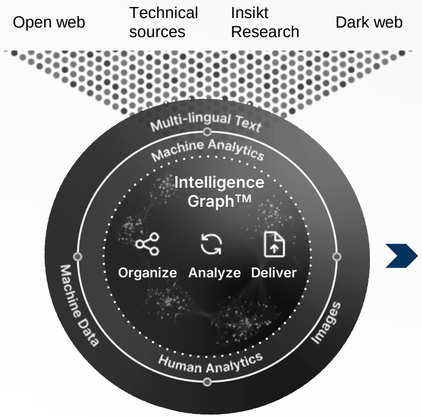
Threat profiling automatization

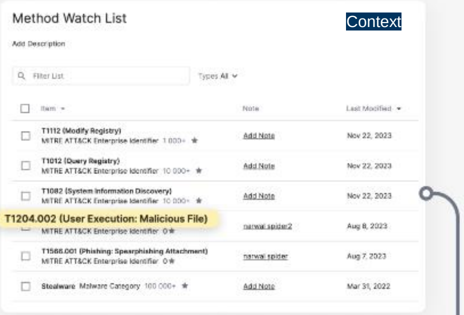
Collect->Analyze->Identify->Prioritize->Profile Threat Behavior



Uses Recorded Future's cyber attack collection **[NLP]** analyzed for targeting of your industry, tech stack, vulnerabilities and third-parties to surface relevant actors

Research reporting on threat actors **[Insikt]** to understand targets, motives & tactics, techniques and procedures (TTPs)

Method Watch List monitors MITRE tactics & techniques



Method Watch List

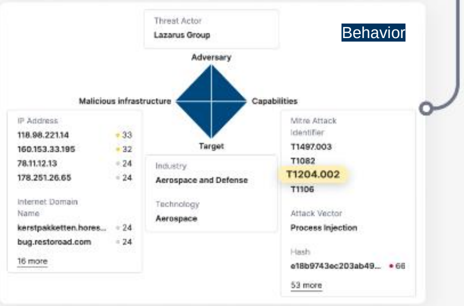
Context

Add Description

Filter List   Types All

□ Item	Note	Last Modified
□ T1112 (Modify Registry) MITRE ATT&CK Enterprise Identifier 1 000+ ★	Add Note	Nov 22, 2023
□ T1012 (Query Registry) MITRE ATT&CK Enterprise Identifier 10 000+ ★	Add Note	Nov 22, 2023
□ T1082 (System Information Discovery) MITRE ATT&CK Enterprise Identifier 10 000+ ★	Add Note	Nov 22, 2023
T1204.002 (User Execution: Malicious File) MITRE ATT&CK Enterprise Identifier 0 ★	narwal spider2	Aug 8, 2023
□ T1566.001 (Phishing: Spearphishing Attachment) MITRE ATT&CK Enterprise Identifier 0 ★	narwal spider	Aug 7, 2023
□ Stealware Malware Category 100 000+ ★	Add Note	Mar 31, 2022

Insikt Validated Cyber Attack Note
with Diamond Model includes this technique



Behavior

Threat Actor
Lazarus Group

IP Address
118.98.221.14 33
160.153.33.195 32
78.11.12.13 24
178.251.26.65 24

Internet Domain Name
kerstpakketten.hores... 24
bug.restoroad.com 24
16 more

Industry
Aerospace and Defense

Technology
Aerospace

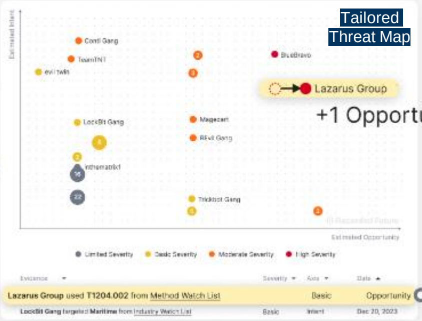
Mitre Attack Identifier
T1497.003
T1082
T1204.002
T1106

