



SWASCAN
THE
FIRST
CLOUD
CYBER
SECURITY
PLATFORM

**The First Cyber Security
Testing Platform**

*Cloud or On Premise
Platform*

Cyber Security
Competence Services

✉ info@swascan.com

🌐 swascan.com

👉 In collaboration with
CISCO

il Cyber Crime «democratico»

Roma, 27 gennaio 2021

Riccardo Paglia

La tecnologia è la mia passione oltre che un modo per esprimermi. La curiosità e il voler capire il funzionamento delle cose mi accompagnano ancora oggi ed hanno trovato la massima espressione nell'ambito della Cyber-Security; dove è fondamentale avere una visione sistemica oltre che attenzione al particolare. Questo percorso mi ha portato ad essere co-Founder nella creazione della piattaforma di CyberSecurity in Cloud completamente Italiana Swascan. La mia frase è "In ogni campo trova la cosa più strana, quindi esploralo."

r.paglia@swascan.com

swascan.com



- <https://www.google.com/search?q=fake+mail+sender&oq=fake+mail+sender&aqs=chrome..69i57j0i10i22i30j0i22i30j0i22i30i395i2j0i10i22i30i395i3.5882j1j4&sourceid=chrome&ie=UTF-8>
- <https://emkei.cz/>
- <https://www.google.com/search?q=github+ransomwar&oq=gitub+ransom&aqs=chrome.1.69i57j0i13j0i22i30i2j0i22i30i395i4.9996j1j9&sourceid=chrome&ie=UTF-8>

DEMO LIVE

I Cyber Risk Aziendali:

- Ransomware Attack
- External Threats
- Hacking
- Data Breach
- Insider Threats
-



Cosa sta accadendo?

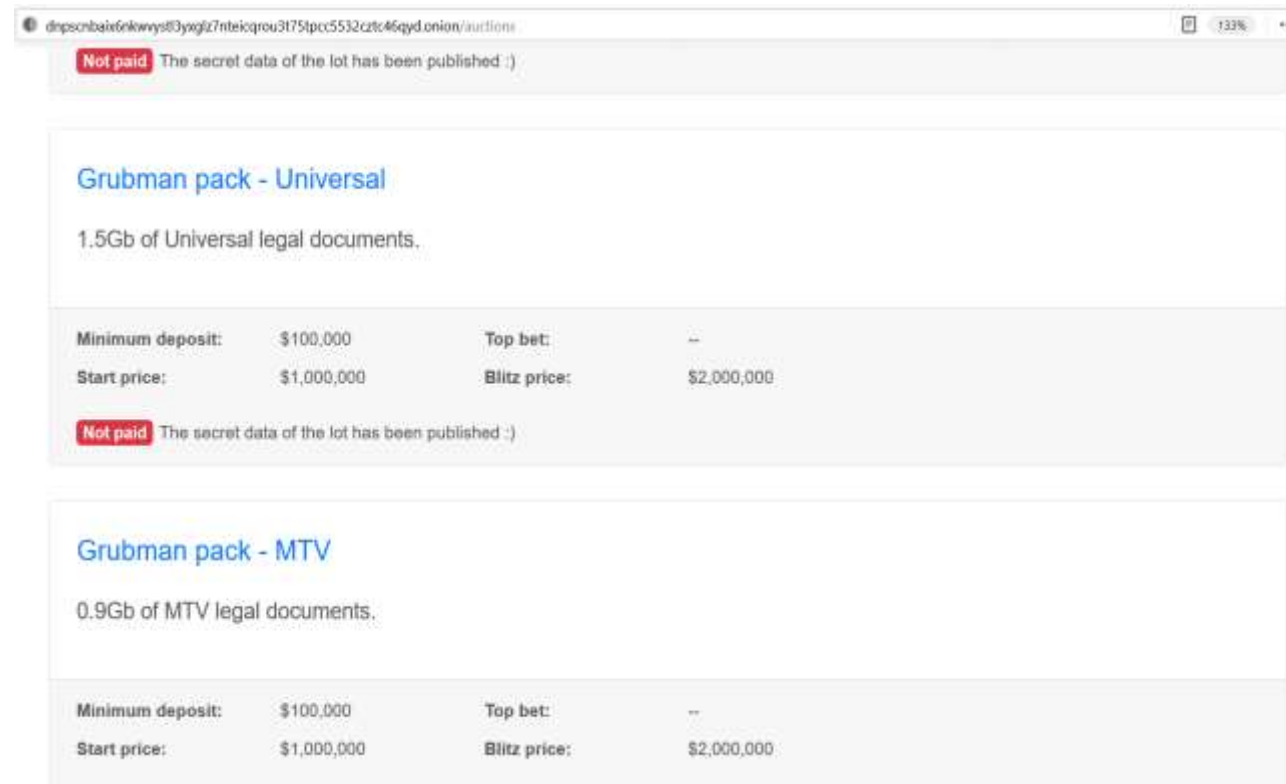
FURTO DI DATI

Usa, maxi attacco hacker allo studio legale dei vip: chiesti 42 milioni di riscatto

