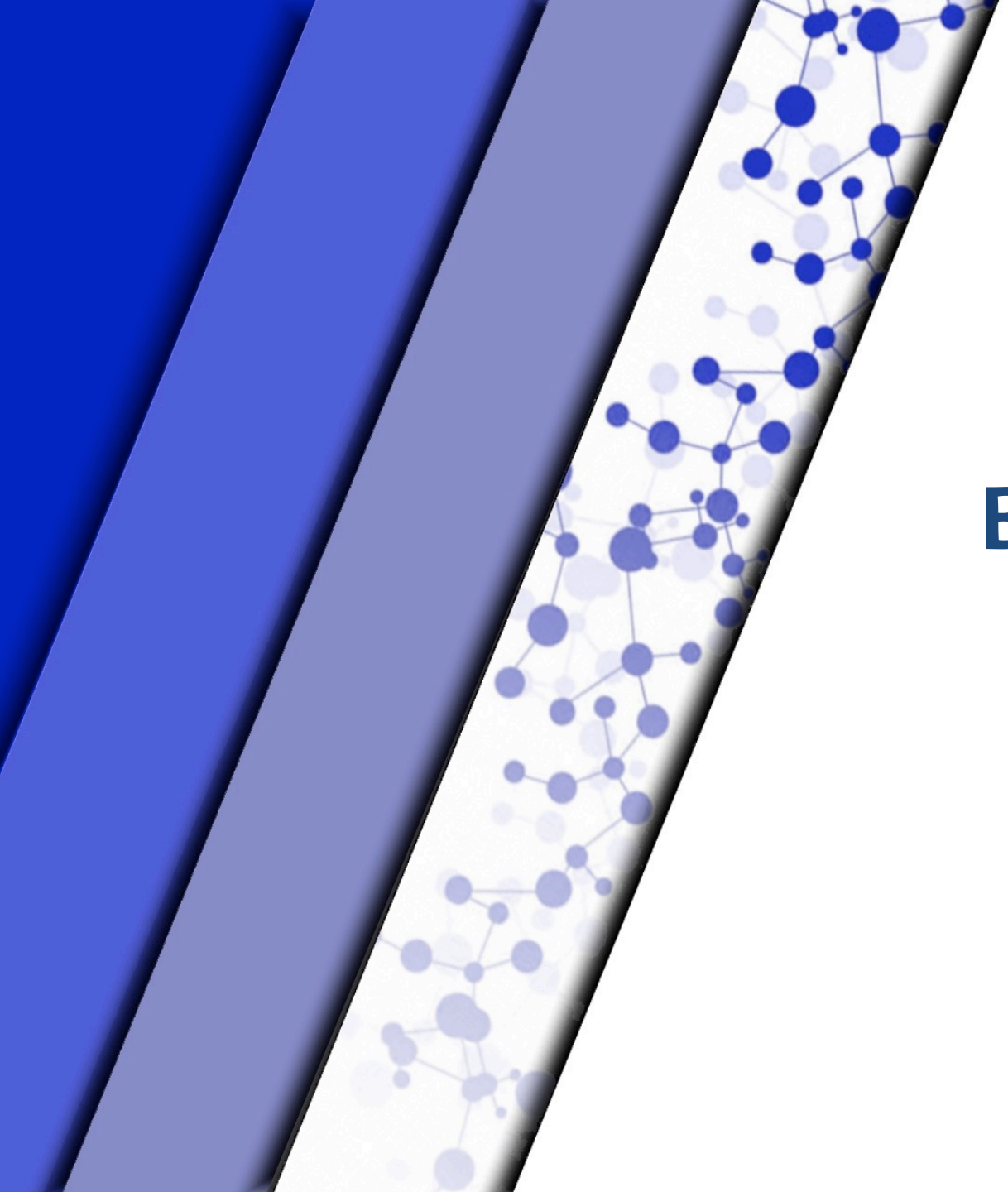


CERTFin

Banche e Sicurezza 2022 -

Threat Landscape Scenario for the Italian Financial Sector

Simone Coltellese

Cyber Security and Fraud Analyst

Threat Landscape Scenario for the Italian Financial sector

