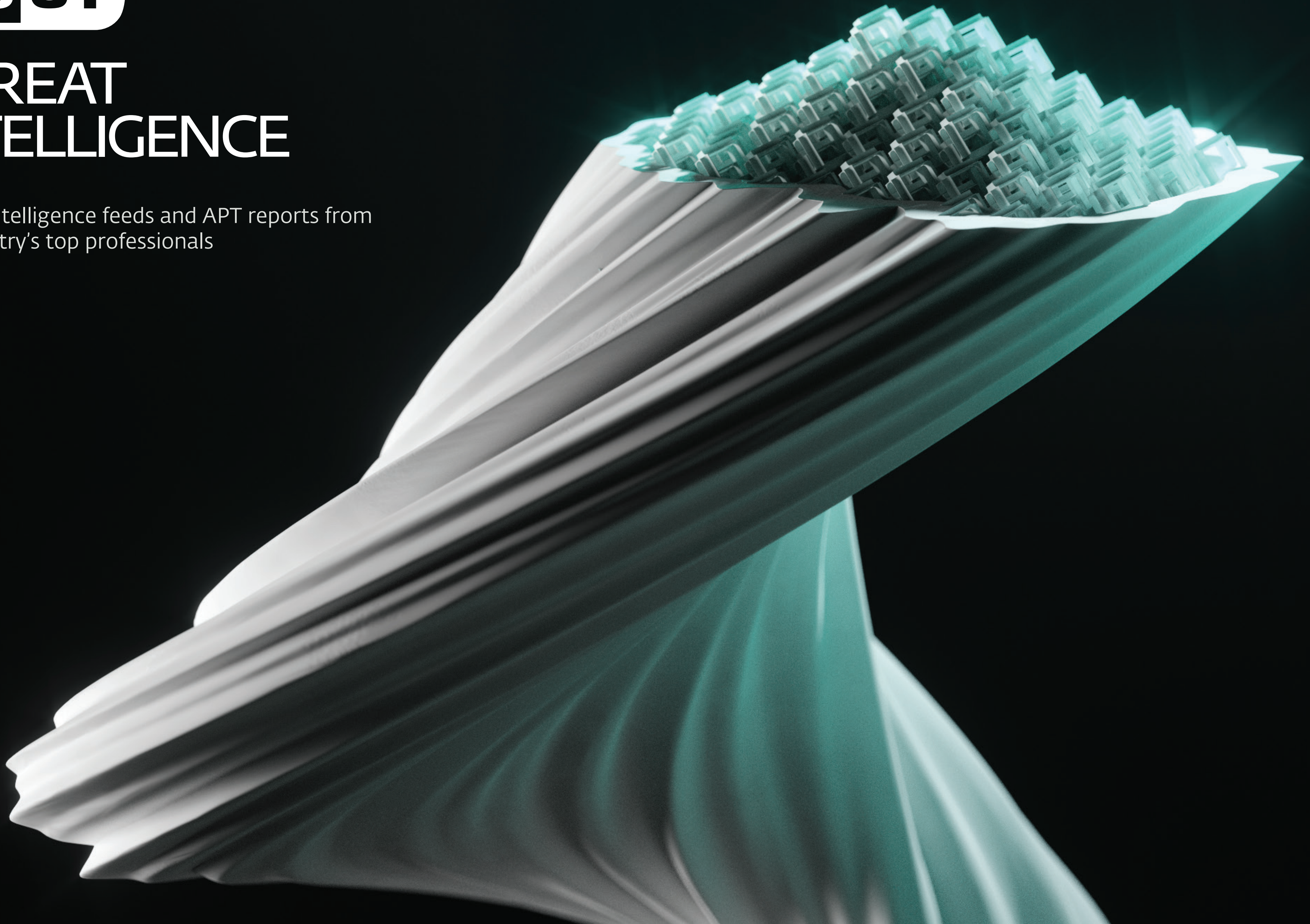
THREAT INTELLIGENCE

Unique intelligence feeds and APT reports from the industry's top professionals



Why threat intelligence?

Stop information overload and get data relevant to your organization

OVERCOME INFORMATION OVERLOAD

Ransomware, zero-days, advanced persistent threats, targeted attacks and botnets are all concerns for businesses around the world. The problem is that, due to the volume of different threats, organizations are unable to easily understand which proactive defenses and mitigations are the most important.