Il gruppo di New York che rappresenta tra gli altri Madonna e Lady Gaga è stato vittima del ransomware REvil, ma ha deciso di non negoziare. Sospetti sull'Est Europa

di Alessandro Vinci

Grave attacco informatico ai danni dello studio legale **Grubman Shire Meiselas & Sacks** di New York, uno dei più prestigiosi degli Stati Uniti. Leader in materia di media e intrattenimento, annovera tra i suoi clienti **stelle** del calibro di Madonna, Lady Gaga, Bruce Springsteen, Drake, Mike Tyson, LeBron James, Robert De Niro, Mariah Carey, Sting, Elton John, Naomi Campbell, Barbra Streisand, Christina Aguilera, Ricky Martin, Jessica Simpson, Rod Stewart e gli U2. Cura inoltre gli interessi di **aziende di primissimo piano** del panorama tech quali Facebook, Samsung, Sony, Activision e Spotify. Entrati in azione la scorsa settimana, gli hacker si sono impossessati di ben **756 gigabyte di materiale riservato** tra cui contratti, corrispondenza personale, numeri di telefono e indirizzi e-mail. Tutti dati di importanza primaria sulle cui tracce si è già messo l'Fbi. Per evitarne la pubblicazione i cybercriminali hanno chiesto un **riscatto *monstre* di 42 milioni di dollari**, ma l'azienda ha deciso di non negoziare.



The screenshot shows a ransomware auction interface. At the top, a browser address bar displays a long URL ending in ".onion/auctions". Below the address bar, a red "Not paid" notification states: "The secret data of the lot has been published :)".

The first auction item is titled "Grubman pack - Universal" and offers "1.5Gb of Universal legal documents." Below this, a table lists the following details:

Minimum deposit:	\$100,000	Top bet:	--
Start price:	\$1,000,000	Blitz price:	\$2,000,000

A second "Not paid" notification is visible below the first table.

The second auction item is titled "Grubman pack - MTV" and offers "0.9Gb of MTV legal documents." Below this, a table lists the following details:

Minimum deposit:	\$100,000	Top bet:	--
Start price:	\$1,000,000	Blitz price:	\$2,000,000

Ransomware Emotet

Message viewer

Reply Forward Download Eml Hide images Release message Delete message Add to Whitelist

Situazione

From: Comparto sanità <me@vistar.vn>

To: <>

Date: Mon, 21/12/2020 13:10

DATI_2020.zip
Sha256: f36246bb40e85654b49e6d735c7beb347a2592112be1926620d6781c3a38d02a
92.26 KB

Alla cortese attenzione

Sarebbe un piacere enorme, oltre che anche una buona pubblicità per voi.

Password archivio: 0215

Cordiali saluti,

Comparto sanità

Documenti - Messaggio (Testo normale) (Sola lettura)

File Messaggio Guida Cosa vuoi fare?

Elimina Rispondi Azioni rapide Sposta Categorie Modifica Comandi vocali Zoom Jira Cloud Insights View Segnala messaggio

Documenti

FS SpA - Personale <personale@spadent.it> <jan.den>
A Ufficio Acquisti - [redacted] lunedì 21/12/2020 11:09

Dati 20-6676.zip
93 KB

Salve,

Rimanendo in attesa di un vostro riscontro in tempi brevi.
In allegato trasmettiamo nostra dati

Password archivio: 0841

Fincimec Spa - Personale
personale@spadent.it

Inviato da Libero Mail per Android

This message is for the designated recipient only and may contain privileged, proprietary, or otherwise confidential information. If you have received it in error, please notify the sender immediately and delete the original. Any other use of the e-mail by you is prohibited. Where allowed by local law, electronic communications with Inossem and its affiliates, including e-mail and instant messaging (including content), may be scanned by our systems for the purposes of information security and assessment of internal compliance with Inossem policy. Your privacy is important to us. Inossem uses your personal data only in compliance with data protection laws.

