ITALY

Threat Landscape Report

SOCRadar®

September 2022

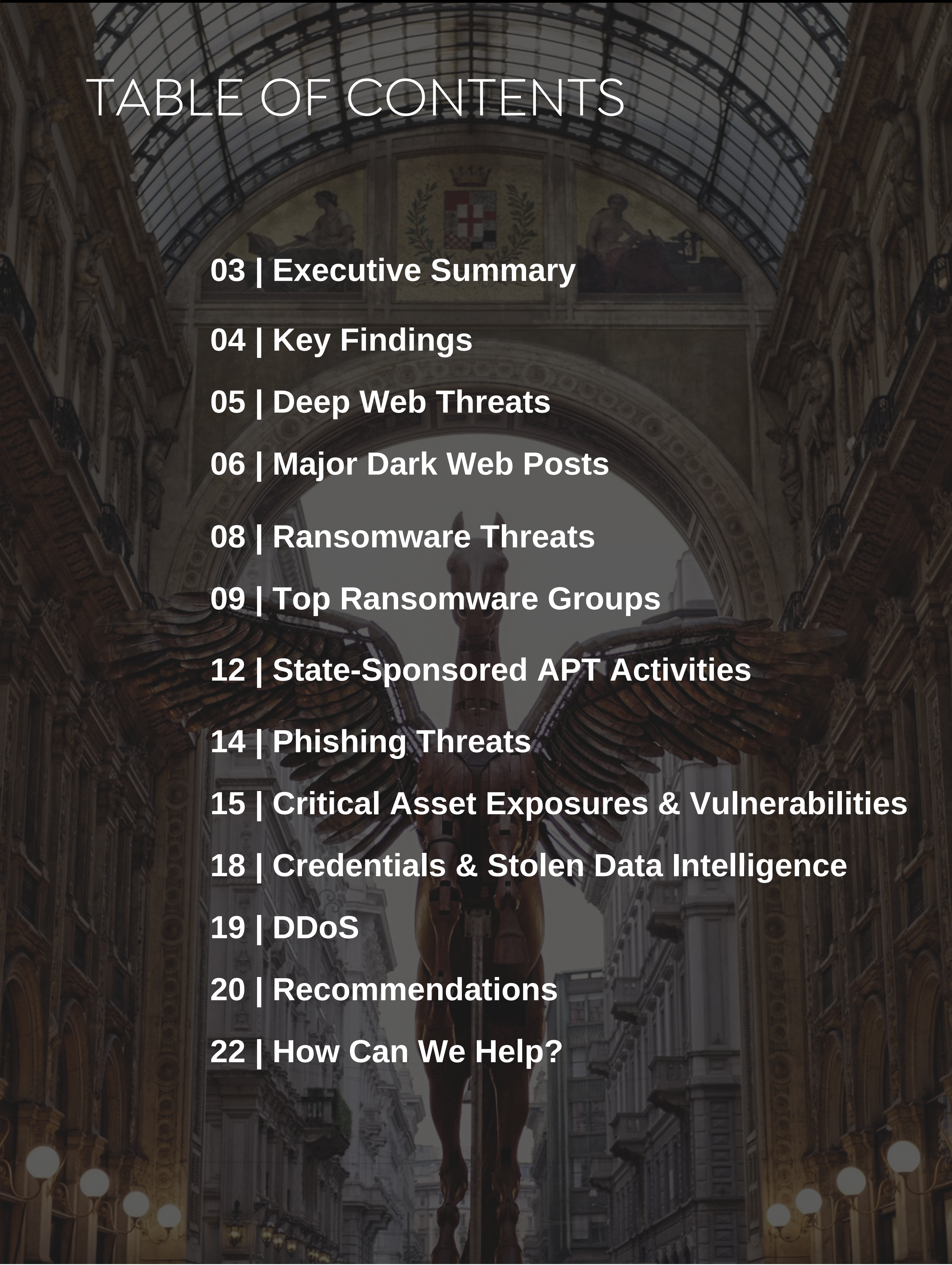


TABLE OF CONTENTS

EXECUTIVE SUMMARY

Since the beginning of the COVID-19 pandemic, cyber risks have noticeably increased in Italy. Therefore, the Italian government announced its first National Cybersecurity Strategy this year in May. The strategy, developed by the Italian National Cybersecurity Agency, has many objectives and aims to address some challenges, including "To predict the evolution of the cyber threats to reduce their impact on national infrastructure and organizations from different industries." This strategy necessitates a more detailed understanding of the cybersecurity threats to many industries operating in Italy.

A rapidly growing digital perimeter formed a much larger attack surface than before. One of the most significant risks throughout the pandemic was email compromise. The average cost of a data breach in Italy is $3.74 million, which may be the result of various incidents, including email compromise, according to IBM's Cost of A Data Breach 2022 report. And also, about 61 % of Italy's email compromise cases occurred in the Northern part, where many companies have headquarters.

SOCRadar monitored 14,323 dark web posts between June 2021 and June 2022 to better understand Italy's threat landscape. About 3,417 of these posts were about threats in Europe. The number of threats against Italy was 333 among them.

In this report, SOCRadar characterizes the threat landscape by leveraging the activity of threat actors, malware campaigns, new critical vulnerabilities and exploits, data collected from open threat sharing platforms, and SOCRadar's comprehensive data monitoring, collection, classification, and analysis.

SOCRadar's unique perspective on understanding threat actors and their TTPs comes from combining information gathered from the SOCRadar CTIA Team's deep/dark web threat research, HUMINT observations, cybersecurity vendor blogs, and social media trends.

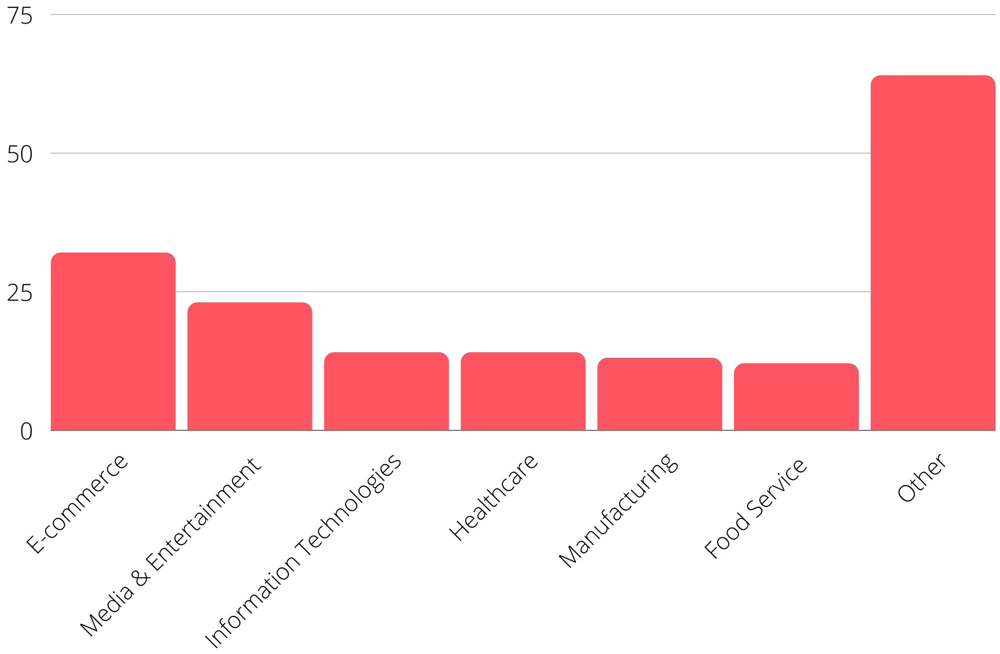
This report provides organizations with an understanding of evolving cyber threats relevant to Italy to enable security leaders to make better decisions. The intelligence provided in SOCRadar Threat Landscape Report can be used to plan organization-wide security programs, make investment decisions, and define cybersecurity requirements.

