

Home | Cyber Crime | Cyber warfare | APT | Data Breach | Deep Web | Digital ID | Hacking |
 Hacktivism | Intelligence | Internet of Things | Laws and regulations | Malware | Mobile |
 Reports | Security | Social Networks | Terrorism | ICS-SCADA | EXTENDED COOKIE POLICY |
 Contact me |

Reports Security Social Networks Terrorism ICS-SCADA
 EXTENDED COOKIE POLICY Contact me

RansomEXX ransomware leaks files stolen from Italian luxury brand Zegna

August 6, 2021 By [Pierluigi Paganini](#)

Sponsc

1 P

2 D

4 B

See Als

PixFutu



RansomEXX ransomware operators hit the popular Italian luxury fashion house Ermenegildo Zegna Holding and started leaking stolen files.

Zegna is one of the most famous Italian luxury fashion houses. It was founded in 1910 by Ermenegildo Zegna in Trivero, Biella Province of the Piedmont region of Northern Italy.



[Ermenegildo Zegna Group](#) is the largest menswear brand in the world by revenue. As of 2018, Ermenegildo Zegna operated 480 retail stores (267 of which company-owned) across the world. Following the company's strongly export-oriented strategy, exports account for over 90% of total sales.

The revenue of the company was €1.159 billion as 2018.

Home | Cyber Crime | Cyber warfare | APT | Data Breach | Deep Web | Digital ID | Hacking |
 Hacktivism | Intelligence | Internet of Things | Laws and regulations | Malware | Mobile |
 Reports | Security | Social Networks | Terrorism | ICS-SCADA | EXTENDED COOKIE POLICY |
 Contact me |

Reports Security Social Networks Terrorism ICS-SCADA
 EXTENDED COOKIE POLICY Contact me

published: 2021-08-06, visits: 671, leak size: 20.74GB

[FILELIST]

[Part 1 of 43] [500.0MB] [MD5: 7db882a04a9e9c91587066f85ce4d216]
 [Part 2 of 43] [500.0MB] [MD5: f8c787e67b364812a63de3c9d471ecf2]
 [Part 3 of 43] [500.0MB] [MD5: 6fda7b74cecb8d561f599e9feef2fd92]
 [Part 4 of 43] [500.0MB] [MD5: 31ad4859d5d5d513075556a8c8eb57f8]
 [Part 5 of 43] [500.0MB] [MD5: ce15b81367d6a8e00a8f76d576c3d8a9]
 [Part 6 of 43] [500.0MB] [MD5: 69cb707ae0a8d291ee9a7dcf8da85d18]
 [Part 7 of 43] [500.0MB] [MD5: 7246792eada55d81df43b76ca3a5519a]
 [Part 8 of 43] [500.0MB] [MD5: 2154232933482659f3d941da49c32752]
 [Part 9 of 43] [500.0MB] [MD5: c2348443470ae34bfeb7a589336fde29]
 [Part 10 of 43] [500.0MB] [MD5: c5637244d26028d4139d4513d3ed3879]
 [Part 11 of 43] [500.0MB] [MD5: d842b764425f557d7e20815f66644d98]
 [Part 12 of 43] [500.0MB] [MD5: 2cb5cf1eacfe3880cdb30b233e09ae2f]
 [Part 13 of 43] [500.0MB] [MD5: 77406aa7111c62f0b88445d45ac02d56]
 [Part 14 of 43] [500.0MB] [MD5: 2e09c3174b6ab5327a6a3b813118ecfa]
 [Part 15 of 43] [500.0MB] [MD5: 2bfbd2e898bcad9a63f669d717ce6541]
 [Part 16 of 43] [500.0MB] [MD5: e1374d51fb6db4fae1ae28f9338a5986]
 [Part 17 of 43] [500.0MB] [MD5: 7b77b512d0c788db900acfd62276726]

The RansomEXX gang has been active since 2018 under the name Defray, in June 2020 the group rebranded as RansomEXX. The RansomEXX ransomware targets both Windows systems and virtual machines running [VMware ESXi servers](#).

Recently the RansomEXX gang infected the systems at [Italy's Lazio region](#) causing problems for the ongoing COVID19 vaccination campaign. This week the ransomware gang [RansomEXX](#) ransomware gang hit the Taiwanese manufacturer and distributor of computer hardware GIGABYTE and claims to have stolen 112GB of data.

Follow me on Twitter: [@securityaffairs](#) and [Facebook](#)

[Home](#) | [Cyber Crime](#) | [Cyber warfare](#) | [APT](#) | [Data Breach](#) | [Deep Web](#) | [Digital ID](#) | [Hacking](#) | [Hacktivism](#) | [Intelligence](#) | [Internet of Things](#) | [Laws and regulations](#) | [Malware](#) | [Mobile](#) | [Reports](#) | [Security](#) | [Social Networks](#) | [Terrorism](#) | [ICS-SCADA](#) | [EXTENDED COOKIE POLICY](#) | [Contact me](#) |

[Reports](#) [Security](#) [Social Networks](#) [Terrorism](#) [ICS-SCADA](#)
[EXTENDED COOKIE POLICY](#) [Contact me](#)

[Personal Data Protection](#)

[Data Breach Settlement](#)

[Data Privacy Policy](#)

[Data Analytics Reports](#)

**Center
Intern**

Subscri

Security

Dear Friend,
below the list of the
cyber security field

Pierluigi Paganini

(**SecurityAffairs** – hacking, Zegna)

Share this:



Twitter



Print



LinkedIn



Facebook



More

SHARE ON



Pierluigi Paganini

Pierluigi Paganini is member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group and Cyber G7 Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC