Clusit
Associazione Italiana
per la Sicurezza Informatica

ASTREA Advanced Security, Training
Research, Events Agency

SECURITY SUMMIT

Security Summit

Milano 19-20-21 marzo 2024

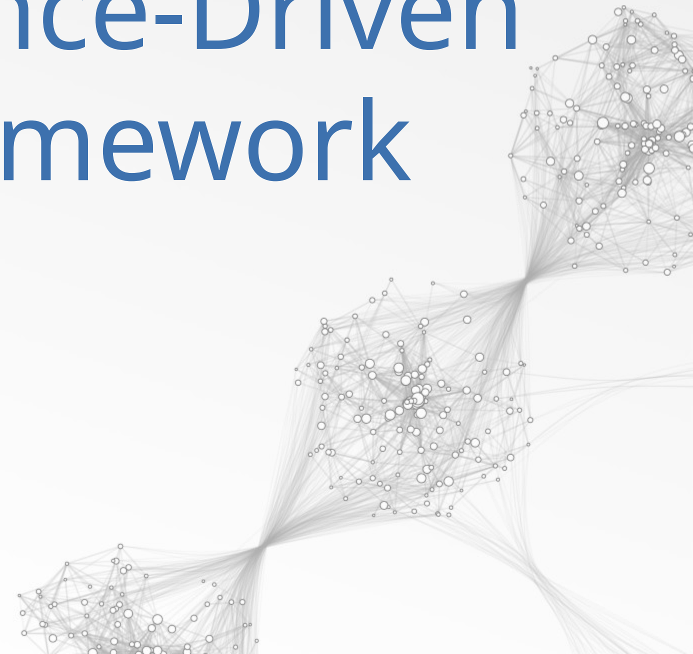
Building an Intelligence-Driven Risk Reduction Framework

