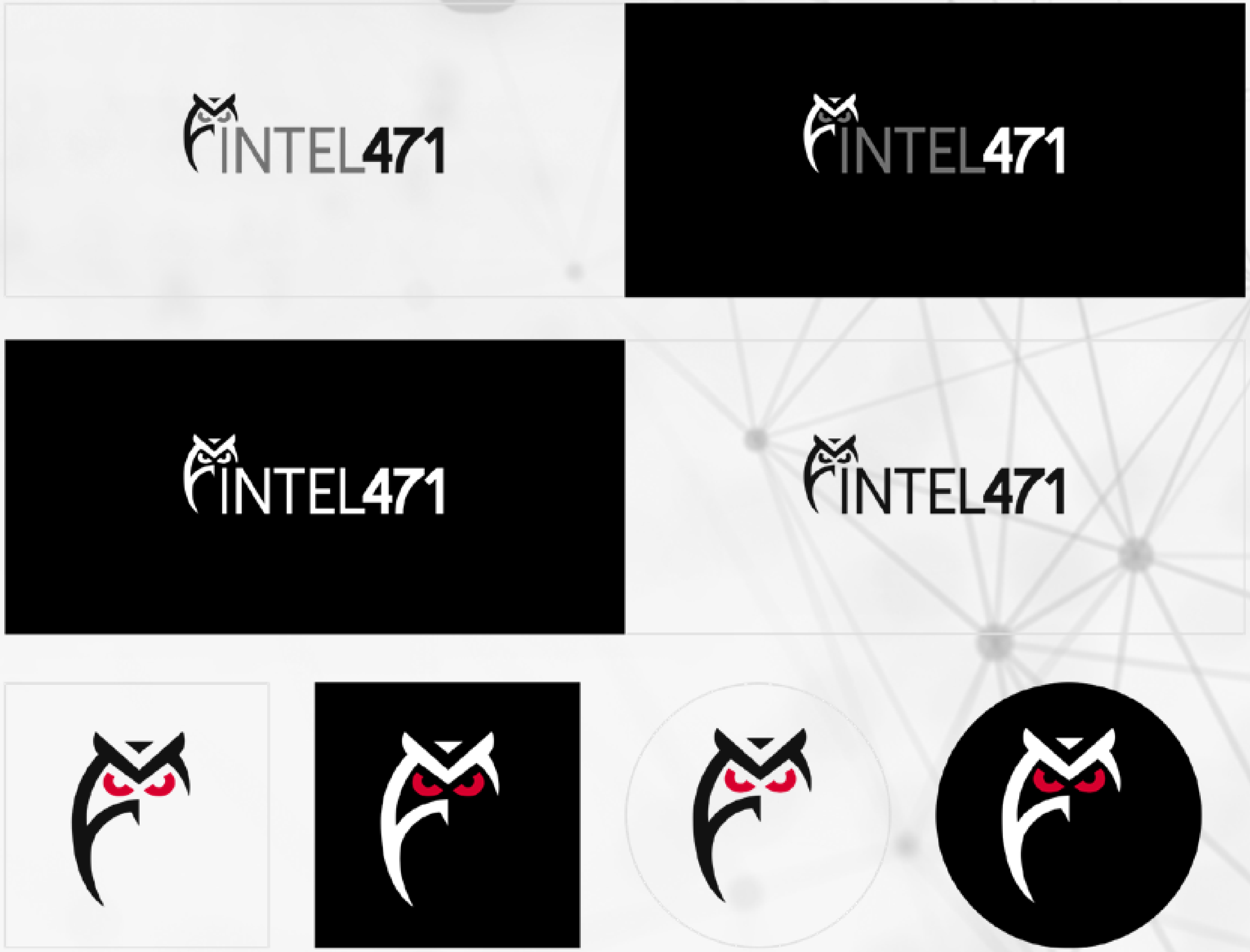
The owl can be separated and used as an independent element ("bug") for social media and other uses with limited space.

The owl can also be removed and the wordmark used to accomidate spacing and for stronger identity.



Reverse Color



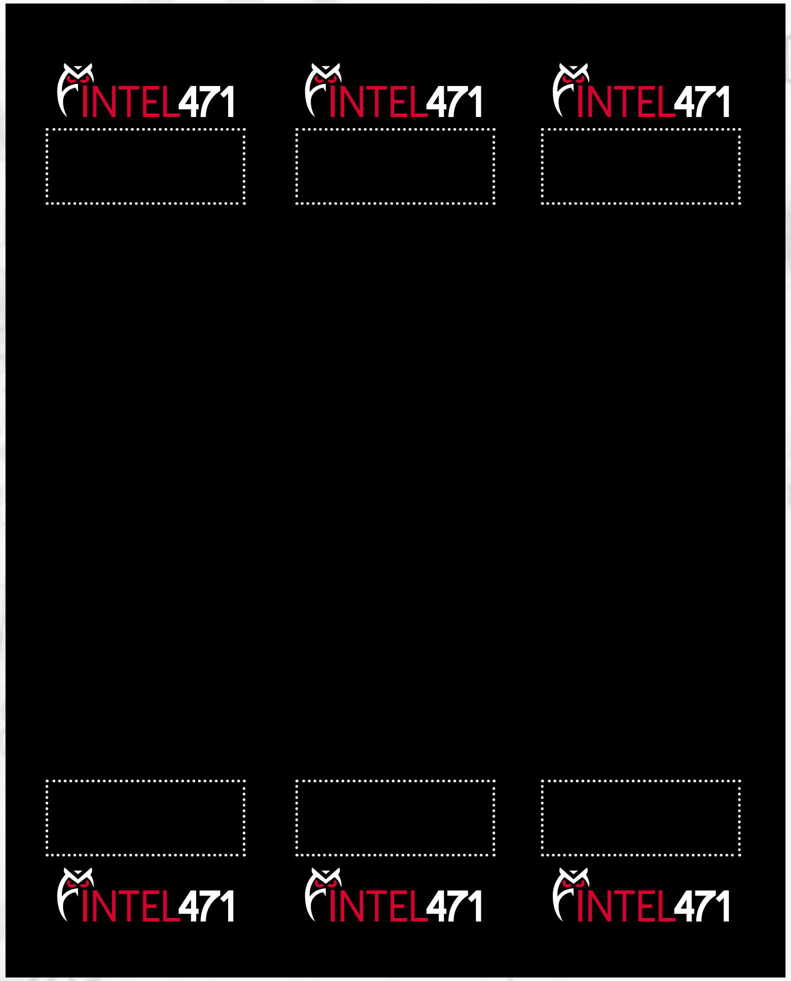


LOGO POSITIONING

The logo should be used on a light background in a position of prominence. It should always have the required clear space around it. Do not use it more than once on a page. You should only use the black and white or reverse alternative when the color logo is not an option.

The logo can be used in-line with endorsement marks. If you have any questions about this, please contact us at the information listed on the last page.

Do not use the logo in the middle of a sentence or paragraph. Preferred positions are right, center, or left at the top or bottom of a page with the required clear space around it. The exact placement and positioning within the guidelines are flexible, as indicated with the dotted white rectangles in the sample to the right.



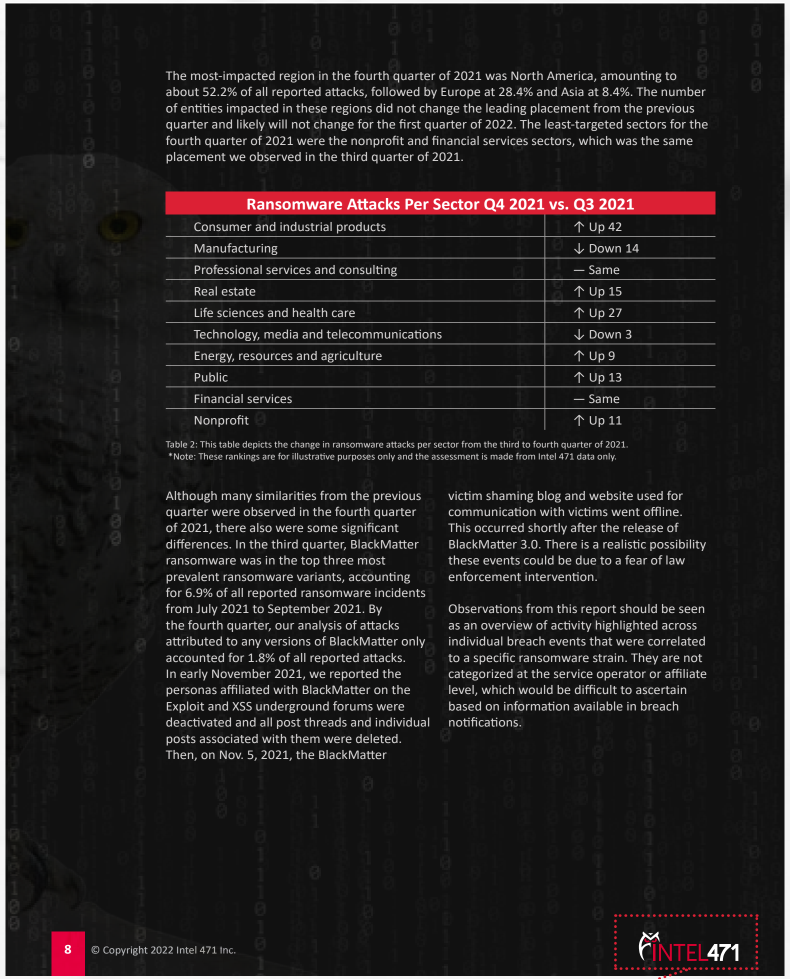
Logo placement top right

INTEL471

White Paper
March 2022

Ransomware Variants
Intelligence Bulletin

Logo placement top left



The most-impacted region in the fourth quarter of 2021 was North America, amounting to about 52.2% of all reported attacks, followed by Europe at 28.4% and Asia at 8.4%. The number of entities impacted in these regions did not change the leading placement from the previous quarter and likely will not change for the first quarter of 2022. The least-targeted sectors for the fourth quarter of 2021 were the nonprofit and financial services sectors, which was the same placement we observed in the third quarter of 2021.