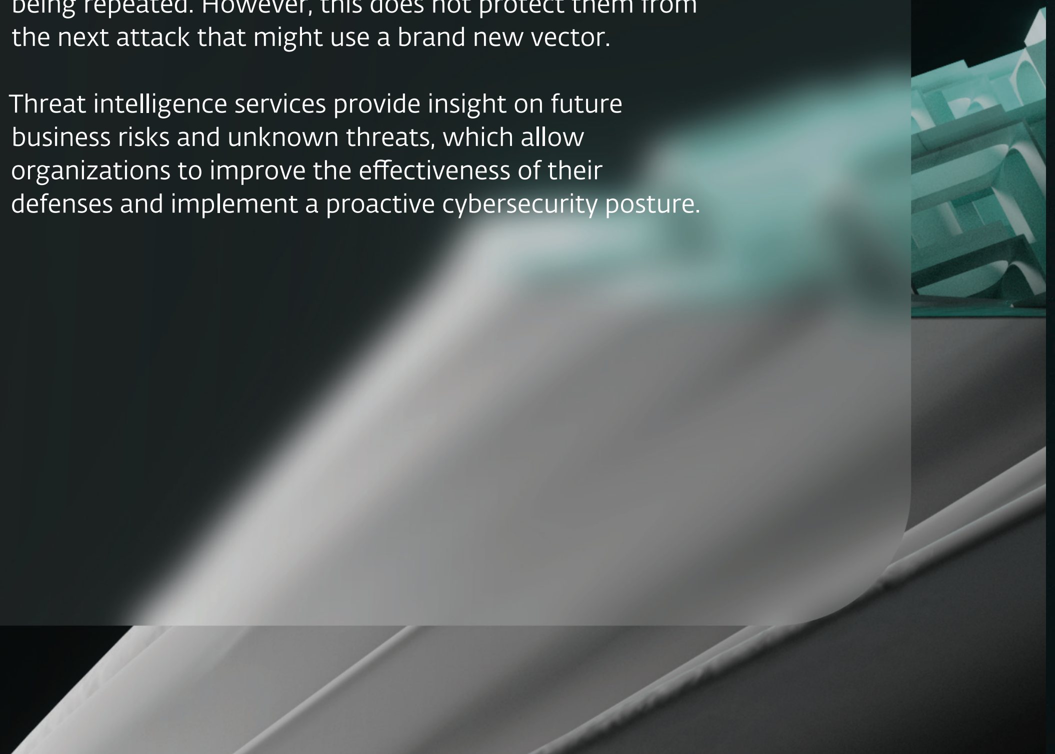
This ultimately leads to organizations scrambling to try and find meaningful information among limited data sets, such as their own networks, or the extremely large datasets that they find via external sources. Threat intelligence services help sift through the information overload and provide the most relevant information for specific organizations.

Threat intelligence services allow organizations to prioritize emerging threats quickly and easily, which leaves them more time to proactively implement new defenses against them.

FIGHT THREATS PROACTIVELY

Today's cybersecurity landscape is constantly evolving with new attack methods and never before seen threats. When an attack or data breach occurs, organizations are typically surprised that their defenses were compromised, or are completely unaware that the attack even happened. After the attack is finally discovered, organizations rush to reactively implement mitigations to stop this attack from being repeated. However, this does not protect them from the next attack that might use a brand new vector.

Threat intelligence services provide insight on future business risks and unknown threats, which allow organizations to improve the effectiveness of their defenses and implement a proactive cybersecurity posture.