Massimiliano Brugnoli, Recorderfuture
19 marzo 2024 orario 16.30 - 17.00

Building an Intelligence-Driven Risk Reduction Framework

Massimiliano Brugnoli - Sales Engineer

Recorded Future



Agenda

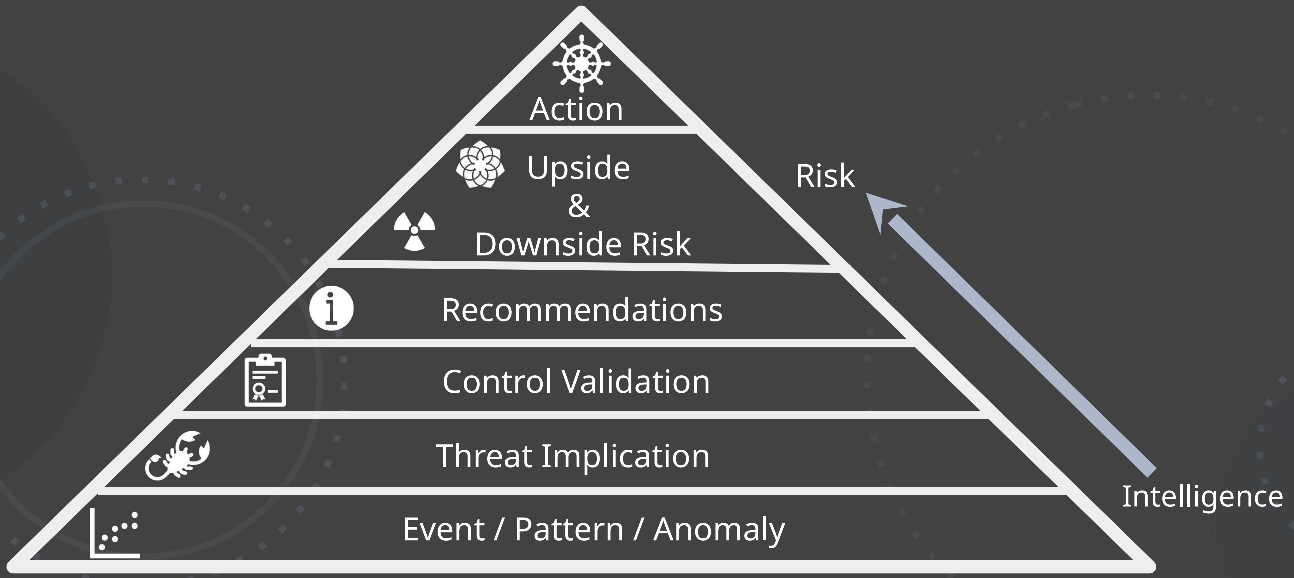
❑ Why Intelligence

❑ Adversary behavior

❑ Threat profiling

❑ Risk reduction

Intelligence to Risk (I2R) Pyramid

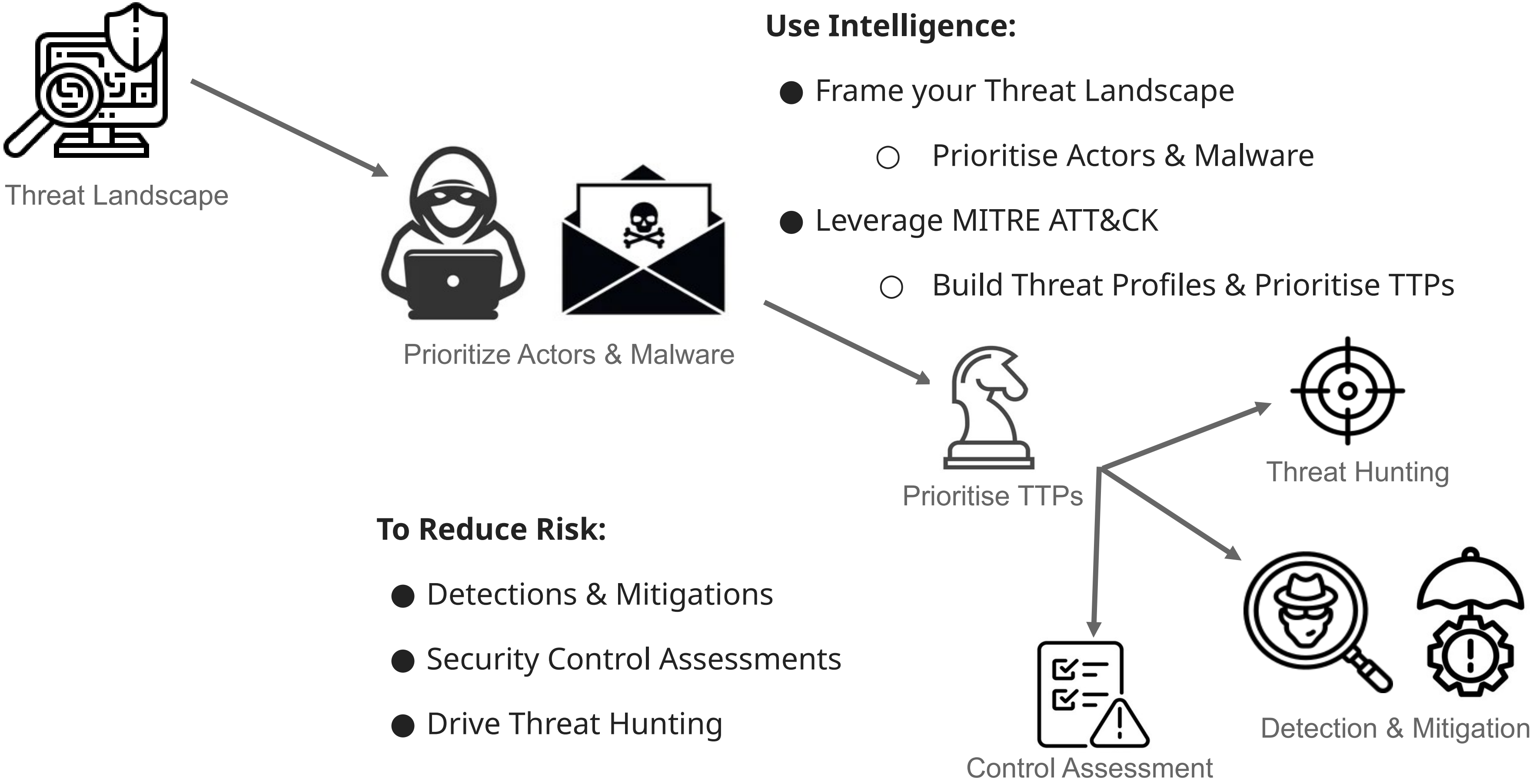


Source: Levi Gundert & Dylan Davis, Recorded Future

Overview: Structured and Repeatable

Use Intelligence:

- Frame your Threat Landscape
  - Prioritise Actors & Malware
- Leverage MITRE ATT&CK
  - Build Threat Profiles & Prioritise TTPs



