



**CERTFin**

# **Banche e Sicurezza 2022 -** **Threat Landscape Scenario** **for the Italian Financial Sector**

**Simone Coltellese**

*Cyber Security and Fraud Analyst*



## TABLE OF CONTENTS

EXECUTIVE SUMMARY	3
METHOD	6
GLOSSARY	9
TOP THREATS	11
THREATS TARGETING BANKING ORGANIZATIONS – RANSOMWARE ROUNDUP	13
INTRODUCTION & TREND	15
REVIL	21
CLOP	24
BLACKMATTER	26
CONTI	29
LOCKBIT 2.0	30
RANSOMWARE TTP ANALYSIS	33
VULNERABILITIES	39
THREATS TARGETING END USERS	42
INTRODUCTION	42
SHARKBOT: A NEW GENERATION OF ANDROID TROJANS IS TARGETING BANKS IN EUROPE	51
A FOCUS ON BYPASSING VOICE BIOMETRIC SYSTEMS	54
CONCLUSIONS AND OUTLOOK	59
CREDITS	62

## METHOD

**RATING CRITERIA**

**MITRE ATT&CK**

**SOURCES**

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

<p>REVIL</p>		<p>First Seen: 2019  <b>Nationality:</b> RU  <b>Bus Model:</b> RaaS  Extortion Schema: Quatruple</p>	<p>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.</p>
<p>CLOP</p>		<p>First Seen: 2019  <b>Nationality:</b> RU  <b>Bus Model:</b> RaaS  Extortion Schema: Quatruple</p>	<p>Description: ClOp 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.</p>
<p>BLACKMATTER</p>		<p>First Seen: 2019  <b>Nationality:</b> RU  <b>Bus Model:</b> Raas  Extortion Schema: Double</p>	<p>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.</p>
<p>CONTI</p>		<p>First Seen: 2020  <b>Nationality:</b> RU  <b>Bus Model:</b> RaaS  Extortion Schema: Double</p>	<p>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.</p>
<p>LOCKBIT 2.0</p>		<p>First Seen: 2021  <b>Nationality:</b> ?  <b>Bus Model:</b> Raas  Extortion Schema: Double</p>	<p>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.</p>

Product	Vulnerability	CVSS Score	REvil	CIoP	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	
Kaseya VSA	CVE-2021-31207 (Proxy Shell)	7.2	X			X	
	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					
Acellion'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

Reconnaissance	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
T1595 Active Scanning	T1189 Drive-By Compromise	T1059 Command And Scripting Interpreter	T1546 Event Triggered Execution	T1546 Event Triggered Execution	T1553 Subvert Trust Controls
T1592 Gather Victim Host Information	T1078 Valid Accounts	T1059.001 Command and Scripting Interpreter: Powershell	T1546.008 Event Triggered Execution: Accessibility Features	T1546.008 Event Triggered Execution: Accessibility Features	T1553.002 Subvert Trust Controls: Code Signing
T1589 Gather Victim Identity Information	T1078.002 Valid Accounts: Domain Accounts	T1059.005 Command and Scripting Interpreter: Visual Basic	T1546.015 Event Triggered Execution: Component Object Model Hijacking	T1546.015 Event Triggered Execution: Component Object Model Hijacking	T1553.005 Subvert Trust Controls: Mark-Of-The-Web Bypass
T1590 Gather Victim Network Information	T1566 Phishing	T1059.003 Command and Scripting Interpreter: Windows Command Shell	T1547 Boot Or Logon Autostart Execution	T1547 Boot Or Logon Autostart Execution	T1027 Obfuscated Files Or Information
	T1566.001 Phishing: Spearphishing Attachment	T1059.007 Command and Scripting Interpreter: Javascript	T1547.004 Boot or Logon Autostart Execution: Winlogon Helper Dll	T1547.004 Boot or Logon Autostart Execution: Winlogon Helper Dll	T1027.002 Obfuscated Files or Information: Software Packing
	T1566.002 Phishing: Spearphishing Link	T1204 User Execution	T1547.009 Boot or Logon Autostart Execution: Shortcut Modification	T1547.009 Boot or Logon Autostart Execution: Shortcut Modification	T1027.005 Obfuscated Files or Information: Indicator Removal From Tools
	T1190 Exploit Public-Facing Application	T1204.001 User Execution: Malicious Link	T1543 Create Or Modify System Process	T1134 Access Token Manipulation	T1036 Masquerading
	T1133 External Remote Services	T1204.002 User Execution: Malicious File	T1543.003 Create or Modify System Process: Windows Service	T1134.001 Access Token Manipulation: Token Impersonation/Theft	T1134 Access Token Manipulation
		T1569 System Services	T1078 Valid Accounts	T1543 Create Or Modify System Process	T1134.001 Access Token Manipulation: Token Impersonation/Theft
		T1569.002 System Services: Service Execution	T1078.002 Valid Accounts: Domain Accounts	T1543.003 Create or Modify System Process: Windows Service	T1070 Indicator Removal On Host
		T1203 Exploitation For Client Execution	T1133 External Remote Services	T1055 Process Injection	T1070.001 Indicator Removal on Host: Clear Windows Event Logs
		T1559 Inter-Process Communication	T1176 Browser Extensions	T1055.001 Process Injection: Dynamic-Link Library Injection	T1070.004 Indicator Removal on Host: File Deletion
		T1559.002 Inter-Process Communication: Dynamic Data Exchange		T1078 Valid Accounts	T1562 Impair Defenses
		T1047 Windows Management Instrumentation		T1078.002 Valid Accounts: Domain Accounts	T1562.001 Impair Defenses: Disable Or Modify Tools
					T1564 Hide Artifacts



## Initial Access

T1189

Drive-By Compromise

T1078

Valid Accounts ^

T1078.002

Valid Accounts: Domain  
Accounts

T1566

Phishing ^

T1566.001

Phishing: Spearphishing  
Attachment

T1566.002

Phishing: Spearphishing  
Link

T1190

Exploit Public-Facing  
Application

T1133

External Remote Services

**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 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](http://www.certfin.it) or write to [ricerca@certfin.it](mailto:ricerca@certfin.it)*