Ransomware Attacks Per Sector Q4 2021 vs. Q3 2021	
Consumer and industrial products	↑ Up 42
Manufacturing	↓ Down 14
Professional services and consulting	— Same
Real estate	↑ Up 15
Life sciences and health care	↑ Up 27
Technology, media and telecommunications	↓ Down 3
Energy, resources and agriculture	↑ Up 9
Public	↑ Up 13
Financial services	— Same
Nonprofit	↑ Up 11

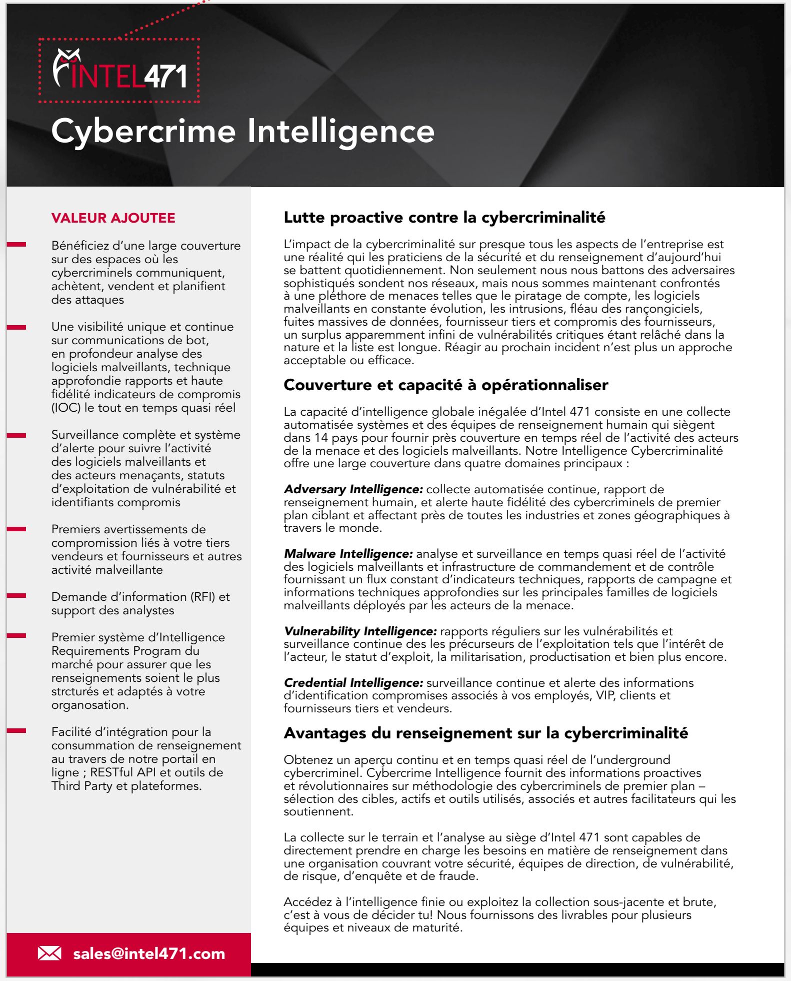
Table 2: This table depicts the change in ransomware attacks per sector from the third to fourth quarter of 2021.
*Note: These rankings are for illustrative purposes only and the assessment is made from Intel 471 data only.

Although many similarities from the previous quarter were observed in the fourth quarter of 2021, there also were some significant differences. In the third quarter, BlackMatter ransomware was in the top three most prevalent ransomware variants, accounting for 6.9% of all reported ransomware incidents from July 2021 to September 2021. By the fourth quarter, our analysis of attacks attributed to any versions of BlackMatter only accounted for 1.8% of all reported attacks. In early November 2021, we reported the personas affiliated with BlackMatter on the Exploit and XSS underground forums were deactivated and all post threads and individual posts associated with them were deleted. Then, on Nov. 5, 2021, the BlackMatter victim shaming blog and website used for communication with victims went offline. This occurred shortly after the release of BlackMatter 3.0. There is a realistic possibility these events could be due to a fear of law enforcement intervention.

Observations from this report should be seen as an overview of activity highlighted across individual breach events that were correlated to a specific ransomware strain. They are not categorized at the service operator or affiliate level, which would be difficult to ascertain based on information available in breach notifications.

8 © Copyright 2022 Intel 471 Inc.

INTEL471



INTEL471

Cybercrime Intelligence

VALEUR AJOUTEE

- Bénéficiez d'une large couverture sur des espaces où les cybercriminels communiquent, achètent, vendent et planifient des attaques
- Une visibilité unique et continue sur communications de bot, en profondeur analyse des logiciels malveillants, technique approfondie rapports et haute fidélité indicateurs de compromis (IOC) le tout en temps quasi réel
- Surveillance complète et système d'alerte pour suivre l'activité des logiciels malveillants et des acteurs menaçants, statuts d'exploitation de vulnérabilité et identifiants compromis
- Premiers avertissements de compromission liés à votre tiers vendeurs et fournisseurs et autres activité malveillante
- Demande d'information (RFI) et support des analystes
- Premier système d'Intelligence Requirements Program du marché pour assurer que les renseignements soient le plus strcturés et adaptés à votre organosation.
- Facilité d'intégration pour la consummation de renseignement au travers de notre portail en ligne ; RESTful API et outils de Third Party et plateformes.

✉ sales@intel471.com

Lutte proactive contre la cybercriminalité

L'impact de la cybercriminalité sur presque tous les aspects de l'entreprise est une réalité qui les praticiens de la sécurité et du renseignement d'aujourd'hui se battent quotidiennement. Non seulement nous nous battons des adversaires sophistiqués sondent nos réseaux, mais nous sommes maintenant confrontés à une pléthore de menaces telles que le piratage de compte, les logiciels malveillants en constante évolution, les intrusions, fléau des rançongiciels, fuites massives de données, fournisseur tiers et compromis des fournisseurs, un surplus apparemment infini de vulnérabilités critiques étant relâché dans la nature et la liste est longue. Réagir au prochain incident n'est plus un approche acceptable ou efficace.

Couverture et capacité à opérationnaliser

La capacité d'intelligence globale inégalée d'Intel 471 consiste en une collecte automatisée systèmes et des équipes de renseignement humain qui siègent dans 14 pays pour fournir près couverture en temps réel de l'activité des acteurs de la menace et des logiciels malveillants. Notre Intelligence Cybercriminalité offre une large couverture dans quatre domaines principaux :

Adversary Intelligence: collecte automatisée continue, rapport de renseignement humain, et alerte haute fidélité des cybercriminels de premier plan ciblant et affectant près de toutes les industries et zones géographiques à travers le monde.

Malware Intelligence: analyse et surveillance en temps quasi réel de l'activité des logiciels malveillants et infrastructure de commandement et de contrôle fournissant un flux constant d'indicateurs techniques, rapports de campagne et informations techniques approfondies sur les principales familles de logiciels malveillants déployés par les acteurs de la menace.

Vulnerability Intelligence: rapports réguliers sur les vulnérabilités et surveillance continue des les précurseurs de l'exploitation tels que l'intérêt de l'acteur, le statut d'exploit, la militarisation, productisation et bien plus encore.

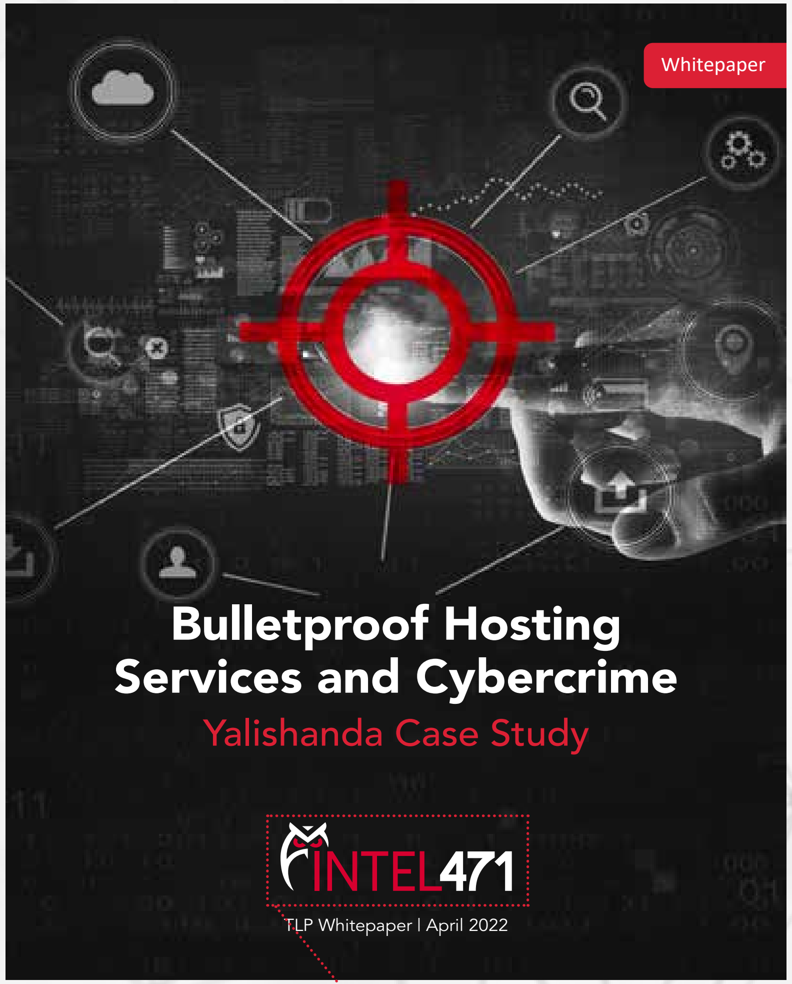
Credential Intelligence: surveillance continue et alerte des informations d'identification compromises associés à vos employés, VIP, clients et fournisseurs tiers et vendeurs.

Avantages du renseignement sur la cybercriminalité

Obtenez un aperçu continu et en temps quasi réel de l'underground cybercriminel. Cybercrime Intelligence fournit des informations proactives et révolutionnaires sur méthodologie des cybercriminels de premier plan – sélection des cibles, actifs et outils utilisés, associés et autres facilitateurs qui les soutiennent.

La collecte sur le terrain et l'analyse au siège d'Intel 471 sont capables de directement prendre en charge les besoins en matière de renseignement dans une organisation couvrant votre sécurité, équipes de direction, de vulnérabilité, de risque, d'enquête et de fraude.

Accédez à l'intelligence finie ou exploitez la collection sous-jacente et brute, c'est à vous de décider tu! Nous fournissons des livrables pour plusieurs équipes et niveaux de maturité.