Threat Landscape

Prioritize Actors & Malware

Prioritise TTPs

Threat Hunting

Control Assessment

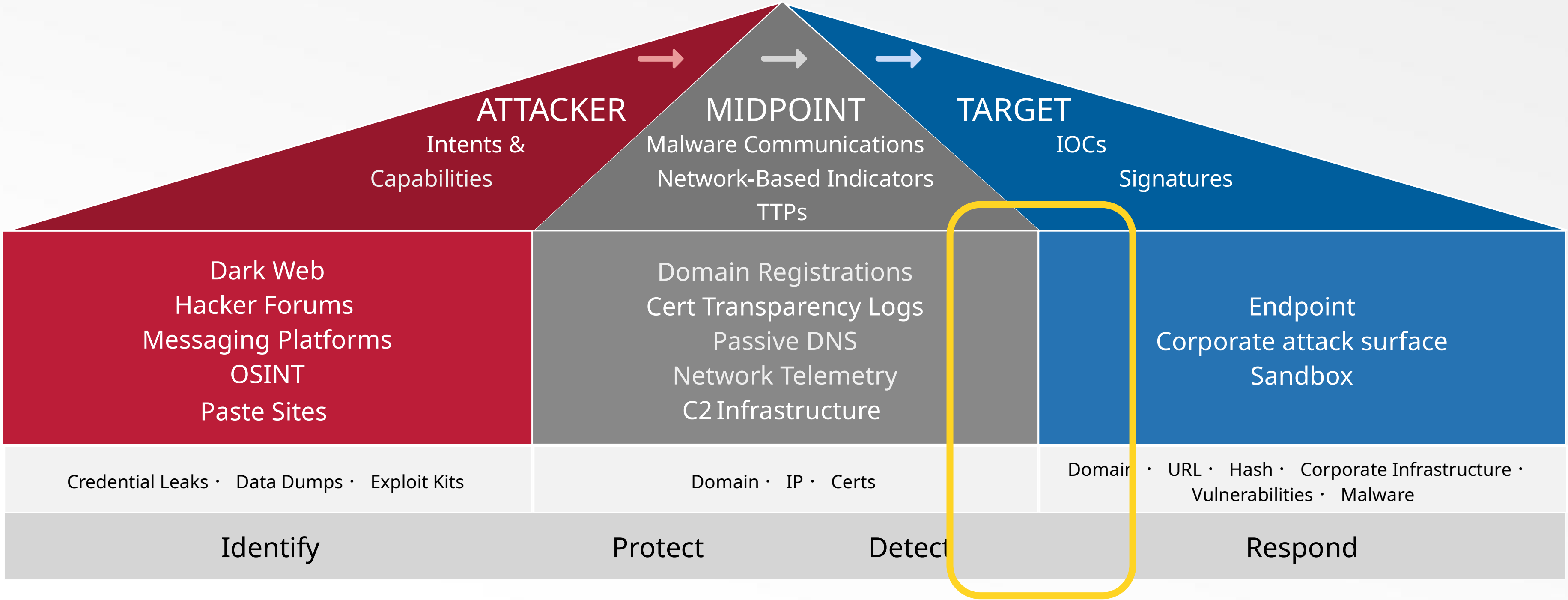
Detection & Mitigation

To Reduce Risk:

- Detections & Mitigations
- Security Control Assessments
- Drive Threat Hunting

Window of opportunity

Visibility From Attackers Through Midpoint to Targets



ATTACKER
Intents & Capabilities

MIDPOINT
Malware Communications
Network-Based Indicators
TTPs

TARGET
IOCs
Signatures

Dark Web
Hacker Forums
Messaging Platforms
OSINT
Paste Sites

Domain Registrations
Cert Transparency Logs
Passive DNS
Network Telemetry
C2 Infrastructure