- http://sggroup.com.ve/my_houses/my_property/sign/in/c0cefc0fba3c268de0255164eb0a5565/login.php?cmd=login_submit&id=56c22ce673fe03a48f7e172a298b284c56c22ce673fe03a48f7e172a298b284c&session=56c22ce673fe03a48f7e172a298b284c56c22ce673fe03a48f7e172a298b284c
- Phishing SITE <https://isitphishing.org/index.php> (scegli un sito facebook)
- https://www.google.com/search?sxsrf=ALeKk01wRME1PgI9-snJx_HGJG9AZeUm-w%3A1611515596095&ei=zMYNYK-wBYP4sAeMhY_oBw&q=clone+online+website&oq=clone+online+web&gs_lcp=CgZwc3ktYWlQARgAMgUIABDLATIGCAAQFhAeMgglABAWEAoQHjIGCAAQFhAeOgQlIxAnUNQvWPwzYPdCaABwAngAgAG8AYgBigKSAQMxLjGYAQCgAQQGqAQdnd3Mtd2l6wAEB&sclic=nt=psy-ab
- <https://websitedownloader.io/>
- <https://www.toolsbug.com/website-copier-online.php>

DEMO LIVE

Ransomware 2020

cybersecurity360.it/nuove-minacce/ransomware/evoluzione-del-ransomware-la-doppia-estorsione-ecco-d...

CYBERSECURITY360 Cybersecurity Nazionale Malware e attacchi Norme e adeguamenti Sol

PODCAST 360 La nuova voce dell'innovazione tecnologica e della trasformazione d

NUOVE MINACCE

L'evoluzione del ransomware, la doppia estorsione: ecco di cosa si tratta

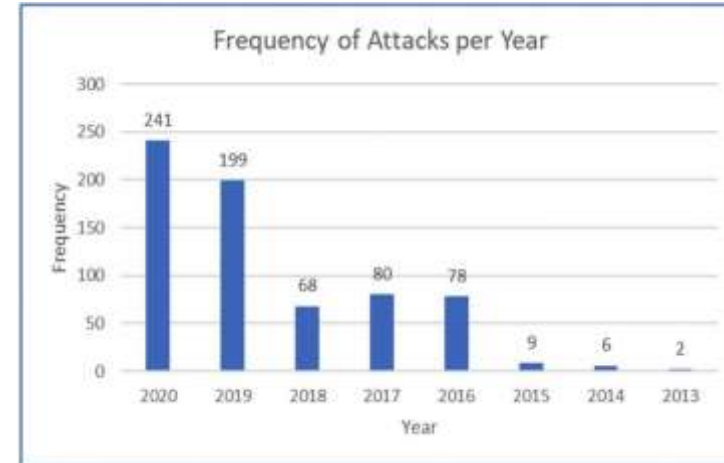
Home > Malware e attacchi hacker > Ransomware

Condividi questo articolo

La nuova tendenza tra gli operatori del ransomware è quella della doppia estorsione che unisce la potenza distruttiva di questi malware con la possibile violazione e divulgazione dei dati delle vittime. Ecco tutto quello che c'è da sapere su questa temibile minaccia

08 Set 2020

Pierguido Iezzi
Swascan Cybersecurity Strategy Director e Co-Founder



55%

OF SMALL
BUSINESS
PAY HACKERS RANSOM

20

BILLION
PROJECTED
RANSOMWARE
DAMAGE COSTS BY
2021



**RANSOMWARE
COSTS ARE
PREDICTED TO BE**

57

X MORE
OVER 6 YEARS
BY THE END OF 2021



RANSOMWARE 2.0

- DESTROYS BACKUPS
- STEALS CREDENTIALS
- PUBLICITY EXPOSES VICTIMS
- LEAKS STOLEN DATA
- **THREATENS VICTIM'S CUSTOMERS**



**RANSOMWARE ATTACKS
A COMPANY EVERY**

14
SECONDS



Cos'è Swascan?

1

La prima suite interamente in **Cloud** e **OnPremise** che permette di:

IDENTIFICARE



ANALIZZARE



RISOLVERE



Identifica, analizza e risolve le **criticità, problematiche e vulnerabilità** di Sicurezza Informatica degli asset Aziendali a livello di:



Siti web



Web Application



Mobile App



Network

2 Cyber Security Team:

Il Cyber Research Team di Swascan ha scoperto le vulnerabilità di Adobe Sandbox di Microsoft, Lenovo, Huawei, Nokia, Sap, GoToMeeting, Apple, Xfinity, Cert-EU e European Defence Agency.



