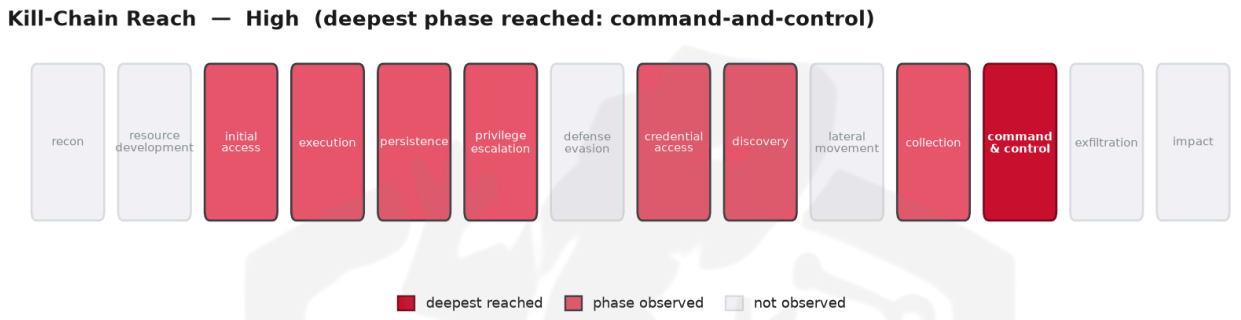
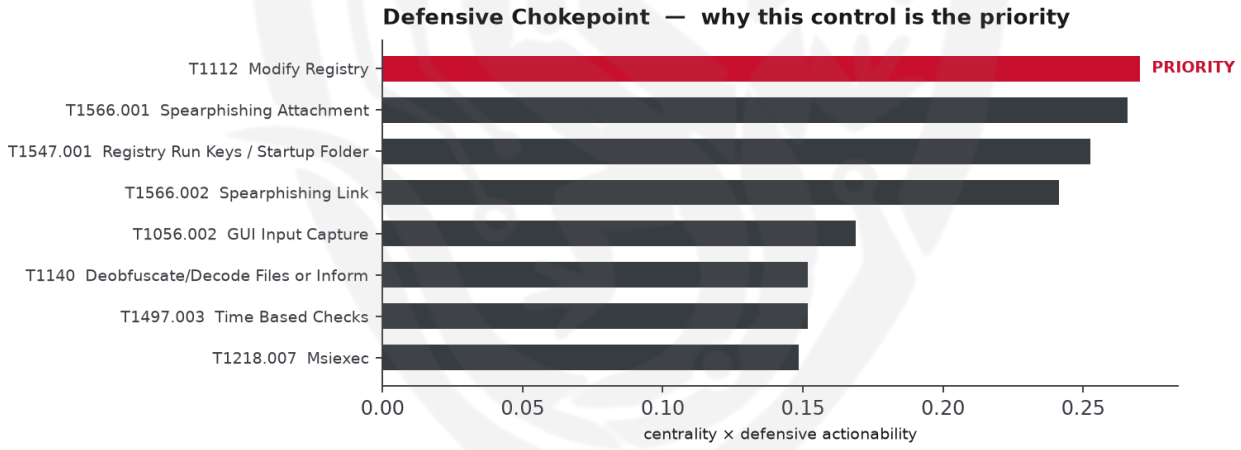
THREAT REPORT: OUSABAN CAMPAIGN BY UNKNOWN_ADVERSARY

Visual Summary



How far down the attack chain this campaign reached; deepest phase in crimson.



The control that most disrupts the attack (priority in crimson).

Summary

The observed cluster of activity, attributed to an unknown threat actor, has been targeting financial sectors in Portugal and Spain with the Ousaban, Metamorfo, and Casbaneiro malware families. The primary concern is the potential for sensitive data compromise, and priority should be given to monitoring and restricting access to sensitive registry keys. The threat actor's use of various techniques, including screen capture and keylogging, poses a significant risk to the targeted organizations.

Threat Overview

The threat actor, responsible for the Ousaban campaign, utilizes a range of malware families, including Ousaban, Metamorfo, and Casbaneiro, to target financial institutions in the Iberian Peninsula. The

campaign's victimology suggests a focus on the finance sector, with the threat actor employing techniques such as screen capture, keylogging, and symmetric cryptography to achieve their objectives.