KEY FINDINGS

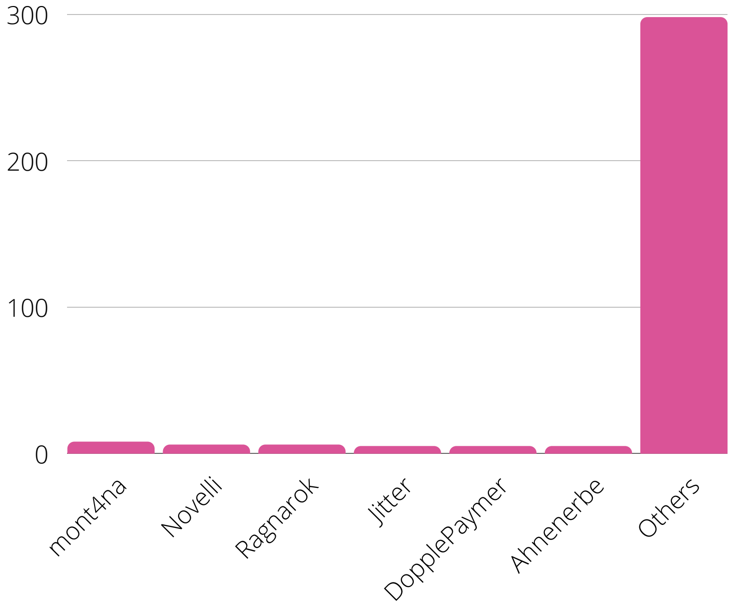
- Top ransomware threat actors targeting Italy are LockBit 2.0, Conti, and AlphaVM Blackcat.
- Between June 2021 – June 2022, SOCRadar monitored 2,931 ransomware incidents. 192 of them were targeting Italy. According to SOCRadar Dark Mirror data, 61 % Italian organizations experienced a ransomware attack.
- According to SOCRadar's DarkMirror data, E-Commerce, Media & Entertainment, and Information Technology were the most targeted industries.
- The notable APT groups that have targeted Italian organizations are Doppel Spider, Labyrinth Collima, Pinchy Spider, Twisted Spider, Venomous Bear, and Wizard Spider.
- The most common malware in Italy is Emotet.
- According to SOCRadar's extensive data, 66 % of phishing attempts against Italian firms used HTTPS protocol.
- The most impacted city by DDoS attacks in Italy was Milan, a metropolis in Italy's northern Lombardy region. DDoS attacks mostly affected Telecom Italia S.p.An in Italy.
- 221,270 Italian users have been infected with Stealer (Redline, Raccoon, Vidar, etc.).
- The number of 2,796,910 were stolen credentials belonging to .it domains on sale on the dark web.
- Some hosts are still vulnerable to the following vulnerabilities: 5,013 hosts to Heartbleed (CVE-2014-0160), 61 hosts to EternalBlue (CVE-2017-0144), and 1,179 hosts to BlueKeep (CVE-2019-0708).
- The systems belonging to the Italian IP zone had more than 7 million open ports. Approximately twenty-seven thousand of them were RDP ports.

Dark Web Threats

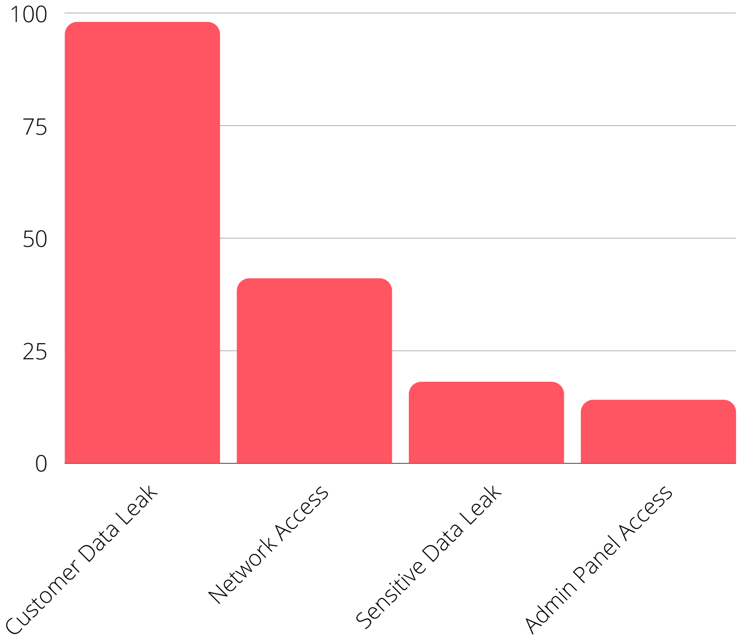
SOCRadar DarkMirror Data shows that between June 2021 – June 2022, the most targeted industries were E-Commerce, Media & Entertainment, and Information Technology. More than half of the posts on the dark web captured by SOCRadar DarkMirror were customer data leaks for Italian companies, followed by sensitive data leak posts, including the leaks of companies' sensitive internal data. Sensitive data leak consists of dark web posts including internal confidential data of companies, top secret governmental data, employee PII, and much more. Following sensitive data leaks, the second most common threat category was customer data leak, consisting of dark web posts leaking customer PIIs of Italian companies. In addition, in the same period, six actors stood out among the post owners who made posts about Italy on the dark web. According to SOCRadar's review, the frequency of shares of these actors was higher than the others.



The most targeted industries in Italy based on DarkMirror Intelligence data



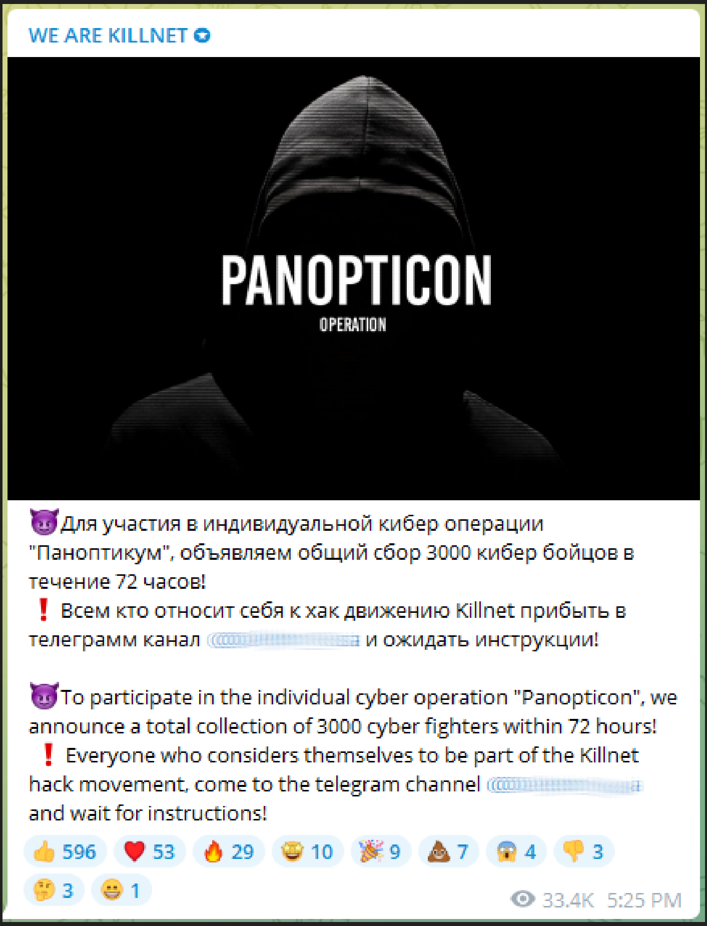
Dark web threats post owners in Italy based on DarkMirror Intelligence data