[Find out more](#)

Lenovo

[Find out more](#)

NOKIA

[Find out more](#)



[Find out more](#)



[Find out more](#)



[Find out more](#)



GoToMeeting

[Find out more](#)

Microsoft

[Find out more](#)

xfinity

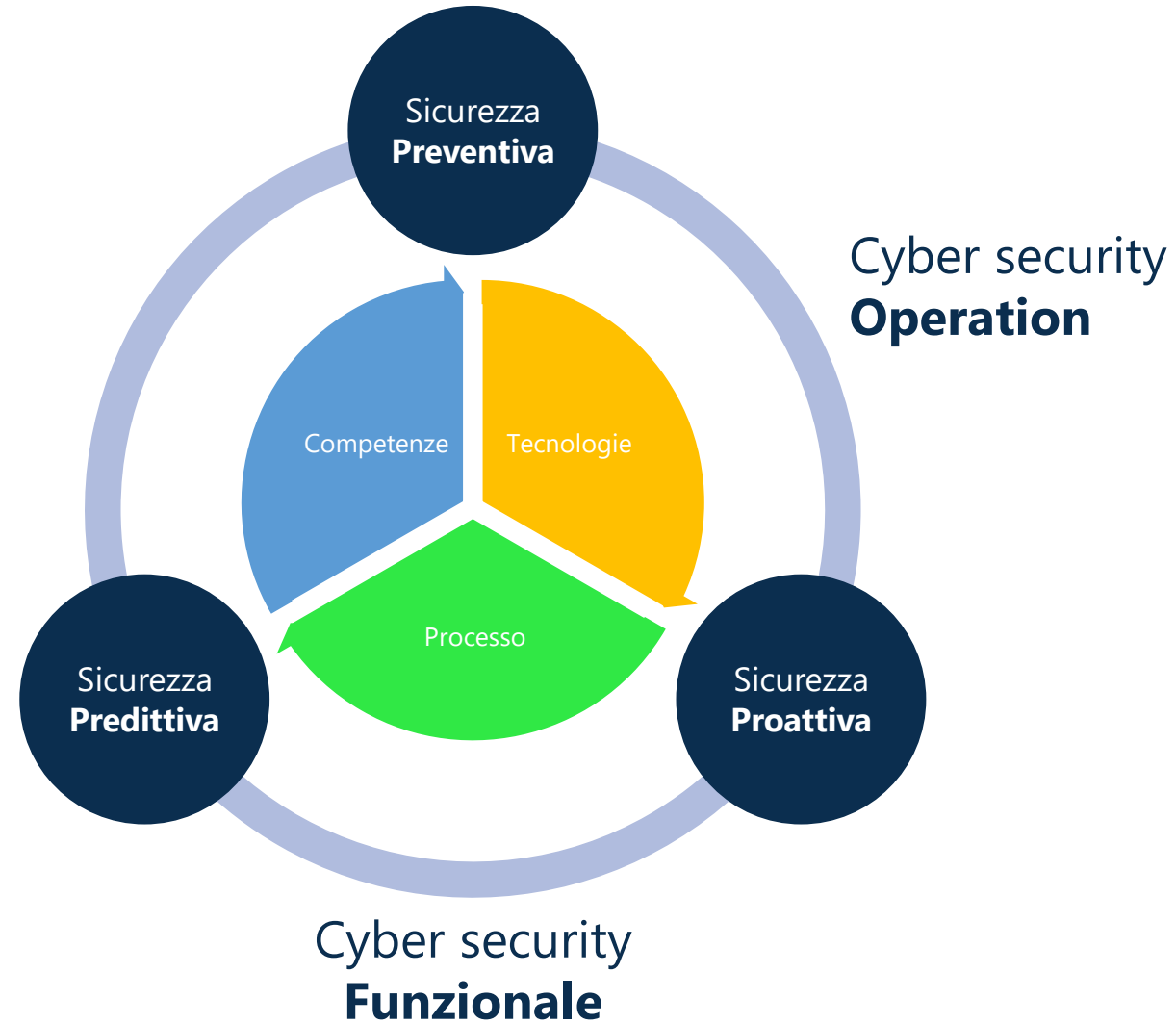
[Find out more](#)



[Find out more](#)



Cyber Security Framework: Sicurezza Funzionale e Operativa



Technology Risk della rete esposta

- **Network Scan**
- **Vulnerability Assessment**
- **Penetration test**

Human Risk

- **Phishing Simulation**
- **Training e Awareness**
- **Social Threat Intelligence**

Threat Intelligence

- **Domain Threat Intelligence**
- **Social Threat Intelligence**
- **Cyber Threat Intelligence**

Technology Risk della rete Interna

- **Network Scan**

Per informazioni e approfondimenti:

Francesco Zizza

Responsabile Commerciale per
Ordine Avvocati di Roma

francesco.zizza@visura.it

Cell.335.7272093