Attack Chain and Priority Control

The observed attack chain involves a combination of techniques, including spearphishing, malicious file execution, and system checks, ultimately leading to the modification of registry keys. The priority technique, T1112 Modify Registry, serves as a critical chokepoint in the attack chain. To mitigate this threat, the recommended priority control is to "Monitor sensitive registry keys for modification; restrict registry-edit tools for unprivileged users."

Infrastructure and Corroboration

The malicious infrastructure associated with this campaign is hosted on providers such as BL Networks, Omegatech LTD, and QWINS Ltd. Additionally, abuse.ch has corroborated the presence of the RustyStealer malware family, which may be related to the observed activity. However, according to AbuseIPDB, there are no indicators with a confidence level of 80% or higher, with the highest confidence seen being 0%.

Technical Appendix

Ground-truth telemetry from the source pulse; analytical scores are secondary and clearly labelled.

Observed Techniques (ATT&CK, expert-tagged by source)

- T1113 Screen Capture
- T1056.001 Keylogging
- T1204.002 Malicious File
- T1573.001 Symmetric Cryptography
- T1497.001 System Checks
- T1566.002 Spearphishing Link
- T1566.001 Spearphishing Attachment
- T1115 Clipboard Data
- T1218.007 Msiexec
- T1140 Deobfuscate/Decode Files or Information
- T1497.003 Time Based Checks
- T1185 Browser Session Hijacking
- T1112 Modify Registry
- T1547.001 Registry Run Keys / Startup Folder
- T1056.002 GUI Input Capture
- T1027 Obfuscated Files or Information
- T1070.004 File Deletion
- T1071.001 Web Protocols
- T1059.005 Visual Basic

- T1204.001 Malicious Link

Analytical Scores

- Priority technique (graph chokepoint): T1112 Modify Registry (centrality 0.2846).
- Operational risk: High (score 0.636, reaches command-and-control).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5398; reference threshold tau = 0.6).
- These are behavioural resemblances for defensive playbook cross-referencing, not an identity assessment. Where the source pulse names an actor, that attribution is authoritative; the overlaps below neither confirm nor contest it.

Nearest historical profiles by behavioural overlap (resemblance only):

Historical Profile	Behavioural Overlap
FIN4	0.5398
Molerats	0.5199
Windshift	0.4928
RedCurl	0.4795
Darkhotel	0.4777

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: RustyStealer.
- Note: enrichment raises the severity signal (an IOC at or above 80% AbuseIPDB confidence, or a confirmed malware-family hit). This is context, not a change to the source assessment.

Indicators of Compromise (defanged — non-clickable)

The network and file indicators observed in this activity are listed below for blocklisting:

Type	Indicator	Context
IP	162[.]33[.]179[.]46	AbuseIPDB 0% (US) · AS399629 BL Networks
IP	91[.]92[.]240[.]140	AbuseIPDB 0% (DE) · AS202412 Omegatech LTD

Type	Indicator	Context
IP	78[.]40[.]209[.]32	AbuseIPDB 0% (FI) · AS213702 QWINS Ltd
IP	213[.]159[.]64[.]191	AbuseIPDB 0% (DE)
Domain	controlfacturas[.]site	
Domain	faturanova[.]xyz	
Domain	facture-arsys[.]duckdns[.]org	
Domain	faturanova[.]duckdns[.]org	
Hash	d4eb4ff02df659fdeec17d36b77084627469623bb3c7d16383d257404b52d1c3	RustyStealer
Hash	18205d398e5df7d38705dbdc700ccb46	
Hash	22e3cd043e36a9c0bad1479ad4c3214a	
Hash	26c0aee6c79935ee6da46e6444f1c109	RustyStealer
Hash	ebb680f7ae4db6cdc426b8112d2536b6	
Hash	11ca4e19ea79f68aaf23c4afe472dbc03833002c	
Hash	1ec576cf0c82c023f2eb380809588980b98cd296	
Hash	26b9b123e0f664dd9792b820255fe991496cf2d6	RustyStealer
Hash	6e37b4a0c1d747d19abb6736a1ec3293972d3e0f	
Hash	18fd38988d58dd930f5992d448cc09a9400c1eafba76b820b9a83239ac48cf4e	
Hash	19ac18a50abb48dc0ea9524850acfaec49359e6b3bcc67c6193c2d56da812c71	
Hash	1e77992666acbbfa0d01fcefa9cc8fbdac291e0681b35745be27c6dfb159a375	
Hash	21b24f7ee1f6bdbbb670f0394d66009ee0daa8ced57048298da715e88f7a7cdd	