Whitepaper

Bulletproof Hosting Services and Cybercrime

Yalishanda Case Study

INTEL471

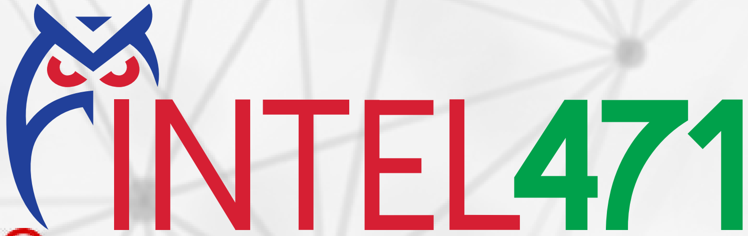
TLP Whitepaper | April 2022

Logo placement bottom right

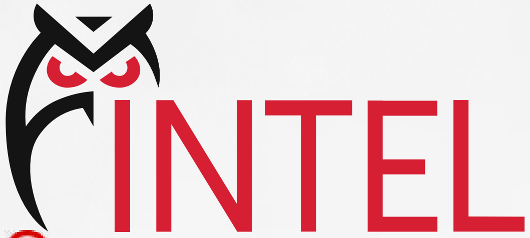
Logo placement bottom middle

LOGO DON'TS

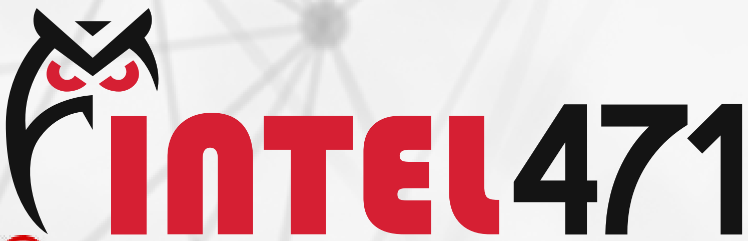
Intel 471 logo should never be altered. The guidelines apply for all elements use to create the logo and any content that is owned and controlled by Intel 471. Using our logo consistently ensures brand recognition and allows for creativity elsewhere.



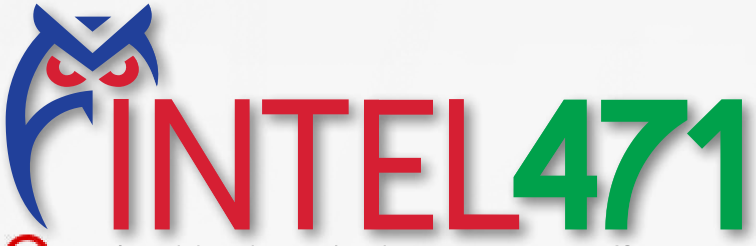
Don't change approved company colors.



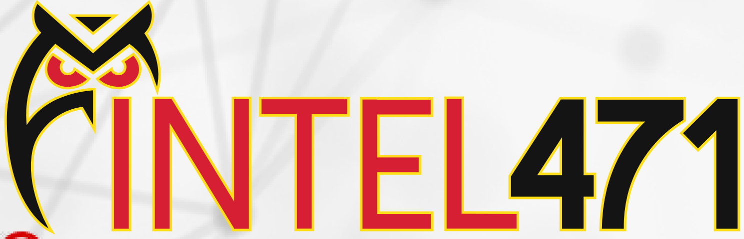
Don't use logo without complete logotype.



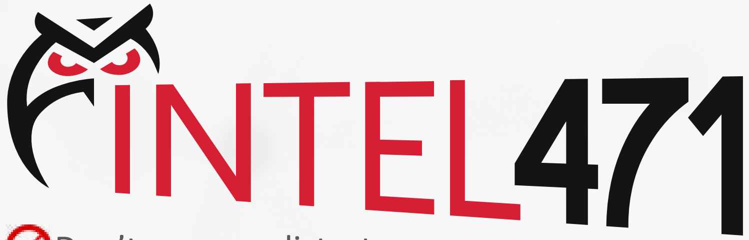
Don't change or substitute approved fonts.



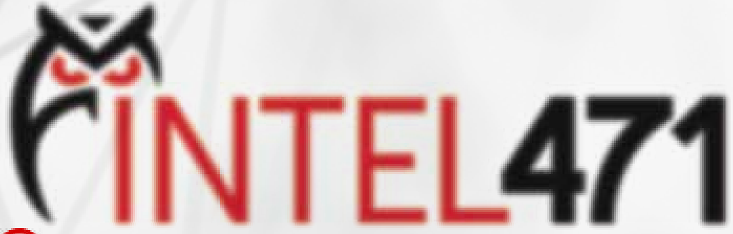
Don't add a drop shadow or mirror effects.



Don't use a stroke around any part of logo.



Don't warp or distort appearance.



Don't blur or add digital effects.

LOGO TYPOGRAPHY

The typeface Avenir Book reflects the authenticity of Intel 471's knowledge of cyber security and their products and services. It is balanced with the Avenir bold font to bring in the modern day visual. These fonts may be substituted for Arial if Avenir is not available.

TYPOGRAPHY FOR MARKETING

Headline: Avenir Bold

Aa Bb Cc Dd Ee Ff Gg Hh Ii Jj Kk Ll Mm Nn Oo Pp Qq Rr Ss Tt Uu Vv Ww Xx Yy Zz

Subhead or Body Copy: Avenir Medium

Aa Bb Cc Dd Ee Ff Gg Hh Ii Jj Kk Ll Mm Nn Oo Pp Qq Rr Ss Tt Uu Vv Ww Xx Yy Zz

Body Copy: Avenir Book

Aa Bb Cc Dd Ee Ff Gg Hh Ii Jj Kk Ll Mm Nn Oo Pp Qq Rr Ss Tt Uu Vv Ww Xx Yy Zz

SUBSTITUTE TYPOGRAPHY

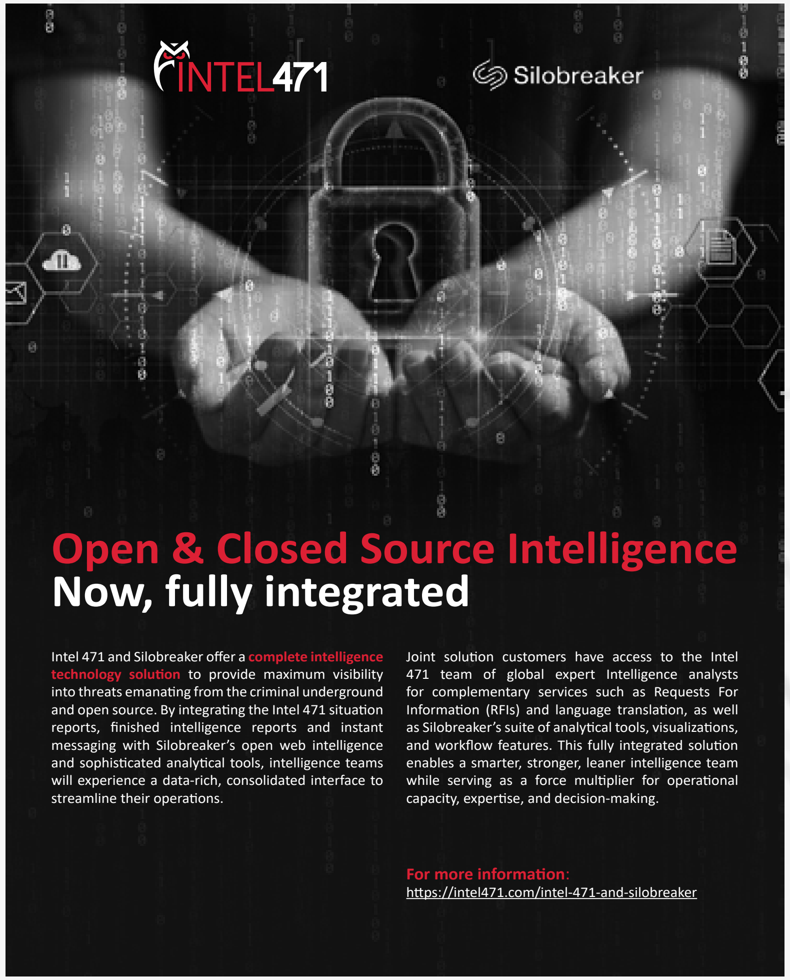
Headline: Arial Black

Aa Bb Cc Dd Ee Ff Gg Hh Ii Jj Kk Ll Mm Nn Oo Pp Qq Rr Ss Tt Uu Vv Ww Xx Yy Zz

Subhead or Body Copy: Arial Regular

Aa Bb Cc Dd Ee Ff Gg Hh Ii Jj Kk Ll Mm Nn Oo Pp Qq Rr Ss Tt Uu Vv Ww Xx Yy Zz

Typography use examples

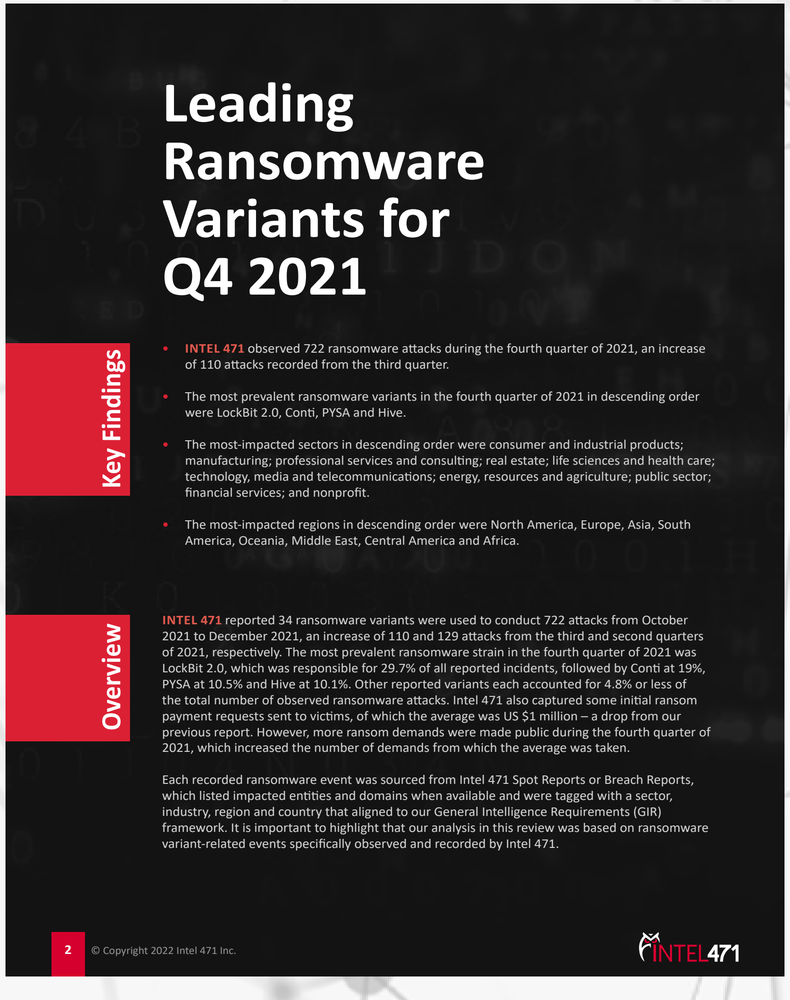


Open & Closed Source Intelligence
Now, fully integrated

Intel 471 and Silobreaker offer a **complete intelligence technology solution** to provide maximum visibility into threats emanating from the criminal underground and open source. By integrating the Intel 471 situation reports, finished intelligence reports and instant messaging with Silobreaker's open web intelligence and sophisticated analytical tools, intelligence teams will experience a data-rich, consolidated interface to streamline their operations.