Endpoint
Corporate attack surface
Sandbox

Credential Leaks · Data Dumps · Exploit Kits

Domain · IP · Certs

Domain · URL · Hash · Corporate Infrastructure · Vulnerabilities · Malware

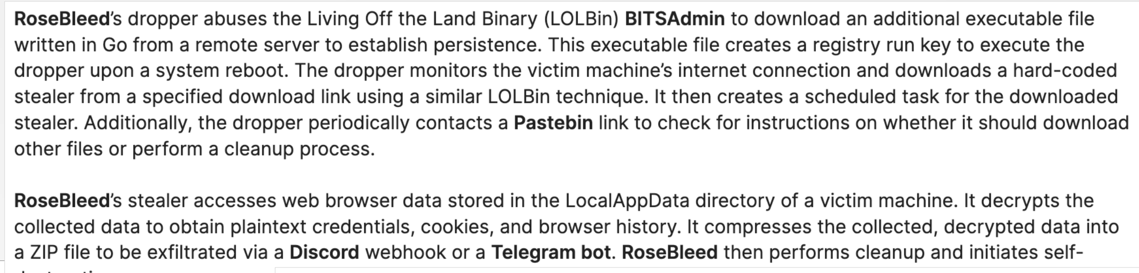
Identify | Protect | Detect | Respond

Window of opportunity

Recorded Future®

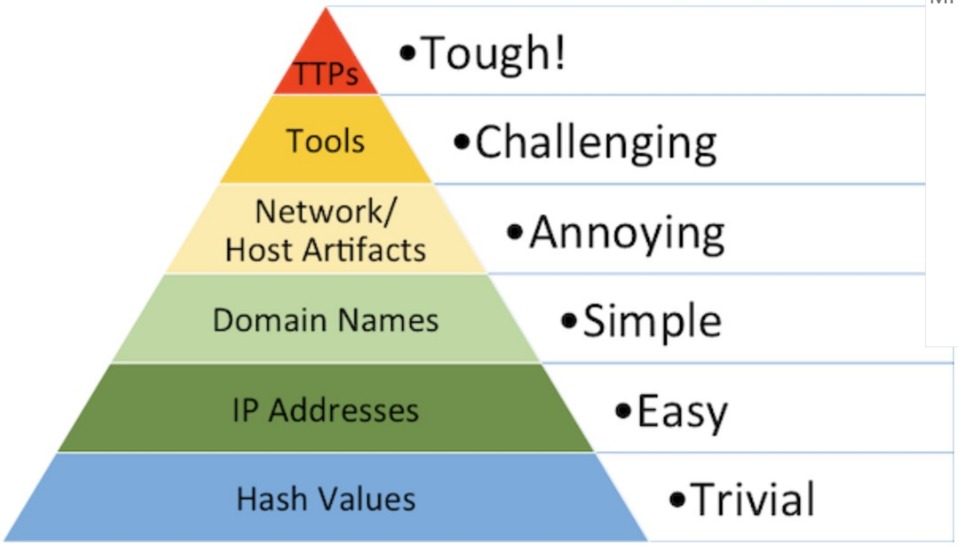
Why behavior

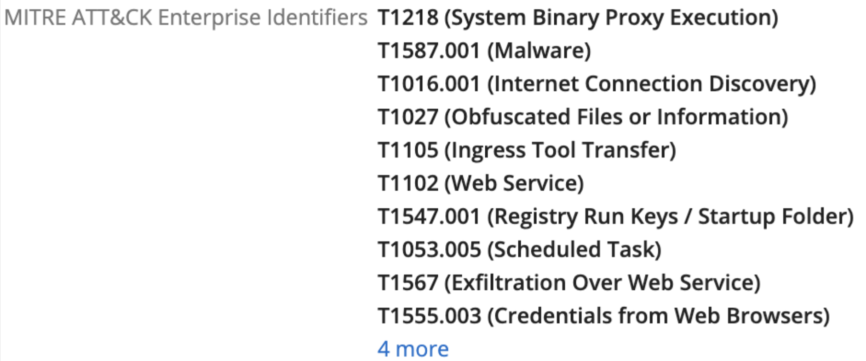
IOC vs TTPs



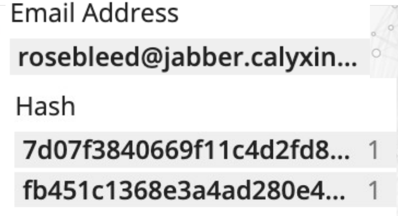
RoseBleed's dropper abuses the Living Off the Land Binary (LOLBin) **BITSAdmin** to download an additional executable file written in Go from a remote server to establish persistence. This executable file creates a registry run key to execute the dropper upon a system reboot. The dropper monitors the victim machine's internet connection and downloads a hard-coded stealer from a specified download link using a similar LOLBin technique. It then creates a scheduled task for the downloaded stealer. Additionally, the dropper periodically contacts a **Pastebin** link to check for instructions on whether it should download other files or perform a cleanup process.

RoseBleed's stealer accesses web browser data stored in the LocalAppData directory of a victim machine. It decrypts the collected data to obtain plaintext credentials, cookies, and browser history. It compresses the collected, decrypted data into a ZIP file to be exfiltrated via a **Discord** webhook or a **Telegram bot**. **RoseBleed** then performs cleanup and initiates self-destruction.





MITRE ATT&CK Enterprise Identifiers	**T1218 (System Binary Proxy Execution)** **T1587.001 (Malware)** **T1016.001 (Internet Connection Discovery)** **T1027 (Obfuscated Files or Information)** **T1105 (Ingress Tool Transfer)** **T1102 (Web Service)** **T1547.001 (Registry Run Keys / Startup Folder)** **T1053.005 (Scheduled Task)** **T1567 (Exfiltration Over Web Service)** **T1555.003 (Credentials from Web Browsers)** 4 more



Email Address

rosebleed@jabber.calyxin...