Type	Indicator	Context
Hash	48723a33bab89f174750576f9a62da35b3b9e5ac31a5a8f1ce9859a1b35bf8b8	
Hash	4c9fdc2823da505ef339d43c6ad38499b7e3447736733e42b5ab6b1afcfd42aa	
Hash	4ca2c863d740bb7022776dccabd8ae34bb9998768928042d76ebcf08984eefcb	
Hash	540ee1936e61d2344b5ebc93485589a351ec2f113a9b4940ae16f3baa4807392	
Hash	5837e47198a20877e1b04b270c36d9194206ee38d4f32fe3151b3c3b396c4f0d	
Hash	5a2ed557c357ba8f96f2d55a8a00695987806b5df766cd1dfdab0cbed111774a	
Hash	5e06af187b45476ade0d953e834fced6197d0a33ac60c2575877660e26ab15e8	
Hash	65c1a998bac48e02b52b1c850cd500e9fb87521e21755c3a4a491243f5f9a700	
Hash	6bc2e11b0917f47d0557288c4f0cb20bd7589185943b989a969fdc6d3704ee73	
Hash	9d07a83cf89685651ea8992047ae694c24f6ddef193044357debd15ce07a64fe	
Hash	9e81ade09cc18f0fc09d73e72d2e0bffad02f52fdcc26553e473cee8cabc1567	
Hash	e2f0c2d4c1552cd81fa012043e4a5ac832582b639b7b6b7eccc0c4802d7a8ad8	
Hash	e6e78eb2e9bd41a4bc62f7ad54d095ea9813864bebe37172ae30a1afa631fe14	
Hash	fadbb8061715128bebecf7bc59132b6bb04fe8cc39b965aa5b8722dffe28d7e7	
Hash	ffb9eb47cc0cb2f43e04a10dc84df13d04bca1ebacbe47fad0b669728de2f59c	

Reputation by AbuseIPDB · malware attribution by abuse.ch · Geo/ASN data by IP2Location LITE.

Flame Cell // Adversary Pivot [BETA]

BETA. A hypothetical tabletop projection, anchored to documented ATT&CK behaviour and technique co-occurrence across 170 tracked groups. It is not a prediction; treat it as a war-game prompt and review before acting. Spot a pivot that looks wrong? norbert@salacti.com

- **Control applied:** T1112 Modify Registry (persistence)
- **Observed here:** the threat actor used T1547.001 Registry Run Keys / Startup Folder here as an alternative persistence technique.
- **Projected pivot:** T1547.001 Registry Run Keys / Startup Folder (persistence)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The actor could pivot to using T1547.001 Registry Run Keys / Startup Folder to maintain persistence, potentially by adding malicious entries to the Startup folder or Run/RunOnce registry keys, which may allow them to regain a foothold after the block on modifying the registry. This technique may be used to execute malicious code or scripts at startup, which would likely be a key objective for the actor. To counter this, the mandated defensive control of auditing Windows Startup folders and Run/RunOnce registry keys for unauthorized entries and alerting on .lnk or script creation in Startup by browser/email temp paths should be implemented.

Detection and hardening for the pivot (T1547.001 Boot or Logon Autostart Execution)

- **Telemetry:** Sysmon (registry + process); EDR autostart/ASEP inventory
- **Detect:**
  - Sysmon 13 (registry value set) on Run/RunOnce keys under HKLM & HKCU ...\CurrentVersion\Run*
  - Sysmon 11 for shortcuts/scripts created in Startup folders
  - Periodic ASEP (autostart extensibility point) diff against a known-good baseline
- **Harden:**
  - Restrict write access to autostart registry keys and Startup folders
  - Application control to block unsigned autostart binaries
- **MITRE:** M1047 Audit, M1038 Execution Prevention · DS0019 Service, DS0024 Windows Registry, DS0022 File