Dark web threats post types in Italy based on DarkMirror Intelligence data

Major Dark Web Posts

Killnet Cyber Attacks Against Italy and NATO Countries



WE ARE KILLNET

😈Для участия в индивидуальной кибер операции "Паноптикум", объявляем общий сбор 3000 кибер бойцов в течение 72 часов!
❗ Всем кто относит себя к хак движению Killnet прибыть в телеграмм канал [redacted] и ожидать инструкции!

😈To participate in the individual cyber operation "Panopticon", we announce a total collection of 3000 cyber fighters within 72 hours!
❗ Everyone who considers themselves to be part of the Killnet hack movement, come to the telegram channel [redacted] and wait for instructions!

👍 596 ❤️ 53 🔥 29 🤩 10 🎉 9 💩 7 😱 4 👎 3 🤔 3 😁 1

👁 33.4K 5:25 PM

On the 29th of May, Italy's CSIRT team posted an alert on its webpage about the risk of cyberattacks against public and private entities. (1)

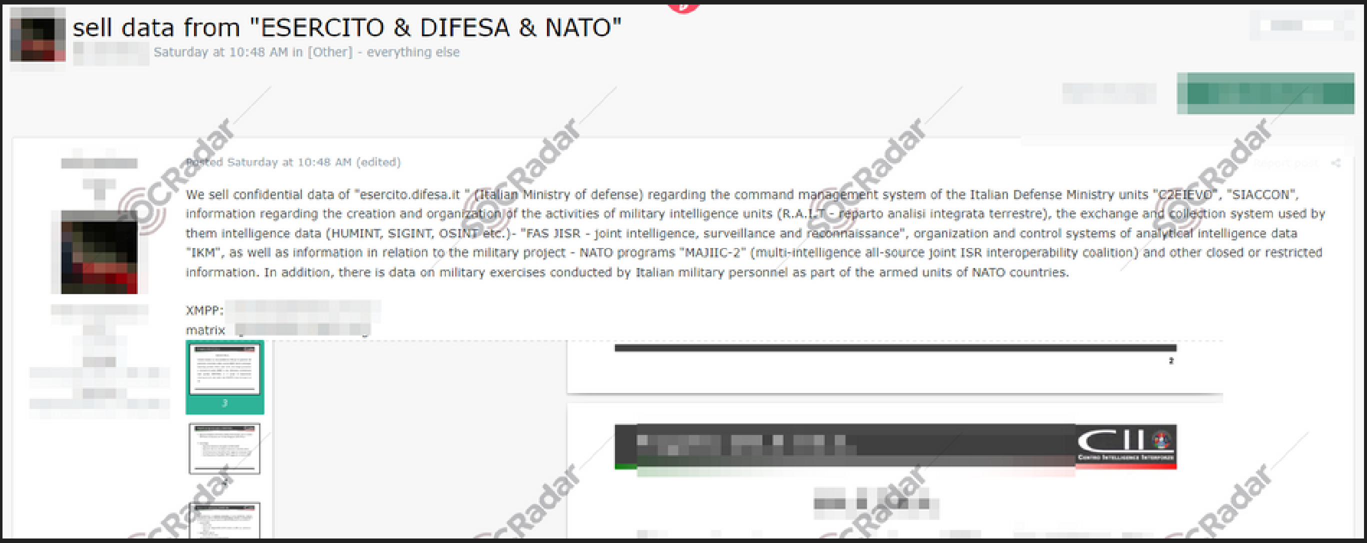
Risks are mentioned as DDoS attacks aimed at causing disruptions and service outages.

Cyber risks deriving from the Ukraine situation continue. Italy's CSIRT team is stating that the attack campaigns recently on national sites were claimed by Russian Actors.

Killnet, a pro-Russian group that attacks countries supporting Ukraine, had posted on their telegram channel showing the signs of DDoS attack plans.

Killnet attacks appear to have an impact on Italian ministry websites, as per media reports.

Sensitive Documents of Italian Ministry of Defense is on Sale



sell data from "ESERCITO & DIFESA & NATO"

[redacted] Saturday at 10:48 AM in [Other] - everything else

Posted Saturday at 10:48 AM (edited)

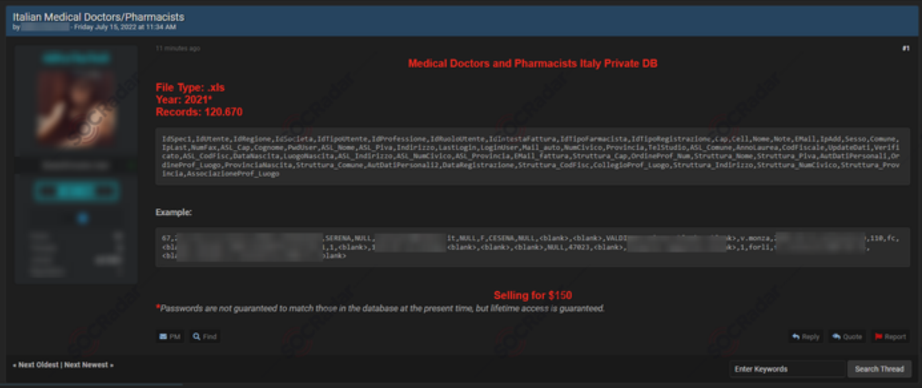
We sell confidential data of "esercito.difesa.it " (Italian Ministry of defense) regarding the command management system of the Italian Defense Ministry units "C2EIEVO", "SIACCON", information regarding the creation and organization of the activities of military intelligence units (R.A.I.T - reparto analisi integrata terrestre), the exchange and collection system used by them intelligence data (HUMINT, SIGINT, OSINT etc.)- "FAS JISR - joint intelligence, surveillance and reconnaissance", organization and control systems of analytical intelligence data "IKM", as well as information in relation to the military project - NATO programs "MAJIIC-2" (multi-intelligence all-source joint ISR interoperability coalition) and other closed or restricted information. In addition, there is data on military exercises conducted by Italian military personnel as part of the armed units of NATO countries.

XMPP: [redacted]
matrix [redacted]

On August 6, in a hacker forum monitored by SOCRadar, a new alleged sensitive document sale is detected for the Italian Ministry of Defense. In addition, there is data on military exercises conducted by Italian military personnel as part of the armed units of NATO countries.