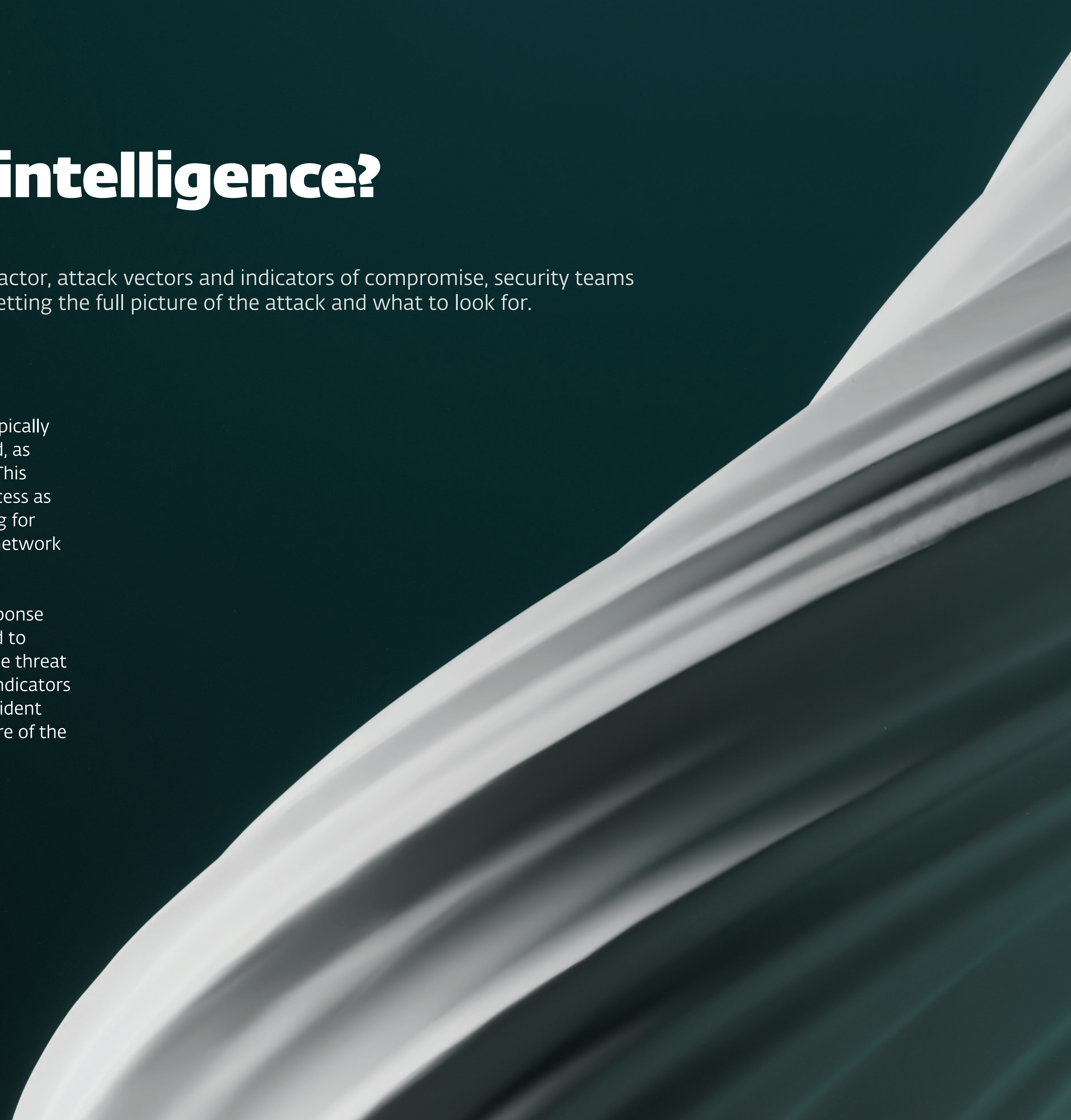
Why threat intelligence?

By providing information on the threat actor, attack vectors and indicators of compromise, security teams can reduce incident response time by getting the full picture of the attack and what to look for.

ACCELERATE INCIDENT RESPONSE

When a data breach occurs, security teams typically need to figure out how the incident happened, as well as identify which devices were affected. This process is usually a very long and manual process as engineers sift through their network searching for abnormalities which might indicate that the network was compromised.

Threat intelligence services allow incident response teams to fully understand and quickly respond to data breaches. By providing information on the threat actor, malware behavior, attack vectors and indicators of compromise, security teams can reduce incident response time by understanding the full picture of the attack as well as what to look for.



The ESET advantage

Human expertise backed by machine learning. Our reputation system, LiveGrid® is made up of 110 million sensors worldwide, and verified by our R&D centers.

1

HUMAN EXPERTISE BACKED BY MACHINE LEARNING

The use of machine learning to automate decisions and evaluate possible threats is a vital part of our approach. But it is only as strong as the people who stand behind the system. Human expertise is paramount in providing the most accurate threat intelligence possible, because threat actors can be intelligent opponents.

2

STRONG REPUTATION SYSTEM — LIVEGRID®

ESET Endpoint products contain a cloud reputation system which feeds relevant information about the most recent threats and benign files. Our reputation system, LiveGrid® is made up of 110 million sensors worldwide, the output of which is verified by our R&D centers. This gives customers the highest level of confidence when viewing information and reports within their console.

