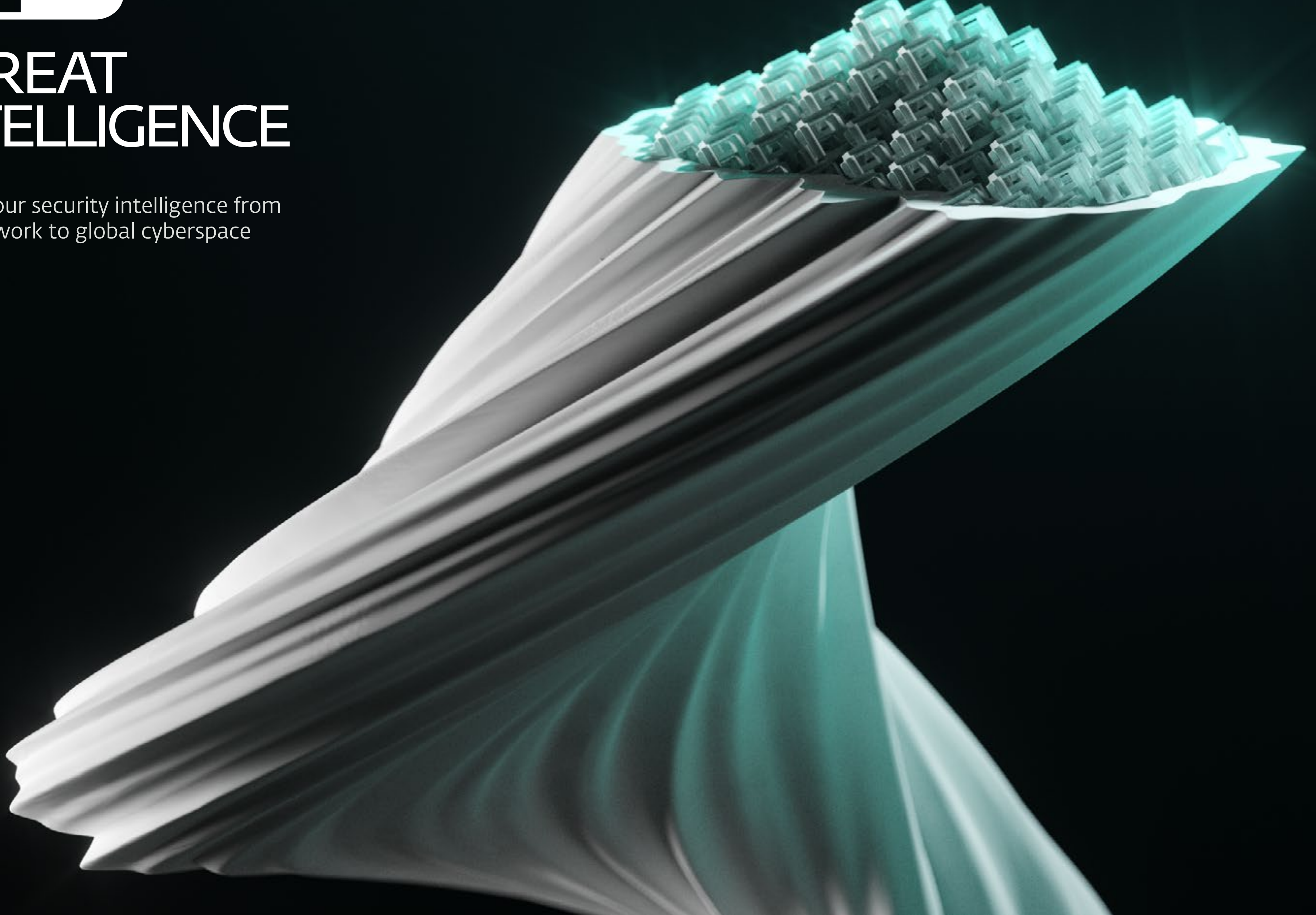