Attack Vector
Process Injection

Hash
e18b9743ec203ab49... 66
53 more

Threat Map

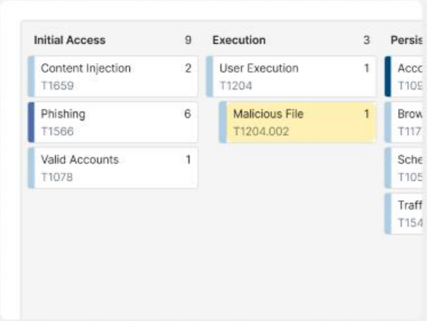
Lazarus Group's **opportunity score increases by 1**, because the threat actor used the TTP monitored in your Watch List



Evidence	Severity	Axis	Date
Lazarus Group used T1204.002 from Method Watch List		Basic	Opportunity
LockBit Gang targeted Maritime from Industry Watch List	Basic	Intent	Dec 20, 2023

TTP MITRE Matrix

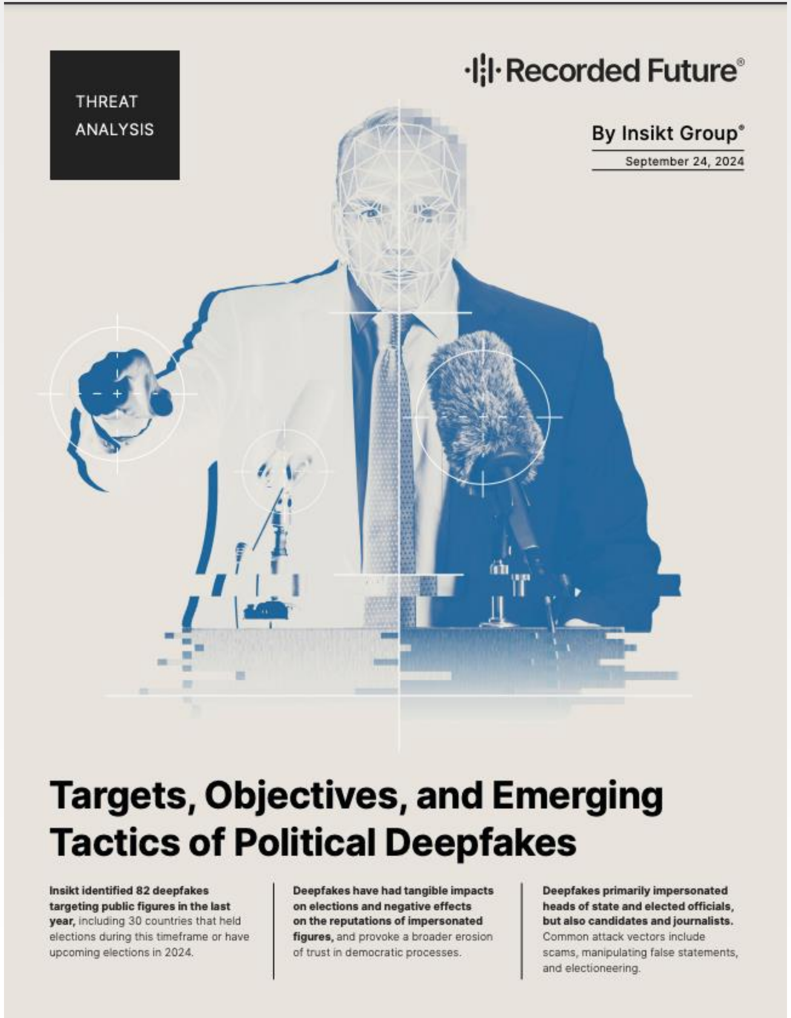
Lazarus Group's use of the TTP triggers a count in your **TTP MITRE Matrix**



Initial Access 9	Execution 3	Persis
Content Injection 2 T1659	User Execution 1 T1204	Acco T109
Phishing 6 T1566	Malicious File 1 T1204.002	Brow T117
Valid Accounts 1 T1078		Sche T105
		Traff T154