3

EU ORIGINS, WORLDWIDE PRESENCE

Based in the European Union, ESET has been in the security industry for over 30 years, has 22 offices worldwide, 13 R&D facilities and a presence in over 200 countries and territories. This helps to provide our customers with a global perspective on all the most recent trends and threats.

The ESET advantage

GET UNIQUE INSIGHTS

ESET gathers threat intelligence from a unique range of sources and has unparalleled in-the-field experience that helps you fight increasingly sophisticated cybersecurity attacks.

MAKE CRUCIAL DECISIONS, FASTER

Anticipate threats and make faster, better decisions thanks to comprehensive ESET reports and curated feeds. Reduce your exposure to prevailing threats, forewarned by experts.

AUTOMATE THREAT INVESTIGATION

ESET technology searches for threats constantly, across multiple layers, from pre-boot to resting state. Benefit from telemetry on all countries where ESET detects emerging threats.

STAY AHEAD OF ADVERSARIES

ESET follows the money, specifically monitoring those places where we have detected APT groups that target Western companies: Russia, China, North Korea, Iran. You'll know about new threats first.

IMPROVE YOUR SECURITY POSTURE

Informed by ESET intelligence feeds, enhance your threat hunting and remediation capabilities, block APTs and ransomware, and improve your cybersecurity architecture.

Advanced Persistent Threat (APT) Reports

PUTTING OUR BEST RESEARCH AT YOUR FINGERTIPS

Our research team is well known in the digital security industry, thanks to our award winning We Live Security blog. The team's excellent research and APT activity summaries are available, along with much more detailed information. ESET customers get an exclusive early preview of all We Live Security content.

MAKE CRUCIAL DECISIONS FAST

All this helps organizations make crucial decisions and provides a strategic advantage in the fight against digital crime. It brings an understanding of what is happening on the 'bad side of the internet' and provides crucial context, so that your organization can make internal preparations quickly.

ACTIONABLE, CURATED CONTENT

Reports provide a great deal of context for what is going on and why. Thanks to this, organizations can prepare in advance for what might be coming. Importantly, our experts make sure the content is easy to understand.

ACCESS TO ESET ANALYST

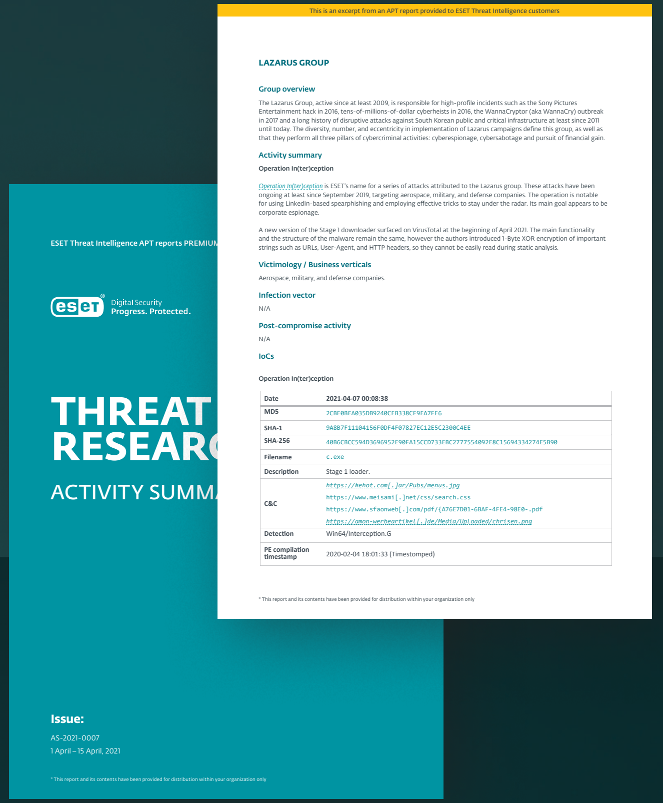
Every customer ordering the APT Reports PREMIUM package will have also access to an ESET analyst for up to four hours each month. This provides the opportunity to discuss topics in greater detail and help resolve any outstanding issues.

WITH APT REPORTS, YOU GET

- Access to private, in-depth technical analysis
- APT activity summary reports
- A monthly summary for your C-level executives
- Direct access to an ESET cybersecurity professional
- Access to our MISP server

IN-DEPTH ANALYSIS

The package includes monthly in-depth technical analysis reports describing recent campaigns, new toolsets and related subjects. You'll also get an activity summary report every two weeks that describes the latest APT campaigns ESET researchers have been tracking from various threat actors, as well as their targets and, of course, the associated Indicators of Compromise (IoCs). A monthly overview combines information from all Technical Analysis and Activity Summary reports released in the previous month into a shorter and more digestible form.