Major Dark Web Posts

Database of Italian Healthcare Workers is on Sale



Italian Medical Doctors/Pharmacists
by [redacted] - Friday July 15, 2022 at 11:34 AM

11 minutes ago #1

Medical Doctors and Pharmacists Italy Private DB

File Type: .xls
Year: 2021*
Records: 120.670

```
IdSpec1,IdUtente,IdRegione,IdSocieta,IdTipoUtente,IdProfessione,IdRuoloUtente,IdIntestaFattura,IdTipoFarmacista,IdTipoRegistrazione,Cap,Cell,Nome,Note,EMail,IpAdd,Sesso,Comune,
IpLast,NumFax,ASL_Cap,Cognome,PwdUser,ASL_Nome,ASL_Piva,Indirizzo,LastLogin,LoginUser,Mail_auto,NumCivico,Provincia,TelStudio,ASL_Comune,AnnoLaurea,CodFiscale,UpdateDati,Verifi
cato,ASL_CodFisc,DataNascita,LuogoNascita,ASL_Indirizzo,ASL_NumCivico,ASL_Provincia,EMail_fattura,Struttura_Cap,OrdineProf_Num,Struttura_Nome,Struttura_Piva,AutDatiPersonali,Or
dineProf_Luogo,ProvinciaNascita,Struttura_Comune,AutDatiPersonali2,DataRegistrazione,Struttura_CodFisc,CollegioProf_Luogo,Struttura_Indirizzo,Struttura_NumCivico,Struttura_Prov
incia,AssociazioneProf_Luogo
```

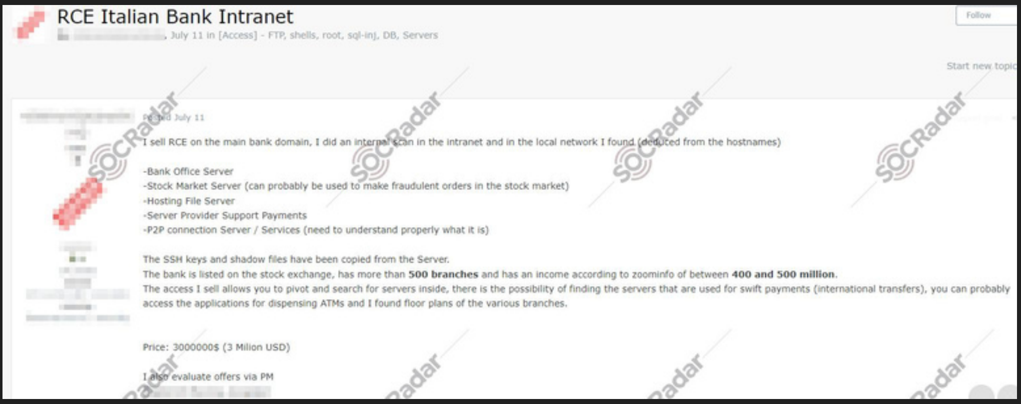
Example:

```
67,[redacted],SERENA,NULL,[redacted]it,NULL,F,CESENA,NULL,<blank>,<blank>,VALDI[redacted]k>,v.monza,[redacted],110,fc,
<bl[redacted]1,1,<blank>,1[redacted]<blank>,<blank>,<blank>,NULL,47023,<blank>,[redacted]k>,1,forli,[redacted],
<bl[redacted]lank>
```

Selling for $150
**Passwords are not guaranteed to match those in the database at the present time, but lifetime access is guaranteed.*

On the 15th of July, in a hacker forum monitored by SOCRadar, a new alleged medical database sale was detected for Italy.

RCE Exploit for an Italian Bank is on Sale



RCE Italian Bank Intranet
[redacted], July 11 in [Access] - FTP, shells, root, sql-inj, DB, Servers

Posted July 11

I sell RCE on the main bank domain, I did an internal scan in the intranet and in the local network I found (deducted from the hostnames)

-Bank Office Server
-Stock Market Server (can probably be used to make fraudulent orders in the stock market)
-Hosting File Server
-Server Provider Support Payments
-P2P connection Server / Services (need to understand properly what it is)

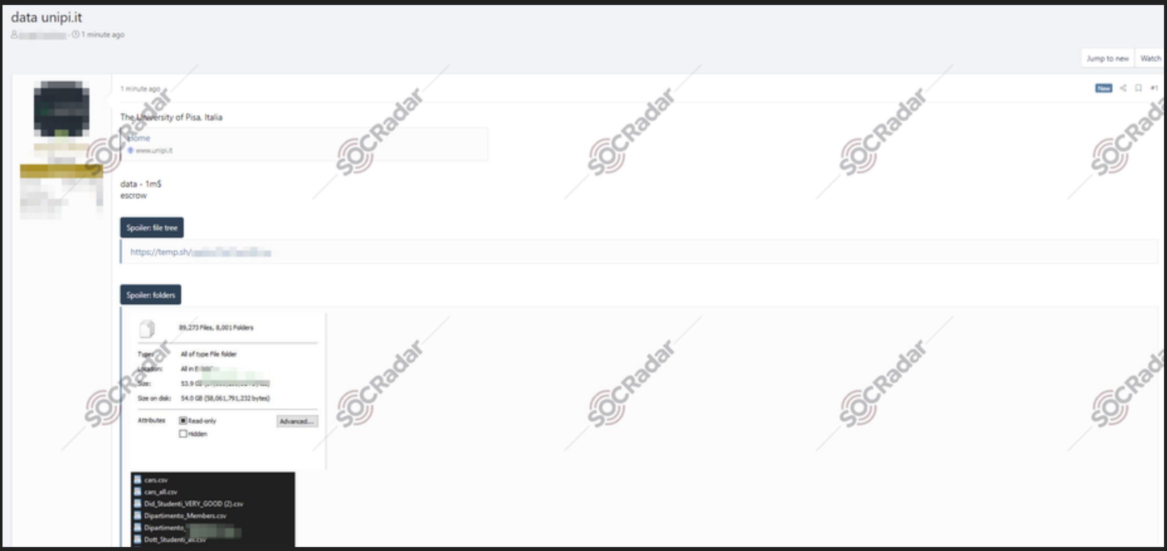
The SSH keys and shadow files have been copied from the Server.
The bank is listed on the stock exchange, has more than **500 branches** and has an income according to zoominfo of between **400 and 500 million**.
The access I sell allows you to pivot and search for servers inside, there is the possibility of finding the servers that are used for swift payments (international transfers), you can probably access the applications for dispensing ATMs and I found floor plans of the various branches.

Price: 3000000$ (3 Milion USD)

I also evaluate offers via PM

On July 11th, SOCRadar discovered the sale of a remote code execution exploit for an Italian Bank in a hacker forum.