Hash

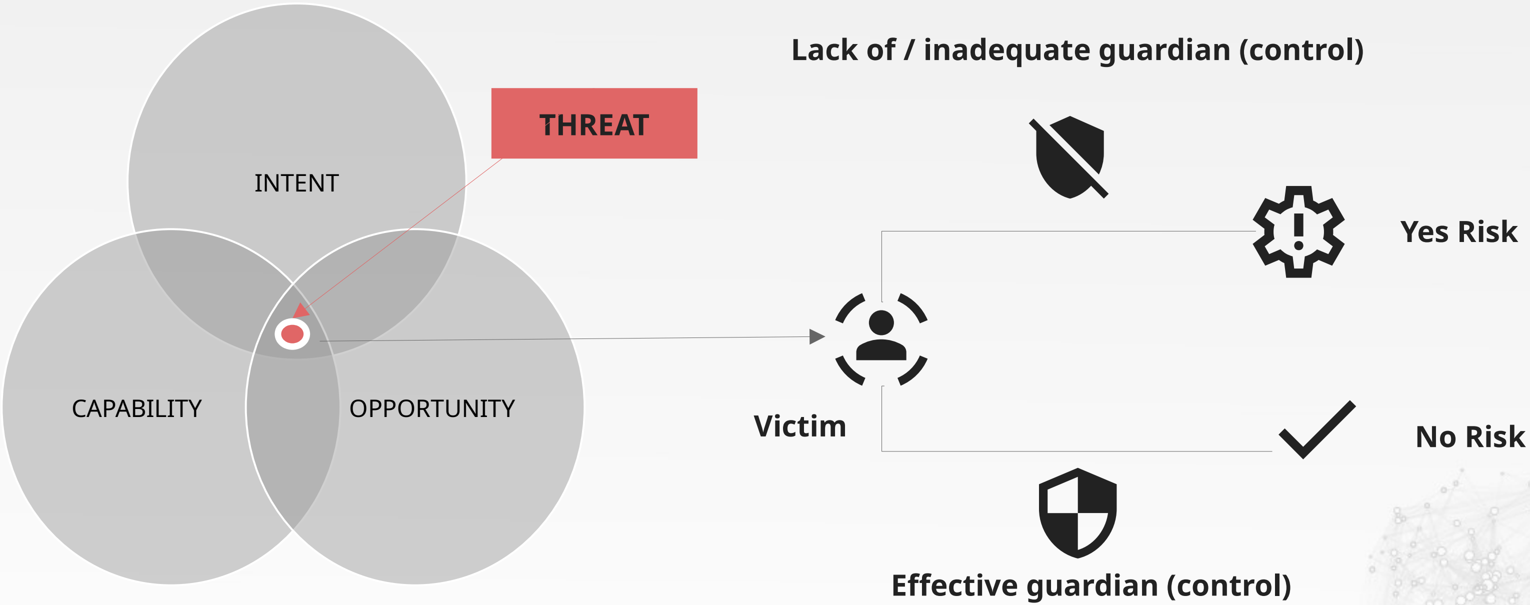
7d07f3840669f11c4d2fd8... 1

fb451c1368e3a4ad280e4... 1

Source: Pyramid of Pain: David J Bianco

Components of a threat

Threat to Risk



THREAT

INTENT

CAPABILITY

OPPORTUNITY

Lack of / inadequate guardian (control)

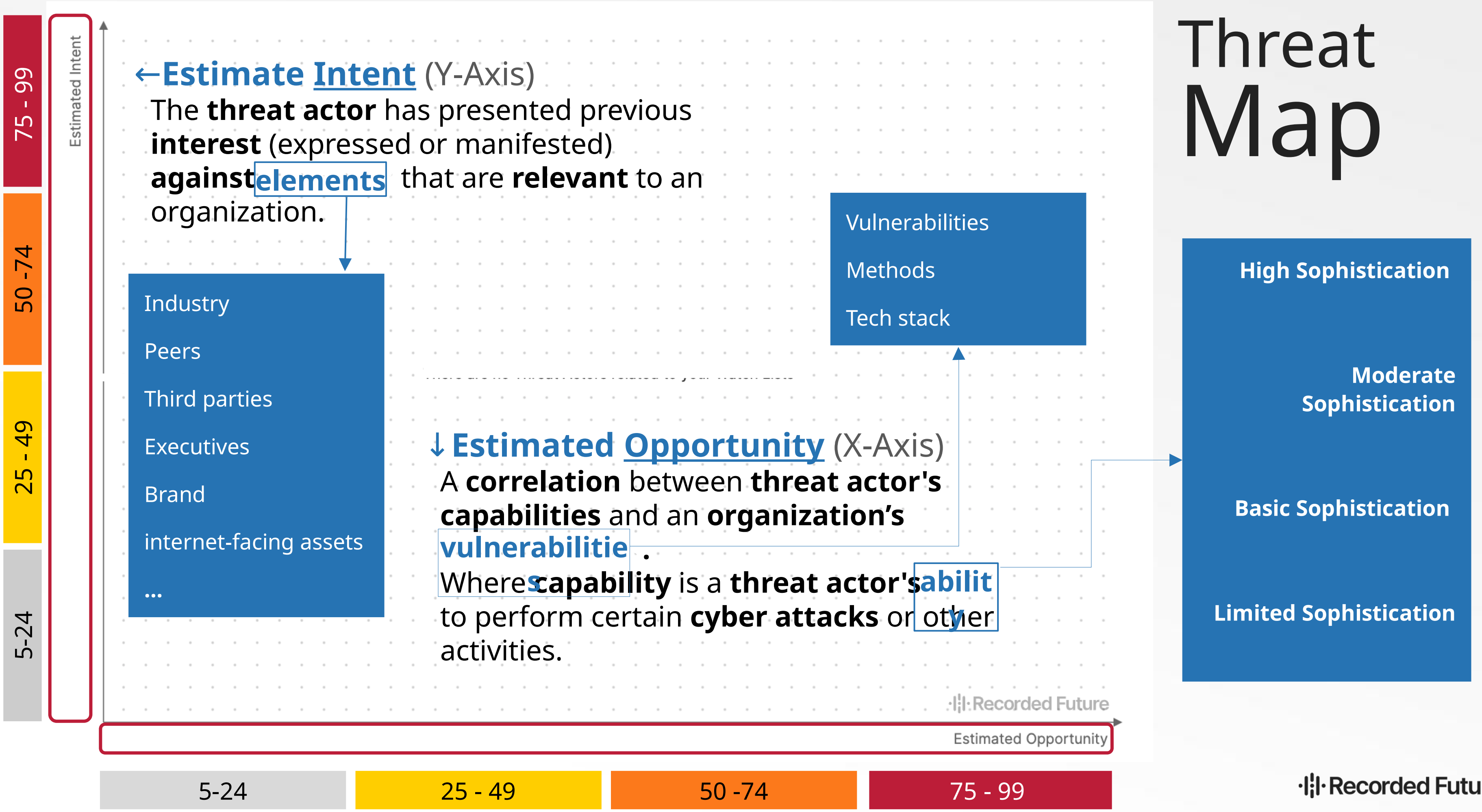
Victim

Yes Risk

No Risk

Effective guardian (control)

Threat Map



←Estimate Intent (Y-Axis)

The **threat actor** has presented previous **interest** (expressed or manifested) **against elements** that are **relevant** to an organization.

- Industry
- Peers
- Third parties
- Executives
- Brand
- internet-facing assets
- …

↓Estimated Opportunity (X-Axis)

A **correlation** between **threat actor's capabilities** and an **organization's vulnerabilities**.