ESET Threat Intelligence APT reports PREMIUM

eset Digital Security Progress. Protected.

THREAT RESEARC

ACTIVITY SUMMA

Issue:

AS-2021-0007

1 April – 15 April, 2021

* This report and its contents have been provided for distribution within your organization only

This is an excerpt from an APT report provided to ESET Threat Intelligence customers

LAZARUS GROUP

Group overview

The Lazarus Group, active since at least 2009, is responsible for high-profile incidents such as the Sony Pictures Entertainment hack in 2016, tens-of-millions-of-dollar cyberheists in 2016, the WannaCryptor (aka WannaCry) outbreak in 2017 and a long history of disruptive attacks against South Korean public and critical infrastructure at least since 2011 until today. The diversity, number, and eccentricity in implementation of Lazarus campaigns define this group, as well as that they perform all three pillars of cybercriminal activities: cyberespionage, cybersabotage and pursuit of financial gain.

Activity summary

Operation In(ter)ception

Operation In(ter)ception is ESET's name for a series of attacks attributed to the Lazarus group. These attacks have been ongoing at least since September 2019, targeting aerospace, military, and defense companies. The operation is notable for using LinkedIn-based spearphishing and employing effective tricks to stay under the radar. Its main goal appears to be corporate espionage.

A new version of the Stage 1 downloader surfaced on VirusTotal at the beginning of April 2021. The main functionality and the structure of the malware remain the same, however the authors introduced 1-Byte XOR encryption of important strings such as URLs, User-Agent, and HTTP headers, so they cannot be easily read during static analysis.

Victimology / Business verticals

Aerospace, military, and defense companies.

Infection vector

N/A

Post-compromise activity

N/A

IoCs

Operation In(ter)ception

Date	2021-04-07 00:08:38
MD5	2CBE0BEA035DB9240CEB338CF9EA7FE6
SHA-1	9A8B7F11104156F0DF4F07827EC12E5C2300C4EE
SHA-256	40B6CBCC594D3696952E90FA15CCD733EBC2777554092E8C15694334274E5B90
Filename	c.exe
Description	Stage 1 loader.
C&C	https://kehot.com[.]ar/Pubs/menus.jpg https://www.meisami[.]net/css/search.css https://www.sfaonweb[.]com/pdf/{A76E7D01-6BAF-4FE4-98E0-.pdf https://amon-werbeartikel[.]de/Media/Uploaded/chrisen.png
Detection	Win64/Interception.G
PE compilation timestamp	2020-02-04 18:01:33 (Timestomped)

* This report and its contents have been provided for distribution within your organization only

Availability of ESET Threat Intelligence reports and feeds vary by country. Please contact local ESET representative for more information.

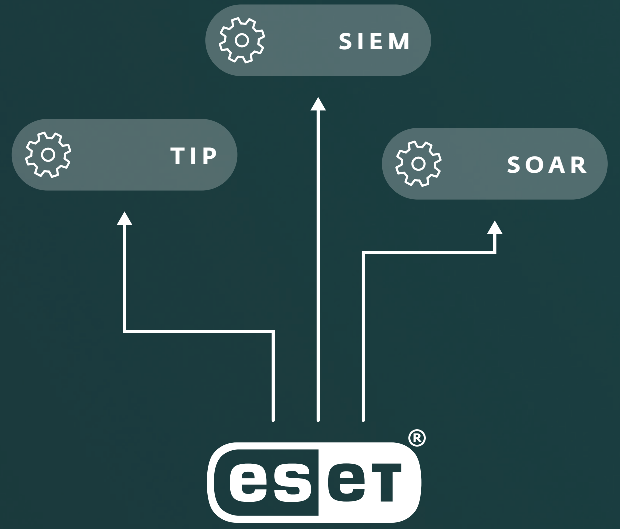
Integrate ESET Threat Intelligence into your system