Database and Sensitive Documents of University of Pisa are Leaked



data unipi.it
[redacted] · 1 minute ago

1 minute ago

The University of Pisa, Italia

Home
www.unipi.it

data - 1m$
escrow

Spoiler: file tree

https://temp.sh/[redacted]

Spoiler: folders

89,273 Files, 8,001 Folders

Type: All of type File folder
Location: All in [redacted]
Size: 53.9 G[redacted]
Size on disk: 54.0 GB (58,061,791,232 bytes)

Attributes ■ Read-only
□ Hidden

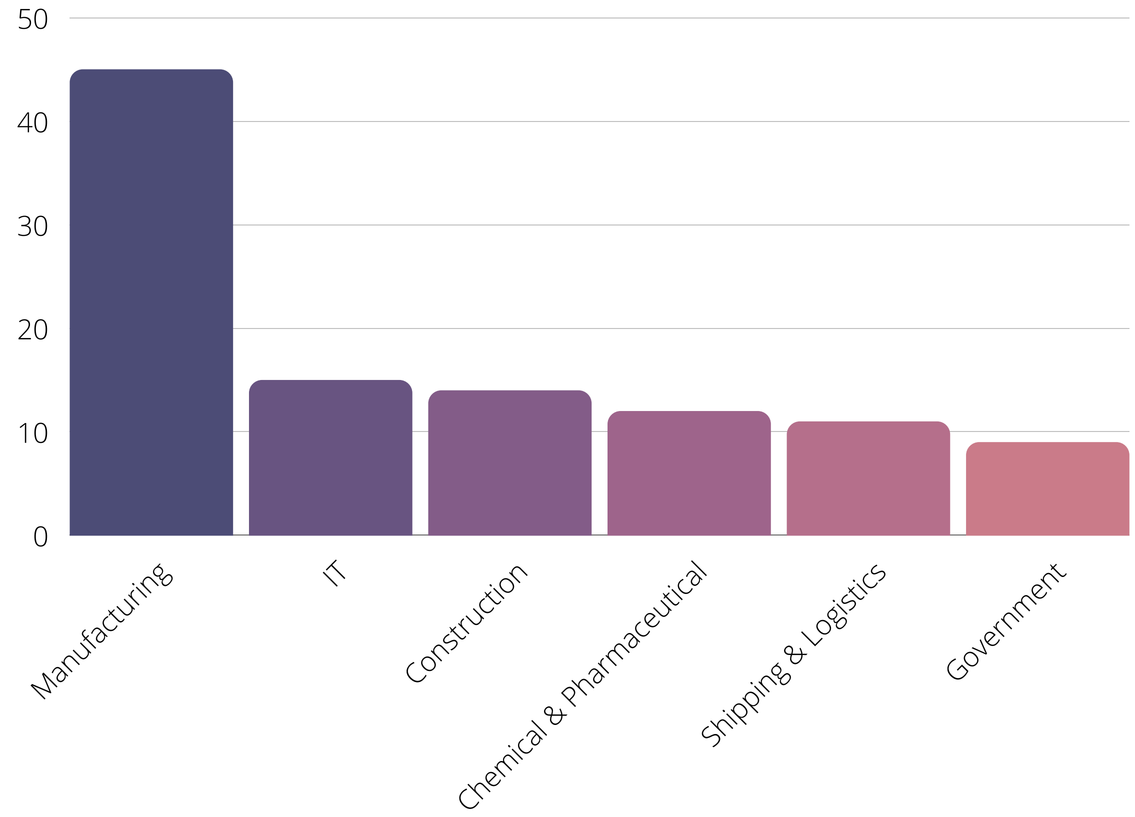
cars.csv
cars_all.csv
Did_Studenti_VERY_GOOD (2).csv
Dipartimento_Members.csv
Dipartimento_[redacted]
Dott_Studenti_all.csv

On June 20th, SOCRadar discovered an alleged database leakage for the University of Pisa.

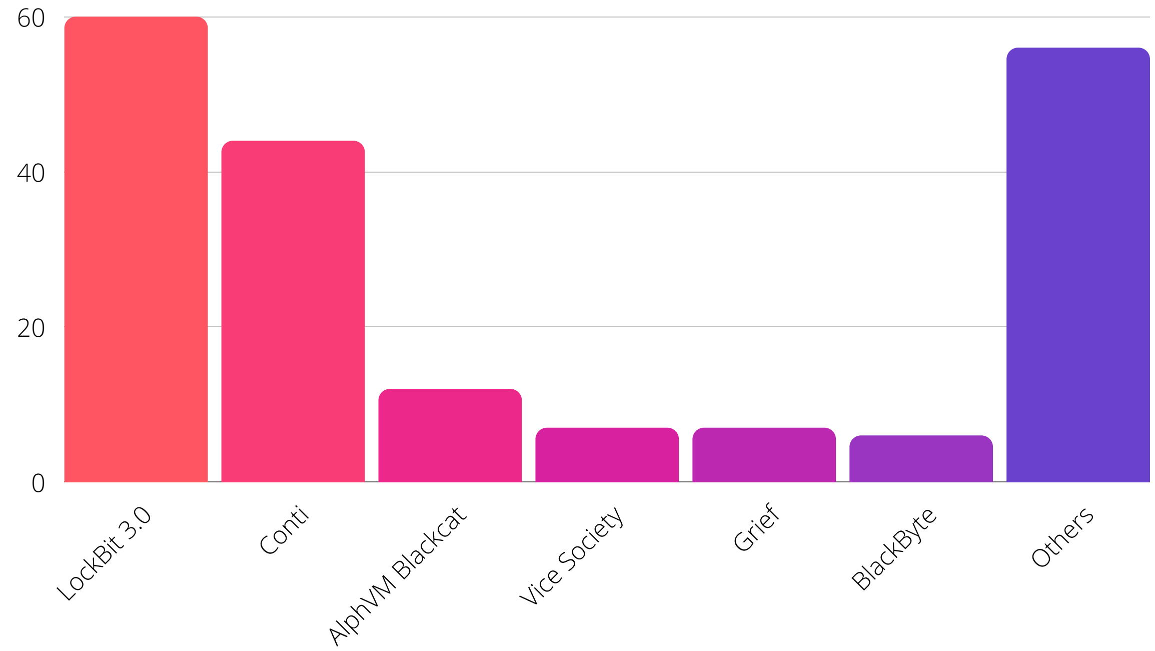
Ransomware Threats

Italy is among the top 10 countries regarding the number of posts submitted by ransomware gangs. 60 % of organizations in Italy dealt with ransomware attacks in the first half of 2022. It is no surprise considering that 61 % of Italian organizations have been hit with a ransomware attack in the past 12 months. (2)

Extortion payments are not allowed in Italy by law, meaning the payments are illegal. Still, the average ransom payment is around $710.000.



Most targeted sectors in Italy by ransomware groups last 12 months



Top ransomware groups targeting Italian organizations

Top Ransomware Groups

LockBit 3.0

- Ransomware-as-a-service (RaaS) operator.
- Has one of the best-designed locker algorithms regarding encryption speed and overall functionality.
- As of late June 2022, the gang declared that a new version of their locker is out: LockBit 3.0. LockBit 3.0 has more outstanding capabilities and functionalities than the old vault. The latest version can be considered a massive threat to organizations worldwide.