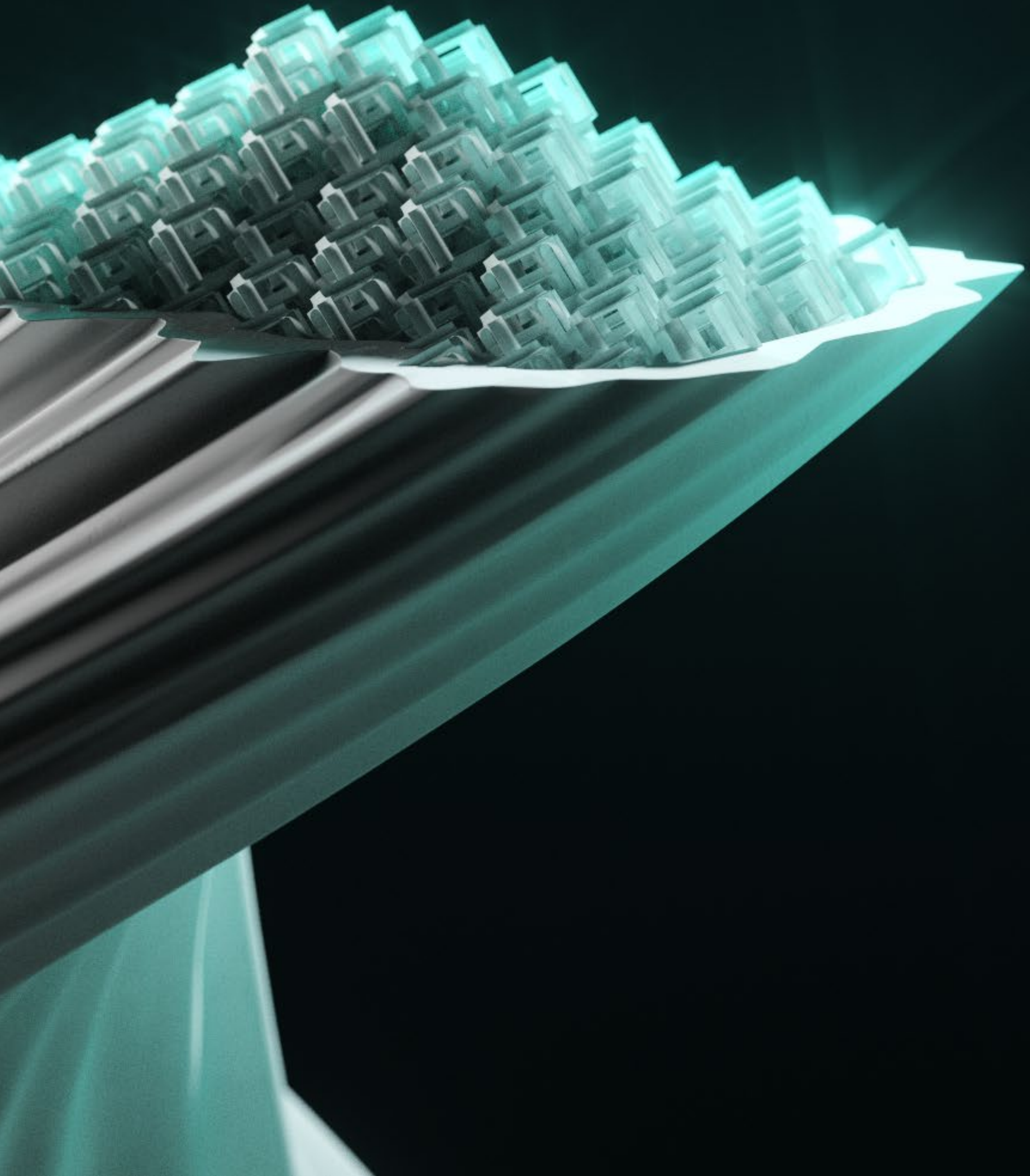
THREAT INTELLIGENCE