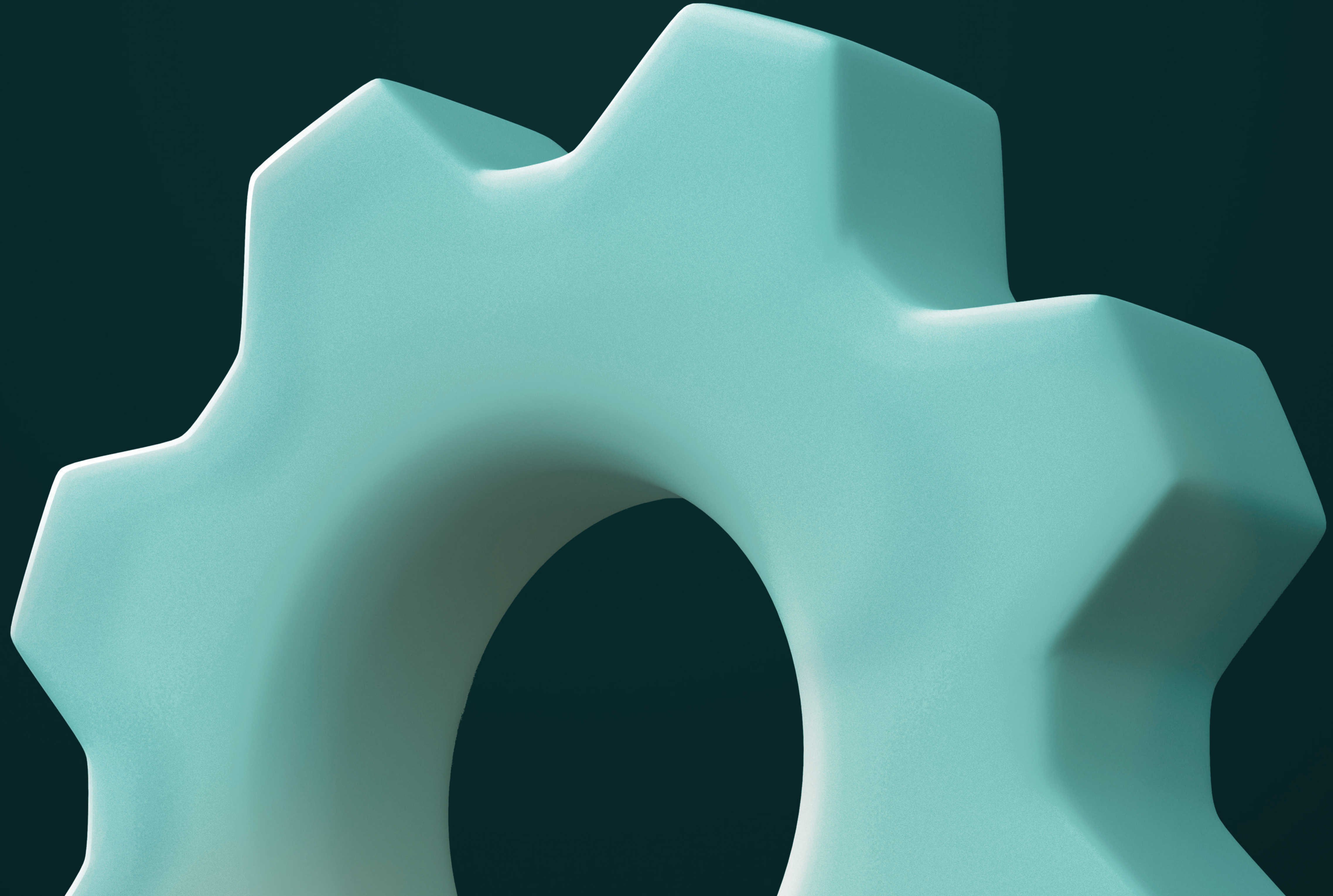
Integrating ESET telemetry is simple and will enrich your **TIP**, **SIEM** or **SOAR**

We have a **comprehensive API with full documentation**

We supply data in **standardized formats** - such as JSON and STIX feeds via TAXII – so that integration into any tool is possible

For IBM QRadar, Anomali, and Logpoint we have **step-by-step integration manuals** for fast and easy implementation – and we're continually adding others





ESET proprietary intelligence feeds

Enrich your view of the worldwide threat landscape based on unique telemetry. ESET feeds come from our research centers around the globe, providing a holistic picture and enabling you to quickly block IoCs in your environment. Feeds are in the formats • JSON • STIX 2.0

MALICIOUS FILES FEED

Understand which malicious files are being seen in the wild. The feed features domains which are considered malicious, including domain name, IP address, detection of file downloaded from URL, and detection of the file which was trying to access the URL. This feed consists of shared hashes of malicious executable files and associated data.