Where **capability** is a **threat actor's ability** to perform certain **cyber attacks** or other activities.

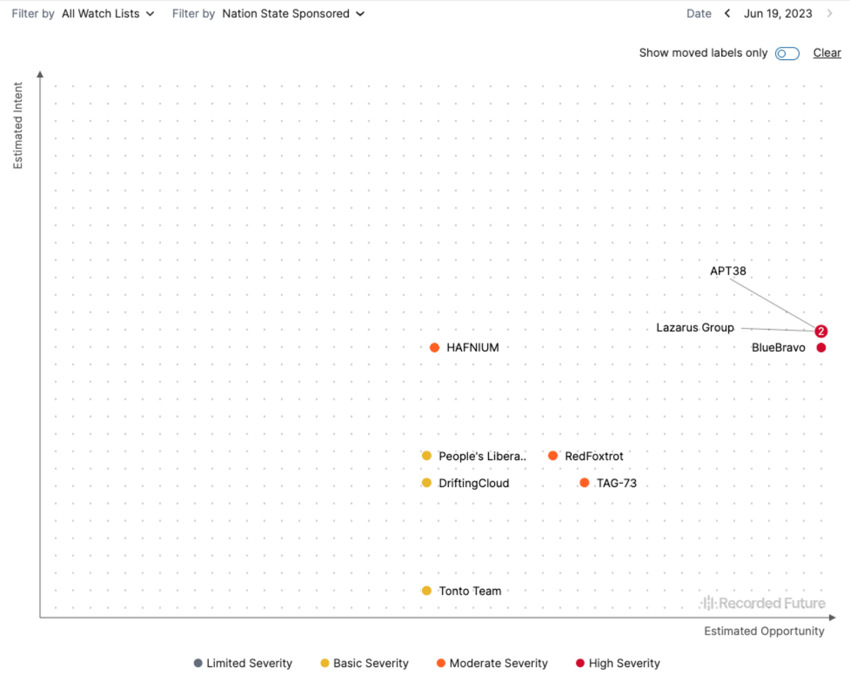
- Vulnerabilities
- Methods
- Tech stack

- High Sophistication
- Moderate Sophistication
- Basic Sophistication
- Limited Sophistication