Extend your security intelligence from
local network to global cyberspace





What is a Threat Intelligence solution?

ESET's Threat Intelligence service provides global knowledge gathered by ESET threat intelligence experts on targeted attacks, advanced persistent threats (APTs), zero-days and botnet activities.

These items are traditionally difficult for security engineers to discover, who can only access information within their local network.

Why Threat Intelligence?

Threat Intelligence reports and feeds help sift through the information overload and provide the most relevant information for specific organizations.

INFORMATION OVERLOAD

Zero-days, advanced persistent threats, targeted attacks and botnets are all concerns for industries across the world. The problem is, due to the amount of different threats, organizations are unable to easily understand which proactive defenses and mitigations are the most important.

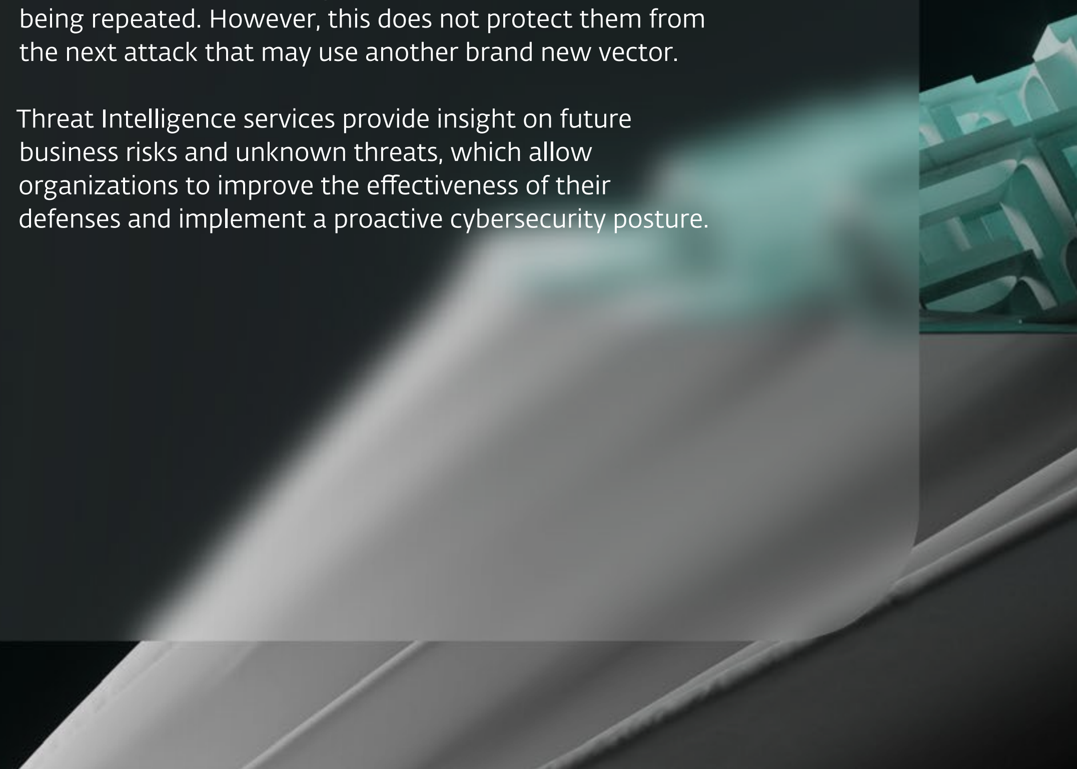
This ultimately leads to organizations scrambling to try and find meaningful information among limited data sets, such as their own networks, or the extremely large datasets that they find via external sources. Threat Intelligence services help sift through the information overload and provide the most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

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

PROACTIVE VS. REACTIVE

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 may use another 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.