DOMAIN FEED

Block domains which are considered malicious. The feed includes domain names, IP addresses, and the dates associated with them. The feed ranks domains based on their severity, which lets you adjust your response accordingly, for example, to only block high severity domains.

IP FEED

This feed shares IPs considered to be malicious and the data associated with them. The structure of the data is very similar to that used for the Domain and URL Feeds. The main use-case here is to understand which malicious IPs are currently prevalent in the wild, block those IPs which are of high severity, spot those that are less severe, and investigate further, based on additional data, to see if they have already caused harm.

URL FEED

Similar to Domain Feed, the URL Feed looks at specific addresses. It includes detailed information on data related to the URL, as well as information about the domains which host them. All the information is filtered to show only high confidence results and includes easy to understand information on why the URL was flagged.

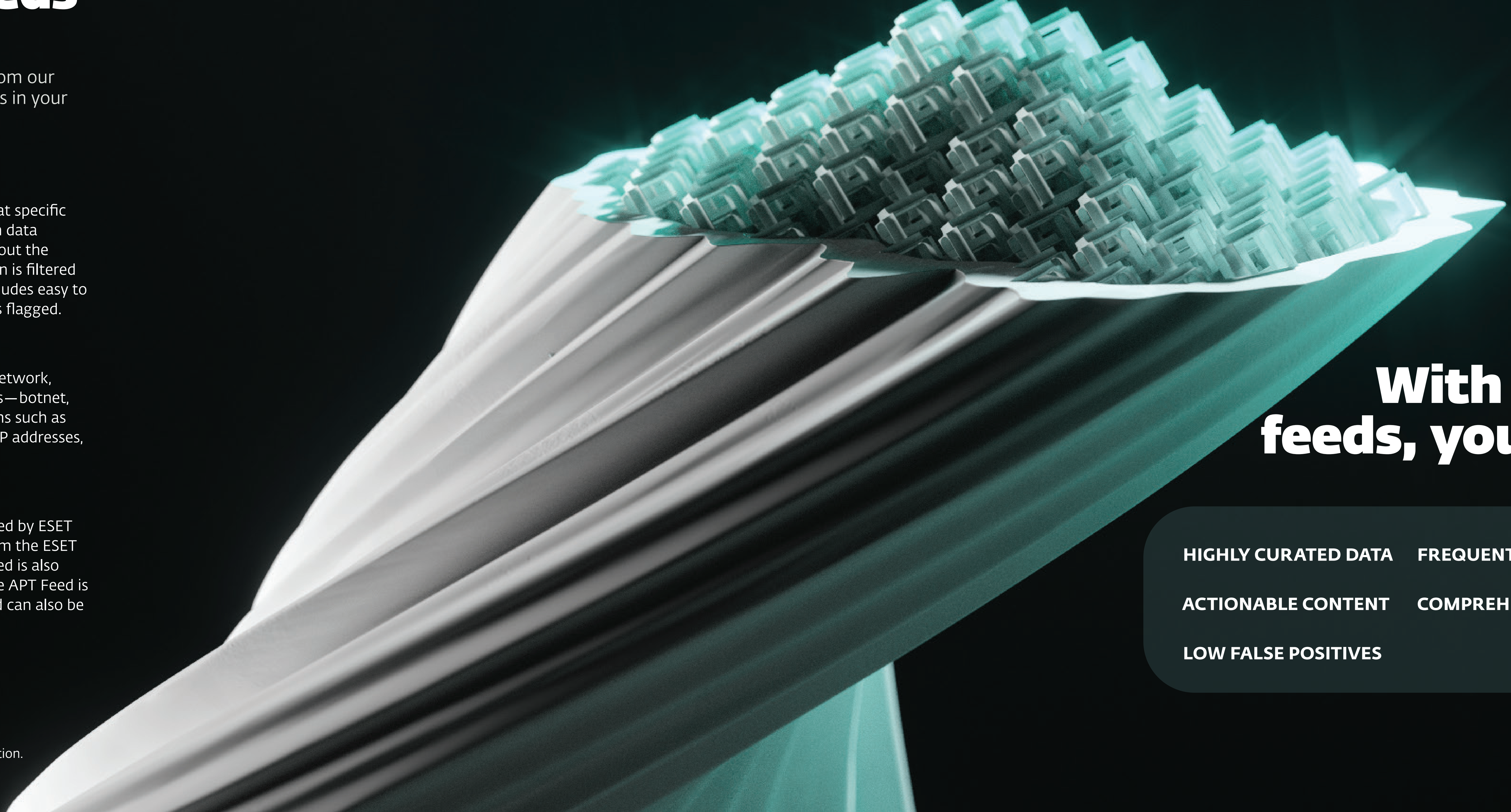
BOTNET FEED

Based on ESET's proprietary botnet tracker network, Botnet feed features three types of sub-feeds—botnet, C&C and targets. Data provided includes items such as detection, hash, last alive, files downloaded, IP addresses, protocols, targets and other information.