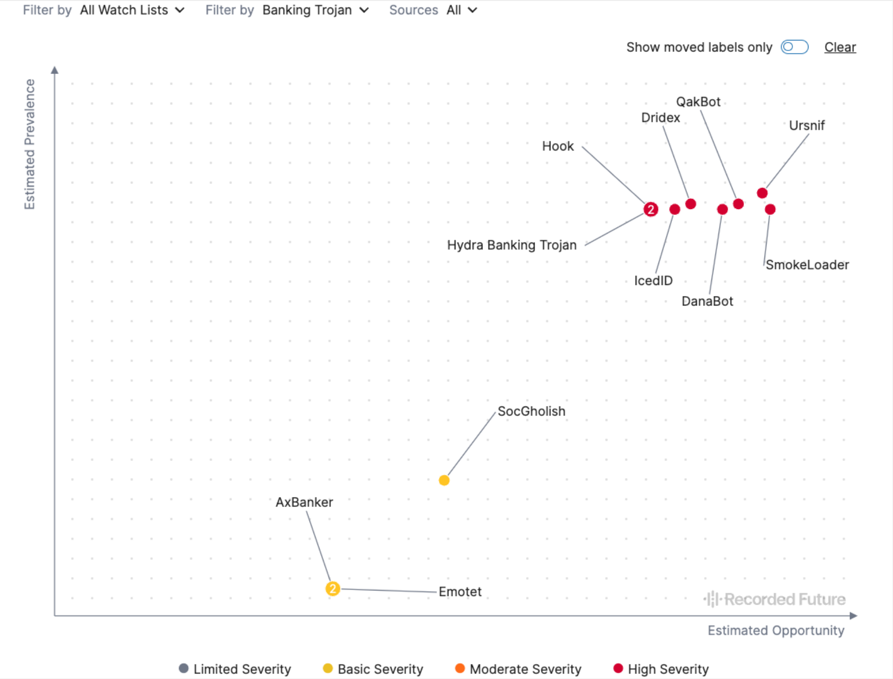
Recorded Future®

Threat Landscape with Recorded Future

Threat Actors Map



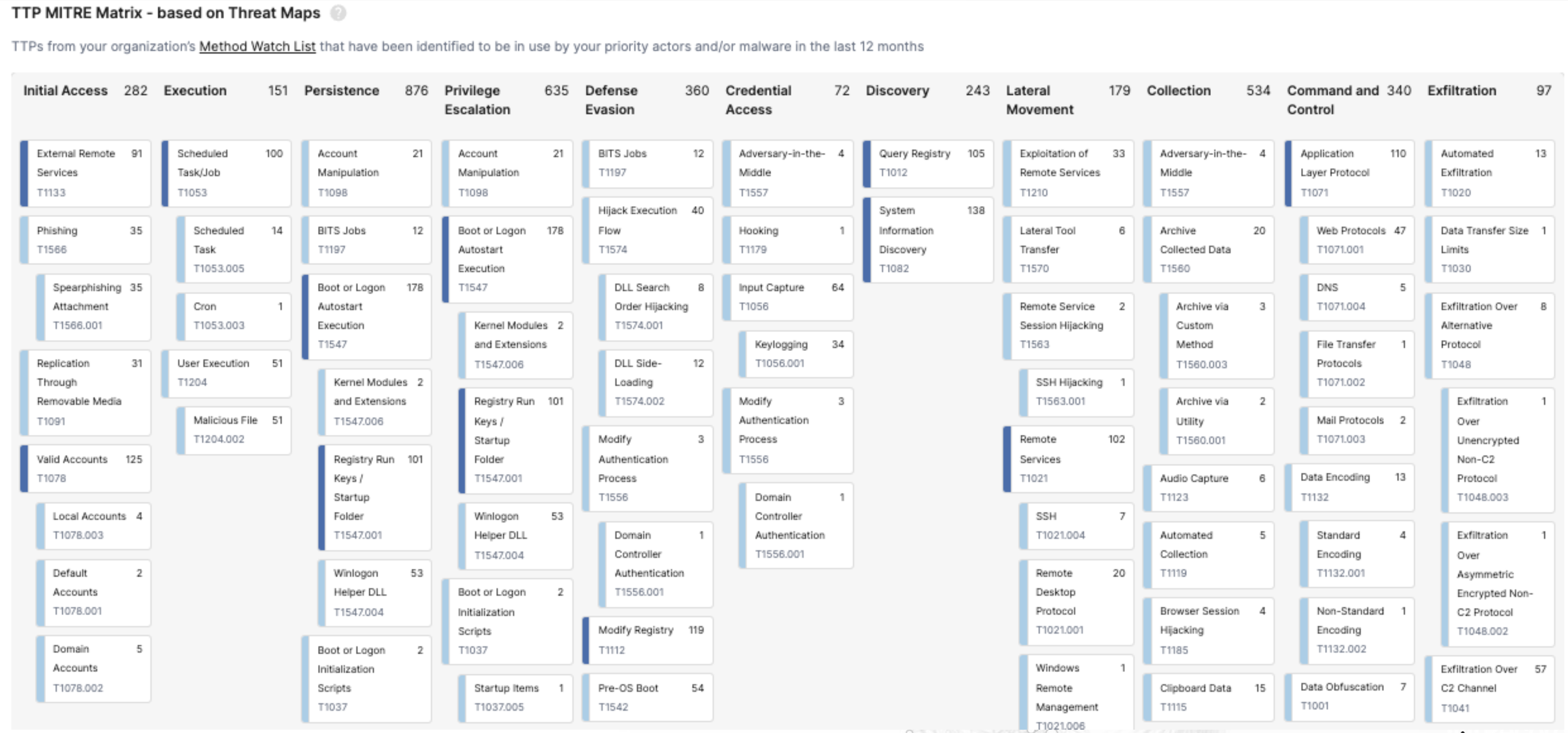
Malware Map



Source: Recorded Future Threat Maps

Threat Profiling with MITRE ATT&CK

Recorded Future allows you to aggregate adversary ATT&CK Identifiers at scale based on human analysis, technical analysis & open source collection.



TTP MITRE Matrix - based on Threat Maps

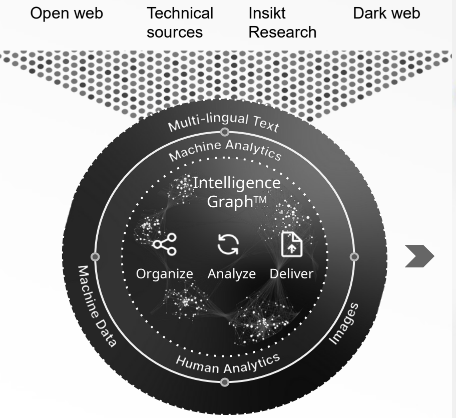
TTPs from your organization's Method Watch List that have been identified to be in use by your priority actors and/or malware in the last 12 months