Joint solution customers have access to the Intel 471 team of global expert Intelligence analysts for complementary services such as Requests For Information (RFIs) and language translation, as well as Silobreaker's suite of analytical tools, visualizations, and workflow features. This fully integrated solution enables a smarter, stronger, leaner intelligence team while serving as a force multiplier for operational capacity, expertise, and decision-making.

For more information:
https://intel471.com/intel-471-and-silobreaker



Leading Ransomware Variants for Q4 2021

Key Findings

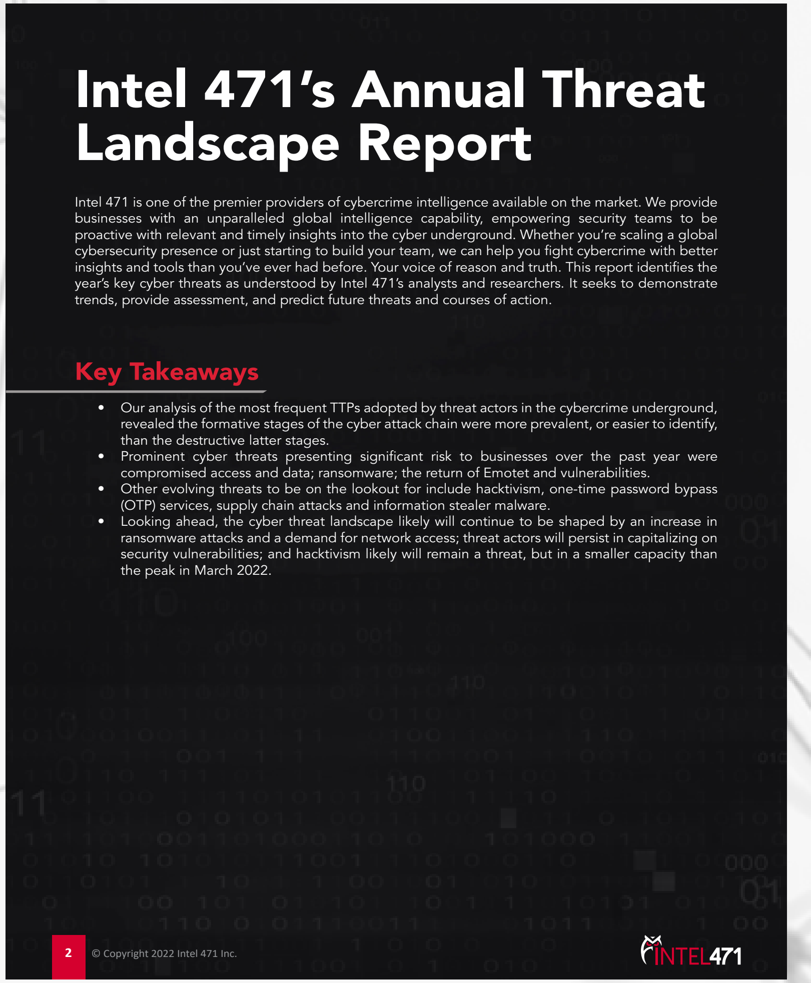
- **INTEL 471** observed 722 ransomware attacks during the fourth quarter of 2021, an increase of 110 attacks recorded from the third quarter.
- The most prevalent ransomware variants in the fourth quarter of 2021 in descending order were LockBit 2.0, Conti, PYSA and Hive.
- The most-impacted sectors in descending order were consumer and industrial products; manufacturing; professional services and consulting; real estate; life sciences and health care; technology, media and telecommunications; energy, resources and agriculture; public sector; financial services; and nonprofit.
- The most-impacted regions in descending order were North America, Europe, Asia, South America, Oceania, Middle East, Central America and Africa.

Overview

INTEL 471 reported 34 ransomware variants were used to conduct 722 attacks from October 2021 to December 2021, an increase of 110 and 129 attacks from the third and second quarters of 2021, respectively. The most prevalent ransomware strain in the fourth quarter of 2021 was LockBit 2.0, which was responsible for 29.7% of all reported incidents, followed by Conti at 19%, PYSA at 10.5% and Hive at 10.1%. Other reported variants each accounted for 4.8% or less of the total number of observed ransomware attacks. Intel 471 also captured some initial ransom payment requests sent to victims, of which the average was US $1 million – a drop from our previous report. However, more ransom demands were made public during the fourth quarter of 2021, which increased the number of demands from which the average was taken.

Each recorded ransomware event was sourced from Intel 471 Spot Reports or Breach Reports, which listed impacted entities and domains when available and were tagged with a sector, industry, region and country that aligned to our General Intelligence Requirements (GIR) framework. It is important to highlight that our analysis in this review was based on ransomware variant-related events specifically observed and recorded by Intel 471.

2 © Copyright 2022 Intel 471 Inc.



Intel 471's Annual Threat Landscape Report

Intel 471 is one of the premier providers of cybercrime intelligence available on the market. We provide businesses with an unparalleled global intelligence capability, empowering security teams to be proactive with relevant and timely insights into the cyber underground. Whether you're scaling a global cybersecurity presence or just starting to build your team, we can help you fight cybercrime with better insights and tools than you've ever had before. Your voice of reason and truth. This report identifies the year's key cyber threats as understood by Intel 471's analysts and researchers. It seeks to demonstrate trends, provide assessment, and predict future threats and courses of action.

Key Takeaways

- Our analysis of the most frequent TTPs adopted by threat actors in the cybercrime underground, revealed the formative stages of the cyber attack chain were more prevalent, or easier to identify, than the destructive latter stages.
- Prominent cyber threats presenting significant risk to businesses over the past year were compromised access and data; ransomware; the return of Emotet and vulnerabilities.
- Other evolving threats to be on the lookout for include hacktivism, one-time password bypass (OTP) services, supply chain attacks and information stealer malware.
- Looking ahead, the cyber threat landscape likely will continue to be shaped by an increase in ransomware attacks and a demand for network access; threat actors will persist in capitalizing on security vulnerabilities; and hacktivism likely will remain a threat, but in a smaller capacity than the peak in March 2022.

2 © Copyright 2022 Intel 471 Inc.

PRIMARY AND ACCENT COLORS

Our company primary colors are red and black. This presents a strong mood of optimism, passion, and trust. Our alternate colors are amber, yellow, and white. We have carefully selected these colors and feel they do not compromise the strength of our brand.

COLORS FOR PRINT

RED: PRIMARY
CMYK: 9, 100, 88, 0
RGB: 214, 0, 47
#D6002F

BLACK: PRIMARY
CMYK: 73, 67, 65, 82
RGB: 18, 18, 18
#121212

AMBER: ACCENT
CMYK: 11, 53, 97, 0
RGB: 221, 136, 45
#DD882D

TEAL: ACCENT
CMYK: 86, 31, 49, 8
RGB: 0, 128, 128
#008080

GRAY: ACCENT
CMYK: 57, 48, 48, 15
RGB: 112, 112, 112
#707070

COLORS FOR DIGITAL

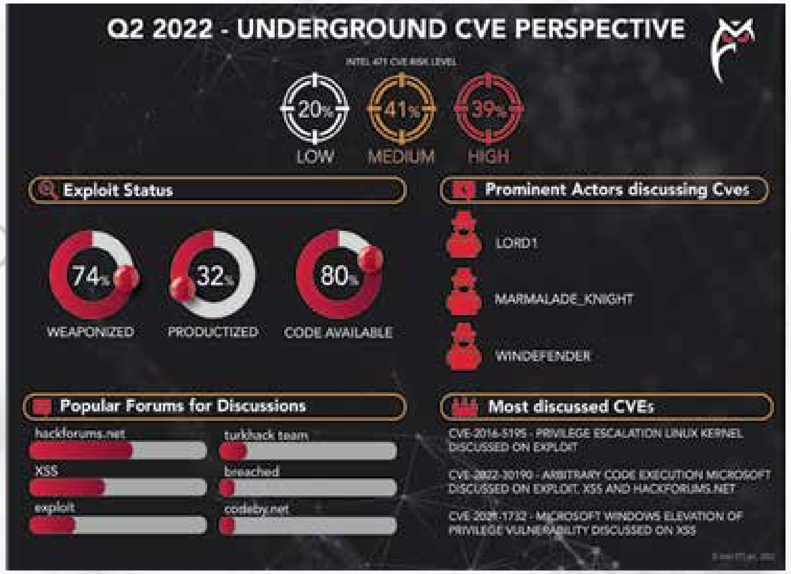
RED: PRIMARY
CMYK: 0, 100, 75, 20
RGB: 196, 17, 52
#CC0033

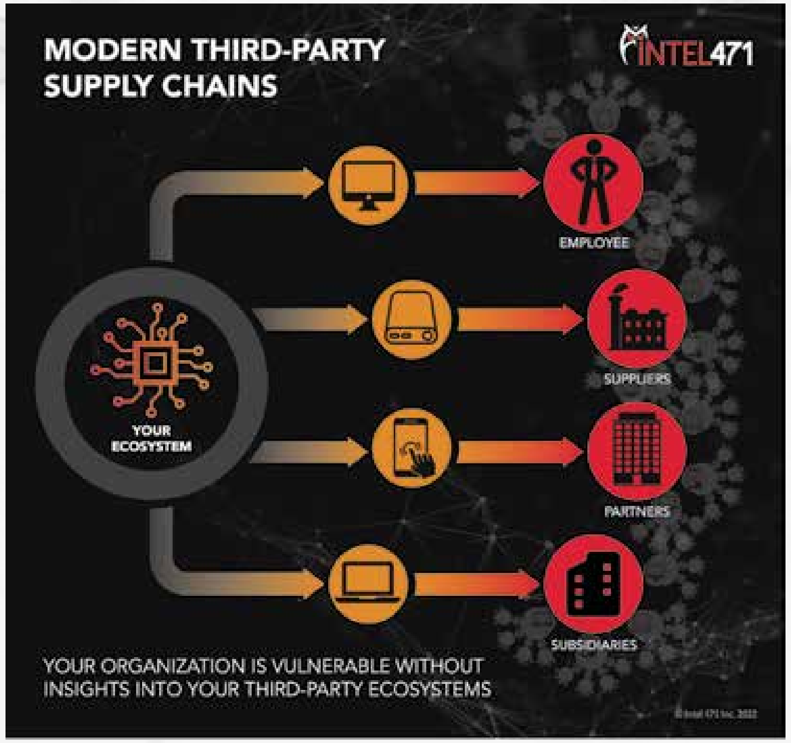
BLACK: PRIMARY
CMYK: 0, 0, 0, 95
RGB: 27, 27, 27
#1B1B1B