APT FEED

This feed consists of APT information produced by ESET research. In general, the feed is an export from the ESET internal MISP server. All the data that is shared is also explained in greater detail in APT reports. The APT Feed is also part of APT reports offering, but the feed can also be purchased separately.

Availability of ESET Threat Intelligence reports and feeds vary by country. Please contact your local ESET representative for more information.



With ESET feeds, you get

- HIGHLY CURATED DATA
- FREQUENT UPDATES
- ACTIONABLE CONTENT
- COMPREHENSIVE API
- LOW FALSE POSITIVES

About ESET

For more than 30 years, ESET® has been developing industry-leading IT security software and services to deliver comprehensive, multilayered protection against cybersecurity threats for businesses and consumers worldwide. ESET has long pioneered machine learning and cloud technologies that prevent, detect and respond to malware. ESET is a privately owned company that promotes scientific research and development worldwide.

ESET IN NUMBERS

1bn+	400k+	200+	13
internet users protected	business customers	countries & territories	global R&D centers

SOME OF OUR CUSTOMERS

protected by ESET since 2016
more than 32,000 endpoints

ISP security partner since 2008
2 milion customer base

protected by ESET since 2017
more than 9,000 endpoints

protected by ESET since 2016
more than 4,000 mailboxes

Why choose ESET?

SOME OF OUR TOP AWARDS

ISO SECURITY CERTIFIED

ISO SECURITY CERTIFIED

ESET is compliant with ISO/IEC 27001:2013, an internationally recognized and applicable security standard in implementing and managing information security. The certification is granted by the third-party accredited certification body SGS and demonstrates ESET's full compliance with industry-leading best practices.

INDUSTRY RECOGNITION

Recognized as Established Vendor in 2021 Gartner® Peer Insights™ 'Voice of the Customer': EPP

ESET recognized for giving back to the community with a 2021 Tech Cares Award from TrustRadius

Gartner, "Gartner® Peer Insights™ 'Voice of the Customer': Endpoint Protection Platforms", By Peer Contributors, 25 November 2021. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. The Gartner Peer Insights Customer First badge is a trademark and service mark of Gartner, Inc., and/or its affiliates, and is used herein with permission. The Gartner Peer Insights Customer First program constitutes an organization's commitment to solicit reviews from its customers using programmatic sourcing strategies and best practices. They neither represent the views of, nor constitute an endorsement by, Gartner or its affiliates.
Read more: https://blogs.gartner.com/reviews-pages/customer-first-landing-page/

Why choose ESET?

ANALYST RECOGNITION

IDC ANALYZE THE FUTURE

ESET has been recognized as a Major Player in endpoint security in the IDC MarketScape: Worldwide Modern Endpoint Security for Enterprises 2021 and and IDC MarketScape Modern Endpoint Security for Small and Midsize Businesses 2021 Vendor Assessment.

THE RADICATI GROUP, INC. A TECHNOLOGY MARKET RESEARCH FIRM

ESET has been recognized as a `Top Player' for the fourth year in a row in Radicati's Advanced Persistent Threat (APT) Protection - Market Quadrant 2021.

MITRE ATT&CK

The rigorous MITRE ATT&CK Evaluation demonstrated the undeniable qualities of ESET EDR technology and validated the strong vision for ESET Inspect's future.

> “*The implementation was very straightforward. In cooperation with ESET's well-trained technical staff, we were up and running our new ESET security solution in a few hours.*”
>
> IT Manager, Diamantis Masoutis S.A., Greece, 6,000+ seats

> “*We were most impressed with the support and assistance we received. In addition to being a great product, the excellent care and support we got was what really led us to move all of Primoris' systems to ESET as a whole.*”
>
> Joshua Collins, Data Center Operations Manager, Primoris Services Corporation, USA, 4,000+ seats

Digital Security
Progress. Protected.