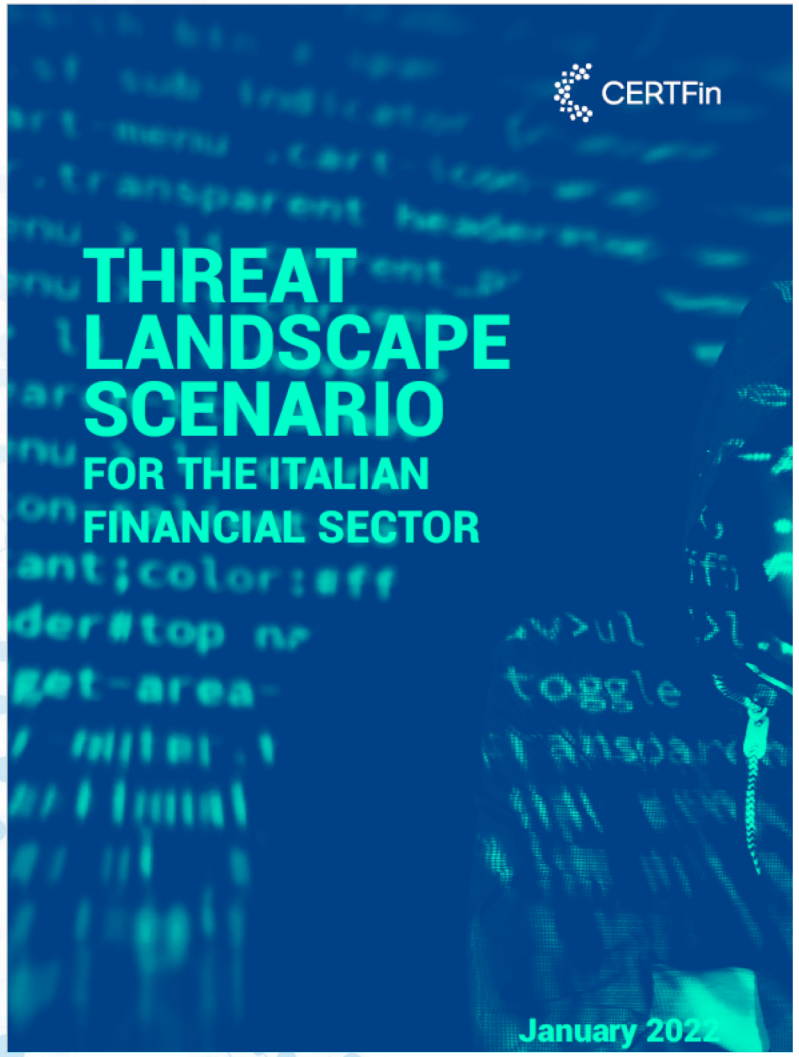


TABLE OF CONTENTS

METHOD

RATING CRITERIA

MITRE ATT&CK

SOURCES

The Golden era of Ransomware

Ransomware has become one of the most significant cybersecurity threats that organizations have to face nowadays:

+150% increase of Ransomware only in the 2020*

64% of RaaS model related attacks*

+130 different ransomware families have been active since 2020 to today**

*Source: Group-IB
** Source: VirusTotal

Ransomware Identikit

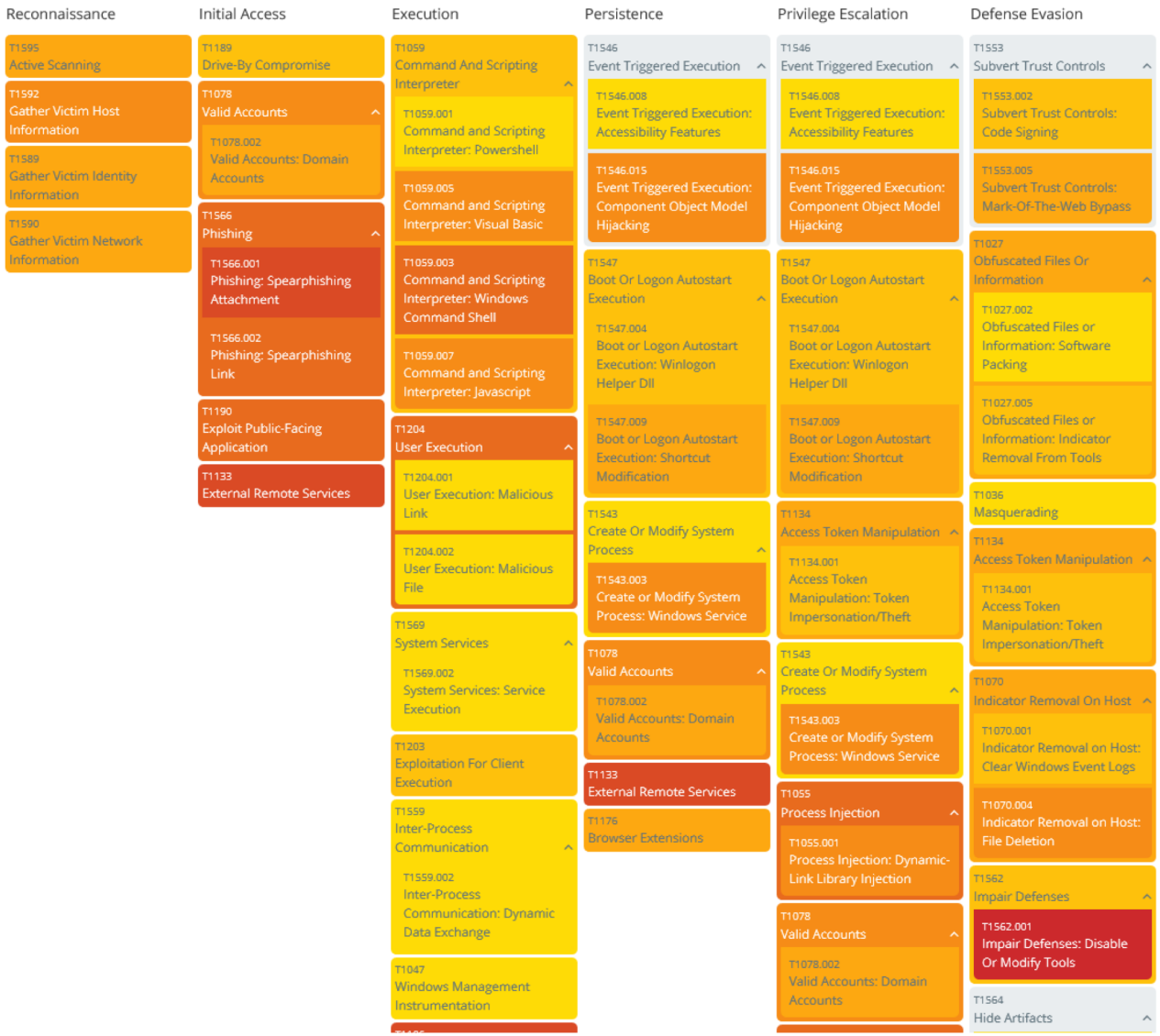
REVIL		**First Seen:** 2019 **Nationality**: RU **Bus Model:** RaaS **Extortion Schema**: Quatruple	**Description: REvil ransomware (also known as Sodinokibi) is one of the most notorious RaaS providers to have emerged in 2019. Since then, its affiliate program has aimed at recruiting partners with different skillsets. Their backgrounds and potential targets give reasonable grounds to believe that the operators behind the group are Russian-based.**
CL0P		**First Seen:** 2019 **Nationality:** RU **Bus Model:** RaaS **Extortion Schema**: Quadruple	**Description: Cl0p is regarded to be a Russian-based cybercriminal group that has been active since early 2019. Having emerged as a variant of another ransomware group called CryptoMix, it is responsible for several infamous Big Game Hunter19 attacks, which are reportedly associated with other threat actors such as FIN11 (often linked to TA505) and UNC2546.**
BLACKMATTER		**First Seen:** 2019 **Nationality:** RU **Bus Model:** Raas **Extortion Schema**: Double	**Description: BlackMatter is a Russian-speaking ransomware group that has been active since July 2021. It is believed to be a reemergence or rebranding of DarkSide and REvil due to the timing with which they both went dark (May and July, respectively) after high-profile attacks.**
CONTI		**First Seen:** 2020 **Nationality:** RU **Bus Model:** RaaS **Extortion Schema**: Double	**Description: Conti is a ransomware variant first observed in early 2020, used by cybercriminals to conduct ransomware attacks against multiple sectors and organisations worldwide, including Australia. Conti is offered as a Ransomware-as-a-Service (RaaS), enabling affiliates to utilise it as desired, provided that a percentage of the ransom payment is shared with the Conti operators as commission.**
LOCKBIT 2.0		**First Seen:** 2021 **Nationality:** ? **Bus Model:** Raas **Extortion Schema**: Double	**Description: LockBit was first detected in 2019, known by its "ABCD" moniker due to the extension used on the encrypted files. In June 2021, the group rebranded as LockBit 2.0 and started incorporating double-extortion layers into its arsenal, as well as offering the StealBit exfiltration tool in its RaaS operations.**