AMBER: ACCENT
CMYK: 0, 25, 75, 20
RGB: 209, 162, 75
#CC9933

TEAL: ACCENT
CMYK: 81, 20, 42, 1
RGB: 0, 153, 153
#009999

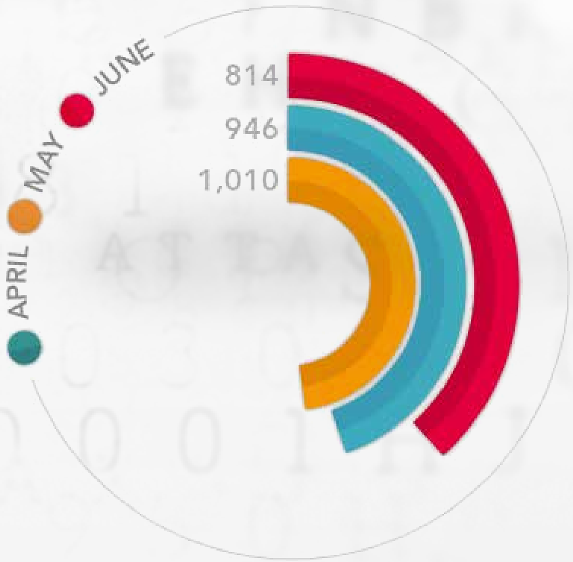
GRAY: ACCENT
CMYK: 60, 51, 51, 20
RGB: 102, 102, 102
#666666




MODERN THIRD-PARTY SUPPLY CHAINS
INTEL471
YOUR ECOSYSTEM
EMPLOYEE
SUPPLIERS
PARTNERS
SUBSIDIARIES
YOUR ORGANIZATION IS VULNERABLE WITHOUT INSIGHTS INTO YOUR THIRD-PARTY ECOSYSTEMS
© Intel 471 Inc. 2022

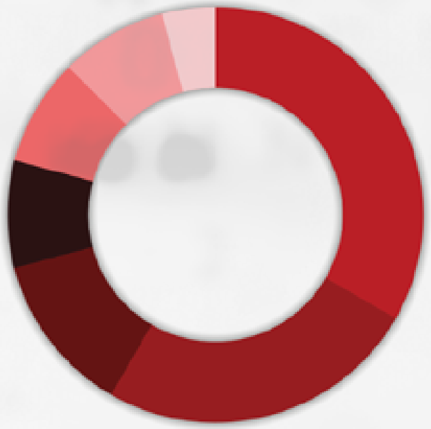
Color use examples

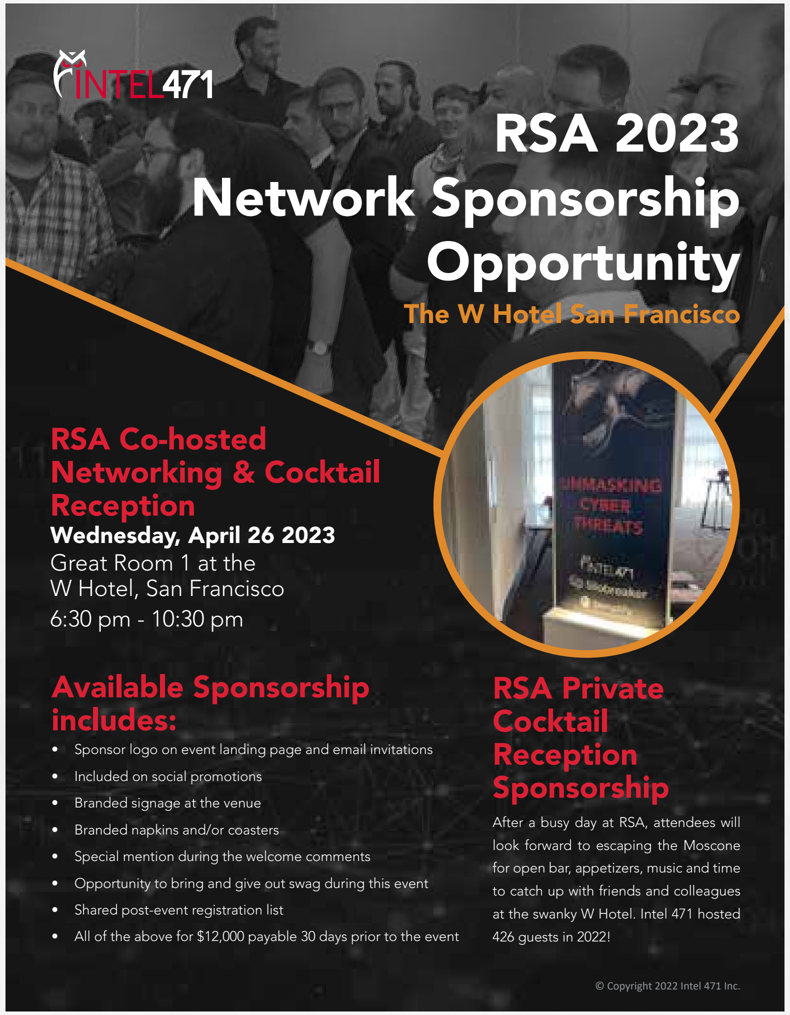
GOOGLE CLOUD



Victim Revenue

33.4%	Not Available
25%	10-50 million
12.5%	Over 1 billion
8.3%	500 million-1 billion
8.3%	50-100 million
8.3%	100-500 million
4.2%	5-10 million





RSA 2023 Network Sponsorship Opportunity

The W Hotel San Francisco

RSA Co-hosted Networking & Cocktail Reception

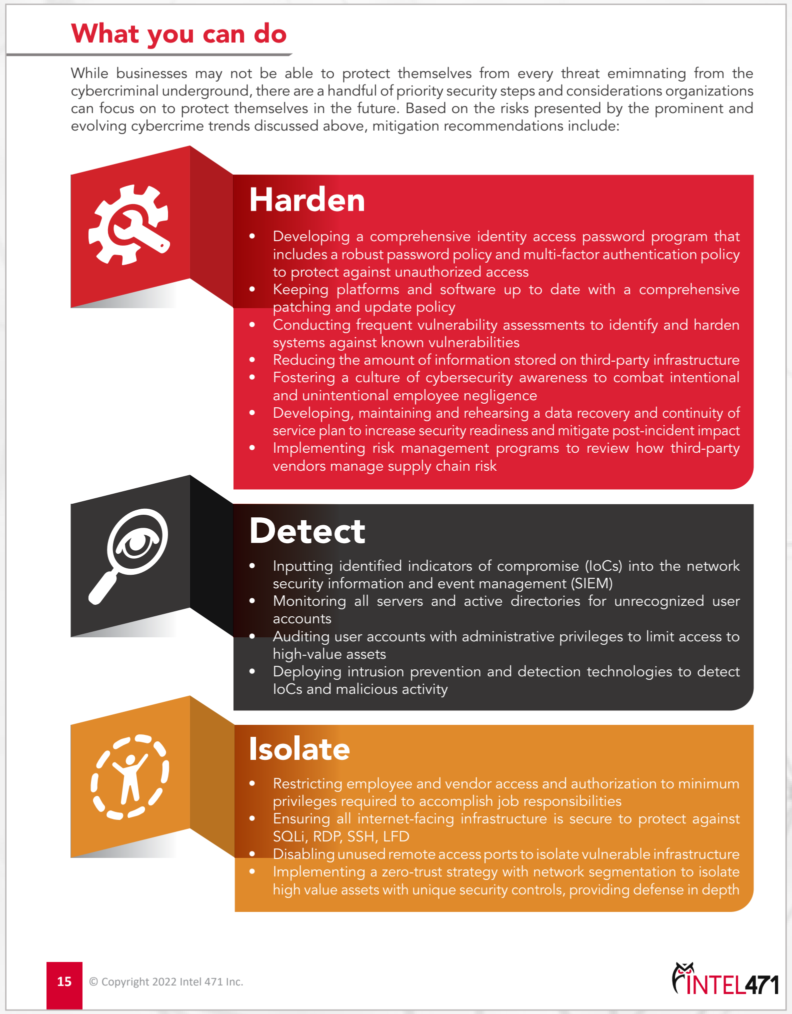
Wednesday, April 26 2023
Great Room 1 at the
W Hotel, San Francisco
6:30 pm - 10:30 pm

Available Sponsorship includes:

- Sponsor logo on event landing page and email invitations
- Included on social promotions
- Branded signage at the venue
- Branded napkins and/or coasters
- Special mention during the welcome comments
- Opportunity to bring and give out swag during this event
- Shared post-event registration list
- All of the above for $12,000 payable 30 days prior to the event

RSA Private Cocktail Reception Sponsorship

After a busy day at RSA, attendees will look forward to escaping the Moscone for open bar, appetizers, music and time to catch up with friends and colleagues at the swanky W Hotel. Intel 471 hosted 426 guests in 2022!



What you can do

While businesses may not be able to protect themselves from every threat emimnating from the cybercriminal underground, there are a handful of priority security steps and considerations organizations can focus on to protect themselves in the future. Based on the risks presented by the prominent and evolving cybercrime trends discussed above, mitigation recommendations include:

Harden

- Developing a comprehensive identity access password program that includes a robust password policy and multi-factor authentication policy to protect against unauthorized access
- Keeping platforms and software up to date with a comprehensive patching and update policy
- Conducting frequent vulnerability assessments to identify and harden systems against known vulnerabilities
- Reducing the amount of information stored on third-party infrastructure
- Fostering a culture of cybersecurity awareness to combat intentional and unintentional employee negligence
- Developing, maintaining and rehearsing a data recovery and continuity of service plan to increase security readiness and mitigate post-incident impact
- Implementing risk management programs to review how third-party vendors manage supply chain risk

Detect

- Inputting identified indicators of compromise (IoCs) into the network security information and event management (SIEM)
- Monitoring all servers and active directories for unrecognized user accounts
- Auditing user accounts with administrative privileges to limit access to high-value assets
- Deploying intrusion prevention and detection technologies to detect IoCs and malicious activity

Isolate

- Restricting employee and vendor access and authorization to minimum privileges required to accomplish job responsibilities
- Ensuring all internet-facing infrastructure is secure to protect against SQLi, RDP, SSH, LFD
- Disabling unused remote access ports to isolate vulnerable infrastructure
- Implementing a zero-trust strategy with network segmentation to isolate high value assets with unique security controls, providing defense in depth

15 INTEL471

TEXTURE BACKGROUND

Photo-realistic imagery is preferred over computer-generated renders. When choosing background images, look for dark, monochrome, low contrast photography, abstract, or graffiti images.