MITRE TTPs

Initial Access
T1078 Valid Accounts
T1190 Exploit Public-Facing Application
Execution
T1047 Windows Management Instrumentation
T1059 Command and Scripting Interpreter
T1059.003 Windows Command Shell
Persistence
T1547.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
Privilege Escalation
T1055 Process Injection
Defense Evasion
T1055 Process Injection
T1070.004 Indicator Removal on Host: File Deletion
T1112 Modify Registry
T1497 Virtualization/Sandbox Evasion
Credential Access
T1056.004 Credential API Hooking
T1110 Brute Force
Discovery
T1012 Query Registry
T1018 Remote System Discovery
T1057 Process Discovery
Lateral Movement
T1021 Remote Services
T1021.001 Remote Services: Remote Desktop Protocol
T1021.002 Remote Services: SMB/Windows Admin Shares
Collection
T1056.004 Credential API Hooking
Command and Control (C2)
T1090.003 Proxy: Multi-hop Proxy
Exfiltration
T1567.002 Exfiltration Over Web Service: Exfiltration to Cloud Storage
Impact
T1486 Data Encrypted for Impact
T1490 Inhibit System Recovery

Source: (3)

Conti

- Ransomware-as-a-service (RaaS) operator, believed to be originated in Russia.
- One of the most active ransomware gangs, Conti is actively targeting enterprises worldwide.
- After the gang's stand in the cyber-crisis between Russia and Ukraine, their internal chats and locker source code were leaked by a Ukrainian hacker who previously has gained access to Conti's internal systems.

MITRE TTPs

T1016 System Network Configuration Discovery
T1018 Remote System Discovery
T1021.002 Remote Services: SMB/Windows Admin Shares
T1027 Obfuscated Files or Information
T1049 System Network Connections Discovery
T1055.001 Process Injection: Dynamic-link Library Injection
T1057 Process Discovery
T1059.003 Command and Scripting Interpreter: Windows Command Shell
T1078 Valid Accounts
T1080 Taint Shared Content
T1083 File and Directory Discovery
T1106 Native API
T1110 Brute Force
T1133 External Remote Services
T1135 Network Share Discovery
T1140 Deobfuscate/Decode Files or Information
T1190 Exploit Public Facing Application
T1486 Data Encrypted for Impact
T1489 Service Stop
T1490 Inhibit System Recovery
T1558.003 Steal or Forge Kerberos Tickets: Kerberoasting
T1566.001 Phishing: Spearphishing Attachment
T1566.002 Phishing: Spearphishing Link
T1567 Exfiltration over Web Service

Source:(4)

AlphVM BlackCat

- First emerged in November 2021.
- Actively recruits ex-REvil and ex-BlackMatter members.
- The group's locker is written in Rust programming language, unlike other popular ransomware lockers.

MITRE TTPs

T1027.002 – Obfuscated Files or Information: Software Packing
T1027 – Obfuscated Files or Information
T1007 – System Service Discovery
T1059 – Command and Scripting Interpreter
TA0010 – Exfiltration
T1082 – System Information Discovery
T1490 – Inhibit System Recovery
T1485 – Data Destruction
T1078 – Valid Accounts
T1486 – Data Encrypted For Impact
T1140 – Encode/Decode Files or Information
T1202 – Indirect Command Execution
T1543.003 – Create or Modify System Process: Windows Service
T1550.002 – Use Alternate Authentication Material: Pass the Hash

Source: (5)

State-Sponsored APT Activities

Significant APT Groups

- Doppel Spider
- Labyrinth Collima
- Pinchy Spider
- Twisted Spider
- Venomous Bear
- Wizard Spider

SOCRadar collects Advanced Persistent Threat (APT) IOC Feeds from several public and private sources and sensors. These feeds are free and refreshed daily.

DOWNLOAD

Top 5 Malwares Targeting Italy

1	Trojan-Ransom.JS.Alien.gen	15,23 %
2	Trojan-Ransom.Win32.Blocker.pef	7,78 %
3	Trojan-Ransom.Win32.Crypmodng.gen	7,31 %
4	Trojan-ransom.win32.Crypren.gen	7,11 %
5	Trojan-Ransom.Win32.Crypmod.gen	5,76 %

Top 5 Exploits in Italy

1	Exploit.MSOffice.CVE-2018-0802.gen	37,38 %
2	Exploit.MSOffice.CVE-2017-11882.gen	29,37 %
3	Exploit.Win32.CVE-2011-3402.a	14,49 %
4	Exploit.OLE2.Wahel.a	2,71 %
5	Exploit.MSOffice.CVE-2017-0199.h	2,41 %

Source: (6)

Malware Campaigns

Emotet: 14 Italian campaigns identified with "Documents" themed campaigns sent via email with ZIP attachments with passwords containing LNK and XLS files; Emotet is unquestionably the most widespread malware in Italy.

Coper: Two Italian campaigns have been identified aimed at transmitting an APK via SMS to install the Coper banking trojan. (7)

Qakbot: Two Italian "Resend" themed campaigns sent via email with a link to download a ZIP file containing LNK.

Formbook: Italian campaign-themed "Order" conveyed by email with ZIP attachments.

Ursnif: Italian campaign-themed "Documents" conveyed by email with XLSX attachments.

sLoad: Italian campaign-themed "Payments" conveyed via certified email with ZIP attachments containing an additional ZIP containing a malicious VBS. (8)

AgentTesla: Italian "Order" themed campaign conveyed via email with XLSX attachments.

Brata: Italian "Banking" themed campaign conveyed via SMS with a link to download an APK file bearing the name of another well-known Italian banking institution.

Lokibot: two campaigns on the subject of "Contracts" and "Documents" conveyed through DOC attachments.

Phishing Threats

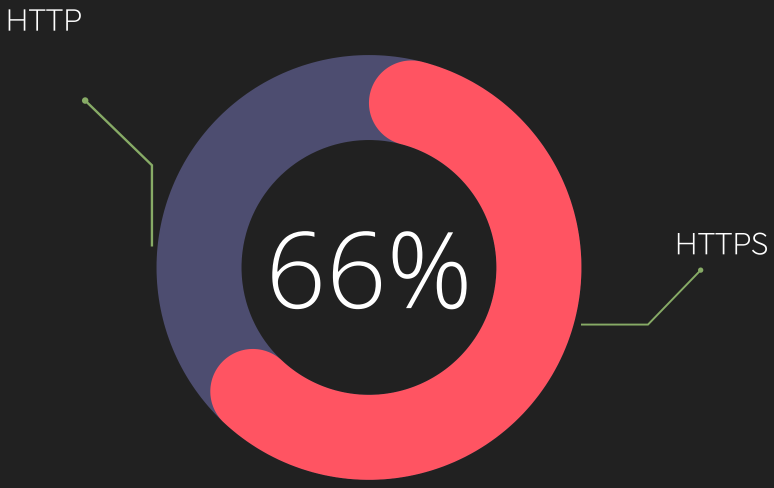
SOCRadar's comprehensive data suggests that approximately 66 % of phishing attacks against Italian organizations were in HTTPS. This shows us that threat actors prefer using HTTPS to trick victims into believing their phishing scams. This also means that even if a website is secured with the "HTTPS" protocol, the chances of getting hit by a phishing attack should again be a concern. Threat actors are using more complex ways to pursue their malicious aims. People should be careful about potential phishing attacks no matter how the website is secured.

Distributed via email and SMS. Aiming the finance industry as well as campaigns aimed at the theft of webmail credentials.

+ 1,400

Phishing attacks detected over the last 12 months

According to data from SOCRadar, about 66 % of all phishing websites now use the HTTPS protocol. Attackers were increasingly using HTTPS to entice their victims to click on malicious links.



Search Your Domain On Phishing Radar

Enter your domain

Critical Asset Exposures & Vulnerabilities

As of July 2022, Italy had more than 7 million open ports, according to SOCRadar Attack Surface Management data, some of which were Remote Desktop Protocol (RDP) ports (approximately 27 thousand open RDP ports, port 3389).