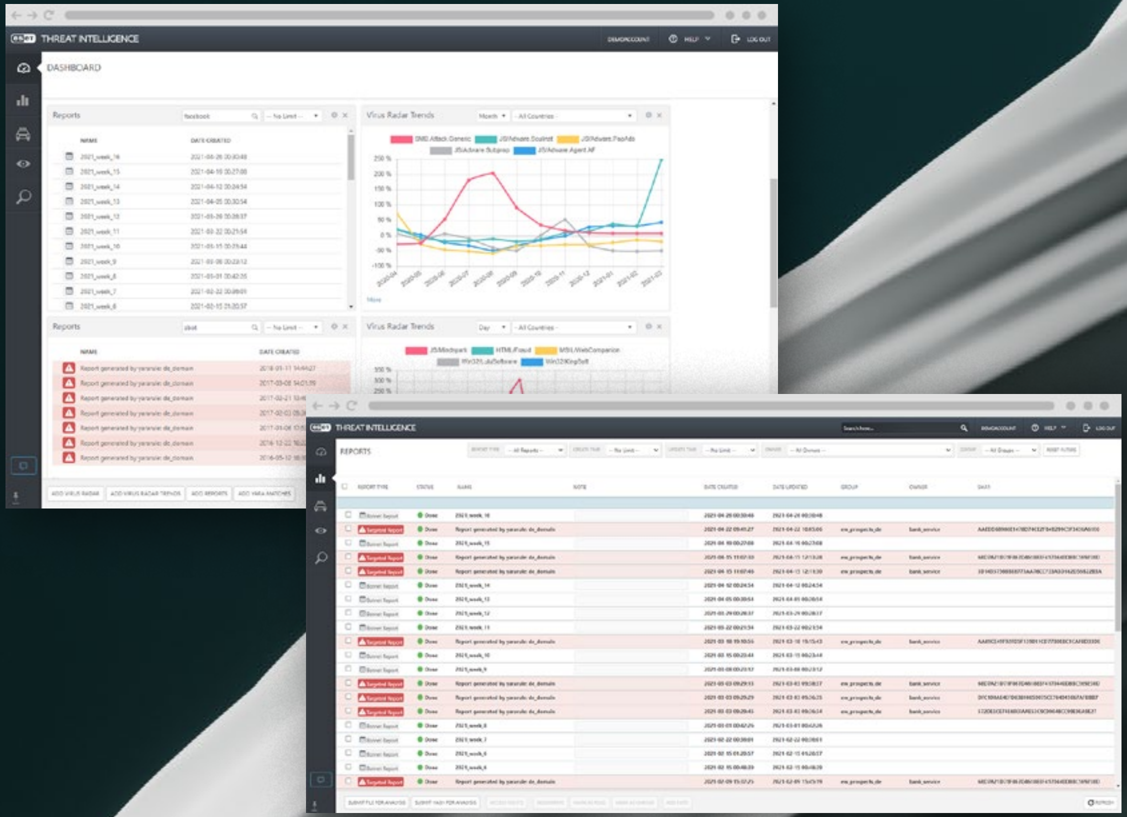
Why Threat Intelligence?

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

INCIDENT RESPONSE SUPPORT

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 typically a very long and manual process as engineers sift through their network searching for abnormalities which may indicate a compromise occurred.

Threat Intelligence services allow incident response teams to fully understand and quickly respond to data breaches. By providing information on the threat actor, malware behaviour, 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 difference

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.

The ESET difference

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, due to the threat actors being 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, and verified by our R&D centers, which 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 worldwide perspective on all the most recent trends and threats.