BACKGROUND

MARKETING IMAGES

- We like to show technical images
- We like show underground hackers
- We like to show the owl that reflect our brand
- We like to show cyber security themes
- We treat our images with brand colors
- We like to use monochrome images for a dramatic mood

IMAGERY

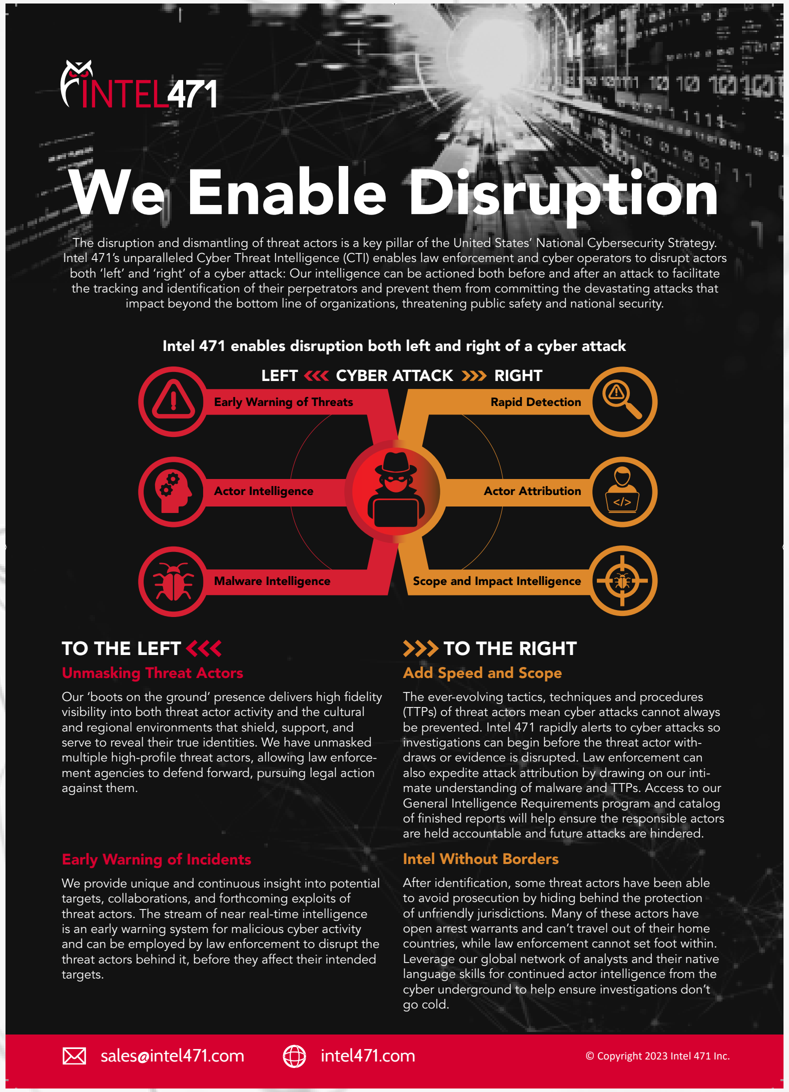
MARKETING

MARKETING

Intel 471 will use all marketing materials to help the business stand apart from the competition. They will be our primary link between our company and the customers. Showcasing our logo with our products and services will help reinforce our brand. We will be strategic with placement so that we can convey a concise message to our audience.

BRANDING

We will use our brand to enrich our products and services. We will give meaning to our organization by creating and shaping our identity in consumers' minds. Our goal is to help people quickly identify and experience our brand, and give them a reason to choose our products over our competition by clarifying our differences. Our success will be to attract and retain loyal customers and other stakeholders by delivering a product that is always aligned with what the brand promises.



INTEL471

We Enable Disruption

The disruption and dismantling of threat actors is a key pillar of the United States' National Cybersecurity Strategy. Intel 471's unparalleled Cyber Threat Intelligence (CTI) enables law enforcement and cyber operators to disrupt actors both 'left' and 'right' of a cyber attack: Our intelligence can be actioned both before and after an attack to facilitate the tracking and identification of their perpetrators and prevent them from committing the devastating attacks that impact beyond the bottom line of organizations, threatening public safety and national security.

Intel 471 enables disruption both left and right of a cyber attack

LEFT <<< CYBER ATTACK >>> RIGHT

Early Warning of Threats

Rapid Detection

Actor Intelligence

Actor Attribution

Malware Intelligence

Scope and Impact Intelligence

TO THE LEFT <<<

Unmasking Threat Actors

Our 'boots on the ground' presence delivers high fidelity visibility into both threat actor activity and the cultural and regional environments that shield, support, and serve to reveal their true identities. We have unmasked multiple high-profile threat actors, allowing law enforcement agencies to defend forward, pursuing legal action against them.

Early Warning of Incidents

We provide unique and continuous insight into potential targets, collaborations, and forthcoming exploits of threat actors. The stream of near real-time intelligence is an early warning system for malicious cyber activity and can be employed by law enforcement to disrupt the threat actors behind it, before they affect their intended targets.

>>> TO THE RIGHT

Add Speed and Scope

The ever-evolving tactics, techniques and procedures (TTPs) of threat actors mean cyber attacks cannot always be prevented. Intel 471 rapidly alerts to cyber attacks so investigations can begin before the threat actor withdraws or evidence is disrupted. Law enforcement can also expedite attack attribution by drawing on our intimate understanding of malware and TTPs. Access to our General Intelligence Requirements program and catalog of finished reports will help ensure the responsible actors are held accountable and future attacks are hindered.

Intel Without Borders

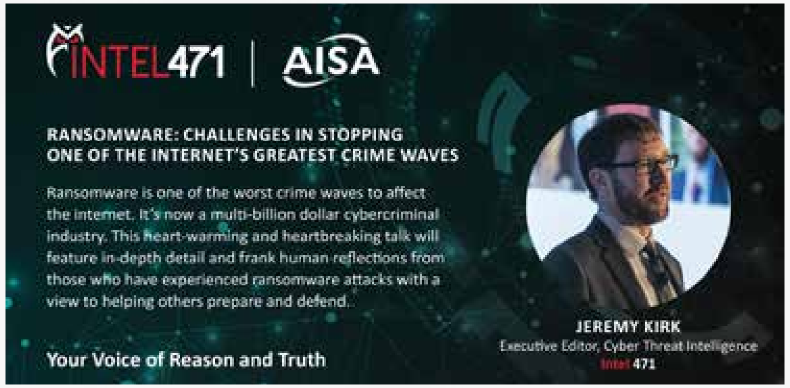
After identification, some threat actors have been able to avoid prosecution by hiding behind the protection of unfriendly jurisdictions. Many of these actors have open arrest warrants and can't travel out of their home countries, while law enforcement cannot set foot within. Leverage our global network of analysts and their native language skills for continued actor intelligence from the cyber underground to help ensure investigations don't go cold.

✉ sales@intel471.com   🌐 intel471.com   © Copyright 2023 Intel 471 Inc.

INTEL471

Your window into cyber underground

Intel 471 empowers security teams to be proactive with our relevant and timely insights into the cyber underground



INTEL471 | AISA

RANSOMWARE: CHALLENGES IN STOPPING ONE OF THE INTERNET'S GREATEST CRIME WAVES

Ransomware is one of the worst crime waves to affect the internet. It's now a multi-billion dollar cybercriminal industry. This heart-warming and heartbreaking talk will feature in-depth detail and frank human reflections from those who have experienced ransomware attacks with a view to helping others prepare and defend.

Your Voice of Reason and Truth

JEREMY KIRK
Executive Editor, Cyber Threat Intelligence
Intel 471

INTEL471

www.intel471.com

Protect your organization, your assets and your people from cybercriminals.

INTEL471

Want help winning the ransomware fight?

Download our GIR Handbook

Learn more at
intel471.com

INTEL471

Defend Against Retail-Centric Fraud & Cyber Threats

Protect your assets and brand from reputational and financial harm

DOWNLOAD WHITEPAPER

INTEL471

FIGHT CYBER THREATS AND WIN

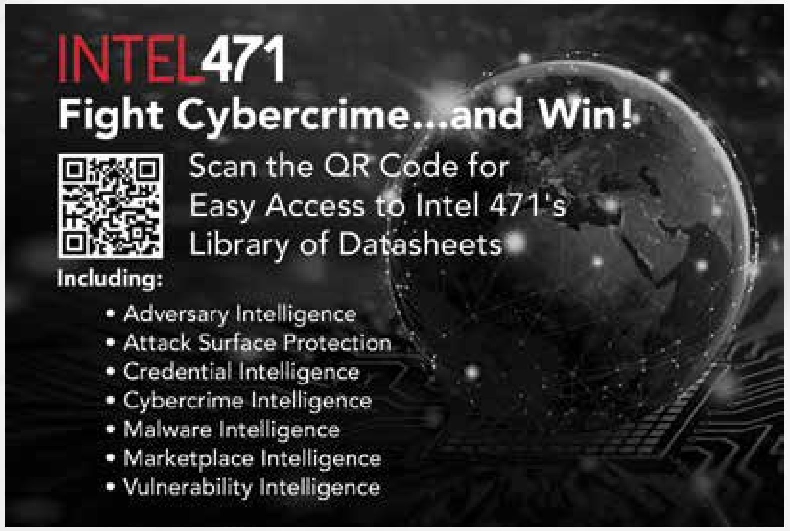
Your organisation deserves the best cyber threat intelligence

INTEL471

Your Voice of Reason and Truth

COLLATERAL

We will use a collection of media to support the sales of our products and services. Materials such as Datasheets, Whitepapers, Powerpoint Presentations, Decks, and Videos will be utilized as sales tools. Our collateral will enhance our brand through a consistent message and other media, and use a balance of information and promotional content.



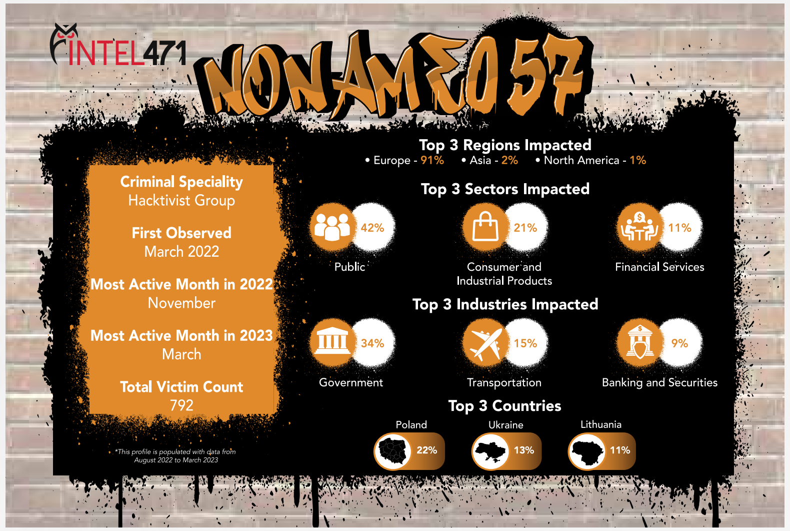
INTEL471

Fight Cybercrime...and Win!