Source: Recorded Future

Recorded Future®



THREAT ANALYSIS

Recorded Future®

By Insikt Group®

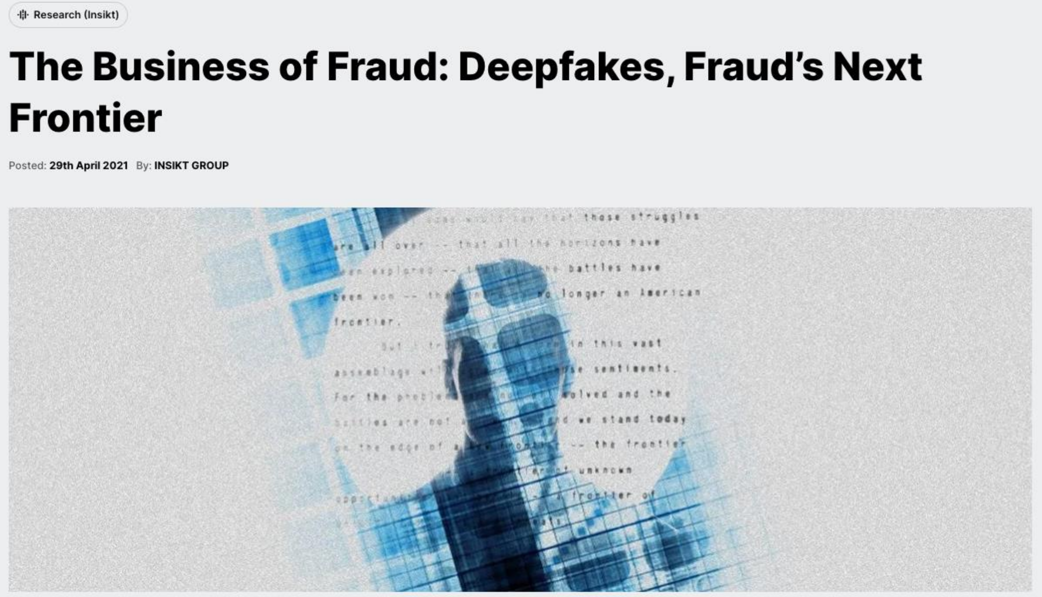
September 24, 2024

Targets, Objectives, and Emerging Tactics of Political Deepfakes

Insikt identified 82 deepfakes targeting public figures in the last year, including 30 countries that held elections during this timeframe or have upcoming elections in 2024.

Deepfakes have had tangible impacts on elections and negative effects on the reputations of impersonated figures, and provoke a broader erosion of trust in democratic processes.

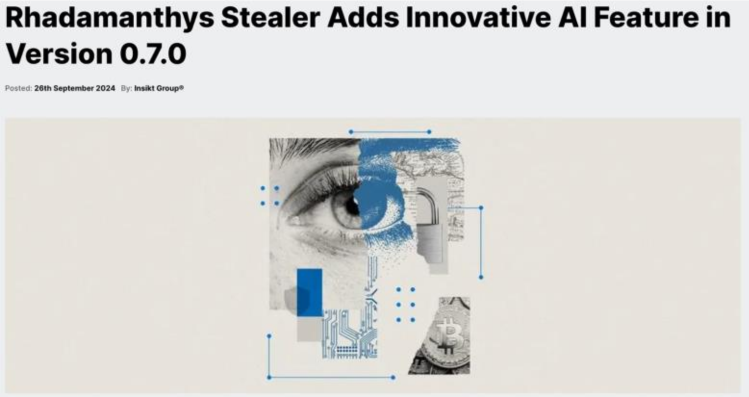
Deepfakes primarily impersonated heads of state and elected officials, but also candidates and journalists. Common attack vectors include scams, manipulating false statements, and electioneering.



Research (Insikt)

The Business of Fraud: Deepfakes, Fraud's Next Frontier

Posted: **29th April 2021** By: **INSIKT GROUP**



Rhadamanthys Stealer Adds Innovative AI Feature in Version 0.7.0

Posted: **26th September 2024** By: **Insikt Group®**

Thank you

Contact us at:

italy@recordedfuture.com

Browser Extension:
instant access to threat intelligence from any web-based resource.

Free Access to our Malware Sandbox
Upload and analyze malware samples, through our state-of-the-art sandbox

View Your Digital Footprint from an Attacker's Perspective
Discover historical DNS records and identify changes in the blink of an eye.

https://www.recordedfuture.com/free-products