Open RDP ports pose a significant threat to companies with compromised credentials or brute-force attacks since threat actors can remotely access a company's network through RDP protocol. Critical Asset Exposure is a substantial consideration in building a strong security posture.

Below, you can see the open port data in Italy on the 1st of July, 2022.

Port	Protocol	Service
7170: 933.671	TCP/UDP	NSRP
80: 893.742	TCP	HTTP
443: 849.565	TCP	SIP
5060: 679.719	TCP/UDP	HTTPS
8089: 413.104	TCP	Web E-mail Rules
123: 300.837	UDP	NTP
22: 237.131	TCP/UDP/SCTP	SSH
2000: 156.547	TCP	Callbook
8008: 135.406	TCP	Fortinet
179: 130.787	TCP/UDP/SCTP	BGP

As of July 2022, SMB Authentication was disabled on approximately 33 % of SMB ports belonging to Italian organizations. In addition, even though the following vulnerabilities were patched for a long time, there were 5013 hosts vulnerable to Heartbleed (CVE-2014-0160) and 61 hosts vulnerable to EternalBlue (CVE-2017-0144), and 1179 hosts vulnerable to BlueKeep (CVE-2019-0708).

Attackers could exploit these vulnerabilities, and as a result, Italian companies could suffer significant losses from critical cyber-attacks. If the number of Remote Code Execution vulnerabilities is high, there will be an increased number of ransomware attacks affecting Italian enterprises.

Apart from these long-before-patched vulnerabilities, in the last year, Italian companies have suffered cyber-attacks that stemmed from other significant vulnerabilities threat actors actively exploited.

Here are some crucial vulnerabilities and the number of vulnerable hosts in Italy as of the 30th of June, 2022:

CWE Name	Number of Vulnerable Hosts	CVE ID	CVSSv3
Integer Overflow or Wraparound	145,945	CVE-2022-22721	9,8
Inconsistent Interpretation of HTTP Requests (HTTP Request Smuggling)	145,942	CVE-2022-22720	9,8
Improper Initialization	145,941	CVE-2022-22719	7,5
Out-of-bounds Write	142,594	CVE-2021-44790	9,8
Server Side Request Forgery (SSRF)	141,419	CVE-2021-40438	9,0
NULL Pointer Dereference	141,418	CVE-2021-34798	7,5
Out-of-bounds Write	141,418	CVE-2021-39275	9,8
Allocation of Resources Without Limits or Throttling	130,738	CVE-2022-30522	7,5
Out-of-bounds Read	126,103	CVE-2022-28330	5,3
Integer Overflow or Wraparound	126,102	CVE-2022-28614	5,3

In addition to critical vulnerabilities and vulnerable hosts in Italy, below, you can see the most used software in Italy and their vulnerabilities.

Product	Host Count	TOP CVEs
AkamaiGHost	294,033	CVE-2022-22719 CVE-2022-22720 CVE-2022-22721 CVE-2021-44790 CVE-2021-34798 CVE-2021-39275 CVE-2021-40438 CVE-2022-30522 CVE-2022-28330 CVE-2022-28614
Apache httpd	268,991	
MikroTik Bandwidth-test Server	145,403	
nginx	107,275	CVE-2015-0204 CVE-2015-4000 CVE-2018-19935 CVE-2019-9637 CVE-2019-9638 CVE-2019-9639 CVE-2019-9641 CVE-2018-19395 CVE-2018-19396 CVE-2015-9253
OpenSSH	128,171	
CloudFront httpd	117,758	
BGP	93,076	

Source: (9)

Credentials & Stolen Data Intelligence

Stealer Logs

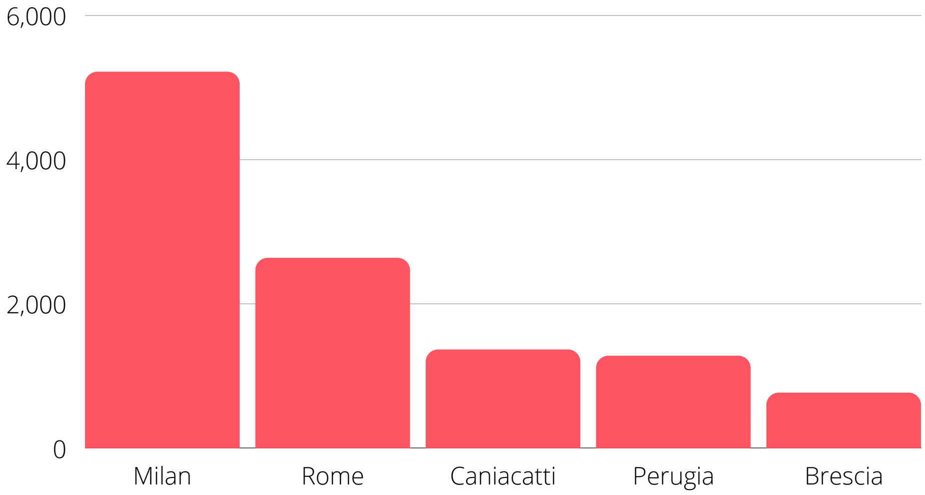
- "221,270" Italian users have been infected with Stealer (Redline, Raccoon, Vidar, etc.) Logs.
- "2,796,910" credentials that access ".it" domains are leaked from the users and distributed on the dark and deep web.

Top Leaked Domains:

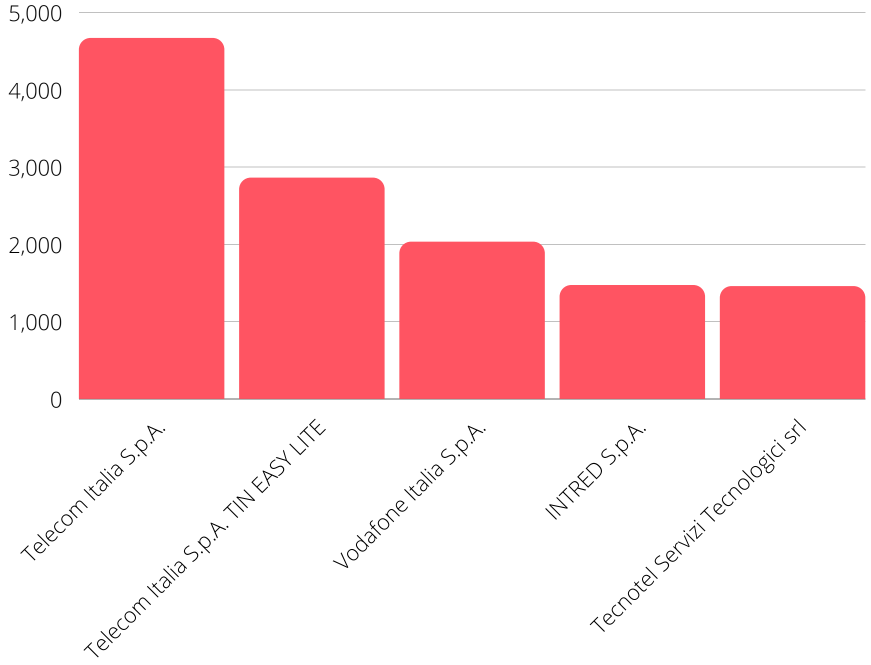
- paste.it
- kahoot.it
- amazon.it
- tim.it
- ebay.it
- aruba.it
- rabb.it
- libero.it
- inps.it
- Pec.it

DDoS

Top Cities Effected From DDoS Attacks



Top Organizations Effected From DDoS Attacks



DDoS Attacks from Italy

35,383

"Recursion: Enabled" Devices

"Recursion: Enabled" Devices

2,845

"UPnP Enabled" Devices

DDoS Campaigns

The latest DDOS attacks against national and international individuals since 11 May were carried out using different techniques than the most common volumetric type 1 DDOS attacks. Thus, the widely used protection systems determined that it passed unnoticed. They are in the market against such attacks as they occur using limited bandwidth.