Initial Access 282	Execution 151	Persistence 876	Privilege Escalation 635	Defense Evasion 360	Credential Access 72	Discovery 243	Lateral Movement 179	Collection 534	Command and Control 340	Exfiltration 97
External Remote Services 91 T1133	Scheduled Task/Job 100 T1053	Account Manipulation 21 T1098	Account Manipulation 21 T1098	BITS Jobs 12 T1197	Adversary-in-the-Middle 4 T1557	Query Registry 105 T1012	Exploitation of Remote Services 33 T1210	Adversary-in-the-Middle 4 T1557	Application Layer Protocol 110 T1071	Automated Exfiltration 13 T1020
Phishing 35 T1566	Scheduled Task 14 T1053.005	BITS Jobs 12 T1197	Boot or Logon Autostart Execution 178 T1547	Hijack Execution Flow 40 T1574	Hooking 1 T1179	System Information Discovery 138 T1082	Lateral Tool Transfer 6 T1570	Archive Collected Data 20 T1560	Web Protocols 47 T1071.001	Data Transfer Size Limits 1 T1030
Spearphishing Attachment 35 T1566.001	Cron 1 T1053.003	Boot or Logon Autostart Execution 178 T1547	Kernel Modules and Extensions 2 T1547.006	DLL Search Order Hijacking 8 T1574.001	Input Capture 64 T1056		Remote Service Session Hijacking 2 T1563	Archive via Custom Method 3 T1560.003	DNS 5 T1071.004	Exfiltration Over Alternative Protocol 8 T1048
Replication Through Removable Media 31 T1091	User Execution 51 T1204	Kernel Modules and Extensions 2 T1547.006	Registry Run Keys / Startup Folder 101 T1547.001	DLL Side-Loading 12 T1574.002	Keylogging 34 T1056.001		SSH Hijacking 1 T1563.001	Archive via Utility 2 T1560.001	File Transfer Protocols 1 T1071.002	Exfiltration Over Unencrypted Non-C2 Protocol 1 T1048.003
Valid Accounts 125 T1078	Malicious File 51 T1204.002	Registry Run Keys / Startup Folder 101 T1547.001	Winlogon Helper DLL 53 T1547.004	Modify Authentication Process 3 T1556	Modify Authentication Process 3 T1556		Remote Services 102 T1021	Audio Capture 6 T1123	Mail Protocols 2 T1071.003	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol 1 T1048.002
Local Accounts 4 T1078.003		Winlogon Helper DLL 53 T1547.004	Boot or Logon Initialization Scripts 2 T1037	Domain Controller Authentication 1 T1556.001	Domain Controller Authentication 1 T1556.001		SSH 7 T1021.004	Automated Collection 5 T1119	Data Encoding 13 T1132	Exfiltration Over C2 Channel 57 T1041
Default Accounts 2 T1078.001		Boot or Logon Initialization Scripts 2 T1037	Startup Items 1 T1037.005	Modify Registry 119 T1112			Remote Desktop Protocol 20 T1021.001	Browser Session Hijacking 4 T1185	Standard Encoding 4 T1132.001	
Domain Accounts 5 T1078.002				Pre-OS Boot 54 T1542			Windows Remote Management 1 T1021.006	Clipboard Data 15 T1115	Non-Standard Encoding 1 T1132.002	
									Data Obfuscation 7 T1001	

Source: Recorded Future Platform

Threat profiling automatization

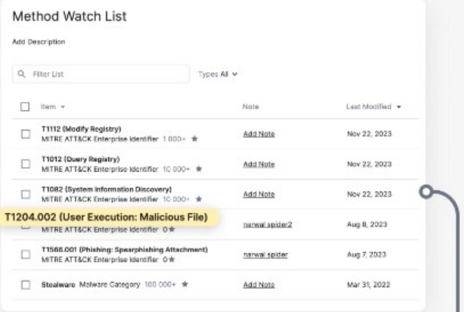
Collect->Analyze->Identify->Prioritize->Profile Threat Behavior



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



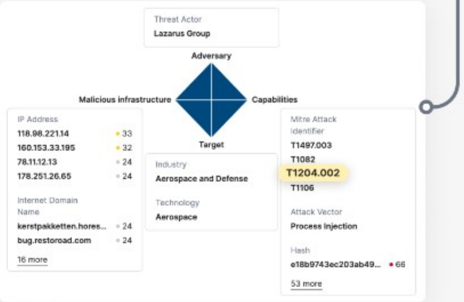
Method Watch List

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



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

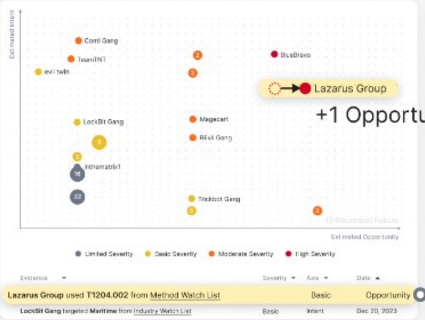
Attack Vector
Process Injection

Hash
e18b9743ec203ab49... 66

53 more

Threat Map

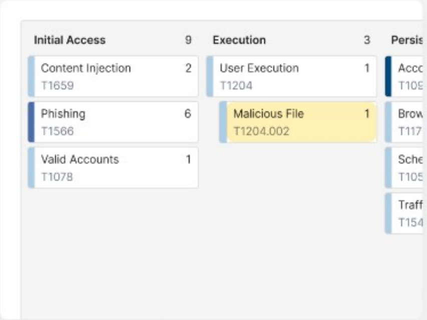
Lazarus Group's **opportunity score increases by 1**, because the threat actor used the TTP monitored in your Watch List



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 T1659	2	User Execution T1204	1	Acco T109
Phishing T1566	6	Malicious File T1204.002	1	Brow T117
Valid Accounts T1078	1			Sche T105
				Traff T154

Source: Recorded Future

Reduce Risk… Driven by Intelligence

Now What…

Control Assessments

- **Why**: understand security posture
- **How**: Red/Purple teaming to find security gaps

Detections & Mitigations

- **Why**: investment protection
- **How**: TTPs for persistent detection

Threat Hunting

- **Why**: minimize post-compromise intrusion
- **How**: proactive hunts for malicious activities

Intelligence-led security

There’s No Such Thing As Bad Weather.

Just inappropriate clothing.

Thank you

Recorded Future Free tools

https://www.recordedfuture.com/platform/browser-extension

https://go.recordedfuture.com/cyber-daily

Contact us: italy@recordedfuture.com