Scan the QR Code for Easy Access to Intel 471's Library of Datasheets

Including:

- Adversary Intelligence
- Attack Surface Protection
- Credential Intelligence
- Cybercrime Intelligence
- Malware Intelligence
- Marketplace Intelligence
- Vulnerability Intelligence



INTEL471

NONAME057

Criminal Speciality
Hacktivist Group

First Observed
March 2022

Most Active Month in 2022
November

Most Active Month in 2023
March

Total Victim Count
792

*This profile is populated with data from August 2022 to March 2023

Top 3 Regions Impacted

• Europe - 91% • Asia - 2% • North America - 1%

Top 3 Sectors Impacted

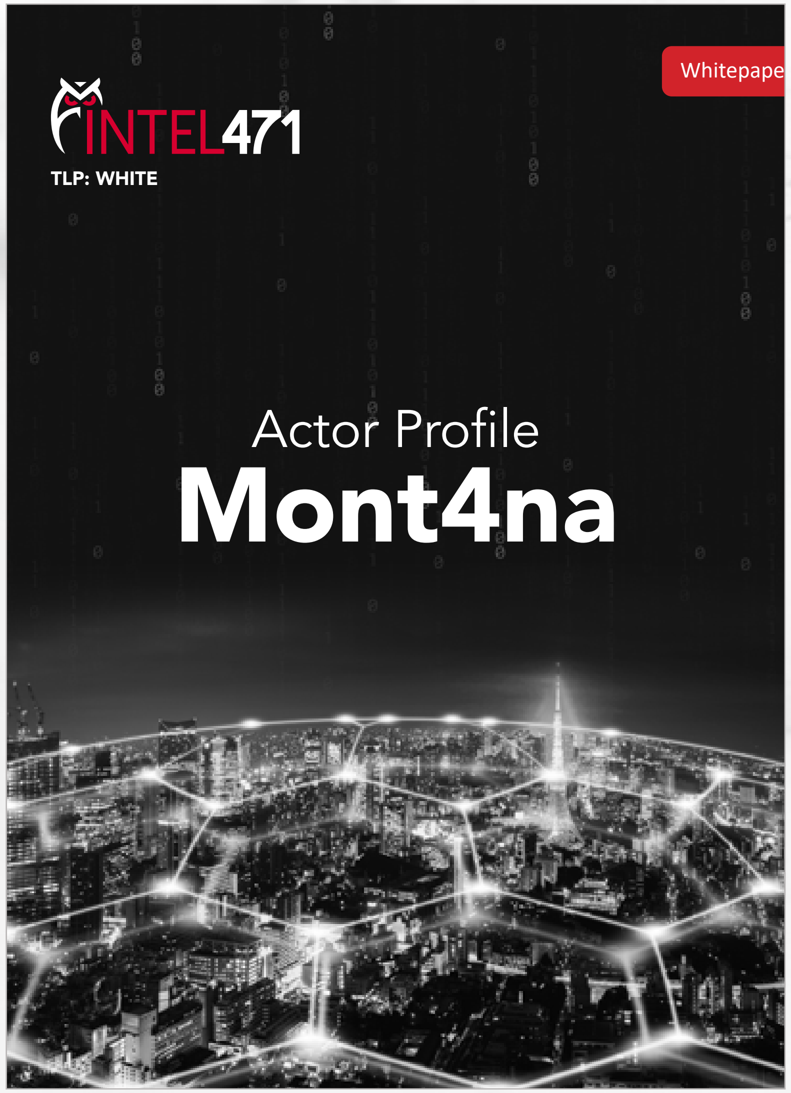
Public	Consumer and Industrial Products	Financial Services
42%	21%	11%

Top 3 Industries Impacted

Government	Transportation	Banking and Securities
34%	15%	9%

Top 3 Countries

Poland	Ukraine	Lithuania
22%	13%	11%



Whitepape

INTEL471

TLP: WHITE

Actor Profile

Mont4na

INTEL471

CU-GIRH

CYBER UNDERGROUND GENERAL INTELLIGENCE REQUIREMENTS HANDBOOK

INTEL471

Building an intelligence plan

A Hands-On Workshop with Intel 471

Are you an intelligence practitioner or stakeholder looking to gain hands-on experience building or enhancing your organization's intelligence plan? Then this workshop is for you! Intel 471 presents an exclusive training for building a successful intelligence program by offering our secret sauce used to safeguard organizations worldwide.

In this exclusive training, you will learn:

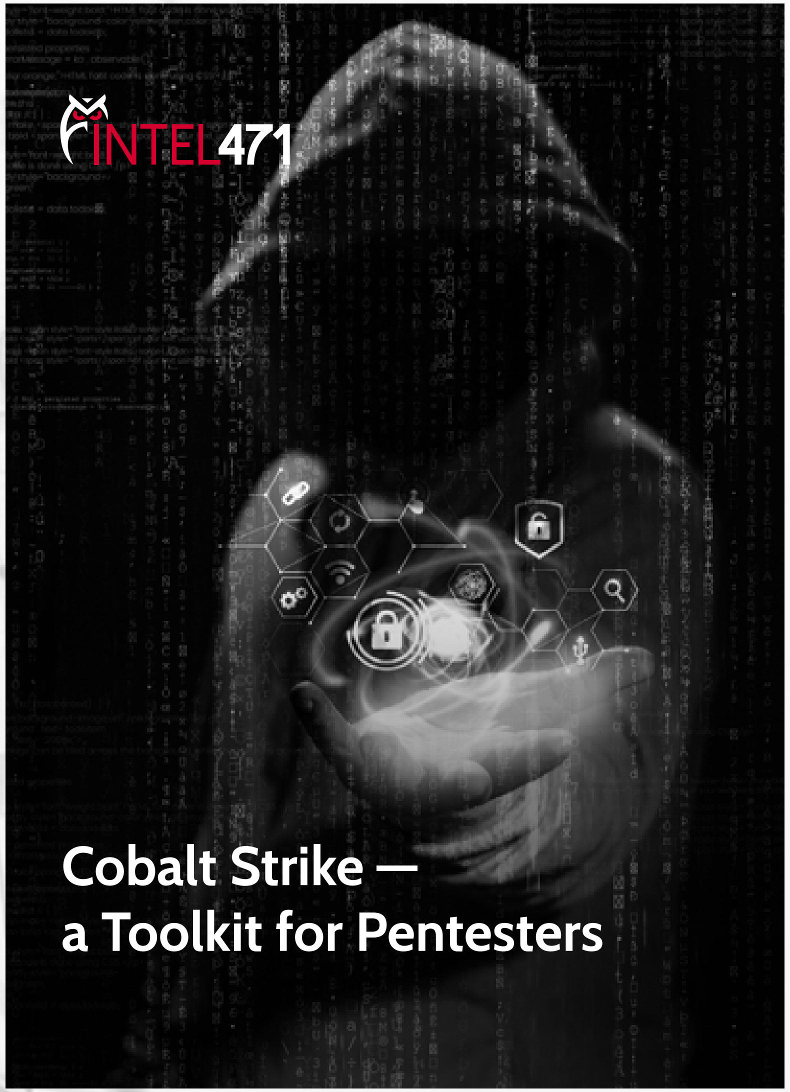
- How to align intelligence plans with stakeholder needs, both individually and at scale
- The core fundamentals of building an intelligence plan
- How to efficiently counter threats and save your organization time and money

See you there!

WORKSHOP DATE:
WED. MAY 17TH, 2023
9:00 A.M.-1:00 P.M. EST

This virtual training led by Intel 471's Chief Intelligence Officer, Michael DeBolt, and Intelligence Operations Coordinator, Garrett Carstens, will include instruction and a scenario-based practical exercise, non-proprietary tools, as well as a catalog of "take home" resources, including training videos, templates, and worksheets that can be used in your own environment.

Participants will receive a copy of the latest GIR Handbook, an intelligence planning workbook, templated planning documents, samples of completed materials, and access to demonstration videos.



INTEL471

Cobalt Strike — a Toolkit for Pentesters

INTERNET AND SOCIAL MEDIA

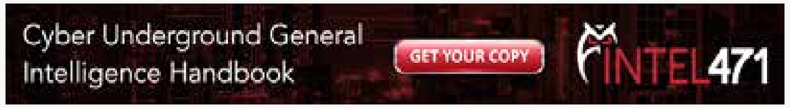
We use social media and the internet to attract clients, get their feedback and build customer loyalty. This has led to an increase in our market reach, including international markets. We require our brand colors, fonts, and images for all designs in a continued effort to strengthen our company's identity.