These DDOS techniques, defined as an application type, aim to saturate the resources of the systems that provide the services, including web servers. In this specific case, the so-called "Slow HTTP" technique was found, which, as a rule, uses HTTP GET requests to saturate the available connections of a web server. (10)

References

(1): https://www.csirt.gov.it/contenuti/rilevato-potenziale-rischio-di-attacco-informatico-ai-danni-di-enti-ed-organizzazioni-nazionali-al01-220529-csirt-ita
(2): https://statistics.securelist.com/country/italian%20republic/ransomware/month
(3): https://www.picussecurity.com/resource/lockbit-2.0-ransomware-ttps-used-in-emerging-ransomware-campaigns
(4): https://www.picussecurity.com/resource/lockbit-2.0-ransomware-ttps-used-in-emerging-ransomware-campaigns
(5): https://www.sentinelone.com/labs/blackcat-ransomware-highly-configurable-rust-driven-raas-on-the-prowl-for-victims/
(6): https://cert-agid.gov.it/statistiche/
(7): https://cert-agid.gov.it/news/trojan-bancario-coper-anche-italia/
(8): https://t.me/certagid/302
(9): Shodan.io
(10): https://www.csirt.gov.it/contenuti/attacchi-ddos-ai-danni-di-soggetti-nazionali-ed-internazionali-avvenuti-a-partire-dall11-maggio-2022-analisi-e-mitigazione-bl01-220513-csirt-ita

RECOMMENDATIONS

- In Italy, as in other countries, ransomware poses a significant threat to all industries. Integrating threat intelligence platforms such as SOCRadar, primarily SIEM, SOAR, Big Data, and preventive security technologies is of great importance. Be instantly aware of cyber attacks or benefit from threat hunting to combat this threat. On the other hand, periodic "business continuity tests" and keeping backups in "immutable storage areas" stand out among the measures to be taken to be prepared against ransomware attacks.

- Due to the problems in patch management processes, threat actors exploit vulnerabilities such as "Heartbleed, EternalBlue, and BlueKeep," patched long ago, instead of infiltrating organizations with zero-day exploit codes. It seems that this situation can be solved by making the patch management processes as mature as possible and risk-oriented prioritization of the institutions. Development of the exploit code within 24 hours after a vulnerability is released makes it difficult to install patches even in the most mature institutions. Institutions should focus on virtual patching solutions at these points and effectively operate the threat hunting process based on the information they obtain from the SOCRadar platform.

- Since remote management ports such as RDP continue to play a significant role in hacking everywhere, from large companies to entrepreneurs, especially "ports accessible from the internet" need to be monitored by cyber security teams. At this point, SOCRadar significantly reduces the workload of cybersecurity teams by closely monitoring open ports.

- Since employee and access information obtained with "thief" type malware is sold to threat actors on the dark web, the stolen information should be closely monitored, and necessary measures should be taken as soon as possible. At this point, it is possible to be aware of these accounts as quickly as possible, as SOCRadar scans the dark web for such corporate leaks.

- Closely following the TTPs of APT groups such as "Doppel Spider, Labyrinth Collima, Pinchy Spider, Twisted Spider, Venomous Bear, Wizard Spider" will ensure that the groups are "under the radar" by searching for them in threat hunting and making changes in the command and control centers and infrastructures of the groups. Thanks to SOCRadar, it is also possible to access the activities and TTPs of threat actors from the Threat Actor/Malware section.

RECOMMENDATIONS

1. Keeping Track of the Vulnerabilities on Digital Assets

There are particular vulnerabilities and sometimes zero-days that threat actors exploit. SOCRadar discovers almost all of your digital assets and their vulnerabilities. SOCRadar's External Attack Surface Mapper tracks your digital assets and the software versions installed on the assets and their vulnerabilities. Therefore, you stop attacks before they start.

2. Identifying and Monitoring Threat Actors

Many organized threat actors like APTs have signature Tactics, Techniques, and Procedures (TTPs). Some of them are only actives and specific regions and sectors. Monitoring the threat landscape and threat actors will make your defenses stronger. SOCRadar's threat intelligence threat feeds, IOCs, IOAs will give you the proactive readiness you need.

3. Phishing Control

Social engineering and phishing are still the starting attack vectors for many cyber attacks. In addition to your company's training for not clicking untrusted links and email attachments without verifying their authenticity, SOCRadar can discover impersonating and typo-squatting domains which could be used for phishing campaigns against your customers and employees.

4. Dark Web and Deep Web Awareness

Threat actors often find their way into systems by purchasing credentials or intelligence from dark and deep web forums and chatter channels. SOCRadar monitors these channels and creates alarms and incidents for anything related to your company.

In addition to these steps, there are more things to protect yourself, such as:

- You could create strict identity and access management policies by utilizing multiple-factor authentication (MFA) and one-time-password (OTP) technologies for your employees.
- User and payment verification for clients. Research shows most people agree with increased protection in check-out pages as long as an explanation is provided.
- You could protect your endpoints, including POS and IoT devices using trusted security hardware software as much as possible.
- You must have backup policies and practices. In addition, you should have multiple recent copies (preferably at least one offline) of your critical data and settings and configurations of your security devices.

HOW CAN WE HELP?

SOCRadar provides Extended Cyber Threat Intelligence (XTI) that combines,

- Cyber Threat Intelligence,
- Digital Risk Protection, and
- External Attack Surface Management Services.

SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the era of transformation.

Darknet and Deep Web Monitoring

SOCRadar's fusion of its unique dark web Recon technology with the human analyst eye achieves further to provide in-depth insights into financially-targeted APT groups and threat landscape.

Credit Card Monitoring

Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

Protecting Customers' PII

Scan millions of data points on the surface web, deep web, and darknet to accurately identify the leakage of your customers' personally identifiable information (PII) in compliance with regulations.

360-Degree Visibility

Achieve digital resiliency by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

See SOCRadar in action

Get Free Access

ABOUT SOCRadar®

SOCRadar provides an early warning system with an extended threat intelligence platform. Extended Threat Intelligence (XTI) tool that is enriched with External Attack Surface Management and Digital Risk Protection. Its false-positive free platform helps companies proactively defend themselves against cyber incidents. SOCRadar is empowered with strong AI algorithms and a highly talented analyst team, together they eliminate false positives.

FOLLOW US!

DISCOVER SOCRADAR® FREE EDITION

With SOCRadar® Free Edition, you'll be able to:

- **Discover your unknown hacker-exposed assets**
- **Check if your IP addresses tagged as malicious**
- **Monitor your domain name on hacked websites and phishing databases**
- **Get notified when a critical zero-day vulnerability is disclosed**

GET FREE ACCESS

CONTACT US

✉ info@socradar.io

☎ +1 (571) 249-4598

651 N Broad St, Suite 205,
Middletown, DE 19709