Exploited Vulnerabilities

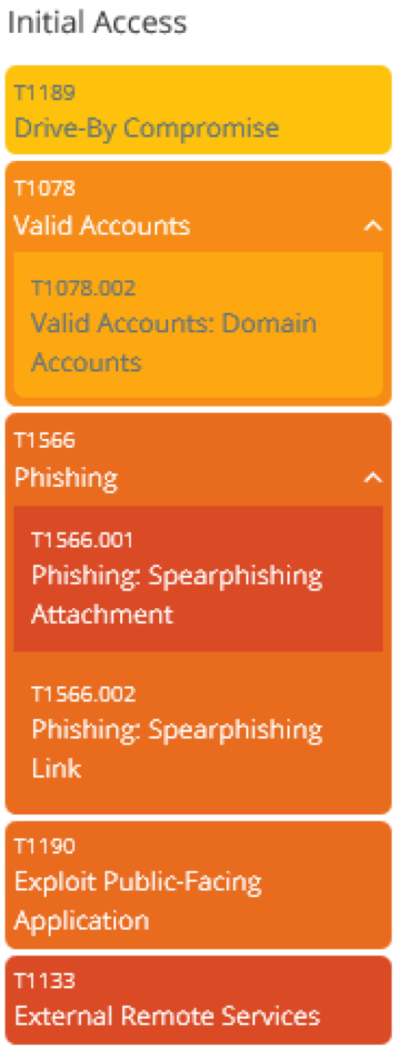
Product	Vulnerability	CVSS Score	REvil	Cl0p	BlackMatter	Conti	LockBit 2.0
Oracle WebLogic Server	CVE-2019-2725	9.8	X				
Fortinet FortiOS/ FortiProxy	CVE-2018-13379	9.8	X			X	X
	CVE-2018-13374	8.8				X	
Pulse Connect Secure	CVE-2019-11510	10	X				
Win32k	CVE-2018-8453	7.8	X				
Microsoft Exchange Server	CVE-2021-27065	7.8	X				
	CVE-2021-26858	7.8	X				
	CVE-2021-26857	7.8	X				
	CVE-2021-26855	9.8	X				
	CVE-2021-34523 (Proxy Shell)	9.8	X		X		
	CVE-2021-34473 (Proxy Shell)	9.8	X		X		
	CVE-2021-31207 (Proxy Shell)	7.2	X		X		
Kaseya VSA	CVE-2021-30116	9.8	X				
	CVE-2021-30118	9.8	X				
	CVE-2021-30117	8.8	X				
	CVE-2021-30121	8.8	X				
	CVE-2021-30201	8.8	X				
	CVE-2021-30119	5.4	X				
	CVE-2021-30120	7.5	X				
Accellion's File Transfer Appliance (FTA) instances	CVE-2021-27101	9.8		X			
	CVE-2021-27102	7.8		X			
	CVE-2021-27103	9.8		X			
	CVE-2021-27104	9.8		X			
HP LaserJet and Samsung product	CVE-2021-3438	7.8				X	
Windows Print Spooler	CVE-2021-34527	8.8				X	
Netlogon Remote Protocol	CVE-2020-1472	10				X	
Confluence Server and Data Center	CVE-2021-26084	9.8					X

CERTFin

Ransomware TTP Analysis



MITRE ATT&CK: Initial Access



Initial Access (TA0001): consists of techniques that use various entry vectors to gain their initial foothold within a network.

Most used techniques used to break into the organization's network:

- T1133 (**External Remote Services**)
- T1190 (**Exploit Public-Facing Application**)
- T1566.001 (**Spear phishing Attachment**)

Threat evolution in 2022 – Preview

- Threat landscape influenced by the conflict between Russia and Ukraine. EU sanctions increased the risks of cyber attacks against west organizations, including those of the financial sector.
- Increase in DDoS attacks.
- Increase in wiper attacks.
- Ransomware will not decrease.

Thank You!

CERTFin

Defend. Inform. Evolve.

For more info visit www.certfin.it or write to ricerca@certfin.it