Advanced Persistent Threat (APT) Reports

PUTTING OUR BEST RESEARCH AT YOUR FINGERTIPS

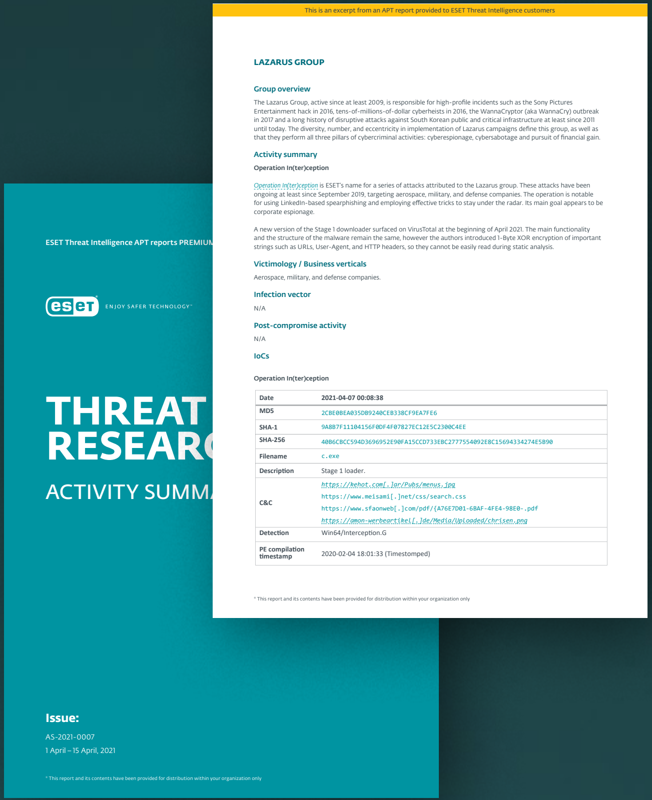
Our research team is well known in the digital security environment, thanks to our award winning We Live Security blog. Their great research and APT activity summaries are available, with much more detailed information at your disposal.

ACTIONABLE, CURATED CONTENT

Reports provide a great deal of context to what is going on and why. Thanks to this, organizations can prepare in advance for what might be coming. It's not just the reports themselves – they are curated by our experts who put them in a human-readable format.

MAKE CRUCIAL DECISIONS FAST

All this helps organizations to 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.



ESET Threat Intelligence APT reports PREMIUM

ESET ENJOY SAFER TECHNOLOGY™

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.

ESET proprietary intelligence feeds

Get a quick, real-time look at the worldwide threat landscape. Our feeds come from our research centers based around the globe to get a holistic picture, and quickly block IoCs in your environment. Feeds are in the formats JSON and STIX 2.0.

MALICIOUS FILES FEED

Understand which malicious files are being seen in the wild. 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 is shared hashes of malicious executable files and associated data.

DOMAIN FEED

Block domains which are considered malicious including domain name, IP address, and the date associated with them. The feed ranks domains based on their severity, which lets you adjust your response accordingly, for example only block high-severity domains.

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 human-readable 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.

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

About ESET

For more than 30 years, ESET® has been developing industry-leading IT security software and services, delivering instant, comprehensive protection against evolving cybersecurity threats for businesses and consumers worldwide. ESET is privately owned. With no debts and no loans, we have the freedom to do what needs to be done for the ultimate protection of all our customers.

ESET IN NUMBERS

110m+	400k+	200+	13
users worldwide	business customers	countries & territories	global R&D centers

SOME OF OUR CUSTOMERS

Canon

protected by ESET since 2016
more than 14.000 endpoints

ISP security partner since 2008
2 milion customer base

MITSUBISHI MOTORS

protected by ESET since 2017
more than 14,000 endpoints

Allianz Suisse

protected by ESET since 2016
more than 4,000 mailboxes

Why choose ESET?

SOME OF OUR TOP AWARDS

AV comparatives Certified EPR 2020 Strategic Leader
SE Labs AAA JAN-MAR 2021 ENTERPRISE ENDPOINT PROTECTION
AV TEST av-test.org 2020 AWARD BEST ANDROID SECURITY ESET Endpoint Security
G2 Leader WINTER 2021
canalys CYBERSECURITY CHAMPION 2020
Gartner peerinsights customers' choice 2019 ™

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.

ANALYST RECOGNITION

FORRESTER®

ESET was included in the Now Tech: Enterprise Detection And Response, Q1 2020 report — Forrester's overview of 29 enterprise Detection and Response solutions.

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

ESET retains its 'Top Player' status in Radicati's 2021 APT Protection Market Quadrant report.

Gartner Peer Insights is a free peer review and ratings platform designed for enterprise software and services decision makers. Reviews go through a strict validation and moderation process to ensure information is authentic. Gartner Peer Insights reviews constitute the subjective opinions of individual end users based on their own experiences, and do not represent the views of Gartner or its affiliates.

“*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