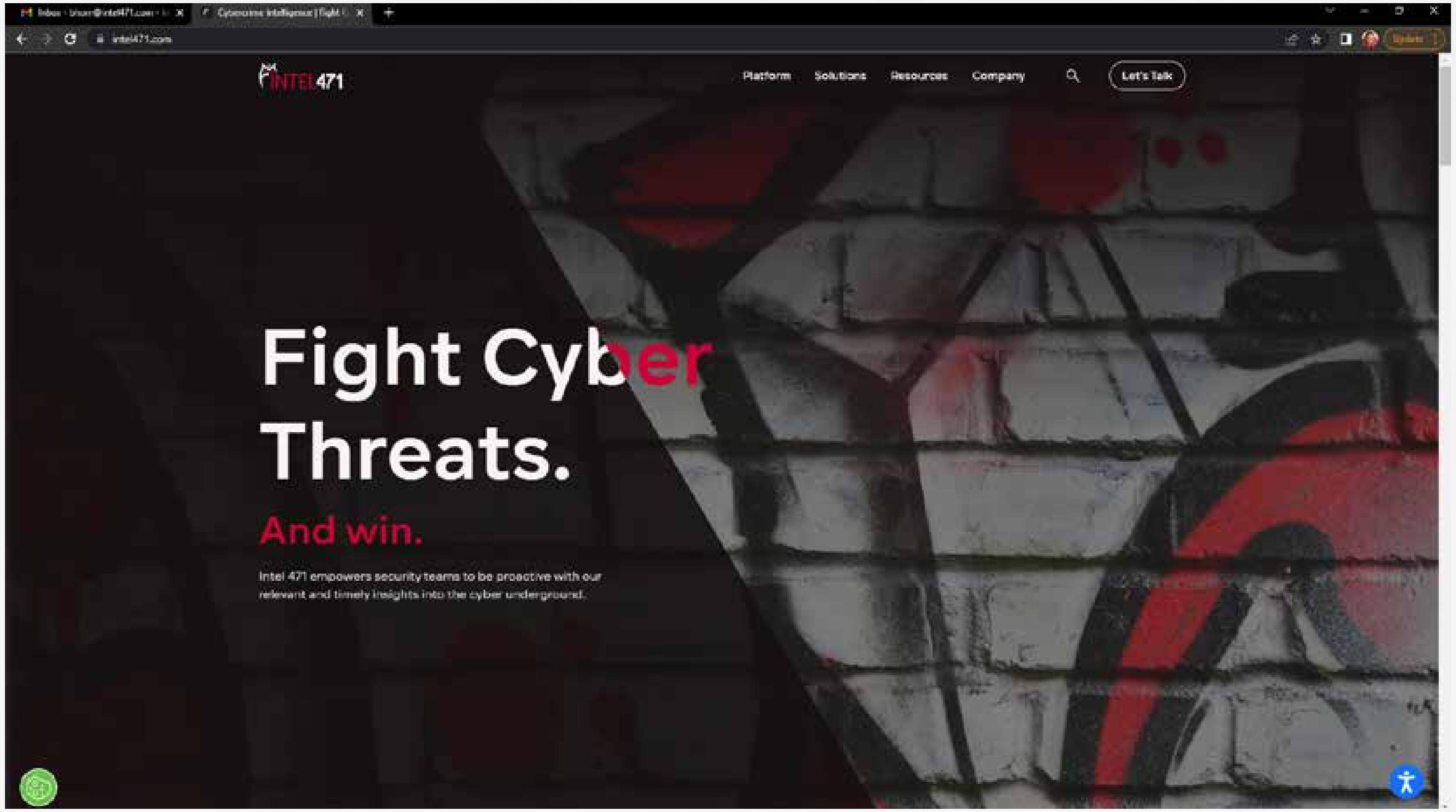
MALWARE - ANALYSIS - ICM ★ VOICE OF REASON AND TRUTH ★ ADVERSARY
INTEL471
INTELLIGENCE DEPARTMENT
INTEL 471 INTELLIGENCE DEPARTMENT
INTEL 471'S SITUATION ROOM BRIEFING
Russia / Ukraine Conflict and
Cybercrime Underground Implications
VOICE OF REASON AND TRUTH

INTEL471
Using Cyber Frameworks to Action
CTI and Enhance Your Security Posture

black hat®
MIDDLE EAST AND AFRICA
15 - 17 November 2022, Riyadh Front Exhibition Centre, Saudi Arabia
Visit Intel 471 at the AmiViz booth, Hall 3, stand #C50
INTEL471
AmiViz
Enterprise Marketplace

INTEL471
Defend Against Fraud and Retail-Centric Threats
Identify key threats impacting the retail industry to protect your assets and brand against reputational and financial harm
DOWNLOAD WHITEPAPER

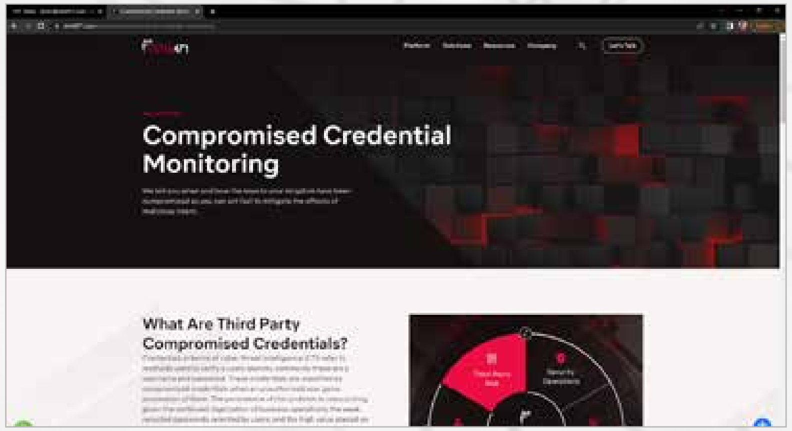




Fight Cyber Threats.

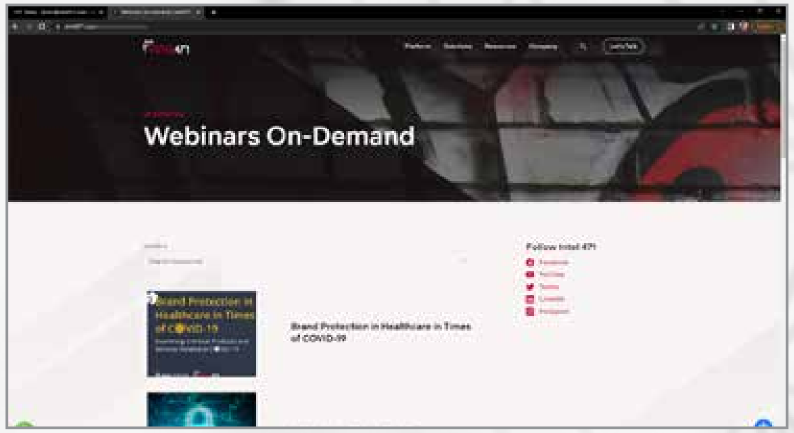
And win.

Intel 471 empowers security teams to be proactive with our relevant and timely insights into the cyber underground.



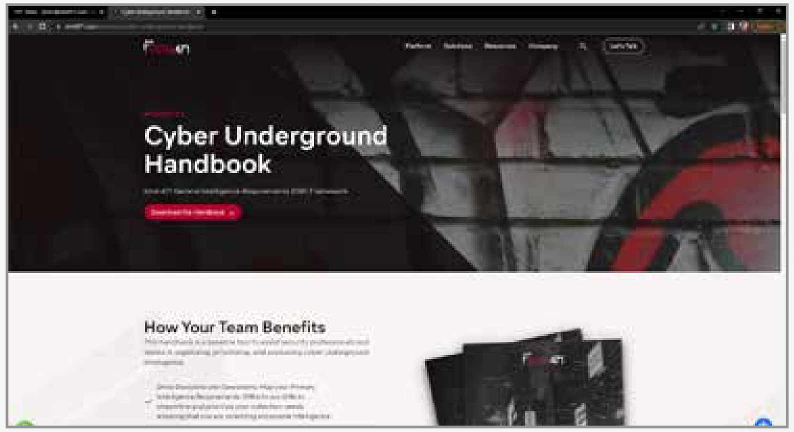
Compromised Credential Monitoring

What Are Third Party Compromised Credentials?



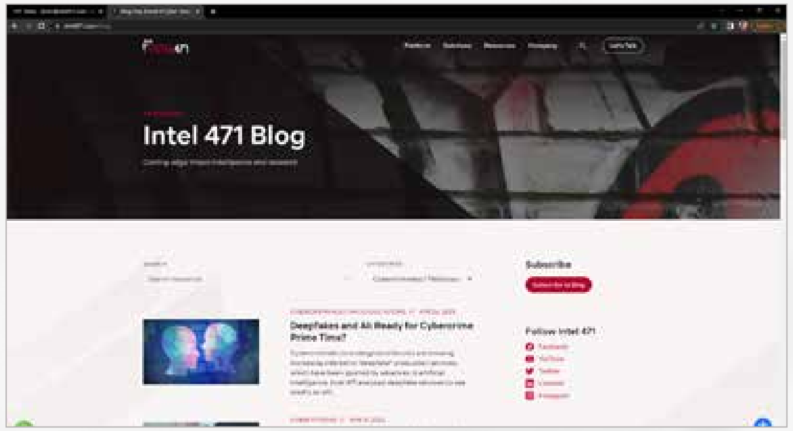
Webinars On-Demand

Brand Protection in Healthcare in Times of COVID-19



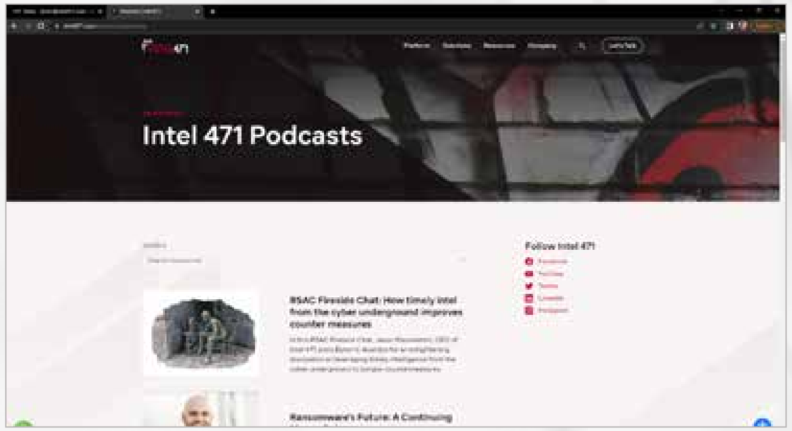
Cyber Underground Handbook

How Your Team Benefits



Intel 471 Blog

Deepfakes and AI Ready for Cybercrime Prime Time?



Intel 471 Podcasts

RSAC Fireside Chat: How timely intel from the cyber underground improves counter measures

Ransomware's Future: A Continuing

EVENTS

We sieze every opportunity to share valuable insights with potential clients such as establishing an agile security program; fostering a human-centric, security-conscious culture; devolving risk ownership; and establishing a new simplified cybersecurity mesh architecture. Our brand sends a clear message that we are evolving and remain knowledgable of effective defences to prevent cyber attacks.

INTEL471
Not all CTI Solutions are Created Equal
exabeam
COLORTOKENS
Unified Zero Trust Platform
ForgeRock
Your Voice of Reason and Truth

ForgeRock
tform
dentities
rgeRock
Rockwell Automation
00:01
Minutes Matter. Seconds Count.
DEEP OBSERVABILITY PIPELINE
East-West Visibilit
Eliminate blind spots
Enhance logs with L4-L7 m
Decrypt TLS 1.3 with comp

Secure
What Matter
Protect Privileged Ac
for your Hybrid workfo
INTEL 471
a regulation.
Y POLICY MANAGEMENT
Threat intelligence
es your
r defen rategy
You
uth

0GLAX0
PASSW
099 D0H

CONCLUSION

Intel 471 continues to provide our clients with unparalleled global intelligence capability for humans and machines. Whether scaling their cybersecurity presence or just starting to build their team, we can help fight cyber threats.

INTEL471

1209 N. Orange
Wilmington, DE 19801
800.833.1471
intel471.com